CENTER FOR HUMAN RIGHTS & GLOBAL JUSTICE
NYU SCHOOL OF LAW

NYU LAW

Contesting the Foundations of Digital Public Infrastructure

What Digital ID Litigation Can Tell Us About the Future of Digital Government and Society

By Katelyn Cioffi, Victoria Adelmant, Danilo Ćurčić, Brian Kiira, Grecia Macías, and Yasah Musa

August 28, 2023

Many governments and international organizations have embraced the transformative potential of 'digital public infrastructure' (DPI)—a concept that refers to large-scale digital platforms run by or supported by governments, such as digital ID, digital payments, or data exchange platforms. However, many of these platforms remain heavily contested, and recent legal challenges in several countries have vividly demonstrated some of the risks and limitations of existing approaches. In an event organized by the Center for Human Rights and Global Justice at NYU School of Law entitled "Contesting the Foundations of Digital Public Infrastructure: What Digital ID Litigation Can Tell Us About the Future of Digital Government and Society," we discussed four case studies from Uganda, Mexico, Kenya, and Serbia. What connects the experiences in these countries is that efforts to introduce new national-scale digital platforms have had harmful impacts on the human rights of marginalized groups—and triggered legal challenges led by civil society organizations. These four examples therefore hold important lessons for policymakers, highlighting the urgent need for effective safeguards, mitigations, and remedies as the development and implementation of DPI continues to accelerate.

'Digital public infrastructure,' or DPI, has taken a strong hold at the highest levels of policymaking. Seen as a "critical enabler of digital transformation" that can "improve public service delivery at scale," the concept of DPI is being rapidly and enthusiastically embraced in countries around the world.

There is no single, authoritative definition of DPI—it remains an "evolving concept"—but the term generally refers to large-scale digital platforms built for the public interest. The Digital Public Goods Alliance defines DPI as "solutions and systems that enable the effective provision of essential society-wide functions and services in the public and private sectors"; while the Bill & Melinda Gates Foundation describes it as a "digital network that enables countries to safely and efficiently deliver economic opportunities and social services to all residents." Recently, the G20 Digital Economy Ministers, together with the United Nations Development Programme (UNDP), jointly adopted a description of DPI as "a set of shared digital systems that should be secure and interoperable, that can be built on open standards and promote access to services for all, with governance and community as core components."

Analogies to physical infrastructure are common: DPI is often described as "rails on which easy-to-use digital products and services can be built to benefit entire populations." Much like physical infrastructure, DPI often emphasizes the building of foundational components, commonly including digital ID, digital payment systems, and data exchange platforms, upon which further public and private systems can be "stacked." This means that these 'foundational layers' can be used to introduce and scale further online services and applications.

There are many potential benefits to investing in DPI. For instance, some of the earliest arguments suggested that DPI could be an alternative to the dominance of private companies in defining digital public spaces and in building large-scale platforms that have a profound impact on human rights. Digital *public* infrastructure, therefore, entails a central role for governments and public institutions in building foundational systems, standards, and governance for an increasingly digitalized society.

In the past few years, excitement surrounding DPI has been growing. In the wake of the COVID-19 pandemic, numerous success stories emerged of countries leveraging DPI to deliver services, and whether a country had strong DPI in place was seen as a key factor determining how quickly individuals could receive emergency payments from governments during the height of the crisis. As a result, the DPI agenda has recently gained significant traction, as many work to replicate and scale these successes. At an event on the Future of Digital Cooperation during the 77th UN General Assembly, the UN Secretary General said that: "Digital Public Infrastructure offers the means to turbocharge recovery from the COVID-19 pandemic, bridge the digital divide, and advance progress in the Sustainable Development Goals."

Meanwhile, the Director of the International Monetary Fund has stated that DPI is "the most effective accelerator of inclusion that there is"; and similar sentiments have been expressed by leaders at the World Bank, UN bodies, and private philanthropic organizations.

First mover countries have also been eager to share their technologies and approaches to building DPI. For instance, India has made DPI a centerpiece of its time holding the G20 presidency, where it has proposed a multi-stakeholder "One Future Alliance" to synergize efforts around DPI; the Indian government has signed several MOUs with governments from countries such as Sierra Leone, China, Russia, and Papua New Guinea to share its DPI experience with them; and the U.S. and India recently announced their intention to work in partnership to enable the creation of DPI in developing countries.

Digital identity as a foundation for digital public infrastructure

A key component of these DPI initiatives is the building out of digital identification systems, which can support verification of identity attributes and authorization of access to different systems or services. This, in turn, will allow public or private entities to securely ascertain certain details about the identity of individuals accessing services remotely. Such systems make up an indispensable layer of DPI.

Indeed, digital ID is often described as "foundational" to DPI itself. In India, the digital identification system was named 'Aadhaar'—meaning 'foundation'—to signify its role in creating the "bedrock" of the India Stack. And the UK's Minister for Digital Infrastructure has written that "[h]aving an agreed digital identity that you can use easily and universally will be the cornerstone of future economies."

Given that digital ID systems are so central to DPI initiatives, creating the very foundations upon which countless public and private services will be 'stacked,' it is imperative that these systems provide a *solid* foundation. But even as investment in DPI continues to grow, the many challenges, risks, and limitations that these critical digital infrastructures will face are becoming ever-clearer.

Examining the Foundations

Around the world, there is clear evidence that the digital systems that are being put in place as the 'foundations' for digital societies are in many cases embedding exclusions, inequalities, and harms. Across very different contexts, a similar range of problems and risks have been emerging as digital public infrastructure is rolled out. As national-scale digital ID systems are built and connected with other 'layers' of digital infrastructure, blind spots are appearing that have raised questions about whether such initiatives are able to deliver on their promises. Alongside many other civil society organizations, scholars, and activists, we have been raising the alarm about the realities of digital ID systems for several years.

Our expert speakers

Keynote speaker **Nanjala Nyabola**, along with panelists **Brian Kiira**, Program Officer at the Initiative for Social and Economic Rights (ISER), Uganda; **Grecia Macías**, Lawyer at Red en Defensa de los Derechos Digitales (R3D), Mexico; **Danilo Ćurčić**, Program Coordinator at the A11 Initiative, Serbia; **Yasah Musa**, Program Manager at the Nubian Rights Forum, Kenya; and moderators and organizers **Victoria Adelmant** and **Katelyn Cioffi**, discussed the harms and risks arising from the implementation of DPI in each country.

On June 21, 2023, we came together to discuss some of these risks and realities in an event organized and hosted by the Center for Human Rights and Global Justice at NYU School of Law. Drawing upon our experiences as advocates and litigants involved in raising awareness of the risks in current approaches to DPI, we discussed relevant lessons from recent legal challenges in Uganda, Mexico, Kenya, and Serbia.

Each of these cases deals with a different approach to meeting digital identity needs, and is situated in a different political, economic, and social context. Yet these cases give useful examples of what can go wrong with digital public infrastructure initiatives—and what kinds of safeguards, mitigations, and remedies must be put in place to avoid risks and exclusions becoming embedded into these 'foundational layers.'

Public systems do not necessarily serve the public interest

When it comes to what can go wrong, these four cases first highlight one of the key features of these systems: they are "accelerators of intent" that can be used for both positive and negative purposes. One of the central objections to allowing private companies to build digital infrastructure is that they will prioritize profits over other social goods, including democracy, equality, and human rights. However, it does not necessarily follow that *public* platforms will automatically incorporate these desirable values. They may be and, in some instances have been, designed and built primarily to exclude marginalized groups from accessing public services. If digital public infrastructure acts as an 'accelerator of intent,' it could therefore help to make governments more efficient at discriminating against minorities.

Even in the absence of any specific intent to exclude or discriminate, governments' digital initiatives in many countries have displayed a worrying tendency to shut out those who are most vulnerable, as various technological, financial, physical, or administrative barriers lead to the exclusion of groups such as older persons, women, ethnic minorities, and those living in poverty.

In Uganda, for instance, mass exclusion relating to the national digital ID system, known as *Ndaga Muntu*, has now been well documented. A series of barriers, as well as problems with the design of the system, have ensured that millions of Ugandans remain locked out of the national digital ID. Despite these shortcomings, however, the system has been integrated with numerous social welfare programs, including the country's successful cash transfer program for older persons. Since presentation of the national ID is now a mandatory requirement for accessing a variety of services, the result has been thousands of vulnerable individuals shut out from access to social security payments, healthcare, and a range of other public and private services. In order to address this exclusion, three civil society organizations brought a legal challenge in 2022 in the High Court of Uganda, seeking primarily a court order that will allow for the use of alternative forms of identification.

> *"So there is this discrimination that is happening that is all hinged upon the possession or not of the national ID. And … for us the national ID now seems to be so centrally entrenched in everyone's life, whether it is registering a SIM card, opening a bank account, it is right there. So it is one that you have to have."*
>
> ***Brian Kiira, Initiative for Social and Economic Rights, Uganda***

Similar exclusionary effects have been seen in Serbia, where through its Social Cards Law the government introduced a complex new digitized system for identifying and enrolling beneficiaries in social welfare programs. On the basis of the Citizens' Unique Personal Number, the system brings together 135 different government datasets to enable algorithmic decision-making in the delivery of welfare benefits. The law was presented as a means of making the social protection system more accurate—to include those who should be included and exclude anyone who should not be in the system. But the effects have been stark, with 15% of beneficiaries having their benefits payments suspended after this data-driven system has flagged them as having too high income.

A key problem is that the data the system is analyzing is decontextualized: a person might receive a lump sum of funds that they had previously been underpaid, and this payment could flag them as being over the relevant income threshold and no longer eligible for benefits. The data does not tell the full story, and individuals are not given the chance to explain their circumstances. This large-scale digital public infrastructure—arising from an unprecedented data aggregation exercise leveraging the foundational identity system—is thereby leading to serious exclusions, particularly among persons with disabilities and members of the Roma community. This is why the A11 Initiative has brought a constitutional challenge, arguing not only that the law violates standards around data processing, but also that there has been little transparency about the system.

> *"Nobody knows how the system works because it was not made transparent. So the only information we could collect was based on interviews of people working within the social protection system and individuals who are actually trying to get their benefits ... But it's 135 different data sets that were collected through many different national registries ... and everything is based on something that is called Citizens' Unique Personal Number."*
>
> ***Danilo Ćurčić, A11 Initiative, Serbia***

In Kenya, organizations like the Nubian Rights Forum (NRF) have been working for several years to hold the government accountable for the exclusions surrounding the national digital identification system. Named *Huduma Namba* (meaning 'service number'), this digital ID was intended to be linked to countless public and private services, including: enrolling in a public school, registering as a voter, opening a bank account, accessing universal health care services or social protection services, and even registering for an electricity connection.

Kenyan minority groups, including members of the Nubian community and Somali-Kenyans, have long fought to address exclusion of these groups from accessing official identity documentation. The introduction of DPI initiatives—including the introduction of the use of digitized biometrics, data exchange, and the linkage of many public and private services to the digital ID 'layer'–has exacerbated these problems. Amidst continuing patterns of both direct and indirect discrimination against certain ethnic groups, the push to conceptualize the digital ID as a foundation would lead to widespread exclusion. A landmark decision of the High Court of Kenya in 2021 found multiple deficiencies in the legal procedures surrounding the *Huduma Namba* system and in effect halted the project.

Additionally, the NRF along with Data Rights and the Kenya Human Rights Commission have filed a case in a French High Court arguing that IDEMIA, the company that had contracted with the Kenyan government to provide technology for the *Huduma Namba* system, did not undertake the necessary human rights due diligence, including a human rights risk assessment, before providing the technology.

The need for such *ex ante* rights-based assessments was also a key issue in recent litigation in Mexico. The Mexican government has made numerous efforts to introduce biometrics into civil registration and national ID, policing, and border control—and also into SIM card registration. In 2021, the Senate proposed a new law that would create the *Padrón Nacional de Usuarios de Telefonía Móvil* (PANAUT), a centralized database that would include the biometric data of all mobile phone users. Civil society organization Red en Defensa de los Derechos Digitales (R3D) was one of several organizations involved in challenging PANAUT. Their work helped to spark widespread public concern about the proposed system: for instance, over 70,000 individuals submitted individual briefs to raise concerns about the introduction of the PANAUT system.

In a 2022 decision, the Supreme Court specifically recognized the high risks associated with collecting biometric data at such a large scale, and the impact that this could have on individuals' privacy rights. Setting an important precedent, the Court found that the use of biometrics was disproportionate, and that the entire PANAUT system was therefore invalid.

Who safeguards the public interest in an age of digital government?

In many ways, these examples demonstrate the important role that civil society organizations play in safeguarding human rights. In all the cases discussed, such organizations have played a pivotal role in sharing information about the introduction of new systems, in researching and documenting instances of human rights risks and violations, and in bringing these challenges directly to decision-makers through advocacy and litigation. This has led to important new precedents, to increased public awareness, and to the introduction of some mitigations to offset some of the harmful effects of new systems. In short, the involvement of civil society organizations has led to better outcomes.

However, the very need to resort to litigation and to fight long and protracted legal battles, often simply to obtain information, must also be partially seen as a failure. This is first of all a problem of participation and consultation, where a lack of consultation with civil society organizations and affected communities has led to failures to incorporate appropriate human rights safeguards throughout system design and implementation. It is also a failure in transparency, communication, and democratic debate about the conceptualization and operation of such systems. And finally, it is a failure of imagination, as the enthusiasm surrounding these digital systems leads proponents not to adequately consider, anticipate, or plan for potential risks.

> *"These are paradoxes that many of us are contending with as we are being told that efficiency is good, that more data delivers more efficient government, that smart cities deliver more efficient government. Well, is the reason why these social services are not being allocated to people the fact that they don't have digital IDs, or the fact that the government did not want to allocate them those resources in the beginning? That's not a technical question. You can't engineer that. The solution to that question, that is a political question, that is a social question, that is a normative question that must be engaged with before we provide these questionable governments with this tremendous capacity for collecting, sorting, ordering people, allocating people's identities and thereby allocating people resources from the state."*
>
> ***Nanjala Nyabola, author, and keynote speaker in this event***

A key problem, then, across many of these efforts to roll out DPI as 'the means to turbocharge recovery from the pandemic and advance progress in the Sustainable Development Goals,' is that these aims cannot be achieved without serious attention being paid to the social and political questions that are inextricably linked to the building of these infrastructures. And without a meaningfully participatory approach that allows for critique, as well as a serious commitment to the necessary safeguards, the foundations upon which digital societies will be built may entrench many of the problems that DPI is intended to overcome.

A way forward: safeguards, mitigations, and remedies

The four cases discussed above have arisen in different contexts, across different jurisdictions, and contest different elements of efforts to develop DPI. But some common lessons emerge as to how best to address the human rights harms that can arise in the implementation of digital public infrastructure.

> *"Data privacy, inclusion, and a careful, participatory approach are essential elements in ensuring the success and effectiveness of the Unique Personal Identifier system. By addressing these issues, the government can build a robust, secure, and equitable digital infrastructure that benefits all Kenyan citizens."*
>
> ***Yasah Musa, Nubian Rights Forum, Kenya***

The first lesson is that there are many tools available to assess risk *ex ante*, to introduce new safeguards, and to design remedies, which are not presently being used in most cases. This includes human rights impact assessments and data privacy impact assessments, as well as consultation and participation with those who may be affected. In several of the cases above, the central demand is not that the government abandon all DPI initiatives, but that risk assessments be undertaken in advance and that safeguards and remedies be put in place throughout. Mitigating measures must be seen as central concerns, and not subsidiaries to the broader project. Evidence-based assessments should not only help to identify and mitigate risks, but also to assess technological tools against their intended purpose—and to interrogate whether the use of certain technologies is necessary and proportionate.

> *"[The Supreme Court decision in Mexico] gives us the recognition that biometric data is really sensitive data. It's not just the same as a password. It's just not the same as any other data… [the Court] recognized the sensitivity that biometric data has and how you need to pass a strict scrutiny test in order to address that, in order to see that the measure is proportional to the final objective that you want to have. And also it established that when you are dealing with the massive collection of data, specifically biometric data, you have to have a previous… specifically when it's done by a state actor, you have to have a privacy assessment beforehand."*
>
> ***Grecia Macías, Red en Defensa de Los Derechos Digitales, Mexico***

A second takeaway from these four case studies has been the need to incorporate remedies and mitigations into every stage of the design and implementation of these systems. While DPI may indeed hold great promise, the lure of techno-solutionism should not blind policymakers to the existence of risks and harms. Experience has already shown that decisions at both the design stage and in implementation will often lead to exclusion. When it comes to design, common factors have included the over-use of biometrics and failure to account for differences in experiences across different groups. During implementation, choices such as mandatorily integrating or linking the foundational digital platform to critical public services have been a common cause of access denials and exclusions. These case studies also demonstrate the likelihood of system failures in many of the contexts in which these digital platforms are deployed, whether due to electricity or internet outages, environmental conditions, or social and political realities, which can have a dramatic effect on the overall efficacy of the system.

Understanding the potential impacts of these choices in each context takes time, and many civil society organizations have urged governments not to rush into implementing systems without comprehensive consideration of the broad range of potential risks. Another common mitigation demanded by civil society organizations has been not to link these systems mandatorily to critical services when individuals remain excluded from the foundational system itself. In Uganda, for instance, the litigants in the case are asking for a court order that alternative forms of identity will be allowed. Given that exclusion is likely to be an ongoing challenge for such an ambitious project, they are also asking for ongoing judicial oversight and for the establishment of an accountability mechanism to ensure that the management of the national ID system remains in compliance with human rights.

A third and final lesson is about the importance of the accessibility of information about these foundational digital platforms. Such systems often involve proprietary technology, often provided by foreign companies, and complex algorithmic models that make it difficult to understand how data is being processed, used, and shared. This not only frustrates public participation and consultation, it makes it much more difficult to identify the root causes of problems, to correct errors, and to design remedies that will safeguard human rights.

These cases may complicate rosy narratives about the transformative potential for DPI, but they also provide pathways to alternative visions for the future. There is no doubt that the efficacy of the safeguards outlined here will vary significantly based on context and history, including factors such as the strength of political institutions, as well as cultural and social relationships—one size does not fit all. But more appropriate systems and approaches can be designed by engaging in context-specific, purpose-based policy-making that centers consultation and participation. Approaches to DPI could include proper mitigations through the use of impact assessments that look beyond technical system design to understand how human beings will interact with new technologies and processes, and how new technologies will layer onto existing social and political realities. And crucially, harms can be halted more quickly by incorporating accessible remedies throughout the process of building DPI.

By learning from existing experience around the world, and especially from contestation arising from affected communities, efforts to roll out DPI would have a much greater chance of realizing their promised benefits. Only through utilizing the full suite of safeguards do policymakers have a chance to ensure that these 'rails on which digital products and services are built' can indeed benefit entire populations and form a solid and inclusive foundation.

Watch the video recording of the event here, and download the transcript here.

Further Resources

Kenya

Nubian Rights Forum, *The UPI: Empowering Kenyans or Excluding Marginalized Communities?*, May 22, 2023, https://www.nubianrightsforum.org/the-upi-empowering-kenyans-or-excluding-marginalized-communities/

Kenya Human Rights Commission, Nubian Rights Forum and NGO Data Rights Files Case Against Biometric Tech Giant IDEMIA in France for Failure to Consider Human Rights Risks, July 29, 2022 https://www.khrc.or.ke/2015-03-04-10-37-01/press-releases/766-kenya-human-rights-commission-nubian-rights-forum-and-ngo-data-rights-files-case-against-biometric-tech-giant-idemia-in-france-for-failure-to-consider-human-rights-risks.html

Mexico

Red en Defensa de Los Derechos Digitales, *Acción De Inconstitucionalidad 82/2021 Y Su Acumulada 86/2021 Asunto: Se Presenta Escrito En Calidad De Amicus Curiae*, Https://R3d.Mx/Wp-Content/Uploads/Amicus-Panaut-08022022.Pdf

Red en Defensa de Los Derechos Digitales, SCJN debe declarar inconstitucionalidad del PANAUT, April 21, 2022, https://r3d.mx/2022/04/21/scjn-debe-declarar-inconstitucionalidad-del-panaut/

Serbia

A 11 Initiative for Social and Economic Rights, (Anti)social cards, October 14, 2022, https://www.a11initiative.org/en/antisocial-cards/

ESCR-Net, Serbia joins the group of countries where discriminatory government-driven algorithms are challenged in court, November 29, 2022, https://www.escr-net.org/news/2022/press-release-serbia-joins-group-countries-where-discriminatory-government-driven

Uganda

Katelyn Cioffi, Human rights gateway or gatekeeper: Digital IDs on trial in Uganda, Open Global Rights, July 24, 2023, https://www.openglobalrights.org/human-rights-gateway-gatekeeper-digital-ids-uganda/

Nita Bhalla, Uganda sued over digital ID system that excludes millions, Reuters, May 15, 2022, https://www.reuters.com/article/uganda-tech-biometrics-idUSL3N2X32RG

Initiative for Social and Economic Rights, Unwanted Witness, and the Health Equity and Policy Initiative, Civil Society sues Government over Ndaga Muntu National ID: Mandatory Digital ID Threatens Lives!, April 25, 2022, https://iser-uganda.org/wp-content/uploads/2022/07/Digital_ID_Litigation_Press_Statement.pdf