DIGITAL PUBLIC INFRASTRUCTURE (DPI): EMERGING CHALLENGES AND ISSUES IN INTERNATIONAL FINANCIAL LAW

by

Anupriya S

ABSTRACT

Digital public infrastructure is slowly becoming the base for many financial services. It includes systems such as digital identity, instant payments, and sharing of financial data with consent. These systems help people receive government benefits, make payments, and open bank accounts more easily. But they also bring legal problems, especially when personal data, private companies, and cross-border transactions are involved.

This paper looks at the legal issues connected with digital public infrastructure in international financial law. At present, there is no one international law that covers DPI completely. Payments, data protection, cybersecurity, and digital identity are handled under different laws in different countries. Because of this, companies and users face confusion when a DPI-based service works across borders.

The paper studies India, the European Union, and Brazil. These three examples show that countries are building DPI in different ways, but the law has not developed at the same speed. The paper points out problems such as weak cybersecurity, unclear liability when fraud or system failures happen, digital exclusion of people without documents or smartphones, and differences in data-protection rules. It argues that DPI should be treated as important financial infrastructure and should be regulated more clearly.

Finally, the paper suggests that countries should follow common principles for DPI, improve cooperation between regulators, protect consumer rights, and provide offline or assisted options for people who cannot use digital systems. A balanced legal framework is needed so that DPI can support financial inclusion without putting users at risk.

Keywords: Digital Public Infrastructure; International Financial Law; Digital Identity; Cybersecurity; Financial Inclusion; Cross-Border Payments.

Indian Journal of Law and Jurisprudence | Licensed under Creative Commons — https://creativecommons.org/licenses/by/4.0/ | DOI: 10.5281/zenodo.24466996 | Title: Digital Public Infrastructure (DPI): Emerging Challenges and Issues in International Financial Law

INTRODUCTION

Digital public infrastructure or DPI, is now an important part of modern financial and government systems. It includes digital identity systems, digital payment platforms, data-sharing systems, and public registries. These systems help people, businesses, and governments access services such as banking, welfare payments, taxation, remittances, credit, and online commerce.

DPI is different from normal e-government projects because it works as shared infrastructure. One system can support many public and private services. For example, a digital identity system may be used to open a bank account, receive government benefits, verify a customer, or access online services.

The growth of DPI has created new legal issues in international financial law. Traditional financial laws were mainly made for banks, payment companies, securities markets, and national regulators. DPI brings together governments, private technology companies, banks, and large amounts of personal data. This creates questions about licensing, consumer protection, fraud, system failure, cybersecurity, data privacy, cross-border data transfer, and financial exclusion.

Cross-border payments show these problems clearly. DPI-based payment systems can make payments faster and cheaper, but they need common technical standards and cooperation between regulators. At present, there is no complete global system to regulate all cross-border payment providers. Data-protection laws also differ between countries, which creates uncertainty for DPI systems that handle identity and financial data across borders.

This article studies DPI as an emerging issue in international financial law. It examines digital identity, interoperable payments, and data-sharing systems. It focuses on privacy, cybersecurity, financial integrity, financial inclusion, and accountability between public and private actors. The article compares India, the European Union, and Brazil. It argues that DPI should be treated as critical financial infrastructure and should be governed through clear rules on interoperability, privacy, security, accountability, and inclusive access.

IJLJ ISSN: 2583-2794

CONCEPT OF DIGITAL PUBLIC INFRASTRUCTURE (DPI)

Digital public infrastructure (DPI) means the basic digital systems that a country uses to provide public and private services safely and at a large scale. It is not a single technology or application. Instead, it is a foundation on which many services can be built.[1]

[1] World Bank Grp., Digital Public Infrastructure and Services, https://www.worldbank.org/ext/en/topic/digital-and-ai/digital-public-infrastructure-and-services

DPI usually includes three main parts: digital identity, digital payments, and data-sharing systems. A digital identity system helps a person prove who they are online. A digital payment system allows money to be sent and received quickly between individuals, businesses, and the government. A data-sharing system allows authorised institutions to exchange information with the consent of the person concerned.[2]

The main purpose of DPI is to make services accessible, secure, and interoperable. "Accessible" means that people should be able to use the system, including those with limited digital skills or resources. "Secure" means that personal and financial data must be protected from misuse, fraud, and cyberattacks. "Interoperable" means that different systems, banks, government departments, and service providers should be able to work together.

DPI is different from ordinary e-government projects. An e-government project may serve only one department or one service, such as applying for a certificate online. DPI, however, supports many services at the same time. For example, a digital identity system may be used to open a bank account, receive welfare benefits, verify a customer, file taxes, or access healthcare services. In financial law, DPI is important because it affects access to money and financial services. It can improve financial inclusion by helping people open accounts, receive government transfers, and make digital payments. At the same time, it raises legal concerns about privacy, cybersecurity, data protection, fraud, liability, consumer rights, and cross-border regulation.

Therefore, DPI should be understood as critical infrastructure. It is not only a technological tool but also a legal and institutional system that affects financial inclusion, data protection, financial stability, and public trust.[3]

INDIA'S PATH TO DIGITAL PUBLIC INFRASTRUCTURE

Key reforms and initiatives | 2000–2024

This timeline presents selected milestones that helped build India's digital public infrastructure (DPI). It distinguishes between the creation of a regulatory framework and the later operational rollout of a system.

[2] United Nations Development Programme (UNDP), Digital Public Infrastructure, https://www.undp.org/digital/digital-public-infrastructure

[3] World Bank Grp., Global Digital Public Infrastructure Program (May 6, 2026), https://www.worldbank.org/en/results/2026/05/06/global-digital-public-infrastructure-program.

2000–2010	**FOUNDATIONS OF ELECTRONIC BANKING** • Internet and electronic banking expanded, supported by banking and information-technology regulation. • Aadhaar was launched in 2009, beginning the development of a national digital identity system. *Accuracy notes: Use broad wording for this period unless citing a particular banking rule or launch date.*
2011–2015	**DIGITAL IDENTITY AND INCLUSION** • Aadhaar enrolment and use expanded. • Pradhan Mantri Jan-Dhan Yojana (PMJDY) launched on 28 August 2014 to expand access to bank accounts. • Digi Locker launched on 1 July 2015, enabling digital issuance and access to documents. *Accuracy notes: These are distinct milestones; PMJDY is a financial-inclusion programme, while Aadhaar and Digi Locker provide identity/document infrastructure.*
2016–2018	**DIGITAL PAYMENTS AND PUBLIC SERVICES** • RBI issued the Account Aggregator Directions on 2 September 2016 (the framework came later into operational use). • UPI was launched in 2016; BHIM followed in December 2016. • UMANG was launched in 2017 to provide access to multiple government services through one platform. *Accuracy notes: Do not describe the Account Aggregator ecosystem as fully operational in 2016; its official launch was in September 2021.*
2019–2020	**PAYMENT REGULATION AND EMERGENCY DIGITAL SERVICES** • RBI issued Guidelines on Regulation of Payment Aggregators and Payment Gateways on 17 March 2020. • Aarogya Setu was launched in April 2020 during the COVID-19 pandemic. *Accuracy notes: The payment-aggregator framework was developed through RBI's 2019 discussion process and 2020 guidelines.*
2021–2022	**CONSENT-BASED DATA SHARING AND OPEN NETWORKS** • The Account Aggregator ecosystem was officially launched on 2 September 2021, enabling consent-based financial-data sharing. • ONDC was registered as a Section 8 company in December 2021; its first order was recorded on 29 April 2022. *Accuracy notes: ONDC is an open network for digital commerce; it should not be described as a payment regulator.*
2022–2024	**STRONGER DIGITAL FINANCE SAFEGUARDS** • RBI issued its Digital Lending Guidelines on 2 September 2022. • In 2023, RBI provided for operation of pre-sanctioned credit lines at banks through UPI. • RBI issued the Payment Aggregator–Cross Border framework on 31 October 2023. • In August 2024, RBI announced a public repository of digital lending apps reported by regulated entities. *Accuracy notes: These milestones concern consumer protection, credit access and cross-border payment regulation; they are not all new DPI platforms.*

CONTEMPORARY LEGAL AND REGULATORY CHALLENGES IN DIGITAL PUBLIC INFRASTRUCTURE

The rapid development of digital public infrastructure has created several emerging issues in international financial law. These issues arise because DPI combines technology, public administration, private companies, financial services, and large-scale personal data processing.

1. Regulatory fragmentation

Financial laws are mostly made and enforced within individual countries. However, DPI-based services, especially digital payments and identity verification, often operate across borders. This creates uncertainty about which country's law applies, which regulator has authority, and how disputes should be resolved. Different licensing rules, consumer-protection standards, and supervisory practices can also lead to regulatory gaps.[4]

2. Cross-border payments

DPI can make cross-border payments faster, cheaper, and more transparent. However, interoperability between payment systems is difficult because countries use different technical standards, legal rules, and supervisory systems. Issues such as payment finality, fraud prevention, currency conversion, dispute resolution, and access for foreign payment providers remain unsettled.[5]

3. Data protection and privacy

DPI depends on the collection and processing of personal, financial, and identity data. This raises concerns about consent, purpose limitation, data security, and the right to correction or deletion. When data crosses borders, different data-protection laws may apply. This creates uncertainty for financial institutions, technology providers, and users.[6]

IJLJ ISSN: 2583-2794

4. Data sovereignty

Many countries want control over data generated within their territory. They may require data to be stored locally or restrict its transfer abroad. While such rules may protect national

[4] World Bank Grp., Digital Public Infrastructure and Services, https://www.worldbank.org/ext/en/topic/digital-and-ai/digital-public-infrastructure-and-services

[5] Comm. on Payments & Mkt. Infrastructures, Bank for Int'l Settlements, CPMI Cross-border Payments Programme, https://www.bis.org/committees/cpmi/cross-border-payments/overview

[6] World Bank Grp., Trust by Design: Securing Digital Development (June 9, 2026), https://www.worldbank.org/en/results/2026/06/09/trust-by-design-securing-digital-development.

security and privacy, they can also affect cloud-based financial services, fraud monitoring, payment processing, and international supervisory cooperation.

5. Cybersecurity and systemic risk

As DPI becomes essential for payments, identity verification, and government benefits, cyberattacks or technical failures can have serious consequences. A failure in a major payment system or identity database may affect millions of users and disrupt financial services. This makes cybersecurity, incident reporting, business continuity, and resilience important legal issues.

6. Financial integrity and inclusion

DPI can support anti-money-laundering and know-your-customer requirements by improving identity verification. However, strict digital identity requirements may exclude people who do not have documents, smartphones, internet access, or digital literacy. Financial law must therefore balance crime prevention with the right to access basic financial services.[7]

7. Liability and accountability

It is often unclear who is responsible when a DPI-based service fails. Liability may involve the government, identity authority, payment operator, bank, fintech company, technology vendor, or merchant. Clear rules are needed for fraud, unauthorised transactions, data breaches, service outages, and consumer compensation.

8. Public-private governance

DPI is often built and operated through cooperation between governments and private companies. This raises questions about procurement transparency, vendor lock-in, intellectual property, audit rights, data access, and public control over essential services. The state should remain accountable for critical public functions, even where private companies provide technical services.

9. Interoperability and dependence

Interoperability is necessary for DPI to work across institutions and borders. However, countries that depend on foreign platforms, standards, or technology providers may face risks

[7] Financial Action Task Force, Guidance on Digital Identity 8–10 (2020), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity-report.pdf.**

of digital dependence. This can affect national autonomy, competition, and equal participation in global standard-setting.

BRIDGING BORDERS: THE INTERNATIONAL FRAMEWORK FOR DIGITAL PUBLIC INFRASTRUCTURE

No comprehensive international treaty presently regulates digital public infrastructure in its entirety. Rather, DPI is governed through a fragmented combination of international institutions, non-binding standards, regional instruments, and domestic legislation. While this framework encourages international cooperation, it also produces regulatory inconsistency and gaps in governance.

1. Bank for International Settlements and CPMI

The Bank for International Settlements (BIS), through the Committee on Payments and Market Infrastructures (CPMI), plays an important role in payment-system regulation. It develops principles for payment, clearing, and settlement systems and works on improving cross-border payments.[8]The CPMI focuses on issues such as payment-system access, interoperability, data exchange, and standardisation. Its work is relevant to DPI because digital payment infrastructure must be safe, efficient, and accessible. However, its standards are mainly directed at payment systems and financial market infrastructures; they do not provide a complete legal framework for digital identity or data-sharing systems.

2. Financial Stability Board

The Financial Stability Board (FSB) works to promote international financial stability. It examines risks arising from new financial technologies, including digital payments, crypto-assets, and cross-border payment arrangements. The FSB has supported the G20 roadmap for enhancing cross-border payments. This roadmap addresses problems such as high cost, slow speed, limited access, and lack of transparency. These issues are directly relevant to DPI-based payment systems. However, the FSB's work is mainly policy-oriented and does not itself create binding obligations for states.

[8] Comm. on Payments & Mkt. Infrastructures & Technical Comm. of the Int'l Org. of Sec. Comm'ns, Principles for Financial Market Infrastructures (Apr. 2012), https://www.bis.org/publ/cpmi101a.pdf.

3. Financial Action Task Force

The Financial Action Task Force (FATF) sets global standards for anti-money laundering (AML) and counter-terrorist financing (CTF). Its rules require financial institutions to identify customers, monitor transactions, and report suspicious activity.[9]DPI can support these requirements through digital identity and electronic KYC systems. However, FATF standards also create challenges for inclusion. If identity verification is too strict or digital-only, persons without documents, mobile phones, or internet access may be excluded from financial services. Therefore, DPI must support risk-based and proportionate compliance.

4. International Monetary Fund

The International Monetary Fund (IMF) provides policy advice and technical assistance on financial stability, digital money, payment systems, and financial integrity. Its work on fintech, digital currencies, and DPI highlights the need for sound legal frameworks, consumer protection, data governance, and cybersecurity.[10]The IMF recognises that digital financial services must be safe, legally anchored, and supportive of financial integrity. Its work is important for DPI because it connects technological development with monetary stability, financial supervision, and development needs.

5. World Bank

The World Bank supports DPI as a tool for development and financial inclusion. It describes DPI as foundational digital building blocks designed for public benefit, especially digital identity, payments, and data exchange.[11]The World Bank focuses on access, interoperability, inclusion, and responsible implementation. Its work is useful for understanding how DPI can support development goals. However, like other international guidance, it does not create directly enforceable international legal obligations.

6. OECD

The Organisation for Economic Co-operation and Development (OECD) has developed guidance on digital government, data governance, privacy, and digital public infrastructure.

[9] Fin. Action Task Force, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations (2012, as amended), https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.

[10] Tobias Adrian & Tommaso Mancini-Griffoli, The Rise of Digital Money, IMF FinTech Notes No. 2019/001 (July 2019), https://www.imf.org/en/Publications/fintech-notes/Issues/2019/07/15/The-Rise-of-Digital-Money-47096.

[11] World Bank Grp., Digital Public Infrastructure and Services, https://www.worldbank.org/ext/en/topic/digital-and-ai/digital-public-infrastructure-and-services

The OECD defines DPI as shared, secure, and interoperable digital systems that support access to public and private services.[12]The OECD also promotes interoperability between privacy and data-protection frameworks. This is important because DPI systems often process personal and financial data across borders. However, OECD instruments are generally recommendations rather than binding treaties.

7. Regional and national frameworks

Regional systems also influence DPI. The European Union has developed detailed rules on digital identity, payments, data protection, and cybersecurity. These include the GDPR, PSD2, the Instant Payments Regulation, and the European Digital Identity Wallet framework. Other countries and regions are developing their own DPI systems.[13] India has developed Aadhaar, UPI, and the Account Aggregator framework. Brazil has developed Pix under the supervision of the Banco Central do Brasil. These national systems show that DPI is developing faster than international law.

CASE STUDIES: INDIA, THE EUROPEAN UNION, AND BRAZIL

India, the European Union, and Brazil represent three distinct legal and institutional approaches to digital public infrastructure. India has developed large-scale digital identity and payment systems; the European Union follows a rights-based and regionally harmonised regulatory model; and Brazil has established a central-bank-led public payment infrastructure.

1. India: Aadhaar, UPI, and the DPDP Act

India is an important case study because it has developed DPI at a very large scale. Its main systems include Aadhaar for digital identity, the Unified Payments Interface (UPI) for interoperable digital payments, and the Account Aggregator framework for consent-based financial data sharing.[14]

Aadhaar provides a unique identity number and biometric authentication. It is used for welfare transfers, subsidies, tax administration, and financial verification. UPI allows instant payments between different banks and payment service providers. These systems have helped

[12] Org. for Econ. Coop. & Dev. (OECD), Digital Public Infrastructure for Digital Governments 5–7 (2024), https://www.oecd.org/en/publications/digital-public-infrastructure-for-digital-governments_ff525dc8-en.html.
[13] Unique Identification Auth. of India, Aadhaar, https://uidai.gov.in (last visited Nov. 17, 2026); Nat'l Payments Corp. of India, Unified Payments Interface (UPI), https://www.npci.org.in/what-we-do/upi
[14] The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, No. 18 of 2016, India Code (2016); Nat'l Payments Corp. of India, Unified Payments Interface (UPI), https://www.npci.org.in/what-we-do/upi

expand digital financial services, but they also raise concerns about exclusion, consent, data protection, fraud, and liability.[15]

India's Digital Personal Data Protection Act, 2023 is relevant because it governs the processing of digital personal data. It recognises the importance of individual rights, lawful processing, consent, data security, and accountability. However, questions remain about how these rules apply to financial data sharing, cross-border transfers, and government access to data.[16]

Legal issues to discuss:

1. Whether Aadhaar-based KYC excludes persons without valid documents.
2. Whether UPI provides adequate protection against fraud and unauthorised transactions.
3. How liability is divided among banks, payment service providers, NPCI, merchants, and users.
4. Whether India's data-protection framework is sufficient for cross-border DPI.

2. European Union: Digital Identity Wallet, PSD2, and GDPR

The European Union provides a rights-based and regulation-heavy model. Its key instruments include the General Data Protection Regulation (GDPR), the Payment Services Directive 2 (PSD2), the Instant Payments Regulation, and the European Digital Identity Wallet framework.[17]

The EU Digital Identity Wallet is intended to allow citizens to prove their identity and share selected personal information with public and private service providers. It can also be used for payment authentication. The EU approach gives importance to user control, data minimisation, security, and interoperability across Member States.[18]

The GDPR protects personal data and sets rules on lawful processing, consent, data subject rights, security, and cross-border data transfers. PSD2 regulates payment services and promotes open banking through access to payment account information. The Instant Payments Regulation seeks to remove barriers to instant euro credit transfers.[19]

[15] Reserve Bank of India, Master Direction on Digital Payment Security Controls (Feb. 18, 2021), https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032.
[16] The Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[17] Regulation (EU) 2016/679 (GDPR), 2016 O.J. (L 119) 1; Directive (EU) 2015/2366 (PSD2), 2015 O.J. (L 337) 35; Regulation (EU) 2024/886 (Instant Payments Regulation), 2024 O.J. (L 2024/886).
[18] Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 Apr. 2024 Amending Regulation (EU) No. 910/2014 as Regards Establishing the European Digital Identity Framework, 2024 O.J. (L 2024/1183)
[19] Regulation (EU) 2016/679, supra note 4; Directive (EU) 2015/2366, supra note 4; Regulation (EU) 2024/886, supra note 4.

Legal issues to discuss:

- Whether the Digital Identity Wallet can meet AML and KYC requirements without excessive data sharing.
- How GDPR interacts with payment fraud monitoring and law-enforcement access.
- Whether the EU model can be adopted by countries with weaker digital infrastructure.
- How the EU balances privacy rights with financial integrity and innovation.

3. Brazil: Pix, Banco Central do Brasil, and LGPD

Brazil is a strong example of central-bank-led DPI. Its instant payment system, Pix, was created and regulated by the Banco Central do Brasil. Pix allow individuals, businesses, and government bodies to make instant payments using identifiers such as mobile numbers, e-mail addresses, or random keys.[20]

Pix is important because participation is mandatory for many authorised financial institutions and payment institutions. This has supported rapid adoption and financial inclusion. However, mandatory participation also raises questions about market concentration, operational risk, cybersecurity, and the central bank's role as both regulator and operator. Brazil's General Data Protection Law, known as the LGPD, protects personal data and applies to digital data processing. It works alongside banking secrecy rules and central-bank supervision. The Brazilian model therefore combines public control over payment infrastructure with data-protection safeguards.

THE GOVERNANCE DEFICIT IN DIGITAL PUBLIC INFRASTRUCTURE

The existing legal and regulatory framework for digital public infrastructure is incomplete and fragmented. Although international organisations have developed guidance on payments, data protection, financial integrity, and digital governance, there is no single international framework that deals with DPI as a whole. This creates uncertainty for governments, financial institutions, technology providers, and users.

IJLJ ISSN: 2583-2794

1. Absence of a unified international DPI framework

There is no comprehensive international treaty or global regulatory body exclusively responsible for DPI. Payment systems are addressed by institutions such as the BIS, CPMI,

[20] Banco Central do Brasil, Resolution BCB No. 1 of Aug. 12, 2020, https://www.bcb.gov.br/content/estabilidadefinanceira/pix/Pix_Regulation/Resolution_BCB_1.pdf

FSB, and FATF. Data protection is mainly governed by national laws and regional instruments. Digital identity is regulated mostly at the national or regional level.[21]

Because of this division, DPI systems that combine identity, payments, and data sharing are not governed in a coordinated manner. A system may comply with payment rules in one country but face uncertainty under data-protection, cybersecurity, or consumer-protection laws in another.

2. Incomplete regulation of cross-border payment providers

Cross-border payment services are increasingly provided by non-bank entities, fintech companies, and DPI-based platforms. However, supervisory rules for such providers are not uniform across jurisdictions. Some countries impose licensing, capital, governance, and reporting requirements, while others have less developed systems.[22]

This creates regulatory arbitrage, where providers may operate in jurisdictions with weaker supervision. It also creates difficulties in consumer protection, fraud prevention, and cross-border enforcement.

3. Lack of harmonised data-protection rules

DPI depends on the processing of identity, financial, and transactional data. However, data-protection laws differ across countries in relation to consent, data localisation, cross-border transfer, breach notification, retention, and enforcement.

These differences create uncertainty for DPI systems that operate across borders. A payment or identity system may be lawful in one jurisdiction but face restrictions in another. The absence of interoperable privacy frameworks also makes international cooperation difficult.

4. Unclear rules on data sovereignty and cross-border data flows

Many countries impose data-localisation or data-residency requirements. These rules may be intended to protect national security, privacy, and regulatory oversight. However, they can restrict cloud-based financial services, real-time payment processing, fraud monitoring, and international supervisory cooperation.[23]

[21] World Bank Grp., Digital Public Infrastructure and Services, https://www.worldbank.org/ext/en/topic/digital-and-ai/digital-public-infrastructure-and-services

[22] Fin. Stability Bd., G20 Roadmap for Enhancing Cross-Border Payments: Priority Actions for Achieving the G20 Targets 8–12 (Feb. 23, 2023), https://www.fsb.org/uploads/P230223.pdf.

[23] Org. for Econ. Coop. & Dev. (OECD), Digital Public Infrastructure for Digital Governments 9–14 (2024), https://www.oecd.org/en/publications/digital-public-infrastructure-for-digital-governments_ff525dc8-en.html.

The existing framework does not clearly balance data sovereignty with the need for cross-border data flows in financial services. This creates legal uncertainty for DPI operators and financial institutions.

5. Weak cybersecurity and resilience standards

DPI systems are critical infrastructure because they support payments, identity verification, welfare transfers, and access to financial services. A cyberattack, data breach, or technical failure can affect millions of users.

However, cybersecurity and resilience requirements are not uniform across countries. There is no comprehensive international framework requiring DPI operators to follow common standards for incident reporting, business continuity, system testing, third-party risk management, and recovery after failure.

6. Insufficient protection against digital exclusion

DPI can improve financial inclusion, but it can also exclude persons who do not have identity documents, smartphones, internet access, digital literacy, or stable residence. Strict digital KYC and identity-verification rules may prevent vulnerable groups from accessing banking, welfare benefits, and payment services.

The existing framework does not sufficiently require offline alternatives, grievance mechanisms, non-discrimination safeguards, or assisted access for persons unable to use digital systems.

7. Unclear liability and consumer redress

It is often unclear who is legally responsible when a DPI-based service fails. Liability may involve the government, identity authority, payment operator, bank, fintech company, technology vendor, merchant, or user.[24]

For example, in cases of unauthorised transactions, identity fraud, data breaches, or payment failures, consumers may not know whom to approach for compensation. The absence of clear liability rules weakens trust in DPI and reduces effective consumer protection.

[24] Comm. on Payments & Mkt. Infrastructures, Bank for Int'l Settlements, Expanding Access to Payment Systems: Considerations for a Path Forward 12–16 (Feb. 2026), https://www.bis.org/pages/cpmi-cross-border-payments-programme/pietf-payment-systems-feb-2026.pdf.

8. Limited governance of public-private partnerships

DPI is often developed through cooperation between governments and private technology companies. This raises concerns about procurement transparency, vendor lock-in, intellectual property rights, data access, audit rights, and long-term public control.

Existing legal frameworks do not always clearly define the responsibilities of public authorities and private providers. This can weaken accountability, especially where a private company operates critical public infrastructure.

9. Limited participation of developing countries

International standards for payments, data, cybersecurity, and digital identity are often developed by advanced economies and international institutions. Developing countries may lack technical capacity, negotiating power, or resources to participate fully in standard-setting.[25]This can lead to digital dependence, where countries adopt foreign systems or standards without adequate local adaptation. It may also affect competition, national autonomy, and equitable access to global financial infrastructure.

FROM FRAGMENTATION TO COHERENCE: A NEW LEGAL FRAMEWORK FOR DIGITAL PUBLIC INFRASTRUCTURE

The existing framework for digital public infrastructure is fragmented because payment law, data-protection law, cybersecurity law, consumer law, and financial regulation are dealt with separately. A better approach is not to create one global regulator for DPI, but to develop a coordinated framework based on common principles, cooperation between regulators, and enforceable national implementation.

1. Recognition of DPI as critical financial infrastructure

States should recognise DPI systems as critical financial infrastructure when they support essential services such as digital identity, payments, welfare transfers, financial data sharing, or access to banking.

This recognition would require DPI operators to meet higher standards for security, continuity, risk management, audit, and incident reporting. It would also allow regulators to supervise DPI systems in a manner similar to other important financial market infrastructures.

[25] World Bank, Digital Public Infrastructure 5–8 (2025), https://openknowledge.worldbank.org/server/api/core/bitstreams/582c0d73-d367-423c-831d-0640814a7349/content.

2. A coordinated international DPI framework

International organisations such as the BIS, IMF, World Bank, OECD, FATF, and FSB should coordinate their work on DPI. They should develop common principles rather than separate and inconsistent guidance.[26]

These principles should cover digital identity, interoperable payments, data sharing, cybersecurity, consumer protection, financial integrity, and cross-border cooperation. The framework should be flexible enough to respect national legal systems and development priorities.

3. Interoperability by design

DPI systems should be interoperable by design. This means that different banks, payment providers, government departments, and private service providers should be able to connect with the system through open and secure standards.[27]

Interoperability should include:

- Common technical standards for payments and identity verification.
- Secure application programming interfaces, or APIs.
- Portability of customer data with proper consent.
- Fair and non-discriminatory access for authorised service providers.
- Avoidance of vendor lock-in and excessive dependence on one provider

4. Privacy-by-design and data protection

DPI should follow the principle of privacy-by-design. Privacy and security protections should be built into the system from the beginning, not added later.[28]

The framework should require:

- Lawful and transparent processing of personal data.
- Clear and informed consent where required.
- Purpose limitation and data minimisation.
- Strong encryption and access controls.
- Data accuracy and correction rights.
- Independent oversight and effective remedies for data breaches.

[26] Fin. Stability Bd., G20 Roadmap for Enhancing Cross-Border Payments: Priority Actions for Achieving the G20 Targets (Feb. 2023), https://www.fsb.org/uploads/P230223.pdf.
[27] Org. for Econ. Coop. & Dev. (OECD), Digital Public Infrastructure for Digital Governments 10–14 (2024), https://www.oecd.org/en/publications/digital-public-infrastructure-for-digital-governments_ff525dc8-en.html.
[28] Regulation (EU) 2016/679 (General Data Protection Regulation), 2016 O.J. (L 119) 1, arts. 5, 25.

5. Risk-based financial integrity

Anti-money-laundering and know-your-customer rules should remain important, but they should be applied in a risk-based manner. This means that stricter checks should be applied where the risk of money laundering or terrorist financing is higher, while low-risk services should not be burdened with excessive requirements. The framework should support tiered KYC, electronic verification, and alternative methods of identity proof. This will help prevent digital exclusion while maintaining financial integrity.[29]

6. Clear liability and consumer protection

The law should clearly allocate responsibility among DPI operators, banks, payment service providers, technology vendors, merchants, and users. Consumers should know whom to approach when fraud, unauthorised transactions, data breaches, or system failures occur.[30]

The framework should provide: -

- Clear rules on liability for unauthorised transactions.
- Time-bound complaint and refund procedures.
- Compensation for losses caused by system failure or negligence.
- Access to dispute-resolution mechanisms.
- Special protection for vulnerable users.

7. Cybersecurity and resilience obligations

DPI operators should be required to maintain strong cybersecurity and operational resilience. They should conduct regular risk assessments, penetration testing, and system audits.[31]

The framework should require:

- Incident reporting to regulators.
- Business-continuity and disaster-recovery plans.
- Protection against cyberattacks and data breaches.
- Supervision of third-party technology providers.
- Regular stress testing of critical systems.

[29] Fin. Action Task Force, Guidance on Digital Identity 8–10 (2020), https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-on-Digital-Identity-report.pdf.

[30] Comm. on Payments & Mkt. Infrastructures, Bank for Int'l Settlements, Expanding Access to Payment Systems: Considerations for a Path Forward 12–16 (Feb. 2026), https://www.bis.org/pages/cpmi-cross-border-payments-programme/pietf-payment-systems-feb-2026.pdf.

[31] Reserve Bank of India, Master Direction on Digital Payment Security Controls (Feb. 18, 2021), https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032.

8. Accountable public-private governance

Where DPI is built or operated with private companies, the state should retain ultimate responsibility for essential public functions. Private providers may supply technology or operational services, but public authorities must ensure transparency, accountability, and public interest.

The framework should require:

- Transparent procurement processes.
- Clear contracts with private vendors.
- Audit rights for regulators.
- Data-access rights for supervision.
- Limits on vendor lock-in.
- Public accountability for service failures.

9. Cross-border cooperation

Because DPI-based payments and data flows often cross borders, countries should improve regulatory cooperation. Regulators should share information, coordinate supervision, and respond jointly to cyber incidents and fraud.

The framework should encourage:

- Mutual recognition of trusted digital identity systems.
- Cooperation between financial supervisors.
- Compatible data-protection standards.
- Cross-border incident-notification arrangements.
- International cooperation against fraud and money laundering.

10. Inclusive access and human oversight

DPI should not become a condition for accessing basic financial services. The framework should require inclusive design and alternative access channels for persons who cannot use digital systems.

This includes:

- Offline or assisted service options.
- Simple user interfaces and local-language support.
- Grievance redress mechanisms.
- Protection against discrimination.

- Human review in decisions that seriously affect rights or access to services.

CONCLUSION

Digital public infrastructure has gradually become a key part of financial and governmental systems. It provides the basic digital foundation for identity verification, payments, data sharing, welfare transfers, and access to financial services. If designed properly, DPI can help more people participate in the formal economy, lower the cost of transactions, and make public services easier to access. At the same time, DPI raises difficult legal questions. Financial regulation developed mainly to deal with banks, payment companies, securities markets, and national supervisors. DPI does not fit neatly within these categories because it involves governments, private technology firms, financial institutions, and large volumes of personal data. As a result, issues such as licensing, fraud, consumer protection, liability, cybersecurity, data sovereignty, and cross-border data transfers remain uncertain.

The experiences of India, the European Union, and Brazil demonstrate that DPI can be organised in different ways. India has built identity and payment systems on a very large scale. The European Union has focused on harmonised rules and strong protection of individual rights. Brazil has placed its instant payment system under the direct control of the central bank. These models show that there is no universal approach to DPI, but each offers lessons for other countries.

The central weakness of the present system is fragmentation rather than the total absence of rules. Payments, data protection, cybersecurity, digital identity, and consumer rights are regulated separately across different laws and institutions. This approach is inadequate for DPI, which often operates across borders and supports several financial services at the same time.

DPI should therefore be treated as critical financial infrastructure. Countries and international bodies should work towards a common framework based on interoperability, privacy-by-design, proportionate financial-integrity rules, cybersecurity, clear allocation of liability, accountable public-private governance, and inclusive access. Such a framework should guide national laws rather than replace them.

Ultimately, DPI can support financial inclusion and better public services, but only if law keeps pace with technology. A balanced approach is necessary so that innovation and access are not achieved at the cost of privacy, security, consumer rights, and public confidence.

IJLJ ISSN: 2583-2794