

Digital Sovereignty and Cross-Border Compliance in Internet Governance

Murdoch M. Watney

University of Johannesburg, South Africa

mwatney@uj.ac.za

Abstract: The internet was once imagined as a global, interoperable infrastructure, transcending borders, and fostering openness. John Perry Barlow and other early theorists envisioned a decentralised digital commons governed through shared technical standards rather than sovereign authority. By 2026, however, this vision has been profoundly challenged. Governments worldwide exert control over online spaces through surveillance mandates, data localisation laws, and content regulation, reshaping the contours of digital governance. This discussion examines the legal dimensions of digital sovereignty and its practical manifestation in cross-border compliance, focusing on how states assert authority over infrastructures and platforms. Case studies illustrate divergent approaches. Russia's ban on WhatsApp and Telegram calls reinforces sovereignty through communication restrictions. The United Kingdom's Online Safety Act prioritises user protection but raises freedom of expression concerns. The European Union's Digital Services Act harmonises accountability across member states while adding compliance burdens. In the United States, the extraterritorial reach of the CLOUD Act and Federal Trade Commission warnings against foreign pressures on encryption highlight tensions between national security and global interoperability. South Africa's July 2025 ruling compelling Facebook to disclose offender identities in a child protection case demonstrates how domestic law can override corporate resistance. Australia's ban on social media for children under sixteen further illustrates sovereignty extending into social policy. These examples reveal how sovereignty pressures accelerate fragmentation, eroding interoperability, weakening trust in multilateral institutions, and extending into societal domains such as safety, identity, and cultural values. Platform responses ranging from localisation to global adoption of strict standards mitigate risks but also entrench fragmentation. Viewed collectively, digital sovereignty is not merely a regulatory trend but a structural transformation of internet governance. Rather than converging toward consensus, the internet is increasingly defined by jurisdictional conflicts and sovereign claims. The central question is whether reconciliation through multilateral frameworks and technical standards remains possible, or whether fragmentation will persist as the defining condition of the digital order.

Keywords: Digital sovereignty, Internet governance, Platform accountability, Legal fragmentation, Cross-border compliance

1. Introduction

Digital sovereignty and cross-border compliance are reshaping the foundations of internet governance. What was once envisioned as a borderless digital commons is now increasingly fragmented by national laws, surveillance mandates, and regulatory frameworks. Early theorists such as John Perry Barlow envisioned cyberspace as a decentralised and open realm, free of government regulation and defined by its own community norms (Goldsmith and Wu, 2006). His *Declaration of the Independence of Cyberspace* captured the idea of the internet as a global commons governed through shared technical standards rather than sovereign authority.

The following examples illustrate how divergent legal frameworks challenge global platforms and complicate the vision of a unified internet:

- China's Cybersecurity Law which took effect in 2017, makes data localisation mandatory for any company wishing to operate within the country with the consequence that companies such as Apple, LinkedIn and Airbnb have complied placing millions of Chinese users' data within reach of the government (Tager, 2021).
- Russia restricted voice and video calls on communication platforms like WhatsApp and Telegram in August 2025, citing national security and fraud concerns (Abbasova, 2025).
- The United Kingdom (UK) Online Safety Act imposes duties on platforms to remove harmful content. It prioritises user protection but raises freedom of expression concerns and compliance burdens (Walsh, 2025).
- The European Union (EU) Digital Services Act, enforced from 2025, harmonizes accountability across member states, yet adds compliance burdens for global platforms (Wong, 2025).
- The United States (US) Clarifying Lawful Overseas Use of Data Act (US CLOUD Act) enacted in 2018 (Tager, 2021; Morton, 2025) and the 2025 Federal Trade Commission (FTC) warnings highlight tensions between national security imperatives and global interoperability (FTC, 2025).
- In South Africa, the Gauteng High Court compelled Meta in July 2025 to disclose offender identities in a landmark child pornography case, demonstrating how domestic law can override corporate resistance (Pongweni, 2025).

- In December 2025 Australia became the first country to impose a blanket ban on social media for children under 16, with fines of up to A\$50 million for non-compliance. This child-protection measure illustrates how sovereignty can reshape online participation and impose new compliance burdens on global platforms (Australia eSafety.gov.au, 2025; Dick, 2025).

Global technology companies must navigate overlapping and sometimes conflicting obligations. Compliance is no longer optional but it is enforced through fines, bans, and reputational risk. Platforms adopt a “comply where you operate” strategy, tailoring policies to each jurisdiction, but this creates fragmentation. Instead of a single set of global norms, companies face a patchwork of sovereignty claims (Allison, 2025).

The outcome is a fractured internet, where sovereignty increasingly overrides international norms. Jurisdictional conflicts undermine interoperability, weaken trust, and reshape digital governance. Rather than converging toward consensus, states are asserting authority over data flows, platform accountability, and online speech signalling a new era of digital geopolitics.

The discussion explores how national assertions of digital sovereignty and cross-border compliance obligations reshape the governance of the internet, and what implications this fragmentation hold for global technology platforms and international law.

2. Understanding Internet Governance and Digital Sovereignty

Internet governance refers to the structures, processes, and norms through which authority is exercised and compliance is enforced in digital environments (Kleinwächter, 2021).

Two dominant models frame this debate. The multilateral model emphasises the role of states acting collectively through international organisations and treaties. It reflects traditional diplomacy, where governments negotiate rules and standards across borders, often through institutions such as the United Nations or the International Telecommunication Union. Alongside this, the multi-stakeholder model has emerged as a distinctive approach to internet governance. Promoted by forums such as the Internet Governance Forum (IGF), it recognises that no single actor can control the internet and therefore includes governments, corporations, civil society, technical communities, and international organisations in decision-making processes. This model emphasises inclusivity, dialogue, and shared responsibility, aiming to balance diverse interests while maintaining global interoperability. The tension between these approaches has been evident since the World Summit on the Information Society (WSIS) in 2003 and 2005, where states such as China and Russia argued for stronger intergovernmental control, while Western governments and civil society defended multi-stakeholder inclusivity (WSIS, 2003).

These models illustrate that governance is not monolithic but contested. While multilateralism reflects state-to-state negotiation and multi-stakeholderism promotes inclusivity, both share the assumption that governance requires cooperation across borders.

Against this backdrop, cyber sovereignty challenges these cooperative models by re-centring authority within the nation-state (Tager, 2021). Digital sovereignty is best understood as a particular governance approach. Magee (2025) defines it as “the ability of a governing body, such as a national government, to control the tech stacks and data flows within its boundaries. For instance, in a digitally sovereign state, any data centres within its physical boundaries and locally hosted software are beholden only to the laws of that country.” Sovereignty narrows governance to territorial authority, contrasting with models that emphasise openness, interoperability, or shared responsibility across borders. Tager (2021) opines that since “governments define their national interests so differently, the way this sovereignty is invoked varies vastly.”

The practical consequence of sovereignty is the challenge of cross-border compliance. Since digital infrastructures and data flows routinely traverse national boundaries, global platforms must reconcile conflicting legal regimes. A company hosting data in Europe, operating servers in the United States, and serving users in Africa may simultaneously be subject to EU privacy rules, US disclosure laws, and African judicial orders. Compliance in one jurisdiction can create liability in another, forcing platforms to adopt layered strategies that balance local authority with global interoperability. Cross-border compliance thus becomes the hinge between sovereignty and governance. It is where abstract claims of authority translate into concrete obligations for technology companies, and where fragmentation begins to take shape.

By situating sovereignty within governance and highlighting cross-border compliance as its practical manifestation, this section establishes the conceptual foundation for examining how different jurisdictions assert authority in the digital sphere. The following analysis will explore the impact of the rise of digital sovereignty on cyber governance and the diverse approaches states have adopted to enforce their claims.

3. Impact of the Rise of Digital Sovereignty on Cyber Governance

The rise of digital sovereignty marks a fundamental turning point in the evolution of internet governance.

Once celebrated as a borderless commons, the internet is increasingly subject to the authority of nation-states, each asserting control over digital infrastructures, data flows, and online speech. Goldsmith and Wu (2006) warned that the illusion of a unified, global internet would give way to fragmented governance structures shaped by national interests. Today, those predictions are materialising with unprecedented force.

Governments justify sovereignty claims on multiple grounds. Security imperatives drive states to impose surveillance mandates and cybercrime legislation, framed as necessary to protect citizens from terrorism, fraud, or foreign interference. Economic imperatives are equally powerful, with data localisation laws and taxation regimes designed to capture value from global technology platforms, ensuring that digital wealth does not escape national borders. Cultural imperatives add another layer, as content regulation reflects domestic values, political priorities, and identity concerns. Together, these motivations illustrate why sovereignty has become the dominant lens through which states approach digital governance.

The Geneva Internet Platform's 2026 outlook underscores how this shift is clustering around three major hubs, namely the US, China and the EU. Each represents a distinct model of sovereignty. The US emphasises national security and extraterritorial reach, exemplified by the CLOUD Act. China pursues a comprehensive model of digital control, embedding sovereignty into its "Great Firewall" and data governance regime. The EU, meanwhile, seeks to harmonise accountability through supranational regulation, most notably the Digital Services Act. These hubs are not merely legal frameworks, but they are geopolitical poles around which global fragmentation accelerates.

In practice, sovereignty manifests through concrete regulatory actions. Surveillance laws compel companies to disclose data across borders, even when this conflicts with privacy norms elsewhere. Data localisation requirements force platforms to store information within national jurisdictions, undermining the free flow of data. Accountability frameworks such as the EU's Digital Services Act and the UK's Online Safety Act impose compliance burdens that reshape platform operations. Social policy interventions, such as Australia's 2025 ban on social media use for children under sixteen, extend sovereignty into the realm of digital participation itself. Each of these measures forces global companies to adopt a "comply where you operate" strategy, layering obligations across jurisdictions and eroding the coherence of global norms (Allison, 2025).

The result is a contested digital order in which sovereignty increasingly overrides international law and multilateral norms. Jurisdictional conflicts undermine interoperability, weaken trust, and complicate the operations of global platforms. The Geneva Internet Platform (2026) highlights that fragmentation is not only legal but also economic and emotional. Geoeconomics, manifested in trade and taxation fragmentation, places additional burdens on companies with global footprints. Geo-emotions, meanwhile, reveal a growing disconnect between public scepticism and industry optimism about artificial intelligence, a divergence that carries significant political implications.

Digital sovereignty, therefore, is not simply a matter of law, but it is a multidimensional phenomenon reshaping the internet's future across governance, economics, and society.

4. Platform Responses to Jurisdictional Demands

Global technology companies are no longer passive actors in the face of sovereignty claims. As states assert authority through legislation, regulation, and judicial rulings, platforms must adapt their strategies to survive in fragmented digital environments. Their responses reveal both the limits of compliance and the ways corporate adaptation itself shapes the trajectory of internet governance.

The investigations into Grok, the generative AI tool integrated into X, illustrate the complexity of platform responses. In January 2026, Ofcom in the United Kingdom launched a probe under the Online Safety Act after reports that Grok had been used to generate sexualised deepfake images, including child sexual abuse material (Hayes et al, 2026). Within days, California's Department of Justice opened its own investigation, citing non-consensual explicit imagery of women and children (Hayes et al, 2026). Meanwhile, the European Commission had already fined X €120 million in December 2025 under the Digital Services Act which is the first major fine imposed under the new regime for deceptive design practices and failures in transparency. These overlapping actions demonstrate how a single platform can be subject to simultaneous sovereignty claims across jurisdictions. For X and its AI subsidiary xAI, compliance meant cooperating with Ofcom's safety probe,

responding to California's enforcement demands, and absorbing the financial and reputational impact of the EU fine. The Grok case underscores how sovereignty pressures are not only legal but also political, reflecting divergent cultural attitudes toward safety, speech, and accountability.

Other platforms face similar dilemmas. Meta has repeatedly been compelled to comply with domestic rulings, most notably in South Africa in July 2025, when the Gauteng High Court ordered the company to disclose offender identities in a child protection case (Pongweni, 2025). Meta's response was to comply with the ruling while simultaneously lobbying for clearer international frameworks to avoid conflicting obligations. This dual strategy, namely compliance paired with advocacy illustrates how platforms attempt to mitigate fragmentation while protecting their global operations.

Microsoft has adopted a different approach, often choosing to implement the strictest standards globally. Following the European Union's General Data Protection Regulation (GDPR) and later the Digital Services Act, Microsoft extended compliance measures beyond Europe, applying them across markets. This strategy reduces the risk of conflicting obligations but increases operational costs. It also demonstrates how supranational regulation can exert influence far beyond its territorial scope, effectively exporting sovereignty through corporate adaptation.

TikTok provides another example of platform response under sovereignty pressure. Facing bans in India and restrictions in the US, TikTok has invested heavily in localisation strategies. These include establishing data centres within Europe such as Ireland, Norway, Finland, to comply with EU requirements and negotiating with regulators to maintain market access. It has also engaged third-party oversight to reassure regulators. Yet these efforts have not prevented ongoing scrutiny, illustrating the limits of corporate adaptation in the face of geopolitical tensions.

In August 2025, the US FTC cautioned American companies that complying with foreign demands to weaken encryption or censor content could violate section 5 of the FTC Act, which prohibits unfair and deceptive practices. This intervention forces US platforms to resist certain foreign sovereignty claims, prioritising domestic consumer protection over global harmonisation. It highlights how compliance strategies are not only reactive but also shaped by regulatory signals that pre-emptively constrain corporate adaptation.

Taken together, these examples reveal five primary strategies of platform response, namely

- Compliance with local rulings (Meta),
- Global adoption of strict standards (Microsoft),
- Localisation to appease regulators (TikTok),
- Management of overlapping jurisdictional enforcement (X/Grok), where platforms confront sovereignty claims that cannot easily be harmonised, and
- Pre-emptive resistance, illustrated by the 2025 warning from the US FTC that US companies must protect domestic customers against foreign laws and regulations that violate privacy and security.

These strategies demonstrate that platforms are not merely subjects of regulation but active participants in shaping the fragmented digital order. By exporting standards, lobbying for frameworks, or restructuring infrastructure, corporations themselves influence the trajectory of governance. Yet each strategy carries trade-offs, and none resolves the underlying tension between sovereignty and interoperability. Instead, corporate adaptation mitigates risks while reinforcing the reality that sovereignty claims are accelerating the disintegration of global internet governance.

5. Implications of State Sovereignty and Platform Adaptation for Global Internet Governance

The interplay between state sovereignty and platform adaptation has profound implications for the future of global internet governance. What emerges is not a coherent system but a fragmented digital order in which jurisdictional claims increasingly override multilateral norms. Platforms, by adopting compliance, localisation, or global standardisation strategies, inadvertently reinforce this fragmentation. Their responses mitigate immediate risks but also entrench the reality that sovereignty is shaping the internet's trajectory more decisively than cooperative governance models.

5.1 Erosion of Interoperability

As states impose divergent rules on data localisation, content moderation, and safety standards, the seamless flow of information across borders is disrupted. Platforms must build parallel infrastructures to satisfy conflicting

demands, undermining the technical and social coherence of the internet. TikTok's European data centres and Russia's domestic DNS root servers illustrate how sovereignty pressures force duplication of infrastructure. This fragmentation is not only legal but also economic, as compliance costs rise and market access becomes conditional on sovereign approval. Smaller firms, lacking resources to duplicate infrastructure, are disproportionately affected, reinforcing the dominance of large incumbents. Interoperability is also cultural. Users in different jurisdictions experience different versions of the internet, shaped by divergent moderation rules and safety standards.

5.2 Weakening of Trust in Governance Institution

Multilateral and multi-stakeholder forums, once central to internet governance, are increasingly side-lined as states assert unilateral authority. The Geneva Internet Platform's 2026 outlook warns that sovereignty claims are clustering around geopolitical hubs such as the US, China, and the EU, leaving smaller states to navigate a patchwork of rules without meaningful influence. Institutions like the Internet Governance Forum (IGF) and ICANN, designed to foster inclusivity and shared responsibility, struggle to remain relevant when powerful states impose rules extraterritorially. Hybrid initiatives such as the Global Forum on Cyber Expertise (GFCE) provide pragmatic coordination, but they lack binding authority. This imbalance risks deepening inequalities in digital participation, creating a tiered internet where some states set norms while others merely absorb them.

5.3 Societal Consequences

Sovereignty pressures also carry significant societal consequences. Measures such as Australia's ban on social media for children under sixteen, India's prohibition of TikTok (Chow, 2025), or Ofcom's probe into Grok's deepfake imagery illustrate how sovereignty extends into questions of identity, safety, and cultural values (Hayes et al., 2026). These interventions reshape not only platform operations but also the lived experience of digital citizenship. Sovereignty claims increasingly intersect with AI governance, as seen in the EU's AI Act, which imposes binding obligations on developers, contrasted with the US reliance on voluntary frameworks (Ashkara 2025). The divergence between public scepticism and industry optimism about artificial intelligence, highlighted in the Geneva Internet Platform's 2026 report, underscores how governance is entangled with social trust and political legitimacy. Sovereignty also reshapes freedom of expression, as regulatory traditions diverge between jurisdictions for example, the UK's Online Safety Act prioritises user protection, while US law emphasises First Amendment rights.

5.4 Geopolitical Consequences

Separate from societal impacts, sovereignty claims are producing geopolitical consequences. Analysts warn of the emergence of the "splinternet" (also referred to as the balkanised internet or the Westphalian web), where the internet fragments into competing blocs aligned with democratic or authoritarian regimes (Tager, 2021). The risk of fragmentation is triggered not only by governments undermining interoperability through national internet networks, but also by efforts to enforce one state's digital regulations extraterritorially or to block information flows across borders.

The rivalry between the US and China over technology standards, combined with the EU's regulatory assertiveness, risks dividing the internet into spheres of influence. The US has sought to limit Chinese influence through sanctions on companies such as Huawei, while China has entrenched its "Great Firewall" and promoted its own standards for 5G and AI. The EU, meanwhile, has leveraged instruments such as the Digital Services Act and Digital Markets Act to extend its regulatory reach globally, effectively exporting European sovereignty through corporate compliance. Russia's "sovereign internet" law and its efforts to build domestic DNS root servers further illustrate how states embed sovereignty into technical infrastructure.

This fragmentation is reinforced by trade disputes, sanctions, and geopolitical competition, embedding digital governance within broader struggles for global power. Regional coalitions such as the African Union's Digital Transformation Strategy or ASEAN's digital frameworks illustrate how smaller states seek collective leverage, but many remain caught between dominant hubs, forced to align or risk exclusion from global digital markets. The 2026 World Economic Forum echoed these concerns, warning that sovereignty claims are clustering around major hubs and that geopolitical fragmentation risks undermining trust in global governance institutions (World Economic Forum, 2026).

5.5 AI Governance Consequences

Sovereignty claims increasingly intersect with artificial intelligence, producing consequences that mirror broader internet governance fragmentation. The European Union's AI Act represents the most ambitious attempt to

regulate AI globally, imposing binding obligations on developers through a risk-based framework (Ashkara 2025). High-risk systems must meet strict requirements for transparency, human oversight, and conformity assessments, while prohibited practices such as social scoring are banned outright. By contrast, the US has relied on voluntary frameworks, such as the NIST AI Risk Management Framework and executive orders, leaving compliance largely to industry discretion. China has adopted a state-driven model, embedding AI governance within its broader cyber sovereignty agenda, including mandatory security reviews and restrictions on generative AI content.

The consequence of this divergence is a fragmented regulatory landscape in which developers and platforms face uneven obligations depending on jurisdiction. Compliance asymmetry raises costs in Europe, creates flexibility but weaker protections in the US, and subjects firms in China to direct state control. This unevenness affects innovation and competitiveness: companies in stricter jurisdictions may struggle with compliance burdens, while those in looser regimes exploit regulatory gaps.

AI governance also shapes public trust. Citizens in the EU experience higher levels of legal protection, while US users rely on corporate self-regulation, and Chinese citizens encounter state-directed oversight. These differences reinforce divergent perceptions of AI safety, legitimacy, and accountability. As AI systems become embedded in critical infrastructure, healthcare, and education, the absence of global standards risks undermining interoperability and reinforcing the splintering of digital governance. The 2026 World Economic Forum highlighted this divergence, noting that AI regulation has become a proxy for sovereignty claims and that competing regimes risk fragmenting the future of intelligent systems (World Economic Forum, 2026).

Viewed collectively, sovereignty claims in AI governance demonstrate how emerging technologies are becoming arenas for jurisdictional competition. Just as data localisation and content regulation fractured the internet, divergent AI regimes threaten to fragment the future of intelligent systems, embedding sovereignty into the very architecture of technological innovation.

6. Reconciling Sovereignty and Global Governance

The accelerating rise of digital sovereignty raises a critical question, namely whether the fragmented jurisdictional demands can be reconciled with the vision of a global, interoperable internet? While the trajectory of governance suggests deepening disintegration, several pathways remain open for balancing sovereignty with cooperation.

6.1 Multilateral Frameworks

One possibility lies in multilateral frameworks. Initiatives within the United Nations, the International Telecommunication Union, and the OECD continue to explore mechanisms for harmonising digital rules (Nye, 2021). Yet their influence is limited by the reluctance of powerful states to cede authority. Without binding commitments, multilateralism risks becoming symbolic rather than substantive, producing declarations rather than enforceable norms.

6.2 Technical Standardisation

A second pathway is technical standardisation. Organisations such as the Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C) maintain protocols that underpin interoperability regardless of political borders. By embedding compliance into technical design, these standards can mitigate fragmentation even when legal regimes diverge. However, sovereignty claims increasingly challenge the universality of standards, as states demand localisation or proprietary systems for example, China's promotion of alternative 5G standards and Russia's push for domestic DNS root servers (Tager, 2021).

6.3 Corporate Adaptation

A third avenue is corporate adaptation. As seen with Microsoft's global application of EU rules, platforms can voluntarily adopt the strictest standards across markets, effectively exporting regulatory norms. This strategy reduces conflict but places disproportionate power in the hands of corporations, raising questions about accountability and legitimacy. Moreover, not all companies can absorb the costs of global compliance, leaving smaller actors vulnerable and reinforcing inequalities in digital governance.

6.4 Regional Coalitions

A fourth pathway is regional coalitions. The EU's Digital Services Act demonstrates how supranational regulation can project sovereignty collectively, balancing national interests with shared accountability. Similar coalitions in

Africa, Asia, or Latin America could provide smaller states with greater leverage in shaping digital governance, countering the dominance of US and Chinese models. The African Union's Digital Transformation Strategy (2020–2030) and ASEAN's digital integration initiatives illustrate early moves toward regional frameworks.

6.5 Hybrid Governance Models

Finally, emerging hybrid governance models may offer pragmatic compromises. Overlapping institutions such as technical bodies, trade agreements, corporate codes of conduct, and national laws may collectively shape outcomes. Public-private partnerships, such as the Global Forum on Cyber Expertise (GFCE), illustrates how states and corporations can collaborate without formal treaties. Established in 2015, GFCE now includes more than 250 partners and operates regional hubs in Africa, Asia, and Latin America. Its 2025–2027 Implementation Plan focuses on cyber capacity building, national strategy development, and incident response coordination. While GFCE cannot enforce compliance, it has practical impact by matching countries with donors, reducing duplication of projects, and strengthening resilience in the Global South. This illustrates how hybrid arrangements, though fragmented, can provide flexible mechanisms for reconciling sovereignty with interoperability.

In sum, these pathways suggest that reconciliation is possible but fraught. Sovereignty will remain a defining feature of digital governance, yet its impact can be moderated through multilateral dialogue, technical standards, corporate adaptation, regional coalitions, and hybrid governance models. The future of the internet will depend on whether these mechanisms can sustain interoperability without eroding the legitimacy of national authority. If they fail, fragmentation may become the permanent condition of the digital order.

7. Conclusion in Respect of Digital Sovereignty and the Future of Internet Governance

Digital sovereignty has moved from a marginal concept to a defining force in the evolution of internet governance. What began as a contest between multilateral and multi-stakeholder models has now been reshaped by the assertive authority of nation-states. Case studies from Russia, the UK, the EU, the US, China, South Africa, and Australia illustrate the diverse ways sovereignty manifests in practice through technological restrictions, protective duties, supranational regulation, extraterritorial reach, judicial enforcement, and social policy interventions.

Platform responses reveal the limits of adaptation. Whether through compliance with local rulings, global adoption of strict standards, localisation strategies, or navigating simultaneous multi-jurisdictional enforcement, companies are compelled to operate within a fragmented digital order. Their strategies mitigate risks but also reinforce the reality that sovereignty is accelerating disintegration.

The implications are profound. Interoperability is eroding, trust in global governance institutions is weakening, and societal consequences are multiplying as sovereignty extends into questions of safety, identity, and participation. While pathways for reconciliation exist by means of multilateral frameworks, technical standards, corporate adaptation, and regional coalitions, they remain fragile and contested.

Ultimately, digital sovereignty is not simply a legal doctrine but a multidimensional phenomenon reshaping governance, economics, and society. It signals a future in which the internet is less a borderless commons and more a contested domain of overlapping jurisdictions. Barlow's early vision of an open, decentralised, and interoperable infrastructure now stands in stark contrast to this reality. Whether fragmentation can be moderated or will become permanent remains the central challenge for policymakers, platforms, and citizens alike. The future of the internet will be defined not only by sovereignty claims but by the capacity of platforms and institutions to manage cross-border compliance. It is here, in the reconciliation of overlapping obligations, that the contest between fragmentation and cooperation will be decided.

Ethics Declaration. I did not need ethical clearance.

AI Declaration: I acknowledge the use of Microsoft Co-pilot as an assistive grammar tool during my research. The final work reflects my own analysis, argumentation, and interpretation of the subject matter.

References

- Abbasova, V. (2025) "WhatsApp Faces Growing Restrictions in Russia", [online], https://caspiannews.com/news-detail/whatsapp-faces-growing-restrictions-in-russia-2025-12-25-0/?utm_source=copilot.com.
- Allison, A. (2025) "Role of International law in combatting cross-border cybercrime: addressing jurisdictional and enforcement challenges", [online], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5806362.

- Antoniuk, D. (2025) "Russia curbs WhatsApp, Telegram calls to counter cybercrime", [online], https://therecord.media/russia-restricts-voice-calls-whatsapp-telegram-cybercrime?utm_source=copilot.com.
- Ashkara Z. (2025) "The EU AI Act in 2025: a detailed overview of recent developments", [online], https://www.aiactblog.nl/en/posts/ai-act-ontwikkelingen-2025?utm_source=copilot.com.
- Australia esafety.gov.au. (2025) "Stay social off socials" [online], https://www.esafety.gov.au/sites/default/files/2025-11/SMMA_Factsheet_Digital.pdf?utm_source=copilot.com.
- Chow, A. (2025) "Here is what happened when India banned TikTok in 2020", [online], <https://time.com/7208112/what-happened-when-india-banned-tiktok/>.
- Dick, S. (2025) "Australia's social media ban for under-16s starts today. Here is what you should know", [online], https://www.abc.net.au/news/2025-12-10/australias-social-media-ban-for-under-16s-starts-today/106119800?utm_source=copilot.com.
- EU Digital Service Act. (2025) [online], <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act>.
- Geneva Internet Platform. (2026) "Weekly #244 looking ahead: Our annual AI and digital forecast", [online], <https://dig.watch/newsletters/dw-weekly/dw-weekly-244>.
- Global Forum on Cyber Expertise (GFCE). (2026) "GFCE is the platform for international cooperation on strengthening cyber capacity and expertise globally", [online], https://thegfce.org/?utm_source=copilot.com.
- Goldsmith, J. and Wu, T. (2006) *Who controls the internet* Oxford University Press, US, p vii, 17 – 27, 58, 81, 84, 183 – 184.
- Hayes, C., Chia, O. and Mahon, L. (2026) "X to stop Grok AI from undressing images of real people after backlash", [online], <https://www.bbc.com/news/articles/ce8gz8g2qnlo>.
- Kleinwächter, W. (2021) "Cybersecurity, Internet governance and the multistakeholder approach", [online], <https://hcss.nl/wp-content/uploads/2021/12/Kleinwaechter.pdf>.
- Magee, T. (2025) "What is digital sovereignty – and why should your business care?" [online], <https://www.raconteur.net/technology/what-is-digital-sovereignty>.
- Morton, P. (2025) "Understanding the implications and risks of the US Cloud Act", [online], <https://www.claromentis.com/blog/understanding-the-implications-and-risks-of-the-us-cloud-act>.
- Pongweni, T. (2025) "Meta held accountable by SA court in fight against online child sexual abuse", [online], <https://www.dailymaverick.co.za/article/2025-07-24-meta-held-accountable-by-sa-court-in-fight-against-online-child-sexual-abuse/>.
- Sabou, M. (2025) "Regulation on Network Data Security Management", [online] <https://appinchina.co/government-documents/regulation-on-network-data-security-management/>.
- Tager, J. (2021) "Introduction: The new guard post of cyberspace" [online], <https://pen.org/report/splintered-speech-digital-sovereignty-and-the-future-of-the-internet/>.
- UK Ofcom. (2026) "Ofcom launches investigation into X over Grok sexualised imagery", [online], https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/ofcom-launches-investigation-into-x-over-grok-sexualised-imagery?utm_source=DiploMail&utm_campaign=a29768a7ac-EMAIL_CAMPAIGN_2026_01_16_01_58&utm_medium=email&utm_term=0_4510155485-a29768a7ac-120762130.
- UK Online Safety Act: Explainer. (2025), [online], <https://www.gov.uk/government/publications/online-safety-act-explainer/online-safety-act-explainer>.
- UK Press release. (2026) "Government to drive action to improve children's relationship with mobile phones and social media", [online], https://www.gov.uk/government/news/government-to-drive-action-to-improve-childrens-relationship-with-mobile-phones-and-social-media?utm_source=copilot.com.
- US FTC. (2025) "FTC Chairman Ferguson warns companies against censoring or weakening the data security of America at the behest of foreign powers", [online], https://www.ftc.gov/news-events/news/press-releases/2025/08/ftc-chairman-ferguson-warns-companies-against-censoring-or-weakening-data-security-americans-behest?utm_source=copilot.com.
- Walsh, M. (2025) "A guide to the OSA and its implementation: two year anniversary edition", [online], <https://www.onlinesafetyact.net/analysis/a-guide-to-the-osa-and-its-implementation/>.
- Wong, J. (2025) "EU fines Elon Musk's X £120 million over blue check practices in first major digital Service Act Enforcement", [online], https://www.btimesonline.com/articles/176417/20251230/eu-fines-elon-musk-s-x-€120-million-over-blue-check-practices-in-first-major-digital-services-act-enforcement.htm?utm_source=copilot.com.
- World Economic Forum. (2026). *Global Cooperation in the Age of Digital Sovereignty*. Davos Agenda 2026 Report. [online], <http://www.weforum.org>.
- World Summit on the Information Society. "Declaration of Principles" (2003) [online], https://www.itu.int/net/wsis/docs/geneva/official/dop.html?utm_source=copilot.com.