

# From Information Integrity to Epistemic Centralization: Stigmatized Knowledge, Suppressed Discourses, and the United Nations' Global Digital Compact

*A Scripture-First Critical Analysis of Networked Digital Governance*

Sixbert SANGWA<sup>1\*</sup>

<sup>1</sup>Open Christian University, Sacramento, California, United States

\*Correspondence: [ssangwa@openchristian.education](mailto:ssangwa@openchristian.education)

## Abstract

This article examines the United Nations' Pact for the Future and its annexed Global Digital Compact as an emerging architecture of digital metagovernance with significant implications for stigmatized knowledge, suppressed discourse, and epistemic freedom. Rather than equating global digital coordination with a fully fledged world government, the article distinguishes globalization, harmonization, interoperability, centralization, and epistemic authority. Using a critical documentary analysis of major UN-system, regulatory, and policy texts from 2003 to 2026, supported by PRISMA-informed corpus documentation and Scripture-first normative reflection, the study argues that the most defensible diagnosis is networked centralization: a layered system of agenda-setting, soft-law standardization, infrastructural dependency, platform governance, AI coordination, and shared categories of legitimate digital knowledge. The analysis shows how concepts such as information integrity, trust, safety, resilience, harmful content, misinformation, disinformation, and authoritative sources may address real digital harms while also creating conditions for epistemic overreach, viewpoint policing, function creep, and the suppression of inconvenient or nonconforming claims. Bringing global-governance theory, governmentality, surveillance capitalism, agenda-setting and framing theory, scholarship on stigmatized knowledge, and Christian theological ethics into conversation, the article contends that digital governance must be judged not only by efficiency, inclusion, and safety, but also by its treatment of truth, conscience, dissent, human dignity, due process, national sovereignty, and the legitimate diversity of peoples before God. The article concludes by proposing safeguards for rights-constrained coordination, including viewpoint-neutral due process, independent oversight, auditability, anti-function-creep protections, protection for dissenting inquiry, preservation of offline alternatives, and non-coercive digital participation.

**Keywords:** *Global Digital Compact; Pact for the Future; stigmatized knowledge; suppressed discourse; information integrity; epistemic centralization; digital governance; surveillance capitalism; digital identity; platform governance; Christian ethics; conscience; technocracy*

**Accepted:** Jul 05, 2026

**Published:** Jul 05, 2026

## CITATION

Sangwa, S. (2026). *From Information Integrity to Epistemic Centralization: Stigmatized Knowledge, Suppressed Discourses, and the United Nations' Global Digital Compact*. *Open Journal of Stigmatized Knowledge & Suppressed Discourses*, Vol. 2(2). Open Christian Press.

## DOI:

[10.65655/openchristianpress.139](https://doi.org/10.65655/openchristianpress.139)

## COPYRIGHT

Open Journal of Stigmatized Knowledge & Suppressed Discourses is published by Open Christian Press. This work is licensed under the Creative Commons Attribution (CC BY) license. Copyright © 2026 by author.

## PUBLISHER INFO

Open Christian Press - the publishing arm of Open Christian University - is produced in partnership with the Center for Faith and Work.

## DISCLAIMER

The views expressed in this work are solely those of the author and do not necessarily represent the positions of the publisher, the funders, or the author's affiliated institution.

# 1. Introduction: Digital Governance as Epistemic Ordering

On 22 September 2024, the United Nations General Assembly adopted the Pact for the Future, including annex I, the Global Digital Compact (GDC), as part of the Summit of the Future process (United Nations General Assembly [UNGA], 2024a). The Pact presents itself as a response to interconnected global risks that exceed the capacity of any single state and therefore require renewed, sustained, and strengthened international cooperation. Its digital annex is especially consequential because it does not address only one technology or one sector. It links universal connectivity, digital public infrastructure, data governance, online safety, human rights, platform accountability, artificial intelligence, and UN follow-up mechanisms within a single normative architecture.

This architecture is not emerging in a technological vacuum. The International Telecommunication Union (2025) estimates that almost three-quarters of the global population are now online, while 2.2 billion people remain offline. The World Bank's 2025 Identification for Development data indicate that approximately 800 million people still lack official identification and at least 2.8 billion lack access to government-recognized digital identity for secure online transactions (World Bank, 2025). The Atlantic Council's CBDC Tracker reported in May 2026 that 146 countries and currency unions, representing more than 98% of global GDP, were exploring central bank digital currencies, while the Bank for International Settlements found that 91% of surveyed central banks were exploring retail CBDCs, wholesale CBDCs, or both (Atlantic Council, 2026; Illes et al., 2025). These developments do not prove a single hidden plan. They do, however, show that the material conditions for interoperable digital governance are rapidly maturing.

The central concern of this article is epistemic rather than merely technical. Digital governance does not simply govern devices, infrastructures, data flows, and platforms. It also governs the public status of knowledge. Once global institutions, state

regulators, platform companies, expert panels, fact-checking systems, AI assessment bodies, and cybercrime frameworks converge around categories such as misinformation, disinformation, harmful content, information integrity, trusted sources, resilience, and authoritative information, they do more than describe digital harms. They shape what may circulate as legitimate public knowledge. They influence which claims are amplified, contested, labelled, demonetized, down-ranked, investigated, archived, removed, or treated as socially dangerous.

This does not mean that misinformation, disinformation, hate speech, propaganda, and AI-enabled manipulation are imaginary. The Pact and GDC are responding to genuine harms. Digital technologies can amplify fraud, incitement, synthetic media, foreign interference, reputational attacks, exploitative targeting, and attacks on democratic trust. The question is not whether digital harms should be ignored. They should not be ignored. The question is whether the institutional response to those harms can create a second-order problem: the concentration of epistemic authority in a transnational governance ecology that increasingly decides the boundaries of acceptable knowledge and dissent.

## 1.1 Background and problem statement

The Pact and GDC stand within a longer institutional genealogy. The World Summit on the Information Society (WSIS) in Geneva in 2003 and Tunis in 2005 articulated a people-centered information society and institutionalized multistakeholder internet-governance coordination (International Telecommunication Union [ITU], 2003, 2005). The 2015 WSIS+10 outcome document reaffirmed this trajectory, while the 2019 High-level Panel on Digital Cooperation, the 2020 Roadmap for Digital Cooperation, the 2021 report *Our Common Agenda*, and the 2023 policy brief on a Global Digital Compact progressively broadened the agenda from internet governance to digital public goods, AI, trust, security, data, and institutional architecture (High-level Panel on Digital Cooperation, 2019; United Nations, 2020, 2021, 2023a; UNGA, 2015b). The 2024 Pact consolidated those strands, and the post-2024 architecture has

continued through the creation of the United Nations Office for Digital and Emerging Technologies and the establishment of the Independent International Scientific Panel on Artificial Intelligence and the Global Dialogue on AI Governance (United Nations Office for Digital and Emerging Technologies, 2025; UNGA, 2025).

The problem is not cooperation as such. A responsible critique must distinguish cooperation from centralization, and centralization from conspiracy. Cooperation may be needed where harms are transnational, technical, and distributed. Centralization, however, arises when authority, standards, categories, infrastructures, and interpretive power increasingly concentrate in fewer institutional nodes, even when formal sovereignty remains with states. The article therefore rejects two weak readings. It rejects institutional complacency, which treats every global digital initiative as benign because it uses the language of rights and inclusion. It also rejects sensational inflation, which treats every instance of multilateral coordination as proof of imminent world government.

The more defensible diagnosis is networked centralization. Under networked centralization, no single world sovereign directly governs the digital realm. Instead, agenda-setting, soft-law standards, interoperability requirements, platform governance, digital identity systems, AI assessment bodies, cybercrime cooperation, and funding or benchmarking mechanisms become mutually reinforcing. The effect is not direct command but structured dependency. The central question becomes: who can define the categories, standards, infrastructures, and knowledge criteria through which others must increasingly operate?

## 1.2 Research aim and questions

The aim of this article is to examine how the Pact for the Future and Global Digital Compact participate in the formation of networked digital governance and how that architecture may affect stigmatized knowledge, suppressed discourse, public dissent, and Christian conscience. The study is guided by four research questions:

*RQ1. How do the Pact for the Future and Global Digital Compact construct the categories of legitimate and illegitimate digital knowledge?*

*RQ2. How do concepts such as information integrity, trust, safety, resilience, harmful content, and disinformation function as epistemic frames within global digital governance?*

*RQ3. How might soft-law convergence, platform governance, digital identity, AI assessment, cybercrime cooperation, and interoperable digital infrastructures contribute to the stigmatization or suppression of contested knowledge?*

*RQ4. What safeguards are needed to preserve truthful inquiry, public dissent, theological conscience, epistemic pluralism, and human dignity without denying the real harms of manipulation, propaganda, and digital falsehood?*

## 1.3 Contribution to the Open Journal of Stigmatized Knowledge & Suppressed Discourses

This article contributes to the journal's concern with knowledge that is marginalized, discredited, labelled, suppressed, or treated as dangerous by dominant institutions. It does not romanticize stigmatized knowledge. Some stigmatized claims are false, poorly evidenced, manipulative, or morally dangerous. Yet the category remains analytically important because institutional rejection does not by itself prove falsehood, and dissenting knowledge has often been marginalized before being reconsidered, refined, or vindicated.

The article's distinctive contribution is to locate stigmatized knowledge within the emerging architecture of global digital governance. It asks how information-integrity regimes, platform moderation, digital identity, AI assessment, and cross-border cybercrime cooperation can shape not only what people know, but what they are allowed to ask, doubt, test, publish, or confess. It also brings Scripture-first Christian discernment into conversation with digital-governance scholarship, arguing that Christian critique must resist both gullibility toward institutional consensus and undisciplined speculation about hidden power.

## 2. Conceptual Framework: Stigmatized Knowledge, Epistemic Centralization, and Networked Governance

### 2.1 Stigmatized knowledge and suppressed discourse

Michael Barkun's notion of stigmatized knowledge is useful because it names claims that adherents understand as excluded, rejected, or marginalized by authoritative knowledge institutions (Barkun, 2013, 2016). Such knowledge may include religious interpretations, dissident political analysis, alternative medical claims, fringe science, suppressed-document claims, and conspiracy narratives. The concept does not decide truth in advance. It describes a social and epistemic location: a claim exists in tension with institutions that claim authority to distinguish knowledge from error.

This distinction matters because the phrase conspiracy theory has become both an analytic category and a rhetorical weapon. Psychological research rightly shows that conspiracy beliefs can be associated with distrust, perceived loss of control, motivated reasoning, group identity, and resistance to correction (Douglas et al., 2017, 2019; van Prooijen & Douglas, 2017). Yet public use of the label can also terminate inquiry prematurely. A claim may be dismissed not because it has been carefully falsified, but because its implications are institutionally inconvenient or socially costly. The task is therefore disciplined discernment: neither automatically accepting stigmatized knowledge as truth nor automatically accepting institutional rejection as proof of falsehood.

Suppressed discourse includes both overt restriction and softer mechanisms of visibility control. In digital environments, suppression can occur through deletion, demonetization, account suspension, automated downranking, search demotion, warning labels, opaque fact-checking, payment-platform restrictions, deboosting, advertiser exclusion, professional sanctions, or anticipatory self-censorship. Some of these

practices may be justified where speech directly incites harm, enables fraud, or violates clear legal standards. The danger appears when broad harm categories are used without transparency, notice, proportionality, appeal, or viewpoint-neutral safeguards.

### 2.2 Information integrity as an epistemic-governance frame

The GDC's section on information integrity declares access to relevant, reliable, and accurate information and knowledge essential to an inclusive, open, safe, and secure digital space. It also commits states to strengthen cooperation against misinformation, disinformation, hate speech, and information manipulation in a manner consistent with international law (UNGA, 2024a). The language is normatively attractive. Few would openly defend manipulation, hate, or falsehood. Yet precisely because the vocabulary is morally attractive, it deserves careful analysis.

Agenda-setting theory helps explain how repeated institutional attention makes certain problems appear more urgent than others (McCombs & Shaw, 1972). Framing theory adds that the way a problem is named and morally charged shapes the range of acceptable remedies (Entman, 1993). Framing digital speech through information integrity, safety, resilience, and trusted sources does not merely identify problems. It directs attention toward particular forms of expert-led, platform-mediated, state-corporate, and standards-based intervention. The frame can protect the public from real manipulation, but it can also create a presumption that disagreement with institutional definitions of truth is itself a threat to social order.

This is the epistemic ambiguity at the heart of the GDC. The same language that can strengthen media literacy, platform transparency, and independent journalism can also justify overbroad moderation, administrative suspicion of dissent, and dependence on official or semi-official truth pipelines. The question is not whether information integrity is good in the abstract. The question is who defines integrity, by what standards, with what

safeguards, and with what remedies when authorized systems are wrong.

### 2.3 Networked centralization and governmentality

Networked centralization refers to the concentration of practical governance power through mutually reinforcing networks rather than through a single formal sovereign. It arises when institutions do not directly command all behavior but shape the standards, incentives, categories, infrastructures, and expectations through which conduct becomes governable. The concept therefore avoids the imprecision of claiming that the UN is constructing a world digital government while also avoiding the naivete of assuming that non-binding instruments have no political effect.

Foucault's concept of governmentality, especially as reconstructed by Lemke (2011), helps clarify how power can operate through norms, expertise, metrics, classification, and self-regulation. Under governmentality, power does not always announce itself as censorship or command. It appears as guidance, best practice, capacity building, audit readiness, platform responsibility, risk mitigation, resilience training, dashboard indicators, or interoperability standards. Such mechanisms can produce compliance because actors learn to govern themselves according to accepted categories before coercion is needed.

In global digital governance, this means that soft law matters. Declarations, guidelines, principles, scientific panels, reporting processes, and review meetings may not be directly enforceable, but they can shape subsequent hard law, procurement rules, donor priorities, research funding, platform policies, risk assessments, and domestic regulatory templates. The GDC's high-level review process during the eighty-second session of the General Assembly gives this architecture a continuing institutional life (UNGA, 2024a).

### 2.4 Surveillance capitalism and platform power

Zuboff's account of surveillance capitalism shows that contemporary digital governance is layered

onto a market order already shaped by behavioral data extraction, profiling, attention optimization, and prediction (Zuboff, 2019). Major platforms do not merely host speech. They structure visibility, relevance, virality, monetization, reputation, and public credibility. Gillespie (2018) therefore describes platforms as custodians whose moderation decisions shape the conditions of online public life. Gorwa (2019) similarly argues that platform governance involves the rules, practices, interfaces, and decision systems through which platforms manage users, content, data, and third-party relationships.

This creates a paradox for the GDC. The platforms whose business models have often intensified information disorder are also invited to become partners in correcting it. UN and UNESCO documents call for transparency, accountability, researcher access, and rights-respecting moderation (UNESCO, 2023; UNGA, 2024a). Those safeguards are important. Yet the political economy remains unresolved. If information integrity is implemented through the same data-intensive platforms that profit from attention capture, society may receive more centralized speech governance without a corresponding redistribution of communicative power.

### 2.5 Scripture-first discernment and the limits of technocracy

A Scripture-first approach does not mean that public evidence, legal analysis, social theory, or technical expertise are irrelevant. It means that Christian moral judgment is finally normed by Scripture rather than by institutional prestige, platform affect, technocratic consensus, or fear-driven speculation. Scripture gives categories for truth, false witness, human dignity, conscience, idolatry, Babel-like centralization, and coercive power.

The Babel account in Genesis 11:1-9 warns against human unity ordered to self-exaltation, security, and autonomous name-making rather than obedience to God. This does not condemn all cooperation. It cautions against totalizing projects

that collapse plurality into a single human scheme of control.

The doctrine of the image of God in Genesis 1:26-27 grounds human dignity in divine creation rather than administrative visibility or digital legibility.

The command against false witness in Exodus 20:16 means that Christians must oppose lies, manipulation, and slander, including when such harms occur through digital systems.

At the same time, the warning in Revelation 13:16-17 provides a sober moral pattern concerning systems that condition economic participation on allegiance or credentials. The article does not claim that current digital-governance projects are the final fulfillment of that text. It argues more modestly that Scripture trains Christians to scrutinize systems that can fuse recognition, exchange, conscience, and coercive authority.

### 3. Methodology

#### 3.1 Design

The study uses a critical documentary-analysis design supported by Scripture-first normative reflection. It does not claim to be an empirical content analysis of a quantified text corpus, an NLP-assisted discourse study, a systematic review, or a meta-analysis. The PRISMA-informed record included below is used only to make document selection transparent. It records the identification, screening, exclusion, and inclusion of documents used in the argument. It should not be read as a claim to exhaustive database coverage or statistical synthesis.

Critical documentary analysis is appropriate because the research questions concern the language, assumptions, institutional logic, safeguards, and implications of public governance texts. The method prioritizes primary institutional documents, official legal texts, and peer-reviewed

scholarship. It distinguishes verified fact, plausible interpretation, and unsupported speculation. Verified fact refers to claims supported by official documents, credible public records, peer-reviewed scholarship, or reliable institutional data. Plausible interpretation refers to disciplined analytical or theological judgment consistent with the evidence but open to correction. Unsupported speculation refers to claims asserting hidden causal chains, final prophetic fulfillment, or certainty beyond what the evidence and Scripture support.

#### 3.2 Corpus and source selection

The primary corpus comprises major UN-system and closely related normative texts from 2003 to 2026: the WSIS Geneva Declaration and Tunis Agenda, the 2030 Agenda and WSIS+10 outcome document, the High-level Panel report *The Age of Digital Interdependence*, the Roadmap for Digital Cooperation, *Our Common Agenda*, the 2023 policy brief on a Global Digital Compact, UNESCO's Recommendation on the Ethics of Artificial Intelligence, UNESCO's Guidelines for the Governance of Digital Platforms, the United Nations Global Principles for Information Integrity, the Pact for the Future and its GDC annex, the 2024 UN Convention against Cybercrime, the 2024 UN system white paper on AI governance, the creation of ODET, and the 2025 resolution establishing the UN AI Panel and Global Dialogue.

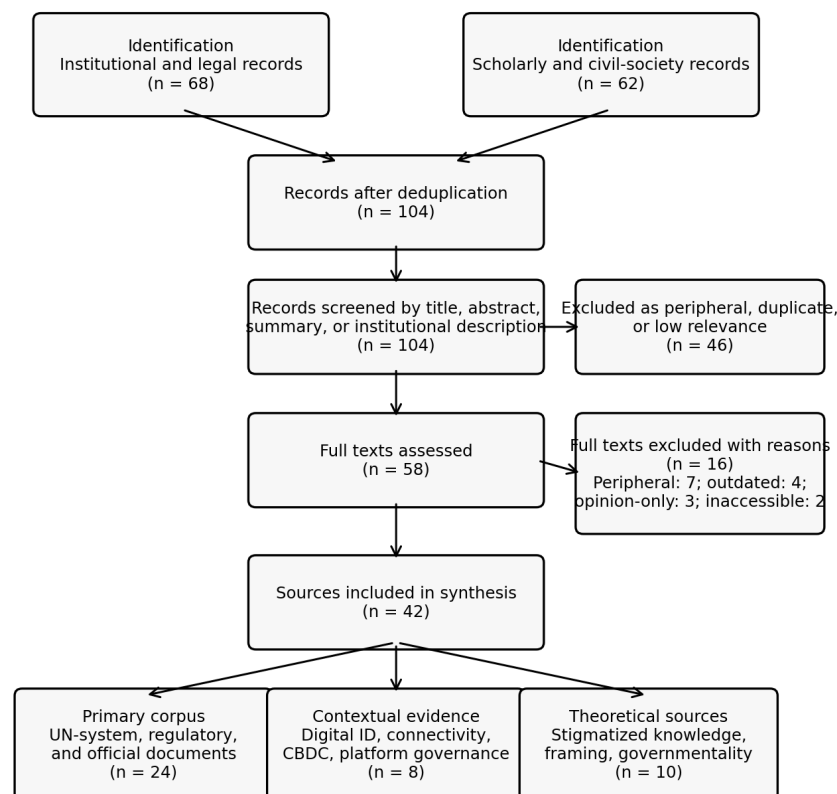
Contextual sources include ITU connectivity statistics, World Bank ID4D data, BIS and Atlantic Council CBDC evidence, and EU regulations on platform governance, digital identity, and AI. Theoretical sources include scholarship on stigmatized knowledge, conspiracy belief, agenda-setting, framing, governmentality, surveillance capitalism, platform governance, digital identity, and AI governance. Civil-society sources were used selectively where they illuminate human-rights concerns around surveillance, cybercrime, digital identity, or online speech.

**Table 1. PRISMA-informed documentary source selection record**

| Stage          | Records or documents                                                                                                                                                             | Count        | Decision logic                                                                                                                                                                |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Identification | Official institutional, legal, regulatory, scholarly, and civil-society records identified through UN, UNESCO, ITU, World Bank, BIS, EU, publisher, and citation-chain searches. | 130          | Broad capture of potentially relevant sources on the GDC, information integrity, digital identity, platform governance, AI governance, cybercrime, and stigmatized knowledge. |
| Deduplication  | Duplicate records, repeated versions, superseded copies, and mirror pages removed.                                                                                               | 26 removed   | Where official and mirror copies existed, official institutional sources were preferred.                                                                                      |
| Screening      | Titles, abstracts, summaries, and institutional descriptions screened for direct relevance.                                                                                      | 104 screened | Peripheral materials, general commentary, and materials unrelated to governance, knowledge classification, or suppression risk were excluded.                                 |
| Eligibility    | Full texts assessed for authority, relevance, recency, and evidentiary value.                                                                                                    | 58 assessed  | Primary documents and peer-reviewed scholarship were prioritized over polemical commentary.                                                                                   |
| Exclusion      | Full-text exclusions.                                                                                                                                                            | 16 excluded  | Peripheral to research questions (7), outdated or superseded (4), opinion-only without evidentiary value (3), inaccessible or insufficiently verifiable (2).                  |
| Inclusion      | Sources retained for synthesis.                                                                                                                                                  | 42 included  | Twenty-four primary official or regulatory sources, eight contextual data or policy sources, and ten theoretical sources were used as the core evidentiary base.              |

*Note. This PRISMA-informed record documents corpus construction for a critical documentary analysis. It does not claim meta-analysis, exhaustive systematic-review coverage, or quantitative effect synthesis.*

Figure 1 presents the PRISMA-informed document-selection flow. The figure is included to make the source-audit process transparent and replicable without overstating the method as a systematic review.



Note. The flow is PRISMA-informed for transparency in document selection. It does not claim meta-analysis or exhaustive systematic-review coverage.

**Figure 1. PRISMA-informed source selection flow for the documentary corpus**

Note. The flow records the source selection process used for this article. It is PRISMA-informed for transparency but does not claim meta-analysis.

### 3.3 Analytical procedure, trustworthiness, and limitations

The analysis proceeded in four steps. First, documents were mapped chronologically to establish the genealogy from WSIS to the Pact, GDC, ODET, and AI follow-up architecture. Second, the texts were examined for categories that centralize epistemic authority, including information integrity, trust, safety, resilience, harmful content, authoritative information, misinformation, disinformation, and platform accountability. Third, the analysis identified infrastructure-linked mechanisms, including digital

identity, data governance, AI assessment, content moderation, cybercrime cooperation, and CBDC-adjacent developments. Fourth, the findings were interpreted through the conceptual framework of stigmatized knowledge, networked centralization, governmentality, surveillance capitalism, framing theory, and Scripture-first Christian ethics.

Trustworthiness was strengthened through source hierarchy, triangulation, and conceptual discipline. Official claims were checked against official sources where possible. Regulatory claims were grounded in legal texts. Technical and economic claims were supported by institutional data sources such as ITU, World Bank, BIS, and the Atlantic Council. Interpretive claims were stated as interpretations, not as hidden certainties. Theological claims were

treated as normative judgments rooted in Scripture rather than as empirical proof of prophetic fulfillment.

The study has limits. It does not interview UN officials, platform companies, civil-society organizations, or affected communities. It does not measure platform moderation outcomes or conduct a computational corpus analysis. It does not prove intention, conspiracy, or causality in a strict positivist sense. Its strength lies in transparent conceptual clarification, close reading of public documents, and disciplined synthesis across official, regulatory, scholarly, and theological sources.

## 4. Findings and Discussion

The findings are organized around the four research questions. They show that the UN digital-governance architecture is cumulative, that information integrity functions as an epistemic-governance frame, that several infrastructure and platform layers can make suppression easier even without formal censorship, and that Christian discernment requires both truthfulness and resistance to coercive knowledge regimes.

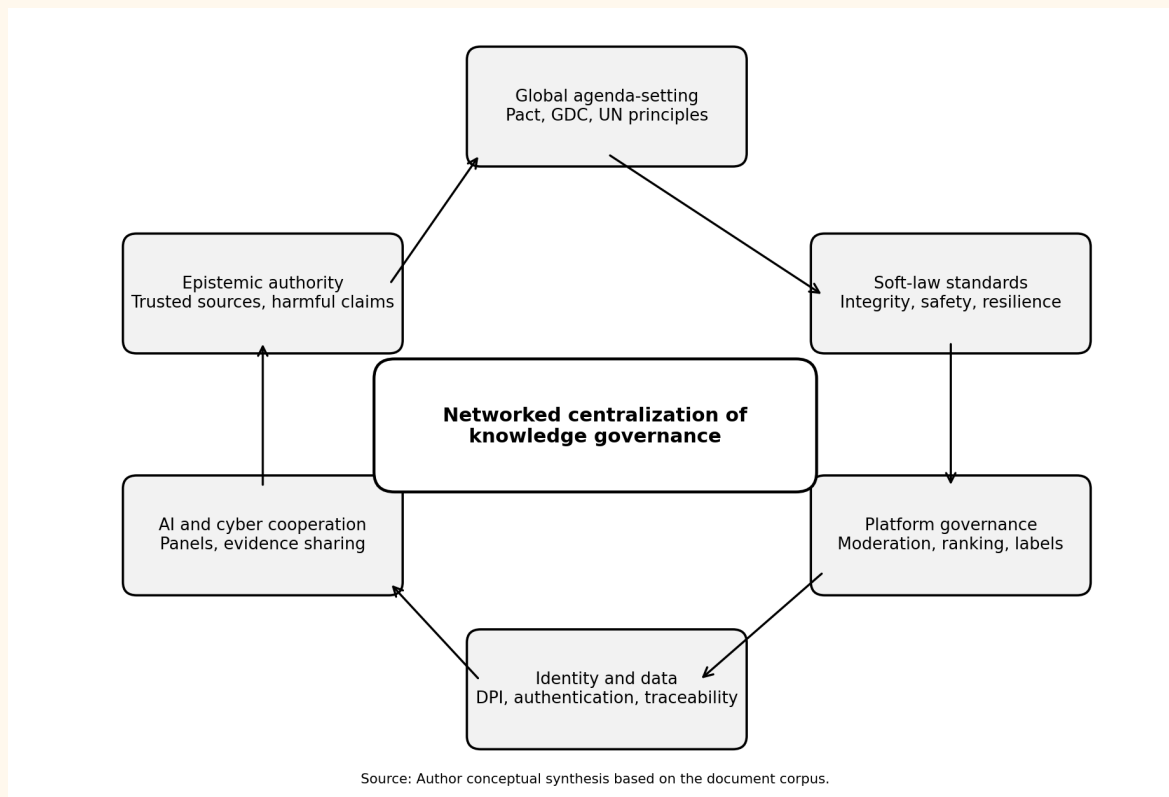
### 4.1 From digital cooperation to networked centralization

The first finding is that the UN digital-governance architecture is cumulative rather than episodic. WSIS established a normative and institutional vocabulary for an inclusive information society and multistakeholder internet governance. The Roadmap for Digital Cooperation expanded this vocabulary into areas such as universal connectivity, digital public goods, digital inclusion,

human rights, AI cooperation, trust, security, and stronger institutional architecture (United Nations, 2020). Our Common Agenda then situated digital cooperation within a larger renewal of multilateralism (United Nations, 2021). The 2023 GDC policy brief specified principles and proposed action pathways, and the 2024 Pact consolidated those pathways into a General Assembly-adopted political instrument (United Nations, 2023a; UNGA, 2024a).

This genealogy matters because it shows that the Pact is not simply rhetorical. It is one layer in a long institutional sequence. The establishment of ODET and the 2025 AI Panel and Global Dialogue further institutionalize follow-up capacity (UNGA, 2025; United Nations Office for Digital and Emerging Technologies, 2025). This does not amount to a world digital government. The field remains dispersed across states, regional blocs, technical bodies, private firms, civil society, courts, central banks, and international organizations. Yet soft-law instruments can still shape future hard law, procurement standards, platform practices, donor requirements, assessment mechanisms, and domestic regulation.

The most defensible conclusion is therefore asymmetrical: the UN architecture has not abolished national sovereignty, but it can increase the costs of opting out of certain digital trajectories. States may retain formal authority while becoming dependent on shared standards, interoperable infrastructures, common vocabularies, benchmarking expectations, AI assessment frameworks, and platform-governance norms. Figure 2 illustrates this networked centralization loop.



**Figure 2. Networked centralization and epistemic governance loop**

*Note. The figure represents the conceptual synthesis developed in this article. It does not imply direct causality or a single command center.*

## 4.2 Information integrity and the classification of legitimate knowledge

The second finding is that information integrity functions as an epistemic-governance category. In the GDC, information integrity is connected to relevant, reliable, accurate, timely, fact-based, multilingual, and science-based information, as well as to cooperation against misinformation, disinformation, hate speech, and information manipulation (UNGA, 2024a). The text also calls on platforms to enhance transparency around terms of service, content moderation, recommendation algorithms, and the handling of personal data.

The positive side is clear. People need access to reliable information during crises. Independent journalism, media literacy, transparency, and platform accountability are public goods. Vulnerable populations can be harmed by fraudulent claims, incitement, manipulative

targeting, and synthetic media. A Christian ethic of truth cannot treat false witness lightly.

The risk is equally clear. Concepts such as reliable, accurate, safe, harmful, authoritative, and science-based are not self-applying. They require institutions to interpret them. Under conditions of epistemic centralization, dominant actors can turn flexible categories into administrative filters. A claim may be treated as harmful not because it is false in a narrow factual sense, but because it is destabilizing, politically inconvenient, religiously nonconforming, difficult to administer, or contrary to the policy consensus. In that situation, information integrity can drift from process integrity into viewpoint management.

This risk is not an argument for ungoverned falsehood. It is an argument for procedural humility. A governance regime that lacks due process, correction mechanisms, contestability, viewpoint neutrality, and independent review may convert legitimate safety concerns into a machinery of epistemic exclusion. The public should be

protected from manipulation, but it should also be protected from overconfident gatekeepers of truth.

### 4.3 Platform governance and suppression risk

The third finding is that platform governance is the most immediate site where epistemic centralization becomes visible. Platforms structure the visibility and circulation of knowledge through ranking, recommendation, removal, demonetization, labels, search visibility, account verification, advertiser policies, and data access. The EU Digital Services Act demonstrates how platform governance is moving from voluntary self-regulation toward enforceable due-diligence obligations for online intermediaries and very large online platforms (European Union, 2022). UNESCO's platform guidelines similarly call for human-rights-based governance, transparency, due diligence, independent oversight, and multistakeholder participation (UNESCO, 2023).

Such interventions may strengthen accountability. They may compel platforms to explain terms of service, offer appeals, report moderation patterns, and open data to researchers. Yet they also normalize a world in which private infrastructures mediate public truth under pressure from regulators and international norms. In practice, suppression risk often appears less like overt state censorship and more like friction: lower reach, warning labels, account restrictions, demonetization, delayed appeals, or exclusion from advertising and payment ecosystems.

The problem is intensified by asymmetry. Governments, large platforms, international organizations, and funded expert networks have greater capacity to define credible information than small publishers, churches, dissident researchers, whistleblowers, minority communities, and independent journalists. When a contested claim challenges institutional consensus, the claimant may face a triple burden: proving the claim, defending the right to ask the question, and overcoming the reputational stigma of being labelled conspiratorial or harmful.

### 4.4 Digital identity, conditional participation, and function creep

The fourth finding is that digital identity introduces an infrastructural dimension to knowledge governance. The GDC does not mandate one global identity system, and it should not be described as doing so. Yet it sits alongside a broader global push for legal identity, digital public infrastructure, and digitally verifiable credentials. The World Bank's 2025 data show both the persistence of exclusion and the growing importance of digital identity for online transactions (World Bank, 2025). The EU's revised eIDAS Regulation establishes a European Digital Identity Framework and includes safeguards such as user control, free issuance for natural persons, voluntary use, separation of wallet data, and access to services by other existing identification and authentication means (European Union, 2024a).

The point is not that all digital identity is oppressive. Identity can protect people from exclusion, fraud, statelessness, and administrative invisibility. For many vulnerable communities, lack of identity restricts access to banking, employment, mobility, health care, SIM cards, and social protection. The question is what happens when identity systems become infrastructural switch points. When access to welfare, finance, mobility, health, education, communications, and public services increasingly depends on machine-readable credentials, identity becomes more than documentation. It becomes a gate.

Function creep occurs when systems built for one purpose expand into others. Civil registration can become welfare authentication. Welfare authentication can become payment eligibility. Payment eligibility can become behavioral scoring. Online safety tools can become speech traceability. Cybercrime evidence procedures can become generalized surveillance. The risk is not inevitable, but it is structurally plausible wherever interoperability is treated as an unquestioned good and legal purpose limitation is weak.

#### 4.5 AI governance, expert panels, and epistemic authority

AI governance adds a new layer of epistemic centralization because AI systems increasingly mediate search, summarization, education, moderation, translation, risk assessment, and public decision support. UNESCO's 2021 Recommendation on the Ethics of Artificial Intelligence created a global normative vocabulary around human dignity, rights, diversity, and oversight (UNESCO, 2021). The UN system white paper on AI governance and the 2025 AI Panel and Global Dialogue move the issue from abstract ethics toward standing institutional assessment (UN System Chief Executives Board for Coordination, 2024; UNGA, 2025).

Scientific and expert assessment can be valuable. Complex technologies require expertise. Yet expert panels also shape which risks become visible, which evidence counts, which technical standards travel, and which social concerns are treated as legitimate. This is why representation, transparency, public reporting, contestability, and epistemic humility are vital. If AI governance becomes dominated by high-capacity states, major firms, elite universities, and well-funded think tanks, the global majority may be governed by standards it did not meaningfully shape.

For OJ-SKSD's concern with suppressed discourse, the AI layer is especially important because AI tools can automate classification. Labels such as misinformation, extremism, hate, harmful medical content, or coordinated inauthentic behavior can be produced at scale. Automated systems can make suppression faster, less visible, and harder to appeal. Governance must therefore require explainability, human review, audit trails, and meaningful redress where automated systems materially affect speech or participation.

#### 4.6 Cybercrime cooperation and evidentiary centralization

The 2024 United Nations Convention against Cybercrime widens the governance perimeter from platform standards and AI assessment into cross-

border criminal cooperation and electronic evidence sharing (UNGA, 2024b). Cybercrime is real and serious. Ransomware, fraud, child exploitation, malicious intrusion, and transnational digital crime require international cooperation. Yet broad cybercrime instruments can also create risks for journalists, researchers, security experts, dissidents, religious minorities, and civil-society actors if domestic legal systems define online offences expansively or politically.

The key concern is evidentiary centralization. Once digital evidence-sharing procedures become normalized across borders, the reach of domestic surveillance can travel through international cooperation. The appropriate response is not to reject cybercrime cooperation, but to condition it on legality, necessity, proportionality, judicial authorization, rights review, transparency, and limits on repurposing data. Otherwise, the same tools used against ransomware can be used against dissent under the language of public order, misinformation, or national security.

#### 4.7 Stigmatized knowledge in the global digital order

The fifth finding is that the emerging digital-governance order will not stigmatize all knowledge equally. Some kinds of discourse are more vulnerable than others. These include claims that challenge official narratives during crises, religious interpretations of technological control, national-sovereignty objections to global standards, minority scientific views, critiques of corporate platform power, whistleblower claims, dissident geopolitical analysis, and anti-technocratic arguments about digital identity or programmable money.

Some of these claims may be false, exaggerated, or poorly evidenced. Some may be manipulative. Yet a free society cannot rely on stigma as a substitute for evaluation. The epistemic health of the public sphere depends on the ability to distinguish falsehood from dissent, speculation from inquiry, and manipulation from unpopular truth. The label disinformation should not become a container into which powerful actors place whatever is inconvenient to administer.

The article therefore proposes a threefold discipline. First, verified fact should be documented through public evidence, official records, credible reporting, or peer-reviewed research. Second, plausible interpretation should be allowed where evidence supports concern but not certainty. Third, unsupported speculation should be resisted,

especially when it asserts hidden causal chains, final prophetic fulfillment, or certainty without sufficient warrant. This discipline protects society from both deception and censorship. It also protects Christian witness from both naivete and panic.

**Table 2. Selected UN-system instruments and their epistemic-governance implications**

| Instrument and year                                | Institutional locus | Epistemic-governance function                                                                        | Centralization risk                                                                            | Built-in safeguard                                                        |
|----------------------------------------------------|---------------------|------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------|
| WSIS Geneva Declaration (2003)                     | ITU and UN system   | Frames an inclusive information society as a global agenda.                                          | Creates shared normative vocabulary for digital development.                                   | People-centered and rights-grounded language.                             |
| Tunis Agenda (2005)                                | ITU and UN system   | Institutionalizes multistakeholder internet governance.                                              | Normalizes global coordination around internet governance processes.                           | No single internet authority; IGF is deliberative.                        |
| Roadmap for Digital Cooperation (2020)             | Secretary-General   | Bundles connectivity, digital public goods, AI, trust, security, and institutional architecture.     | Moves digital governance beyond technical internet questions toward public-governance systems. | Human-rights commitments and stakeholder inclusion.                       |
| Policy Brief 5: A Global Digital Compact (2023)    | Secretary-General   | Specifies objectives and action pathways for digital cooperation.                                    | Consolidates shared categories for trust, data, platforms, and AI governance.                  | Rights-based and multistakeholder framing.                                |
| Global Principles for Information Integrity (2024) | United Nations      | Stabilizes vocabulary around information integrity, trust, resilience, and digital harms.            | May narrow boundaries of legitimate disagreement if implemented without due process.           | Pluralism, independent media, and rights language.                        |
| Pact for the Future and GDC (2024)                 | UN General Assembly | Integrates connectivity, online safety, data governance, platform accountability, and AI governance. | Creates networked centralization through soft law, review, and institutional follow-up.        | National contexts, human rights, and stakeholder participation.           |
| UN Cybercrime Convention (2024)                    | UN General Assembly | Expands cross-border cooperation and electronic evidence sharing.                                    | May extend surveillance or speech-related enforcement through broad implementation.            | Human-rights and privacy clauses, though implementation remains critical. |
| UN AI Panel and Global Dialogue (2025)             | UN General Assembly | Creates standing mechanisms for AI assessment and deliberation.                                      | Expert assessment may become an epistemic filter if representation is weak.                    | Balanced representation and non-prescriptive scientific assessment.       |

*Note. The table summarizes the analytical reading of key documents. It does not imply malign intent in any instrument.*

#### 4.8 Scripture-first reflection: truth, conscience, and human dignity

A Scripture-first reflection must be sober. Christians should not claim more than Scripture and evidence warrant. The existence of global digital governance, information-integrity language, digital identity, CBDCs, and AI panels does not prove that the final eschatological system has arrived. Yet Scripture does provide durable moral categories for evaluating such systems.

First, truth matters because God is true and false witness is sin. The command in Exodus 20:16 forbids lying against one's neighbor, and this

includes institutional, algorithmic, and platform-mediated forms of distortion.

Second, conscience matters because human beings stand before God. The apostolic warning in Acts 5:29 reminds believers that obedience to God cannot be surrendered to human authority when the two conflict.

Third, human dignity matters because persons bear God's image, as taught in Genesis 1:26-27. The person is not reducible to a data subject, risk score, credential, wallet, or governable node.

Fourth, Babel remains a warning. Genesis 11:1-9 shows that human coordination can become rebellion when unity is ordered to autonomous control rather than humility before God.

Finally, Revelation 13:16-17 should be invoked with care. It is not a license to declare every digital system the mark of the beast. It is, however, a serious biblical warning about the coercive fusion of economic participation, social recognition, political power, and allegiance.

The Christian contribution to this debate is therefore neither panic nor accommodation. It is moral clarification. Digital governance must be judged not only by inclusion metrics, efficiency, safety, and resilience, but by whether it preserves the irreducible dignity of persons, the freedom of conscience, the possibility of truthful dissent, and the legitimate plurality of peoples under God.

## 5. Policy and Theological Implications

### 5.1 Safeguards for epistemic pluralism

Information-integrity initiatives should focus on process integrity rather than viewpoint conformity. The aim should be to make information ecosystems more transparent, accountable, and contestable, not to entrench a permanent priesthood of approved knowledge. This requires notice, reason-giving, appeal rights, independent audits, public-interest researcher access, transparent error correction, and viewpoint-neutral due process where moderation affects reach, monetization, or participation.

Governance should protect independent media, minority scholarship, religious speech, whistleblowing, and good-faith dissent, even when such discourse is uncomfortable. Falsehood should be challenged with evidence. Manipulation should be exposed. Fraud should be punished. Incitement and direct harms should be addressed proportionately. But broad administrative categories should not be allowed to swallow dissent.

### 5.2 Safeguards against function creep

Digital identity, data governance, and cybercrime cooperation require strict purpose limitation. The same identifier should not become a general-

purpose key across every sector without democratic authorization, data minimization, independent oversight, and meaningful alternatives. Systems should be federated where possible, privacy-preserving by design, auditable, contestable, and legally constrained. Offline channels should remain available for basic entitlements. No person should be cut off from essential services because a digital credential fails, is unavailable, or is refused for reasons of conscience.

CBDC-adjacent developments require similar caution. The article does not claim that CBDCs are a UN invention. Their principal engines are central banks, monetary authorities, and bodies such as the BIS. Yet digital identity, interoperable public infrastructure, and programmable payment systems are materially compatible. For that reason, cash or non-programmable payment options, legislative scrutiny, privacy protections, and nondiscrimination rules should be preserved.

### 5.3 Safeguards for conscience and Christian public witness

Christian public witness must defend truth and conscience together. Christians should oppose falsehood, slander, and manipulative digital speech. They should also resist systems that require moral conformity, religious compromise, or ideological assent as a condition of ordinary participation. The church should not retreat from public technological ethics, but neither should it baptize technocratic consensus as though shared governance language were morally neutral.

This means that Christian institutions, journals, pastors, educators, and scholars should cultivate disciplined discernment. Claims should be tested. Evidence should be weighed. Prophecy should not be turned into speculation. Institutional claims should not be accepted merely because they are official. Stigmatized claims should not be accepted merely because they are suppressed. The Christian posture is neither credulity nor cynicism. It is truthful watchfulness under Scripture.

**Table 3. Knowledge-governance risks and safeguards**

| Domain                 | Suppression risk                                                                                                | Vulnerable discourse                                                                                      | Necessary safeguard                                                                                              |
|------------------------|-----------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| Information integrity  | Broad harm categories become containers for politically convenient meanings.                                    | Dissenting scholarship, minority religious claims, national-sovereignty critiques, and contested science. | Viewpoint-neutral due process, reason-giving, appeals, transparent definitions, independent review.              |
| Platform governance    | Moderation, ranking, labels, demonetization, and search demotion suppress visibility without formal censorship. | Independent journalism, churches, whistleblowers, small publishers, and dissident researchers.            | Transparency reports, audit rights, appeal mechanisms, researcher access, and proportionality rules.             |
| Digital identity       | Credentials become switch points for services, mobility, finance, and communication.                            | Persons without ID, conscientious objectors, marginalized groups, and political or religious dissenters.  | Offline alternatives, data minimization, federated design, purpose limitation, non-discrimination, due process.  |
| AI governance          | Expert panels and automated classifiers shape what counts as trustworthy knowledge.                             | Global-majority perspectives, theological claims, minority languages, and non-dominant epistemologies.    | Representative governance, public reporting, contestable assessments, human review, and audit trails.            |
| Cybercrime cooperation | Electronic evidence sharing expands surveillance or speech-related enforcement.                                 | Journalists, researchers, activists, security experts, religious minorities, and opposition voices.       | Judicial authorization, necessity, proportionality, rights review, transparency, and limits on data repurposing. |
| Digital payments       | Programmable or identity-linked payments create economic coercion risk.                                         | Lawful association, religious conscience, political dissent, and alternative economic participation.      | Cash or non-programmable options, legislative scrutiny, privacy by design, and viewpoint nondiscrimination.      |

*Note. The safeguards aim to preserve legitimate coordination while resisting epistemic overreach and function creep.*

## 6. Conclusion

The United Nations' Pact for the Future and Global Digital Compact do not create a formal world digital government. A serious scholarly critique should not claim that they do. The digital-governance field remains distributed across states, regional bodies, firms, technical communities, civil society, courts, central banks, and international organizations. Most UN instruments remain political commitments, principles, guidelines, or coordination frameworks rather than directly enforceable supranational commands.

Yet non-binding does not mean insignificant. The evidence supports a more precise conclusion: the Pact and GDC participate in networked centralization. They thicken a layered architecture of agenda-setting, soft-law standardization, platform accountability, interoperable infrastructure, data governance, AI assessment, cybercrime cooperation, and shared categories of legitimate digital knowledge. The greatest danger is not only surveillance in the narrow sense. It is epistemic centralization: the concentration of interpretive authority over what may be known, doubted, published, labelled, ranked, challenged, or treated as harmful.

This architecture can serve public goods. Connectivity, legal identity, data protection, safer platforms, cybercrime cooperation, and AI accountability matter. But they must not be purchased at the cost of conscience, dignity, due process, national responsibility, epistemic pluralism, or truthful dissent. OJ-SKSD's central concern is therefore not peripheral to digital governance. It is at the heart of the matter. A society that governs speech without humility can suppress truth while claiming to defend it. A church that critiques technology without evidence can bear false witness while claiming discernment. The way forward is neither institutional sedation nor conspiratorial inflation, but disciplined, Scripture-normed, evidence-bound vigilance.

## Declarations

### Ethics statement

This study used publicly available documents and secondary sources only. No human participants, interviews, surveys, private data, or experimental procedures were involved. Formal human-subjects ethics approval was therefore not required.

### Data availability statement

All documents analyzed are publicly available through the official institutional, legal, publisher, or archival URLs listed in the reference section. The PRISMA-informed corpus record is reported in Table 1 and Figure 1. No proprietary dataset was created.

### Funding statement

No external funding was received for this study.

### Conflict of interest statement

The author is affiliated with Open Christian University. Because the target journal is published by Open Christian Press, editorial handling and peer review should be conducted independently of the author to avoid any real or perceived conflict of interest. The author declares no financial conflict of interest.

## Author contribution statement

Sixbert SANGWA is responsible for the conception, design, analysis, interpretation, writing, and final approval of the manuscript.

## References

- Atlantic Council. (2026). Central Bank Digital Currency Tracker. <https://www.atlanticcouncil.org/cbdctracker/>
- Barkun, M. (2013). *A culture of conspiracy: Apocalyptic visions in contemporary America* (2nd ed.). University of California Press. <https://www.ucpress.edu/book/9780520276826/a-culture-of-conspiracy>
- Barkun, M. (2016). Conspiracy theories as stigmatized knowledge. *Diogenes*, 62(3-4), 114-120. <https://doi.org/10.1177/0392192116669288>
- Beduschi, A. (2019). Digital identity: Contemporary challenges for data protection, privacy and non-discrimination rights. *Big Data & Society*, 6(2), 2053951719855091. <https://doi.org/10.1177/2053951719855091>
- Beduschi, A. (2021). Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations. *Data & Policy*, 3, e15. <https://doi.org/10.1017/dap.2021.15>
- Douglas, K. M., Sutton, R. M., & Cichocka, A. (2017). The psychology of conspiracy theories. *Current Directions in Psychological Science*, 26(6), 538-542. <https://doi.org/10.1177/0963721417718261>
- Douglas, K. M., Uscinski, J. E., Sutton, R. M., Cichocka, A., Nefes, T., Ang, C. S., & Deravi, F. (2019). Understanding conspiracy theories. *Political Psychology*, 40(S1), 3-35. <https://doi.org/10.1111/pops.12568>
- Entman, R. M. (1993). Framing: Toward clarification of a fractured paradigm. *Journal of Communication*, 43(4), 51-58. <https://doi.org/10.1111/j.1460-2466.1993.tb01304.x>
- European Union. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act). <https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng>
- European Union. (2024a). Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework. <https://eur-lex.europa.eu/eli/reg/2024/1183/oj/eng>
- European Union. (2024b). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
- Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press. <https://yalebooks.yale.edu/book/9780300261431/custodians-of-the-internet/>
- Gorwa, R. (2019). What is platform governance? *Information, Communication & Society*, 22(6), 854-871. <https://doi.org/10.1080/1369118X.2019.1573914>

- High-level Panel on Digital Cooperation. (2019). The age of digital interdependence. United Nations. [https://www.un.org/techenvoy/sites/www.un.org.technvoy/files/hlp\\_on\\_digital\\_cooperation\\_report\\_final.pdf](https://www.un.org/techenvoy/sites/www.un.org.technvoy/files/hlp_on_digital_cooperation_report_final.pdf)
- Illes, A., Kosse, A., & Wierts, P. (2025). Advancing in tandem: Results of the 2024 BIS survey on central bank digital currencies and crypto. Bank for International Settlements. <https://www.bis.org/publ/bppdf/bispap159.htm>
- International Telecommunication Union. (2003). Geneva Declaration of Principles: Building the Information Society, a global challenge in the new millennium. <https://www.itu.int/net/whis/docs/geneva/official/dop.html>
- International Telecommunication Union. (2005). Tunis Agenda for the Information Society. <https://www.itu.int/net/whis/docs2/tunis/off/6rev1.html>
- International Telecommunication Union. (2025). Measuring digital development: Facts and Figures 2025. <https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx/>
- Lemke, T. (2011). Foucault, governmentality, and critique. Routledge. <https://www.routledge.com/Foucault-Governmentality-and-Critique/Lemke/p/book/9781594516382>
- McCombs, M. E., & Shaw, D. L. (1972). The agenda-setting function of mass media. *Public Opinion Quarterly*, 36(2), 176-187. <https://doi.org/10.1086/267990>
- UNESCO. (2021). Recommendation on the ethics of artificial intelligence. <https://www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence>
- UNESCO. (2023). Guidelines for the governance of digital platforms: Safeguarding freedom of expression and access to information through a multi-stakeholder approach. <https://www.unesco.org/en/internet-trust/guidelines>
- United Nations. (2020). Road map for digital cooperation: Implementation of the recommendations of the High-level Panel on Digital Cooperation. [https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap\\_for\\_Digital\\_Cooperation\\_EN.pdf](https://www.un.org/en/content/digital-cooperation-roadmap/assets/pdf/Roadmap_for_Digital_Cooperation_EN.pdf)
- United Nations. (2021). Our Common Agenda: Report of the Secretary-General (A/75/982). <https://digitallibrary.un.org/record/3939309>
- United Nations. (2023a). Our Common Agenda policy brief 5: A Global Digital Compact. <https://digitallibrary.un.org/record/4011891>
- United Nations. (2024a). United Nations Global Principles for Information Integrity. <https://www.un.org/en/information-integrity/global-principles>
- United Nations Development Programme. (2023). 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 General Assembly. (2015a). Transforming our world: The 2030 Agenda for Sustainable Development (A/RES/70/1). <https://digitallibrary.un.org/record/3923923>
- United Nations General Assembly. (2015b). Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society (A/RES/70/125). <https://digitallibrary.un.org/record/819076>
- United Nations General Assembly. (2024a). The Pact for the Future (A/RES/79/1). <https://digitallibrary.un.org/record/4061879>
- United Nations General Assembly. (2024b). 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>
- 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). <https://digitallibrary.un.org/record/4087699>
- United Nations Office for Digital and Emerging Technologies. (2025). About the Office for Digital and Emerging Technologies. <https://www.un.org/digital-emerging-technologies/content/about>
- United Nations Statistics Division. (n.d.). UN Legal Identity Agenda. <https://unstats.un.org/legal-identity-agenda/>
- United Nations System Chief Executives Board for Coordination. (2024). United Nations system white paper on AI governance: An analysis of the UN system's institutional models, functions, and existing international normative frameworks applicable to AI governance. <https://unsceb.org/sites/default/files/2024-04/United%20Nations%20System%20White%20Paper%20on%20AI%20Governance.pdf>
- van Prooijen, J.-W., & Douglas, K. M. (2017). Conspiracy theories as part of history: The role of societal crisis situations. *Memory Studies*, 10(3), 323-333. <https://doi.org/10.1177/1750698017701615>
- Ward, C., & Voas, D. (2011). The emergence of conspiratorism. *Journal of Contemporary Religion*, 26(1), 103-121. <https://doi.org/10.1080/13537903.2011.539846>
- World Bank. (2025). Identification for Development (ID4D) global dataset. <https://id4d.worldbank.org/global-dataset>
- Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. PublicAffairs. <https://www.hachettebookgroup.com/titles/shoshana-zuboff/the-age-of-surveillance-capitalism/9781610395700/>