

From Digital Cooperation to Coordinated Governance: A Critical Interdisciplinary Analysis of Centralization in the United Nations' Pact for the Future and Global Digital Compact

Sixbert Sangwa

Open Christian University, California, USA

Correspondence: ssangwa@openchristian.education

Abstract

Purpose: This article examines whether the United Nations' Pact for the Future and its annexed Global Digital Compact (GDC) constitute a substantive move toward centralized digital governance or a more limited form of coordinated multilateral steering. It addresses a key weakness in current debate: official accounts often understate institutional concentration, while critical commentary sometimes overstates the emergence of a de facto world government. **Design:** The study employs qualitative document analysis of the principal United Nations digital-governance instruments from the World Summit on the Information Society to the 2025 implementation architecture. This core analysis is complemented by comparative examination of adjacent regulatory and policy developments in platform governance, digital identity, digital public infrastructure (DPI), artificial intelligence (AI), information integrity, and central bank digital currencies (CBDCs). **Findings:** The analysis shows that the UN framework does not create a binding global sovereign. It does, however, deepen transnational coordination through agenda-setting, standards diffusion, expert authority, implementation networks, and infrastructural interoperability. Centralization therefore operates not mainly through direct legal command, but through discursive, technical, epistemic, and infrastructural pathways. While this architecture may enhance inclusion, interoperability, and human-rights language, it also creates risks of epistemic concentration, function creep, infrastructural dependence, and expanded public-private governance over identity, information, and access to digital services. **Originality/value:** The article advances the debate by distinguishing formal sovereignty from institutional thickening and by showing that the GDC should be interpreted neither as empty symbolism nor as an imminent world-government project. Instead, it is best understood as a polycentric architecture of coordinated governance. The article further contributes an integrated normative framework that combines global governance theory, surveillance capitalism, governmentality, and a restrained Christian ethical lens centred on subsidiarity, human dignity, and limits on power. **Practical implications:** The article proposes safeguards grounded in due process, privacy, contestability, transparency, epistemic pluralism, and dignity-preserving governance.

Keywords: *Global Digital Compact; United Nations digital governance; digital centralization; digital public infrastructure; digital identity governance; information integrity; AI governance*

Cite as: Sangwa, S. (2026). From Digital Cooperation to Coordinated Governance: A Critical Interdisciplinary Analysis of Centralization in the United Nations' Pact for the Future and Global Digital Compact Open Journal of AI, Ethics and Society, Vol 2(1). [10.65655/OpenChristianPress.2026.97](https://doi.org/10.65655/OpenChristianPress.2026.97)

1. Introduction

The United Nations' Pact for the Future, adopted on 22 September 2024, and its annexed Global Digital Compact (GDC) represent the most ambitious multilateral attempt in recent years to consolidate norms for the governance of digital infrastructures, data flows, platforms, and artificial intelligence (United Nations,

2024a, 2024b). The GDC is not a treaty and does not create a supranational government. Yet it matters precisely because contemporary governance is no longer exhausted by formal sovereignty. In the digital sphere, authority increasingly operates through standards, interoperability requirements, benchmarking, multistakeholder coordination, expert panels, and infrastructures that quietly reorder what states, firms, and

citizens can do. A serious analysis therefore cannot stop at the formal claim that the Compact is “only” soft law. It must examine whether soft law, when coupled with platforms, identity systems, and international coordination mechanisms, can nevertheless centralize agenda-setting power and reshape the conditions of autonomy (Abbott & Snidal, 2000; Plantin et al., 2018; Scholte, 2023).

This question has become more urgent because the GDC did not emerge in isolation. It extends a longer institutional lineage: the World Summit on the Information Society (WSIS), the Internet Governance Forum (IGF), the Secretary-General’s High-level Panel on Digital Cooperation, the 2020 Roadmap for Digital Cooperation, Our Common Agenda, the 2023 policy brief on a Global Digital Compact, the 2024 United Nations Global Principles for Information Integrity, the 2024 final report of the High-level Advisory Body on Artificial Intelligence, the United Nations Legal Identity Agenda, and the DPI safeguards process led by the United Nations Development Programme (UNDP) and the Secretary-General’s technology architecture (United Nations, 2019, 2020, 2023, 2024c; United Nations Advisory Body on Artificial Intelligence, 2024; United Nations Statistics Division, n.d.; United Nations Development Programme [UNDP], 2024b). By 2025, the institutional picture had thickened further with the creation of the United Nations Office for Digital and Emerging Technologies (ODET) and the General

Assembly’s establishment of an Independent International Scientific Panel on AI and a Global Dialogue on AI Governance (Office for Digital and Emerging Technologies, 2025a, 2025b, 2025c; UN General Assembly, 2025).

The central analytical problem is therefore not whether the United Nations has announced a one-world digital state. It has not. The more serious question is whether multilateral digital cooperation is gradually consolidating a layered architecture of coordination that centralizes three things at once: first, the categories through which digital problems are publicly understood; second, the technical pathways through which people authenticate themselves, access services, and participate in digital markets; and third, the expert and institutional forums through which legitimate responses are defined. Centralization, in this article, refers not only to direct legal command but also to the concentration of rule-shaping, standard-setting, epistemic authority, and infrastructural dependence (Abbott & Snidal, 2000; Plantin et al., 2018; Curran, 2023). Figure 1 shows the article’s core analytical finding: in the UN digital-governance architecture, centralization operates not only through formal legal command but also through agenda-setting, standardization and interoperability, expert coordination, and infrastructural dependence. These mechanisms yield discursive, technical, epistemic, and infrastructural forms of centralization, even in the absence of supranational sovereignty.

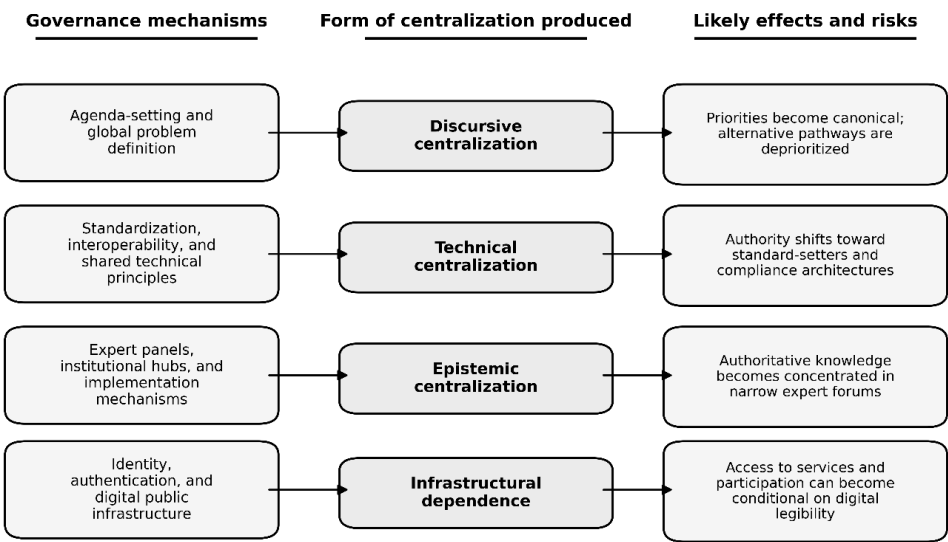


Figure 1. Modes and Mechanisms of Digital Centralization in the UN Governance Architecture. Core claim: the GDC does not create a binding global sovereign, but it can still centralize power through soft-law coordination, standards diffusion, epistemic authority, and infrastructural interdependence.

The article responds to a further weakness in existing commentary. Official accounts frequently present the GDC as an unqualified public good, emphasizing inclusion, interoperability, safety, and rights. Critical commentary often performs a necessary corrective, but some critiques collapse important distinctions between coordination and coercion, between soft law and binding law, and between risk scenarios and demonstrated policy effects. That conflation weakens otherwise valid concerns. This article therefore adopts a more disciplined posture: it neither romanticizes multilateral digital cooperation nor treats every UN digital initiative as proof of imminent totalized control. Instead, it asks what forms of centralization are actually being built, through which mechanisms, and with what safeguards or deficits.

The contribution is fourfold. First, it reconstructs the institutional genealogy of UN digital governance from WSIS to the post-2024 implementation architecture. Second, it shows that the GDC advances a real form of centralization, though primarily through coordination, standards diffusion, and epistemic consolidation rather than direct sovereignty transfer. Third, it locates the GDC within a wider ecosystem that includes digital identity, DPI, platform governance, AI governance, and adjacent financial digitization debates, while carefully distinguishing what the GDC does from what it does not do. Fourth, it develops a normative evaluation that combines global governance theory, surveillance capitalism, governmentality, framing analysis, and a restrained Christian ethical lens centered on human dignity, limits on power, and subsidiarity.

Table 1. Major United Nations digital-governance initiatives relevant to centralization/globalization, 2003-2025

UN initiative / instrument	Primary governance move	Centralization relevance
WSIS Geneva Declaration (2003)	Foundational principles for an inclusive information society	Creates the constitutional vocabulary of global digital cooperation.
Tunis Agenda and IGF mandate (2005-)	Institutionalizes multistakeholder internet-policy dialogue	Centralizes convening power without creating binding legal authority.
UN Legal Identity Agenda Task Force (2018-)	Inter-agency coordination on legal identity and CRVS-ID interoperability	Moves identity from a domestic registry issue toward a coordinated global development agenda.
The Age of Digital Interdependence (2019)	Expands digital governance beyond internet management	Reframes digital issues as systemic multilateral governance problems.
Roadmap for Digital Cooperation (2020)	Eight action areas: connectivity, public goods, inclusion, rights, AI, trust, cooperation architecture	Provides the operational blueprint for later institutional layering.
Our Common Agenda and Policy Brief 5 (2021-2023)	Places the GDC inside broader UN reform	Links digital governance to multilateral-system redesign.
UN Global Principles for Information Integrity (2024)	Human-rights-based framework for information ecosystems	Centralizes epistemic governance norms around integrity, resilience, and trusted information.
Governing AI for Humanity (2024)	Recommends international AI governance architecture	Normalizes a standing UN role in AI evidence production and coordination.
Pact for the Future and GDC (2024)	Shared commitments on connectivity, rights, data governance, and AI	Consolidates digital governance into a single multilateral reference framework.
UN Convention against Cybercrime (2024)	Creates treaty-based cooperation on cybercrime and electronic evidence	Represents a harder legal form of centralization in a specific domain.
Universal DPI Safeguards Framework (2024)	Guidance for safer, more inclusive digital public infrastructure	Formalizes common guardrails around foundational digital systems.
ODET; AI Scientific Panel and Global Dialogue (2025)	Creates standing organizational and epistemic infrastructure inside the UN	Transforms aspiration into durable implementation capacity.

Note. Compiled by the author from ITU (2003, 2005), United Nations (2019, 2020, 2023, 2024a, 2024b, 2024c, 2024d), United Nations Statistics Division (n.d.), UNDP (2024b), Office for Digital and Emerging Technologies (2025a), and United Nations General Assembly (2025).

Figure 2 below visualizes the manuscript's historical argument that UN digital governance developed through cumulative institutional layering rather than abrupt sovereign transfer.

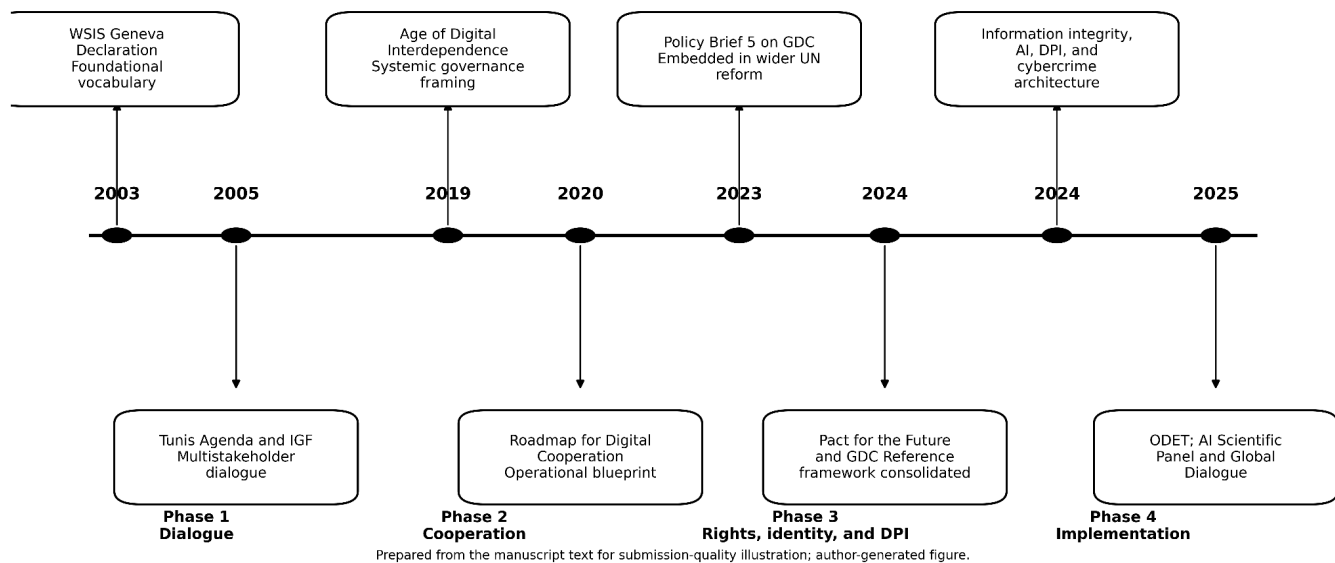


Figure 2. Institutional Layering of UN Digital Governance, 2003–2025. The timeline traces the movement from WSIS and the IGF to the Roadmap for Digital Cooperation, the Global Digital Compact, and the 2025 implementation architecture centred on ODET and the AI Scientific Panel and Global Dialogue.

2. Literature Review and Research Gap

Scholarship on the GDC and adjacent digital-governance debates has converged on two broad insights. The first is that contemporary digital governance is increasingly “post-hegemonic” and multistakeholder: authority is distributed across states, international organizations, firms, technical bodies, and civil society rather than monopolized by any single actor (Scholte, 2023). The second is that this apparent distribution does not necessarily guarantee pluralism, because infrastructures, standards, and platform intermediaries can silently re-concentrate practical power. The institutional form may be multistakeholder while the operational consequences remain highly asymmetric (Plantin et al., 2018; Gorwa, 2019).

Recent work on the GDC itself illustrates this tension. Gwagwa and Mollema (2024) argue that the Compact should guard against cultural imposition and hermeneutical injustice by avoiding the export of the digital-regulatory priorities of powerful jurisdictions to the rest of the world. Their intervention is valuable because it shifts debate away from technological inevitability and toward representational justice: who defines the problem, whose categories travel globally, and

which social contexts become the implicit norm. That question is central to any analysis of globalization that takes asymmetry seriously. It also clarifies why the strongest objections to centralization are not only constitutional or geopolitical, but also epistemic and civilizational.

At the same time, the political economy of digital governance cannot be understood without attention to surveillance capitalism. Curran (2023) extends the discussion beyond behavioral extraction as such and emphasizes systemic dependence: as digital systems become more integrated, social and economic life becomes more vulnerable to failure, manipulation, and concentration effects. This insight matters for the GDC because multilateral coordination often presumes interoperable, scalable infrastructures. Scalability can produce real efficiency gains, but it can also intensify the consequences of design errors, political misuse, or exclusion from core systems. Infrastructural efficiency and systemic fragility may grow together.

Human-rights scholarship and advocacy on digital identity and DPI likewise warns against naïve developmentalism. Rights-based approaches do not deny the value of identity systems or digital infrastructure.

Rather, they insist that inclusion claims be evaluated together with privacy, contestability, proportionality, and the risk of exclusion through system design (Access Now, 2024; OHCHR, 2024; UNDP, 2023). This is particularly important because the language of “public infrastructure” often carries a strong legitimating effect. Infrastructure sounds neutral, foundational, and unquestionably beneficial. Yet infrastructures are never merely technical. They institutionalize permissible flows, define access conditions, and create new chokepoints. A rights-based analysis therefore asks not only whether infrastructure exists, but who governs it, under what standards, with what review mechanisms, and with what exit options for affected persons.

A related literature on platform regulation has shown that attempts to discipline platform power can also institutionalize it. UNESCO’s 2023 Guidelines for the Governance of Digital Platforms adopt a human-rights-centered approach that emphasizes freedom of expression and access to information, but the broader regulatory field also reveals the danger of regulatory capture and the normalization of platforms as quasi-public governors (UNESCO, 2023; Gorwa, 2019; Helberger et al., 2018). This duality is visible in the European Union’s Digital Services Act and AI Act. They seek to constrain digital harms through due diligence, systemic-risk management, and harmonized rules, yet they also consolidate a regulatory model in which large intermediaries remain indispensable governors of the information environment (European Parliament and Council of the European Union, 2022, 2024b). For the purposes of this article, the significance of these instruments is comparative: they demonstrate how governance can centralize through risk management and compliance architectures even when the stated objective is to protect rights.

Three major gaps follow. First, much of the literature treats UN digital governance, platform regulation, digital identity, DPI, and AI governance as separate silos, even though policymakers increasingly connect them in practice. Second, critical debate often fails to distinguish between formal centralization and infrastructural or epistemic centralization, which are analytically different but politically intertwined. Third, work that incorporates theology or biblical ethics often slips into deterministic or prophetic certitude, while secular work may ignore how questions of dignity, authority, and conscience animate

public resistance to centralized governance. This article addresses these gaps by offering an integrated analysis that is both empirically disciplined and normatively explicit.

3. Theoretical Framework

3.1. Global governance and institutional thickening

Global governance scholarship helps explain why digital centralization today is unlikely to take the form of a classical world state. Contemporary governance more often proceeds through what may be called institutional thickening (Abbott & Snidal, 2000; Scholte, 2023): the creation of additional forums, principles, coordinating offices, technical panels, reporting cycles, and implementation networks that structure conduct without eliminating state sovereignty. Scholte’s (2023) account of multistakeholder global governance in a post-hegemonic setting is especially useful here. It directs attention to the production of norms and procedures under conditions where no single power can dictate outcomes absolutely, yet asymmetries remain embedded in resources, technical capacities, and agenda-setting access. This lens allows the GDC to be read neither as empty symbolism nor as a world-government charter, but as a significant node in the expanding architecture of digital coordination.

3.2. Surveillance capitalism and infrastructural dependence

The second lens is surveillance capitalism, understood here not simply as a business model but as an architecture of extraction and dependence. Curran’s (2023) argument is especially important because it reframes the question from privacy loss alone to systemic risk. The more that identification, payment, data sharing, content ranking, and service delivery are integrated into interoperable digital environments, the greater the potential payoff from efficiency and the greater the potential damage from concentration. This perspective helps explain why soft-law coordination can have hard social consequences. When institutions, markets, and welfare systems depend on a small set of interoperable infrastructures, governance becomes materially consequential even without formal compulsion.

3.3. Governmentality and framing

A Foucauldian perspective on governmentality sharpens the analysis further (Lemke, 2002). Governmentality draws attention to governance by shaping the field of possible action rather than merely

issuing commands. In digital policy, this occurs through taxonomies of risk, performance indicators, “best practice” templates, content-integrity standards, audit procedures, and benchmarked notions of safety, trust, resilience, or inclusion. The language of information integrity is instructive here. It frames the digital problem not primarily as a conflict over speech, power, and political contestation, but as a problem of ecosystem health, trust, and public resilience (United Nations, 2024c). Framing is never innocent. It channels what counts as harm, what counts as a solution, and which actors appear competent to intervene. Governmentality therefore complements global governance theory by showing how soft norms become governing rationalities (Lemke, 2002).

3.4. Human dignity, subsidiarity, and a restrained Christian ethical lens

The final lens is ethical and theological. This article does not treat biblical material as empirical proof of international political outcomes. Instead, it uses Christian political ethics as a critical vocabulary for evaluating power concentration. Two ideas are especially relevant. The first is the *imago Dei*, which grounds human worth in more than administrative legibility or economic utility (Genesis 1:26-27; 5:1-3; 9:6). Human beings are not exhausted by their data traces, nor should access to civic participation depend on total visibility to institutional systems. The second is a principle analogous to subsidiarity: power should be exercised at the lowest level consistent with justice and the common good (Carozza, 2003), because concentration can erode agency, accountability, and conscience. In biblical terms, the Tower of Babel (Genesis 11:1-9) is best read here not as a predictive code for modern institutions, but as a cautionary narrative about the temptation to confuse coordination, mastery, and moral legitimacy. As a political ethic, it warns against the belief that technical integration by itself resolves the problem of human fallibility. This restrained theological lens strengthens, rather than replaces, the secular concern for limits, contestability, and human dignity.

4. Method

This study uses qualitative document analysis and comparative policy tracing. The core corpus comprises principal UN instruments and institutional documents from 2003 to 2025, including the WSIS outcomes, the

High-level Panel on Digital Cooperation report, the Roadmap for Digital Cooperation, Our Common Agenda Policy Brief 5, the Pact for the Future, the GDC, the United Nations Global Principles for Information Integrity, the Advisory Body’s final AI report, the UN Legal Identity Agenda materials, DPI safeguards outputs, and post-adoption implementation materials associated with ODET and the AI Panel and Dialogue architecture (United Nations, 2019, 2020, 2023, 2024a, 2024b, 2024c; UN Advisory Body on Artificial Intelligence, 2024; Office for Digital and Emerging Technologies, 2025a, 2025b, 2025c; UN Statistics Division, n.d.; UNDP, 2024a, 2024b).

The comparative corpus includes external but adjacent regulatory and policy materials that illuminate implementation pathways or analogous governance forms: UNESCO’s platform-governance guidelines, the European Union’s Digital Services Act, AI Act, and European Digital Identity Framework, World Bank identification datasets and analysis, BIS CBDC survey findings, OHCHR reports, and selected peer-reviewed scholarship on surveillance capitalism, global digital governance, and cultural injustice in digital regulation (Curran, 2023; European Parliament and Council of the European Union, 2022, 2024a, 2024b; Gwagwa & Mollema, 2024; Illes et al., 2025; OHCHR, 2022, 2024; UNESCO, 2023; World Bank, 2025a; Pswarayi-Riddihough et al., 2025).

The analysis proceeded in three stages. First, the documents were read genealogically to reconstruct how the UN digital-governance agenda evolved from connectivity and internet dialogue toward broader coordination over AI, information integrity, identity systems, and DPI. Second, the texts were coded conceptually for recurring governance moves: standardization, interoperability, risk management, multistakeholder coordination, rights-protective language, institutional creation, and implementation pathways. Third, these patterns were compared with adjacent regulatory developments to distinguish what the UN itself mandates from what it enables, legitimizes, or accelerates indirectly.

This design is more modest than some computational approaches, but it is deliberately so. The original manuscript contained quantitative and NLP-style claims that, in their present form, were not fully demonstrable

from the evidence available. For a publishable article, methodological credibility is more important than performative sophistication. The present design therefore prioritizes traceable interpretation over unverified metricization. Its limits are clear: document analysis cannot establish causal effects with the precision of interviews, ethnography, or longitudinal implementation data. It can, however, identify institutional direction, conceptual consolidation, and legally or politically salient shifts in governance architecture.

5. Findings and Discussion

5.1. From dialogue to institutional densification

The first major finding is historical. Since WSIS, UN digital governance has moved through at least three phases. The WSIS phase was primarily constitutional and dialogic. It articulated an inclusive, people-centered information society and created the Tunis Agenda's multistakeholder logic, including the mandate for the IGF, which the United Nations Secretary-General has convened annually since 2006 (International Telecommunication Union, 2003, 2005; United Nations Department of Economic and Social Affairs, n.d.; United Nations Department of Economic and Social Affairs, n.d.). The second phase, crystallized in the 2019 High-level Panel report and the 2020 Roadmap for Digital Cooperation, expanded the agenda from internet governance to a wider digital-governance architecture including connectivity, digital public goods, human rights, AI cooperation, trust and security, and more effective institutional arrangements (United Nations, 2019, 2020). The third phase, culminating in the 2024 Pact and GDC and extending into the 2025 implementation architecture, is more operational. It adds panels, offices, safeguards frameworks, implementation portals, and follow-on processes that convert aspiration into organized multilateral machinery.

This development matters because centralization in global governance often occurs through cumulative layering rather than abrupt legal rupture. The establishment of ODET on 1 January 2025 is especially significant in this respect. Officially, the office was created to advance inclusive, rights-based, multistakeholder digital cooperation while respecting national priorities and contexts (Office for Digital and Emerging Technologies, 2025a). That language is important and normatively constructive. Yet

institutionally it also indicates that digital governance has become sufficiently central to UN strategy to warrant a dedicated organizational hub. Likewise, the General Assembly's 2025 decision to establish an Independent International Scientific Panel on AI and a Global Dialogue on AI Governance gives the UN a more formalized role in producing AI-related evidence and convening normative discussion (Office for Digital and Emerging Technologies, 2025c). The result is not world government, but it is unmistakably more than occasional diplomacy.

5.2. The GDC centralizes primarily through standards, coordination, and agenda-setting

A second finding is that the GDC's centralization logic is best understood as coordinated steering rather than direct legal supremacy. The Compact explicitly builds on the WSIS outcomes and aims to strengthen global digital cooperation through shared commitments on connectivity, rights, data governance, and AI-related institutional development (United Nations, 2024b). Its force lies in three interlocking moves.

First, it centralizes discourse. The GDC defines the legitimate global agenda: closing digital divides, promoting rights online, building safe and secure digital spaces, strengthening data governance, and improving AI governance. Agenda-setting on this scale matters because it shapes how states, donors, technical communities, and firms prioritize resources. The issue is not that these goals are inherently objectionable. Many are normatively compelling. The issue is that global problem definitions often privilege some path dependencies over others. Once connectivity, DPI, information integrity, and AI governance are framed as the canonical pillars of digital progress, alternative priorities such as market concentration, infrastructural exit rights, low-tech resilience, or decentralization by design can become secondary.

Second, the GDC centralizes via standardization and interoperability. The text repeatedly assumes that digital inclusion requires interoperable systems, shared principles, and institutional coherence across national boundaries (United Nations, 2024b). Interoperability is a functional good, but it also has a political dimension. Systems that work together create larger governance spaces, longer chains of dependency, and more influence for the actors who set the standards. Standardization is therefore never merely technical. It redistributes authority

toward the bodies that define what counts as compliant infrastructure, trustworthy identity, valid data governance, or acceptable AI oversight (Abbott & Snidal, 2000; Plantin et al., 2018).

Third, the GDC centralizes epistemically. Its post-adoption architecture channels authority toward expert panels, multistakeholder processes, and institutional hubs that organize what counts as authoritative knowledge about digital harms and remedies. This is especially visible in the areas of information integrity and AI. The more that global governance relies on expert summaries, scientific panels, implementation frameworks, and risk taxonomies, the more that epistemic power becomes concentrated even where legal coercion remains diffuse.

5.3. Identity, legal personhood, and DPI reveal the infrastructural core of centralization

The third finding is that digital identity and DPI constitute the infrastructural core of contemporary centralization. The GDC does not explicitly impose a universal biometric digital ID, and accuracy requires saying so plainly (United Nations, 2024b). However, the broader UN ecosystem has clearly moved toward a model in which legal identity, digital authentication, and DPI are treated as foundations for inclusion, service delivery, and digital transformation (United Nations Statistics Division, n.d.; UNDP, 2023, 2024a, 2024b). The UN Legal Identity Agenda Task Force, established in 2018 and involving 13 UN agencies, exists to help member states achieve SDG target 16.9 on legal identity for all (United Nations Statistics Division, n.d.). UNDP's guidance on digital legal identity explicitly links identity systems to broader DPI architectures while insisting on rights-based governance (UNDP, 2023).

The developmental rationale is clear. Identification can expand access to services, enable remote authentication, reduce administrative friction, and support more inclusive digital economies. The World Bank's latest data underscore the real stakes: more than 800 million people still lack official proof of identity, and 2.8 billion lacked access to digital ID for online transactions in 2024 (Pswarayi-Riddihough et al., 2025; World Bank, 2025a). In developmental terms, identity deficits are exclusionary. Yet the same data also clarify why identity systems are politically consequential. When access to welfare, SIM cards, banking, voting, travel, and online services is progressively mediated through digital

credentials, identity becomes a powerful point of infrastructural governance. This concern is reinforced by African-focused scholarship showing how universal digital identity systems can converge inclusion goals, biometric surveillance risks, and data-sovereignty tensions in a single governance architecture (Sangwa, 2025a).

This is precisely why rights-centered critiques remain indispensable. Access Now (2024) warns that DPI discourse can become a rebranding and expansion of problematic digital identity models if privacy, contestability, and human-rights safeguards are subordinated to administrative efficiency. OHCHR's surveillance reporting likewise underscores the risk that digital systems designed for service delivery can become tools of monitoring, profiling, and control absent legality, necessity, proportionality, and independent oversight (OHCHR, 2022, 2024). The significance for the present article is straightforward: centralization becomes especially potent when it moves from the level of discourse into the level of access architecture. If identity becomes the gateway to participation, then governance over identity becomes governance over civic possibility itself.

5.4. Information integrity advances a human-rights vocabulary but also concentrates epistemic authority

The fourth finding concerns information integrity. The United Nations Global Principles for Information Integrity are more sophisticated and rights-aware than many critics allow. They emphasize societal trust and resilience, independent and pluralistic media, transparency and research, public empowerment, and healthy incentives, and they expressly place these principles within a human-rights framework (United Nations, 2024c). Compared with cruder anti-fake-news paradigms, this is a substantive improvement. It signals awareness that information governance cannot be reduced to censorship or ad hoc content removal.

Even so, a critical concern remains. Information integrity is an attractive frame precisely because it fuses descriptive and normative force. To defend "integrity" sounds inherently benign; few actors will publicly oppose it. But the frame also performs a subtle political move: it shifts debate away from questions such as who defines legitimacy, whose expertise becomes authoritative, how dissent is protected, and when harm mitigation shades into managed public discourse. Governmentality is

helpful here. The issue is not only what gets prohibited. It is also what institutional and platform actors learn to optimize for: authoritative sources, trusted signals, systemic-risk reduction, and resilience narratives. Those may all be justifiable aims. Yet they also centralize epistemic filtering.

UNESCO's 2023 guidelines reveal the same duality. They place freedom of expression and access to information at the center of platform governance, which is normatively important (UNESCO, 2023). But the broader regulatory tendency, visible as well in the European Union's Digital Services Act, is to govern platforms through due diligence, systemic-risk frameworks, transparency duties, and structured cooperation between public authorities, researchers, and intermediaries (European Parliament and Council of the European Union, 2022). Such frameworks can restrain abuse, but they can also normalize a governance environment in which a relatively small number of public and private institutions become the managers of legitimate information flows. The central danger is therefore not simply overt censorship. It is the quieter consolidation of authorized epistemic pipelines (Gorwa, 2019; Helberger et al., 2018). Related work on misinformation law and free speech similarly shows that harm-mitigation frameworks can drift toward overbroad management of dissent unless due process, viewpoint pluralism, and principled safeguards for lawful expression are preserved (Sangwa & Mutabazi, 2025a)

5.5. Comparative regulatory convergence and its implications

A fifth finding is comparative. The UN's digital-governance architecture is influential partly because it aligns with broader regulatory convergence rather than operating as a self-sufficient command center. The Advisory Body's 2024 report, *Governing AI for Humanity**, explicitly emerged from the Roadmap for Digital Cooperation and advanced recommendations for

international AI governance (United Nations Advisory Body on Artificial Intelligence, 2024). The subsequent establishment of the AI Scientific Panel and Global Dialogue in 2025 further institutionalized this trajectory (Office for Digital and Emerging Technologies, 2025c). Yet much of the hard legal development still occurs elsewhere, particularly within the European Union, which now has an integrated legal framework spanning platform risk management, AI, and digital identity (European Parliament and Council of the European Union, 2022, 2024a, 2024b).

This convergence has two implications. First, it shows that the UN is not acting alone; digital centralization is polycentric. International organizations, regional regulators, development banks, technical communities, and private platforms collectively shape the field. Second, it suggests that soft-law frameworks can still be powerful when they operate in a favorable ecosystem. UN norms gain traction not because they coerce directly, but because they resonate with donor priorities, regional legislation, development practice, and corporate compliance structures. In this sense, the GDC is neither empty symbolism nor the sole engine of change. It is a multiplier and coordinator. Adjacent scholarship on programmable CBDCs further suggests that once payment rails, digital identity, messaging standards, and AI-enabled compliance are linked, the practical reach of coordinated governance can expand well beyond the formal text of any single multilateral instrument (Sangwa & Mutabazi, 2025b). The Figure 3 below clarifies that the UN is not acting alone, but its digital-governance architecture interacts with regional regulation, development implementation actors, UNESCO's platform-governance framework, BIS payment-standard debates, and private platforms or technical intermediaries.

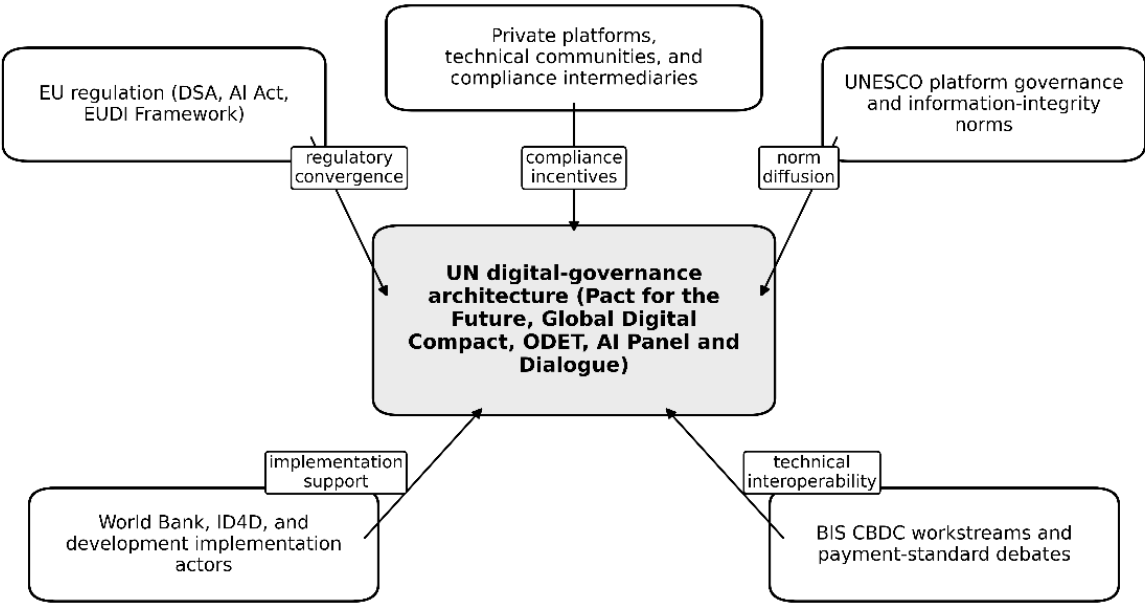


Figure 3. Polycentric Ecosystem of Digital-Governance Convergence. Interpretive point: the UN is not a self-sufficient command center. Its influence grows because its soft-law architecture aligns with regional regulation, development practice, technical standards, and platform compliance structures. The figure therefore illustrates the manuscript’s claim that centralization is polycentric and reinforced through convergence rather than direct command.

Table 2. Comparative regulatory convergence and analytical implications

Domain	UN vector	External comparator	Opportunity	Risk / caution
Digital identity and DPI	UN Legal Identity Agenda, GDC, DPI safeguards	EU Digital Identity Framework / EUDI Wallet	Interoperability and service access	Function creep, exclusion, and infrastructural dependence
Platforms and information integrity	GDC; UN Principles for Information Integrity	UNESCO Guidelines; EU DSA	Accountability and transparency	Consolidation of authorized epistemic pipelines
Artificial intelligence	HLAB-AI report; AI Panel and Global Dialogue	EU AI Act	Shared risk vocabularies and evidence structures	Expert over-centralization and compliance asymmetry
Cybercrime and cross-border evidence	UN Convention against Cybercrime	Domestic and regional e-evidence regimes	Improved cooperation	Due-process and civil-liberties concerns
Payments and monetary digitization	Adjacent to, but not mandated by, the GDC	BIS CBDC workstreams and national pilots	Efficiency and inclusion	Identity-payment-data linkage can intensify control risks

Note. Compiled by the author from United Nations (2024b, 2024c, 2024d), UNESCO (2023), European Parliament and Council of the European Union (2022, 2024a, 2024b), Office for Digital and Emerging Technologies (2025c), and Illes et al. (2025)

5.6. Ethical and theological evaluation: dignity, limits, and the politics of scale

The final finding is normative. The best ethical critique of the emerging architecture is not that global digital cooperation is intrinsically illegitimate. A fragmented world with no common rules is also dangerous. Rather, the critique is that institutions often underestimate how quickly coordination can become dependence and how easily inclusion can become

conditional inclusion. The developmental case for identity, connectivity, platform accountability, and AI governance is real. So too is the risk that these systems, once made foundational, alter the default relationship between person and institution.

A human-capabilities perspective reinforces this point. Governance is justified insofar as it expands substantive freedoms, not merely administrative visibility or transaction speed (Nussbaum, 2011). Theologically, the

imago Dei intensifies the same concern. Human persons should not be reduced to administratively legible units within interoperable systems. Their dignity exceeds the value of efficient classification, and recent digital-ethics scholarship has similarly argued that contemporary technologies should be assessed against non-negotiable conceptions of human worth rather than administrative convenience (Umbrello & O'Hara, 2025; Teo, 2023). That conviction does not prohibit digital governance. It does, however, require strict limits. Systems must preserve privacy, contestability, and spaces of lawful dissent. They must avoid making total visibility the price of participation.

A restrained biblical reading also illuminates the problem of scale. The story of Babel is a cautionary narrative about the temptation to confuse technical unity and collective ambition with moral legitimacy. Read politically, the point is not hostility to cooperation as such. It is skepticism toward concentrated projects that confuse capacity with moral authority. Likewise, Acts 17:26 and Romans 13:1-7 can be read together as affirming political

order while also implying that authority is limited, derivative, and accountable. In practical policy terms, that yields a preference for layered governance with strong local accountability (Carozza, 2003), rather than seamless architectures whose scale outruns avenues of redress. The relevant warning is not prophetic sensationalism. It is moral realism about fallible institutions and the perennial temptation to sacralize technocratic coordination.

Relevant scriptural touchpoints for this ethical reading include Genesis 11:1-9, Acts 17:26, Romans 13:1-7, Acts 5:29, and, more cautiously in some Christian traditions, Revelation 13:16-17. Figure 4 synthesizes the article's normative conclusion, linking the major risks identified in the analysis, including epistemic concentration, infrastructural dependence, function creep, exclusion, and reduced dissent space, to the principles and institutional safeguards needed to make digital governance contestable, reviewable, and compatible with human dignity.

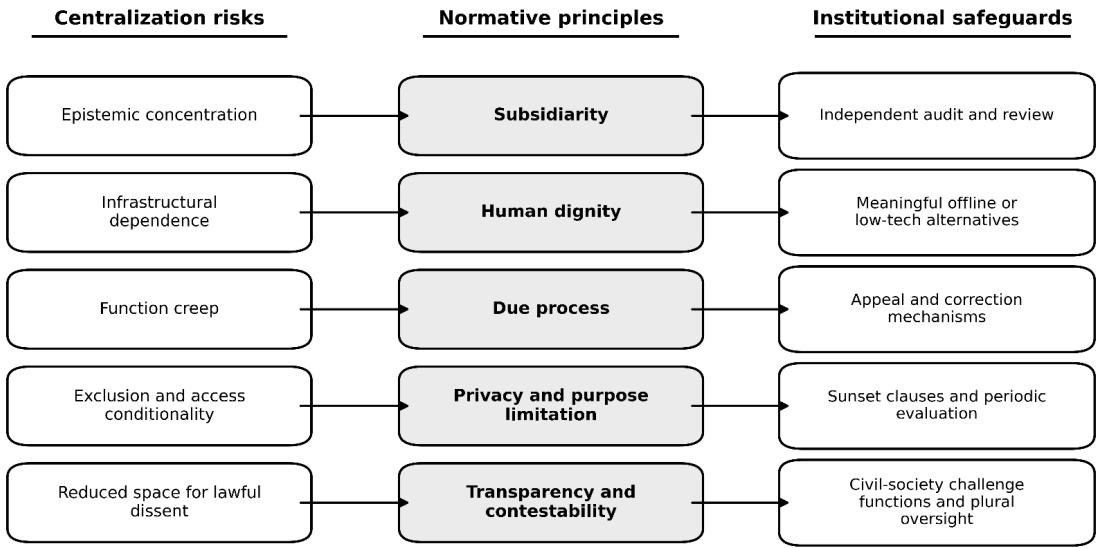


Figure 4. Safeguards Framework for Contestable and Dignity-Preserving Digital Governance. Policy logic: coordination is not rejected; it is made legitimate only when power remains limited, reviewable, and answerable to the dignity and agency of affected persons

6. Policy Recommendations

The analysis supports six recommendations. First, the UN digital-governance architecture should operationalize subsidiarity more clearly. Global coordination is often necessary for interoperability, safety, and cross-border harms, but not every governance

function should migrate upward. The GDC's implementation guidance should therefore distinguish more explicitly between what requires global norm-setting, what requires regional coordination, and what should remain nationally or locally contestable.

Second, digital identity and DPI initiatives should be conditioned on rights-by-design safeguards, not merely accompanied by them rhetorically. That includes legal purpose limitation, data minimization, meaningful alternatives for people unable or unwilling to use digital channels, regular independent audits, appeal mechanisms, and protection against function creep. Where identity becomes necessary for essential services, procedural justice must be especially robust (Office of the United Nations High Commissioner for Human Rights, 2022, 2024; United Nations Development Programme, 2023; Access Now, 2024).

Third, the information-integrity agenda should prioritize epistemic pluralism alongside harm mitigation. This means stronger commitments to due process, transparency of moderation or ranking interventions, meaningful access for independent researchers, and explicit protections for lawful dissent, minority viewpoints, and non-state perspectives. “Integrity” should not become a vocabulary that immunizes authorities from scrutiny (United Nations, 2024c; UNESCO, 2023).

Fourth, the AI governance architecture should be tied to enforceable public-accountability norms rather than confined to expert consensus. The 2025 AI Panel and Global Dialogue are important institutional gains, but expert bodies should not become substitutes for democratic contestation. Their legitimacy will depend on transparency, geographic balance, disciplinary diversity, and publicly accessible reasoning (United Nations General Assembly, 2025).

Fifth, comparative regulatory convergence should not translate into developmental coercion. Low- and middle-income countries should not be forced, through aid conditionality or technical path dependence, into adopting identity, platform, or AI frameworks that they lack the legal and institutional capacity to govern safely. The rights-based commitments in UNDP and OHCHR materials should therefore be treated as entry conditions, not aspirational add-ons (OHCHR, 2024; UNDP, 2023).

Sixth, the UN should treat institutional concentration itself as a governance risk. Centralization can improve coordination, but it also increases the consequences of error, exclusion, or capture. Periodic review, sunset mechanisms for non-binding implementation frameworks, external evaluation, and structured civil-society challenge

functions would make the architecture more contestable and therefore more legitimate.

7. Conclusion

The Pact for the Future and the Global Digital Compact do not inaugurate a digital world state. They do, however, consolidate a more coordinated and institutionally dense form of global digital governance. Their centralizing effects are real, but they operate mainly through agenda-setting, standards diffusion, expert authority, and infrastructural interdependence rather than formal supranational sovereignty. That distinction matters. It clarifies why both celebratory and apocalyptic readings are inadequate.

The strongest critical conclusion is therefore institutional rather than sensational. The GDC should be understood as part of a broader shift from fragmented digital governance toward layered transnational coordination over the terms of inclusion, legitimacy, and technical interoperability. In a world marked by deep digital inequality, cyber insecurity, platform concentration, and rapid AI development, some degree of coordination is necessary. Yet coordination becomes dangerous when it is treated as self-justifying, when rights language substitutes for enforceable safeguards, or when infrastructures of access become infrastructures of dependence.

A publishable and analytically serious critique of the UN’s digital agenda must therefore do two things at once. It must acknowledge the genuine developmental and governance problems that the GDC seeks to address. And it must insist that global digital cooperation be judged not only by the scale of its ambitions but by the limits it places on its own power. The future of digital governance should not be measured merely by interoperability, safety, or administrative reach. It should be measured by whether human beings remain more than data subjects, whether lawful dissent remains possible, and whether the architectures built in the name of inclusion remain answerable to the dignity and agency of the persons they govern.

References

Abbott, K. W., & Snidal, D. (2000). Hard and soft law in international governance. International Organization,

- 54(3), 421–456.
<https://doi.org/10.1162/002081800551280>
- Access Now. (2024, October 24). A human rights-centered approach to digital public infrastructure.
<https://www.accessnow.org/guide/digital-public-infrastructure/>
- Carozza, P. G. (2003). Subsidiarity as a structural principle of international human rights law. *American Journal of International Law*, 97(1), 38–79.
<https://www.cambridge.org/core/journals/american-journal-of-international-law/article/subsidiarity-as-a-structural-principle-of-international-human-rights-law/E7CE150E892CF4593B950F4F308AE12F>
- Curran, D. (2023). Surveillance capitalism and systemic digital risk: The imperative to collect and connect and the risks of interconnectedness. *Big Data & Society*, 10(1), 1–12.
<https://doi.org/10.1177/20539517231177621>
- European Commission. (n.d.). European digital identity.
https://commission.europa.eu/topics/digital-economy-and-society/european-digital-identity_en
- European Parliament and Council of the European Union. (2022). Regulation (EU) 2022/2065 of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union*, L 277, 1–102.
<https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>
- European Parliament and Council of the European Union. (2024a). Regulation (EU) 2024/1183 of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. *Official Journal of the European Union*, L 2024/1183.
<https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng>
- European Parliament and Council of the European Union. (2024b). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*, L 2024/1689.
<https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
- Gorwa, R. (2019). What is platform governance? *Information, Communication & Society*, 22(6), 854–871.
<https://doi.org/10.1080/1369118X.2019.1573914>
- Gwagwa, A., & Mollema, W. J. T. (2024). How could the United Nations Global Digital Compact prevent cultural imposition and hermeneutical injustice? *Patterns*, 5(11), Article 101078.
<https://doi.org/10.1016/j.patter.2024.101078>
- Helberger, N., Pierson, J., & Poell, T. (2018). Governing online platforms: From contested to cooperative responsibility. *The Information Society*, 34(1), 1–14.
<https://doi.org/10.1080/01972243.2017.1391913>
- Illes, A., Kosse, A., & Wierds, P. (2025). Advancing in tandem: Results of the 2024 BIS survey on central bank digital currencies and crypto (BIS Papers No. 159). Bank for International Settlements.
<https://www.bis.org/publ/bppdf/bispap159.htm>
- International Telecommunication Union. (2003). Declaration of principles: Building the information society, a global challenge in the new millennium. World Summit on the Information Society.
<https://www.itu.int/net/wsis/docs/geneva/official/dop.html>
- International Telecommunication Union. (2005). Tunis Agenda for the Information Society. World Summit on the Information Society.
https://www.itu.int/net/wsis/documents/doc_multi.asp?id=2267&lang=en
- Lemke, T. (2002). Foucault, governmentality, and critique. *Rethinking Marxism*, 14(3), 49–64.
<https://doi.org/10.1080/089356902101242288>
- Lerner, C. S. (2018). The tower of Babel revisited: Global governance as a problematic solution to existential threats. *North Carolina Journal of Law & Technology*, 19(1), 69–121.
<https://scholarship.law.unc.edu/ncjolt/vol19/iss1/4/>
- Nussbaum, M. C. (2011). *Creating capabilities: The human development approach*. Harvard University Press.
<https://www.hup.harvard.edu/books/9780674072350>
- Office for Digital and Emerging Technologies. (2025a). Office for Digital and Emerging Technologies. United Nations.
<https://www.un.org/digital-emerging-technologies/>
- Office for Digital and Emerging Technologies. (2025b). Global Digital Compact. United Nations.
<https://www.un.org/digital-emerging-technologies/content/global-digital-compact>
- Office for Digital and Emerging Technologies. (2025c). AI panel and dialogue. United Nations.
<https://www.un.org/global-digital-compact/en/ai>

- Office of the United Nations High Commissioner for Human Rights. (2022, September 15). Spyware and surveillance: Threats to privacy and human rights growing, UN report warns. <https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report>
- Office of the United Nations High Commissioner for Human Rights. (2022). The right to privacy in the digital age (A/HRC/51/17). <https://www.ohchr.org/en/documents/thematic-report/s/ahrc5117-right-privacy-digital-age>
- Office of the United Nations High Commissioner for Human Rights. (2024). A/HRC/56/45: Mapping report: Human rights and new and emerging digital technologies. <https://www.ohchr.org/en/documents/thematic-report/s/ahrc5645-mapping-report-human-rights-and-new-and-emerging-digital>
- Plantin, J.-C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media & Society*, 20(1), 293–310. <https://doi.org/10.1177/1461444816661553>
- Pswarayi-Riddihough, I., Singh, K., Ansar, S., & Wolff, J. (2025, October 30). Global progress in identification: 3 findings from the latest data. *World Bank Blogs*. <https://blogs.worldbank.org/en/digital-development/global-progress-in-identification--3-findings-from-the-latest-data>
- Sangwa, S. (2025a). Universal Digital Identity in Africa: Biometric Surveillance, Data Sovereignty, and Eschatological Risks. *Open Journal of AI, Ethics & Society* (ISSN: 3105-3076), 1(2). <https://doi.org/10.65655/8tws4c18>
- Sangwa, S., & Mutabazi, P. (2025a). Misinformation Laws and Free Speech: Biblical Theology and Constitutional Principles for Global Social Media Governance. *Open Journal of Business Theology* (ISSN : 2788-709X), 5(3). <https://doi.org/10.65655/0nwajh64>
- Sangwa, S., & Mutabazi, P. (2025b). Programmable CBDCs, Digital Identity, ISO 20022, and AI: Reconfiguring Power in Payment Infrastructures. *Open Journal of Stewardship Economics & Ethical Innovation* (ISSN: 3105-3068), 1(2). <https://doi.org/10.65655/p0w2r666>
- Scholte, J. A. (2023). Norm dynamics in a post-hegemonic world: Multistakeholder global governance after liberal order. *Review of International Political Economy*, 30(4), 987-1013. <https://doi.org/10.1080/09692290.2023.2213441>
- Teo, S. A. (2023). Human dignity and AI: Mapping the contours and utility of human dignity in addressing challenges presented by AI. *Law, Innovation and Technology*, 15(1), 241–279. <https://doi.org/10.1080/17579961.2023.2184132>
- Umbrello, S., & O'Hara, P. (2025). Human dignity in the digital age. *Journal of Ethics and Emerging Technologies*, 35(1). <https://doi.org/10.55613/jeet.v35i1.165>
- UNESCO. (2023). Guidelines for the governance of digital platforms. <https://www.unesco.org/en/internet-trust/guidelines>
- United Nations Advisory Body on Artificial Intelligence. (2024). Governing AI for humanity: Final report. https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf
- United Nations Department of Economic and Social Affairs. (n.d.). Internet Governance Forum. <https://publicadministration.un.org/en/themes/digital-government/wsisis/internet-governance-forum>
- United Nations Development Programme. (2023, September 15). Governing digital legal ID systems effectively to ensure inclusion and respect for human rights. <https://www.undp.org/digital/blog/governing-digital-legal-id-systems-effectively-ensure-inclusion-and-respect-human-rights>
- United Nations Development Programme. (2024a). The DPI approach: A playbook. <https://www.undp.org/publications/dpi-approach-playbook>
- United Nations Development Programme. (2024b, September 22). UN releases Universal DPI Safeguards Framework to promote safe and inclusive digital public infrastructure. <https://www.undp.org/press-releases/un-releases-universal-dpi-safeguards-framework-promote-safe-and-inclusive-digital-public-infrastructure>
- United Nations General Assembly. (2025). Terms of reference and modalities for the establishment and functioning of the Independent International

- Scientific Panel on Artificial Intelligence and the Global Dialogue on Artificial Intelligence Governance (A/RES/79/325). United Nations Digital Library.
https://digitallibrary.un.org/record/4087699/files/A_RES_79_325-EN.pdf
- United Nations Statistics Division. (n.d.). UN Legal Identity Agenda.
<https://unstats.un.org/legal-identity-agenda/>
- United Nations. (2019). The age of digital interdependence: Report of the UN Secretary-General's High-level Panel on Digital Cooperation.
https://www.un.org/techenvoy/sites/www.un.org/techenvoy/files/hlp_on_digital_cooperation-report_final.pdf
- United Nations. (2020). Roadmap for digital cooperation.
https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf
- United Nations. (2023). Our Common Agenda: Policy brief 5. A Global Digital Compact—An open, free and secure digital future for all.
<https://www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-global-digital-compact-en.pdf>
- United Nations. (2024a). Pact for the Future (A/RES/79/1).
<https://www.un.org/en/summit-of-the-future/pact-for-the-future>
- United Nations. (2024b). Global Digital Compact.
https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf
- United Nations. (2024c). United Nations Global Principles for Information Integrity.
<https://www.un.org/sites/un2.un.org/files/un-global-principles-for-information-integrity-en.pdf>
- United Nations. (2024d). United Nations Convention against Cybercrime; Strengthening international cooperation for combating certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes (A/RES/79/243).
<https://digitallibrary.un.org/record/4071955>
- World Bank. (2025a). Identification for Development (ID4D) global dataset.
<https://id4d.worldbank.org/global-dataset>