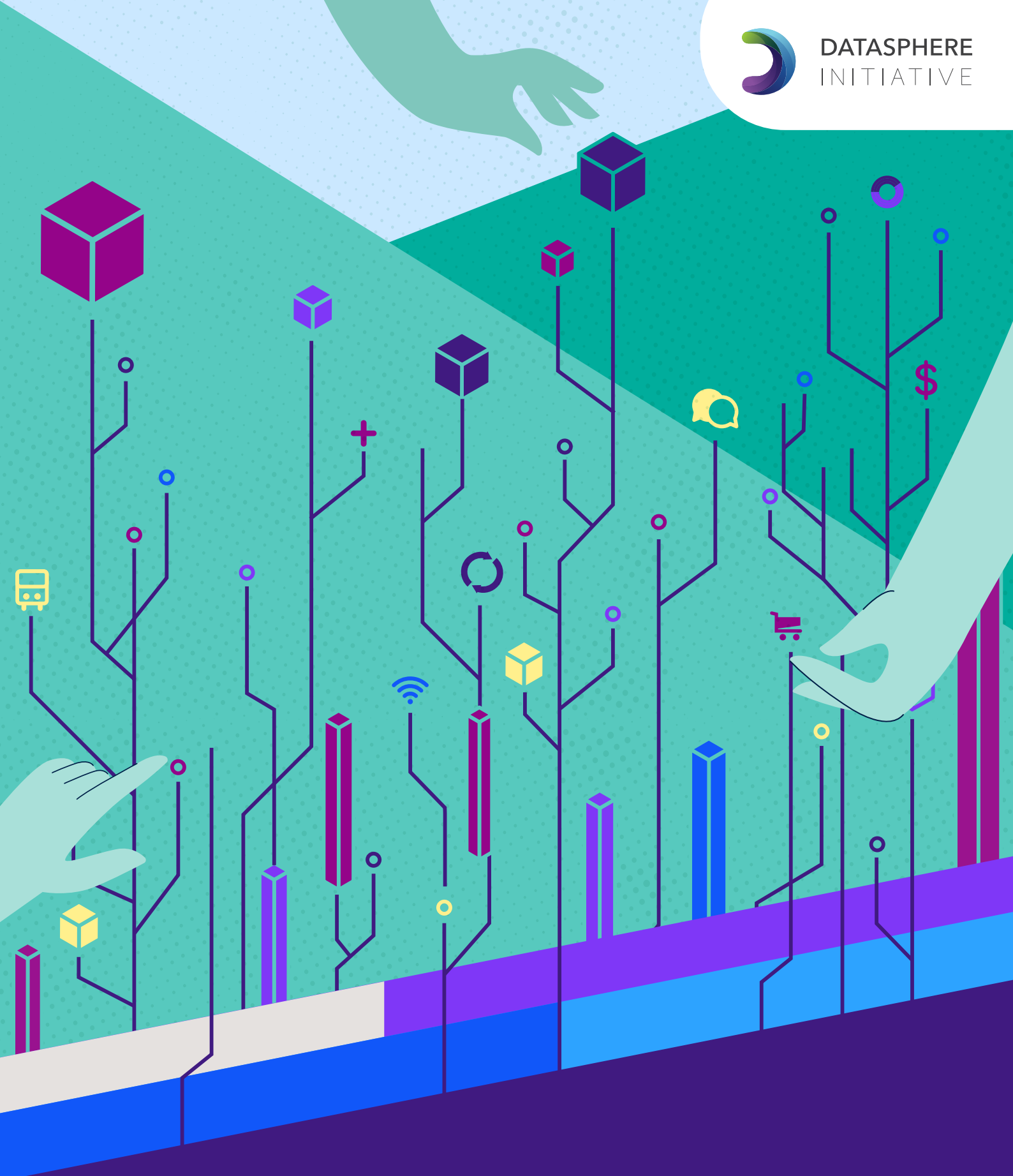
DATASPHERE INITIATIVE



Sandboxes for DPI

Co-creating the blocks of digital trust

About the Datasphere Initiative

The Datasphere Initiative is a think and do tank that catalyzes meaningful dialogues and co-creates actionable and innovative approaches to respond to data challenges and harness opportunities across borders. Our mission is to equip organizations to responsibly unlock the value of data for all. For more information, visit www.thedatasphere.org or contact info@thedatasphere.org.

About this report

This report was first developed as a working paper presented at the Global Sandbox Forum Inaugural Meeting in July 2024 and then further developed in an online roundtable in December 2025 and through individual consultations with experts. This report summarizes the findings of a study on sandboxes in the field of Digital Public Infrastructure — those that have been announced, are in development, or have been completed. The study aims to identify patterns across the examples analyzed, focusing on the reasons behind their creation.

Table of contents

Acknowledgements

When preparing this report, the Datasphere Initiative team held consultations with various stakeholders in the form of in-person and online meetings. The report has however been drafted under the sole responsibility of the Datasphere Initiative and does not engage the actors listed. The Datasphere Initiative is thankful to all those who shared their expertise and experience which helped the production of the report.

Datasphere Initiative team: **Lorrayne Porciuncula**, Executive Director, **Sophie Tomlinson**, Director of Programs, **Maria Marinho**, Director of Research, **Mariana Rozo-Paz**, Policy, Research and Project Management Lead, **Morine Amutorine**, Lead Africa Sandboxes Forum, **Risper Onyango**, Research Associate, **Thiago Guimaraes Moraes**, Senior Fellow, Datasphere Initiative.

Contributors in their personal capacity: **Carolyn Nguyen**, Board Member, Datasphere Initiative, **Martin Hullin**, Board member, Datasphere Initiative, **Astha Kapoor**, Co-founder and Director at Aapti Institute, **Verena Kontschieder**, Co-CEO Opendata.ch, Program Lead Prototype Fund Switzerland, **Jonathan Middleton**, Director Financial Services, NayaOne, and **Yasodara Córdova**, Deputy Director at Dataprev.

The report counted with editorial and design support from **Maíra Carvalho**, Communications Lead, **Nicholas Field**, Director Operations and Development, and **Barbara Miranda**, Design Thinking Lead of the Datasphere Initiative.

Executive Summary

As governments invest in foundational digital systems that shape how people identify themselves, access services, move money, and share information, a recurring question is how to build Digital Public Infrastructure (DPI) responsibly. **This report explores how sandbox approaches are being applied to DPI, and how they can support more inclusive, accountable, and adaptive DPI development.**

By mapping emerging practices and examining the rationales, opportunities, and limitations of sandboxes, this analysis seeks to contribute to a more grounded understanding of how experimentation can be used to manage risk, build institutional capacity, and strengthen trust in DPI initiatives.

Both DPI and sandboxes are still nascent and fast-evolving fields and little systematic work has been done to explore where these two worlds intersect. How can sandbox approaches support the design, governance, and implementation of DPI? What kinds of sandboxes are emerging around identity, payments, and data exchange? And what can early experiments tell us about building digital public systems that are inclusive, accountable, and resilient?

Digital Public Infrastructure is an emerging policy and practice domain focused on society-wide digital capabilities that are essential to participation in modern economic and social life. These foundational systems - most commonly digital identity, digital payments, and data exchange - sit beneath countless public and private services. Once deployed, they are difficult to reverse. Their design and development choices therefore carry unusually high stakes: they can expand inclusion and resilience at scale, or entrench exclusion, surveillance, and institutional mistrust just as deeply.

At the same time, governments are increasingly turning to sandboxes as experimentation tools for navigating uncertainty in the face of rapid technological change. **Sandboxes** are controlled learning environments designed for structured experimentation under defined governance frameworks, timeframes, and built-in safeguards to support iterative, multi-actor collaboration and evidence-based decision-making. While sandboxes have become more common in areas such as financial regulation, data governance, and AI, their application to DPI remains limited and poorly understood.

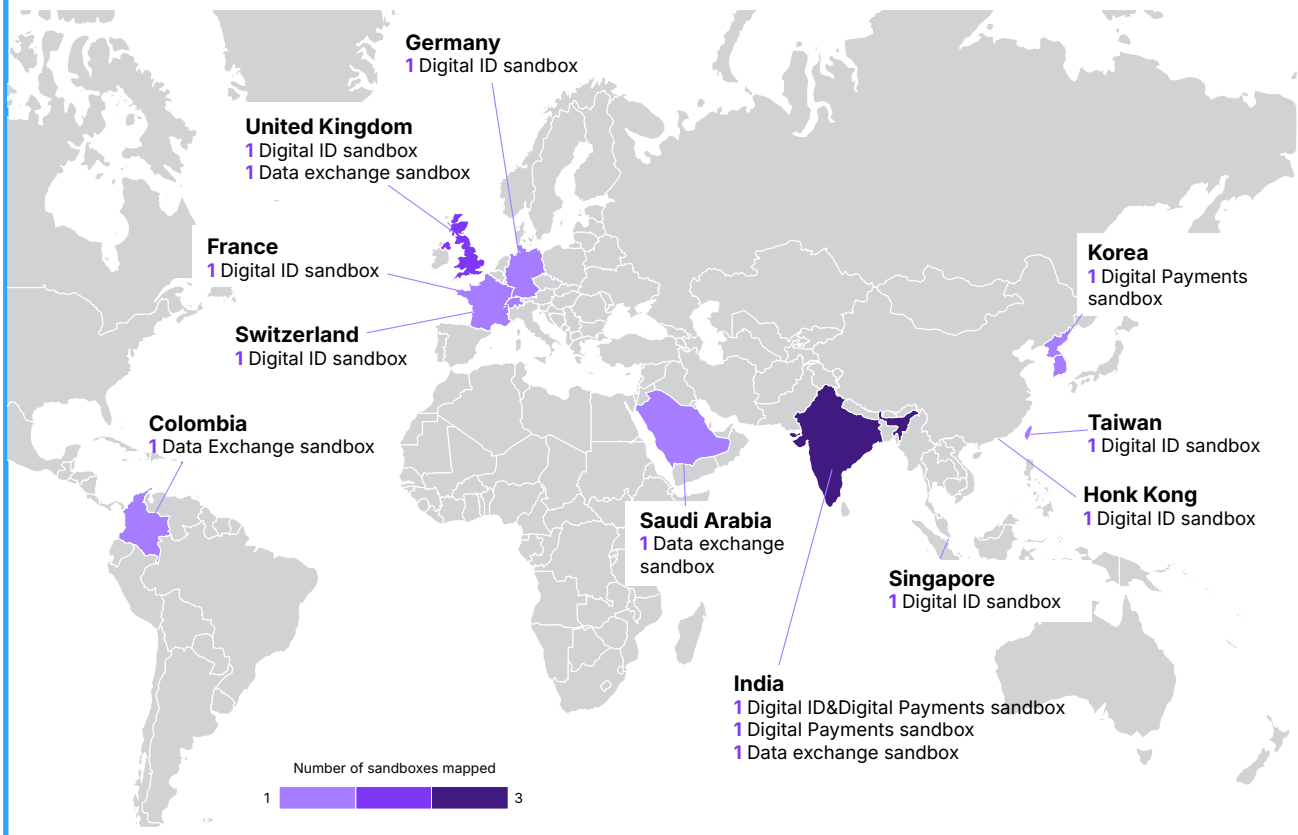
This report represents a first effort to examine that intersection. It investigates how governments are using experimentation in the context of DPI, maps sandboxes across countries, and distills early lessons on how structured experimentation can help move DPI development from hype-driven deployment toward evidence-based and trust-building systems.

A Global Snapshot of DPI Experimentation

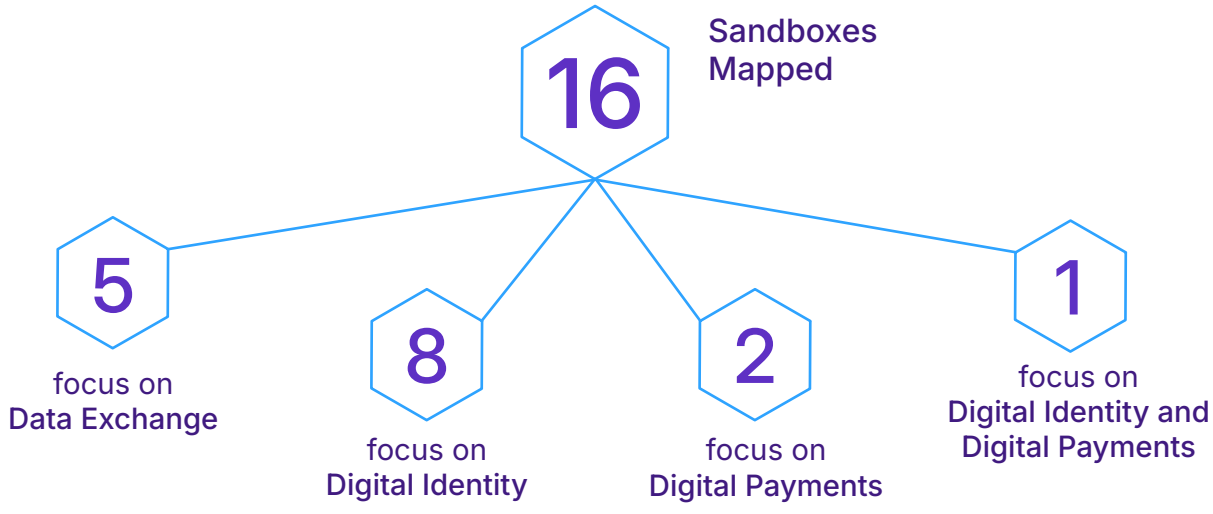
A first-of-its-kind empirical mapping

Moving beyond theory, this examination maps 14 national sandboxes across 11 jurisdictions and 2 regional sandboxes, offering the first global baseline of how governments are using sandbox experimentation to build resilient digital foundations.

A global snapshot of DPI sandboxes.



Note: The map shows 14 national sandboxes. It does not include the regional sandboxes such as the European Digital Wallet and EU Interoperability Regulatory Sandbox Hub.



Key takeaways

Feedback loops and institutional learning are features of successful DPI

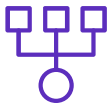
Analysing cases of experimentation with digital identity, payments, data exchange, and interoperability highlight how successful DPI is not built through linear planning or one-off policy decisions, but through continuous experimentation, feedback loops, and institutional learning. While early efforts were not explicitly labeled as sandboxes at the time, they share key characteristics: controlled experimentation, real-world testing, cross-institutional collaboration, and an emphasis on learning before scaling.

DPI adoption depends on trust

DPI outcomes are not primarily dictated by technology but also in governance choices. When designed poorly or governed weakly, DPI can entrench exclusion and expose vulnerabilities. The need for trust in DPI for it to be adopted at scale is a multifaceted and recurring challenge to be addressed by more inclusive and practical digital governance approaches.

Hybrid sandbox models are emerging

As DPI choices are deeply interdependent — linking technical design with legal rights — countries often adopt hybrid sandboxes. These environments allow governments to test technical components of DPI as well as governance and regulation, reducing the gap between how systems work and how they are governed.



Testing is done upstream

Sandboxes allow governments to shift DPI experimentation "upstream", testing safeguards for privacy, inclusion, and human rights before systems are deployed at population scale. This prevents "silent failures" where technically functional systems quietly exclude marginalized groups.

Identity is the primary testbed, followed by data exchange and payments

Most current DPI experimentation focuses on digital identity (9 of 14 sandboxes) as some countries are testing digital identity systems to ensure security and interoperability before nationwide rollout. The focus of sandboxes then shifts to data exchange and interoperability testing. Sandboxes in the financial sector continuously support solutions for digital payments systems.

Recommendations

The choice of investing in DPI is dependent on the delicate equilibrium of balancing the opportunities and risks of global markets with digital sovereignty. Moreover, as DPI systems become more interconnected and entangled with AI, the cost of failure rises. Ultimately, the question facing DPI is not whether experimentation is needed, but how it is carried out, who leads it, to what end and whether it can build trust in the process. By institutionalizing iterative testing upstream, sandboxes can help shift DPI development away from rigid implementation and toward systems that are legitimate and responsive to the people they are meant to serve. However, for sandboxes to have a role in supporting DPI design and deployment they must be treated not as one-off pilots, but as institutional capabilities necessary for governments world-wide:

1. **Government agencies need clear mandates that link experimentation to decision-making.** Sandboxes can surface inclusion gaps, cybersecurity vulnerabilities, or operational constraints early, helping to prevent harms from becoming entrenched. Public sector officials need the resources, mandates and the impetus to act on sandbox learnings as well as clear mechanisms to ensure that insights generated meaningfully inform policy, procurement, and system architecture.

2. **Investment in DPI needs to be accompanied by strengthening public-sector capacity for cross-disciplinary and cross-stakeholder collaboration.** Without inclusive design and implementation, DPI sandboxes risk becoming symbolic exercises, missing opportunities for bringing affected communities and relevant expertise into the design process, and safeguards that can make DPI transparent and accountable.

3. **Governments and ecosystem actors need the confidence, skills, and resources to continuously learn and adapt.** This involves training and mindset shifts in the public sector to learn from failings and adapt to emerging challenges and uncertainty, as well as technical capacity-building to examine legal, policy, and oversight questions alongside technical design and real-world use.

Looking ahead, the relevance of sandboxes and collaborative experimentation for DPI governance is only set to grow. Much like digital public goods provide shared, open foundations for building and scaling digital systems, sandboxes could offer the public sector common testing facilities, methodologies, and governance practices that support continuous learning, iteration, and value creation. As the challenges we face become ever more digital, complex and cross-cutting, the future of DPI will be shaped not only by what is built, but by how societies choose to test, adapt, and learn along the way.

Introduction

Digital Public Infrastructure (DPI) is often described as the set of inclusive, interoperable, and publicly accountable[1] digital building blocks that allow governments to provide safe and inclusive services to people at scale.[2] Capabilities that enable people to participate in society are in constant evolution, but the three capabilities that various countries have converged on to manage as DPI[3] are the abilities to digitally verify identities, securely send or receive money, and safely exchange personal information.[4] In fact, DPI is not simply another category of digital systems. Its defining characteristic is its foundational nature[5] and once deployed, it reshapes how people access services, how states exercise authority, and how markets operate.

While the term itself remains relatively new, DPI has rapidly gained recognition as a critical enabler of digital transformation and a cornerstone for closing digital divides. The African Union,[6] the United Nations Global Digital Compact,[7] and successive G20 Presidencies, India in 2023, Brazil[8] in 2024, and South Africa[9] in 2025, have all positioned DPI as a development accelerator. This growing political consensus has been matched by a surge in investment and experimentation,[10] reflected in initiatives such as the "50 in 5"[11] campaign, which aims to support 50 countries to design, launch, and scale core DPI components within five years.

1 Eaves D. Sandman J. (n.d), What is Digital Public Infrastructure? Codevelop

2 UNDP (n.d), The Universal DPI Safeguards Framework is live, United Nations Office for Digital and Emerging Technologies.

3 Frischmann, B. (2012). Infrastructure: The Social Value of Shared Resources. Oxford University Press.

4 Eaves D. Sandman J. (n.d), What is Digital Public Infrastructure? Codevelop

5 Digital, AI and Innovation Hub (n.d.), *Digital Public Infrastructure (DPI)*, UNDP

6 African Union (2024) *African Digital Compact*, African Union.

7 United Nations (2024) *Global Digital Compact*, United Nations Office for Digital Technologies.

8 G20 India (2023) *G20 Framework for systems of digital public infrastructure*, G20 India.

9 Ministry of External Affairs India (2024) *Declaration on Digital Public Infrastructure, AI and Data for Governance - Joint Communiqué*, Government of India.

10 Ministry of External Affairs India (2024) *Declaration on Digital Public Infrastructure, AI and Data for Governance - Joint Communiqué*, Government of India.

11 50 in 5 Campaign.

This foundational role makes DPI a double-edged sword.[12] When designed and governed well, it can dramatically expand access to essential services, inclusive economic growth, expand access to new types of financial services through digital payments, tackle corruption, and strengthen the economic resilience of households at unprecedented scale.[13] When designed poorly or governed weakly, it can just as effectively entrench exclusion, normalize surveillance, concentrate power, and lock entire populations into systems that are opaque and difficult to contest. The difference between these outcomes is not primarily technological. It lies in governance choices: who is involved, whose interests are prioritized, what safeguards are built in, and how uncertainty and risk are managed over time.

These governance challenges are not hypothetical. In many parts of the world, DPI is being deployed in contexts marked by historical mistrust,[14] risks of exclusion and surveillance,[15] gaps in digital literacy, connectivity and recurring privacy violations,[16] particularly among marginalized communities. Additionally, as DPI expands across sectors and becomes more deeply embedded in public service delivery, early design and governance choices become increasingly difficult to reverse. Once encoded in legal frameworks, institutional practices, and technical architectures, governance failures are harder to detect, contest, and correct.

International frameworks and principles, such as the United Nations Development Program (UNDP) *Universal Digital Public Infrastructure Safeguards*[17] that recognizes the need to proactively mitigate risks at both individual and societal levels, and the Organization for Economic Co-operation and Development (OECD) 2024 Report[18] on Digital Public Infrastructure which similarly provides guidance on building secure, interoperable systems to enhance public service delivery, are essential but do not on their own resolve the practical challenge facing governments: how to experiment, learn, and adapt.

[12] Diamond A., Gaur R. (2024), *Digital public infrastructure can bring enormous benefits – or pose significant risks. Safeguards make the difference*. Digital Impact Alliance.

[13] UNDP (2023), *The Human and Economic Impact of Digital Public Infrastructure: A quantitative analysis of the potential impact of digital public infrastructure by 2030 across the finance, climate and justice sectors*, UNDP.

[14] The case of Uganda's National Digital ID system. Aparo (2023), CIPESA, *Uganda's Digital ID System Hinders Citizens' Access to Social Services*, CIPESA.

[15] The case of Brazil's National Civil Identification System. Boni, Garrote,Meira, Paschoalini (2022) *Between visibility and exclusion: mapping the risks associated with the National Civil Identification System and the usage of its database by the gov.br platform. Associação Data Privacy Brasil de Pesquisa*, Data Privacy Brazil.

[16] The case of Kenya's National Digital ID system. Macdonald (2024), *Kenya's national digital ID: Lofty project on a bumpy ride*, Biometric Update.

[17] UNDP (2024) *Universal Digital Public Infrastructure Safeguards*, UNDP.

[18] OECD (2024), *Digital Public Infrastructure For Digital Governments: Oecd Public Governance Policy Papers No. 68*

It is precisely under these conditions, high stakes, irreversible design choices, asymmetric power, and deep uncertainty, that the case for human-centric design choices and collaborative testing in the context of DPI becomes compelling. This can be achieved by using tools that offer a way to explore new technologies, governance arrangements, and institutional roles in a controlled setting, allowing learning and adjustment before full-scale deployment. Sandboxes are such a tool and despite their expanding use in areas such as financial regulation and data governance, the role of sandboxes in the context of DPI remains under-examined. At the same time, despite the rapid global expansion of DPI, there has been little systematic exploration of how sandboxes can support DPI design, governance, and implementation. Both fields remain nascent, and until this report and the research effort led by the Datasphere Initiative, there have been minimal attempts to examine the nexus between them. This report therefore represents a first effort to investigate, document, and categorize sandbox experiments in the context of DPI.

The report explores how sandbox approaches are being applied to DPI across different regions and sectors, and how they can support more inclusive, accountable, and adaptive DPI development. By mapping emerging practices and examining the rationales, opportunities, and limitations of DPI sandboxes, the report seeks to contribute to a more grounded understanding of how experimentation and co-creation can be used to manage risk, build institutional capacity, and potentially strengthen trust in DPI initiatives.

The report begins by defining what sandboxes for DPI are, building on and updating earlier work by the Datasphere Initiative, including the *Sandboxes for data: Creating spaces for agile solutions across borders report* (2022).[19] Drawing on emerging issues for trust-building in DPI and perspectives from governments, the private sector, and civil society, the report examines why sandboxes are increasingly being used to manage the opportunities and risks of DPI, while also identifying challenges and limitations. It then maps where DPI sandboxes are being deployed globally, tracing early pioneers as well as emerging practices as the ecosystem evolves. The concluding section offers recommendations for actors designing DPI sandboxes and outlines forthcoming work, including case studies, co-creation labs, and a practical toolkit on how to design and implement DPI sandboxes.

This report builds on the work of the Datasphere Initiative and its Global Sandboxes Forum – a collaborative space dedicated to exchanging sandbox ideas, best practices, and real-world applications. Initially developed as a discussion paper for the inaugural Global Sandboxes Forum meeting in July 2024, the report has evolved through expert consultations and policy dialogues, including online events ahead of the 2026 India AI Impact Summit.[20]

[19] Datasphere Initiative (2022). *Sandboxes for data: creating spaces for agile solutions across borders*.

[20] Carvalho (2025). *Experts Urge Real-World Testing for AI-Powered Digital Public Infrastructure: Lessons Ahead of the AI Impact Summit 2026*, Datasphere Initiative.

What are DPI sandboxes?

This section clarifies the conceptual foundations of DPI and sandboxes. It traces the evolution of DPI as a policy concept and highlights the high stakes involved in designing and governing these foundational systems. It introduces the notion of sandboxes and further distinguishes between regulatory, operational, hybrid and other emerging sandboxes, illustrating how different models support DPI development at various stages. Across these models, the defining feature of DPI sandboxes is not only what is tested, but who participates and how insights are translated into institutional practice.

Building on this framing, the section traces how experimentation has shaped the development of DPI over time, moving from implicit practice to an explicit policy tool. It begins with the experiences of DPI pioneers, countries and initiatives that embedded iterative testing, flexibility, and real-world experimentation into their DPI journeys, even when these approaches were not formally labeled as sandboxes. The section concludes with a proposed definition of DPI sandboxes which is subsequently used throughout this report.

Defining DPI

The growing emphasis on DPI reflects a broader recognition that many countries have historically relied on fragmented, proprietary, or siloed digital systems to deliver essential services. These approaches often limit interoperability, increase dependency on single vendors, and exacerbate exclusion for populations unable to access or trust digital services. DPI emerged as a way to articulate an alternative: shared, open-source, public-interest digital foundations that can be reused across sectors, reduce duplication, and support innovation while safeguarding rights.[21]

The concept of DPI has gained global prominence in recent years and became widely recognized during India's G20 Presidency in 2023, which marked a critical moment in consolidating a shared international understanding of these systems. During the G20 Digital Economy Ministers' Meeting, DPI was framed as *"a set of shared digital systems that are secure and interoperable and can support the inclusive delivery of and access to public and private services at societal scale"*.[22]

The first expert guidance on DPI released by the United Nations Development Programme (UNDP) also referenced these definitions[23] and helped to anchor DPI as a policy-relevant concept. Building on India's definition, UNDP describes DPI as *"a set of shared digital systems which are secure and interoperable, built on open standards, and specifications to deliver and provide equitable access to public and/or private services at societal scale and are governed by enabling rules to drive development, inclusion, innovation, trust, and competition and respect human rights and fundamental freedoms."*[24] DPI has since been referenced by the Organisation for Economic Cooperation and Development (OECD).[25]

In 2024, the definition was further refined by Co-Develop, a global not-for-profit fund focused on advancing DPI globally. Co-Develop defines DPI as *"society-wide digital capabilities that are essential to participation in society and markets as a citizen, entrepreneur, and consumer in a digital era."*[26] This formulation places greater emphasis on participation, agency, and inclusion, highlighting DPI not only as technical infrastructure but as a core enabler of social and economic life.

---

[21] Ahmed Fathy & Luo (2025) *Building digital public infrastructure for cities and communities A strategic framework for city leaders, officials, ministers, and policymakers*. United for Smart Sustainable Cities (U4SSC) initiative; National Telecom Regulatory Authority (NTRA), Egypt; International Telecommunication Union (ITU).

[22] G20 India (2023) *G20 Framework for systems of digital public infrastructure*, Government of India.

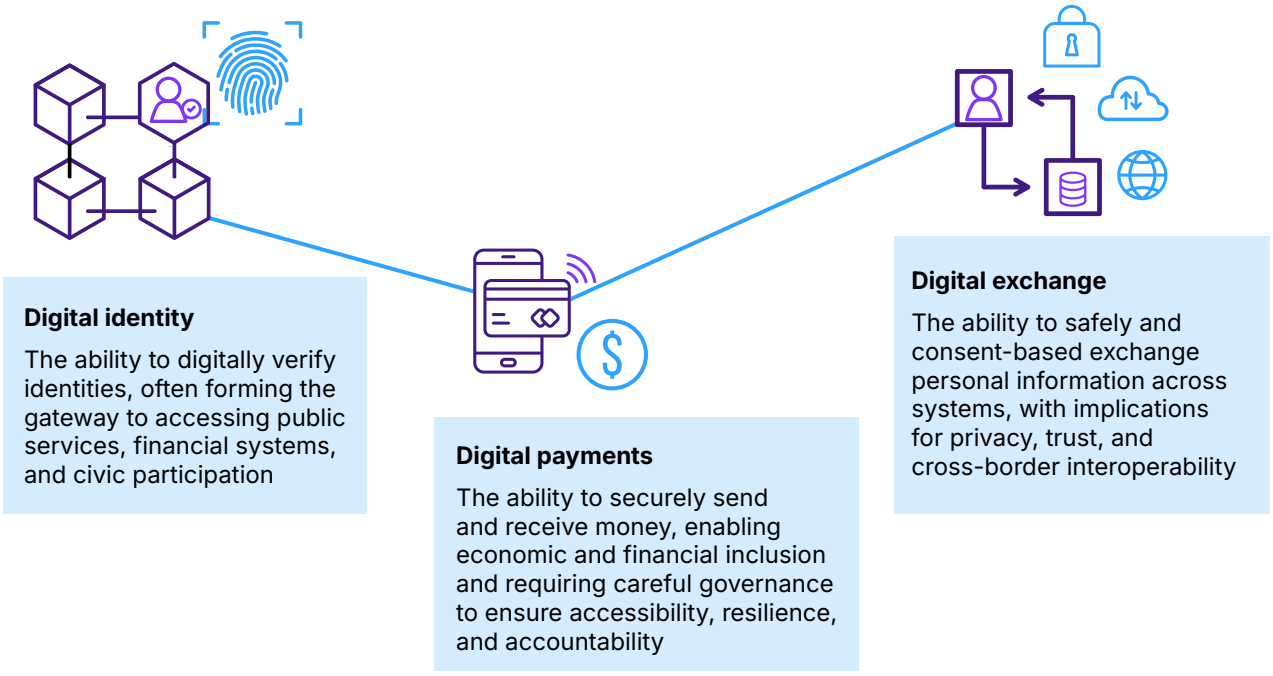
[23] A DPI compendium and playbook developed by the United Nations Development Programme (UNDP).

[24] UNDP (2023). The DPI Approach: A Playbook. UNDP Publications.

[25] OECD (2024) Digital public infrastructure for digital governments, OECD Public Governance Policy Papers.

[26] Co-Develop (n.d.). What is Digital Public Infrastructure?

Co-Develop operationalized this definition by identifying three core DPI layers:



A critical element of this concept is the understanding of data itself as infrastructure. Building on efforts to move beyond traditional views of infrastructure as physical assets like roads or bridges, this definition aligns with an expanded definition of infrastructure that includes digital components like cloud computing, broadband networks, and data.[27] By treating data exchange as a core infrastructural layer of DPI, countries recognize that the flow of information and the datasphere[28] is vital to modern social and economic life.

By framing DPI as "society-wide digital capabilities", Co-Develop's definition underscores the far-reaching consequences of how these systems are designed and governed. Decisions made at the DPI layer, such as identity verification rules, data-sharing standards, or payment rails, can shape access to services, market participation, and the distribution of power across society. As a result, DPI carries higher stakes than many sector-specific digital systems, requiring careful testing, oversight, and accountability before being deployed at scale.

[27] OECD (2015). Data-Driven Innovation: Big Data for growth and well-being. OECD Publishing.

[28] Datasphere Initiative (2022). Hello Datasphere: Towards a system approach to data governance. Datasphere Initiative.

For the purposes of this report, the Datasphere Initiative adopts the Co-Develop definition of DPI. This approach reflects both the growing convergence around these three foundational layers and the relevance of this framing for understanding where experimentation, risk, and governance challenges most frequently arise.

Defining Sandboxes

Originally developed by financial technology regulators like the UK Financial Conduct Authority (FCA)[29] and inspired by enclosed software testing environments used by programmers,[30] sandboxes have evolved into tools for the exploration and governance of emerging technologies, including AI.

This report builds on the definition introduced by the Datasphere Initiative in the *Sandboxes for Data* report (2022), which helped establish a shared understanding of data sandboxes as "safe spaces to test new technologies and practices against regulatory frameworks, or to experiment with innovative uses and means of governing data".[31] Since its publication, this definition has been widely referenced and applied across sectors and geographies, while also evolving in response to diverse policy contexts, governance challenges, and practical implementations.

Reflecting these learnings and drawing on accumulated evidence from sandbox initiatives worldwide, this report adopts an updated definition:

> A sandbox is a controlled learning environment designed for structured experimentation under defined governance frameworks, timeframes, and built-in safeguards to support iterative, multi-actor collaboration and evidence-based decision-making.

[29] Quan (n.d.) *A Few Thoughts on Regulatory Sandboxes*. Stanford PACS.

[30] Alaassar, A., AL. Mention and TA. Helge (2021), *Exploring a new incubation model for FinTechs: Regulatory Sandboxes Technovation*.

[31] In 2022 the Datasphere Initiative defined sandboxes as "safe spaces to test new technologies and practices against regulatory frameworks or experiment with innovative uses and means of governing data". Since then, the concept has evolved, which merited a new updated definition.

Box 1. The challenge of defining sandboxes

Sandboxes have never been a single, fixed institutional form. From their earliest uses in financial regulation to their expansion across data, AI, and emerging technologies, "sandboxing" has evolved as a flexible governance approach rather than a uniform model. This evolution makes sandboxes inherently complex to define in singular or static terms. Across domains and jurisdictions, the core mindset of experimentation, agility, and iterative learning remains consistent, but the way it is expressed varies widely.

This variation reflects differences in legal traditions, regulatory cultures, institutional capacity, and societal expectations around risk, trust, and collaboration. In some contexts, sandboxes are formal regulatory instruments embedded in legislation and supervision frameworks; in others, they function as collaborative testbeds, policy pilots, or learning environments convened by public agencies, the private sector, civil society, or multi-stakeholder partnerships. Terminology also differs; what is called a "sandbox" in one jurisdiction may appear as a "pilot", "testbed" or "test environment" in another, even when the underlying logic of experimentation is similar.

The diversity of sandbox models also mirrors differing priorities. Some emphasize market entry and innovation speed, while others foreground rights protection, inclusion, and public accountability. Many seek to balance all. Iteration may take the form of technical testing and performance evaluation, or of participatory design, community feedback, and institutional learning. These choices are shaped by local histories, incentives, and the communities most affected by the systems under development.

This diversity of sandbox efforts adds to the complexity of neatly categorizing sandboxes or creating a fixed taxonomy. As a relatively new and rapidly evolving field, sandboxes continue to be shaped through practice, adaptation, and learning across divergent contexts. Rather than fitting into stable typologies, sandbox models often blur boundaries and change over time, underscoring the need for continued observation and reflection as the field matures.

What unites sandboxes is not institutional form, but established governance to enable actors' learning from practical cases, adjust course before scale, or test how technologies or safeguards operate together in practice. This plurality is particularly important in the context of DPI, where experimentation must respond simultaneously to technical complexity, societal impact, and the need to build durable public trust.[32]

[32] Amutorine, M., Onyango, R., Rozo-Paz, M., Porciuncula, L. (2025). *Moving fast together: How sandboxes can help build trust in Digital Public Infrastructure*. Datasphere Initiative; Rozo-Paz, M. (2025).*TrustStack: filling the marble jar of digital trust*. Datasphere Initiative.

Building on its work across data and AI governance, the Datasphere Initiative introduced a taxonomy of sandboxes in the Sandboxes for Data report (2022), classifying them according to the primary objective of the experiment, distinguishing between regulatory, operational, and hybrid sandboxes.[33] While these categories are not rigid, they have provided a widely adopted lens for understanding how different sandbox models contribute to DPI development and governance.

Broadly speaking, **regulatory sandboxes** are centered on regulatory learning and governance experimentation, generating evidence to inform existing or future rules, policies, standards, compliance and guidance, while **operational sandboxes** focus on technical learning, providing access to data, software, or infrastructure to test, validate, and improve products, services, or processes. There are also the so-called **hybrid sandboxes** that provide a mix of these two objectives. Drawing on sandbox practice, experiences and lessons learned through the Global Sandboxes Forum[34] and the Africa Sandboxes Forum,[35] this report revisits and refines this taxonomy, presenting updated characterizations for each sandbox type (Box 2).

Box 2. Types of sandboxes

A **regulatory sandbox** is a controlled experimentation environment centered on regulatory learning or compliance, generating evidence to inform existing or future rules, policies, standards, and guidance.

Regulatory sandboxes are often coordinated by a regulatory authority or another public entity - such as a ministry or a municipality - bringing together multiple actors (e.g., companies, public sector actors, academia, civil society) to experiment with innovations at different stages of maturity, adopting incentives for participation such as regulatory flexibility (e.g. waivers, temporary licenses, or derogations) or dialogue with public authorities. Operating under a defined governance, testing plan and built-in safeguards, regulatory sandboxes can have several goals, such as fostering innovation, enhancing safety, facilitating market access, and protecting human rights. Regulatory sandboxes can span across local, national, or multi-country contexts, and support cross-sectoral and cross-regulatory cooperation.

In the context of DPI, regulatory sandboxes can support risk assessment and monitoring of technologies that may affect the infrastructure's reliability, citizens' rights and access to services, or public trust, helping policymakers anticipate challenges rather than reacting to harms after deployment. The Bank of Thailand's regulatory sandbox, for example, offers a controlled environment to test technology-enabled financial innovations that may impact payment systems and financial stability, balancing innovation with consumer protection and oversight.

[33] Datasphere Initiative (2022), *Sandboxes for data: creating spaces for agile solutions across borders*, Datasphere Initiative.

[34] Datasphere Initiative. Global Sandboxes Forum (website).

[35] Datasphere Initiative. Africa Sandboxes Forum (website).

An **operational sandbox** is an environment that provides access to data, software or infrastructure to enable the testing, validation, and improvement of standards or technical aspects of products, services, or processes (e.g., feasibility, scalability, interoperability, efficiency, or functionality), under real or simulated conditions.

It can be coordinated by any entity - including companies, public sector bodies, academia, or civil society - and supports experimentation with data or any technology across different stages of maturity, from early design to testing and validation, and under local, national, or multi-country contexts. In this way, an operational sandbox contributes to technical learning, improves safety and performance, facilitates market access, and generates practical outputs. For instance, a good example of an operational sandbox is the FCA's Digital Sandbox, delivered in partnership with NayaOne.[36] The sandbox enables innovative companies to develop and test their products in a safe and secure environment, with support from the FCA.[37]

In DPI contexts, operational sandboxes can help ensure that systems are grounded in actual use cases rather than conceptual designs, enabling diverse end users to interact with platforms and surface usability, consent, data-flow and inclusion issues early on. Singapore's Singpass API Developer Portal Sandbox, for instance, provides a controlled staging environment where developers can test and refine integrations within the National Digital Identity ecosystem, enabling secure authentication and consent-based data sharing across public and private services prior to live deployment.

A **hybrid sandbox** combines elements of both regulatory and operational approaches. These models allow stakeholders to both test technical aspects, and to engage stakeholders in dialogues about regulation and governance while providing some form of access to data, infrastructure, or shared technical environments. For instance the AI Assurance Sandbox by IMDA (Singapore Infocomm, Media Development Authority) and AI Verify Foundation is a hybrid sandbox which provides a testing ground for builders or deployers of GenAI applications (not the underlying foundation models) to get them tested by specialist technical testers.[38] The Sandbox is also open to sector regulators who want to develop and get real-life feedback on their AI governance and/or testing guidelines. Insights from the Sandbox also inform policy guidance of IMDA.[39]

Hybrid sandboxes should be understood as existing along a spectrum: in some cases, the emphasis lies primarily on operational experimentation, while in others regulatory guidance plays a more prominent role alongside technical testing. What characterizes a sandbox as hybrid is the presence of both dimensions, regardless of how they are weighted.

Hybrid sandboxes are increasingly relevant for DPI, where technical design and governance choices are deeply interdependent and where decisions taken at foundational layers, such as identity or data exchange, can multiply both benefits and harms across downstream applications.

[36] NayaOne (2023), *NayaOne selected to build and operate the FCA Digital Sandbox*, NayaOne.

[37] The 2025 FCA Supercharged Sandbox builds on the existing Digital Sandbox providing advanced compute power to further support AI innovation.

[38] AI Verify Foundation(2025) *Global AI Assurance Sandbox*.

[39] IMDA (202), *Singapore launches new tools to help businesses protect data and deploy AI in a trusted ecosystem*, IMDA.

Other emerging sandboxes capture a set of evolving experimentation models that do not yet fall squarely within regulatory or operational categories, but are increasingly relevant as governance practices adapt to technological and societal change.

The observation of new uses of sandboxes point to the possible emergence of **policy or legislative-oriented sandboxes** as new forms of governance experimentation. While promising, such approaches remain at an early and exploratory stage and will require sustained reflection, research and continued observation of practice and unique attributes before they can be distinguished as new sandbox categories.

Recognizing both their potential and their current exploratory nature, this report treats policy and legislative sandboxes as areas for continued consideration, rather than presenting them as a distinct new category, anticipating further rigorous analysis and evidence-building as their deployment matures.

An illustrative example is the proposal advanced within Chile's National Congress to establish a sandbox as an institutional mechanism to support legislative innovation and governance in the context of AI and digital transformation.[40] Drawing on principles of experimental governance, the proposal envisions a structured testing environment within the legislative branch that would enable parliamentarians and other stakeholders to anticipate the societal impacts of emerging technologies, assess policy options, and generate evidence to inform legislative processes prior to the adoption of formal laws.

[40] Ramírez, Urriola (2025). "Hacia un Congreso innovador: propuesta para la implementación de un sandbox tecnológico en el Poder Legislativo chileno". Hemiciclo. Revista de estudios parlamentarios. Chamber of Deputies of Chile. Year 13. No. 26. 2025. pp. 169-176.

DPI experimentation and prototyping

Because both fields of study "sandboxes" and "DPIs" are still nascent, until this report, there were minimal explorations on the nexus between them. However, early experiences in experimenting with DPI have been reported and provide useful insights on the roots of DPI experimentation and how the concept of DPI sandboxes has evolved.

It is important to note, that while the term DPI has recently gained global traction, some argue that DPI is not a sudden invention and ii represents the modern culmination of concepts such as e-government[41] or digital government that have been refined over the last 20 years.[42] These earlier efforts also grappled with the need for agile governance and often utilized experimental spaces — precursors to modern sandboxes — to test how digital tools could modernize the state. However, where e-government often focused on the digitization of existing bureaucratic processes, DPI represents a more integrated and "society-wide" arrangement designed to support both public and private sector innovation on top of shared rails, fostering the role of "government as a platform".[43]

There are various experimental and prototyping-like efforts in DPI that have not been called DPI sandboxes but provide sandbox-like traits and useful learnings on understanding the potential of these models. These early initiatives — often emerging from applied research, public interest technology, or cross-sector collaboration — demonstrate how iterative experimentation, real-world testing, and multi-stakeholder engagement have long been integral to the development of digital systems intended for public use. The cases from India (Box 3), Brazil (Box 4) and Estonia (Box 5), although not explicitly framed as DPI sandboxes illustrate how controlled experimentation with identity, data, and financial systems generated practical insights on inclusion, interoperability, and governance. Together, these experiences help ground contemporary sandbox approaches in a longer history of experimentation and learning, and provide important context for understanding how inclusive and trustworthy DPI can be designed and scaled.

[41] Heeks, R. (2001). Understanding e-Governance for Development. iGovernment Working Paper Series.

[42] Eaves, D. and Rao, K. (2025). Digital Public Infrastructure: a framework for conceptualisation and measurement. UCL Institute for Innovation and Public Purpose.

[43] Eaves, D., Mazzucato, M. and Vasconcellos, B. (2024). Digital public infrastructure and public value: What is 'public' about DPI?. UCL Institute for Innovation and Public Purpose.

Box 3. India: from pilots to population-scale infrastructure

India offers a particularly instructive example of how large-scale DPI can be built through sustained experimentation, iteration, and co-creation, long before the language of "sandboxes" became mainstream.

India's DPI stack, anchored in digital identity (Aadhaar), digital payments (UPI), and data exchange and document services (DigiLocker), was not the result of a single, monolithic launch. Rather, it evolved through continuous cycles of testing, prototyping, and incremental scaling. Early versions of these systems were piloted in limited geographies and use cases, often beginning with a handful of states or institutions, before gradually expanding to millions and eventually billions of transactions. This approach allowed policymakers and technologists to observe real-world behavior, identify risks, and adapt systems over time.

As practitioners involved in India's DPI journey have emphasized,[44] early experimentation focused on stress-testing foundational elements: biometric accuracy and deduplication, data quality, device standards, encryption flows, authentication latency, and transaction capacity. Systems were deliberately pushed to failure to understand breakpoints and to design fallback mechanisms, an approach that mirrors the logic of operational sandboxes, even if it was not labeled as such at the time. This iterative stress-testing proved essential to challenge assumptions and ensure resilience at scale, particularly in low-connectivity environments and among populations with diverse literacy levels.

Recent initiatives demonstrate how India is formalizing these experimental practices.[45] In 2023, the Unique Identification Authority of India (UIDAI) launched an operational sandbox to enable fintechs and start-ups to safely integrate and test core Aadhaar APIs, including e-KYC and authentication journeys, before live deployment.[46] The sandbox provides a controlled environment for experimentation, addressing a long-standing gap in India's digital ecosystem where innovators previously had limited access to test identity-based services without incurring high costs or regulatory uncertainty. In its first year alone, the sandbox attracted over 150 applications, supported 15 start-ups, and facilitated more than one million test authentications, significantly reducing product validation timelines while strengthening safeguards around identity use.[47]

India's journey underscores a central insight: **successful DPI is not built through linear planning or one-off policy decisions, but through continuous experimentation, feedback loops, and institutional learning**. Long before sandboxes became a formal policy tool, India embedded sandbox-like logic into its DPI development process. As countries now grapple with the convergence of DPI and AI, India's experience highlights why structured experimentation, co-creation, and mechanisms for course correction are not optional add-ons, but core components of trustworthy and inclusive digital public infrastructure.

[44] Prabhu, Jain (2024), *Transformative Innovation Policy in Practice: The Case of India's Digital Public Infrastructure*.

[45] Rozo-Paz (2025), *Key insights for AI-powered DPI ahead of the India AI Impact Summit 2026*, Datasphere Initiative.

[46] MSC (2025), *The Aadhaar (UIDAI) sandbox for digital identity and finance innovation*, MSC.

[47] Unique Identification Authority of India (2026), *Developer Section*, Unique Identification Authority of India.

Box 4. Brazil: iterating and testing digital payments

Brazil's PIX initiative offers a particularly illustrative example of how a state-led digital public infrastructure can also function as a space for cultural change, continuous experimentation, and structured collaboration with private-sector actors. Pix is Brazil's instant payment system operated by the Central Bank of Brazil (BCB), officially launched in November 2020 as part of a broader strategy to modernize the national payments system and promote financial inclusion, efficiency, and competition.[48] Its origins, however, date back several years earlier. As early as 2016, the BCB began actively encouraging the development of an open instant payment solution, including by convening an international workshop to expose Brazilian market actors to experiences from other jurisdictions.[49] At the time, existing innovations, such as mobile payments via QR codes, were largely closed systems, requiring both payer and payee to be clients of the same institution. By 2018, it had become clear that market coordination failures and competing private interests would prevent the emergence of an open, interoperable solution. In response, the BCB assumed a leadership role as a neutral public authority, positioning itself as the designer, operator, and steward of a shared payments infrastructure. This decision led to the creation of Pix as an open, interoperable system with centralized settlement and governance, fundamentally reshaping payment practices in Brazil, consolidating Pix as a core component of the country's DPI.

Pix was designed from the outset through an open and iterative governance model that embedded experimentation and multistakeholder collaboration into its development, through the establishment of a working group and a permanent Pix Forum, which structured ongoing dialogue on rules, standards, and technical evolution. At the same time, the Central Bank retained control over the core infrastructure, enabling controlled experimentation, gradual rollout, and trust-building at scale. Available 24/7 with real-time settlement, Pix enables individuals, businesses, and public entities to make and receive payments using simple identifiers such as QR codes, phone numbers, or tax IDs, without dependence on traditional card networks. Its rapid and widespread adoption represented a major shift in everyday payment practices in Brazil: Pix grew from 9.4 billion transactions totaling approximately R$5 trillion in 2021 to 63 billion transactions and R$26.4 trillion in value in 2024 - equivalent to roughly 2.5 times Brazil's annual GDP.[50] Today, Pix is used by nearly 170 million individuals - effectively the vast majority of the adult population in Brazil - and more than 20 million companies, significantly lowering transaction costs, expanding access to digital payments for previously underserved populations, and consolidating Pix as a core component of the country's DPI.

[48] Banco Central Do Brasil (2026), *About Pix*, Banco Central Do Brasil.

[49] Banco Central Do Brasil (2023), *Relatório de Gestão do Pix Concepção e primeiros anos de funcionamento*, Banco Central Do Brasil.

[50] Banco Central do Brasil (2025), *Pix 5 anos – a Inovação que Redefiniu o Dinheiro no Brasil*. Banco Central do Brasil.

Within this broader experimental and collaborative ecosystem, Pix later served as the technological backbone for a testing case conducted under the BCB's regulatory sandbox program. Proposed by Itaucard, the project explored the integration of Pix's instant settlement infrastructure with credit card functionalities, allowing credit card holders and Itaú Unibanco account holders to make payments either upfront or in installments by scanning Pix QR codes via a smartphone application.[51] The key innovation lay in operationalizing credit transactions directly from a post-paid account while preserving Pix's core promise of instant settlement for merchants. The sandbox environment enabled the project to be piloted with partner merchants and gradually expanded to a large pool of users, generating real transaction data under close regulatory supervision. No systemic or operational failures were identified, and the sandbox allowed detailed observation of transaction flows, cancellations, and user behavior, including constraints related to credit limits or blocked cards. Based on positive user acceptance, the Central Bank extended the monitoring period of the project to support learning about potential future functionalities, while making clear that any regulatory changes would depend on deliberation within Pix's multistakeholder governance structures.[52]

This experience highlights several key lessons about the value of sandboxes for testing new functionalities on top of DPI. In particular, the sandbox enabled the assessment of installment payments via Pix as a feature with strong potential to enhance inclusivity and access to digital payments, especially for users who cannot afford to pay for higher-value purchases in a single transaction.

At the same time, sandbox testing allowed regulators and operators to evaluate risks related to credit exposure, defaults, and consumer protection - all critical factors for preserving trust in a payment system that operates at national scale. Importantly, the Pix experience shows how sandbox experimentation can support the transition from testing to market deployment: following positive results and regulatory learning, installment-based Pix solutions have moved beyond the sandbox and are now offered by several banks as a payment option (Pix Parcelado), under different business models and risk arrangements. Sandbox experimentation on DPI can generate evidence to inform regulatory oversight and multistakeholder governance, enabling functional expansion while safeguarding the stability, reliability, and public trust of core infrastructures like Pix.

[51] Banco Central Do Brasil (2023), *Relatório de Gestão Sandbox Regulatório*, Banco Central Do Brasil.

[52] Banco Central Do Brasil (2023), *Ata da trigésima reuniao ordinária do comite estratégico de gestao do sandbox regulatório (CESB)*,Banco Central Do Brasil.

Box 5. Estonia: A DPI journey centered on citizens and agility

Estonia's DPI journey is widely regarded as one of the most mature and coherent in the world, rooted in a "digital-by-design" approach to public administration.[53] Rather than building monolithic e-government systems, Estonia focused early on digitizing core state registers and enabling secure data exchange between them. This vision materialized through X-Road (X-Tee), a foundational interoperability layer that allows public and private actors to exchange data securely and efficiently, while remaining embedded in a strong legal and data governance framework.[54] Citizens retain visibility and control over how their data is used, reinforcing trust as the digital ecosystem scales to support over 1,700 services across sectors.[55]

A defining feature of Estonia's approach has been its commitment to modularity, reuse, and openness. Key DPI components such as X-Road have been released as open-source digital public goods and adopted or adapted by dozens of countries.[56] This building-block logic extends beyond data exchange to digital identity, e-signatures, open data portals, and AI-enabled public services. Initiatives like the Digital Government Code Repository (Koodivaramu) further institutionalize experimentation and reuse by making government-developed source code openly available, reducing duplication and enabling faster prototyping across agencies and with the private sector.[57]

Experimentation is also central to how Estonia engages globally on DPI. As a co-lead of GovStack, Estonia has helped shape a shared implementation framework that translates DPI principles into practical, deployable building blocks. GovStack explicitly integrates experimentation through the GovStack Sandbox, a demonstration and testing environment where governments and service providers can learn, prototype, and validate how interoperable components, such as information mediators, digital ID, or data exchange, work together in real service journeys.[58] This sandbox approach lowers the risk of lack of adoption, supports capacity building, and enables countries to tailor solutions to local contexts while adhering to common standards.

Rather than treating sandboxes as isolated tools, Estonia uses them as learning infrastructures embedded in long-term digital transformation strategies. Through GovStack trainings, sandbox environments, and global partnerships, Estonia positions experimentation as a bridge between analysis and implementation, allowing governments to start small, test responsibly, and scale sustainably. This combination of strong governance, open digital public goods, and structured experimentation has enabled Estonia not only to build a resilient national DPI ecosystem, but also to export practices, tools, and values that continue to shape global DPI conversations.

[53] Price, Rodriguez, Alberto (2024), *Learning from International DPI Efforts*, New America.

[54] Leosk (2022), *Estonian Case – The development and promotion of Digital Public Infrastructures*, Observer Research Foundation.

[55] Clark, J., Marin, G., Ardic Alper, O.P., Galicia Rabadan, G.A. (2025), *Digital Public Infrastructure and Development: A World Bank Group Approach. Digital Transformation White Paper, Volume 1*, World Bank.

[56] Estdev (2025), From Analysis to Action: GovStack as the DPI Implementation Framework for Better Public e-Services, Estdev.

[57] E-estonia (2019), Estonia creates a public code repository for e-governance solutions, E-estonia.

[58] Estdev (2025), From Analysis to Action: GovStack as the DPI Implementation Framework for Better Public e-Services, Estdev.

Beyond India, Brazil and Estonia, a range of early initiatives across regions experimented with digital identity, payments, data exchange, and interoperability in ways that closely resemble what are now described as DPI sandboxes. While these efforts were not explicitly labeled as sandboxes at the time, they shared key characteristics: **controlled experimentation, real-world testing, cross-institutional collaboration, and an emphasis on learning before scale.**

These initiatives emerged from diverse institutional settings — central banks, digital government agencies, academic networks, and regional cooperation platforms — but collectively illustrate how sandbox-like approaches have long underpinned successful DPI development. They provide important insights into how trust, interoperability, and governance challenges can be surfaced early, adapted to context, and addressed iteratively before nationwide or cross-border deployment.

In Latin America and the Caribbean (LAC), regional and national initiatives have provided early examples of sandbox-like experimentation around digital identity and interoperability. At the regional level, the Red GEALC initiative on the LAC Digital Citizen[59] program stands out as a structured, iterative process to test cross-border digital identity interoperability among public authorities in the region. Through successive cohorts - currently reaching its fourth iteration - the initiative has enabled countries such as Uruguay, Argentina and Brazil to pilot technical, legal, and governance arrangements for mutual recognition of digital identities in a controlled setting, before any binding regional deployment. In collaboration with the GEALC Network, Uruguay began testing cross-border integration in 2023, linking ID Uruguay with Argentina's digital ID broker, Autenticar, and with the Brazilian Gov.BR, in 2024, to assess compatibility.[60] Although not formally framed as a sandbox, the initiative operates as an experimental environment focused on learning, trust-building, and institutional coordination across jurisdictions.

At the national level, El Salvador's Tenoli[61] initiative offers another example of a sandbox-like experience for experimenting with digital public infrastructure. Public sector institutions tested interoperability within government using the same platform adopted by Estonia, X-Road platform, to enable trusted information sharing between public authorities. X-Road provides a dedicated "playground" environment in which interoperability solutions can be piloted in a controlled, low-risk setting. This setup allowed government actors to experiment with real data flows, institutional data-sharing arrangements, technical standards, and operational workflows, as well as clarifying roles and responsibilities among participating institutions. In practice, Tenoli mirrored the core features of an operational sandbox: controlled experimentation, real-world testing, and iterative learning aimed at reducing implementation risks, building institutional capacity, and supporting a gradual and coordinated transition toward broader public-sector interoperability.

[59] Red GEALC (2025), LAC Digital Citizen and DPI Summit, Red de Gobierno Electrónico de América Latina y el Caribe (Red GEALC)

[60] 50 in 5 (2025), *Building Trust Across Borders: Latin America's Path to Interoperable Digital ID*, 50 in 5.

[61] X-Road (2024), First Steps Towards Interoperability in the Public Sector of El Salvador, X-Road Global.

In Africa, similar sandbox-like approaches have emerged to support experimentation with DPI in contexts marked by institutional diversity and rapid digital transformation. The Upanzi Network[62] is an initiative coordinated by academic institutions in partnership with public sector actors across East Africa, functioning as a collaborative testbed where countries can prototype, test, and compare DPI components such as digital identity systems, payment infrastructures, and data-sharing architectures. Rather than focusing on immediate large-scale deployment, the network emphasizes experimentation, applied research, and peer learning across jurisdictions with different institutional capacities and legal frameworks. This regional setup allows participants to explore interoperability challenges, governance trade-offs, and context-specific design choices in real or near-real world conditions, while benefiting from shared technical expertise and comparative insights. In this sense, Upanzi closely resembles an operational sandbox operating at regional scale, where experimentation is used to surface risks early, generate evidence, and inform more sustainable and interoperable DPI design choices before national or cross-border scaling.

A final example is Rwanda's Center for Digital Public Infrastructure, launched by the Rwanda Information Society Authority (RISA):[63] the Center is explicitly conceived as a dynamic testbed for emerging DPI solutions, supporting the piloting, iteration, and evaluation of digital identity, data exchange, and other foundational infrastructures in a controlled environment. Rwanda aims to align technical innovation with policy objectives, regulatory considerations, and capacity-building efforts across the public sector, embedding experimentation within a dedicated institutional setting. This approach allows government actors to test new DPI components and governance arrangements incrementally, assess their societal and operational impacts, and refine them before rolling out an innovation nationwide.

Defining DPI sandboxes

In the absence of a universally agreed definition of DPI sandboxes, and given the evolving definition of DPI and the wide variation in how sandboxes are labeled across regions and policy domains, this report adopts a functional, layer-based approach that prioritizes the role of experimentation in advancing core components of DPI.

Under this approach, ***DPI sandboxes* are defined as sandboxes that are designed to test, pilot, or operationalize technologies, standards, or governance arrangements within at least one DPI layer**. Within these initiatives, experimentation is explicitly oriented toward strengthening, scaling, or enabling DPI. The mapping of DPI sandboxes identified through this approach is presented further in the report (Table 1, page.48).

[62] Carnegie Mellon University Africa (n.d.), Upanzi: Digital Public Infrastructure Research, Carnegie Mellon University Africa.

[63] RISA (2024), Rwanda Launches the Center for Digital Public Infrastructure: A New Era of Innovation and Inclusion, Rwanda Information Society Authority.

Specifically, an initiative is classified as a DPI sandbox when its experimental scope focuses on one or more of the following DPI layers:

Digital identity systems

enhancing a verifiable identity, including authentication mechanisms, credentials, digital wallets, or identity interoperability

Digital payments systems

enhancing financial inclusion, including payment rails, settlement infrastructure, central bank digital currencies, or public payment platforms

Data exchange and/or interoperability layers

enhancing secure data flows, including data-sharing platforms, APIs, registries, consent mechanisms, or cross-system interoperability frameworks

Importantly, this definition distinguishes DPI sandboxes from other sandboxes that may interact with or rely on DPI, but are not designed around DPI experimentation itself. There are sandboxes that have supported DPI that are not designed as DPI sandboxes, but enable experimentation which can support or inform DPI or DPI-enabled solutions. In such cases, several sectoral sandboxes, most commonly those led by central banks or other financial regulators, have enabled experimentation that interfaces directly with national payment or data infrastructures. While such initiatives can generate valuable learning for DPI development, DPI layers are not their primary object of experimentation.

Across these different sandbox models, what distinguishes DPI sandboxes is not merely experimentation, but who experiments, how, and to what end. When intentionally designed, sandboxes can bring public authorities, private innovators, civil society organizations, youth groups, and diverse affected communities into shared spaces of learning and co-creation. They make collaboration tangible, embed lived experience into system design, and help translate abstract principles, such as inclusion, accountability, and trust, into operational practice. At the same time, they require careful design to avoid tokenistic participation, opacity, or the loss of insights once experimentation concludes.

Why sandboxes for DPI?

This section explores the opportunities and challenges sandboxes can bring to DPI initiatives. Exploring some of the challenges emerging from DPI cases worldwide, this section identifies how sandboxes can play a useful role in supporting interoperability, trust building efforts, fostering inclusion and addressing human rights and cybersecurity risks. When considering why to use a sandbox model for DPI it is also important to consider the different incentives and challenges governments, companies, civil society alike may face when deciding to design or participate in DPI sandboxes. The section concludes with an overview of rationale and considerations for relevant DPI stakeholders.

Trust as a key lever for DPI

Trust is a critical dimension of successful DPI implementation that is still too often overlooked. Experience from countries[64] indicates that DPI evolves over time and that linear, rigid implementation approaches tend to fall short. Instead, DPI systems evolve through iteration and adaptation, often revealing governance weaknesses as they scale.

Across contexts, evidence points to recurring trust-related challenges: exclusion of marginalized groups from identity systems,[65] weak accountability for biometric surveillance[66] and data reuse. As well as, limited transparency in procurement and vendor relationships, and minimal public participation in system design and oversight. These challenges are compounded as DPI expands across sectors, linking identity, payments, health, social protection, and other services into highly interconnected digital ecosystems.

Taken together, these challenges are not isolated technical failures, but symptoms of a deeper governance gap[67] in how trust is conceived and operationalized in DPI development. Too often, trust is treated as something that will follow once systems are rolled out and benefits materialize. The opposite is also true: where trust is absent at the design stage, DPI adoption stalls, resistance grows, and harms accumulate, often borne disproportionately by those with the least power to contest them. Trust cannot be assumed as an outcome of technological deployment; it must be deliberately built into systems through human-centric inclusive design, transparent governance, accountability mechanisms, and robust safeguards for security and human rights.

Box 6. Learning from trust challenges in DPI rollouts

In October 2021, the Central Bank of Nigeria launched the eNaira, making Nigeria the second country in the world, after the Bahamas, to introduce a fully public central bank digital currency (CBDC).[68] While the initiative was driven by ambitious goals around financial inclusion and innovation, early uptake remained limited, with many wallets inactive. Concerns around privacy, particularly perceptions of surveillance linked to anti–money laundering features, combined with usability challenges, affected public confidence and adoption.[69] A parallel illustration can be seen in France's experience with the *Alicem* digital identity initiative,[70] which highlights how questions around core design choices, transparency, and user trust can slow adoption even in high-capacity institutional settings. Together, these cases underscore the importance of addressing trust-related considerations early in the design and testing of DPI, and of creating spaces for iterative learning and engagement before and after systems are deployed at scale.

[64] UNDP (2023), *Accelerating the SDGs through Digital Public Infrastructure: A Compendium of the Potential of Digital Public Infrastructure*, UNDP.

[65] Anri van der Spuy, Bhandari V.,Trikanad S., Tshering Paul Y. (2021), *Towards the Evaluation of Socio-Digital ID Ecosystems in Africa: Comparative analysis of findings from ten country case studies*, Centre for Internet and Society (CIS), and Research ICT Africa (RIA)

[66] Ibid

[67] World Economic Forum. (2024). *Technology policy: Responsible design for a flourishing world*. White Paper, Global Future Council on the Future of Technology Policy.

[68] Ree J. (2023), *Nigeria's eNaira, One Year After*, International Monetary Fund.

[69] Ibid.

[70] Vitard A . (2019), *Alicem will be deployed as early as November despite the criticism*, The Digital Factory.

Key DPI challenges for sandbox-based learning

Trust in DPI is multi-layered.[71] It is continuously shaped not only by participation, legal safeguards, and institutional legitimacy, but also by how systems manage data, integrate AI, ensure cybersecurity, account for long-term sustainability, and operate across borders. These elements do not function independently and are not one-off boxes to check. Design choices made in one area often have cascading effects across others, shaping how DPI is perceived, adopted, and contested over time. Sandboxes cannot resolve all governance challenges, but experimentation, grounded in iteration, transparency, and collective learning, can provide a structured way to surface trade-offs, test safeguards, and generate actionable evidence on areas for improvement before and after roll out.

The sections below outline key DPI challenges and explore how they could be addressed through sandbox-based experimentation.

Rights and inclusion

Trust in DPI is deeply tied to the protection of fundamental rights and the inclusion of diverse populations in system design, deployment and governance.[72] These safeguards cannot rely solely on post-hoc enforcement. Once DPI systems are embedded into institutional practice and service delivery, rights violations become significantly harder to detect, contest, and reverse. Decisions made at early design and deployment stages, which are often framed as technical or operational, can lock in exclusion, surveillance, or discrimination at scale, as has been witnessed in the deployment of several digital identities systems.[73]

Poorly governed DPI can hard-code bias and exclusion into foundational systems. Failures in identity systems can prevent access to healthcare or social protection; opaque data-sharing arrangements can enable surveillance without meaningful oversight; and weak grievance mechanisms can leave individuals without recourse when errors occur. As DPI expands across sectors and populations, these risks intensify.

Sandboxes provide a means to surface such issues early and iteratively by testing DPI use cases with diverse user groups and institutional settings, allowing governments to identify who is left out, why, under what conditions and whether any new risks are emerging. A sandbox also potentially enables innovators to start considering how they support inclusion early on in developing solutions if they're outside government but using DPI infrastructure to deliver their services.

---

[71] Rozo-Paz, M. (2025). *TrustStack: filling the marble jar of digital trust*. Datasphere Initiative.

[72] Rozo-Paz, M., Smye, J., Panda, S. (2023). Enhancing Inclusion in Digital Identity Policies and Systems: An Assessment Framework. Berkman Klein Center on Internet and Society at Harvard University.

[73] Anri van der Spuy, Bhandari V.,Trikanad S., Tshering Paul Y. (2021), *Towards the Evaluation of Socio-Digital ID Ecosystems in Africa: Comparative analysis of findings from ten country case studies*, Centre for Internet and Society (CIS), and Research ICT Africa (RIA)

When intentionally designed, sandboxes also create space for stakeholders such as civil society - whose participation in DPI has often been peripheral or consultative rather than embedded[74] - to engage in DPI experimentation, scrutinize risks, advocate for human rights protections, ensure that emerging technologies align with public values and guarantee that underserved and underrepresented communities' perspectives are heard.[75]

For instance, Indonesia's regulatory sandbox for the E-malaria Program was developed through a participatory action research process that brought together regulators, health officers, innovators, academics, and community stakeholders to jointly design the sandbox model and guidelines.[76] Supported by the Ministry of Health, this process enabled diverse voices to shape how digital health innovations for malaria elimination would be tested under regulatory supervision.

In this way, intentionally inclusive sandboxes can function as governance interventions that challenge dominant assumptions about "average users" and focus on how rights protections, inclusion measures, and redress mechanisms function at the level of service access and institutional practice, before exclusion becomes systemic, and as a mechanism for monitoring and improvement if exclusion is identified after deployment.

Data and AI

The growing interdependence between DPI and AI introduces additional layers of risk and opportunity.[77] AI is no longer simply layered onto DPI as an optional enhancement; it is often embedded within core DPI functions, shaping how public services are delivered, decisions are made, and individuals are recognized, assessed, or targeted. AI is considered capable of significantly enhancing DPI through multilingual interfaces, speech recognition, personalization, fraud detection, and predictive analytics, improving accessibility and efficiency, particularly in diverse and resource-constrained contexts. At the same time, it can amplify existing bias, opacity, and exclusion.

DPI provides the data foundations, interoperability, and institutional scaffolding that AI systems require to be context-appropriate, accountable, and rights-respecting. In this regard, rights-related risks arise less from service delivery alone and more from how automated decision-making, data flows, and model design choices interact across DPI layers. This AI-DPI integration unfolds across multiple layers of technical and governance stacks: decisions taken at foundational layers such as digital identity systems, data exchange mechanisms, or eligibility determination, can propagate risks across downstream, AI-enabled applications.

---

[74] Onyango R. (2025), DPI can be transformative for Africa's digital future. Civil society has a critical role to play. Digital Impact Alliance

[75] Datasphere Initiative (2025) *Sandboxes for AI: Tools for a new frontier*, Datasphere Initiative.

[76] Fuad A, Tiara A, Kusumasari RA, Rimawati R, Murhandarwati EEH. (2023) Introducing a Regulatory Sandbox Into the Indonesian Health System Using e-Malaria as a Use Case: Participatory Action Study. J Med Internet Res. 2023 Dec 5;25:e47706.

[77] Sengupta, A., Barbosa, A. C. ., & Samdub, M. T. (2025). Understanding interrelationships between AI and digital public infrastructure (DPI) in India and Brazil. *The African Journal of Information and Communication (AJIC)*, 35, 1-11.

Sandboxes offer a structured space to examine these interactions before they become entrenched. Sandboxes allow governments and stakeholders to collaboratively develop new standards and test how AI-driven DPI functions interact with rights, institutions, and social realities in specific contexts - whether municipal, national, or regional. This supports evidence-based assessments of viability, risk, and distributional impact, informing proportionate and scalable safeguards that can evolve alongside technology. Rather than an inclusion-focused analysis, sandboxes in this context can enable early scrutiny of automated bias, opacity, privacy risks, and accountability gaps before AI-driven practices become difficult to reverse.[78]

Cybersecurity and resilience

As DPI becomes more interconnected and population-scale, it also introduces significant cybersecurity and privacy risks, particularly with respect to long-term data protection, system interoperability, and governance oversight.[79] As countries connect more services and users, the system's "attack surface" expands, increasing exposure to a range of threats, including ransomware, service disruption, and data breaches.[80] As a consequence, cybersecurity failures in DPI do not only compromise data; they directly erode trust in public institutions and can rapidly stall adoption of digital public services.

Sandboxes can help test security controls, incident response mechanisms, and governance arrangements under simulated or limited-risk conditions. This enables governments to identify vulnerabilities, clarify roles and responsibilities, and strengthen institutional preparedness before failures occur at scale.

Sustainability and environment

The expansion of DPI carries significant environmental and social consequences[81] that extend far beyond system operation. In high-income countries, DPI growth drives energy-intensive data centres, cooling systems, and network infrastructure, increasing electricity and water demand and contributing directly to greenhouse gas emissions. At the same time, the physical foundations of these systems: batteries, servers, devices, and transmission networks,[82] depend on minerals such as cobalt, manganese, lithium, and graphite,[83] which are extracted primarily in developing countries. This creates a pronounced global imbalance: while high-income countries reap the benefits of accessible, efficient digital services,

[78] For more information on AI sandbox examples see: Sandboxes for AI: Tools for a new frontier.

[79] Joseph, Mtakai. (2026). Cybersecurity Implications of Digital Public Infrastructure (DPI) Rollouts in Emerging Economies: A Kenya Huduma Namba Case Study. ResearchGate.

[80] Pswarayi-Riddihough I, Ghislain de Salins, Eichholtzer M. (2025), Resilient, secure and trusted: The next frontier for Digital Public Infrastructure, World Bank Blogs.

[81] Office of the United Nations Secretary-General's Envoy on Technology (2024), Leveraging DPI for Safe and Inclusive Societies: Interim Report, UNDP.

[82] UNCTAD (2024), Digital Economy Report 2024: Shaping an environmentally sustainable and inclusive digital future. UNDP.

[83] Ibid.

resource-rich developing countries bear disproportionate environmental and social costs, including deforestation, water contamination, ecosystem degradation, and labor-intensive extraction with limited local value capture.[84]

Sandboxes offer a way to create controlled environments to test energy-efficient architectures, renewable energy integration, alternative cooling methods, and transparent reporting of environmental footprints. They can also support experimentation with policies that align DPI deployment with domestic energy and sustainability goals, helping governments explore trade-offs across the DPI lifecycle and generate context-specific evidence for more responsible strategies.

Recent developments in Moldova[85] illustrate this potential: in July 2024 Parliament adopted legislation establishing regulatory sandboxes for energy production, distribution, and consumption.[86] The law provides a legally sanctioned, time-bound testing environment, allowing temporary and targeted exemptions from selected regulatory and fiscal requirements to support innovation aligned with a just energy transition. In doing so, the framework opens space for ''green'' DPI sandboxes in sustainable energy, including the integration of low-carbon gases into renewable gas networks, the deployment of smart grids, and the integration of renewable energy sources.

Cross-border challenges and digital sovereignty

As DPI scales, it increasingly operates across jurisdictions, linking people, services, and data flows beyond national borders. This creates a dual governance challenge. On the one hand, DPI requires cross-border interoperability: alignment of technical standards, mutual recognition of credentials, coordinated oversight, and shared approaches to data governance. On the other hand, the development of DPI is often linked to a country's efforts to establish and extend sovereign control over digital systems.[87]

Governments are under growing pressure to assert digital sovereignty and strategic autonomy over systems that are foundational to public service delivery, national security, and economic resilience. Since the release of the report *We Need To Talk About Data*[88] by the Internet & Jurisdiction Policy Network in 2022, which pointed to the risk of polarization and of using "sovereignty" as a catch all policy, pursuits towards digital or data sovereignty have been on the rise. Thought leaders in the Global South, such as Kapoor have documented increasing

[84] Brown C., Boyd D., Kara S. (2022), Landscape Analysis of Cobalt Mining Activities from 2009 to 2021 Using Very High Resolution Satellite Data (Democratic Republic of the Congo), MDPI.

[85] UNDP (2024), The new sandbox law on the development of innovative solutions in the energy sector has been adopted by Parliament. UNDP.

[86] Ibid.

[87] Eaves, D., Rao, K. (2024). What is Digital Public Infrastructure and why does it matter? World Economic Forum.

[88] De La Chapelle, B. and L. Porciuncula (2021). We Need to Talk About Data: Framing the Debate Around Free Flow of Data and Data Sovereignty. Internet and Jurisdiction Policy Network

instances of sovereignty seen through the lens of statehood and national security rather than through the rights of people to exert their own agency.[89] Beyond limited definitions of localization only, others have also sought to frame digital sovereignty as digital self-determination, highlighting it not as an effort of technical isolation, but as the active building of national capacities that ensure the autonomy of decision-making and the protection of national strategic interests.[90]

DPI is increasingly entangled with such questions of digital sovereignty - the ability of governments to govern data, software, infrastructure, and public services within their borders while maintaining strategic autonomy in a globally interconnected ecosystem.[91] In practice, sovereignty is not only about national legislation or localization; it also encompasses broader questions of resilience, agency, and the capacity to shape public systems amid geopolitical competition, global supply chain dependencies, and the dominance of proprietary technologies.[92]

Many DPI systems today rely heavily on foreign cloud providers, proprietary platforms, and non-open standards.[93] This dependence can constrain governments' ability to make autonomous decisions, expose critical infrastructure to external legal or political pressures, and entrench technological power imbalances. Vendor lock-in often manifests through long-term contracts with limited flexibility, high costs, and limited adaptation to local contexts. Surveys from ID4Africa show that national identity authorities rank vendor lock-in as a top concern, because it directly affects their ability to maintain control over systems and safeguard citizen data.[94]

It should be noted that sovereignty concerns are not limited to the Global South or low- and middle-income countries. In the current geopolitical climate, European states, including France, Germany, Denmark, Estonia, and Finland, are pursuing digital autonomy to reduce reliance on foreign technology.[95]

These dynamics are not contradictory, but they are often treated as such. In practice, DPI development must navigate the tension between enabling cross-border collaboration and preserving the ability of states to govern critical digital systems in line with public values, rights, and domestic priorities.

[89] Kapoor, A. (2025). Whose sovereignty is it anyway? UNDP.

[90] Jiang M, Belli L, eds. (2025). *Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance*. Cambridge University Press.

[91] OECD (2021), Development Co-Operation Report 2021: Shaping A Just Digital Transformation. OECD.

[92] Microsoft (n.d), Digital Sovereignty.

[93] Ibid.

[94] OECD (2021), Development Co-Operation Report 2021: Shaping A Just Digital Transformation. OECD.

[95] Joos T. (2025), Cloud Sovereignty: How Berlin and Paris Are Trying to Draw a European Line, InCyber News

Sandboxes can provide structured spaces to explore the tension between cross-border DPI collaboration and national digital sovereignty. Sandboxes could allow governments, regulators and other actors to test interoperability standards, mutual recognition arrangements, and coordinated oversight mechanisms across jurisdictions without committing to irreversible policy or infrastructure choices. This is particularly important where DPI ambitions extend beyond national borders, such as in regional identity frameworks, cross-border payments, or data-sharing initiatives.

Sandboxes also provide a practical mechanism to navigate complex trade-offs without retreating into isolation or rigid localization mandates. They enable governments to stress-test vendor dependencies, evaluate alternative system architectures, and experiment with configurations that balance resilience, local agency, and interoperability. When designed with cross-border dimensions, sandboxes can support collective sovereignty through shared standards, reciprocal safeguards, and coordinated governance arrangements.

Ultimately, sandboxes help move debates on digital sovereignty from abstract or symbolic claims toward evidence-based, pragmatic strategies. By surfacing legal, technical, and institutional frictions early, they enable authorities to protect national interests, uphold citizen rights, and sustain trust in DPI within an interconnected digital landscape. In this sense, sandbox-based learning can be a core component of effective DPI governance before systems are deployed at scale.

Sandboxes as laboratories for co-creation to support trust-building

If designed inclusively and implemented effectively DPI sandboxes can create controlled environments to test not only technical functionality, but also governance choices, cybersecurity controls, and accountability arrangements before systems are deployed at scale.

Sandboxes cannot guarantee success, but they can mitigate silent failures that erode trust and legitimacy. While the opportunities and risks around trust-building are dependent on historical, political and cultural contexts, sandboxes can help investigate assumptions, surface risks, test safeguards and co-create human-centric solutions.

Sandboxes also offer an opportunity to operationalize rights protections in practice. Within sandbox environments, elements such as consent models, data minimization strategies, redress mechanisms, transparency requirements, and oversight arrangements can be stress-tested under realistic conditions. This enables policymakers, regulators, and implementers to examine how rights safeguards function across different populations, use cases, and institutional settings, and to identify unintended consequences early.

Sandboxes can make collaboration tangible by offering a structured co-creation space where government entities, civil society organizations, technologists, and private companies can test interoperability, values alignment, and co-design in action, ensuring each actor's agency, decision-making power and contributions are respected. The upcoming section identifies the incentives and risks stakeholders may face when designing and collaborating in DPI sandboxes.

Why and for whom? Understanding stakeholder incentives in DPI sandboxes

Public sector

Governments occupy both the moral and operational heart of DPI. They define the legal frameworks that govern data, identity, and digital service delivery; they allocate public resources to build and maintain core systems; and they bear ultimate responsibility for inclusion, accountability, and trust. Countries such as India[96] and Estonia[97] have shown what DPI can achieve. India's Aadhaar identity system and Unified Payments Interface (UPI) have together reshaped financial inclusion and digital service delivery for over a billion people, creating a foundation upon which both government and private services are built. Estonia's X-Road platform,[98] developed by government agencies and stewarded through a multi-stakeholder governance model, enables secure data exchange between public and private systems, reducing duplication and improving citizen access to services.

However, governments routinely encounter deep challenges as they move from isolated pilots to full-scale DPI deployments. The institutional incentives and constraints governments face can make the use of sandboxes neither automatic nor straightforward.

Public authorities are frequently under pressure to deliver large-scale, citizen-facing systems quickly, often within rigid procurement rules, political timelines, and limited fiscal space. Coordination across ministries and sectors is notoriously difficult; fragmentation that can result in siloed approaches to standards, conflicting mandates, and gaps in accountability.

At the same time, DPI systems carry high stakes for public trust, constitutional rights, and political accountability, even as many governments grapple with how to govern emerging risks associated with advanced technologies - from algorithmic bias and exclusion to data misuse and cybersecurity vulnerabilities - within the context of national DPI. These pressures can make public institutions risk-averse, discouraging experimentation even where uncertainty around technical design, governance arrangements, or societal impact is high.

[96] Sánchez-Cacicedo A. (2024), *India's Digital Public Infrastructure: a Success Story for the World?*, Institut Montaigne.

[97] Digital Frontiers (2022), *Estonian Case – The development and promotion of Digital Public Infrastructures*, Observer Research Foundation.

[98] e-Estonia (n.d.), X-road - Interoperability services, e-Estonia.

Sandboxes provide governance innovation[99] precisely calibrated to these challenges. By operating within a clearly defined scope, time horizon, and governance framework, sandboxes allow governments to test DPI components, regulatory interpretations, or cross-agency coordination mechanisms without committing to irreversible policy or infrastructure decisions.[100] They provide a safe environment for regulators and delivery agencies to learn from real-world use,[101] surface implementation challenges early, clarify capabilities and mandates, and adjust rules or standards based on evidence rather than assumption. This is particularly valuable where formal legal frameworks are still evolving or where institutional roles and responsibilities remain contested.

As mentioned previously, Moldova adopted legislation establishing regulatory sandboxes for energy production, distribution, and consumption, opening space for future "green DPI" experimentation such as smart grids, renewable integration, and data-enabled energy management within a legally sanctioned, time-bound framework. By permitting real-world experimentation within clearly defined boundaries, Moldova's example signals a move toward more adaptive, evidence-informed regulation, rather than rigid, one-size-fits-all approaches.

Another key benefit for the public sector is the opportunity to engage directly and iteratively with other stakeholders under controlled conditions. Sandboxes can reduce adversarial dynamics by shifting interactions with private firms and civil society from compliance-driven oversight to collaborative problem-solving.[102] They also create a documented evidence base that public officials can use to justify regulatory choices, defend design decisions, and communicate transparently with political leaders and the public. In this sense, sandboxes do not weaken regulatory authority; rather, they strengthen it by grounding decision-making in tested practices, shared learning, and demonstrable safeguards.

Private sector

As is the case in the development of many layers of technological development, private sector participation in DPI is uneven and often shaped by patterns of market concentration that can significantly influence how public infrastructure is used, governed, and valued. In several countries, large firms with substantial capital, technical capacity, and existing market power have been able to integrate early and deeply into DPI systems, often with deep dependency mechanisms solidified through contractual clauses. Their early entry can allow them to gather valuable data and shape technical standards, interoperability practices, and even user expectations in ways that reinforce their dominance, effectively turning open public infrastructure into de facto proprietary ecosystems.

---

[99] Appaya, M. S., Gradstein, H. L., & Haji Kanz, M. (2020). *Global Experiences from Regulatory Sandboxes*, World Bank; Appaya and Haji (2020), *Four years and counting: What we've learned from regulatory sandboxes*, World Bank Blogs.

[100] Fintech Notes No. 8 (2020), *Global Experiences from Regulatory Sandboxes, Finance, Competitiveness and Innovation Global Practice*, World Bank Group.

[101] Organisation for Economic Cooperation and Development (2022), *Harnessing the power of AI and emerging technologies*, OECD Digital Economy Papers.

[102] Crampes, C., & Estache, A. (2023), *Efficiency vs. equity concerns in regulatory sandboxes*, Toulouse School of Economics.

In India, while UPI was deliberately designed as an interoperable payment infrastructure,[103] its rapid adoption led to the concentration of transaction flows among a small number of private applications.[104] As UPI became the backbone of everyday digital payments, this growing dependence exposed structural concentration within the ecosystem, raising concerns about systemic risk. Although UPI is institutionally decentralized by design, in practice its use has become heavily dominated by a few private applications such as PhonePe and Google Pay.[105] This concentration has prompted questions about operational resilience, digital sovereignty, cybersecurity exposure, competitive neutrality, and the capacity of regulators to effectively oversee risks that emerge when critical public payment infrastructure is mediated by a limited number of private actors.

In such cases, large firms do not merely build on DPI; they shape usage patterns, pricing power, and innovation pathways, sometimes narrowing the diversity of services and actors that can realistically participate.

For smaller firms and start-ups, these concentration dynamics are compounded by structural barriers that make meaningful participation in the digital economy, including DPI, particularly difficult – sandboxes therefore can provide a path forward. Integrating with national identity systems, payment rails, or data-sharing frameworks often requires significant upfront investment in security, compliance, and specialised technical expertise,[106] long before any commercial return is likely. In India's DPI ecosystem, while a handful of well-capitalized fintechs have successfully scaled on top of Aadhaar and UPI, many smaller start-ups have struggled with onboarding requirements, certification costs,[107] and frequent changes to technical standards. Comparable challenges have emerged in Australia's Consumer Data Right regime, where smaller firms and fintechs have reported difficulty keeping pace with complex accreditation processes and compliance obligations,[108] even as large banks and technology providers are better resourced to absorb these costs.

The result is a reinforcing cycle which is not unique to DPI: dominant firms are able to engage early, influence standards, and scale quickly, while smaller and potentially more innovative actors are delayed, excluded, or pushed into narrow niches. This imbalance not only distorts competition and market dynamics but also undermines the broader public-interest objectives of DPI, strengthening the case for sandbox mechanisms that can lower entry barriers for public interest innovations, diversify participation, and prevent patterns of exclusion from becoming locked into public infrastructure by default.

---

[103] Sen J. (2025), India's Unified Payments Interface (UPI) system and its transformative impact P.35, Systemic Risk Centre Discussion Paper No 131.

[104] Desai H., Mukhija K. (2026), UPI Market Concentration: Is India's Payment Infrastructure too Centralized to Fail? AMLEGALS

[105] Desai H., Mukhija K. (2026), UPI Market Concentration: Is India's Payment Infrastructure too Centralized to Fail? AMLEGALS

[106] Amagarat F. (2025), Building a Foundation for Digital Public Infrastructure in Financial Services, AfricaNenda

[107] Ratan A. (2024), How fintechs can address the rising challenge of compliance costs, YourStory.

[108] Hilton A., Zaurrini R., McGrath G. (2024), Resetting Australia's Consumer Data Right, Ashurst.

Sandboxes directly address these dynamics by creating structured, time-bound, and supervised environments in which a wider range of actors, including smaller firms and early-stage innovators, can engage with DPI at an early stage, without committing to full-scale deployment or exposing themselves to immediate enforcement action; which lowers the technical, financial, and regulatory thresholds that typically advantage dominant incumbents. For firms working with identity, payments, or data-sharing infrastructure, this enables early testing of authentication flows, consent mechanisms, liability models, and interoperability standards in collaboration with regulators and DPI operators, rather than relying on isolated interpretations of evolving requirements. Additionally, in contexts where formal regulations are still taking shape, sandbox participation also provides smaller actors with early visibility into likely policy directions, helping them align product design with emerging legal expectations and reducing the risk that DPI standards are effectively set by incumbents before broader participation becomes possible.

Beyond risk mitigation, sandboxes can function as spaces for collaboration with public sector organizations, academia or NGOs. Firms that participate in DPI sandboxes may gain access to shared datasets, compute, technical support, or proof of concept validation processes that would otherwise be unavailable, particularly to smaller actors. Successful participation can serve as a signal to investors, customers, and public authorities that a company's solutions have been tested against public-interest safeguards and real-world constraints. Over time, this can help shift private-sector engagement in DPI away from ad hoc pilots or privileged partnerships toward more open, competitive, and accountable ecosystems.

In this sense, sandboxes can reshape the conditions under which companies engage with public infrastructure, enabling private innovation to scale in ways that reinforce trust, inclusion, and long-term system resilience rather than undermining them. While an objective of DPI sandboxes can be to provide regulatory guidance, data access may be more attractive to smaller firms. Meanwhile, larger multinationals may see benefits in DPI sandboxes that boost tech adoption for smaller firms in their supply chains or provide opportunities for contributing to standard setting processes.

Civil society

Civil society organizations (CSOs) play a distinctive and indispensable role in the governance of DPI by acting as intermediaries between technical systems and their societal consequences. Unlike public authorities or private firms, civil society actors may represent communities most affected by DPI deployments, including populations exposed to exclusion, surveillance, or administrative harm. Across jurisdictions, CSOs have engaged in DPI-related processes by scrutinizing digital identity systems, monitoring the use of data in public service delivery,[109] and shaping public narratives around consent, accountability, and redress.

[109] Onyango R. (2025), The People's Network: Civil Society Organizations in Digital Public Infrastructure Development in Africa, Digital Impact Alliance.

In Uganda, civil society organizations such as the Initiative for Social and Economic Rights (ISER) and Unwanted Witness[110] have played a critical role in documenting and responding to failures in DPI. Their research and advocacy revealed that the rollout of the National Digital ID system (Ndaga Muntu) resulted in the exclusion of more than 23 percent of eligible citizens from accessing health and social services due to identity verification failures.[111] These impacts were not evenly distributed; refugees, stateless persons, and rural populations were disproportionately affected, illustrating how weaknesses in DPI design and implementation can translate directly into the denial of fundamental rights.

At the global level, civil society networks have also played a formative role in articulating shared principles for DPI, particularly in relation to human rights, inclusion, and accountability. Organizations engaging through multilateral processes, including those linked to UN agencies and global digital cooperation initiatives, have pushed for DPI frameworks that go beyond efficiency and scale to address issues such as data protection and minimization,[112] meaningful consent, grievance redress, and oversight.[113]

Despite these contributions, civil society participation in DPI governance remains structurally constrained and frequently reactive. CSOs are often brought into policy processes late, after core design choices have already been made and when systems are nearing deployment. Many organizations lack sustained access to technical documentation, test environments, or decision-making forums where infrastructure standards are set, limiting their ability to influence outcomes in meaningful ways. Resource constraints further exacerbate this challenge, particularly in low- and middle-income countries where civil society groups may be expected to engage with complex digital systems without commensurate funding or technical support.

Sandboxes offer a structural response to this governance gap by embedding civil society participation directly into the experimentation and learning phase of DPI development. They enable CSOs to engage proactively rather than reactively. Within such environments, civil society actors can observe how DPI components function in practice, assess impacts on different user groups, and raise concerns grounded in empirical evidence rather than abstract principle.

For civil society, this evidence base enhances advocacy capacity and shifts engagement from oppositional critique toward collaborative and informed governance. For governments and private actors, it provides early warning signals and social validation that systems have been tested not only for technical performance but for societal impact.

---

[110] Cioffi K., Kiira A., Mukasa D., Nabwowe – Kasule A., Namusobya S., Nattabi V., Ray A., Sempala A., Christiaan van Veen. (2021), Chased Away and Left to Die: How a National Security Approach to Uganda's National ID Has Led to Wholesale Exclusion of Women and Older Persons, Center for Human Rights and Global Justice, Initiative for Social and Economic Rights, and Unwanted Witness.

[111] Cioffi K., Kiira A., Mukasa D., Nabwowe – Kasule A., Namusobya S., Nattabi V., Ray A., Sempala A., Christiaan van Veen. (2021), Chased Away and Left to Die: How a National Security Approach to Uganda's National ID Has Led to Wholesale Exclusion of Women and Older Persons, Center for Human Rights and Global Justice, Initiative for Social and Economic Rights, and Unwanted Witness.

[112] Almeida E., Martins P. (2025), Digital Identity and Digital Public Infrastructure: Recommendations For a Fair Information Architecture, Data Privacy Brasil.

[113] Airan A., Hodigere S., Sridharan S., Natarajan S. (2024), The Governance of Digital Public Infrastructure, Aapti Institute.

Box 7. Youth as DPI adoption accelerators[114]

Young people are often treated as end-users or beneficiaries of DPI, yet in practice they play a far more influential role in shaping how DPI is adopted, trusted, and sustained. Across many contexts, young people act as informal intermediaries between digital systems and wider communities. For instance, behind the adoption of a digital payment application, an online government service, or a digital identity credential by an older adult or a first-time user, there is frequently a young person explaining how the system works, troubleshooting errors, and signaling that it can be trusted. In environments where fear, misinformation, or past experiences of exclusion undermine confidence in public digital systems, these everyday acts of guidance and reassurance can be decisive for uptake.

This dynamic suggests a broader governance insight: young people are not only affected by DPI, they actively mediate its social legitimacy. Their position as early adopters, digital translators, and community connectors makes them powerful "trust spreaders" within families, peer networks, and local communities. When young people understand, question, and help shape how DPI systems function, they can accelerate adoption and normalize use in ways that formal awareness campaigns or top-down mandates often cannot. Conversely, when young people distrust or feel excluded from these systems, skepticism can propagate just as quickly.

Despite this, young people are rarely engaged as core stakeholders in the design and testing of DPI. Sandboxes offer a concrete mechanism to change this. By involving young people directly in sandbox experimentation, through usability testing, co-design, feedback loops, and governance discussions, DPI developers can surface adoption barriers, concerns, and unintended impacts early, before systems are scaled. This understanding also draws on Datasphere's youth engagement practice, including the Youth4Data Lab Toolkit, which has shown how equipping young people to critically engage with data-driven systems enables them to articulate trust concerns and act as effective intermediaries between digital technologies and their communities. This rationale is not only grounded in human rights and intergenerational justice, but also in effectiveness: experimentation that meaningfully includes young people is more likely to result in DPI systems that are understood and actively used across generations.

An emerging example of this approach is the COR Sandbox, which focuses on online redress mechanisms for children and intentionally involves children as core stakeholders within the sandbox itself. Rather than treating children solely as protected subjects, the COR Sandbox recognises them as knowledgeable users of digital systems with unique insights into how grievance, reporting, and redress mechanisms function in practice.[115] While the focus of the COR Sandbox is on digital services provided by market players, this model illustrates how sandboxes can move beyond consultation toward shared experimentation, offering a template for how youth engagement could be embedded more systematically across DPI sandboxes.

[114] Rozo-Paz, M (2026), Why digital public infrastructure needs a youth-centered trust strategy, Datasphere Initiative.

[115] COR Sandbox (website).

Why not? The risks and limitation of a sandbox model

While sandboxes offer significant potential for DPI development, they hold several important limitations that must be acknowledged and addressed.

Challenges in meaningful stakeholder engagement

DPI systems affect multiple sectors, requiring broad participation from various regulators, civil society organizations, and affected communities. However, rallying these diverse stakeholders is already an uphill task, and ensuring meaningful engagement from civil society and affected communities can be neglected, especially in the face of limited resources.

Beyond simply bringing stakeholders to the table, establishing communication channels that reduce information asymmetries and enable effective collaboration presents a significant challenge. Different stakeholders often possess varying levels of technical understanding about DPI systems, regulatory processes, and sandbox methodologies. Without deliberate efforts to bridge these knowledge gaps through accessible communication and information sharing, participation can remain superficial even when stakeholders are nominally included.

This risk becomes particularly pronounced as stakeholder groups widen and sector representatives are expected to independently identify and engage relevant community groups. For instance, a representative from a Ministry of ICT running a DPI sandbox might engage ICT based community representatives while forgetting or not prioritizing others from health, education, and other sectors. Yet the DPI system being tested will be used across all these sectors, leaving critical gaps in representation and input.

To some extent, engaging all stakeholders requires starting with sensitization and knowledge building for them to effectively contribute to the process. This is additional work that, if not planned for from the outset, can become a challenge and consequently be neglected. When civil society and affected communities are excluded, or when communication channels fail to enable genuine understanding and collaboration, sandboxes risk reinforcing existing power asymmetries rather than democratizing DPI development.

Opacity and weak accountability mechanisms

Sandboxes require a comprehensive approach that includes clear documentation, monitoring and audit mechanisms in order to increase transparency throughout the testing process. However, when sandbox initiatives lack these comprehensive methodologies, they create accountability gaps even when this is not their intention.

Without clear documentation, monitoring and audit mechanisms the very flexibility that makes sandboxes valuable for innovation can also enable opacity if proper oversight structures are not embedded from the beginning. Sandbox procedures must ensure transparency by making visible not only successes but also failures, such as, unintended consequences, and potential harms to affected communities.

This challenge is compounded by the fact that sandbox methodologies are still evolving, particularly outside the financial sector where they originated. As sandboxes come in different forms and approaches evolve based on purpose and context, potential sandbox projects can get lost or overwhelmed by lack of clarity on how to implement transparent and accountable experimentation processes.

Governance gaps post-sandbox and pathways to institutionalization

Insights generated during experimentation are often lost if there is no pathway to institutionalization, policy reform or technical adjustments or integration. This relates directly to comprehensive sandbox planning that anticipates the transition from testing to lesson learning and the embedding of outcomes into DPI development and implementation processes for the future.

A critical challenge is the establishment of monitoring systems that enable continuous data collection and iterative learning processes throughout and beyond the sandbox period. Without clear mechanisms for continuous improvement, sandboxes may function as one time experiments rather than ongoing learning environments. The absence of systematic monitoring means that opportunities to refine and adapt based on emerging evidence are missed, and valuable insights that could inform evidence based regulations and guidelines goes unused.

Resource intensity and competing deliverables

Setting up DPI systems can already feel rushed as authorities work to meet their digital transformation goals. Countries often have targets to meet, and this can pose a challenge to sandboxes achieving their effective potential even if they were deployed.

In the first place, sandboxes require additional time, human resources, and financial investment, which in the eyes of someone meeting a deadline can appear as a delay to implementation. As established above, sandboxes are most beneficial when they are used as a learning tool requiring extensive documentation of not just the outcomes but also the processes that go into the testing. This is extra work that can compete with other pressing deliverables.

The tension between rapid deployment and thorough experimentation means that sandboxes may be rushed through or inadequately resourced, undermining their core purpose of enabling careful, iterative learning.

Determining if a sandbox is the right tool

These challenges and risks do not make sandboxes less suitable for DPI but rather highlight the complexity of implementing them effectively. They underscore the need to critically and comprehensively plan, design, implement and evaluate sandboxes in order for them to be worth the investment.

These challenges also present a useful starting point to reflect on other suitable alternatives to sandboxes that could be the right solutions for the challenge at hand. It is key to pause and ask whether a sandbox is actually the right tool, which requires careful reflection and assessment. Other approaches can provide controlled spaces for testing new technologies, products and services, including test beds such as UK's NHS Test Beds Programme,[116] living labs such as European Network of Living Labs (ENoLL)[117] and policy prototypes such as Meta's Open Loop program.[118]

To support this decision-making process, the OECD has proposed a structured suitability assessment (the "Sandbox Test"),[119] which offers a set of guiding questions to help policymakers assess whether a sandbox is the right regulatory or policy instrument to address a given problem, considering factors such as regulatory frameworks, stakeholder ecosystem, market and technology conditions, and benefits, risks and resources available. Tools such as this test can help ensure sandboxes are deployed strategically and are aligned with policy goals.

It is also useful to draw on complementary governance frameworks that broaden how experimentation, collaboration, and trust are operationalized within DPI. Aapti Institute's *DPI Governance Guide* responds to the relative underinvestment in DPI governance by providing lifecycle-wide guidance that goes beyond regulation and implementation alone.[120] The guide highlights collaboration and co-creation as a core governance principle (Principle 3),[121] emphasizing multi-stakeholder engagement across government, the private sector, civil society, open-source communities, and end users. To operationalize this principle, the guide outlines a diverse set of governance tools, including codified consultation processes, participatory feedback mechanisms, open and interoperable technical architectures, modular system design, and the establishment of expert committees and advisory bodies with broad stakeholder representation. Sandboxes are included as one such policy instrument and are situated alongside other mechanisms that embed transparency, accountability, and shared learning throughout the DPI lifecycle. Taken together, these approaches illustrate that controlled and iterative experimentation in DPI can be achieved through multiple governance pathways, reinforcing the importance of assessing whether a sandbox is the most appropriate tool for a given context or whether alternative co-creation mechanisms may better advance collaboration and public benefit.

[116] NHS England (n.d), NHS Test Beds Programme, Accelerated Access Collaborative

[117] ENoLL (n.d), European Network of Living Labs, ENoLL Association

[118] Open Loop (n.d), Open Loop Global Program, Meta

[119] OECD (2025). *Regulatory Sandbox Toolkit: A Comprehensive Guide for Regulators to Establish and Manage Regulatory Sandboxes Effectively*. OECD Technical Paper.

[120] Aapti Institute (n.d.) DPI Governance Guide (website).

[121] Aapti Institute (n.d.) Principle 3: Promote collaboration and co-creation towards and public benefit. DPI Governance Guide.

Where are sandboxes for DPI being deployed?

This section presents a global mapping of existing initiatives that function as sandboxes for DPI, including those explicitly branded as DPI sandboxes as well as sandbox environments that enable controlled testing of core DPI components. Together, these three perspectives offer a grounded view of where DPI experimentation is happening, how it is evolving, and what it reveals about building inclusive, interoperable, and trustworthy DPI.

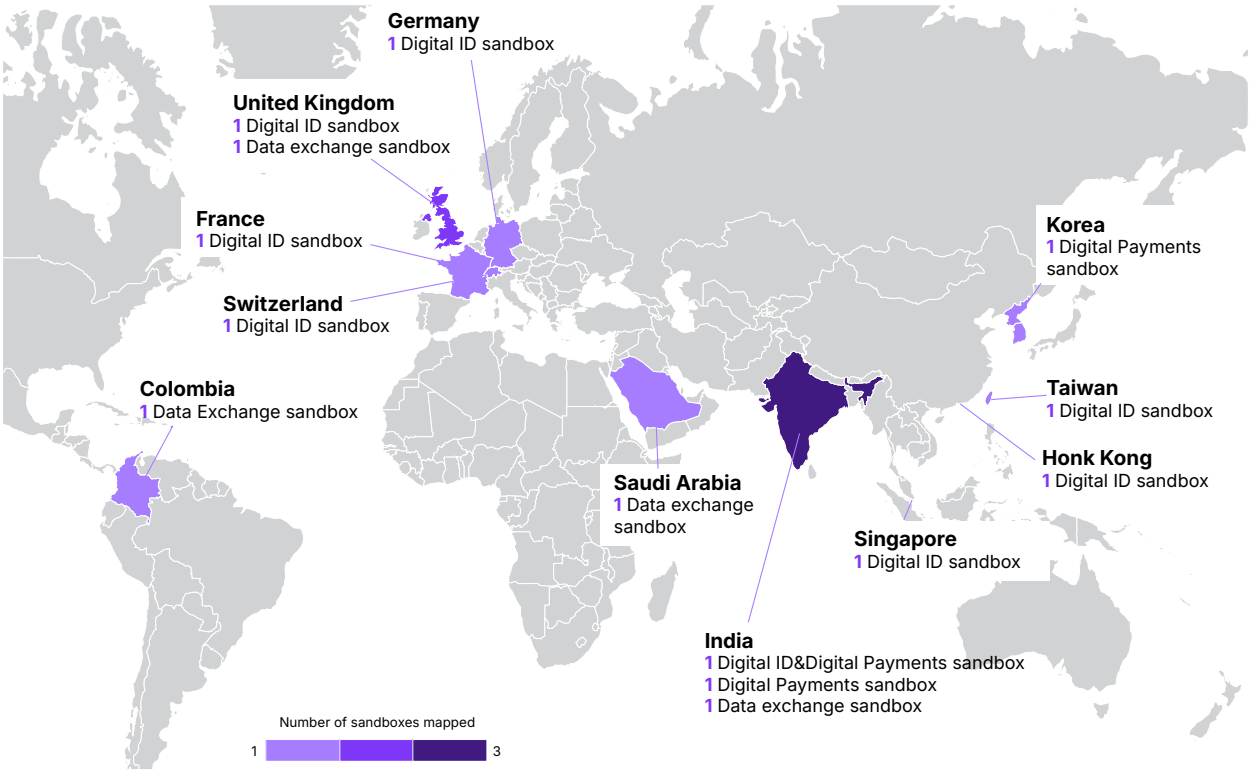
DPI Sandboxes global overview

As elaborated on page 26, DPI sandboxes are defined as: sandboxes that are designed to test, pilot, or operationalize technologies, standards, or governance arrangements within at least one DPI layer.

The section begins with a global map that visualizes the distribution and characteristics of DPI sandboxes across regions (Figure 1) and a detailed table of identified initiatives (Table 1), alongside the methodology used to classify them, accompanied by a note on the methodology used to classify sandbox cases as DPI sandboxes (Box 8). It then synthesizes key trends observed across the ecosystem. Together, these elements offer a snapshot of an ecosystem in formation that is increasingly central to how countries experiment with trust, interoperability, and governance in the development of DPI. Rather than presenting a single model, the overview reveals a diverse and uneven landscape: sandboxes vary widely in scope, institutional leadership, maturity, and objectives, reflecting different stages of digital transformation.

The map below shows 11 jurisdictions in which the Datasphere Initiative has identified DPI sandboxes. Those are: Colombia, France, Germany, Hong Kong, India, Korea, United Kingdom, Saudi Arabia, Singapore, Switzerland and Taiwan. India has three identified sandboxes, the United Kingdom has two, and all other jurisdictions have one sandbox each. Each one of these are examples of sandboxes, in addition to two examples of multi-country sandboxes implemented in the European Union, are listed in Table 1 where their name, lead institution, status, DPI layer, and description is further detailed.

Figure 1. A global snapshot of DPI sandboxes



Note: This is a mapping of 14 national sandboxes. It does not include the regional sandboxes such as the European Digital Wallet and EU Interoperability Regulatory Sandbox Hub.

Box 8. Methodological note on DPI sandboxes

For the purposes of this report, the mapping and analysis focus on DPI sandboxes as a specific category of experimentation and testing initiatives. The database used to produce this mapping was the Dataphere Initiative's Sandbox Inventory, which currently includes 200+ catalogued sandboxes worldwide. The search was not restricted to a specific time period, nor did it start from the first use of the term "DPI". Instead, the focus was placed on the objective of the sandboxes rather than on the terminology itself. For this reason, sandboxes developed before the term DPI became widely used were also included.

Across the mapping, a limited number of such sandboxes that have supported DPI were identified.[122] Most are financial or sectoral regulatory sandboxes, where experimentation has focused on innovations built on top of national digital payment or data infrastructures. Examples include the Brazilian Central Bank's Regulatory Sandbox, which enabled supervised experimentation with solutions interacting directly with Pix, Brazil's national instant payment system;[123] selected cases within South Korea's financial and ICT regulatory sandboxes, where public institutions tested financial data exchange through government-led platforms such as MyData;[124] and the Bank of Thailand's Regulatory Sandbox, which has supported controlled experimentation on digital payment use cases like the Digital RD Project linked to Thailand's national payment infrastructure.[125] While these initiatives generate valuable insights for DPI development, DPI is not their central or defining focus.

As such, sandboxes that are supporting DPI development are analytically relevant as contributors to DPI evolution, but are not classified in this report as DPI sandboxes unless experimentation on a DPI layer is an explicit and intentional component of the sandbox design.

"Explicit" in this context means that experimentation on a DPI layer is clearly articulated in at least one of the following: the sandbox's stated mandate or objectives; official documentation or public descriptions; or the defined scope of testing in at least one sandbox cohort or call for participation.

Accordingly, inclusion in this mapping (Table 1) is based not on whether an initiative is formally labeled a "DPI sandbox", but on whether testing and learning related to DPI layers constitute a core and deliberate focus of the sandbox itself. This approach allows the analysis to capture a diverse set of DPI sandboxes across regions and institutional settings, while maintaining conceptual clarity around what distinguishes DPI-focused experimentation from broader innovation or regulatory testing.

[122] Given the dynamic and rapidly evolving nature of digital public infrastructure (DPI) sandboxes, it is possible that not all relevant initiatives were identified at the time of analysis. Readers who are aware of additional sandbox experiences not included in this study are invited to contact the authors at info@thedatasphere.org, indicating the source of the example, so that the mapping may be updated accordingly.

[123] Central Bank of Brazil. Regulatory Sandbox.

[124] OneTrust (2023). South Korea: Government announces National My Data Innovation Promotion Strategy. OneTrust. Data Guidance.

[125] Bank of Thailand. (n.d.) List of Participants for Digital RD Project under the Regulatory Sandbox.

Table 1. DPI Sandboxes

Sandbox	Country	Lead	Status	DPI layer	Description
Data Sandbox Collaborative Space	Colombia	Ministry of Information and Communications Technologies of Colombia - Digital Government	Completed	Data Exchange	A government-led collaborative sandbox that enables Colombian public entities to pilot and test analytics and Big Data projects in a secure cloud environment, supporting experimentation with real public datasets to develop data-driven solutions to public and citizen challenges. *This sandbox enables national data exchange and interoperability capabilities.*
France Identité Sandbox Environment	France	France Identité	In operation	Digital ID	A Sandbox of France Identité to support early testing of PID presentation in proximity and online. The sandbox is designed for hands-on experimentation: presenting a PID to real verifiers, exploring user journeys, and validating concrete end-to-end flows ahead of the European Digital Identity Wallet deployment *This sandbox is part of the EU's and France's digital identity infrastructure.*
EUDI Wallet: SPRIND Sandbox	Germany	Germany's Federal Agency for Disruptive Innovation (SPRIND)	Announced	Digital ID	In this sandbox, selected relying-party organizations can test their systems and workflows against the government-issued wallet. SPRIND requires prospective wallet service providers to pass sandbox testing before moving to production, helping ensure the German wallet's technical robustness and regulatory compliance. *This sandbox is part of the EU's and Germany's digital identity infrastructure.*
CorpID Sandbox	Hong Kong	Hong Kong's Digital Policy Office	Announced	Digital ID	The CorpID Sandbox is a government-led testing environment that allows corporations and public bodies in Hong Kong to pilot a digital identity, enabling secure authentication and authorized online transactions through proof-of-concept applications before full platform rollout. *This sandbox is part of Hong Kong's digital identity infrastructure.*

Sandbox	Country	Lead	Status	DPI layer	Description
Aadhaar Sandbox	India	Unique Identification Authority of India (UIDAI)	In operation	Digital ID	India's Aadhaar (UIDAI) regulatory sandbox provides FinTechs and startups with a controlled environment to test and integrate Aadhaar APIs for e-KYC and authentication before market launch, accelerating digital identity and financial innovation. Launched in 2023, it supports new use cases aligned with India's digital financial inclusion strategy. *This sandbox supports India's national digital identity and digital payments infrastructure.*
RBI Digital Rupee (e-Rupee) Sandbox	India	Reserve Bank of India	Announced	Digital Payments	The RBI Retail CBDC Sandbox provides fintechs and banks with a regulated, real-world testing environment to experiment with India's digital Rupee, enabling the development of CBDC-enabled payment, wallet, and programmable finance solutions. Launched in 2025, it supports large-scale experimentation while ensuring compliance, security, and regulatory oversight. *This sandbox is part of India's digital payments infrastructure through the testing of a central bank digital currency.*
India Urban Data Exchange (IUDX) Sandbox	India	Ministry of Housing and Urban Affairs	In operation	Data exchange	IUDX's sandbox helps to connect the data generated by several Urban Local Bodies (50 cities have been onboarded) across the country to the users/consumers. Launched in 2018, it provides a data exchange platform to Indian cities. IUDX serves as a seamless interface for data providers and data users, including ULBs, to share, request, and access datasets related to cities, urban governance, and urban service delivery. *This sandbox enables India's data exchange and interoperability capabilities.*

Sandbox	Country	Lead	Status	DPI layer	Description
Sandbox Korea	Korea	Financial Services Commission (Korea)	In operation	Digital Payments	The Korean Financial Regulatory Sandbox provides a controlled environment in which public and private actors can test innovative financial services and data-driven solutions under temporary regulatory exemptions, with the aim of modernizing the financial system and fostering responsible innovation. Within this framework, Korea Credit Information Services (KCIS) - the country's public credit registry - tested the exchange of financial information through MyData, a government-led DPI that enables individuals to better control how their personal data is shared with public and private entities. The sandbox supports experimentation directly on core state-managed data infrastructures. *This sandbox supports experimentation on digital payments infrastructure.*
The European Digital Wallet	Multi-country (EU)	European Commission	In operation	Digital ID	Potential Playground (EU Digital Identity Wallets) is an open, collaborative interoperability test environment created by the France Identité team that allows technology providers to test and validate compliance with EU Digital Identity Wallet (EUDIW) standards, generate regulatory feedback, and support the scaling of interoperable digital identity solutions across Europe. *This sandbox is part of the EU's digital identity infrastructure.*

Sandbox	Country	Lead	Status	DPI layer	Description
EU Interoperability Regulatory Sandbox Hub	Multi-country (EU)	European Commission	In operation	Data Exchange	The Interoperability Regulatory Sandbox Hub is an EU initiative under the Interoperable Europe Act that provides a controlled environment for public authorities to test and validate cross-border interoperability solutions for digital public services, supporting policy experimentation, regulatory learning, and secure data sharing across the EU. *This sandbox enables cross-border data exchange and interoperability for EU digital public services.*
Tawakkalna Sandbox	Saudi Arabia	Saudi Data and Artificial Intelligence Authority (SDAIA)	In operation	Digital Payments	Saudi Arabia's SDAIA launched a regulated sandbox for the Tawakkalna national superapp, allowing private companies to test and integrate digital services with 34 million users within a secure, government-controlled environment to expand public–private digital services. *This sandbox supports Saudi Arabia's data exchange and interoperability.*
Singpass API Developer Portal Sandbox	Singapore	Government Technology Agency	In operation	Digital ID	The portal provides a sandbox (staging) environment where developers can build and test integrations with Singpass-related digital identity and government APIs before going live. It is part of Singapore's National Digital Identity (NDI) ecosystem, which enables secure authentication and consent-based data sharing across public and private services. *This sandbox is part of Singapore's national digital identity and consent-based data-sharing infrastructure.*
E-ID Sandbox	Switzerland	Swiss Confederation	Completed	Data Exchange	A public sandbox where companies and organizations were allowed first contact with the new E-ID solution to test it. *This sandbox supports the rollout of Switzerland's national digital identity infrastructure.*

Sandbox	Country	Lead	Status	DPI layer	Description
Taiwan Digital Identity Wallet (TW DIW)	Taiwan	Ministry of Digital Affairs (MODA)	Announced	Digital ID	A government-led sandbox by Taiwan's Ministry of Digital Affairs enabling public–private testing of a mobile digital identity wallet for credentials like national ID, health insurance, and driver's licenses, with open-source development, regulatory experimentation, and pilots to support interoperable, privacy-preserving digital services. *This sandbox supports the development of Taiwan's national digital identity infrastructure.*
UK Digital Identity Sandbox	United Kingdom	Department for Science, Innovation and Technology (DSIT)	In operation	Digital ID	The UK DSIT's sandbox aims to gather evidence on how digital identity solutions will work in practice in a 'live' environment, build evidence for further policy development to support the emerging market, explore how regulatory and/or other changes can remove blockers to the use of digital identity solutions. *This sandbox is delivered by NayaOne and supports the testing and development of the UK's national digital identity infrastructure.*
UK Smart Data Sandbox	United Kingdom	Department for Business and Trade (DBT)	In operation	Data Exchange	UK DBT's sandbox aims to test cross-sector solutions using high-quality synthetic data in a secure environment. Developed as part of the Smart Data Challenge Prize, the sandbox enables innovators, SMEs, and researchers to prototype applications across multiple sectors while experimenting with data interoperability, consent models, and data standards, and generating evidence to inform future policy and ecosystem development. *This sandbox is delivered by NayaOne and supports the testing and development of the UK's Open Data Exchange infrastructure and enhances consent and data standards approaches.*

Note: The table summarizes DPI sandboxes from around the world. The "Sandbox" column lists the official name of each initiative, while "Country" indicates where it is established or led. "Lead" identifies the main institution or institutions managing the sandbox, and "Status" shows its stage as of February 2026, such as announced or in operation. The "DPI layer" column indicates which DPI layer is being tested within the sandbox (Digital ID, Digital Payments and/or Data Exchange). Finally, the "Description" provides a brief overview of each sandbox's goals, focus areas, and role in supporting DPI innovation.

Key trends and patterns

The global distribution of DPI sandboxes reflects both the growing recognition of DPI as foundational to digital transformation and the early-stage, uneven institutionalization of DPI-focused experimentation across regions. As illustrated in the map above (Figure 1), DPI sandbox initiatives are emerging across Asia, Europe, and Latin America, with fewer formal initiatives identified in North America and Africa.[126] This pattern should be interpreted cautiously, as DPI itself remains a recent and evolving construct, and experimentation practices continue to mature.

The geographic spread of DPI sandboxes suggests that experimentation is taking shape across a wide range of institutional and governance contexts, indicating that DPI experimentation is shaped not only by technological capacity, but also by regulatory cultures, governance models, and differing approaches to public digital infrastructure.

The global mapping of DPI sandboxes reveals a fast-evolving experimentation landscape that differs in important ways from earlier generations of sandboxes, particularly those developed for financial technologies[127] and AI.[128] Several clear trends emerge across regions, sectors, and DPI layers. Together, these trends point to a shift in how governments and ecosystem actors are approaching risk, trust, and learning in the development of foundational digital systems. Given the relatively recent emergence of DPI as a policy framework, these patterns should be understood as provisional, with significant scope for growth, convergence, and cross-regional learning in the years ahead.

Foundational DPI layers shape where experimentation begins

Based on the Datasphere Initiative's mapping, DPI sandboxes have been most frequently focused on **digital identity**. Of the initiatives identified in this report, nine DPI sandboxes explicitly center on digital identity, either as a standalone focus or in combination with other DPI layers (notably India's Aadhaar sandbox, which spans both identity and payments). This prominence reflects the central role of digital identity as a foundational and cross-cutting infrastructure: identity systems underpin access to public services, financial inclusion, data-sharing mechanisms, and cross-border interoperability. Given their systemic impact, digital identity systems often require extensive testing at technical, legal, and governance levels before scaling, making sandboxes a particularly suitable instrument for experimentation.

[126] An African example is Tanzania's proposed Jamii Stack sandbox, planned for launch in 2026, which was not mapped because it did not fit the classifications used in this study.

[127] Datasphere Initiative (2025) *Sandboxes for AI: Tools for a new frontier*, Datasphere Initiative.

[128] Datasphere Initiative (2025) *Sandboxes for AI: Tools for a new frontier*, Datasphere Initiative.

Data exchange and interoperability emerge as the next most prominent focus area, with five DPI sandboxes explicitly designed around data-sharing infrastructures, data governance mechanisms, or interoperability layers. This trend aligns with broader global efforts to move beyond siloed data systems toward integrated, consent-based, and interoperable data architectures.[129] The presence of sandboxes focused on data exchange also reflects the growing recognition that effective DPI depends not only on identity or payments, but on the ability to securely share data across institutions, sectors, and borders. As such, data-focused DPI sandboxes hold particular promise for supporting cross-border collaboration and the future development of regional or transnational DPI ecosystems, an area that remains underexplored but increasingly relevant.

Digital payments are the least represented as a primary focus among the identified DPI sandboxes, with only three sandboxes explicitly designed around payment-related DPI layers, including Aadhaar's combined identity–payments sandbox. This should not be interpreted as a lack of experimentation in digital payments. On the contrary, a large number of sandboxes that support DPI innovation, particularly financial sandboxes led by central banks, support innovations that build on, interface with, or depend upon national payment infrastructures. However, in most of these cases, the public payment system itself is not the primary object of experimentation, but rather the underlying infrastructure upon which new services are tested, or yet, one instance among several other testing plans which are not based on DPI environments. As a result, these initiatives contribute significantly to payment system evolution, yet fall outside the classification of DPI sandboxes adopted in this report.

The rise of hybrid sandboxes for operational and regulatory learning

A defining trend across the global DPI landscape is the emergence of operational sandboxes and hybrid sandboxes that combine operational testing with regulatory learning. Given the infrastructural nature of DPI, sandboxing in this domain increasingly operates as integrated environments where technical design choices, governance arrangements, and regulatory considerations are tested simultaneously.

Across the mapped initiatives, sandbox environments are being used upstream in the value chain, that is, before systems are scaled or institutionalized, to test core DPI components under realistic conditions. Relevant examples include initiatives such as the European Digital Identity Wallet sandbox, India's RBI Digital Rupee (e-Rupee) Sandbox, Germany's EUDI Wallet: SPRIND Sandbox and France's Identité Sandbox Environment. While these initiatives place strong emphasis on operational testing - such as user journeys, consent mechanisms, data flows, and system interoperability - they are frequently linked to compliance, standards-setting, and future regulatory frameworks. This makes them hybrid in practice, even when not formally labeled as such.

[129] Datasphere Initiative (2022). *Sandboxes for data: creating spaces for agile solutions across borders*.

In fact, DPI systems have direct and far-reaching regulatory implications. Key issues related to data protection, liability, standards, and cross-border interoperability are embedded in system design choices and cannot be assessed separately from how the infrastructure actually operates. For this reason, hybrid sandbox settings, where operational testing is combined with regulatory learning, are not only common in the mapping, but often necessary.

Given the scale of DPI deployments, relying on purely operational experimentation could potentially overlook regulatory learnings that are necessary before systems are institutionalized. Regulatory sandboxes can have an important role in generating regulatory learning through experimentation, and how such learning can complement operational testing in hybrid DPI sandbox settings (Box 9). Hybrid sandboxes allow governments and ecosystem actors to test infrastructure in realistic conditions while simultaneously generating evidence to inform rules, oversight, and governance arrangements.

Box 9. Regulatory sandboxes as tools for experimentation

Existing practice demonstrates how regulatory sandboxes can function as practical tools for experimental governance. Kenya's Communications Authority regulatory sandbox,[130] launched in 2023, provides a controlled environment for testing emerging ICT products and services, including AI, IoT, and smart city solutions, while enabling close collaboration between innovators and the regulator to safeguard consumer interests. Korea offers a complementary large-scale model through its integrated, multi-ministerial sandbox system[131] coordinated by the Office for Government Policy Coordination. Covering eight sectors across six ministries, including ICT convergence and financial innovation, Korea's approach combines sector-specific oversight, transparency, and temporary regulatory exemptions to generate evidence and inform regulatory reform.

Integrating hybrid sandboxes more deliberately into DPI experimentation can support adaptive and agile policy evolution,[132] enabling regulators to test rules, clarify responsibilities, and adjust oversight mechanisms alongside technical development. This layered approach, combining operational testing with regulatory experimentation, helps ensure that DPI systems are not only technically robust, but also legally sound, transparent, and scalable. This is particularly relevant for cross-border or cross-regulatory DPI ambitions, where misalignment between regulatory regimes can quickly become a bottleneck. Hybrid sandboxes provide a structured space to explore technical and interoperability standards, as well as coordinated governance approaches, reducing uncertainty and building confidence among participating countries or institutions.

[130] Datasphere Initiative (2025). Africa Sandboxes Outlook: Thinking outside the box for responsible innovation in the age of AI.

[131] Datasphere Initiative (2025). Korea's Financial Sandbox: Adaptive regulation in action.

[132] Rossini, C., Carneiro, G., & Moraes, T. G. (2024). Agile governance for an agile future: Sandboxes for promoting responsible innovation. T20 2024 Task Force 05: Inclusive Digital Transformation.

AI is increasingly embedded within DPI sandbox experimentation

While most sandboxes in the mapping are not labeled as "AI sandboxes", AI is increasingly present within DPI experimentation. This is particularly evident in digital identity sandboxes, where AI is embedded within authentication, verification, and risk-assessment processes rather than treated as a standalone object of testing. This reflects the broader nature of DPI as a complex, multi-layered infrastructure that integrates multiple technologies serving different functions, rather than relying on a single technological component.

A clear example is India's Aadhaar (UIDAI) sandbox, launched in 2023 to enable FinTechs and start-ups to safely test and integrate core Aadhaar APIs for e-KYC and authentication before market deployment. Although the sandbox is framed around digital identity and financial inclusion, participating cohorts have refined biometric authentication flows, AI-enabled KYC models,[133] and AI-driven credit-scoring solutions within the sandbox environment. In its first year, the sandbox supported over one million test authentications and accelerated the development of paperless KYC stacks and contactless biometric solutions, illustrating how AI is tested in practice as part of a national identity infrastructure rather than through a dedicated AI sandbox. Here, AI experimentation is inseparable from broader infrastructural and governance considerations, including interoperability, system performance, and regulatory compliance across sectors.

AI hence appears both as a functional layer, supporting fraud detection, biometric matching, service personalization, or analytics, and as a governance challenge, particularly where automated decision-making intersects with identity, eligibility, or access to services. This trend highlights a key distinction: DPI sandboxes are becoming spaces where AI is tested in context, rather than as a general purpose technology. Unlike standalone AI sandboxes, DPI sandboxes allow stakeholders to examine how AI systems behave when embedded in real public infrastructures, drawing on shared data, interacting with legal frameworks, and affecting rights at scale.[134] Their cross-sectoral nature enables regulators and system designers to observe how AI interacts simultaneously with technical architectures, institutional mandates, and sector-specific governance regimes.

This contextual testing is particularly important because DPI provides the data foundations and institutional scaffolding on which AI systems depend. Poorly governed DPI can hard-code bias, exclusion, or surveillance into AI-enabled public services. As tools designed to accommodate complexity, uncertainty, and interdependencies, sandboxes are particularly well suited to the DPI context, offering a structured space for evidence generation on how multiple technological, regulatory, and institutional elements interact in practice. DPI sandboxes therefore offer a critical opportunity to test AI-DPI interactions upstream, before harms are multiplied across sectors.

[133] AI-enabled Know-Your-Customer (KYC) models are systems that apply artificial intelligence — including machine learning, natural language processing, and pattern recognition — to automate and enhance traditional KYC processes, such as identity verification, document authentication, fraud detection, and risk scoring. These models analyze large volumes of data and aim to reduce manual effort, improve accuracy, and detect anomalies more effectively than rule-based systems, but they also raise important governance considerations related to transparency, explainability, and bias in decision-making. See: IDWise (2025) What is Know Your Customer Artificial Intelligence?, IDWise.

[134] Rozo-Paz (2025), *Key insights for AI-powered DPI ahead of the India AI Impact Summit 2026*, Datasphere Initiative.

Sandboxes are being used as tools for interoperability and ecosystem readiness for DPI

Sandbox experimentation is providing a controlled environment in which interoperability is tested as a live operational practice. Unlike traditional pilots, which are often confined to a single agency or use case, sandboxes are structured to require interaction between multiple systems, institutions, and stakeholders from the outset. By doing so, they expose mismatches in data standards, consent models, liability assumptions, and governance processes that would otherwise remain hidden until full-scale deployment. When interoperability challenges related to data governance, trust, and institutional coordination are addressed only after systems are operational, they can significantly slow adoption and limit the effectiveness of DPI (Box 10).

Take, for instance, developments within the European Digital Identity (EUDI) Wallet Sandbox.[135] Built on the legal framework of the revised eIDAS 2.0 Regulation, the EUDI Wallet initiative is being tested through sandbox environments designed to mirror future production systems and workflows. These environments allow relying parties, wallet providers, and service integrators to validate identity and credential flows before national rollout, including the foundational Person Identification Data (PID) flows and, in later stages, credential attestations such as electronic driving licences and professional qualifications. By placing these elements in a live test environment, the sandbox exposes interoperability issues - such as how different issuers encode credentials, how wallets interpret and present proofs, and how relying services consume and verify attributes - at a stage when protocols and standards can still be refined.[136]

The EUDI Wallet sandbox also functions as more than a technical playground. It incorporates access to the Architecture and Reference Framework (ARF),[137] the technical and standards blueprint for interoperable digital identity across the EU, and supports participant access to developer documentation, reference implementations, and test data that closely reflect production expectations. These features encourage collaboration across public-sector authorities, private technology providers, and relying parties, enabling them to surface and address mismatches in implementation assumptions, user journeys, and data exchange protocols before they become locked into law or large-scale infrastructure.

Similarly in India, Bharat BillPay, a service by the Indian Government that integrates with other government agencies for seamless and easy payments of bills for electricity, gas, water, etc., provides a sandbox environment that third-party players can use for building innovative apps and services.[138] It offers open APIs for fetching and validating bills, facilitating payments, and

[135] Federal Ministry of the Interior of Germany (2026), *EUDI Wallets: Ecosystem Knowledge Centre*, Federal Ministry of the Interior of Germany.

[136] Ibid.

[137] European Commission (2025), EU Digital Identity Wallet Toolbox process, European Commission.

[138] UNDP (2023), *Accelerating the SDGs through Digital Public Infrastructure: A Compendium of the Potential of Digital Public Infrastructure*, UNDP.

tracking transaction status. Bharat BillPay is interoperable as it connects banking and non-banking entities in the bill aggregation business, billers, payment service providers and retail bill outlets. It standardizes the process of bill payment for the entire ecosystem and as of 2022, has enabled US$14 billion in transaction volume.[139]

Box 10. The challenge of embedding interoperability into DPI systems

Uganda's UGHub initiative illustrates both the promise and the complexity of embedding interoperability into DPI systems. UGHub[140] is a government-wide data integration platform developed by the National Information Technology Authority-Uganda (NITA-U) to enable secure, real-time data sharing among Ministries, Departments, and Agencies (MDAs), as well as select private entities, thereby transforming fragmented digital services into a unified digital ecosystem.[141] UGHub has facilitated over 100 million transactions (as of March 2024) while over 60 government ministries, departments, and agencies as well as 73 private sector partners are on board.[142]

Despite its progressive adoption, the platform's ability to deliver on interoperability depends heavily on clarity around data-sharing protocols, consent mechanisms, and governance norms, elements that are still evolving in policy and practice. Research on the integration experience shows that mistrust about data custodianship, uneven stakeholder adoption, and variations in technical readiness across agencies have slowed the pace of integration and underscored the importance of building trust alongside technical integration.[143] In such contexts, a sandbox could provide an invaluable way to simulate real-use scenarios before scaling up, allowing stakeholders to observe actual data flows and consent interactions between systems in a controlled environment.

Participation and institutionalization remain uneven, limiting the potential of DPI sandboxes

The global overview reveals significant unevenness in how DPI sandboxes are institutionalized and who participates in them. Even where these sandboxes exist, participation is often skewed toward government agencies and private sector actors, with civil society organizations, community groups, and affected populations less consistently involved. This imbalance risks reproducing the very trust and legitimacy gaps that sandboxes can address, particularly as DPI systems increasingly structure access to rights, services, and opportunities.

[139] Ibid.

[140] NITA-Uganda (n.d), UGhub Systems and data Integration Platform, Government of Uganda.

[141] Ibid.

[142] Dolan J., Satapathy S., Sabiti B. (2024), *Data can drive shared prosperity for governments, businesses, and citizens: Unlocking it requires trusted data exchange*, Digital Impact Alliance.

[143] Ibid.

This pattern can be partly explained by the infrastructural nature of DPI itself. DPI initiatives focus on foundational systems, such as digital identity, data exchange, or payment rails, and the high level of technical complexity involved in DPI design and implementation can create barriers to meaningful participation, especially where sandbox processes are organized around specialized technical or regulatory discussions. The technical complexity of DPI experimentation could result in technical literacy being implicitly treated as a prerequisite for participation, creating barriers to broader societal engagement. However, this framing risks overlooking other forms of contribution that are equally critical to DPI design and governance. Civil society organizations, community groups, and affected users can provide value-based input on acceptable business and sustainability models, feedback on system usability and accessibility, and perspectives on core public values such as privacy, fairness, transparency, accountability, and inclusion, regardless of their level of technical expertise.

Limited civil society engagement represents a missed opportunity for DPI sandboxes to function as infrastructures for trust rather than technical testbeds alone. Civil society organizations can play a critical role in translating technical design choices into real-world impacts, surfacing contextual risks and inclusion challenges, and bringing rights-based and community perspectives into experimentation. Meaningful engagement does not solely require technical expertise: citizens and civil society actors can contribute value-based perspectives on usability, fairness, privacy, transparency, and acceptable business models, offering insights that are essential to the legitimate and socially aligned development of DPI. Where such engagement is absent, key social impacts and legitimacy concerns may remain insufficiently examined.

At the same time, considering who should run a DPI sandbox is equally important as who participates. Whereas payments-related sandboxes could naturally be run by financial regulators or central banks, digital ID and data-exchange run across the economy. While the sandbox type and objectives will likely determine which agency or government body has full oversight, deciding the governance of DPI sandboxes is not straightforward. As knowledge and use of DPI sandboxes are still nascent, lack of clarity around sandbox regulatory, delivery and promotion mandates will impact not only the speed of sandbox design and implementation but also internal governmental coordination and interoperability of outcomes.

This reinforces a central insight of the mapping: **the value of DPI sandboxes lies not only in what is tested, but in who is able to test, observe, and act on the outcomes**. As DPI systems continue to expand in scope and influence, more intentional and diverse participation, particularly through strengthened civil society engagement, and cross-government collaboration, will be essential to ensure that sandbox experimentation supports inclusive, rights-respecting, and interoperable digital public infrastructure.

Conclusion

This report has explored the growing role of sandboxes as a critical, though still evolving, instrument for designing and governing Digital Public Infrastructure. **Rather than treating DPI and sandboxes as separate technical or policy tools, the analysis shows how they increasingly function as complementary governance approaches.**

One of the central lessons of the report is that DPI has never developed through rigid, linear implementation pathways. Even early pioneers relied on iterative testing, phased roll-outs, and adaptive governance to make systems workable at scale. **What has changed is not the presence of experimentation, but the growing recognition that experimentation must now be made explicit, intentional, and accountable.** As DPI systems become more interconnected, more data-intensive, and increasingly entangled with AI, the risks of exclusion, surveillance, cybersecurity failures, vendor dependency, and governance breakdowns become too high to be addressed after systems are already embedded at population scale.

What ultimately distinguishes DPI sandboxes is not just what is tested, but how experimentation is organized. Their value lies in creating structured spaces where risks can be surfaced early, multiple actors can engage, and lessons can be translated into institutional practices, safeguards, and policy decisions. When done well, sandboxes move DPI development away from reactive problem-solving and toward a more transparent, evidence-based, and participatory form of governance.

The global mapping presented in this report confirms that DPI sandboxes are already happening. Initiatives are emerging across diverse regions and governance contexts, shaped as much by regulatory cultures, institutional capacity, and political priorities as by technological readiness. Across the landscape, experimentation most often begins with digital identity and data exchange layers, reflecting both their foundational role and the significant risks they carry. Payment infrastructures, by contrast, seem to be treated as stable backbones rather than primary objects of testing, even where innovation depends heavily on their reliability and interoperability. However, the proliferation of sandboxes in the financial sector, many of which focus on payment systems, indicates that experimentation around payment infrastructures is already well underway. These initiatives are closely connected to DPI development and offer relevant insights for payment layers as integral components of DPI.

The mapping also reveals a clear shift toward operational and hybrid sandboxes used upstream, before DPI systems are fully deployed or legally entrenched. This reflects a growing awareness that failures in foundational infrastructure are difficult, costly, and politically sensitive to reverse once scaled. At the same time, the relative scarcity of purely regulatory sandboxes in the DPI space should not be mistaken for a lack of regulatory ambition. Instead, it reflects the infrastructural nature of DPI itself. Regulatory choices around privacy, accountability, interoperability, and access are often embedded directly into system architectures, making it impractical to test them in isolation. As a result, regulatory learning in DPI contexts tends to happen through hybrid sandboxes, where legal, policy, and oversight questions are examined alongside technical design and real-world use. Making these regulatory learning objectives more explicit, even where experimentation is operational in form, would significantly strengthen the governance value of DPI sandboxes.

Looking ahead, the relevance of sandboxes for DPI governance is only set to grow. DPI systems rarely operate within neat institutional or jurisdictional boundaries. Data flows, service delivery, and technical dependencies often cross multiple regulators, sectors, and countries, creating governance challenges that cannot be addressed in isolation.

Beyond their role as temporary regulatory instruments, sandboxes can also be understood as emerging digital public tools, that are, foundational, reusable experimentation infrastructures that public institutions can rely on over time. Much like digital public goods[144] provide shared, open foundations for building and scaling digital systems, sandboxes can offer the public sector common testing facilities, methodologies, and governance practices that support continuous learning, iteration, and value creation. Positioned as one of the various potential *digital public tools*,[145] sandboxes have the potential to become part of the core public infrastructure, enabling governments to systematically refine, adapt, and govern digital public systems in an increasingly complex and interconnected environment.

However, the analysis also makes clear that sandboxes are not a silver bullet and require clear planning and resources. Poorly designed sandboxes can reinforce power asymmetries, exclude affected communities, or become symbolic exercises disconnected from real decision-making.

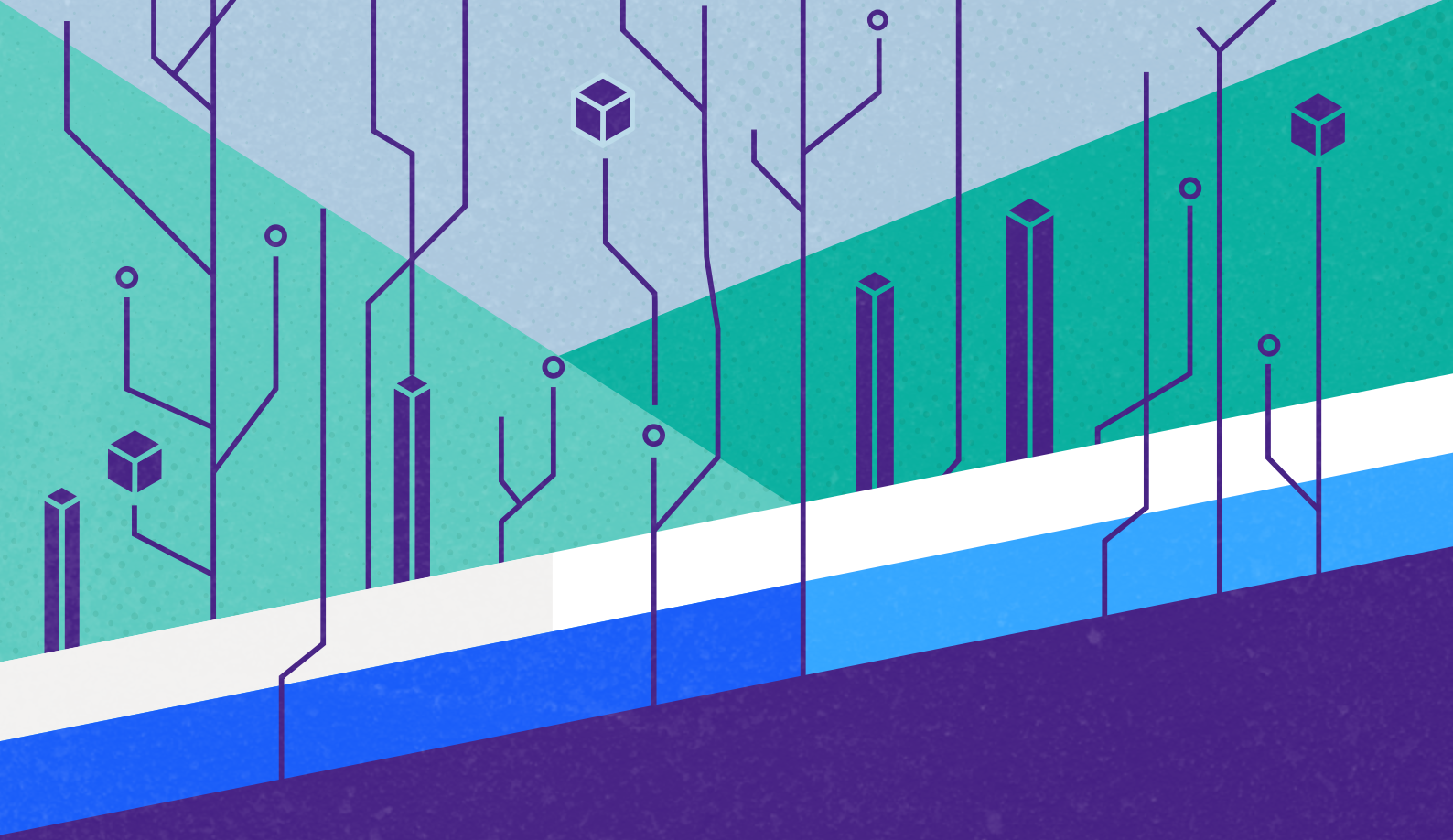
Sandboxes are not a way to defer responsibility or outsource risk — they are about taking uncertainty seriously and managing it in a structured, transparent, and accountable way. Achieving this requires sustained investment in institutional learning, interdisciplinary collaboration, and mechanisms that ensure lessons from sandbox experiments meaningfully shape policy, procurement, and system design. Governments need the resources to design inclusive and effective sandboxes as well as the impetus to act on sandbox learnings. The private sector needs assurances and incentives to participate in sandboxes actively and civil society needs the resources and opportunities to become active participants in sandbox design and implementation. Deeper learnings from DPI sandbox experiences should be transposed to assess their impact, methods, value as well as lessons learnt.

Addressing some of these areas will shape the next phase of the Datasphere Initiative's work. Through co-creation labs, global convenings, and expanded comparative research, Datasphere Initiative will work with governments, companies, academia, and civil society to deepen understanding of how to design and implement DPI sandboxes that are inclusive, trustworthy, and context-appropriate. The goal is not to prescribe a single model, but to strengthen sandboxes as tools for learning, accountability, and public value.

Ultimately, the question facing DPI is not whether experimentation is needed, but how it is carried out and to what end. By institutionalizing iterative testing and embedding trust-building and inclusion upstream, well-designed sandboxes can help shift DPI development away from hype-driven deployment and toward systems that are resilient, legitimate, and responsive to the people they are meant to serve.

[144] Digital Public Goods Alliance (n.d.). Digital Public Goods Standard.

[145] Other Digital Public Tools could be existing experimentation settings or spaces like living labs, policy prototypes, testbeds, among others.



thedatasphere.org