
DIGITAL SOVEREIGNTY AND E-GOVERNANCE: REDEFINING STATE CONSENT IN CONTEMPORARY INTERNATIONAL LAW

Vijayenthira Poopathy DG, LL.M., University of Madras

ABSTRACT

The international legal order has traditionally been organised around the territorially bounded, consenting sovereign State, with State consent serving as the foundational source of binding obligation under treaty law, customary international law, and unilateral acts.¹ The emergence of cyberspace as a domain of governance, commerce, and conflict has unsettled this consensual architecture.² States now assert sovereign claims over data, digital infrastructure, and algorithmic systems through the contested concept of "digital sovereignty," while e-governance mechanisms transform how States exercise authority over their populations and interact across borders.

This doctrinal study examines whether, and to what extent, digital sovereignty is reshaping the doctrine of State consent in contemporary international law. Employing the doctrinal method, it analyses primary sources including the UN Charter, the Vienna Convention on the Law of Treaties, the Budapest Convention on Cybercrime, the General Data Protection Regulation, the Tallinn Manual, and relevant judicial decisions - alongside comparative State practice across the European Union, the United States, China, and India.

The study advances the hypothesis that digital sovereignty does not abolish State consent but compels its doctrinal reconfiguration, identifying three emergent modalities: structural consent, inferred from participation in technical governance systems beyond direct State control; conditional consent, extracted through asymmetric market and infrastructural dependency, as with GDPR adequacy mechanisms;³ and residual consent, whereby States retain only a diminished capacity to withdraw from, rather than shape, governance arrangements set by dominant States or corporations.

¹ Vienna Convention on the Law of Treaties, opened for signature 23 May 1969, 1155 UNTS 331 (entered into force 27 January 1980); Statute of the International Court of Justice art 38(1); *Nuclear Tests (Australia v France)* [1974] ICJ Rep 253.

² United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, UN Doc A/70/174 (22 July 2015).

³ Regulation (EU) 2016/679 (GDPR), arts 45–47.

The study concludes that no uniform customary norm of digital sovereignty has yet crystallised, and proposes a layered normative framework -a foundational instrument, sectoral protocols, and a consent-verification mechanism- to restore substantive consent to digital governance, recommending reform of extraterritorial regulation, mutual legal assistance, and AI governance.

Keywords: Digital Sovereignty, State Consent, E-Governance, Cyberspace, International Law, Data Protection, Extraterritorial Jurisdiction.

CHAPTER 1: INTRODUCTION

1.1 Background of the Study

The international legal order has, since the Peace of Westphalia, organised itself around the territorially bounded, consenting sovereign State⁴. Law-making, jurisdiction, and responsibility were all anchored in the physical fact of territory and the political fact of consent. The emergence of cyberspace as a domain of governance, commerce, and conflict has unsettled this anchorage. Data flows across borders at a velocity and volume that defies territorial logic; governmental functions are increasingly performed through digital platforms hosted on infrastructure located in, or controlled by, other States or private corporations; and decisions affecting citizens are made by algorithms whose operative logic may not be transparent even to the State that deploys them.

Against this backdrop, the notion of "digital sovereignty" has emerged as a contested but increasingly invoked concept in State practice, regional legislation (most prominently the European Union's data protection and digital market regulations)⁵, and scholarly discourse. States now assert sovereign claims not merely over territory and population but over data, networks, algorithms, and the digital infrastructure through which governance is delivered. This study interrogates whether, and to what extent, this assertion of digital sovereignty is reshaping the doctrine of State consent — long regarded as the cornerstone of international legal obligation.

⁴ Treaty of Peace of Münster, 24 October 1648, CTS 1; Charter of the United Nations, 26 June 1945, 1 UNTS XVI, arts 2(1) and 2(7).

⁵ European Commission, *2030 Digital Compass: The European Way for the Digital Decade*, COM(2021) 118 final.

1.2 Meaning and Scope of E-Governance

E-Governance, in its broadest doctrinal sense, refers to the use of information and communication technologies (ICTs) by State organs ⁶to deliver public services, disseminate information, facilitate citizen participation, and conduct inter-State and intra-State administrative functions. It encompasses Government-to-Citizen (G2C), Government-to-Business (G2B), Government-to-Government (G2G), and Government-to-Employee (G2E) interactions. For the purposes of this study, e-governance is examined not as a matter of public administration alone, but as a juridical phenomenon that implicates jurisdiction, data control, cross-border cooperation, and ultimately the consensual basis of international obligations assumed or resisted by States in the digital sphere.

1.3 Concept of Digital Sovereignty

Digital sovereignty may be provisionally defined as the assertion by a State of effective authority and control over data, digital infrastructure, algorithmic systems, and network governance ⁷within, and increasingly beyond, its territorial boundaries. It manifests in three principal dimensions: (a) **data sovereignty** — control over the storage, processing, and transfer of data; (b) **technological sovereignty** — control over the hardware, software, and infrastructural stack underpinning digital governance; and (c) **regulatory/jurisdictional sovereignty** — the capacity to extend legal authority extraterritorially over digital conduct. This tripartite framework is employed throughout the study as an analytical heuristic.

1.4 Research Problem

Classical international law treats State consent as the foundational source of binding obligation ⁸— whether through treaty, custom evidenced by State practice and *opinio juris*, or unilateral acts. The digital environment, however, generates obligations and constraints through mechanisms that do not fit comfortably within this consensual architecture: extraterritorial regulatory regimes (such as the GDPR) bind foreign States and entities without their consent; cyber operations occur in a normative grey zone where consent-based doctrines such as non-

⁶ United Nations Department of Economic and Social Affairs, *United Nations E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development* (2024).

⁷ European Commission, *Shaping Europe's Digital Future* (2020); Cybersecurity Law of the People's Republic of China (2017).

⁸ Statute of the International Court of Justice, art 38(1); Vienna Convention on the Law of Treaties, opened for signature 23 May 1969, 1155 UNTS 331 (entered into force 27 January 1980).

intervention are difficult to apply; and private technology corporations exercise quasi-governmental authority without being subjects of international law at all. The research problem, therefore, is to determine whether the traditional doctrine of State consent remains adequate to regulate digital sovereignty and e-governance, or whether a doctrinal reconceptualization is warranted.

1.5 Research Questions

1. How has the doctrine of State consent historically developed within international law, and what are its conceptual limits?
2. What is the legal content of "digital sovereignty," and how does it interact with established sovereignty doctrine?
3. To what extent do existing international instruments (UN frameworks, the Budapest Convention, the GDPR, the Tallinn Manual) address, displace, or reinforce consent-based obligations in the digital sphere?
4. Does extraterritorial digital regulation constitute a permissible exercise of sovereign jurisdiction or an erosion of the consent principle vis-à-vis third States?
5. Is there an emerging customary norm of digital sovereignty, and if so, what is its relationship to State consent?
6. What normative framework, if any, ought to be developed to reconcile digital sovereignty claims with the consensual foundations of international law?

1.6 Objectives of the Study

(a) To trace the doctrinal evolution of sovereignty and State consent in international law; (b) To examine the legal foundations and dimensions of digital sovereignty; (c) To analyse the international legal frameworks governing e-governance; (d) To assess how digital sovereignty is transforming the operation of State consent; (e) To critically evaluate existing instruments and comparative State practice; and (f) To propose doctrinal and normative recommendations for reform.

1.7 Hypothesis

This study proceeds on the hypothesis that **digital sovereignty does not abolish the doctrine of State consent but compels its doctrinal reconfiguration** — from a binary, territorially-anchored notion of assent or dissent, into a layered, functionally differentiated concept operating across data, infrastructure, and jurisdictional dimensions, often expressed through implied, structural, or institutional forms of consent rather than explicit treaty-based assent.

1.8 Research Methodology (Doctrinal Method)

This study adopts a **doctrinal legal research methodology**, relying on the analysis of primary legal sources (treaties, conventions, United Nations resolutions, judicial and arbitral decisions, and State declarations) and secondary sources (juristic writings, institutional reports, and academic commentary). The doctrinal method is employed to:

(a) identify and systematise the relevant rules and principles of international law bearing upon digital sovereignty and State consent; (b) analyse the internal coherence and adequacy of these rules through textual and contextual interpretation in accordance with Articles 31–32 of the Vienna Convention on the Law of Treaties, 1969;⁹ (c) compare instruments and State practice to discern patterns indicative of customary international law under Article 38(1)(b) of the Statute of the International Court of Justice; and (d) construct, through analytical and normative reasoning, a doctrinal framework addressing identified gaps.

The study is qualitative, library-based, and non-empirical; it does not employ field surveys, interviews, or quantitative analysis, consistent with the doctrinal tradition in international legal scholarship.

1.9 Review of Literature

A substantial body of scholarship addresses sovereignty in cyberspace, though doctrinal treatment of its specific intersection with State consent remains comparatively underdeveloped.

Classical sovereignty scholarship — exemplified in the works on the Westphalian order and the United Nations Charter framework — establishes the territorial and consensual foundations

⁹ Vienna Convention on the Law of Treaties, 1969, arts 31–32

against which digital developments must be assessed. Cyber-law scholarship, including the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, has extended traditional doctrines of sovereignty, non-intervention, and State responsibility into the cyber domain, though with persistent disagreement among experts as to whether sovereignty itself constitutes a binding primary rule or merely a structural principle.

Scholarship on data sovereignty and data localization (addressing instruments such as the European Union's General Data Protection Regulation and national data protection statutes) has examined the tension between extraterritorial regulatory assertions and the traditional jurisdictional bases recognised in the *Lotus* case and subsequent practice. Literature on global internet governance has explored the multi-stakeholder model administered through bodies such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Governance Forum, highlighting the diminished centrality of State consent where private and technical actors play a governing role.

Comparative literature on national approaches — the European Union's strategic autonomy discourse, the United States' open-internet and Cloud Act-based approach, China's cyber-sovereignty doctrine, and India's data protection and digital governance framework — reveals divergent normative starting points that complicate the search for a unified customary rule.

The existing literature, while rich in sectoral analysis, has not adequately synthesised the cumulative effect of these developments upon the doctrine of consent itself. This study seeks to fill that gap by treating consent, rather than sovereignty alone, as the central doctrinal lens.

1.10 Scope and Limitations

The study is confined to public international law doctrine; it does not undertake an empirical or technical assessment of cybersecurity architecture, nor does it examine private international law conflict-of-laws rules in detail except where relevant to jurisdictional sovereignty. The analysis is limited to State practice and instruments reasonably accessible as of the date of writing and does not purport to be exhaustive of all national digital sovereignty legislation. The study does not address criminal procedural cooperation in depth beyond its relevance to the consent doctrine.

1.11 Chapter Scheme

Chapter 2 traces the evolution of sovereignty and consent. Chapter 3 examines the legal foundations of digital sovereignty. Chapter 4 analyses e-governance within international legal frameworks. Chapter 5 constitutes the doctrinal core, examining the transformation of consent. Chapter 6 undertakes comparative analysis of instruments and State practice. Chapter 7 proposes a normative framework. Chapter 8 concludes with findings and suggestions for reform.

CHAPTER 2: THE EVOLUTION OF SOVEREIGNTY AND STATE CONSENT IN INTERNATIONAL LAW

2.1 Origins of Sovereignty in Classical International Law

The doctrine of sovereignty finds its early theoretical articulation in the writings of Jean Bodin and later Thomas Hobbes¹⁰, who conceived of sovereignty as supreme, indivisible authority within a political community. Hugo Grotius and subsequent natural law jurists transposed this internal conception of supreme authority onto the relations between political communities themselves, laying the groundwork for a society of formally equal, independent sovereigns whose mutual relations were to be governed by a law derived substantially from their own consent and practice.

2.2 The Westphalian Framework

The Peace of Westphalia (1648) is conventionally treated as the symbolic origin of the modern State system,¹¹ establishing the principles of territorial integrity and non-interference among formally equal sovereigns. The "Westphalian" model rests on three interlocking premises: (a) the State as the primary, territorially defined unit of international order; (b) the formal equality of States irrespective of material power; and (c) the consequent dependence of international obligation upon the consent of the obligated State. These premises have proved remarkably durable, even as their empirical accuracy and historical pedigree have been questioned by revisionist historians.

¹⁰ Six Books of the Commonwealth; Leviathan.

¹¹ Treaty of Peace of Münster, 24 October 1648, CTS 1; Treaty of Osnabrück, 24 October 1648, CTS 119.

2.3 Development of State Consent as a Principle of International Law

Consent operates as the structural premise of the principal sources of international law identified in Article 38(1) of the Statute of the International Court of Justice¹². Treaty law rests on the maxim *pacta sunt servanda*, codified in Article 26 of the Vienna Convention on the Law of Treaties, 1969¹³, and treaties bind only parties that have consented to be bound, in accordance with the *pacta tertiis* principle reflected in Article 34 of that Convention. Customary international law, though not consensual in the same explicit sense, nonetheless depends upon a general pattern of State practice accepted as law (*opinio juris*), permitting persistent objection by dissenting States. The Permanent Court of International Justice's reasoning in the *Lotus* case is frequently cited for the proposition that restrictions upon the independence of States cannot be presumed and must be traceable, ultimately, to a rule to which States have consented or acquiesced.

2.4 Sovereignty under the Charter of the United Nations

The Charter of the United Nations entrenches sovereign equality as a foundational principle in Article 2(1), and the prohibition on intervention in matters within the domestic jurisdiction of States in Article 2(7).¹⁴ The Friendly Relations Declaration (UN General Assembly Resolution 2625 (XXV), 1970) elaborates the principles of sovereign equality, non-intervention, and the duty not to use force, reaffirming consent as central to the legitimacy of any derogation from a State's domestic authority.

2.5 Contemporary Challenges to Traditional Sovereignty

Globalization, the proliferation of international organizations possessing autonomous law-making or quasi-legislative capacities, the rise of *jus cogens* norms binding irrespective of consent, and the growth of human rights obligations owed *erga omnes* have each, in differing degrees, qualified the strict consensual model. The digital revolution constitutes a further, and in some respects more radical, challenge, because it implicates not merely the scope of sovereign authority but its very object — data, code, and algorithmic processes that are not

¹² Statute of the International Court of Justice, art 38(1).

¹³ Vienna Convention on the Law of Treaties, 1969, arts 26 and 34.

¹⁴ Charter of the United Nations, arts 2(1) and 2(7); Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, GA Res 2625 (XXV) (24 October 1970).

bound by territorial logic at all.

2.6 Theoretical Perspectives on Sovereignty

Three broad theoretical positions inform the present analysis. The **statist/positivist** position regards sovereignty as the unqualified, if increasingly regulated, supreme authority of States, with international law binding only through State consent. The **institutionalist** position regards sovereignty as constituted and qualified by membership in an international institutional order, such that obligations may bind States by virtue of systemic participation rather than discrete consent. The **constitutionalist/cosmopolitan** position treats sovereignty as subordinate to an emerging global legal order organised around human rights and global public goods, of which the digital commons may increasingly be considered one. This study adopts a moderate institutionalist position, treating consent as a still-necessary but increasingly indirect and structurally mediated basis of obligation.

CHAPTER 3: LEGAL FOUNDATIONS OF DIGITAL SOVEREIGNTY

3.1 Emergence of Digital Sovereignty

The term "digital sovereignty" entered policy and legal discourse principally through European Union institutional documents and French and German governmental statements emphasising "strategic autonomy" in digital infrastructure, alongside Chinese assertions of "cyber sovereignty" (*wangluo zhuquan*) articulated in China's 2010 White Paper on the Internet and subsequently embedded in its Cybersecurity Law.¹⁵ Russian and other States' positions before United Nations cyber working groups have similarly asserted sovereign control over national information space. The convergence and divergence of these articulations reveal that digital sovereignty, unlike classical territorial sovereignty, lacks a single agreed doctrinal content; it is asserted polycentrically by States with markedly different political objectives, ranging from data protection and economic competitiveness to information control.

3.2 Sovereignty in Cyberspace

The applicability of the general international law principle of sovereignty to cyberspace was long contested, with debate crystallising around the divergent positions taken by the

¹⁵ Information Office of the State Council of the People's Republic of China, *The Internet in China* (2010); Cybersecurity Law of the People's Republic of China (2017).

International Group of Experts in the Tallinn Manual process: a majority view treating sovereignty as a primary rule capable of independent violation by cyber operations affecting a State's territorial integrity or inherently governmental functions, against a minority view treating sovereignty merely as a structural principle underlying other rules such as non-intervention. The United Nations Group of Governmental Experts (UNGGE) reports of 2013, 2015, and 2021, together with the Open-Ended Working Group (OEWG) process, have affirmed by consensus that international law, including the principle of State sovereignty, applies to State conduct in cyberspace, though without resolving the precise operative content of that affirmation.¹⁶

3.3 Data Sovereignty and Data Localization

Data sovereignty refers to the claim that data generated within, or pertaining to the nationals of, a State remains subject to that State's legal authority irrespective of the physical location of storage or processing. Data localization measures — requiring that data be stored or processed on servers physically located within national territory — represent the principal regulatory technique through which data sovereignty is operationalised¹⁷. Such measures raise tension with the free flow of data underlying global digital trade and with obligations assumed under trade instruments, while simultaneously reasserting territorial control as the basis of jurisdiction over an inherently non-territorial resource.

3.4 Jurisdiction in Cyberspace

Jurisdiction in the digital domain is asserted on overlapping bases — territoriality (where infrastructure, servers, or conduct occur within a State's territory), nationality (regulation of the State's own nationals or registered entities), the protective principle (regulation of conduct causing harm to a State's vital interests), and increasingly an "effects" or "targeting" basis under which a State regulates conduct occurring abroad because its effects, or the entity's deliberate targeting, fall within the regulating State.¹⁸ This last basis, prominently employed in data protection legislation, extends regulatory reach extraterritorially in ways reminiscent of, but doctrinally more expansive than, the effects doctrine developed in competition law

¹⁶ United Nations Group of Governmental Experts, UN Doc A/68/98 (2013); UN Doc A/70/174 (2015); Open-Ended Working Group on ICT Security, Final Report, UN Doc A/75/816 (2021).

¹⁷ Regulation (EU) 2016/679 (General Data Protection Regulation); Digital Personal Data Protection Act, 2023 (India); Cybersecurity Law of the People's Republic of China (2017).

¹⁸ Regulation (EU) 2016/679 (General Data Protection Regulation), art 3

jurisprudence.

3.5 Digital Sovereignty and the Principle of Non-Intervention

The principle of non-intervention, requiring that States refrain from coercive interference in matters within another State's *domaine réservé*, has been invoked in relation to cyber operations directed at electoral processes, critical infrastructure, and governmental data systems. The International Court of Justice's articulation of non-intervention in the *Nicaragua* case ¹⁹— requiring both an element of coercion and interference with matters falling within the target State's domestic jurisdiction — provides the doctrinal template applied, with adaptation, to digital and informational coercion.

3.6 State Responsibility in the Digital Environment

The customary rules of State responsibility, codified in the International Law Commission's Articles on Responsibility of States for Internationally Wrongful Acts (2001), apply to cyber and digital conduct, subject to the acute difficulty of attribution given the use of proxy actors, anonymization technologies, and transnational infrastructure. The attribution rules under Articles 4 to 11 of the ILC Articles — covering organs of the State, persons exercising governmental authority, and conduct directed or controlled by a State — are tested by the digital environment's capacity to obscure the causal chain between State direction and harmful cyber conduct.

CHAPTER 4: E-GOVERNANCE AND INTERNATIONAL LEGAL FRAMEWORKS

4.1 Concept and Evolution of E-Governance

E-governance has evolved from rudimentary electronic record-keeping to integrated digital service delivery, encompassing digital identity systems, e-procurement, digital taxation, online judicial processes, and increasingly algorithmic and artificial-intelligence-assisted administrative decision-making. Its evolution tracks broader trends in public administration theory, from New Public Management's efficiency orientation to contemporary emphases on

¹⁹ Military and Paramilitary Activities in and against Nicaragua, ICJ Reports 1986, pp 106–109, paras 202–205; International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts* (2001), arts 4–11.

digital-era governance and citizen-centric service design.

4.2 E-Governance and Principles of Good Governance

E-governance is frequently justified by reference to principles of good governance — transparency, accountability, efficiency, participation, and the rule of law ²⁰— articulated in instruments such as the United Nations Convention against Corruption (2003) and successive United Nations Development Programme governance frameworks. The doctrinal question is whether these principles, largely emergent from "soft law" and developmental discourse, generate binding international obligations, or remain aspirational standards against which State digital governance is merely evaluated.

4.3 International Legal Instruments Relevant to Digital Governance

Relevant instruments include the United Nations General Assembly resolutions on the use of ICTs (commencing with Resolution 53/70 of 1998)²¹, the Tunis Agenda for the Information Society (2005), the United Nations Commission on International Trade Law's Model Law on Electronic Commerce (1996) and Model Law on Electronic Signatures (2001), the United Nations Convention on the Use of Electronic Communications in International Contracts (2005),²² and regional instruments such as the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention, 2014). These instruments collectively establish facilitative legal infrastructure for electronic governance and commerce without displacing the underlying consensual treaty architecture.

4.4 Role of International Organizations in Digital Governance

The International Telecommunication Union (ITU), the multi-stakeholder Internet Governance Forum, the Internet Corporation for Assigned Names and Numbers (ICANN), the World Trade Organization (in respect of digital trade and e-commerce moratoria), and the United Nations Open-Ended Working Group on ICT security each contribute distinct governance functions, reflecting a fragmented institutional landscape in which technical, economic, and security dimensions of digital governance are addressed by different bodies operating under different

²⁰ United Nations Convention against Corruption, adopted 31 October 2003, 2349 UNTS 41.

²¹ United Nations General Assembly Resolution 53/70, *Developments in the Field of Information and Telecommunications in the Context of International Security*, UN Doc A/RES/53/70 (4 January 1999).

²² United Nations Commission on International Trade Law, United Nations Convention on the Use of Electronic Communications in International Contracts (2005).

participatory and consensual logics. ICANN's governance of the domain name system, in particular, illustrates a governance modality substantially detached from classical inter-State consent, being administered through a multi-stakeholder model in which States participate as one constituency among several.²³

4.5 Human Rights and E-Governance

The application of existing human rights instruments to the digital sphere has been affirmed by the United Nations Human Rights Council's resolutions on the promotion and protection of human rights on the Internet, premised on the principle that offline rights apply equally online. The right to privacy, protected under Article 17 of the International Covenant on Civil and Political Rights,²⁴ has assumed particular salience in relation to State surveillance and data-driven e-governance, as reflected in successive reports of the UN Special Rapporteur on the right to privacy and General Assembly resolutions on the right to privacy in the digital age.

4.6 Transparency, Accountability, and Participation in Digital Governance

Algorithmic decision-making within e-governance systems raises distinct doctrinal concerns regarding transparency and accountability, particularly where automated systems determine eligibility for public benefits, immigration status, or law-enforcement risk assessment. The absence of binding international standards specifically addressing algorithmic governmental decision-making constitutes a significant normative gap, addressed only partially by instruments such as the Council of Europe's Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (2024).

CHAPTER 5: DIGITAL SOVEREIGNTY AND THE TRANSFORMATION OF STATE CONSENT

5.1 Traditional Understanding of State Consent

State consent, in its classical formulation, denotes the voluntary assumption of legal obligation by a State, whether through the explicit conclusion of a treaty, accession to an existing instrument, or the deliberate or acquiescent participation in the formation of customary

²³ Tunis Agenda for the Information Society, World Summit on the Information Society, UN Doc WSIS-05/TUNIS/DOC/6 (18 November 2005), paras 29–40.

²⁴ United Nations International Covenant on Civil and Political Rights, 999 UNTS 171, art 17.

international law.²⁵ The doctrine assumes a discrete, identifiable, and temporally locatable act of will by a sovereign authority, exercised with full knowledge of the obligation assumed.

5.2 Cross-Border Data Flows and Consent

The regulation of cross-border data flows illustrates the strain placed upon this classical model. Instruments such as the European Union's adequacy decision mechanism under Article 45 of the GDPR condition²⁶ the lawful transfer of personal data to third countries upon a unilateral determination by the European Commission that the receiving State's domestic legal framework offers an "essentially equivalent" level of protection — a determination made without the consent, and indeed sometimes against the express objection, of the third State concerned. This represents a form of indirect, unilaterally-imposed regulatory consent substitution: the third State's actual legal practice, rather than its consent, becomes the operative criterion for binding effect upon entities transacting with EU data subjects.

5.3 Cyber Operations and Consent of States

Consent assumes a distinct operative significance in the law of cyber operations, particularly in relation to the doctrine of countermeasures and the circumstance precluding wrongfulness recognised under Article 20 of the ILC Articles on State Responsibility, whereby consent validly given by an injured State precludes the wrongfulness of conduct that would otherwise breach an obligation owed to it.²⁷ Questions arise as to whether consent to routine data-sharing arrangements, cybersecurity cooperation, or the hosting of foreign government cloud infrastructure may be construed as anticipatory consent to associated intrusive measures, and as to the conditions under which such consent may be withdrawn.

5.4 Consent in International Digital Cooperation

Mutual legal assistance treaties and instruments such as the Budapest Convention on Cybercrime establish structured consent mechanisms for cross-border evidence gathering,²⁸ yet are increasingly supplemented by unilateral instruments — such as the United States'

²⁵ Statute of the International Court of Justice, art 38(1); Vienna Convention on the Law of Treaties, 1969.

²⁶ Regulation (EU) 2016/679 (General Data Protection Regulation), art 45.

²⁷ International Law Commission, *Articles on Responsibility of States for Internationally Wrongful Acts* (2001), art 20.

²⁸ Convention on Cybercrime (Budapest Convention), ETS No 185, opened for signature 23 November 2001.

Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018²⁹— that authorise domestic compulsion of data held abroad by entities subject to that State's jurisdiction, without requiring the consent of the State in whose territory the data physically resides. This development illustrates a shift from State-to-State consensual cooperation toward entity-based, jurisdiction-driven compulsion that bypasses the territorial sovereign altogether.

5.5 Impact of Artificial Intelligence on State Consent

Artificial intelligence systems deployed in governance, defence, and regulatory contexts complicate the consent doctrine in a further respect: where AI systems are trained on data, or operate on infrastructure, sourced from multiple jurisdictions, and where their decision logic is opaque even to their State operators, it becomes doctrinally difficult to identify a discrete moment or instrument of State consent to the resulting governance outcomes. The State's consent, if it exists at all, is diffused across procurement decisions, infrastructural dependency, and standard-setting processes in which the State may have limited effective participation, particularly where dominant AI infrastructure is controlled by a small number of private corporations headquartered in a handful of States.

5.6 Reassessment of Consent in Contemporary International Law

The cumulative effect of the foregoing developments suggests that consent in the digital sphere increasingly operates through three modified modalities: (a) **structural consent**, whereby a State's consent is inferred from continued participation in an institutional or technical system (such as the Domain Name System) whose governance it does not directly control; (b) **conditional/coerced consent**, whereby formal consent is extracted under conditions of practical necessity created by asymmetric market or infrastructural power, as with adequacy-decision-driven data protection compliance; and (c) **residual consent**, whereby States retain only the diminished capacity to withdraw from, rather than affirmatively shape, governance arrangements established by dominant States or private actors. This typology forms the analytical foundation for the comparative and normative analysis undertaken in Chapters 6 and 7.

²⁹ Clarifying Lawful Overseas Use of Data Act (CLOUD Act), Pub L No 115–141, Div V, 132 Stat 1213 (2018).

CHAPTER 6: ANALYSIS OF INTERNATIONAL LEGAL INSTRUMENTS AND STATE PRACTICE

6.1 United Nations Frameworks on Digital Governance

The UNGGE and OEWG processes have produced consensus reports affirming the applicability of existing international law, including sovereignty, non-intervention, and due diligence, to State conduct in cyberspace³⁰, while declining to specify the precise legal consequences of sovereignty violations absent a clearer crystallisation of State practice. The 2021 OEWG consensus report's endorsement of a set of voluntary, non-binding norms of responsible State behaviour — building upon the 2015 UNGGE norms — reflects a deliberate preference for soft, consent-friendly instruments over binding treaty obligations, reflecting States' continuing reluctance to commit to hard legal constraints in this domain.

6.2 Budapest Convention on Cybercrime

The Council of Europe's Convention on Cybercrime (Budapest, 2001) remains the principal binding multilateral instrument addressing cybercrime³¹ and cross-border evidentiary cooperation, structured around classical consensual mutual-assistance mechanisms under its Chapter III. Its limited membership outside Europe, and the controversy surrounding its Second Additional Protocol (2022) on enhanced cooperation and direct disclosure of electronic evidence, illustrate the tension between expanding investigative efficiency and preserving the consensual prerogatives of the territorial sovereign.

6.3 General Data Protection Regulation (GDPR) and Extraterritorial Jurisdiction

The GDPR's extraterritorial scope provision under Article 3(2) extends its application to data controllers and processors outside the European Union³² where their processing activities relate to the offering of goods or services to, or the monitoring of, data subjects within the Union. This represents a deliberate and assertive use of the targeting/effects basis of jurisdiction, generating de facto global regulatory influence — the so-called "Brussels Effect" — through market power rather than treaty-based consent, compelling third States and entities to align

³⁰ United Nations Group of Governmental Experts, UN Doc A/70/174 (22 July 2015); Open-Ended Working Group on ICT Security, Final Substantive Report, UN Doc A/75/816 (18 March 2021).

³¹ United Nations Group of Governmental Experts, UN Doc A/70/174 (22 July 2015); Open-Ended Working Group on ICT Security, Final Substantive Report, UN Doc A/75/816 (18 March 2021).

³² Regulation (EU) 2016/679 (General Data Protection Regulation), art 3(2).

domestic standards with EU norms in order to retain market access.

6.4 Tallinn Manual and Cyber Operations

The Tallinn Manual 2.0, while not a binding instrument but a restatement by an independent group of international law experts³³, has nonetheless exercised considerable interpretive influence upon State positions regarding the application of sovereignty, due diligence, and countermeasures doctrines to cyber operations. Its treatment of consent — particularly regarding consensual cyber assistance operations and the limits of anticipatory consent — provides the most doctrinally developed treatment of the consent-cyberspace intersection currently available, notwithstanding its non-binding status.

6.5 National Approaches to Digital Sovereignty

6.5.1 European Union

The European Union's approach integrates data protection (GDPR), digital market regulation (the Digital Markets Act and Digital Services Act), and an explicit policy discourse of "technological sovereignty" and "strategic autonomy," reflecting an institutional model in which sovereignty is exercised collectively at supranational level and projected extraterritorially through regulatory standard-setting.

6.5.2 United States

The United States has historically favoured an open, multi-stakeholder model of internet governance resistant to formal international regulation, while simultaneously asserting expansive extraterritorial jurisdiction over data through instruments such as the CLOUD Act and through the dominant market position of United States-based technology corporations, producing a model of sovereignty exercised through corporate and infrastructural leverage rather than formal territorial assertion.

6.5.3 China

China's cyber sovereignty doctrine, formalised in its 2017 Cybersecurity Law and subsequent

³³ Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017).

Data Security Law (2021) and Personal Information Protection Law (2021), asserts comprehensive State control over data localisation, cross-border data transfer, and content within its "national cyberspace," representing the most territorially assertive contemporary model of digital sovereignty, closely tied to information-control objectives.

6.5.4 India

India's approach, evolving through the Information Technology Act, 2000, the landmark privacy judgment in *Justice K.S. Puttaswamy v. Union of India* (2017) recognising privacy as a fundamental right, and the Digital Personal Data Protection Act, 2023, reflects a hybrid model balancing data localisation imperatives, digital public infrastructure initiatives (such as the India Stack and Aadhaar digital identity system), and an emerging insistence on data sovereignty calibrated to developmental and security objectives, distinct from both the EU's rights-based and China's control-based models.

6.6 Emerging State Practice and Customary International Law

The marked divergence among these national approaches — rights-based, market-based, control-based, and developmental — suggests that, notwithstanding repeated affirmations of the general applicability of international law to cyberspace, the specific content of a customary norm of "digital sovereignty" has not yet crystallised with the degree of uniformity, consistency, and *opinio juris* required under the *North Sea Continental Shelf* standard for customary international law formation.³⁴ What can be observed, instead, is the consolidation of overlapping, State-specific regulatory regimes that interact through indirect, market-mediated, and infrastructural pressure rather than coordinated treaty-based consent — a pattern the present study terms "regulatory parallelism without normative convergence."

CHAPTER 7: TOWARDS A NEW INTERNATIONAL LEGAL FRAMEWORK

7.1 Gaps in Existing International Law

The analysis in preceding chapters identifies several doctrinal gaps: the absence of a binding multilateral instrument defining the content and limits of digital sovereignty; the lack of agreed thresholds for sovereignty violation in cyberspace; the absence of an international framework

³⁴ *North Sea Continental Shelf Cases* (Federal Republic of Germany v Denmark; Federal Republic of Germany v Netherlands) ICJ Reports 1969, p 3, paras 71–77.

governing State use of artificial intelligence in governance functions; and the unresolved status of consent where regulatory effect is achieved through market dominance rather than formal assent.

7.2 Need for International Regulation of Digital Sovereignty

The continuation of fragmented, unilaterally-asserted digital sovereignty regimes carries the risk of an increasingly balkanised "splinternet,"³⁵ in which incompatible national data and infrastructure regimes undermine the interoperability that underlies the economic and developmental benefits of digital connectivity, while leaving weaker States disproportionately exposed to the regulatory and infrastructural leverage of dominant digital powers and corporations.

7.3 Harmonization of Cyber and Data Governance Norms

A harmonisation strategy should prioritise the development of mutually recognised baseline standards for data protection (building upon convergence already observable between GDPR-inspired frameworks across multiple jurisdictions), agreed thresholds for the application of sovereignty and due diligence obligations in cyberspace building upon the Tallinn Manual's interpretive groundwork,³⁶ and structured, treaty-based mutual assistance frameworks that reduce reliance on unilateral compulsion mechanisms such as the CLOUD Act model.

7.4 Legal Challenges of Artificial Intelligence Governance

The governance of artificial intelligence in State functions requires the development of binding or quasi-binding standards addressing transparency, human oversight, and accountability for automated governmental decision-making, building upon emergent instruments such as the Council of Europe's AI Convention, while addressing the specific difficulty that AI infrastructure is frequently controlled by private entities outside the direct sovereign control of the deploying State, requiring innovative consent mechanisms that bind both States and the private infrastructural intermediaries upon which they depend.³⁷

³⁵ United Nations Conference on Trade and Development, *Digital Economy Report* (latest edition discussing fragmentation of digital governance and data regimes).

³⁶ Michael N Schmitt (ed), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press 2017).

³⁷ Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the

7.5 Proposal for a Normative Framework on Digital Sovereignty

This study proposes a layered normative framework comprising: (a) a **foundational charter-level instrument** affirming the applicability of sovereignty, non-intervention, and due diligence to digital conduct, with agreed interpretive guidance reducing present ambiguity; (b) **sectoral protocols** addressing data protection, cybercrime cooperation, and AI governance, structured to permit graduated accession reflecting differing developmental capacities; and (c) an **institutional consent-verification mechanism**, potentially situated within or alongside the United Nations OEWG process, tasked with assessing whether extraterritorial regulatory measures (such as adequacy determinations) meet minimum procedural fairness standards vis-à-vis affected third States, thereby restoring a measure of genuine consensual participation to processes presently characterised by unilateral imposition.

7.6 Recommendations

(a) States should pursue the negotiation of a binding framework convention on the application of sovereignty principles to cyberspace, building on existing soft-law consensus; (b) Extraterritorial data regulation should incorporate formal consultation mechanisms with affected third States prior to adequacy or equivalence determinations; (c) Mutual legal assistance frameworks should be modernised multilaterally to reduce reliance on unilateral compulsion instruments; (d) International standard-setting on AI governance should explicitly address State accountability for privately-developed AI systems deployed in governmental functions; and (e) Developing States should be afforded technical and institutional support to ensure substantive, rather than merely formal, participation in digital governance negotiations.

CHAPTER 8: CONCLUSION

8.1 Findings

The study finds that digital sovereignty, as presently asserted by States, is doctrinally heterogeneous and has not yet crystallised into a uniform rule of customary international law. It finds further that the operation of State consent in the digital sphere has been substantially modified through three identifiable modalities — structural, conditional, and residual consent — displacing the classical model of discrete, voluntary assumption of obligation. Existing

Rule of Law.

international instruments address fragments of the digital governance landscape without providing a coherent, consent-respecting framework for digital sovereignty as a whole.

8.2 Conclusions

The doctrine of State consent remains the indispensable normative foundation of international law, including in the digital sphere; however, its operative mechanics have been transformed by the technical and economic realities of digital infrastructure, such that consent is increasingly exercised — and frequently extracted — through structural participation and market dependency rather than discrete, deliberative assent. This transformation, left unaddressed, risks entrenching asymmetries of digital power as a substitute for genuine consensual international law-making.

8.3 Suggestions for Legal Reform

International law-making institutions should prioritise the development of a framework convention on digital sovereignty, incorporating express procedural safeguards for third-State participation in extraterritorial regulatory determinations, and should extend binding accountability standards to the governance of artificial intelligence systems deployed in State functions, so as to restore a substantively, rather than merely formally, consensual basis to the governance of the digital domain.

BIBLIOGRAPHY

Primary Sources

Treaties and Conventions

- Vienna Convention on the Law of Treaties, 1969
- Charter of the United Nations, 1945
- Statute of the International Court of Justice, 1945
- Council of Europe, Convention on Cybercrime (Budapest Convention), 2001, and its Second Additional Protocol, 2022
- Council of Europe, Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law, 2024
- African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), 2014
- United Nations Convention on the Use of Electronic Communications in International Contracts, 2005
- United Nations Convention against Corruption, 2003
- International Covenant on Civil and Political Rights, 1966

UN Resolutions

- UNGA Resolution 2625 (XXV), Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States, 1970
- UNGA Resolution 53/70, Developments in the field of information and telecommunications in the context of international security, 1998
- UN Human Rights Council and General Assembly resolutions on the right to privacy in the digital age and on human rights on the Internet
- Reports of the UN Group of Governmental Experts (UNGGE), 2013, 2015, 2021
- Reports of the UN Open-Ended Working Group (OEWG) on developments in the field of ICTs, 2021–2025

International Instruments

- UNCITRAL Model Law on Electronic Commerce, 1996
- UNCITRAL Model Law on Electronic Signatures, 2001
- Tunis Agenda for the Information Society, 2005
- European Union, General Data Protection Regulation (EU) 2016/679
- European Union, Digital Markets Act and Digital Services Act
- United States, Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018
- China, Cybersecurity Law (2017), Data Security Law (2021), Personal Information Protection Law (2021)
- India, Information Technology Act, 2000; Digital Personal Data Protection Act, 2023
- International Law Commission, Articles on Responsibility of States for Internationally Wrongful Acts, 2001

Judicial Decisions

- *The Case of the S.S. Lotus* (France v. Turkey), PCIJ Series A, No. 10 (1927)
- *North Sea Continental Shelf Cases* (Federal Republic of Germany/Denmark; Federal Republic of Germany/Netherlands), ICJ Reports 1969
- *Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America), ICJ Reports 1986
- *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (Supreme Court of India)

Secondary Sources

Books

- Schmitt, M.N. (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (Cambridge University Press, 2017)
- Crawford, J., *Brownlie's Principles of Public International Law* (Oxford University Press)

- Shaw, M.N., *International Law* (Cambridge University Press)
- Krasner, S.D., *Sovereignty: Organized Hypocrisy* (Princeton University Press)
- Bradford, A., *The Brussels Effect: How the European Union Rules the World* (Oxford University Press)

Journal Articles

- Schmitt, M.N. and Vihul, L., "Sovereignty in Cyberspace: Lex Lata Vel Non?", *American Journal of International Law Unbound*
- Various contributions on data sovereignty, extraterritorial jurisdiction, and cyber due diligence published in the *European Journal of International Law*, *American Journal of International Law*, *Chinese Journal of International Law*, and *Indian Journal of International Law*

Reports and Commentaries

- United Nations Conference on Trade and Development, *Digital Economy Report* (various years)
- World Economic Forum and Internet Governance Forum proceedings and outcome documents
- European Commission, communications and staff working documents on European digital sovereignty and adequacy decisions.