

Digital Globalization and the Emergence of Transnational Law: Legal Challenges of Data, Technology, and Cross-Border Digital Transactions

Aisha Rafiq

LLM Student, G D Goenka University , Noida.

ABSTRACT

Traditional architecture of law based on principles of state sovereignty, strict territorial jurisdiction is undergoing systemic disruption as a result of the speed of digital globalization. With the widespread use of cloud computing, cross-border data transfers, AI, and blockchain, the traditional relationship between geographical location and regulatory jurisdiction has been broken. In this paper, the shift of the concept of law from a state-centric Westphalian approach to a more polycentric form of transnational governance is discussed. It examines the involvement of non-state actors in the process of norm creation, such as multinational technology firms, hybrid standardization bodies and transnational civil society, who are increasingly engaged in the process of norm creation alongside sovereign states and international organizations.

This paper examines the mechanisms that are developing to facilitate legal conflict resolution in the digital realm through cross-border data transfer regimes, regulatory fragmentation, extraterritorial jurisdictional friction and private technological ordering (*lex cryptographia*). It concludes with the need for institutional change to ensure the interoperability of rule systems, mutual recognition and co-regulatory approaches to maintain legal security, fundamental human rights and trust of trust in a 'hyper-connected global economy.

1. INTRODUCTION: THE DETERRITORIALIZATION OF LAW

The digital globalization, which can be characterised as hyper speed of data exchange, decentralised networks and digital transactions has broken this space alignment of municipal law for domestic affairs and the public international law to mediate relations between the sovereign states¹.

Digital globalization is based on a permeability model in which the physical border is of little or no significance². The information packet-switching, distributed server networks and cloud architectures of digital assets break, re-route and store information across many different jurisdictions at once, in turn creating a virtual environment where human interactions, economic exchanges and algorithmic decision-

¹See Lassa Oppenheim, *International Law: A Treatise* 452–56 (8th ed. 1955); see also Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* 3–9 (1999) (analyzing the evolution and conceptual boundaries of Westphalian sovereignty).

² See Malcolm N. Shaw, *International Law* 1–15 (9th ed. 2021); see also *Island of Palmas Case* (U.S. v. Neth.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928) ("Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.").

making take place without a single geographical location³. The "deterritorialization" of these elements of "human action, property and commercial performance" poses a problem for the legal system: the basis of legislative jurisdiction, of the competency of the courts and of the enforcement of regulation is being weakened by the removal or abstraction of human action, property, and commercial performance from physical territory. This detachment or abstraction of human action, property and commercial performance from physical territory poses a problem for the legal system: the basis of legislative jurisdiction, that of the competency of the courts and that of the enforcement of regulation is being weakened⁴.

The normative architecture of law has broadened, while the traditional architecture of the state is losing ground after failing to assert itself in the context of borderless processes in digital age⁵. Today, the state is no longer the only creator of rules and norms, but rather a polycentric system of transnational law is now in place, which is a dynamic process of norm creation, enforcement and redefinition carried out by a variety of actors⁶, including sovereign states, supranational unions, multinational technology corporations, private industry setting groups, international administrative bodies and civil society⁷.

This research paper delves in this structural transition. It explores the new face of legal authority brought about by digital globalization, looks at the pressing legal issues created by cross-border data transfers and technological innovation, and challenges the new forms of governance that seek to balance state sovereignty with digital integration in the world.

2. The shift from state-centric to transnational legal orders-

A. The Limits of the Westphalian Paradigm in Cyberspace

Traditionally, conflict of laws (private international law) would determine cross-border disputes by determining which of the laws was applicable, based on one or more of several "connecting factors": the law of the place where the contract was formed (*lex loci contractus*); the law of the place of injury (*lex loci delicti*); the domicile of the parties⁸. Traditionally, conflict of laws (private international law) would determine cross-border disputes from a choice of applicable laws based on one or more of several "connecting factors" such as the place where the contract was formed (*lex loci contractus*), the place of injury (*lex loci delicti*), and the domicile of the parties⁹.

These are the conventional connecting factors that get dissolved in cross-border digital transactions:

³See McKinsey Glob. Inst., *Digital Globalization: The New Era of Global Flows* 15–28 (2016); see also Anupam Chander, *The Electronic Silk Road: How the Web Binds the World in Commerce in Violation of the Law*, 118 Yale L.J. 1084, 1088–92 (2009).

⁴See Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L.J. 326, 329–34 (2015); see also Andrew Keane Woods, *Against Data Exceptionalism*, 68 Stan. L. Rev. 729, 735–40 (2016).

⁵See Dan Jerker B. Svantesson, *Solving the Internet Jurisdiction Puzzle* 23–45 (2017); see also David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367, 1370–75 (1996) (arguing that cyberspace radically undermines the relationship between spatial borders and legal control).

⁶See Saskia Sassen, *Territory, Authority, Rights: From Medieval to Global Assemblages* 222–35 (2006); see also Paul Schiff Berman, *Global Legal Pluralism: A Jurisprudence of Law Beyond Borders* 3–20 (2012).

⁷See Terence C. Halliday & Gregory Shaffer, *Transnational Legal Orders*, in *Transnational Legal Orders* 1, 3–12 (Terence C. Halliday & Gregory Shaffer eds., 2015); see also Peer Zumbansen, *Transnational Law, Evolving*, in *Elgar Encyclopedia of Comparative Law* 899, 901–05 (Jan M. Smits ed., 2d ed. 2012).

⁸See Montevideo Convention on the Rights and Duties of States art. 1, Dec. 26, 1933, 49 Stat. 3097, 165 U.N.T.S. 19.

⁹See Restatement (Second) of Conflict of Laws §§ 6, 145, 188 (Am. L. Inst. 1971); see also James Fawcett et al., *International Sale of Goods in the Conflict of Laws* 12–25 (2005).

- An e-commerce contract could be called from servers in three continents, be executed by an automated smart contract and be paid for by a cryptographic token on a distributed ledger. Even if a single situs or geographical location could be determined, it would be an arbitrary concept in theory.¹⁰
- In digital torts, on the other hand for example, a global data breach, algorithmic defamation or online IP infringement the harmful action and its repercussions are spread out over dozens of jurisdictions at the same time¹¹.

B. Conceptualization of the Transnational Law

To capture these non-territorial realities, modern legal scholarship includes the "transnational law" of Philip Jessup ("all law which regulates actions or events that transcend national frontiers")¹² as well as public and private international law and domestic law with transnational effects, which are all conceptualized as "transnational legal orders" of settled complexes of formal-informal legal norms that reappear across jurisdictions to govern human behaviour¹³.

C. Non-State Actors as Normative Creators

The digital globalization has given non-state actors a new role as law makers:

- These companies, also known as multinational technology corporations, have quasi-sovereign control over what constitutes free expression, privacy, and commercial access to billions of people around the world as they are defined by their Terms of Service (ToS), Community Guidelines, and Content Moderation Policies. These contractual agreements are *lex digitalis*, private governance without the intervention of public bailiffs, but by algorithmic enforcement, account suspension and by a digital ban.
- The technical standardisation bodies, like the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), and the World Wide Web Consortium (W3C), similarly codify internet architecture and protocols, and thus regulate internet user possibilities just as much as statutory laws. The technical standardisation bodies, such as the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), and the World Wide Web Consortium (W3C), also determine the underlying code, protocols and architecture of the internet, and thus regulate the possibilities of internet users just as much as do statutory laws.
- TCS Hybrid Networks: The role of NGOs, privacy rights organizations and academic consortia in shaping global norms, through norms challenging by businesses, multi-stakeholder governance processes and soft-law frameworks that inform state law.

3. Main Legal Issues in Trans-Border Digital Transactions -

A. Data Sovereignty vs. Free Cross-Border Data Flows

The free flow of data has resulted in some states taking a defensive stance, with measures taken to ensure

¹⁰ See Aaron D. Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, SSRN Electronic J. 1, 12–18 (2015); see also Gerald Spindler & Fritjof Börner, *E-Commerce Law in Europe and the USA*, 15–28 (2002).

¹¹ See Uta Kohl, *Data Law and Foreign Government Access to Data: Multilateral Public Interest Interventions* 45–62 (2021); see also Dan Jerker B. Svantesson, *A "Cross-Border Internet Jurisdiction Protection treaty" – A Proposal*, 4 J. Internet L. 18, 19–22 (2018).

¹² Philip C. Jessup, *Transnational Law* 1–15 (1956).

¹³ See Halliday & Shaffer, *supra* note 7, at 11–15; see also Peer Zumbansen, *Neither 'Public' nor 'Private', 'National' nor 'International': Transnational Law and Discourse in a European Context*, 3 Eur. L.J. 300, 305–10 (2001).

"digital sovereignty."¹⁴

There are some different policy lenses for states to assert digital sovereignty:

- The EU has established the principle that information protection is a fundamental human right in Article 7 and 8 of the Charter of Fundamental Rights of the EU. The General Data Protection Regulation (GDPR) sets the limitation on the transfer of personal data to non-EU/EEA countries in that the recipient country must provide an "adequate" level of protection, or the data exporter must provide appropriate safeguards such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs).
- It is important to note that national security laws and data localization laws like the Data Security Law and the Personal Information Protection Law (PIPL) in China, the Cyber Security Law in Russia and the Cyber Security and Data Protection Act in India emphasize national control over digital assets, cybersecurity, and capabilities for surveillance.

This ideology division leads to regulatory fragmentation. MEs are exposed to compliance challenges because complying with the disclosure regulations of one jurisdiction (e.g., U.S. discovery order or law enforcement subpoena under the CLOUD Act) may conflict with the data protection/privacy regulations of the other jurisdiction (e.g., GDPR or Chinese data protection laws).

B. The United States' commitment to Republicanism and the principle of popular sovereignty

As a result, states have enacted laws that have explicit extra-territorial application, leading to the emergence of "overlapping jurisdictions" and "international tensions".

The U.S. Clarifying Lawful Overseas Use of Data (CLOUD) Act makes the same point, in that a warrant issued by domestic law enforcement authorities would apply to any service provider within the U.S. jurisdiction, including those storing data outside the physical boundaries of the United States.

These are assertions of jurisdiction beyond the territorial boundary, which create jurisdictional disputes:

- Data Protection Commissioner v. Facebook Ireland Ltd and Maximillian Schrems (Schrems II): The Court of Justice of the European Union (CJEU) ruled that the EU-U.S. Privacy Shield was invalid. In reaching its decision, the CJEU found that U.S. national security surveillance laws (Section 702 of the U.S. Federal Intelligence and Surveillance Act (FISA) and Executive Order 12333) did not meet the standards set by EU law with regard to the protection of personal data, meaning that transfers to U.S. commercial entities were potentially unlawful unless additional technical safeguards were implemented.
- Enforcement Dilemmas: It is difficult to enforce monetary judgments or orders for injunctive remedies against foreign digital actors, even in cases where jurisdiction is validly established under domestic long-arm jurisdictions, without the existence of bilateral treaties or mutual recognition agreements¹⁵.

C. Blockchain, AI, and Smart Contracts:

New legal challenges arise with the speed of the technological development and the law was not intended to deal with the new challenges.

- Smart Contracts and Decentralized Autonomous Organizations (DAOs): Smart contracts; self-executing code which is deployed onto distributed ledgers and automatically act when certain predetermined conditions are met; challenge fundamental concepts of contract law, such as mutual

¹⁴ See Anupam Chander & Uyen P. Le, *Data Nationalism*, 64 Emory L.J. 677, 680–88 (2015); see also Theodore Christakis, *European Digital Sovereignty: Theory and Practice*, 12 Cahiers du Numérique 45, 48–55 (2020).

¹⁵ See Dan Jerker B. Svantesson, *Enforcing Privacy Rights Across Borders: The Challenges and the Path Forward*, 11 Int'l Data Priv. L. 215, 218–22 (2021).

assent, mistake, unconscionability, and remedies available to a court of law. Algorithmic transaction failures or liquidations triggered by tainted data feeds (oracle failures) place traditional legal frameworks at a disadvantage in terms of being able to define a wrongdoer or assert jurisdiction over the transaction in a decentralized anonymous network.

- Moreover, the use of AI tools and automated decision-making by agents of states at different borders introduces new issues on the concepts of tortious liability, IP property rights, and algorithmic bias, with the issues of "tortious liability" and "algorithmic bias" being especially complex. In addition, the training of AI systems across borders based on data from around the world challenges the territorial application of copyright law and the exception for 'fair use'.

4. TRANSNATIONAL GOVERNANCE MECHANISMS EMERGING-

To avoid the fragmentation of the regulatory environment causing a breakdown of the system, multiple public, private and hybrid transnational mechanisms of governance that aim to provide stability and predictability to global transactions have emerged.

A. Bilateral and Multilateral Trade Agreements

International trade law has adapted to deal with barriers created by technology. Regional Trade Agreements (RTAs) today systematically and explicitly include digital trade chapters focused on safeguarding the cross border movement of data and prohibiting digital protectionism:

- The CPTPP: Clearly bans member states from imposing restrictions on cross-border transfer of information using electronic means when this transfer is for the purposes of conducting business and bans localization of computing facilities as a precondition for conducting business.
- The United States-Mexico-Canada Agreement (USMCA): Provides strong digital trade provisions, including a commitment to free data flows, to prevent third parties from being held liable for posting content on their platforms or for any third parties' violations of third party rights, and to prohibit forcing disclosure of source code.

B. Network Meters and Devices

States are moving towards interoperability and mutual recognition options, instead of trying to introduce uniform global legislation which is politically unachievable due to competing geopolitical interests:

- The APEC CBPR system, which is the source of the Global Cross-Border Privacy Rules (CBPR) Forum, will help facilitate personal data transfers from one economy to another while also setting a minimum standard for privacy principles among certified companies, which will be enforced by privacy authorities in a particular economy.
- EU-U.S. Data Privacy Framework (DPF): The European Commission in July 2023 issued an adequacy decision for the EU-U.S. Data Privacy Framework, following the invalidation of Privacy Shield. The framework established structural safeguards, such as a binding redress mechanism: an independent Data Protection Review Court (DPRC) to hear claims from individuals in the EU, to try to close the gap between different legal paradigms.

C. Private Technological Ordering: Lex Cryptographia

The private ordering mechanisms play a key role in the digital economy, alongside state-sponsored measures. Lex Cryptographia is a legal framework based on "self-enforcing smart contracts and decentralized cryptographic protocols".

Although these systems deliver quick and inexpensive solutions to international transactions that take place online, their enforceability under public law and whether or not they meet public policy standards,

as well as under the New York Convention on the Recognition and Enforcement of Foreign Arbitral Awards, is a matter of uncertainty.

5. Restructuring law for a digitalized global society.

Some fundamental reconsideration of core concepts of law is necessary to understand how transnational law developed in the context of digital globalization. A re-thinking of basic concepts of law is needed to grasp the emergence of transnational law in digital globalization. Three normative principles demand attention in the continuous process of law restructuring in order to facilitate the maintenance of its effectiveness, authority and equity:

A. Functional Jurisdiction/Contextual Jurisdiction from Territorial Jurisdiction-

The concept of territorial connection is conventional and should be replaced by dynamic jurisdictional concepts. In addition, smartly defining territorial jurisdiction by "functional" or "effects-based" principles, that is, by the significant and predictable effects of digital activities in a jurisdiction, will be increasingly accepted by courts and legislatures, and will enable regulators to consider data processing within the framework of society's norms and expectations for a specific functional context rather than in the context of formal territorial definitions.

B. The Public-Private Governance of Biodiversity–Regulation and Co-Regulation-

Unilateral state regulation may be unworkable or inflexible because there is a lack of information between the states and technology companies. Co-regulation is an emerging approach to effective digital governance, under which the state imposes binding normative goals, limits on human rights, and oversight of activities with a mandate for private industry or technical bodies to design the technology, implement it, and set the standards. Co-regulation is an approach in which the state sets law-based normative goals, boundaries on human rights, and oversight over activities while delegating the design, implementation, and standard setting of that technology to private industry and technical bodies, as is done in the European Union's Artificial Intelligence Act, which establishes risk-based legal standards, leaving the technical design, implementation, and standard-setting to European standard-setting bodies (CEN/CENELEC).

C. The President's Annual Report on the Administration of the Civil Rights Act of 1964-

Facing both the challenge of preserving fundamental public law values in algorithmic decision making and automated enforcement, such as procedural due process, non-discrimination, transparency and accountability, both technologists and legal architects bear a shared responsibility to work together in this effort.¹⁶

6. CONCLUSION

Digital globalization has created a new type of spatially decentralized legal order that is state-dominated. Digital globalization has unsettled the preexisting state-centric legal order architecture. The separation of economic activity, human relationships and norm-creation from physical territory has revealed the shortcomings of the traditional doctrines of territorial jurisdiction and choice of law. Responding to this, a multi-layered and multi-centred transnational legal order has come to shape, a legal space in which states and supranational institutions, tech corporations and technical standards bodies are continuously negotiating the rules of engagement in a hyper-connected world.

¹⁶See Nicolas Suzor, *Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms*, 24 *Social Media + Society* 1, 3–8 (2018); see also Giovanni De Gregorio, *Digital Constitutionalism in Europe: Reframing Rights and Power in the Algorithmic Society* 55–72 (2022).

On the one hand, this transnational legal development has sparked innovation, unfenced international trade and swift technological rollout, but on the other hand it has led to legal fragmentation, transnational jurisdictional conflicts and threats to state sovereignty and fundamental rights. These tensions need to be addressed by breaking out of limited territorial dogma and adopting jurisdiction models that are functional, interoperability models that are international and co-regulatory partnerships. It is only by applying legal principles to the realities of a deterritorialized digital architecture that the global community can create a transnational legal order, that is innovative and integrates into cross-border flows, while simultaneously ensuring legal certainty, human rights and rule of law.

REFERENCES:

1. Lassa Oppenheim, *International Law: A Treatise* 452–56 (8th ed. 1955); see also Stephen D. Krasner, *Sovereignty: Organized Hypocrisy* 3–9 (1999) (analyzing the evolution and conceptual boundaries of Westphalian sovereignty).
2. Malcolm N. Shaw, *International Law* 1–15 (9th ed. 2021); see also *Island of Palmas Case (U.S. v. Neth.)*, 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928) ("Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State.").
3. McKinsey Glob. Inst., *Digital Globalization: The New Era of Global Flows* 15–28 (2016); see also Anupam Chander, *The Electronic Silk Road: How the Web Binds the World in Commerce in Violation of the Law*, 118 Yale L.J. 1084, 1088–92 (2009).
4. Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L.J. 326, 329–34 (2015); see also Andrew Keane Woods, *Against Data Exceptionalism*, 68 Stan. L. Rev. 729, 735–40 (2016).
5. Dan Jerker B. Svantesson, *Solving the Internet Jurisdiction Puzzle* 23–45 (2017); see also David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 Stan. L. Rev. 1367, 1370–75 (1996) (arguing that cyberspace radically undermines the relationship between spatial borders and legal control).
6. Saskia Sassen, *Territory, Authority, Rights: From Medieval to Global Assemblages* 222–35 (2006); see also Paul Schiff Berman, *Global Legal Pluralism: A Jurisprudence of Law Beyond Borders* 3–20 (2012).
7. Terence C. Halliday & Gregory Shaffer, *Transnational Legal Orders*, in *Transnational Legal Orders* 1, 3–12 (Terence C. Halliday & Gregory Shaffer eds., 2015); see also Peer Zumbansen, *Transnational Law, Evolving*, in *Elgar Encyclopedia of Comparative Law* 899, 901–05 (Jan M. Smits ed., 2d ed. 2012).
8. *Montevideo Convention on the Rights and Duties of States* art. 1, Dec. 26, 1933, 49 Stat. 3097, 165 U.N.T.S. 19.
9. *Restatement (Second) of Conflict of Laws* §§ 6, 145, 188 (Am. L. Inst. 1971); see also James Fawcett et al., *International Sale of Goods in the Conflict of Laws* 12–25 (2005).
10. Aaron D. Wright & Primavera De Filippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, SSRN Electronic J. 1, 12–18 (2015); see also Gerald Spindler & Fritjof Börner, *E-Commerce Law in Europe and the USA* 15–28 (2002).
11. Uta Kohl, *Data Law and Foreign Government Access to Data: Multilateral Public Interest Interventions* 45–62 (2021); see also Dan Jerker B. Svantesson, *A "Cross-Border Internet Jurisdiction Protection Treaty" – A Proposal*, 4 J. Internet L. 18, 19–22 (2018).

12. Philip C. Jessup, Transnational Law 1–15 (1956).
13. Terence C. Halliday & Gregory Shaffer, Transnational Legal Orders, in Transnational Legal Orders 1, 11–15 (Terence C. Halliday & Gregory Shaffer eds., 2015); see also Peer Zumbansen, Neither 'Public' nor 'Private', 'National' nor 'International': Transnational Law and Discourse in a European Context, 3 Eur. L.J. 300, 305–10 (2001).
14. Anupam Chander & Uyen P. Le, Data Nationalism, 64 Emory L.J. 677, 680–88 (2015); see also Theodore Christakis, European Digital Sovereignty: Theory and Practice, 12 Cahiers du Numérique 45, 48–55 (2020).
15. Dan Jerker B. Svantesson, Enforcing Privacy Rights Across Borders: The Challenges and the Path Forward, 11 Int'l Data Priv. L. 215, 218–22 (2021).
16. Nicolas Suzor, Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms, 24 Soc. Media + Soc'y 1, 3–8 (2018); see also Giovanni De Gregorio, Digital Constitutionalism in Europe: Reframing Rights and Power in the Algorithmic Society 55–72 (2022).