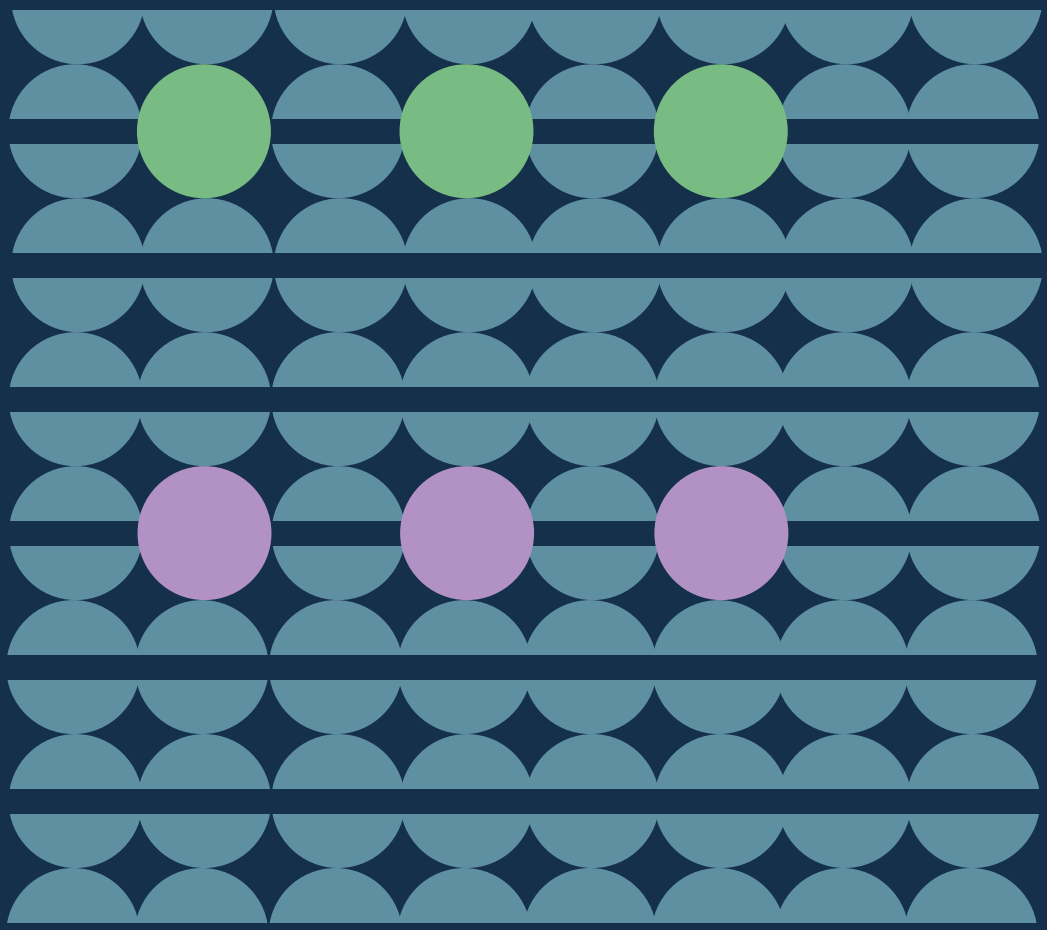
GLOBAL PARTNERS DIGITAL

Human Rights Impact Assessment for Digital Public Infrastructure

A Framework



Acknowledgments

This framework was developed by Rose Payne and Maria Paz Canales, with the invaluable support of Akhil Thomas for its consultation process. Edited and typeset by Global Partners Digital.

It brings together contributions from a range of actors and organisations working across digital governance and human rights. The authors would like to thank all those who shared their expertise, insight and feedback. Their contributions have immeasurably strengthened the conceptual and methodological basis of this framework. Any shortcomings are exclusively the author's responsibility.

We are particularly grateful to David Eaves, Himansu Pandey and Priyanka Bhupalan (UCL Institute for Innovation and Public Purpose); Line Gamrath Rasmussen (Danish Institute for Human Rights - DIHR); Elizabeth Eagen (Cornell University); Christina Dahlman (Swedish International Development Cooperation Agency - Sida); Teresa Barrio (Amnesty International); Subin Mulmi (Nationality for All - NFA); Thomas Lohninger (Epicenter.works); Warren Liu (Odditysay Labs); Poorvi Chawla (Aapti Institute); Stephanie Nicolle (Independent practitioner); Jose Arraiza (Legal Identity, Digital ID & Statelessness expert); Diana Ramírez (Cepei); Bojana Kostić and Michael J. Oghia (GFMD); Marina Meira (Derechos Digitales); Lucía León (Hiperderecho); Arzak Khan (Innovation For Change (I4C) South Asia); Kenmogne Rigobert (Digital Access); and, Kituo Cha Hak (Youth Kenya).

Published **June 2026**

GLOBAL PARTNERS DIGITAL

Contents

Executive Summary

This framework aims to help stakeholders identify, assess, and address the human rights and rule of law impacts of Digital Public Infrastructure (DPI) design and implementation.

It is a framework, not a tool. It offers an adaptable model and methodology for understanding how people and communities interact with DPI systems, identifying risks and designing safeguards to ensure digital transformation is rooted in accountability and public trust. It is designed to be used **across the DPI initiative lifecycle**, from assessment through deployment to decommissioning.

Who is it for?

The framework is designed for anyone involved in the design, deployment, governance, funding, oversight, or assessment of DPI, including: governments, technology providers, private sector partners, civil society, researchers and more.

What does it support users to do?

- Understand how a DPI initiative may affect human rights & rule of law
- Identify who may benefit from, be harmed by a DPI system
- Assess potential risks to users and communities
- Design mitigation measures
- Monitor impacts and respond to emerging risks over time

The four stages of assessment

1. **Planning & Context Assessment**
   Understand the DPI initiative, identify stakeholders, assess socio-technical, legal, and sectoral context.
2. **Data Collection & Risk Measurement**
   Gather evidence to identify potential human rights impacts and assess nature, likelihood, and severity of risks.
3. **Mitigation Measures Design & Rollout**
   Develop and implement measures to prevent, minimise, or remedy identified risks.
4. **Ongoing Evaluation & Impact Management**
   Monitor impacts, review safeguards and measures, adapt responses as DPI and context evolves

1

Introduction

This chapter introduces the concept of **Digital Public Infrastructure (DPI),** explains why a dedicated **Human Rights Impact Assessment (HRIA) framework** is needed and sets out the human rights and rule-of-law foundations underpinning our approach.

Key points

- DPI is becoming a **central component of digital transformation and public service delivery**, particularly in the Global South
- Its rollout carries **significant implications for human rights**, accountability, inclusion, and public trust
- Its development should consider **geopolitical asymmetries** in DPI deployment and the importance of embedding safeguards, oversight, and public-interest considerations into its design and implementation.
- **Currently existing assessment approaches are insufficient** in addressing the unique characteristics of DPI. Instead, we need a DPI-specific HRIA framework capable of assessing risks and impacts throughout the lifecycle of DPI initiatives
- **Human rights and rule of law must be the normative foundation for DPI assessment**. These frameworks offer internationally recognised standards and practical guidance to ensure digital infrastructure is inclusive, transparent, sustainable, and centred on human dignity.

What is Digital Public Infrastructure (DPI)?

DPI is not just technical infrastructure. It is also a governance and human rights issue that directly shapes state-citizen relations.

Digital Public Infrastructure (DPI) is used to refer to **the digital systems and infrastructure that connect people to public services**. In practice, these systems and infrastructures include digital ID, data gathering, and digital payments.

In recent years, DPI has become **a central concept in global digital policy and development discussions**, featuring in the United Nations' (UN) digital transformation agenda, in the outcomes of World Summit on the Information Society (WSIS), and found in the Global Digital Compact (GDC). Beyond the UN, it has consistently appeared in G20 agendas[1]. Countries around the world have implemented DPI, including India[2], Estonia[3], Kenya[4] and Singapore[5] and development funders including the Gates Foundation[6] and the World Bank[7] have dedicated funding to advancing DPI.

DPI is increasingly promoted as a means of delivering key public services and **may become one of the main interfaces for people to interact with their governments**. Its proponents see DPI as a means for governments to "restore state capacity and build public trust to ensure core digital services advance shared goals"[8]. This means DPI can directly impact the exercise of human rights. As DPI gradually becomes a vehicle for service provision, participation and access to justice, it also becomes a key element in the state's responsibility to promote, protect, respect and fulfil its human rights obligations.

DPI inception often goes hand in hand with increased automation of decision-making processes. This can reduce the role of public servants and, under the promise of efficiency, transparency and innovation, **shift practices away from core good governance principles such as accountability, oversight, and due process**.

Definitions of DPI vary across institutions, but they converge around several core characteristics. The G20 (2023) describes DPI as a set of shared digital systems that **provide equitable access to public and private services at scale**, governed by enabling legal frameworks and grounded in human rights and fundamental freedoms, and which must take a secure, interoperable, and open approach.

How institutions define DPI

G20

2023 Digital Economy Ministers Meeting Outcome document: "A set of shared digital systems that should be secure and interoperable, and can be 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 applicable legal frameworks and enabling rules to drive development, inclusion, innovation, trust, and competition and respect human rights and fundamental freedoms. Considering the diverse approaches of G20 members to digital transformation, we recognize that DPI is an evolving concept that may not be limited to sets of digital systems with these characteristics and could be tailored to specific country contexts and can be referred to with different terminology."

Office of the Secretary-General's Envoy on Technology (OSET)

The Universal Digital Public Infrastructure Safeguards Framework: "DPI comprises technological systems and services that operate at the intersection of individuals on one hand, and civic, public and private entities that hold social, political and economic power on the other."

World Bank

Digital Public Infrastructure and Development: DPI is an approach to digitalization focused on creating "foundational, digital building blocks designed for the public benefit." By providing essential digital functions at society scale that can be reused across sectors, DPIs enable public and private service providers to build on these systems, innovate, and roll out new services more quickly and efficiently. Common systems built as DPIs include digital identity and electronic signatures, digital payments, and data sharing. However, to provide DPI functionality, these systems must embed principles such as inclusion, openness, modularity, inclusivity, user-centricity, privacy-by-design, and strong governance.

Organisation for Economic Co-operation and Development (OECD)

Government at a Glance 2025: Digital public infrastructure (DPI) is a key foundation for public service delivery, public sector efficiency and the broader digital economy. There are six key DPI components: digital identity, digital payments, data-sharing systems, digital post, digital notifications and base registries. Governments play a central role in designing, implementing and overseeing this infrastructure, as well as providing the underlying enablers, comprising open-source and interoperability frameworks, and standards for metadata and application programming interfaces (APIs).

Digital Public Goods Alliance

Unpacking concepts & definitions: Refers to solutions and systems that enable the effective provision of essential society-wide functions and services in the public and private sectors. This includes digital forms of ID and verification, civil registration, payment (digital transactions and money transfers), data exchange, and information systems (including sector-specific, i.e. health or education). A country's DPI may include multiple proprietary and/or open-source solutions (including digital public goods).

Taken together, these definitions emphasize DPI's **infrastructural and institutional nature**. DPI brings together technical systems, governance frameworks, and interactions between individuals, states, and private actors. Its foundational nature and cross-sectoral reach mean that human rights impacts can cascade across fields, services and communities, reinforcing the need for rigorous human rights-based evaluation.

However, this strong public administration focus must be **balanced with an understanding of DPI's role in supporting other critical social functions** beyond state service delivery – including public interest journalism, independent media, participatory platforms, citizen science, and other rights-enabling services provided by non-state actors[9]. Any definition should also attend to the geopolitical implications of the provision and deployment of DPI. The promotion of DPI in Global South countries should be critically examined in light of historical colonial dynamics of technological power. New digital infrastructures, identification systems and governance technologies are often rolled out in Global South countries first, using them as spaces for technological experimentation, often in the absence of regulatory frameworks, robust safeguards for human rights and effective accountability mechanisms. The rapid diffusion of DPI models across the Global South therefore cannot be understood solely in terms of innovation or digital inclusion, but also as part of **an international division of technological power** – in which the Global North concentrates development, ownership, and standard-setting, while the Global South serves as a proving ground for large-scale implementation and the testing of social impacts.

Another related issue is DPI's **concentration of technological power** in a small group of technology providers, often based in jurisdictions where regulatory requirements to insert governance and human rights safeguards are limited or non-existent. Even jurisdictions with well-established rule of law and governance norms can struggle to make foreign providers adjust to their domestic requirements.

Everywhere, but particularly in Global South countries, DPI has shown **both its transformative potential and its risks**. It has expanded access to public services for millions, but it has also raised concerns around exclusion, surveillance, data protection and unequal access for marginalized communities. These experiences highlight that DPI is not only a technical infrastructure but also a governance and human rights issue that directly shapes state-citizen relations. When DPI models are imported across jurisdictions with limited adaptation to local social, political, and institutional contexts, there is a risk of amplifying existing inequalities unless supported by appropriate governance structures and sensitive adaptation to the specific cultural context.

"DPI's foundational nature and cross-sectoral reach mean that human rights impacts can **cascade across fields, services and communities, reinforcing the need for rigorous human rights-based evaluation**"

Technical choices can also strongly influence the outcomes of DPI deployment. Privacy-enhancing technologies (PETs), trusted execution environments (TEEs), Fast Identity Online (FIDO) authentication, hardware security keys and authenticators are examples of technical standards that can help DPI align with the public interest and protection of rights[10].

Another related issue is DPI's concentration of technological power in a small group of technology providers, often based in jurisdictions where regulatory requirements to insert governance and human rights safeguards are limited or non-existent. Even jurisdictions with well-established rule of law and governance norms can struggle to make foreign providers adjust to their domestic requirements.

Everywhere, but particularly in Global South countries, DPI has shown **both its transformative potential and its risks.** It has expanded access to public services for millions. But it has also raised concerns around **exclusion, surveillance, data protection and unequal access for marginalized communities**. These experiences highlight that DPI is not only a technical infrastructure but also a governance and human rights issue that directly shapes state-citizen relations. When DPI models are imported across jurisdictions with limited adaptation to local social, political, and institutional contexts, there is a risk of amplifying existing inequalities unless supported by appropriate governance structures and sensitive adaptation to the specific cultural context.

Why a Human Rights Impact Assessment Framework for DPI is needed

DPI is an approach to creating and deploying technology, rather than a specific technology or set of technologies. Existing frameworks may therefore be unsuitable or focus on human rights impacts which are not comprehensive enough for DPI.

Digital Public Infrastructure (DPI) is used to refer to the digital systems and infrastructure that connect people to public services. In practice, these systems and infrastructures include **digital ID, data gathering, and digital payments**.

As DPI becomes central to digital transformation agendas worldwide, particularly across the Global South, the need for systematic human rights assessment is increasingly clear. International initiatives such as the UNDP's "Universal DPI Safeguards Framework"[11] and the Global Digital Compact[12], which call for inclusive, responsible, and rights-respecting digital infrastructures, have laid normative foundations. But there is still **a need for practical methodologies** to identify and assess DPI impacts on human rights throughout its lifecycle in a practical, context-sensitive manner. Our framework offers a blueprint for implementing the Universal DPI Safeguards Framework's call, as part of its "Do no harm" principle, for responsible authorities to conduct lifecycle human rights impact assessments (HRIA) as part of DPI deployment.

As a recent report highlights, "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"[13].

Specific frameworks for DPI often focus on successful implementation and broad risk assessment, rather than human rights. When they do refer to human rights, frameworks often take a principles-based approach. A good example is provided by the "Rights-Respecting Digital Public Infrastructure Principles" adopted by the Freedom Online Coalition (FOC) in 2025[14].

While principles can be a useful guide, understanding how to practically apply them can be challenging in the absence of context-specific guidance.

Potential human rights impacts from DPI vary depending on where it is deployed. Many sectors are inherently high-risk from a human rights perspective because they involve **access to essential services or sectors in which safety is paramount.**

Examples include **healthcare, social care, education and migration**. In these high impact contexts, DPI may be directly linked to decisions about eligibility, prioritisation, enforcement or access, increasing the potential for harm if the system malfunctions, is misused, or embeds bias. This can be identified through the application of HRIA.

DPI in Practice: Opportunities and Human Rights Risks

India Stack

India is often cited as an example of DPI for its "India Stack" ecosystem. Introduced in 2009, it combines the Aadhaar digital identity system, the Unified Payments Interface (UPI) and a range of other mechanisms. These systems have enabled delivery of public services at scale and given millions access to digital payments.

But civil society, researchers and other non-state actors have raised concerns about exclusion from essential services linked to authentication failures, challenges around informed consent and data governance, risks associated with the centralisation and sharing of personal data, and the adequacy of accountability and redress mechanisms.

> **Takeaway:**
> This case study demonstrates both the positive, transformative potential of DPI and the importance of assessing human rights impacts throughout its lifecycle. It highlights the need for robust safeguards, effective oversight, and ongoing evaluation as DPI initiatives evolve and expand.

Uganda's National Identification System (Ndaga Muntu)

Uganda's national identity system, known as Ndaga Muntu, was introduced in 2014 with the stated aims of strengthening identity management, supporting access to public services and improving electoral administration.

As with India Stack, it has also brought human rights challenges. Reports have documented the exclusion of more than 500,000 people from national identification, limiting access to services and civic participation. And concerns have been raised about failures in biometric enrolment and authentication, which disproportionately impact elderly, rural and otherwise underserved populations.

These issues came to the fore in Uganda's contentious 2021 general election, where the national ID system was used for voter registration and electoral verification. The use of DPI in an election with disputed results intensified scrutiny around transparency, accountability, and public trust in both the technology and the broader electoral process.

> **Takeaway:**
> *Uganda's DPI experience shows the importance of assessing how design, implementation and governance choices can impact different user groups, especially in instances (like elections) where digital identity is required to exercise fundamental rights.*

The limits of existing frameworks

Existing HRIA methodologies, such as those developed by the Danish Institute for Human Rights[15], offer valuable tools but may not be fully equipped to address DPI's unique characteristics. Existing HRIA methodologies may also have been designed for use by specific actors in mind, which may limit their relevance to the many actors involved in the creation and deployment of DPI[16]. There is an increasing body of work which focuses on specific technologies, particularly technology which employ algorithms or artificial intelligence, a relevant example is the HUDERIA Methodology adopted by the Council of Europe Committee on Artificial Intelligence[17].

DPI is best understood as **an approach to creating and deploying technology, rather than a specific technology or set of technologies**. As it involves different building blocks which can be flexibly deployed for a number of different applications, existing or general frameworks may be unsuitable or focus on human rights impacts which are not relevant for DPI. Features of DPI which call for a specific approach to HRIAs include:

- **Interdependence**: DPI is built from interoperable "building blocks," meaning that impacts in one component (e.g., identity) can cascade into others (e.g., payments or data-sharing).
- **Many actors**: DPI often brings together public and private actors, and the characteristics of institutions and organisations involved may raise specific risks and raise questions about shared accountability.
- **Entrenched position**: Once deployed, DPI becomes deeply embedded in public administration and service delivery, making ex-post remedy of harm complex.
- **Regulatory environment**: Due to the complex nature of DPI, it may be impacted by complicated and overlapping regulations and laws (e.g., data protection, cybersecurity, telecommunications and public procurement laws). In other cases, DPI deployments occur in contexts with limited institutional safeguards, where regulatory or legal frameworks are lacking.
- **Accountability Building**: When DPI inception happens in a context lacking transparency and institutional safeguards, its design and implementation have to factor the institutional and procedural elements to build accountability. Society needs to be able to scrutinise the decision making to put them in place, their functioning, and be able to identify risks to human rights.

This framework responds to these gaps by providing a DPI-specific Human Rights Impact Assessment (HRIA) model that can be applied flexibly across institutional and social contexts. It aims to provide practical guidance for relevant actors to identify, mitigate, and monitor human rights and rule-of-law risks at every stage of a DPI initiative's lifecycle.

Ultimately, the DPI HRIA framework seeks to operationalise human rights due diligence in digital transformation processes throughout their whole lifecycle, ensuring that digital infrastructures are not only efficient and interoperable but also inclusive, safe, and rights-respecting by design.

Human Rights and Rule of Law as a Framework

Human rights and rule of law offer internationally recognised guidelines to ensure DPI is accountable, rights-respecting and inclusive.

Grounding DPI assessment in human rights and rule of law offers several distinct advantages from an accountability perspective.

First, human rights and the rule of law are **part of the international legal order and benefit from the broad recognition of United Nations member states**.

Second, **UN human rights bodies** such as the Human Rights Council, the Office of the High Commissioner on Human Rights (OHCHR) and Special Rapporteurs **have already done substantial work to unpack the impacts of digital technologies on human rights and rule of law**.

Third, there is **growing interest in embedding human rights considerations into technical bodies**[18] and specialised bodies and treaties concerned with accountability in technologies, particularly AI[19].

Overall, human rights and the rule of law offer us the best approach to address the risks and impacts of DPI creation and deployment. As a framework it **enables us to understand the key factors underpinning accountable and right-respecting design and deployment of DPI**. This helps ensure digital infrastructures are not only efficient and interoperable but also centred in human dignity, inclusive and sustainable development.

UN work relevant to DPI

UN General Assembly (UNGA)

- Resolution "Right to privacy in the digital age" (2022) — A/RES/77/211
- Resolution "Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development" (2024) — A/RES/78/L.49
- Resolution "Promotion and protection of human rights in the context of digital technologies" (2025) — A/C.3/80/L.46/Rev.1

Human Rights Council (HRC)

- Resolution "The Promotion, protection and enjoyment of human rights on the Internet" (2021) — A/HRC/RES/47/16
- Resolution "New and emerging digital technologies and human rights" (2023) — A/HRC/RES/53/29
- Resolution "The Right to privacy in the digital age" (2023) — A/HRC/RES/54/21

OHCHR

- "The right to privacy in the digital age" Report of the Office of the United Nations High Commissioner for Human Rights (2025) - A/HRC/60/45
- Mapping report: human rights and new and emerging digital technologies - Report of the Office of the United Nations High Commissioner for Human Rights - A/HRC/56/45
- The right to privacy in the digital age - Report of the United Nations High Commissioner for Human Rights (2021) - A/HRC/48/31

Special Procedures

- Digital Welfare. Report of the Special Rapporteur on extreme poverty and human rights (2019) — A/74/493
- Surveillance and human rights. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression — A/HRC/41/35
- Facial Recognition Technology Protecting Human Rights in Law Enforcement, Counter-Terrorism and National Security Contexts, Position Paper, June 2026

United Nations Development Programme (UNDP)

- Digital Development Compass
- Universal Digital Public Infrastructure Safeguards Framework

2

Methodology

This section outlines the **overall structure, core concepts and participants** needed to evaluate DPI in line with international human rights standards. It also proposes an overarching assessment methodology that can guide the design, execution, and interpretation of DPI HRIAs.

Key points

- This is **a framework, not a tool.** It purposely leaves room for the future development of practical toolkits and sector-specific methodologies.
- Meaningful involvement of rights-holders, affected communities, marginalised groups, experts, and other actors in the ecosystem is critical for **building trust, understanding impacts and ensuring accountability**.
- The participation of these stakeholders should be embedded **at every stage** of a HRIA
- HRIAs should operate **across the full lifecycle of a DPI.** This ensures iterative risk identification and management rather than one-off evaluation.

Scope

When to use this framework

The framework aims to support assessments at multiple stages of a DPI initiative. It can inform early-stage development, guide ongoing monitoring and review, and aid in evaluating the long-term impacts of systems once deployed.

In addition, it can be used to review the impacts of a system in the process of closing down part or the whole of a system. **It is therefore suitable for use throughout the lifecycle of a DPI project**. Given the diversity of institutional arrangements and stakeholder roles within DPI ecosystems, it is important that the framework is adaptable to different contexts.

A framework — not a tool

This document presents a framework for assessing the human rights implications of DPI. It is not a Human Rights Impact Assessment tool. Rather than providing step-by-step templates or data collection instruments, the framework establishes the theoretical and conceptual foundation upon which DPI-specific HRIAs can be designed and implemented.

The framework outlines the overall structure and core concepts needed to evaluate DPI in line with international human rights standards. It also proposes an overarching assessment methodology that can guide the design, execution, and interpretation of DPI HRIAs. However, it does not prescribe specific format, indicators or procedures for evidence gathering and measurement.

In this sense, the framework should be viewed as a first step. It provides the intellectual and normative grounding for DPI assessments, while recognising that further work is required to translate it into an operational tool. There is an opportunity to expand the framework into a comprehensive DPI HRIA toolkit, with sector-specific methodologies, data collection templates and practical guidance for implementation.

Actors involved in DPI

DPI ecosystems involve a range of actors, including governments, private companies, international organisations and civil society[20].

All of these actors contribute to the design, deployment and governance of digital systems. For this reason, the framework **aims to be flexible and adaptable**, serving as a shared reference point for any actor engaged in DPI development or oversight:

- **Governments** may use the framework to inform policy design, procurement processes and oversight mechanisms. It can help them to integrate human rights due diligence into national digital transformation strategies and guide the planning, commissioning and operation of DPI initiatives.
- **Regulatory, judicial and enforcement bodies** may use the framework to evaluate DPI initiatives when assessing compliance, adjudicating claims, or reviewing the legality of digital systems.
- **Companies that design, deliver, or operate core components of DPI**, or 'building blocks', can use the framework to understand how the choices they make can impact human rights and how to mitigate these.
- **Companies that build services or applications on top of DPI** may use the framework to understand how the foundational systems underpinning their work create specific human rights considerations. By recognising the interdependence of DPI building blocks and downstream use cases, the framework can help these organisations anticipate and mitigate wider impacts linked to the systems they rely on.
- **Technical developers and system architects**, whether working for public agencies, state-owned enterprises or private sector companies, can use the framework to understand the human rights implications of design choices.
- **Civil society organisations and human rights advocates** can draw on the framework to evaluate DPI initiatives, identify areas of risk and engage constructively with governments and private actors. It aims to support evidence-based advocacy by offering an approach to understanding human rights impacts.
- **International organisations and development partners**, including development banks and philanthropic initiatives, may use the framework to guide support for DPI initiatives, ensuring that assistance is aligned with international human rights standards and that programmes include adequate risk assessment and mitigation processes.

Participatory approach

Primary users of DPI often identify risks that technical or institutional perspectives miss. Including their voices is an essential part of building trust and accountability.

The value of a participatory approach

A participatory approach to HRIAs means bringing together **stakeholders involved in the procurement, design, deployment and operation of a digital system, along with individuals and communities who may be affected by it.**

This should be treated as a core element of the assessment process. Without meaningful engagement with those who will interact with the technology in practice, it is not possible to fully understand its potential or actual human rights impacts. This is **particularly important for people from communities that have historically experienced marginalisation or exclusion**. Their experiences can reveal risks that are not visible through institutional or technical perspectives alone. The people who use or are intended to use a service are often referred to as **rights-holders**. Referring to them in this manner helps to underline that this group has specific rights when it comes to a service and that other stakeholder groups may hold responsibilities towards them[21].

For a HRIA to be useful, **it must take a participatory approach**. However, there are other benefits to taking a participatory approach to an assessment – **including increased public transparency, leading to greater trust**. Given the nature of DPI, this trust can be an important driver for adoption and use.

Digital public infrastructure may be used by other entities than intended beneficiaries. In many cases, **DPI functions as a foundational system that other actors rely on or build upon.**

Participation should be structured and embedded **at every stage of an assessment**, from scoping and risk identification through to mitigation and follow-up. Section 3 offers suggestions on how to ensure each stage of an assessment is participatory.

Who should be involved in a HRIA?

Beneficiaries and impacted communities

We are referring here to two distinctive groups of rightsholders by inclusion or exclusion: **primary DPI users** (those using it 2on a daily basis, whose rights are most likely to be impacted); and communities whose rights are impacted by their **exclusion from systems**. Particular attention should be given to groups facing structural exclusion, including women, LGBTQ+, migrants, displaced people, informal workers, persons with disabilities, elder, Indigenous and rural communities.

Proxies for rightsholders and external experts

Where direct participation is not feasible, credible proxies for the views of affected people or groups may be engaged. These may include grassroots organizations, civil society organisations, trade unions, community-based groups, and faith-based organisations with trusted relationships and contextual knowledge.

Individuals and organisations with expertise in human rights.

This includes those with knowledge of digital rights, as well as technical experts with system-level understanding of areas such as data architecture, security, and interoperability. Such perspectives can complement lived experience and operational perspectives. Social scientists and development practitioners with contextual knowledge are also important, particularly those with experience analysing sociotechnical systems. Their perspectives can help bridge the gap between technical design choices and social, economic, and political realities, strengthening the overall quality of the assessment.

Responsible Authorities

Public sector agents responsible for policy development, governance, procurement, and oversight of DPI systems are often best placed to have an overview of potential impacts, have the greatest ability to mitigate any impacts, and may be directly responsible for human rights impacts. These responsible authorities are also likely to lead or commission external assessments.

Given the broad-reaching impact of DPI and its use across government, many different responsible authorities may need to be involved in an assessment. It is necessary, therefore, to consider who should be involved beyond the agency with responsibility for procuring or designing a system. Local authorities or arms length bodies may use DPI for example, and may be best positioned to understand how it is deployed in practice and the impact on beneficiaries. As discussed in Section 3, a key element of planning an assessment is understanding who uses a DPI within government and securing their participation.

Ecosystem operators

Many DPI projects rely on private sector actors to deliver elements of project design, delivery, or operationalisation. Private suppliers, vendors, and system architects play a critical role in shaping design choices and operational practices and should therefore be included. Entities responsible for storing, processing, or sharing data used by DPI systems are central to understanding data protection and privacy risks.

Companies that rely on DPI systems

Developers and technical communities building on DPI components, including open-source contributors, can provide insights into downstream human rights impacts. For this reason, a participatory approach must also consider the full value chain. Relevant actors to include in an assessment may include companies using DPI, for example companies using digital identity systems for eKYC purposes, organisations storing or processing sensitive personal data used by DPI systems, and developers building services or applications on top of open-source components created through DPI initiatives.

Sociotechnical framing

A HRIA for a DPI is not a one off, 'check box' exercise. It requires a diverse set of stakeholders (outlined above) and an approach to technology design, selection and implementation that is sensitive to both its technical and social aspects.

In some cases, risks arise from the context in which DPI is created or implemented, rather than inherent technological shortcomings. There are risks that relate to **function creep** or **deviation from the original purpose** of the technology's implementation.

> Each system must be analysed in terms of the specific context in which it was created and operates. This requires not only technical expertise but also **a close understanding of how local communities and individuals interact with each other and with systems.**

A recent report by **Datasphere Initiative** captures this idea well[23]:

"Trust is a critical dimension of successful DPI implementation that is still too often overlooked [...] Across contexts, evidence points to recurring trust-related challenges: exclusion of marginalized groups from identity systems, weak accountability for biometric surveillance 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 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". (emphasis added)

Trust in DPI implementation flows from effective accountability. Even before inception, sociotechnical framing requires **a governance design able to factor in the lived realities of beneficiaries and impacted communities** (including the legality, necessity and proportionality assessment), as well as mechanisms for public oversight (including the role of human rights activists and media actors).

> 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.

Lifecycle evaluation

DPI does not emerge or operate as a static system. **Assessing human rights impacts across its entire lifecycle is therefore essential.**

Risks and impacts may arise, change, or intensify at different stages of a system's evolution, from conception and design through deployment and ongoing operation. Early design decisions about purpose, architecture, data use or governance may embed structural risks, while later stages may introduce new harms through scaling, repurposing, integration into additional services or changes in institutional or regulatory context. Considering the lifecycle of DPI as an element of the assessment helps to identify not only immediate risks, but also those that might emerge over time.

A lifecycle approach to assessment supports iterative risk identification and management rather than one-off evaluation. By embedding human rights assessment across all lifecycle stages (outlined on next page), **lifecycle evaluation helps ensure that DPI remains aligned with human rights and rule of law standards over time**, and that emerging risks can be identified and addressed before they manifest or compound across the DPI lifecycle or even result in irreversible harm.

Lifecycle Stages of DPI[24]

Conception and Scoping

- The initial scoping of the DPI project includes **defining the public purpose, intended users, and boundaries of the DPI and how it will be deployed**.

Strategy and Design

- Here, high-level design choices are made about **architecture, governance, data flows, and safeguards**, which shape how human rights risks may be embedded or mitigated from the outset.

Development

- Building the DPI, including testing **system performance, data quality and accessibility before deployment** – a key juncture to profile and prevent harm.

Deployment

- Rolling out the DPI into real-world settings and integrating it with services and institutions, **where contextual factors and operational practices can significantly alter the risk profile**.

Operations and Maintenance:

- Active use and maintenance of DPI, requiring **ongoing monitoring, human oversight, and responsiveness to emerging risks**, misuse, or exclusion.

Decommissioning or transition

- Retiring or replacing the DPI, a point when it becomes necessary to **consider continuity of essential services, protection, deletion and portability of data,** and avoidance of new harms during transition to another system.

3

Framework

This section outlines four different stages of a **Human Rights Impact Assessment (HRIA) framework for DPI**. Rather than being seen as prescriptive, it aims to provide adaptable guidance.

1 **Planning and Context Assessment**
Define scope of DPI initiative, identify stakeholders, understand how the system is used, analyse the legal, institutional, social, and technical context in which it operates.

2 **Data Collection and Human Rights Risk Measurement**
Gather evidence to identify potentially affected rights, understand how risks may manifest, and evaluate severity, likelihood, scale, and reversibility.

3 **Mitigation Measures Design and Rollout**
Develop and implement safeguards to prevent, reduce, or remedy adverse human rights impacts. These should be proportionate to risks identified and tailored to the specific context of deployment.

4 **Ongoing Evaluation and Impact Management**
A HRIA is not a one-off exercise. This phase supports continuous monitoring, evaluation, accountability, and adaptation as systems evolve and new risks emerge.

Stage 1
Planning & Context Assessment

Purpose of this stage

This phase lays the foundation for the HRIA. It establishes the scope of the assessment, identifies key stakeholders and how to include them, and builds a shared understanding of the DPI system and its operating context.

This phase is particularly important because **DPI is typically deployed at scale, supports access to essential services, and involves multiple public and private actors across a complex ecosystem**. Decisions taken at this stage shape what risks are identified, whose perspectives are considered, and which impacts may ultimately be overlooked.

Questions to consider

- ☑ Is scope of assessment clearly defined?
- ☑ Do you have a shared understanding of how the DPI operates in practice and who uses it?
- ☑ Have all relevant stakeholders, including affected communities been identified?
- ☑ Which sectors, services or use cases may present elevated risks to human rights and rule of law?
- ☑ What socio-technical factors may influence potential impacts?

Scoping the DPI assessment

The first step is to **establish a shared understanding of the DPI initiative** that is being assessed. This should include clarity on the nature, purpose, and boundaries of the system, and the problems it is intended to address.

However, this information is not sufficient to reflect the ways in which it is actually used in practice. Scoping should recognise that DPI often functions as a **foundational layer** on which other systems, services, or decisions depend. Mapping the ways in which DPI is used across government agencies and services and by other, potentially private sector, actors is therefore a vital first step. This includes understanding whether the DPI provides or mediates access to essential public or private services as this can significantly impact the likelihood and severity of adverse human rights impacts[25].

An important element of understanding actual use will be **assessing the lifecycle of the DPI, or the maturity of how it is being used**. In one context, its use may be well-established, while another government agency may be piloting using it in a new context. It is important to record this information as different lifecycle stages present different risks to human rights.

Understanding how a DPI is used is inextricably linked to understanding who uses it. This includes the range of actors involved in governance, procurement, development, operation, and downstream use of a DPI. These actors will likely hold the information necessary for a comprehensive assessment and effort should be made to fully map the ecosystem of users. In addition, as previously addressed in section 2.3, mapping the actual or anticipated beneficiaries of DPI and impacted communities with the aim of including their perspectives is a foundational step in any assessment. As highlighted above, this includes mapping the populations who may be excluded from using DPI, as they may experience adverse human rights impacts.

The information collected would shed light on crucial questions around on the necessity and proportionality of adoption of the DPI initiative, enabling the examination of alternative pathways to avoid or reduce human rights impacts.

Sectoral use of DPI and implications for human rights

Human rights impacts are **heavily influenced by the specific domains or sectors where DPI is implemented**. Because DPI often involves safety-critical sectors or access to essential services, many deployment areas are inherently high-risk from a human rights standpoint. Where DPI enables or conditions access to essential services, any interruption, error, or exclusion can have immediate and serious consequences. For example, incorrect data may prevent individuals from accessing healthcare or social benefits, while mandatory use may disproportionately affect people with limited documentation, connectivity, or digital literacy[26].

The sectoral risk profile may also be reflected in **the degree of regulatory oversight applied to the domain[27]**. Sectors subject to extensive regulation often indicate historically recognised risks to safety, equality, or fundamental rights. Conversely, weak, fragmented, or unclear regulation may increase the likelihood that human rights risks are insufficiently anticipated or addressed[28]. Scoping should therefore explicitly document the sectors in which the DPI is used, assess the sensitivity of those sectors from a human rights perspective, and consider how sector-specific practices, norms, and regulatory frameworks interact with the design and operation of the DPI. This analysis provides an important foundation for prioritising risks and tailoring the depth and focus of subsequent stages of the HRIA.

The non-exhaustive following table **illustrates the link between DPI development in a sector or domain and possible human rights impacts**. It shows that interactions are complex with frequent impact overlapping over a range of human rights that can be exacerbated in intensity for the domain and sector concerned.

Human rights impacted	DPI type	Use in sector/domain	How the impact can manifest
Freedom from Physical and Psychological Harm	Digital ID, monitoring tools, smart cities, predictive analysis, automated decision making, cloud computing, data sharing and registries.	Access to essential services, public safety and security	• Massive surveillance in public spaces • Arbitrary detention using predictive policing • Discrimination in access to services
Right to Equality Before the Law and to Protection against Discrimination	Digital ID, digital payments, monitoring tools, smart cities, predictive analysis, automated decision making, cloud computing, data sharing and registries.	Access to essential services, civic engagement, public safety and security, predictive policing, migration.	• Allocation of social benefits • Access to employment, education or housing • Access to justice
Right to Privacy	Digital ID, digital payments, monitoring tools, smart cities, predictive analysis, automated decision making, cloud computing, data sharing and registries.	Access to essential services, civic engagement, public safety and security, predictive policing, migration.	• Massive surveillance in public spaces • Targeted surveillance • Exposure of personal data (including biometrics) to malicious actors
Right to Own Property	Digital ID, digital payments, monitoring tools, predictive analysis, automated decision making, cloud computing, data sharing and registries.	Access to essential services, files handling.	• Limitations to access to payment systems • Exclusion from property registers access • Discrimination in access to services

Freedom of Expression and Access to Information	Digital ID, digital payments, participation platforms, monitoring tools, smart cities, predictive analysis, automated decision making, cloud computing, data sharing and registries.	Civic engagement, public safety and security, predictive policing, migration.	• Massive and targeted surveillance in physical spaces • Surveillance and censorship in digital spaces
Freedom of peaceful assembly and association	Digital ID, digital payments, participation platforms, monitoring tools, smart cities, predictive analysis, automated decision making, cloud computing, data sharing and registries.	Civic engagement, public safety and security, predictive policing, migration, files handling.	• Repression in public manifestations • Surveillance and censorship of social organising in digital spaces • Selective repression of migrants or social movements
Freedom of movement and residence	Digital ID, digital payments, monitoring tools, smart cities, predictive analysis, automated decision making, cloud computing, data sharing and registries.	Housing allocation, transport services, public safety and security, predictive policing, migration.	• Massive surveillance in public spaces • Arbitrary detention using predictive policing • Selective repression of migrants or social movements
Right to a Nationality	Digital ID	Access to essential services, civic engagement, public safety and security, predictive policing, migration.	• Statelessness • Essential services exclusion
Right to Take Part in Public Affairs	Digital ID, participation platforms, monitoring tools, predictive analysis, automated decision making, cloud computing, data sharing and registries.	Civic engagement, electronic vote, electoral oversight.	• Vote suppression through exclusion of e-voting systems • Exclusion of vulnerable groups or social movements

Right to Work and to Gain a Living	Digital ID, digital payments, monitoring tools, predictive analysis, automated decision making, cloud computing, data sharing and registries.	Access to essential services, procurement, entrepreneurship support.	• Discrimination in access to employment opportunities • Discrimination in allocation of unemployment benefits
Right to Health	Digital ID, digital payments, monitoring tools, predictive analysis, automated decision making, cloud computing, data sharing and registries.	Access to essential services, healthcare.	• Discrimination in access to healthcare • Discrimination in insurance coverage • Blocking of services by malicious actors
Right to Education	Digital ID, monitoring tools, predictive analysis, automated decision making, cloud computing, data sharing and registries.	Resource allocation, desertion prediction, early intervention, e-learning, files handling.	• Discrimination in access to education • Access to children personal data by malicious actors
Right to social security	Digital ID, digital payments, monitoring tools, predictive analysis, automated decision making, cloud computing, data sharing and registries.	Access to essential services, benefits allocation, early intervention in vulnerable cases, remote assistance, files handling.	• Discrimination in allocation of benefits • Exclusion of vulnerable groups
Rights of the Child	Digital ID, digital payments, monitoring tools, predictive analysis, automated decision making, cloud computing, data sharing and registries.	Benefits allocation, early intervention in vulnerable cases, files handling.	• Discrimination against vulnerable groups • Access to children personal data by malicious actors

Designing a participatory process

A participatory approach should be embedded in the planning stage. Participation helps ensure that the assessment reflects lived experience, power asymmetries, and real-world patterns of use. A participatory approach should be embedded in the planning stage.

To design a participatory approach which is comprehensive and inclusive, assessors should:

- **Conduct early stakeholder mapping** to identify rights-holders, duty-bearers, and responsibility holders across the DPI ecosystem;
- **Identify power imbalances**, barriers to participation, and risks of exclusion;
- **Reach out to participants in good time**, clearly delineate the risks and benefits of participation, and explain how input will influence decisions and outcomes to ensure that participation avoids being extractive.

During the planning stage of the assessment a participatory approach should be used to:

- **Validate assumptions** about system purpose, beneficiaries, and risks with prospective users;
- **Co-define the scope and priorities of the HRIA** with affected groups or their representatives to ensure that measurement reflects the "messy reality" of DPI deployment[29].

Where DPI is used in high-impact contexts or sectors, **deeper, broader or more continuous engagement** is required.

It is essential to clearly communicate the scope of stakeholder participation processes at an early stage, as this shapes expectations and directly influences the outcomes of the process.

Context Assessment

The context assessment examines the conditions in which the DPI is developed, deployed, and used, and how those conditions shape potential risks to human rights.

For DPI, **context is not neutral.** Because these systems often enable access to identity, financial services, healthcare, education, or social protection, failures or exclusions can have severe and immediate consequences. Where DPI is closely connected to decision-making, enforcement, or eligibility determination, the likelihood and severity of human rights impacts increases.

The context assessment therefore provides **a structured way to anticipate risk before it manifests**, drawing on legal, social, technical, and institutional factors. There are a number of different categories for the contextual assessment.

Context category	What this category means	Why this matters for a DPI HRIA	Examples of context that may raise or lower risk
Nature of the technology	The technical characteristics of the DPI, including interoperability, potential for repurposing, and system limitations.	DPI is often designed to be reusable and extensible, increasing the risk of scope creep, dual use, or deployment beyond the original safeguards.	Open APIs, interoperability with third-party systems, unclear constraints on downstream use, lack of understanding of downstream use.
Appropriateness to the problem	Whether the DPI is a suitable and proportionate response to the problem it is intended to solve.	Deploying DPI to address social or policy problems can introduce new risks without addressing root causes, potentially creating avoidable harms.	Evidence that non-digital or less intrusive alternatives were considered; clarity on the problem definition; alignment between system design and policy goals.
Technological maturity	The extent to which the technology is experimental, emerging, or well-established.	Immature or untested technologies may increase uncertainty and the likelihood of unforeseen impacts, particularly at scale.	Pilot deployments, prior use in comparable contexts, independent evaluations, documented limitations.
Scope of deployment	The geographic, demographic, and temporal reach of the DPI.	Scale amplifies impact. DPI systems deployed population-wide, to serve vulnerable groups or over long periods carry higher cumulative human rights risks.	Local versus national deployment; number of people affected; vulnerable groups interacting with it; mandatory versus voluntary use; long-term reliance on the system.

Data quality	The representativeness, accuracy, completeness, and relevance of data used by the DPI.	Poor data quality or lack of pertinence for the relevant population can lead to biased, discriminatory, or exclusionary outcomes, especially for marginalised groups.	Known biases or gaps in datasets; local or foreign data sets; use of proxies; lack of updating mechanisms; traceability of data sources.
Beneficiaries and affected groups	The individuals and groups intended to benefit from the DPI, as well as those indirectly affected or excluded.	DPI may benefit some groups while disadvantaging others, particularly where access is conditional on documentation, connectivity, or digital literacy.	Actual or intended use by children, elders, migrants, persons with disabilities, informal workers, indigenous population, rural populations, or undocumented groups.
Inclusiveness	The extent to which the DPI can be accessed and used without discrimination, and whether alternatives exist.	When DPI becomes a gateway to essential services, lack of inclusiveness can entrench inequality and exclusion.	Accessibility features, language support, offline alternatives, reasonable accommodations, opt-out mechanisms.
Regulatory environment	The legal and policy frameworks governing the DPI and the sector in which it operates.	Strong regulation may mitigate risk, while weak, fragmented, or conflicting frameworks may enable harm or reduce accountability.	Data protection laws, sectoral regulation, oversight bodies, enforcement capacity, regulatory gaps.
Human oversight and accountability	Mechanisms for monitoring, intervention, redress, and review throughout the DPI lifecycle.	Without effective oversight and accountability, harms may persist, escalate, or go unremedied.	Complaint mechanisms, audit processes, independent oversight bodies, access to remedy for affected individuals.

Cybersecurity and data protection	The resilience of the system against misuse, breaches, and malicious attacks, and safeguards for personal data.	Security failures can expose individuals to fraud, surveillance, identity theft, or exclusion from essential services.	Threat modelling, breach response plans, encryption practices, access controls, data governance arrangements.
Institutional and Governance capacity	The ability of the DPI operators to understand the functioning of the systems and its interaction with the relevant population is essential to identify, prevent and mitigate human rights impacts.	The DPI approach implies many public and private services might be involved in the DPI design, deployment and use. Those actors should be multidisciplinary trained in advance and during the whole lifecycle of the DPI.	Technical training on the systems capacities and limitations; socio-technical training or external expertise; human rights training.
Rule of Law and Peace	Absence of institutional structure to guarantee the rule of law and ensure social peace.	Any HRIA would need to deal with the institutional limitations to offer accountability.	DPI insertion in a context affected by fragility of rule of law, conflict and violence increase the risks of deviation of purpose and lack of accountability.

Stage 2

Data Collection & Human Rights Risks Measurement

Purpose of this stage

This stage is about gathering information to understand how humans and systems interact in the DPI's implementation. Using the mapping and assessment design developed in Stage 1, now assessors collect and analyse information to identify, measure, and prioritise human rights risks.

Note: If information gathering has already begun during the context assessment stage, this phase provides an opportunity to expand both the evidence collected and the range of sources consulted.

Questions to consider

- ☑ Have you gathered evidence from diverse perspectives?
- ☑ Have affected communities had the opportunity to participate?
- ☑ Which human rights may be affected, and in what ways?
- ☑ How likely are identified risks to occur, and how severe could their impacts be?
- ☑ Are there certain groups likely to be disproportionately affected?
- ☑ Which risks should be prioritised for mitigation?

Data gathering strategies

Data collection has **two key dimensions**: what should be collected, and how it should be collected to ensure relevance and accuracy. Data gathering methods should include desk research (previous initiatives, statistical data, academic and civil society reports); interviews with internal and external stakeholders, including proxies, experts, users and intended beneficiaries; visits to spaces where the initiative would be deployed; and community gatherings. Data collection can be time- and resource- intensive, so the design of this stage should be attentive to scope and aims. There are less structured ways to collect data that can be effective for particular contexts of application, such leveraging the presence of public agencies or civil society actors already deployed and providing services in situ.

The data collected should provide a quantitative and qualitative approach to risk measurement. Therefore, it needs to be useful to understand the baseline reality of the populations intended to be served by the DPI initiatives in terms of their exercise of human rights and the application of the rule of law.

Extensive data collection is necessary for risk assessment. But methodologies should also prioritize personal data minimization, anonymization, and the avoidance of unnecessary identification of individuals or communities. This is particularly relevant in DPI contexts, where data collection practices may inadvertently enable surveillance, profiling, or other forms of disproportionate monitoring, especially among already vulnerable populations.

Identifying Impacted Human Rights

A multidimensional approach to assessment helps identify which rights might be impacted by a DPI deployment, and how intense these impacts might be.

For the purpose of this framework, we have drawn on the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social, and Cultural Rights (ICESCR) and other instruments,

We suggest considering the following list of potentially impacted rights:

- **Freedom from Physical and Psychological Harm**
- **Right to Equality Before the Law and to Protection against Discrimination**
- **Right to Privacy**
- **Right to Own Property**
- **Freedom of Thought, Religion, Conscience and Opinion**
- **Freedom of Expression and Access to Information**
- **Freedom of peaceful assembly and association**
- **Access to Justice and fair trial guarantees**
- **Right to Take Part in Public Affairs**
- **Right to Work and to Gain a Living**
- **Right to Health**
- **Right to Education**
- **Right to social security**
- **Rights of the Child**
- **Environmental Rights**
- **Rights of indigenous people,**
- **Right to a nationality**
- **Prohibition of discrimination**

Measuring human rights impacts

Measuring the human rights impacts of DPI requires a mixed-methods approach that reflects its scale, interdependence, and the variety of actors involved. As set out in Section 3.2, measurement should combine desk research with interviews, consultations, and observation in deployment settings to build a baseline understanding of how rights are realised in practice and how people experience the system. A comprehensive HRIA integrates multiple sources of evidence and pays attention to impacts, including those that arise downstream through integration into services or decision-making processes.

Understanding the nature of risks

Understanding the nature of risk requires more than identifying which human rights may be affected. It also requires analysing **how a risk manifests**, **how severe it may be**, and **how it is likely to evolve over time**.

- **Scope**: The scope of the risk determines how widely mitigation must be applied. Risks affecting a specific right through a single service or use case may be addressed through targeted safeguards. Risks arising from core DPI components that impact a wide range of rights require system-wide mitigation or might advise against deployment at all.
- **Scale**: The scale of impact influences the urgency and robustness of mitigation. Population-wide or mandatory systems require stronger preventative measures and contingency planning than limited or voluntary deployments.
- **Reversibility**: Where harms are difficult or impossible to reverse – such as exclusion from essential services or long-term data misuse – mitigation should prioritise prevention and fail-safe mechanisms rather than ex post remedies.
- **Probability**: High-likelihood risks should be addressed early and proactively, while lower-probability risks may require monitoring and escalation pathways.
- **Proximity**: Describes how directly the DPI contributes to decision-making or action. Where DPI directly determines eligibility, enforcement, or access, mitigation must focus on accuracy, oversight, and procedural safeguards.

These dimensions reveal how the infrastructural nature of DPI can amplify human rights impacts. DPI is often deployed at population scale, embedded in essential services, and reused across multiple contexts, meaning that even small design or governance failures can have widespread and lasting consequences. Assessing scope and scale **highlights how harms may cascade across services**[30], while reversibility draws attention to risks that are difficult to undo once systems are entrenched. Probability and proximity help clarify whether DPI directly shapes decisions about access, eligibility, or enforcement, or whether impacts arise more indirectly through downstream use.

These dimensions help **distinguish between risks that are local or systemic, temporary or long-term, and speculative or highly likely**, which is essential for prioritisation and proportionality. Key dimensions help us measure the likelihood of a risk-taking place, the severity of that risk, and to what extent that risk is preventable or reversible[31].

The identification and measurement of human rights impacts should apply an intersectional lens. Gender, including the experiences of women and LGBTQ+ groups, race, class and other social markers should be considered across the assessment.

Taken together, these dimensions will build a profile of the risk of adverse human rights impacts. As we propose in Stage 3, **any mitigation measures should be explicitly mapped against these dimensions**, with justification provided for why proposed actions are adequate in light of the assessed risk profile. When designing as assessment for DPI, assessors may apply a scoring system to these dimensions to assist with such justifications.

Positionality

Understanding the position of an actor in relation to a specific DPI helps to clarify both responsibility and the capacity to prevent, mitigate, or remediate harm. For state actors, this responsibility is anchored in their obligations under human rights law; for companies, in the UN Guiding Principles on Business and Human Rights (UNGPs)[32].

DPI typically involves multiple public and private actors whose roles may overlap or evolve over time. As a result, attribution of risk cannot be reduced to a single responsible entity. Instead, it requires an analysis of how actions, decisions and relationships across the ecosystem contribute to human rights outcomes.

In line with the UN Guiding Principles on Business and Human Rights, a useful framing to understand positionality is **whether an entity causes, contributes, is linked to, or is not connected to a human rights harm**[33]:

- **Causation**: An actor causes an adverse human rights impact when its own actions or decisions directly result in the harm. In digital contexts, this includes harms that arise directly from how a DPI is designed, deployed, or used.
- **Contribution**: An actor contributes to an adverse human rights impact when its actions, together with those of others, help bring about the harm, even if it is not the sole or primary cause. Contribution may occur through design choices, data practices, procurement decisions, or failure to prevent foreseeable risks.
- **Directly Linked**: An actor is linked to an adverse human rights impact when the harm is directly connected to its operations, products, services, or technology use through a relationship or value chain, even if the actor did not cause or contribute to the impact. This includes impacts arising at

any stage of the technology lifecycle or ecosystem. Linkage is particularly relevant to DPI, due to its nature as foundational building blocks and the high potential for it to be used in a number of ways by a number of actors.

- **Not connected**: An actor is not connected to an adverse human rights impact when there is no causal, contributory, or meaningful relational link between its activities or technology use and the harm. Where no such nexus exists, the impact falls outside the scope of that actor's human rights due diligence responsibilities.
- **Impacted**: a rights-holder may be connected to but not responsible for human rights impact. Including such actors in a positionality mapping can help In the design of appropriate mitigation measures.

These categories are **neither static nor mutually exclusive**. As DPI systems evolve and governance arrangements change, an organisation's positionality, and therefore its responsibilities and capacity to act, may also shift. The purpose of this analysis is not to determine legal liability, but to support effective human rights due diligence and risk management.

Illustrative example of positionality: Digital ID system

Actor	Role in DPI	Positionality	Ability to mitigate or change outcomes
Government agency	Creating design specifications, procurement, data collection, operation.	Causation	High
Company designing mobile-based application	Application design and user interface development	Causation	High
Company providing data exchange system	Enabling interoperability and data flows	Contribution	Medium
Company using Digital ID for eKYC	Downstream use of DPI for customer verification	Connected	Low
Citizen using Digital ID	Rights-holder interacting with the system	Impacted	None

Challenges of measuring human rights risks

Assessing human rights risks for DPI presents **specific methodological challenges**. These arise both from the characteristics of DPI itself and from the complexity of attributing risks and harms across a distributed ecosystem of actors.

First, DPI is often deployed at population scale. Systems such as digital identity, payments, or data-sharing infrastructure may affect large and diverse groups of people, with impacts that vary significantly across regions, demographic groups, and use cases.

Second, certain DPI characteristics may lack transparency, especially where algorithmic decision-making is involved, or where future uses of DPI building blocks are not fully specified at the point of deployment. As DPI is designed to be reusable and interoperable, risks may only materialise once systems are integrated into new services or contexts. Information about technical components and data usage are required transparency requirements necessary to identify risks of DPI usage.

Third, data collection is complicated by the number and diversity of actors involved in the DPI ecosystem. Relevant information may be held by public authorities, private suppliers, or end beneficiaries of the infrastructure, who each have different incentives, capacities, and disclosure obligations.

Fourth, direct data may be unavailable, incorrect or insufficient to inform decision making, or not representative of the full diversity of the community. In such cases, proxy data, qualitative evidence or participatory inputs may be needed to correctly identify risks.

These challenges reinforce **the importance of a participatory[34] and iterative, lifecycle approach to assessments**. Assessing impacts across the lifecycle, rather than at one static point, will help to illuminate risks that arise downstream. Involving a broad range of stakeholders in an assessment gives a higher likelihood that the impact across a population will be better understood.

Ensuring users of a DPI, whether public or private sector actors, are well-documented and involved (where possible) in the assessment will reveal how systems are used on a day-to-day basis and the impact of their use.

Stage 3

Mitigation Measures: Design & Rollout

Purpose of this stage

This stage moves the HRIA **from risk identification to action**. It focuses on developing and evaluating measures to prevent, minimise, or remedy adverse human rights impacts, with mitigation tailored to the nature and severity of identified risks. Effective mitigation depends on understanding both the risk itself and the roles, responsibilities and capacities of actors.

Questions to consider

- ☑ What measures could prevent, reduce, or remedy identified risks?
- ☑ Which actors are best placed to implement and oversee mitigation measures?
- ☑ Have responsibilities, timelines, and accountability mechanisms been identified?
- ☑ How will ongoing efficacy of measures be assessed?
- ☑ Are there any risks that require ongoing monitoring?

Designing mitigation measures

Mitigation assessment should **explicitly consider trade-offs**, such as between efficiency and fairness, automation and human oversight, or security and accessibility. These trade-offs should be documented transparently, including dissenting views from all stakeholders and unresolved tensions.

Mitigation should not focus solely on technical fixes. Structural risks, such as those arising from mandatory use, lack of alternatives, weak oversight, or power asymmetries, must also be subject to assessment. This means being open to governance, policy, or institutional mitigation measures.

Effective mitigation measures are best designed using a participatory approach. For a fuller discussion on the value and purpose of a participatory approach please see Stage 1.

Key steps include:

- **Establishing participatory mechanisms** including user advisory groups, civil society sounding boards, and community-based monitoring partnerships.
- **Using these groups to co-design mitigation measures** with affected stakeholders and system users, particularly where risks relate to exclusion, discrimination, or access to essential services.
- **Testing proposed safeguards, design changes, and governance mechanisms** with end-users to assess usability and unintended effects.
- **Integrating companies and service providers** to understand how mitigation functions in downstream contexts.
- **Involving developers and technical maintainers** to assess feasibility, limitations, and maintenance requirements.

To ensure that a participatory approach isn't extractive and that stakeholders remain engaged, it's important that stakeholders understand the impact of their involvement. This can be achieved by producing accessible reporting on findings, decisions, and changes made to mitigate human rights impacts on the basis of stakeholder engagement.

A final key element is **the clear allocation of responsibilities** for implementing and following up on mitigation measures. This strengthens accountability and avoids dilution of responsibility for the system.

Assessing the adequacy and effectiveness of mitigation

Mitigation measures should be designed and assessed in light of the key dimensions of risk identified in Stage 2. Their adequacy and effectiveness should be assessed against clear criteria, including:

- Whether they are likely to **meaningfully reduce the likelihood or severity of harm**.
- Whether they are **proportionate to the assessed risk**.
- Whether they are **accessible and understandable to affected populations**.
- Whether they can be **implemented and sustained over time**.
- Where mitigation relies on human oversight or discretion, the assessment should examine whether **sufficient capacity, training, and authority exist to exercise that oversight effectively**.

Stage 4

Ongoing Evaluation & Impact Management

Purpose of this stage

HRIA is an ongoing process, not a one-off exercise. This stage focuses on dynamically monitoring impacts, identifying new and emerging risks and adapting safeguards as the DPI evolves.

Use this stage to test whether mitigation measures are working in practice and whether new risks have emerged.

Questions to consider

- ☑ How will impacts be monitored over time?
- ☑ Are there accessible mechanisms for feedback, complaints, and redress?
- ☑ Have new risks emerged as the DPI has evolved?
- ☑ Are mitigation measures working as intended?
- ☑ How will lessons learned inform future decisions and system changes?
- ☑ Does the DPI continue to align with rights and rule of law principles?

Reporting & Transparency

Reporting and other communication mechanisms are **essential to the effectiveness of the DPI HRIA**. They help sustain continued dialogue with stakeholders across the lifecycle of the initiative.

Reporting and transparency have a twin benefit. **First**, they address stakeholders' concerns around the impacts of the initiative. **Second**, they increase the legitimacy and relevance of the DPI initiative for the ecosystem affected by it.

The accountability of the assessment process only can be fully realised when **participating stakeholders can access its result** and trace the mitigation actions or other decisions informed by its findings.

Reporting and transparency can also provide **additional legitimacy** for the actors in charge of DPI deployment, demonstrating they have sought to align the initiative with human rights and rule of law. Communicating the assessment's results may also strengthen internal political commitment to identifying and preventing human rights and rule of law impacts as of the implementation process.

Reporting should include **relevant information on the initiative itself**, the methodology used for the assessment, data sources (including reference to engagement with stakeholders), findings of the assessment and proposed mitigation measures. This approach enables participating and non-participating stakeholders to examine the assessment, strengthen it and identify when new circumstances or information should trigger a fresh review of findings and mitigation measures.

Information should be communicated in a **user-friendly format**. Tables, timelines or diagrams can help summarise key points. Language should be accessible to both expert and non-expert readers.

Additional communication mechanisms should be considered to share report findings. This might include **a website, traditional media outreach, or in person or virtual meetings to present findings**. Particular attention should be given to reaching stakeholders that input into the assessment process.

Reporting and transparency mechanisms should **carefully balance access to relevant information with the protection of confidentiality and sensitive information**, including personal information from assessment participants and impacted groups.

Ongoing assessment

A lifecycle approach to DPI HRIA demands **ongoing assessment** of how human rights impacts are evolving or manifesting as DPI is rolled out and integrated into services and institutions. **Contextual factors and operational practices** can significantly alter the original assessment of risk profile. A sustained, systemic approach is therefore needed.

Establishing regular evaluation check points will help identify emerging issues or factors, which can be fed back into new mitigation measures or approaches. In extreme cases – when an evolved risk profile means the DPI may now be incompatible with the exercise of human rights – this may trigger a decision to sunset systems.

Mitigation measures should also be assessed across the DPI lifecycle. Measures that are appropriate at design or pilot stages may prove ineffective once a system becomes entrenched or scales up. Mitigation is iterative rather than a one-off intervention.

Transparency around the ongoing evaluation process, including reporting back to stakeholders strengthens legitimacy and creates opportunities to share lessons learned. This enables ongoing improvement of the DPI system and the HRIA process itself. At a minimum, reporting should include information about the systems assessed, the implementation context, data sources, methodology, key findings and mitigation measures, and the actors responsible for implementation[35].

Monitoring systems that enable **continuous data collection and iterative learning** throughout the DPI lifecycle are critical here. Ongoing evaluation requires institutional efforts to collect data and enable stakeholder contributions. Clarity on timeline, process, mechanisms and actors responsible should be established. Without evaluation points it is difficult to adapt DPI systems, the institutional frameworks or the regulatory environment over time. **Checkpoints help ensure DPI's alignment with the exercise of human rights** and respect for rule of law.

Impact management

Impact management should include a baseline plan for implementing the ongoing evaluation, via mitigation measures and ongoing monitoring. Responsibility for mitigation follow up and data monitoring should be clearly allocated. To increase ownership and legitimacy **the impact management plan should be developed collaboratively**, involving beneficiaries and impacted communities, their proxies or external experts, public actors and ecosystem operators.

Impact management should also **assess whether accountability and redress mechanisms are robust and appropriate.** This includes examining formal mechanisms for raising concerns about system functioning and impacts, the capacity of public actors and system operators to process claims and integrate them into the lifecycle assessment, and the ability to provide redress to impacted stakeholders. **Effective grievance mechanisms should be accessible**, use clear and direct language, be transparent in handling and following up on claims, provide opportunities to escalate, and offer remedy when negative impacts are identified.

Dialogue should be considered part of remedy design, including with beneficiaries, impacted communities and their proxies. External human rights and rule of law experts should also be involved in evaluating the effectiveness and appropriateness of grievance mechanisms and remedies.

Grievance mechanisms can act as "**canaries**". They provide an important channel for collecting data on the impact of DPI roll out and can identify harms early. They also help assess whether mitigation measures are working as designed.

Endnotes

[1] See https://t20southafrica.org/wp-content/uploads/2025/01/TF2-Digital-Transformation-Concept-Note.pdf
[2] See https://egovernance.vikaspedia.in/viewcontent/e-governance/online-citizen-services/government-to-citizen-services-g2c/all-about-aadhaar/aadhaar-card?lgn=en
[3] See https://e-estonia.com/solutions/interoperability-services/x-road/
[4] See https://accounts.ecitizen.go.ke/en
[5] See https://portal.singpass.gov.sg/home/ui/login
[6] See https://www.gatesfoundation.org/our-work/programs/global-growth-and-opportunity/digital-public-infrastructure
[7] See https://www.worldbank.org/en/results/2023/10/12/creating-digital-public-infrastructure-for-empowerment-inclusion-and-resilience
[8] Institute for Innovation and Public Purpose, "2025 State of Digital Public Infrastructure Report", 2025, accessed here: https://dpimap.org/iipp-state-of-dpi-report-2025.pdf
[9] https://gfmd.info/cloud-alliance/
[10] See *https://www.notion.so/dpi-privacy/Privacy-in-Digital-Public-Infrastructures-23ab205f824880239987ccb7fd1e56b7*
[11] See https://www.dpi-safeguards.org/framework
[12] See https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf
[13] Datasphere Initiative, "*Sandboxes for DPI: Co-creating the blocks of digital trust"*, 2026, p. 36, accessible at: https://www.thedatasphere.org
[14] Freedom Online Coalition, "Rights-Respecting Digital Public Infrastructure Principles", October 2025, accessible at: https://freedomonlinecoalition.com/rights-respecting-dpi-principles/
[15] Danish Institute for Human Rights, "Human rights impact assessment of digital activities", 2020, accessible at: https://www.humanrights.dk/publications/human-rights-impact-assessment-digital-activities
[16] A useful reference is the tech ecosystem actor mapping provided by BSR and GNI, "Across the Stack Tool", 2022, accessible at: https://globalnetworkinitiative.org/resources/across-the-stack-tool/
[17] Council of Europe, "Methodology for the Risk and Impact Assessment of Artificial Intelligence Systems from the Point of View of Human Rights, Democracy and Rule of Law", 2024, accessible at: https://rm.coe.int/cai-2024-16rev2-methodology-for-the-risk-and-impact-assessment-of-arti/1680b2a09f
[18] See OHCHR reports, ITU resolution, The Seoul declaration
[19] It is the case of the AI International Scientific Panel on AI and the Council of Europe Framework Convention on Artificial Intelligence
[20] United Nations Office of the Secretary-General's Envoy on Emerging Technology, "The Universal DPI Safeguards Framework: A Guide to Building Safe and Inclusive DPI for Societies", September 2024, p. 18, accessible at: A Guide to Building Safe and Inclusive DPI for Societies | Universal DPI Safeguards
[21] The Danish Institute for Human Rights, "Cross-Cutting: Stakeholder Engagement Human Rights Impact Assessment Guidance and Toolbox", 2020, p. 4.

[22] Rahul Mattan, Lexology, Private companies can use Aadhaar infrastructure for identity checks again, February 5 2025, accessible at: https://www.lexology.com/library/detail.aspx?g=b975827d-10ba-489a-89d8-129017c01a3e

[23] Datasphere Initiative, "*Sandboxes for DPI: Co-creating the blocks of digital trust"*, 2026, p. 29 Accessible at: https://www.thedatasphere.org

[24] United Nations Office of the Secretary-General's Envoy on Emerging Technology, "The Universal DPI Safeguards Framework: A Guide to Building Safe and Inclusive DPI for Societies", September 2024, p. 19, accessible at: A Guide to Building Safe and Inclusive DPI for Societies | Universal DPI Safeguards

[25] Access Now, "A human rights-centered approach to digital public infrastructure", Oct 2024, accessible at: https://www.accessnow.org/guide/digital-public-infrastructure/#dpi-harms

[26] Ibid

[27] Council of Europe, Committee on Artificial Intelligence, "HUDERIA Model, Context Based Risk Analysis (COBRA) Resources", 2025, p. 5.

[28] Brookings Institute. "Digital public infrastructure for resilience in fragile contexts", March 2025, accessible at: https://www.brookings.edu/articles/digital-infrastructure-for-resilience-fragile-contexts-balancing-state-and-citizen-protection/

[29] UCL Institute for Innovation and Public Purpose, "Six Months of DPI Measurement Insights: What We've Learned from Our Community of Practice", 6 November 2025, accessible at: https://medium.com/iipp-blog/six-months-of-dpi-measurement-insights-what-weve-learned-from-our-community-of-practice-07675f485ad9

[30] Sameer Suryakant Patil, Anna Maria Collard, Balasubramanian Kalyan Kumar, Achyut Chandra, World Economic Forum, "Security-by-design lessons from India's digital public infrastructure journey", October 2025, accessible at: https://www.weforum.org/stories/2025/10/security-by-design-india-digital-public-infrastructure/

[31] The Danish Institute for Human Rights, "Guidance of HRIA on Digital Activities, Phase 3: Analysing Impacts", 2020, p. 26.

[32] OHCHR, "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework", endorsed by the the Human Rights Council resolution 17/4 of 16 June 2011, accessible at: https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf

[33] Office of the United Nations High Commissioner for Human Rights, *"The Corporate Responsibility To Respect Human Rights: An Interpretive Guide"*, 2012, p. 15; Office of the United Nations High Commissioner for Human Rights, *"Guidance of the Secretary-General: Human Rights Due Diligence for Digital Technology Use"*, 2024 p. 11-12.

[34] J.N. Matias, & M. Price, *"How public involvement can improve the science of AI"*, Proc. Natl. Acad. Sci. U.S.A. 122 (48) e2421111122, November 2025, accessible at: https://doi.org/10.1073/pnas.2421111122

[35] The Danish Institute for Human Rights, "Guidance of HRIA on Digital Activities, Phase 5: Reporting and Evaluation ", 2020, p. 17.

GLOBAL
PARTNERS
DIGITAL