World Journal of Advanced Research and Reviews

eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Review Article)

Structural asymmetries in data ownership, access to information, and human rights enforcement across global digital governance regimes.

Obioma Adesewa Okonkwo *

Associate, Solomon Okedara and Co., Lagos, Nigeria.

World Journal of Advanced Research and Reviews, 2019, 04(02), 238-255

Publication history: Received on 02 December 2019; revised on 25 December 2019; accepted on 30 December 2019

Article DOI: https://doi.org/10.30574/wjarr.2019.4.2.0151

Abstract

The accelerating digital transformation of economies and societies has exposed deep structural asymmetries in data ownership, access to information, and human rights protection across global governance regimes. These asymmetries reflect unequal capacities between states, corporations, and individuals to control, interpret, and benefit from data the most valuable resource of the 21st century. From a broad perspective, disparities in digital infrastructure, legal maturity, and technological sovereignty have produced fragmented regimes where data-rich entities dominate decision-making and innovation, while data-poor nations and communities face exclusion and dependency. The concentration of control among major technology corporations further amplifies information inequalities, enabling opaque data extraction and algorithmic profiling practices that often escape meaningful accountability. At the governance level, divergent regulatory models exemplified by the European Union's rights-based General Data Protection Regulation (GDPR), the United States' market-driven framework, and China's state-centric data sovereignty approach reveal competing philosophies on digital autonomy and human rights enforcement. These differences hinder global policy coherence, complicating efforts to establish equitable standards for cross-border data flows, privacy protection, and algorithmic transparency. Narrowing the focus, this paper critically examines how this governance asymmetries influence fundamental human rights, including the right to privacy, freedom of expression, and access to knowledge. It argues that bridging these divides requires developing a globally coordinated digital rights architecture grounded in fairness, inclusivity, and accountability. Such a framework would ensure that digital governance evolves not as a vehicle of domination or exclusion but as a platform for empowering all stakeholders within the interconnected global information ecosystem.

Keywords: Data Ownership; Digital Governance; Information Asymmetry; Human Rights; Global Regulatory Regimes; Data Justice.

1. Introduction

1.1. Background and Global Context

The emergence of digital governance as a defining feature of global order represents both a technological revolution and a socio-political transformation [1]. Initially, digital systems were designed to facilitate communication and information exchange, but they have evolved into complex governance ecosystems controlling data flows, algorithms, and decision-making processes [2]. As data became the new global currency, its ownership and governance structures began to define geopolitical influence, economic power, and human autonomy [3]. Governments, corporations, and multilateral institutions now compete to define standards that determine how data is collected, processed, and protected across jurisdictions [4].

[*] Corresponding author: Obioma Adesewa Okonkwo

The historical trajectory of digital governance reflects the dual role of technology both as an instrument of empowerment and as a mechanism of control. On one hand, digital platforms have democratized access to information, promoting transparency, participation, and accountability in governance [5]. On the other, they have deepened structural inequalities through surveillance capitalism, algorithmic bias, and monopolization of data infrastructures by a few dominant entities [6]. The rise of global technology corporations has consolidated digital power in the hands of actors capable of shaping not only market dynamics but also public discourse and state sovereignty [7].

These dynamics expose the persistent asymmetry between the Global North and South, where developed economies often dictate data governance norms and standards that developing countries must adopt [8]. The control of cloud computing, cybersecurity standards, and digital platforms by a handful of transnational firms results in dependency structures that undermine national digital sovereignty. At the same time, states are increasingly deploying surveillance technologies in ways that challenge human rights protections, blurring the boundaries between national security and individual freedom [9]. Thus, digital governance today is characterized by tension between transparency and domination a paradox that determines who benefits from technological progress and who remains excluded from its opportunities.

1.2. Problem Statement and Significance

Despite the promise of digital inclusion, global data governance remains profoundly unequal [6]. Wealthy nations and multinational corporations maintain control over data infrastructures, while developing economies struggle to assert digital sovereignty or establish competitive data ecosystems [1]. This asymmetry manifests in the unequal distribution of technical expertise, access to digital markets, and regulatory influence [3]. As a result, countries with limited technological capacity become dependent on foreign platforms for communication, commerce, and public administration, effectively ceding policy autonomy in cyberspace [8].

The imbalance in data control extends beyond economics; it affects fundamental human rights such as privacy, dignity, and equality [4]. The proliferation of surveillance technologies in both democratic and authoritarian regimes has transformed data into a tool for behavioral manipulation and social engineering [5]. In many jurisdictions, individuals lack the legal means to challenge exploitative data practices or demand accountability from powerful corporate or state actors [2]. The opacity of algorithmic systems further erodes access to justice, as automated decision-making increasingly replaces human discretion in critical areas like employment, finance, and border control [9].

The fragmentation of global governance frameworks exacerbates this inequality. Divergent data protection regimes exemplified by the European Union’s GDPR, the U.S. market-driven model, and China’s state-centric approach create regulatory silos that complicate cross-border cooperation [7]. Developing nations, lacking institutional leverage, are often forced to adapt to these external models without the capacity to influence them [3]. The result is a layered system of digital dependency where rights protection and innovation are unequally distributed.

These asymmetries raise profound ethical and legal questions about fairness and accountability in the digital age [1]. The absence of an equitable governance framework threatens the universal application of human rights, while the privatization of data governance by technology companies undermines democratic control. Addressing these issues is vital not only for protecting individual freedoms but also for redefining global justice in an era where power is increasingly exercised through code, algorithms, and data infrastructures [6].

1.3. Research Objectives and Scope

The primary objective of this paper is to analyze the structural asymmetries embedded within global digital governance systems, focusing on how they affect data ownership, human rights, and state sovereignty [2]. It seeks to provide a multidisciplinary assessment that integrates perspectives from international law, ethics, and political economy to understand how governance mechanisms reinforce or mitigate digital inequality [8].

The first objective is to assess how global governance structures including treaties, regional data protection frameworks, and transnational corporate practices create hierarchies in access and control of digital resources [5]. By evaluating these structures, the paper identifies legal and institutional gaps that allow dominant actors to consolidate control over global data flows [1].

The second objective is to examine how human rights enforcement intersects with digital sovereignty [9]. This involves assessing the degree to which international human rights frameworks have adapted to digital environments and whether current legal doctrines adequately address violations stemming from algorithmic discrimination or mass surveillance [7].

The third objective is to explore the ethical and geopolitical implications of asymmetric governance. In particular, it evaluates how national and regional efforts to regulate data ownership intersect with broader questions of fairness, accountability, and digital colonialism [4].

The scope of the research is global but comparative, emphasizing the differing capacities of developed and developing economies to shape the norms of digital governance [3]. Through this analysis, the paper aims to establish an integrative framework for equitable governance that aligns technological innovation with justice, transparency, and human dignity [6].

1.4. Structure of the Paper

This paper is organized to build a comprehensive understanding of digital governance asymmetries from conceptual foundations to applied policy implications. Section 2 explores the historical evolution of digital governance, mapping the institutional, economic, and political factors that created the current asymmetrical order [5]. Section 3 examines data ownership models and their legal underpinnings, highlighting disparities in access and enforcement mechanisms between developed and developing nations [3].

Section 4 analyzes the intersection of human rights law and digital sovereignty, assessing how international frameworks address issues of privacy, surveillance, and algorithmic discrimination [8]. Section 5 evaluates case studies of regional and multilateral governance initiatives, supported by Table 1 and Figure 2, which illustrate comparative data governance approaches [4].

Section 6 synthesizes findings and proposes a framework for equitable digital governance, integrating principles of justice, accountability, and technological inclusivity [1]. Finally, Section 7 concludes with reflections on reimagining global governance to balance innovation with human rights protection [9].

The structure ensures thematic coherence and logical progression, allowing readers to move seamlessly from theoretical exploration to practical policy recommendations while maintaining a critical focus on power, inequality, and ethics in digital governance [2].

2. Theoretical foundations and conceptual frameworks

2.1. Conceptualizing Data Ownership and Sovereignty

Data ownership and sovereignty have emerged as central concepts in contemporary digital governance, reflecting deeper struggles over autonomy, control, and justice in the global information order [8]. The term *data sovereignty* refers to the principle that data generated within a nation's borders should be subject to that nation's laws and governance systems [9]. It encapsulates the idea that data, much like physical resources, constitutes a strategic national asset. However, in practice, data sovereignty is often compromised by transnational corporate infrastructures that host and process information across borders, undermining states' ability to regulate digital environments [10].

Closely related is the notion of *data commons*, which envisions information as a shared resource managed collectively for societal benefit [11]. This paradigm contrasts with privatized models that centralize ownership among a few dominant corporations. The *data commons* approach advocates for open, community-driven management of digital resources, fostering inclusivity, transparency, and equitable innovation [12]. Yet, its implementation faces resistance from powerful technology firms that profit from proprietary data control and algorithmic exclusivity [13]. These dynamics reveal how the digital economy's architecture reinforces monopolies that shape the global distribution of knowledge and economic opportunity [14].

The term *digital colonialism* further captures this imbalance, describing how developed nations and global corporations exert control over digital infrastructures, data flows, and knowledge production in ways that replicate historical patterns of colonial exploitation [15]. Through mechanisms like cloud computing dependency and intellectual property control, developing nations become consumers rather than producers in the digital economy [16]. The privatization of data resources entrenches a digital hierarchy, wherein control of information equates to control of political and economic power [17].

Ultimately, debates around data ownership and sovereignty extend beyond technical regulation they are about self-determination, identity, and justice in the digital age [9]. They challenge policymakers to balance state authority, corporate accountability, and individual autonomy within a rapidly evolving digital ecosystem [10].

2.2. Theories of Information Justice and Asymmetrical Access

The concept of *information justice* provides a philosophical lens for understanding inequalities in data access and governance. Rooted in theories of distributive and procedural justice, it advocates for fair participation in the creation, distribution, and use of information [8]. Information justice aligns with the broader pursuit of social equity, ensuring that individuals and communities benefit equitably from the digital economy [11]. It critiques the assumption that access to technology alone equates to empowerment, emphasizing that structural and institutional barriers often determine who can meaningfully engage in digital ecosystems [14].

From this perspective, asymmetrical access to digital infrastructure reflects deeper systemic inequities. Global South countries face limited access to bandwidth, cybersecurity capabilities, and AI technologies, constraining their participation in international data governance [16]. These disparities mirror long-standing economic hierarchies, where resource distribution and institutional capacity dictate digital inclusion [9]. Furthermore, language barriers, unequal representation in algorithmic datasets, and infrastructural deficits exacerbate digital marginalization [12].

Theories of information justice also emphasize participatory governance the right of affected communities to shape decisions about data collection, storage, and usage [10]. In this context, information asymmetry functions not only as an economic issue but as a democratic deficit that erodes agency and accountability [15]. While initiatives such as open data movements and digital rights advocacy have attempted to bridge this gap, the concentration of power within major technology platforms continues to distort participation [13].

Philosophically, the framework intersects with *capability theory*, which posits that justice requires expanding individuals' real freedoms to use and benefit from technology [17]. When structural asymmetries restrict access to information or exclude communities from decision-making, they violate this principle of justice [8]. Consequently, global digital governance must not only redistribute technological resources but also democratize the institutional processes that determine digital policy [14]. Addressing asymmetry, therefore, requires both technological intervention and ethical reform aimed at embedding inclusivity and fairness within digital infrastructures [11].

2.3. Human Rights Framework in Digital Context

The digital transformation of society has forced a reevaluation of how traditional human rights frameworks apply to virtual spaces [9]. Foundational instruments such as the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) provide the normative grounding for digital rights, encompassing freedoms of expression, privacy, and access to information [10]. These principles affirm that human dignity and equality extend into cyberspace, forming the ethical baseline for digital governance [12].

Regional instruments, such as the European Convention on Human Rights and the African Charter on Human and Peoples' Rights, have further contextualized these norms within local realities [13]. However, the enforcement of digital rights remains inconsistent, particularly in contexts where surveillance, censorship, and algorithmic profiling undermine human autonomy [8]. The principle of *technological neutrality* that laws should apply equally across technologies has proven inadequate in addressing the unique challenges posed by artificial intelligence, big data, and predictive analytics [15]. These technologies operate beyond traditional jurisdictional frameworks, rendering existing rights enforcement mechanisms insufficient [17].

Moreover, the privatization of governance functions by digital corporations complicates accountability structures. When data-driven decisions by non-state actors impact access to healthcare, finance, or political participation, the boundaries of state responsibility blur [16]. In such cases, human rights law must evolve to hold both state and corporate entities accountable for digital harms [11].

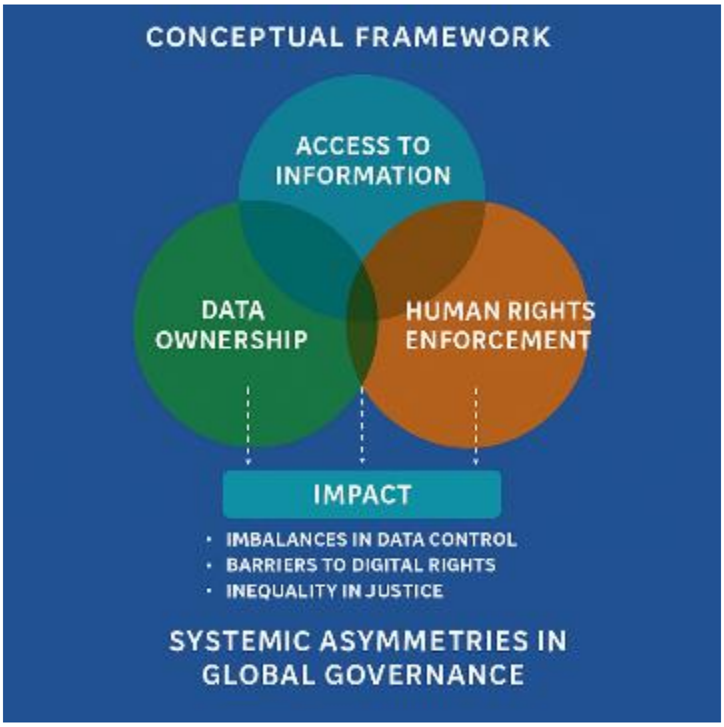


Figure 1 Conceptual framework connecting data ownership, access to information, and human rights enforcement

Figure 1 illustrates the conceptual framework connecting data ownership, access to information, and human rights enforcement. It depicts how imbalances in data control and access directly affect the realization of digital rights and justice, reinforcing systemic asymmetries within global governance [14].

Ultimately, embedding human rights principles into digital governance requires moving beyond reactive regulation toward proactive accountability frameworks that anticipate technological risks [9]. A rights-based digital order demands transparency, inclusivity, and fairness as foundational design principles, ensuring that innovation aligns with human dignity rather than undermining it [10].

3. Data ownership regimes and legal fragmentation

3.1. Western-Centric Data Protection Models

The global discourse on data protection and ownership has been largely shaped by Western frameworks, most notably the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) [16]. These two regimes exemplify contrasting philosophies the GDPR's rights-based approach prioritizes individual autonomy and privacy as fundamental rights, while the CCPA reflects a market-oriented model emphasizing consumer control within a commercial framework [17]. Together, they have redefined global expectations for data governance, yet they also expose asymmetries in regulatory influence between developed and developing economies [18].

The GDPR represents one of the most comprehensive privacy regimes, granting individuals rights such as data access, rectification, erasure, and portability [19]. Its extraterritorial scope extends beyond European borders, compelling global companies to adhere to EU privacy standards if they process data from European residents [20]. While this has elevated privacy standards worldwide, it also imposes substantial compliance burdens on organizations, particularly in developing countries with limited regulatory capacity or technical expertise [21]. The resulting imbalance highlights a form of "regulatory imperialism," where the EU's standards effectively dictate global data governance norms [22].

In contrast, the CCPA adopts a more flexible model centered on consumer choice rather than universal privacy rights [23]. It grants individuals the ability to opt out of data sales and access personal information but lacks the structural rigor of GDPR-style enforcement. Nevertheless, its influence has been significant in shaping corporate data practices, particularly within technology-heavy markets in the United States [24]. The coexistence of these frameworks one grounded in fundamental rights and the other in consumer protection reflects differing cultural and legal traditions regarding privacy and state intervention [25].

However, these Western-centric models create asymmetrical compliance obligations that disproportionately affect nations in the Global South. Smaller economies reliant on digital trade often find themselves compelled to adopt GDPR-like regulations to maintain interoperability with global data markets, even when such frameworks are misaligned with local institutional capacities [17]. Thus, the global data protection landscape reflects not merely divergent philosophies but structural inequalities in who sets the standards and who must adapt to them [19].

3.2. Emerging Economies and Data Sovereignty

In response to Western dominance in digital governance, emerging economies have begun to assert data sovereignty through localized regulatory frameworks [20]. China's Personal Information Protection Law (PIPL), India's Digital Personal Data Protection (DPDP) Act, and Africa's AU Convention on Cybersecurity and Personal Data Protection represent concerted efforts to reclaim control over domestic data ecosystems [23]. These laws signal a paradigm shift from passive compliance with global standards to proactive assertion of regional governance principles [16].

China's PIPL integrates elements of the GDPR's rights-based approach but situates them within a state-centric governance model emphasizing national security and social stability [22]. It establishes stringent requirements for cross-border data transfers, granting the Chinese government oversight of information flows to ensure they do not undermine sovereignty [25]. This reflects an approach that treats data as both an economic resource and a geopolitical instrument [17].

India's DPDP Act, meanwhile, reflects a balancing act between individual privacy and economic development [18]. Emerging from the landmark *Puttaswamy* judgment that recognized privacy as a constitutional right, the Act introduces mechanisms for user consent and accountability but allows significant governmental discretion over data processing [24]. Critics argue that this flexibility risks enabling state surveillance under the guise of regulatory efficiency, blurring the boundaries between protection and control [21].

Africa's AU Convention offers a continental framework for harmonizing data protection laws and promoting cybersecurity cooperation [19]. However, its implementation remains uneven, with many member states lacking the institutional or technical capacity to enforce its provisions effectively [16]. Data localization measures, often justified as tools of sovereignty, have also sparked debate. Proponents view them as necessary to ensure national control over data assets, while opponents caution that they may fragment the global digital economy and hinder innovation [20].

Ultimately, emerging economies' pursuit of data sovereignty illustrates an ongoing struggle to balance autonomy, development, and participation in the global digital order [23]. These efforts mark an important counterpoint to Western regulatory dominance but also reveal internal contradictions between privacy protection and state power [17].

3.3. Cross-Jurisdictional Conflicts and Enforcement Gaps

The coexistence of diverse data protection regimes has produced a fragmented global regulatory environment characterized by jurisdictional overlap and enforcement challenges [18]. As multinational corporations transfer vast quantities of data across borders, they navigate conflicting requirements related to consent, data storage, and disclosure obligations [24]. The resulting tension underscores the lack of a coherent international framework to govern transnational data flows [19].

Case studies such as the EU–U.S. Privacy Shield dispute illustrate these conflicts vividly. Following its invalidation by the Court of Justice of the European Union in the *Schrems II* decision, transatlantic data transfers were left in legal uncertainty, exposing the fragility of cross-border regulatory cooperation [22]. Similar tensions have arisen between the EU and China, where divergent security and privacy standards impede corporate interoperability [20]. These examples highlight how conflicting national interests particularly between privacy protection, economic competition, and national security complicate harmonization efforts [16].

Developing nations face an additional challenge: enforcement. Even when they adopt modern privacy laws, limited institutional capacity often prevents effective monitoring and sanctioning of violations [25]. This enforcement gap enables powerful global actors to exploit regulatory loopholes, perpetuating inequality in digital governance [17].

Table 1 provides a comparative overview of data ownership and protection frameworks across key jurisdictions the EU, USA, China, India, and Africa illustrating how diverse philosophies of privacy and sovereignty intersect with differing enforcement capabilities [21]. The table underscores that, while convergence around privacy principles exists in rhetoric, divergence in enforcement and jurisdiction remains the defining feature of global data regulation [23].

Bridging these divides requires not only legal harmonization but also political consensus on balancing innovation with rights protection [24]. Without such coordination, global data governance risks entrenching asymmetry where powerful actors dictate standards while others remain confined to reactive adaptation [18].

Table 1 Comparative Overview of Data Ownership and Protection Frameworks Across Key Jurisdictions (EU, USA, China, India, and Africa)

Jurisdiction	Core Legal Instrument(s)	Philosophical Foundation	Data Ownership & Sovereignty Approach	Enforcement Mechanisms	Key Challenges
European Union (EU)	General Data Protection Regulation (GDPR, 2018)	Fundamental rights-based model emphasizing privacy and individual autonomy.	Data viewed as an extension of personal identity; strict limits on data processing and cross-border transfer.	Centralized enforcement through national Data Protection Authorities (DPAs) and the European Data Protection Board (EDPB).	Complex compliance burden for SMEs; inconsistencies in DPA interpretation; conflicts with non-EU jurisdictions.
United States (USA)	California Consumer Privacy Act (CCPA, 2020), sectoral laws (HIPAA, COPPA).	Market-driven, consumer protection-oriented framework emphasizing corporate responsibility and self-regulation.	Data ownership implicitly tied to corporate control; limited individual sovereignty.	Enforcement by Federal Trade Commission (FTC) and state-level regulators; litigation-based remedies.	Fragmentation across states; weak federal privacy law; limited data portability and transparency rights.
China	Personal Information Protection Law (PIPL, 2021), Cybersecurity Law (2017), Data Security Law (2021).	State-centric model emphasizing national security and collective interests.	Data treated as a national resource; strong state oversight and localization requirements.	Strict administrative supervision under the Cyberspace Administration of China (CAC) with severe penalties for violations.	Ambiguity between privacy protection and state surveillance; cross-border data transfer restrictions.
India	Digital Personal Data Protection (DPDP) Act (2023).	Rights–development hybrid model balancing innovation and individual privacy.	Data ownership linked to consent; government retains discretionary powers over processing.	Enforcement via Data Protection Board of India; reliance on consent-based compliance mechanisms.	Limited institutional capacity; broad government exemptions; evolving jurisprudence on data localization.
Africa (Regional)	African Union Convention on Cybersecurity and Personal Data Protection (Malabo Convention, 2014); national laws (e.g., Nigeria's NDPA, Kenya's DPA).	Developmental and sovereignty-driven model emphasizing regional integration.	Data sovereignty tied to national security and economic development priorities.	Enforcement through national authorities; emerging regional cooperation under Smart Africa Initiative.	

4. Access to information, inequality, and algorithmic governance

4.1. The Digital Divide and Knowledge Inequality

The digital divide remains one of the most visible manifestations of structural inequality in the global information order [23]. While the early promise of the internet envisioned universal access to knowledge, the reality has been defined by persistent disparities in connectivity, digital literacy, and technological capacity [24]. These disparities not only separate nations but also fragment societies internally, distinguishing between those who can meaningfully engage with digital ecosystems and those who remain excluded [25]. Access to information, once considered a cornerstone of democratic participation, is now mediated through complex algorithmic systems that privilege visibility, engagement, and profitability over equity [26].

Regional differences in digital infrastructure exacerbate this divide. High-income countries dominate data production, AI research, and broadband connectivity, while large portions of the Global South struggle with unreliable access and prohibitive costs [27]. The consequence is a new form of knowledge inequality where data-rich regions drive policy and innovation agendas, effectively marginalizing those unable to participate [28]. Institutions in developing nations often rely on digital infrastructures owned and controlled by Western corporations, leading to dependencies that mirror historical patterns of economic colonialism [29].

Furthermore, the rise of algorithmic curation systems has deepened informational asymmetry. Algorithms determine which information is seen, prioritized, or suppressed shaping public discourse and access to opportunities [30]. Those without technical literacy or representation in algorithmic design face systemic invisibility, where their voices are underrepresented or mischaracterized within digital platforms [31]. The algorithmic bias embedded within search engines, recommendation systems, and social media feeds amplifies existing social hierarchies, reinforcing structural inequalities under the guise of neutrality [23].

Knowledge inequality is thus both a technical and political construct. It reflects unequal participation in the production, validation, and dissemination of knowledge across digital architectures [24]. Bridging this divide requires not just infrastructural investment but also the democratization of data access, algorithmic transparency, and participatory design that centers the rights and agency of digitally marginalized populations [27].

4.2. Algorithmic Transparency and Epistemic Asymmetry

Algorithmic systems now perform functions that were once reserved for human judgment, influencing critical decisions in employment, credit scoring, healthcare, and criminal justice [26]. However, their increasing opacity poses significant challenges to accountability and fairness [25]. The concept of *epistemic asymmetry* captures this imbalance the growing gap between those who design and control algorithms and those subjected to their outcomes [29]. When algorithms operate as “black boxes,” affected individuals lack the information necessary to contest decisions or understand their rationale [23].

Transparency in algorithmic governance is thus a matter of rights enforcement, closely linked to due process and access to information [28]. Yet, full transparency remains elusive because algorithmic models often rely on proprietary technologies protected by trade secrets [31]. This tension between public accountability and corporate confidentiality has created a paradox: the very systems governing social and economic life are shielded from scrutiny under intellectual property law [24].

Attempts to address algorithmic opacity have produced frameworks such as the European Union’s proposed *AI Act* and the U.S. *Algorithmic Accountability Act* [27]. These initiatives seek to impose obligations for explainability, impact assessments, and human oversight, but they also face limitations in scope and enforcement [30]. The challenge lies in operationalizing transparency without undermining innovation or exposing sensitive intellectual property [25].

Moreover, epistemic asymmetry reinforces structural inequalities in digital governance. Those with access to data and technical expertise wield disproportionate influence over decision-making processes, while marginalized groups are relegated to passive roles as data subjects rather than active participants [26]. The opacity of algorithmic decision-making perpetuates biases that disproportionately harm vulnerable populations from racial profiling in predictive policing to discriminatory outcomes in credit algorithms [29].

Ultimately, algorithmic transparency must move beyond disclosure toward interpretability and accountability [31]. It demands mechanisms that empower individuals to understand, contest, and influence algorithmic outcomes while holding both public and private actors responsible for ethical AI design and deployment [24].

4.3. Data Intermediaries and Platform Governance

Digital platforms have evolved into powerful intermediaries that structure how information is produced, accessed, and monetized globally [25]. Big Tech corporations including Meta, Alphabet, Amazon, and Tencent now function as de facto regulators, establishing private governance regimes that transcend national boundaries [23]. Their dominance derives from control over data flows, user attention, and algorithmic infrastructure, positioning them as both gatekeepers of knowledge and arbiters of digital rights [27].

This monopolization of information channels creates profound implications for democratic participation and human rights enforcement [30]. Platforms determine the visibility of content through recommendation systems, thereby influencing political discourse, market behavior, and cultural narratives [28]. The concentration of informational power in corporate hands undermines state sovereignty and public accountability, as major platforms often operate outside the effective jurisdiction of national regulators [24].

The proliferation of misinformation and algorithmically amplified disinformation has further exposed the fragility of current governance models [29]. While content moderation policies aim to curb harmful information, their implementation often lacks transparency, resulting in arbitrary enforcement and suppression of legitimate expression [26]. This dual role of platforms as both enablers of communication and gatekeepers of content illustrates the tension between freedom of expression and the responsibility to prevent harm [31].

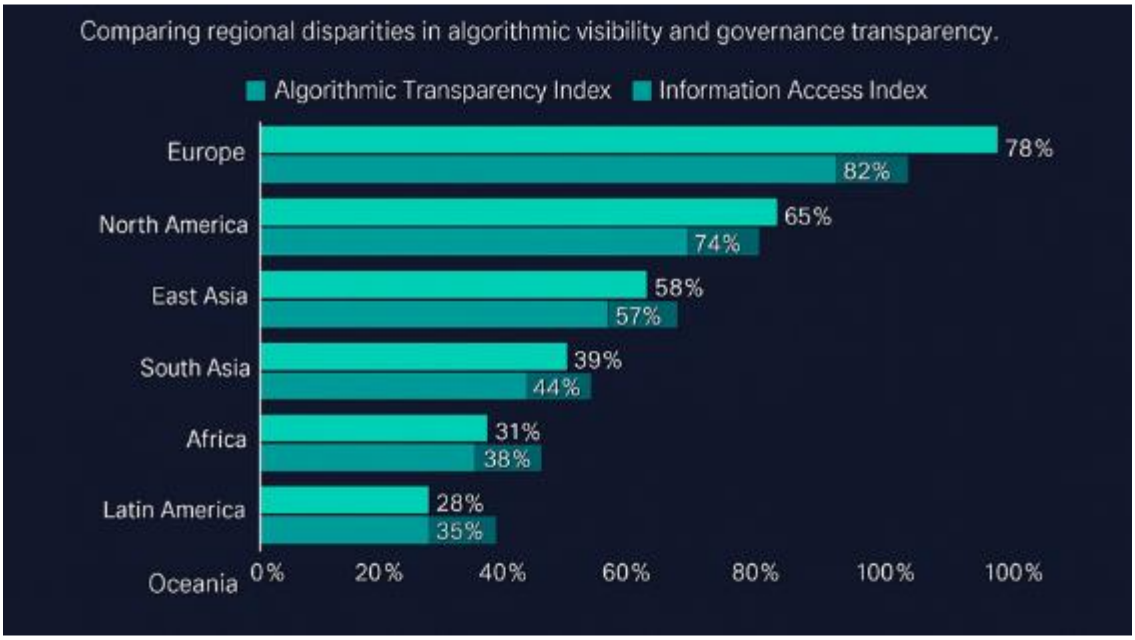


Figure 2 Global distribution of algorithmic transparency and information access index

Efforts to regulate digital intermediaries vary widely across jurisdictions. The European Union's *Digital Services Act (DSA)* and *Digital Markets Act (DMA)* represent attempts to impose accountability obligations on dominant platforms, including transparency in advertising and content moderation practices [27]. However, similar frameworks are lacking in many regions, particularly within the Global South, where weak regulatory institutions allow unchecked corporate influence [23].

Figure 2, titled *Global Distribution of Algorithmic Transparency and Information Access Index [7]*, visualizes disparities in data visibility and governance transparency across regions, underscoring how concentration of digital intermediaries perpetuates informational inequality [25]. The figure highlights that regions with high transparency scores often coincide with strong institutional oversight and legal safeguards, whereas low-scoring regions reflect dependency on foreign platforms and opaque governance structures [30].

To promote equitable digital governance, reforms must prioritize redistributing informational power and enhancing accountability mechanisms for intermediaries [28]. Transparent auditing, open algorithms, and multi-stakeholder governance models can help ensure that platforms operate in alignment with democratic principles rather than monopolistic interests [26].

5. Human rights enforcement and global digital governance

5.1. Digital Rights as Human Rights

The recognition of digital rights as an extension of fundamental human rights marks a pivotal transformation in international law and governance [27]. As digital technologies permeate every dimension of human activity, principles of privacy, freedom of expression, and access to information have evolved into essential safeguards for digital citizenship [28]. The United Nations General Assembly (UNGA) and the Human Rights Council (HRC) have explicitly affirmed that "the same rights that people have offline must also be protected online," establishing a legal and moral foundation for digital rights enforcement [29].

Privacy is now widely regarded as a cornerstone of human dignity and autonomy in the digital sphere. The proliferation of mass surveillance systems, data mining, and behavioral profiling has intensified global debates over the limits of state and corporate power [30]. Instruments such as the International Covenant on Civil and Political Rights (ICCPR) and the Universal Declaration of Human Rights (UDHR) enshrine the right to privacy, yet their application in cyberspace remains fragmented and inconsistent [31]. The exponential growth of artificial intelligence, facial recognition, and predictive analytics technologies challenges these traditional frameworks, requiring a redefinition of the boundaries between legitimate data use and privacy intrusion [32].

Similarly, freedom of expression has acquired new dimensions in the digital era. Platforms like social media, search engines, and digital publishing outlets have become primary arenas for civic engagement and dissent [33]. However, these same platforms have also facilitated censorship, algorithmic filtering, and disinformation at unprecedented scales [34]. The UN Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression has repeatedly warned that digital intermediaries must not act as arbiters of truth without transparent governance mechanisms [35].

Access to information once tied to physical and educational infrastructures is now a determinant of equality in the digital economy [36]. Unequal access to networks, knowledge, and data undermines social inclusion and exacerbates global inequality. As digital rights gain recognition as human rights, their enforcement depends increasingly on multi-level governance that integrates international law, domestic regulation, and corporate accountability [37].

5.2. Extraterritoriality, Accountability, and Corporate Responsibility

The cross-border nature of digital ecosystems complicates the attribution of responsibility among states, corporations, and individuals [28]. Extraterritoriality the principle that human rights obligations may extend beyond national borders has become central to addressing abuses committed by multinational technology corporations operating globally [30]. Yet, enforcement mechanisms remain weak and inconsistent, creating accountability vacuums that enable rights violations to persist unchecked [27].

Corporations that control digital infrastructures wield unprecedented power over personal data, communications, and knowledge distribution [32]. Their decisions from algorithmic design to content moderation directly affect freedom of expression, privacy, and due process [31]. The UN Guiding Principles on Business and Human Rights (UNGPs) outline the corporate responsibility to respect human rights and exercise due diligence, but compliance remains largely voluntary [34]. Many companies adopt self-regulatory codes that lack independent oversight, leading to selective accountability based on reputational risk rather than ethical obligation [33].

Emerging legislative instruments such as the EU's Digital Services Act (DSA), the Corporate Sustainability Due Diligence Directive (CSDDD), and similar proposals in other jurisdictions seek to formalize corporate accountability for human rights impacts in digital contexts [35]. These frameworks introduce obligations for risk assessment, transparency reporting, and stakeholder engagement, effectively integrating human rights principles into the governance of digital enterprises [29].

However, enforcement across borders poses formidable challenges. Companies headquartered in one jurisdiction often operate under different, sometimes conflicting, legal standards elsewhere [37]. For example, U.S.-based technology giants are bound by domestic constitutional protections of free speech that differ markedly from European privacy expectations under the General Data Protection Regulation (GDPR) [28]. The result is a fragmented accountability landscape in which the same corporate action may be lawful in one jurisdiction and a violation in another [31].

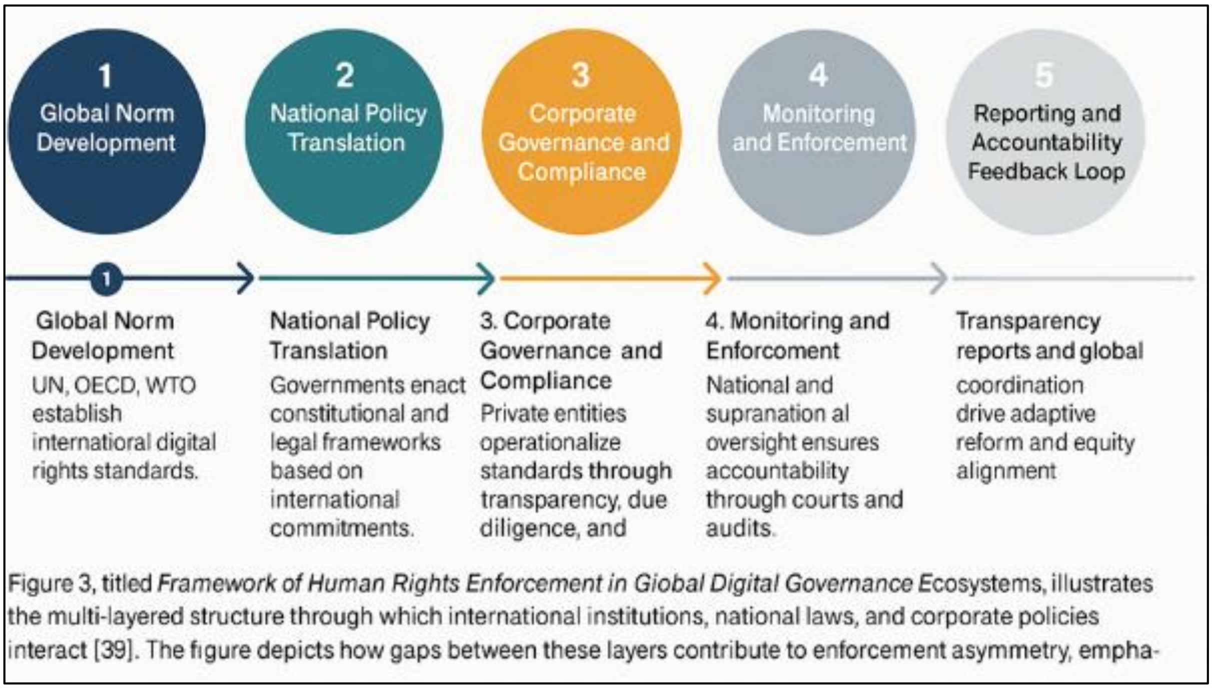
To bridge these asymmetries, scholars advocate for the establishment of international digital accountability mechanisms under the auspices of the United Nations or OECD, capable of adjudicating transnational digital rights disputes [39]. Such institutions would help harmonize corporate obligations and strengthen global governance of human rights in the digital era [33].

5.3. Enforcement Asymmetries Across Regions

Despite widespread recognition of digital rights, enforcement remains uneven across jurisdictions, reflecting varying institutional capacities and political priorities [36]. In Europe, the European Court of Human Rights (ECHR) and the Court of Justice of the European Union (CJEU) have emerged as key venues for adjudicating digital rights disputes [28]. Landmark cases such as *Google Spain SL v. AEPD* established the “right to be forgotten,” reinforcing data subject autonomy and setting precedents for balancing privacy and freedom of information [30].

By contrast, the United States continues to prioritize free expression and innovation over strict privacy enforcement [27]. The First Amendment tradition shapes judicial reluctance to impose content restrictions or grant expansive data protection rights [31]. Courts often defer to private sector self-regulation, resulting in fragmented enforcement and inconsistent protection for users across platforms [32]. This divergence underscores fundamental philosophical differences between rights-based and market-based approaches to governance [35].

In the Asia-Pacific region, enforcement mechanisms remain nascent. The ASEAN Framework on Personal Data Protection promotes regional cooperation but lacks binding force [33]. Similarly, many African and Latin American jurisdictions face enforcement challenges due to limited institutional resources and political instability [38]. These asymmetries create an uneven global terrain where the effectiveness of human rights protection depends heavily on geography, legal infrastructure, and state capacity [29].


1
Global Norm Development
2
National Policy Translation
3
Corporate Governance and Compliance
4
Monitoring and Enforcement
5
Reporting and Accountability Feedback Loop
1

Global Norm Development
UN, OECD, WTO establish internatioral digital rights standards.

National Policy Translation
Governments enact constitutional and legal frameworks based on international commitments.

3. Corporate Governance and Compliance
Private entities operationalize standards through transparency, due diligence, and

4. Monitoring and Enforcement
National and supranation al oversight ensures accountability through courts and audits.

Transparency reports and global coordination drive adaptive reform and equity alignment

Figure 3, titled *Framework of Human Rights Enforcement in Global Digital Governance* Ecosystems, illustrates the multi-layered structure through which international institutions, national laws, and corporate policies interact [39]. The figure depicts how gaps between these layers contribute to enforcement asymmetry, empha-

Figure 3 Framework of human rights enforcement in global digital governance ecosystem

Figure 3, titled *Framework of Human Rights Enforcement in Global Digital Governance Ecosystems*, illustrates the multi-layered structure through which international institutions, national laws, and corporate policies interact [39]. The figure depicts how gaps between these layers contribute to enforcement asymmetry, emphasizing the need for integrated oversight mechanisms that align global standards with local realities [34].

Ultimately, the fragmentation of digital rights enforcement undermines both legal certainty and public trust [30]. Bridging these gaps requires the establishment of interoperable frameworks that ensure consistent protection irrespective of jurisdiction or corporate influence [36].

6. Comparative analysis and structural implications

6.1. North–South Divide in Data Governance

The global digital landscape remains divided along geopolitical and economic lines, reflecting persistent North–South inequalities in technological capacity, data infrastructure, and policy development [36]. High-income countries in the Global North have established advanced digital governance systems supported by robust regulatory frameworks, institutional resources, and technological expertise [37]. In contrast, many developing nations rely heavily on imported digital infrastructure and foreign platforms, resulting in asymmetric dependencies that limit autonomy over data governance [38].

This dependency perpetuates a digital form of economic colonialism, where Western corporations dominate the flow, storage, and monetization of information [39]. The imbalance constrains the ability of developing economies to assert sovereignty over their citizens' data and to participate equitably in global digital trade [40]. As data becomes a strategic resource, the lack of indigenous infrastructure such as data centers, cybersecurity frameworks, and AI governance systems reinforces economic subordination [41].

Policy misalignment further widens this divide. While the European Union and United States set global privacy and data standards, most Global South nations are relegated to policy takers rather than policy makers [42]. As a result, local regulations often mirror foreign models like the GDPR without sufficient adaptation to domestic legal, cultural, or institutional realities [43]. The outcome is a patchwork of laws that appear comprehensive on paper but lack effective enforcement or contextual relevance [44].

Bridging this divide requires strengthening regional digital alliances and investing in capacity building for governance institutions [45]. Without equitable participation in global rule-making, the North–South divide will continue to shape data governance as an instrument of power rather than a mechanism for justice [37].

6.2. Institutional Fragmentation and Regulatory Capture

Institutional fragmentation has emerged as one of the most pressing obstacles to equitable digital governance [38]. The proliferation of overlapping national and international regulations has created a fragmented policy environment, where enforcement gaps and jurisdictional inconsistencies allow corporate actors to exploit loopholes [36]. Multinational technology companies often engage in regulatory arbitrage, relocating operations or data centers to jurisdictions with weaker oversight or lower compliance requirements [39]. This practice undermines the effectiveness of existing regulations and shifts accountability away from users and communities [40].

Regulatory capture compounds the problem. In many jurisdictions, powerful corporate lobbies influence policy formulation, diluting the rigor of data protection laws and promoting self-regulatory mechanisms that prioritize commercial interests over public welfare [42]. The reliance on *soft law* non-binding principles, codes of conduct, and voluntary frameworks allows corporations to portray compliance without undergoing substantive behavioral change [43]. This veneer of accountability conceals the persistence of asymmetry in data access, ownership, and control [44].

Institutional fragmentation is further exacerbated by the absence of a coherent global governance body for digital regulation [45]. While institutions such as the OECD, G20, and United Nations have advanced guiding principles, these remain advisory rather than mandatory [41]. Consequently, disparities in enforcement and legal interpretation continue to proliferate, leaving developing states vulnerable to digital exploitation [37].

Addressing fragmentation requires harmonization at both institutional and policy levels. The creation of interoperable governance standards, cross-border enforcement mechanisms, and inclusive negotiation platforms could prevent corporate dominance from overwhelming public interest [39]. Without such systemic reform, digital governance will remain stratified along lines of power and profit [40].

6.3. Human-Centered and Equitable Governance Framework

To counterbalance existing asymmetries, a shift toward *human-centered and equitable governance* is essential [36]. This approach prioritizes inclusivity, transparency, and fairness as foundational principles for regulating digital ecosystems

[38]. Rather than treating data solely as an economic asset, governance frameworks must recognize it as a collective good linked to human rights and social justice [42]. Such recognition would enable the development of multi-stakeholder models that balance state authority, corporate accountability, and citizen participation [37].

A sustainable digital governance framework requires cooperation between international institutions, regional bodies, and local stakeholders [41]. Collaborative initiatives, such as the African Union Data Policy Framework and the OECD's Global Forum on Technology, provide emerging blueprints for multi-level governance coordination [43]. Embedding ethical standards and transparency mechanisms within these frameworks can ensure that regulatory harmonization does not replicate existing hierarchies but instead empowers marginalized actors in the digital space [40].

Equitable governance also demands robust monitoring mechanisms. Independent oversight bodies equipped with enforcement powers can safeguard against corporate overreach and ensure the equitable distribution of digital dividends [45]. Moreover, adopting universal data-sharing principles akin to environmental sustainability norms can promote fairness in the global digital economy [39].

Table 2, titled *Comparative Matrix of Governance Asymmetries: Institutional Strength, Enforcement Mechanisms, and Data Equity Metrics*, summarizes the disparities in institutional design and regulatory enforcement across key regions [44]. It highlights how countries with strong legal infrastructures and participatory governance frameworks achieve higher data equity outcomes than those relying on ad hoc or voluntary measures [42].

Ultimately, building an equitable governance ecosystem requires integrating ethics with policy ensuring that technological progress advances human dignity, not inequality [38].

Table 2 Comparative Matrix of Governance Asymmetries — Institutional Strength, Enforcement Mechanisms, and Data Equity Metrics

Region / Jurisdiction	**Institutional Strength**	**Regulatory Enforcement Mechanisms**	**Data Equity Metrics**	**Key Observations**
European Union (EU)	Highly institutionalized, with multi-level coordination among the European Commission, EDPB, and national DPAs.	Strongly codified under GDPR; cross-border cooperation; administrative fines and judicial oversight.	High — strong user rights, high transparency standards, and measurable redress mechanisms.	Consistent enforcement but bureaucratically slow; significant influence on global privacy norms.
United States (USA)	Fragmented institutions with overlapping state and federal jurisdictions; heavy reliance on private sector initiatives.	Enforcement through FTC and state-level actions; primarily reactive rather than preventive.	Moderate — consumer protection focus without comprehensive data ownership rights.	Innovation-led ecosystem prioritizes market freedom over equity; limited redress for users.
China	Centralized and state-controlled with vertical regulatory oversight through CAC and related ministries.	Strict administrative enforcement with national security orientation; data localization and content monitoring.	Low to Moderate — strong sovereignty protection but limited user autonomy and transparency.	Governance prioritizes control and national security over participatory rights.
India	Emerging institutional frameworks under the DPDP Act; growing oversight but limited capacity.	Quasi-independent Data Protection Board; consent-driven enforcement with government exemptions.	Moderate — advancing privacy awareness but constrained by infrastructural and legal maturity.	Rapidly evolving but faces enforcement inconsistency and administrative challenges.
Africa (Regional Overview)	Developing institutions with varied national maturity; increasing regional cooperation via	Weak to moderate enforcement; dependent on donor support and regional	Low — uneven access to digital resources and	Governance asymmetry rooted in infrastructural

	Smart Africa and AU frameworks.	harmonization efforts.	fragmented legislative adoption.	inequality and limited legal capacity.
Asia-Pacific (Japan, South Korea, Singapore)	Well-structured regulatory systems balancing innovation and user rights.	Independent oversight agencies with proactive enforcement; frequent cross-border cooperation.	High — clear consent rules, accountability standards, and user protection frameworks.	Exemplary hybrid models combining data protection, economic innovation, and equity.

7. Toward a framework for equitable global digital governance

7.1. Policy Convergence and Global Harmonization

The pursuit of global harmonization in digital governance represents both an urgent necessity and an enduring challenge [41]. Fragmented regulatory regimes have produced inconsistencies that undermine the effectiveness of privacy protection, data transfer rules, and algorithmic accountability frameworks [42]. Achieving interoperability among major international institutions including the Organisation for Economic Co-operation and Development (OECD), the United Nations (UN), and the World Trade Organization (WTO) is vital to establishing coherent standards that balance innovation with human rights protections [43]. These institutions hold distinct yet complementary mandates: the OECD promotes policy coherence and digital best practices, the UN emphasizes human rights and sustainable development, while the WTO governs cross-border trade and digital commerce [44]. Coordinating these efforts can reduce regulatory asymmetries and enable fairer participation by developing economies [45].

However, traditional treaty-making mechanisms often fail to keep pace with technological change. As a result, *soft law* instruments non-binding guidelines, codes of conduct, and voluntary frameworks have become essential tools for flexible governance [46]. Instruments such as the OECD AI Principles, the UN Secretary-General's Roadmap for Digital Cooperation, and the G20 AI Principles provide frameworks for collaboration without imposing rigid obligations [47]. Though their non-binding nature can limit enforcement, they encourage norm diffusion and facilitate gradual convergence across jurisdictions [48].

Regional data partnerships have also emerged as pragmatic vehicles for harmonization. Initiatives like the African Continental Free Trade Area (AfCFTA) Digital Protocol, the EU–Japan Adequacy Agreement, and the ASEAN Data Management Framework demonstrate how cooperative regional instruments can align standards while respecting local contexts [49]. By fostering trust and interoperability, these partnerships can serve as precursors to global consensus on digital governance [50].

Nevertheless, genuine harmonization requires moving beyond procedural alignment toward substantive equity. Policymakers must embed fairness, transparency, and accountability as universal norms within any global governance architecture [44]. Only through this multidimensional convergence can digital governance evolve into an inclusive system that promotes both innovation and justice [46].

7.2. Reinforcing Human Rights Through Data Justice

The notion of *data justice* provides a transformative lens for reconciling technological advancement with social equity [43]. Rooted in principles of fairness, inclusivity, and accountability, data justice emphasizes the redistribution of informational power and the protection of digital rights as integral to human rights enforcement [47]. This framework recognizes that inequities in data ownership and governance mirror broader social injustices, including economic marginalization and structural discrimination [45].

Integrating data justice into policy requires redefining the objectives of digital governance from mere compliance to empowerment [49]. Governments and corporations must commit to transparency mechanisms that reveal how data are collected, processed, and monetized [42]. Initiatives such as algorithmic impact assessments, open auditing systems, and participatory policy consultations can enhance accountability and ensure that governance decisions reflect diverse stakeholder perspectives [46].

Equity and fairness must also be operationalized through inclusive institutional design. Policies should prioritize accessibility for marginalized groups, including women, minorities, and developing regions, who remain disproportionately excluded from digital economies [48]. Furthermore, ethical frameworks for artificial intelligence and data governance should align with international human rights instruments, ensuring that technology development reinforces rather than undermines social justice [50].

By situating human rights at the heart of digital governance, data justice transcends the binary of innovation versus regulation [41]. It offers a holistic approach that acknowledges technology's capacity to both empower and oppress, urging policymakers to design governance structures that safeguard dignity, equity, and democratic participation [44].

7.3. Proposed Global Framework for Data Rights Governance

The proposed *Global Framework for Data Rights Governance* envisions a hybrid model that balances innovation, regulation, and justice within a unified institutional structure [47]. This framework integrates three interdependent pillars: ethical oversight, legal harmonization, and technological accountability [41]. Ethical oversight ensures that digital systems adhere to universal values of fairness and transparency, while legal harmonization promotes interoperability among national and regional data regimes [43]. Technological accountability mandates that corporations and governments remain answerable for algorithmic and data-related impacts on individuals and communities [45].

The framework advocates a multi-stakeholder governance architecture in which governments, civil society, academia, and private actors collaborate to shape digital policy [50]. Such inclusivity fosters legitimacy and responsiveness in global rule-making processes [42]. Additionally, it introduces a global monitoring mechanism under the UN Digital Cooperation Council, designed to evaluate compliance with human rights standards and data equity metrics across jurisdictions [46].

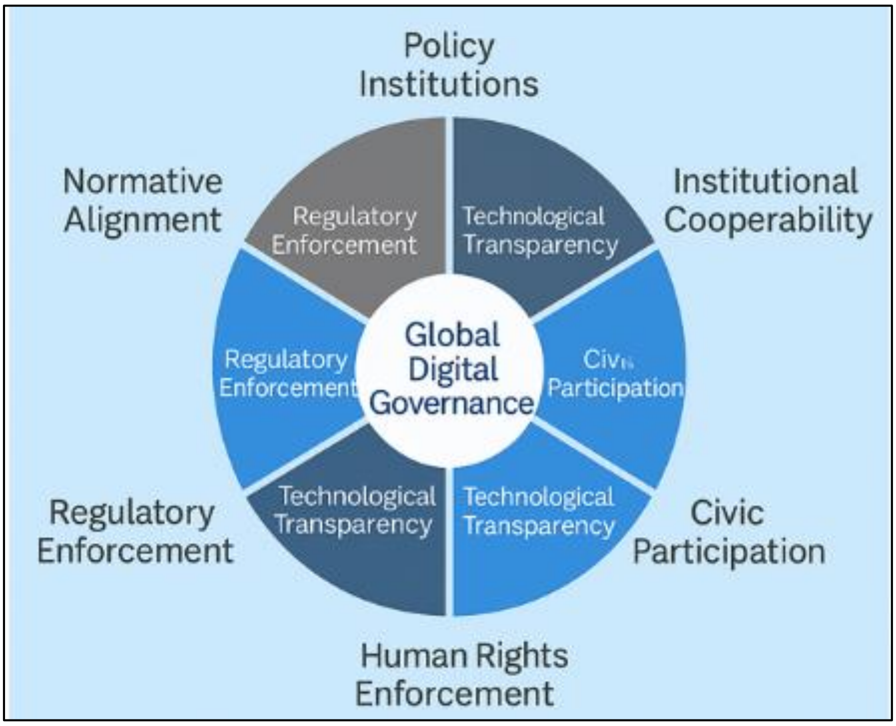


Figure 4 Proposed Model for Equitable Global Digital Governance and Human Rights Enforcement

Figure 4, titled *Proposed Model for Equitable Global Digital Governance and Human Rights Enforcement*, visualizes this structure as an interconnected system linking policy institutions, corporate accountability frameworks, and human rights enforcement mechanisms [49]. It illustrates how normative alignment, institutional cooperation, and technological transparency can collectively sustain equitable digital ecosystems [44].

Ultimately, the framework aspires to transform digital governance into an ethical infrastructure of shared responsibility ensuring that innovation serves humanity's collective good rather than reinforcing systemic inequality [48].

8. Conclusion

The analysis of structural asymmetries in global data governance reveals a complex web of legal, institutional, and ethical disparities that continue to define the digital order. Data has emerged as both an economic asset and a fundamental element of human identity, yet its governance remains deeply uneven across regions and institutions. The investigation highlights how the concentration of digital infrastructure and policymaking power in the Global North reinforces systemic inequalities, marginalizing the Global South and perpetuating a cycle of dependency. These asymmetries are not only technological but also ideological, reflecting differing values about privacy, sovereignty, and the role of the state in regulating digital ecosystems.

A central finding of this study is that digital governance is inseparable from human dignity. The commodification of personal data, expansion of algorithmic surveillance, and privatization of information flows challenge the very principles of autonomy and self-determination that underpin modern human rights. Data sovereignty once seen as a geopolitical objective has evolved into a moral imperative, demanding that nations and individuals alike regain agency over how their information is collected, processed, and utilized. The intersection between data rights and sovereignty thus reflects a broader struggle for equitable participation in the global digital economy. Recognizing data as a human right reframes governance debates beyond mere compliance and into questions of justice, access, and empowerment.

Institutional fragmentation further compounds the problem. While initiatives such as the GDPR, PIPL, and AU Cybersecurity Convention have advanced significant legal protections, their divergence has created a mosaic of inconsistent enforcement and interpretive gaps. These disparities erode global trust and enable corporate and state actors to exploit jurisdictional loopholes. As digital economies expand, the absence of interoperable governance frameworks risks transforming cyberspace into an arena of unchecked power and selective accountability. The path forward requires a reimagining of governance models that are simultaneously global in scope and locally grounded in context.

The future of equitable digital governance lies in multilateral harmonization and institutional reform. Global cooperation under platforms such as the United Nations, OECD, and WTO must move from fragmented dialogue to integrated action. Establishing cross-border data stewardship principles, standardizing digital rights enforcement mechanisms, and embedding human rights criteria in digital trade agreements are essential steps toward coherence. At the same time, regional alliances should continue to develop context-specific governance tools that reflect local legal traditions, cultural values, and developmental priorities.

Finally, future research should focus on empirical evaluation of data governance outcomes examining how laws, policies, and institutional arrangements influence real-world equity, participation, and rights protection. The role of emerging technologies, including artificial intelligence and quantum computing, also demands continuous scrutiny, as their regulatory implications will shape the next phase of global governance evolution.

In sum, achieving fairness in the digital realm requires a transformative shift from technocratic regulation to ethical governance-one rooted in justice, inclusion, and respect for human dignity. Only through such alignment can digital progress truly serve humanity rather than deepen its divides.

Reference

[1] Floridi L, Cowls J. A unified framework of five principles for AI in society. Machine learning and the city: Applications in architecture and urban design. 2022 May 21:535-45.

[2] Mittelstadt Brent, Allo Patrick, Taddeo Mariarosaria, Wachter Sandra, Floridi Luciano. The ethics of algorithms: Mapping the debate. *Big Data & Society*. 2016;3(2):1–21. doi:10.1177/2053951716679679

[3] Kuner Christopher. The General Data Protection Regulation: A commentary. *Oxford University Press*; 2019.

[4] Zuboff Shoshana. *The Age of Surveillance Capitalism: The fight for a human future at the new frontier of power.* New York: PublicAffairs; 2019.

[5] Taddeo Mariarosaria, Floridi Luciano. How AI can be a force for good. *Science*. 2018;361(6404):751–752. doi:10.1126/science.aat5991

[6] van Dijck José, Poell Thomas, de Waal Martijn. *The Platform Society: Public values in a connective world.* Oxford: Oxford University Press; 2018.

[7] Calo Ryan. Artificial intelligence policy: A primer and roadmap. *U.C. Davis Law Review*. 2017;51(2):399–435.

[8] Yeung Karen. Algorithmic regulation: A critical interrogation. *Regulation & Governance*. 2018;12(4):505–523. doi:10.1111/rego.12158

[9] Pasquale Frank. *The Black Box Society: The secret algorithms that control money and information.* Cambridge: Harvard University Press; 2015.

[10] Eubanks Virginia. *Automating Inequality: How high-tech tools profile, police, and punish the poor.* New York: St. Martin's Press; 2018.

[11] West Sarah M, Whittaker Meredith, Crawford Kate. Discriminating systems: Gender, race, and power in AI. *AI Now Institute Report*. 2019;1–33.

[12] Mantelero Alessandro. AI and Big Data: A blueprint for a human rights, social and ethical impact assessment. *Computer Law & Security Review*. 2018;34(4):754–772. doi:10.1016/j.clsr.2018.05.017

[13] Cath Corinne. Governing artificial intelligence: Upholding human rights and dignity. *European Parliament Study*. 2018; PE 624.261.

[14] Balkin Jack M. Information fiduciaries and the First Amendment. *UC Davis Law Review*. 2016;49(4):1183–1234.

[15] Bunn Isabella, Susskind Richard. *The Future of the Professions: How technology will transform the work of human experts.* Oxford: Oxford University Press; 2015.

[16] Kuner Christopher, Marelli Massimo. *Handbook on Data Protection in Humanitarian Action.* Geneva: International Committee of the Red Cross; 2017.

[17] WEF. *Global Risks Report 2019: Insight Report.* Geneva: World Economic Forum; 2019.

[18] Bryson Joanna J, Diamantis Mihailis E, Grant Thomas D. Of, for, and by the people: The legal lacuna of synthetic persons. *Artificial Intelligence & Law*. 2017;25(3):273–291. doi:10.1007/s10506-017-9214-9

[19] Latonero Mark. *Governing Artificial Intelligence: Upholding human rights & dignity.* Data & Society Research Institute; 2018.

[20] Kuner Christopher, Svantesson Dan Jerker, Greenleaf Graham, Bygrave Lee A, Gratton Elizabeth. The OECD guidelines and cross-border data flows. *International Data Privacy Law*. 2017;7(3):161–173. doi:10.1093/idpl/ipx012

[21] de Filippi Primavera, Wright Aaron. *Blockchain and the Law: The rule of code.* Cambridge: Harvard University Press; 2018.

[22] Tapscott Don, Tapscott Alex. *Blockchain Revolution: How the technology behind Bitcoin is changing money, business, and the world.* New York: Penguin; 2016.

[23] Scott Brett, Swan Melanie. *Blockchain: Blueprint for a new economy.* Sebastopol: O'Reilly Media; 2015.

[24] Casey Michael J, Vigna Paul. *The Truth Machine: The blockchain and the future of everything.* New York: HarperCollins; 2018.

[25] Hughes Justin, Savelyev Alexander. The promise and perils of smart contracts. *Stanford Technology Law Review*. 2019;22(1):1–28.

[26] Polcyn Katarzyna. Legal enforceability of smart contracts under EU law. *Computer Law Review International*. 2018;19(5):149–155.

[27] Greenleaf Graham. Global data privacy laws 2019: 132 national laws & many bills. *Privacy Laws & Business International Report*. 2019;157:10–13.

[28] Atanda ED. Dynamic risk-return interactions between crypto assets and traditional portfolios: testing regime-switching volatility models, contagion, and hedging effectiveness. *International Journal of Computer Applications Technology and Research.* 2016;5(12):797–807.

[29] Solove Daniel J, Schwartz Paul M. *Information Privacy Law.* 6th ed. New York: Aspen Publishers; 2018.

[30] van der Sloot Bart, Borgesius Frederik Zuiderveen. The GDPR: A regulatory success story? *International Data Privacy Law*. 2019;9(1):1–3. doi:10.1093/idpl/ipz002

[31] Emmanuel Damilola Atanda. EXAMINING HOW ILLIQUIDITY PREMIUM IN PRIVATE CREDIT COMPENSATES ABSENCE OF MARK-TO-MARKET OPPORTUNITIES UNDER NEUTRAL INTEREST RATE ENVIRONMENTS.

International Journal Of Engineering Technology Research & Management (IJETRM). 2018Dec21;02(12):151–64.

[32] Derera R. Machine learning-driven credit risk models versus traditional ratio analysis in predicting covenant breaches across private loan portfolios. *International Journal of Computer Applications Technology and Research*. 2016;5(12):808-820. doi:10.7753/IJCATR0512.1010.

[33] Nemitz Paul. Constitutional democracy and technology in the age of artificial intelligence. *Philosophical Transactions of the Royal Society A*. 2018;376(2133):20180089. doi:10.1098/rsta.2018.0089

[34] Rouvroy Antoinette, Berns Thomas. Algorithmic governmentality and prospects of emancipation. *Réactivation des savoirs critiques*. 2016;85(3):163–192.

[35] Wirtz Bernd W, Weyerer Jan C, Geyer Carolin. Artificial intelligence and the public sector—Applications and challenges. *International Journal of Public Administration*. 2019;42(7):596–615. doi:10.1080/01900692.2018.1498103

[36] Dignum Virginia. *Responsible Artificial Intelligence: Developing and using AI in a responsible way.* Cham: Springer; 2019.

[37] Cobbe Jennifer. Administrative law and the machines of government. *Law, Technology and Humans*. 2019;1(1):6–26.

[38] Scherer Matthew U. Regulating artificial intelligence systems: Risks, challenges, competencies, and strategies. *Harvard Journal of Law & Technology*. 2016;29(2):353–400.

[39] van Wynsberghe Aimee. Designing robots for care: Care centered value-sensitive design. *Science and Engineering Ethics*. 2013;19(2):407–433. doi:10.1007/s11948-011-9343-6

[40] Crawford Kate, Joler Vladan. Anatomy of an AI system: The Amazon Echo as an anatomical map of human labor, data and planetary resources. *AI Now Institute*; 2018.

[41] West Sarah M. Data capitalism: Redefining the logics of surveillance and control. *Television & New Media*. 2019;20(5):379–395. doi:10.1177/1527476418806090

[42] Couldry Nick, Mejias Ulises A. *The Costs of Connection: How data is colonizing human life and appropriating it for capitalism.* Stanford: Stanford University Press; 2019.

[43] Andrejevic Mark. *Automated Media.* New York: Routledge; 2019.

[44] Pohle Julia, Thiel Thorsten. Digital sovereignty. *Internet Policy Review*. 2019;8(1):1–8. doi:10.14763/2019.1.1383

[45] Taylor Linnet. What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society*. 2017;4(2):1–14. doi:10.1177/2053951717736335

[46] van Zoonen Liesbet. Privacy concerns in smart cities. *Government Information Quarterly*. 2016;33(3):472–480. doi:10.1016/j.giq.2016.06.004

[47] Benvenisti E. Upholding democracy amid the challenges of new technology: what role for the law of global governance?. European Journal of International Law. 2018 Feb;29(1):9-82.

[48] Rumbidzai Derera. HOW FORENSIC ACCOUNTING TECHNIQUES CAN DETECT EARNINGS MANIPULATION TO PREVENT MISPRICED CREDIT DEFAULT SWAPS AND BOND UNDERWRITING FAILURES. International Journal Of Engineering Technology Research & Management (IJETRM). 2017Dec21;01(12):112–27.

[49] Taylor L. What is data justice? The case for connecting digital rights and freedoms globally. Big Data & Society. 2017 Oct;4(2):2053951717736335.

[50] Bellanova R. Digital, politics, and algorithms: Governing digital data through the lens of data protection. European Journal of Social Theory. 2017 Aug;20(3):329-47.