BUILDING THE EUROPEAN DIGITAL PUBLIC INFRASTRUCTURE: RATIONALE, OPTIONS, AND ROADMAP

Camille Ford, Marta Dell'Aquila, Olesya Grabova, Iris Muñoz and Andrea Renda

CEPS IN-DEPTH ANALYSIS

March, 2025-03

SUMMARY

This report illustrates the current wave of reforms aimed at creating digital public infrastructures (DPIs), starting with international experience and moving to current developments in EU Member States and at the EU level. The European Commission has adopted several initiatives in this domain and is expected to further accelerate progress as the momentum for technological sovereignty builds and it becomes more embedded in the agendas of EU institutions. Key initiatives revolve around the EU Digital Identity Wallet, a well-shaped data exchange and governance layer, progress on user-centric public services, and the modernisation of public administration.

We argue that these reforms should be implemented effectively and consistently in the coming years and be accompanied by complementary measures, such as investment in skills, stewardship and compute infrastructure, which would contribute to what is increasingly termed the 'EuroStack'. Altogether, a fully fledged European DPI would boost European GDP, contribute to technological sovereignty, harness strategic autonomy, and improve European competitiveness in digital services in Europe and around the world.

Camille Ford was a Researcher in the GRID unit at CEPS. Marta Dell'Aquila is a Researcher in the GRID unit at CEPS. Olesya Grabova is a Research Assistant in the GRID unit at CEPS. Iris Muñoz was an Intern in the GRID unti at CEPS. Andrea Renda is Director of Research at CEPS and Head of the GRID unit.

CEPS In-depth Analysis papers offer a deeper and more comprehensive overview of a wide range of key policy questions facing Europe. Unless otherwise indicated, the views expressed are attributable only to the authors in a personal capacity and not to any institution with which they are associated.

CEPS ▪ Place du Congrès 1 ▪ B-1000 Brussels ▪ Tel: (32.2) 229.39.11

CONTENTS

LIST OF BOXES

LIST OF FIGURES

LIST OF TABLES

Introduction

Over the past three decades, the internet revolution has gradually permeated all aspects of the economy and society, becoming an unavoidable feature of societal relationships, production processes, and political discourse. The rise of a hyper-connected society has not come without consequences, however, for the internet itself and for the policies that affect it.

Importantly, the internet was born and evolved largely as a privately governed space, shielded from intrusive government regulation. Its initial design features paved the way for unprecedented innovation, but also for growing concentration and value capture, to the detriment of many parts of the economy and even constraining publicly managed spaces for dialogue and social interaction. Today, governments are trying to find their place in the complex dynamics of cyberspace. The rise of digital public infrastructure (DPI) is a way to restore an effective balance between public spaces and private incentives in an ever-growing digital environment.

In this report, we map current European efforts on DPI and place them in the context of ongoing digital transformation. Section 1 briefly recaps three decades of digital transformation. Section 2 describes international initiatives for DPI. Section 3 maps and compares existing DPI-related initiatives in EU Member States. Section 4 illustrates the existing efforts and a possible roadmap towards a ‘EuroStack’, which would encompass a pan-European DPI. Section 5 briefly concludes.

1. THE DNA AND EVOLUTION OF CYBERSPACE, AND THE DAWN OF DPI

In its early days, the web was structured and designed as an open, neutral, end-to-end architecture in which intelligence was distributed at the edges. There was no central filtering or prioritisation of content. Rooted in its 'code', an overarching set of open standards agreed upon by engineers and experts in forums such as the World Wide Web consortium and the Internet Engineering Task Force, the web proved its potential as a formidable engine of permissionless innovation. Anyone willing to join, who had access to connectivity, could participate as a peer; furthermore, no content could be prioritised over any other. This principle, known as 'net neutrality', is still the cornerstone of web governance for the physical and logical layers of its architecture. Yet, the evolution of the web over time has led to noticeable changes in the way content is shared and has created new challenges for those who wish to secure cyberspace as an open, competitive environment where all of society and businesses can thrive.

In short, the DNA of cyberspace revolves around four main characteristics:

(i) the *digitised nature of information*, which allows for seamless data aggregation and replication and an unprecedented dynamic in transactions, based on the overall economic features of information goods;

(ii) *modularity*, which ensures the integration of products and services from different sources and vendors into complex 'system goods', where complementors interoperate (Varian and Shapiro 1999).

(iii) an *end-to-end* architecture, which ensures that information is shared among peers, creating economies of scale known as network effects, and enabling new decentralised forms of exchanges such as the collaborative economy and multi-sided platforms; and

(iv) *Moore's law*, or more generally the exponential growth of compute capacity, which fuels innovation by constantly shifting the frontier of what technology makes possible.

These four foundational characteristics have made the web a powerful source of transformation and innovation, to the extent that policymakers around the world decided, at the outset, not to intervene in order to let the 'network of networks' grow and unleash its full potential. Early internet-related policies – from the WIPO Treaty to the US Telecommunications Act and Communications Decency Act in 1996, to the EU Directives on e-Commerce and on the Information Society at the dawn of the new millennium – took a *laissez faire* stance. This was motivated by the infancy and limited diffusion of the new medium, as well as by the frantic dynamics of the competition observed in cyberspace, marked by the extreme contestability of players gaining a leading edge over others (Altavista, MySpace, and many more).

However, the same features that had made the web so open and powerful also rapidly triggered trends that radically changed the dynamics of cyberspace over time. The explosion of available data and information led users to need intermediaries and platforms that rank, order and organise content to make it more accessible. An overabundance of information, as Herbert Simon had already predicted in the 1950s, led to a poverty of attention, and those players that managed to capture the eyeballs of a sufficient number of users installed a base and ended up gaining enormous power.

A much-needed reintermediation phase was inevitably accompanied by concentration and the reorganisation of business models around the constant engagement of end users. Trends such as virtualisation and 'servitisation' contributed to the emergence of cloud-based giants that today are able to mobilise large chunks of the economy, intermediate and govern significant portions of societal relations. They eventually accumulated resources and data, reflected in market capitalisations that, in some cases, surpassed the USD 3 trillion threshold.

The rise of large online cloud-based giants has radically transformed the dynamics of cyberspace. Net neutrality, once cherished by experts, activists and businesspeople alike, is today only, and partially, a feature of the physical and logical layers of the internet. Above them, the technology stack is the realm of non-neutral practices and technological solutions, from content delivery networks to app stores and algorithmic content moderation, advertising-based business models, and the extreme personalisation of offers fuelled by sophisticated and powerful AI systems. Beyond tech giants, even open-source communities felt the need to reorganise by gradually abandoning non-curated software environments. They started creating alternative software stacks based on modular applications and even 'containerised app' stores.

Alongside this development, the increasing importance of the internet also led to mounting concerns and calls to enhance the security of exchanges and transactions. The spread of cyberattacks, hate speech, and terrorism coordination on the web, and the need to enable applications that securely manage personal, business, and government data, led to an unavoidable move towards deeper filtering and inspection of content. Ultimately, policymakers decided to deviate from the original rule of 'no responsibility for online intermediaries'.

The early days in which on the internet, nobody knew you were a dog (echoing a famous cartoon by Peter Steiner that appeared in the *New Yorker* in 1993) are gone. As a result, today verifying and authenticating the identity of users matters, even more so as both private and public entities rely on the internet to reach out to people and businesses. It matters for commercial reasons, as end users need to ensure that their transactions and use of public services are uniquely attributed to their identity. It matters for political reasons, as people increasingly participate in public life through digital means. It matters for security reasons, as the origin and provenance of speech and information are becoming crucial concerns in modern societies. And it matters for industrial applications, as data spaces often host confidential industrial data that, unlike other types of information, are supposed to be selectively shared, but not made publicly available (Renda 2023).

The emergence of a 'thicker' technology stack (see Renda 2020, 2022), which incorporates various new layers compared with the original design and includes authentication and verification of identity and credentials, is a key transition that will bring forward the internet from adolescence to maturity. Yet which the direction the transition will take is far from trivial. This holds even more so for the EU, where the reintermediation and growth of cyberspace has led to a gradual loss of value, data, and investment to the benefit of other world powers, notably the US, and to an ongoing privatisation of services once considered eminently public.

Recently, in celebrating the 35 years since the birth of the web, its most acknowledged founder Tim Berners-Lee denounced the dysfunctions created on the web by the extent of power concentration, which contradicts the original decentralised spirit. In addition to the rise of a massive personal data market based on the granular profiling of end users and the growth of what Shoshana Zuboff referred to as 'surveillance capitalism' in a widely read book.

No reaction so far has effectively tackled this concern – not even Europe's attempts to intervene through the General Data Protection Regulation (GDPR) or the suite of legislation adopted in the past few years to regulate digital platforms. But new government-led initiatives may soon bridge this gap, including in Europe.

Several questions must be addressed to ensure that the web remains open, innovative, democratic, and decentralised in the years to come, and that Europe stands a chance of aligning its development on EU values, principles, and goals. Key questions revolve around who controls personal and business data, who verifies and authenticates identity, and who intermediates in data transfers. Also, what can public institutions do to ensure that data are kept under the control of end users and collectively used for the pursuit of public services when needed? Addressing them is a matter of technological sovereignty and strategic autonomy, and a possible way to define a path to a new web designed to empower people rather than enslave them.

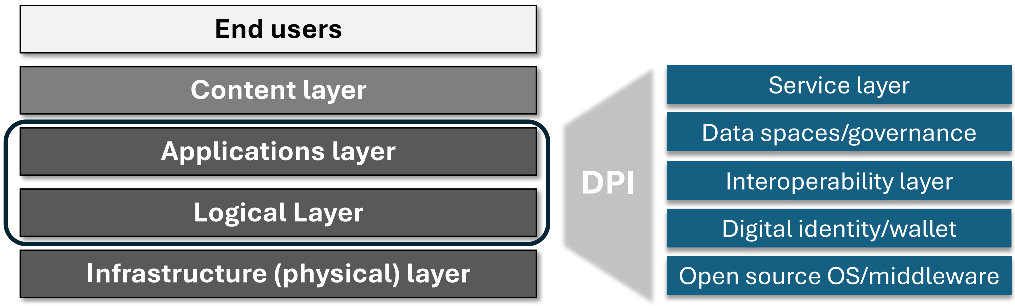
2. WHAT THE DPI IS AND WHY IT MATTERS

One way countries have tried to address the need for sovereign solutions and the adherence of specific layers of the internet architecture to national values and principles is the development of a digital public infrastructure. The definition of what constitutes DPI is still far from univocal, with different countries using different terminologies and referring to slightly different sets of solutions, layers, and applications.

However, the concept of DPI gained prominence during India's G20 presidency in 2023. This led to a broader consensus on its definition as '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' (UNDP, 2023) The recent playbook of the United Nations Development Programme (UNDP) on the DPI, addressed specifically to low- and middle-income countries (LMICs), added to this definition that such services provided at societal scale 'are governed by enabling rules to drive development, inclusion, innovation, trust, and competition and respect human rights and fundamental freedoms'.

Notably, while acknowledging that countries might have different approaches to DPI and may implement components in various ways, the G20 clearly identified three layers (digital ID, digital payments, and data exchange) as fundamental to DPI (see Figure 1). Simply put, DPI can be understood as an intermediate layer (or set of layers) in the technology stack between the physical, logical and application layers (including internet connectivity, devices, servers, data centres, the cloud, and routers) and sectoral applications (for example, e-commerce, social protection, remote education, and telehealth) (World Bank, 2023).

Figure 1 – The original layered internet architecture and DPI layers



Source: Authors' own elaboration

The key advantages of having a well-developed DPI in place can be summarised as follows:

- ***Efficiency***. The digitalisation of public services through a DPI can lead to substantial savings and improved benefits for the public, provided that they operate in a trusted environment. For example, with a well-developed e-identity, wallet, and data exchange layer, people can benefit from fee-free instant payments and powerful solutions such as privacy-friendly data spaces for public services, mobility, health, and more.
- Similarly, in the relationship between government and businesses, the DPI could enable 'zero contact administration', in which several services become automated or available with one click. Therefore, the DPI also promises to streamline procedures and fulfil key objectives such as 'ask only once', as well as to foster a business-friendly experience in the interaction with government. Some authors credit the deployment of a DPI with a very significant boost in GDP: a McKinsey study on seven countries in 2019 found that extending full digital ID coverage (thus, a subset of DPI solutions) could unlock economic value equivalent to 3–13 % of GDP in 2030.
- ***Innovation and growth***. As illustrated in a recent UNDP report, by fostering collaboration between the public and private sectors, DPI can drive innovation and help bridge the digital divide. This infrastructure enhances financial services, healthcare, and government data sharing, leading to broader societal benefits. Additionally, a 2022 report by the UNDP with the Digital Public Goods Alliance and Dalberg Advisors found that DPI stimulates economic growth, boosts financial inclusion, reduces carbon emissions, and improves judicial services, resulting in significant socioeconomic advantages. These include estimated economic growth from 20 % to 33 %. Considering only financial inclusion and lower leakages from social programmes, this could lead to an estimated boost to GDP growth of 1–1.4 % by 2030 in LMICs (UNDP, 2022).
- ***Resilience and technological sovereignty***. Especially when based on open-source software and open standards, the DPI can reduce a country's dependency on single providers, such as large-scale cloud-based giants, which normally leverage their dominance in the cloud to promote additional services (including identity, app stores, payments, and more). By adopting federated and decentralised architectures, and leveraging interoperable services, the DPI aims at offering end users suitable alternatives to existing dominant solutions.
- A well-developed DPI also gives a country the option to move services entirely online in cases of an emergency or crisis. For example, Bandura et al. (2024) estimated that on average, countries with a robust DPI during the COVID-19 crisis were able to reach 51 % of their populations with public services, compared with

16 % in other countries. This meant being able to keep government services, hospitals, schools, and other operations functioning through online channels. Likewise, Ukraine's rapid expansion of its e-government platform (Diia) in response to the Russian invasion demonstrates the practical benefits of a well-developed DPI. The platform enabled the government to offer a wide range of services in several clicks, including digital passports, social service registrations, financial assistance, and damaged property registration, ensuring that essential services remained accessible even amid the disruption of war.

- ***Inclusion***. Many countries face challenges in delivering services efficiently to the public, negatively affecting already marginalised populations. DPI can overcome these challenges by improving the precision and reach of service delivery, and by using the impressive penetration of mobile phones in many countries, including LMICs. For example, as of August 2024, Brazil's instant payment system Pix had approximately 168.15 million registered users, including 153.11 million individuals and 15.04 million companies. The Central Bank of Brazil reported that over 40 million previously unbanked people began using Pix as their primary financial tool, following its launch. This was particularly true for younger people and smaller businesses. Moreover, such an inclusive design improves social welfare by preventing exclusion and ensuring that everyone benefits equitably, thereby upholding constitutional rights. The G20 Global Partnership for Financial Inclusion, prepared under the auspices of the World Bank, emphasised that India's DPI had achieved 47 years of financial inclusion progress in just 6 years.
- ***Self-sovereignty and user empowerment****.* One of the key features of the DPI is its self-sovereign ambition. This implies that end users retain control of their data and have the possibility of switching to alternative providers rather than succumbing to the conglomerate-bundled offers of only a handful of big players. This is because the DPI aims at creating a technology stack that revolves around the freedom of individuals to choose their own solutions in a decentralised environment, while remaining able to interact with other users and with public and private institutions in a seamless way. That said, as explained below, many DPIs remain deeply tied to existing cloud providers and do not always comply with acceptable standards in terms of openness and self-sovereignty (for example, the Indian Aadhaar stores sensitive biometric data (fingerprints and iris scans) linked to personal details, creating a centralised database).

3. International initiatives on DPI

Given its potential for countries at all stages of development over the past few months, DPI has been the subject of a plethora of initiatives around the globe. Multilateral institutions – ranging from various UN agencies, the World Bank and several other multilateral development banks, to privately led organisations and donors such as the World Economic Forum and the Gates Foundation – have launched highly ambitious initiatives in this domain. These are shaping the world of international development, especially in LMICs.

The **UN**, specifically the UNDP, has played a major role in shaping the concept of DPI. Defined by the UNDP as a 'critical enabler of digital transformation' and a 'potential game-changer', the DPI offers possibilities at different levels of government. This includes, inter alia, enhancing public service delivery and development priorities; enabling data sharing across different countries in a region; and identifying trends, best practices, and areas needing improvement within the public sector (OECD, 2024). Globally, DPI can play an important role in accelerating progress towards some of the Sustainable Development Goals (SDGs), as described in Table 1. Within this framework and as part of the SDG Digital event[1], the UNDP and International Telecommunication Union (ITU) launched the High Impact Initiative on DPI in September 2023, outlining five key pillars that unify the efforts of global initiatives, national governments, and organisations:

(i) developing and adopting a universal safeguard framework by all Member States and stakeholders;

(ii) enhancing DPI partnerships with the private sector and community-based organisations in 100 countries, integrating intermediaries into local digital ecosystems to provide broader, more inclusive services;

(iii) promoting the deployment of affordable, secure, and scalable technologies, as well as the technical expertise necessary for the design, deployment, and continuous development of DPI;

(iv) accelerating the integration of sustainable digital technologies for the development of innovative green financing initiatives across 100 countries; and

(v) harmonising global financing endeavours to enhance accessibility to technical assistance, improve governance capacities, and promote open innovation.

[1] The SDG Digital was an event that took place within the SDG Action Weekend in New York in September 2023, bringing together different officials from governments, the private sector, financial institutions, and civil society to discuss the potential of digital technologies in accelerating the achievement of the SDGs and their respective targets.

A 'Roadmap to 2030' offers a strategic plan, segmented into phases with specific goals, to build some progress towards the SDGs[2].

Table 1 – The DPI and the SDGs: a non-exhaustive list of interrelations

SDG	DPI potential effects
SDG1 No Poverty	Increased economic resilience and job opportunities, reduced poverty and extreme poverty
SDG5 Gender Equality	Enhanced service delivery to more than 250 million women
SDG8 Decent Work and Economic Growth	Enhanced access to financial institutions (for example, to people without a bank account)
SDG13 Climate Action	Use of standardised measurement, reporting, and verification systems and connecting carbon registries can result in a reduction of CO_2 emissions

Source: Authors' own elaboration

In September 2024, the UN adopted a Pact for the Future that included a Global Digital Compact, which is the first comprehensive global framework for digital cooperation and AI governance. It recognises digital public goods and infrastructure as key drivers of inclusive digital transformation and innovation, while acknowledging diverse multiple models of DPI. The Global Digital Compact commits to reaching several priority objectives related to DPI by 2030: develop a set of safeguards for safe user-centred DPI for different contexts; exchange best practices and use cases; increase investment and funding towards DPI development; and foster partnerships between the private sector, civil society, academia, government, and international organisations to leverage DPI solutions for the SDGs.

The **World Bank** has highlighted how DPI can promote inclusion, resilience, and innovation, underscoring its potential to drive significant socioeconomic advancement. In this framework, two initiatives have been launched to help spread this approach. One is Identification for Development, which aims to 'build inclusive and trusted ID and civil

[2] Initiatives launched in 2024 feature the development of DPI safeguard principles and the establishment of the Safeguards Action Hub, and the implementation of a coordination mechanism for DPI financing. Additionally, there should be a focus on catalysing the advancement of DPI technologies for green transitions and women's inclusion in DPI. By 2030 – for whichthe goal will be for 100 countries to have implemented safe and inclusive DPI that benefits people and the planet – priority should be given to: strengthening political leadership and international cooperation for DPI; identifying new revenue streams; and unlocking knowledge and capacity for DPI implementation in over 50 LMICs, with the support of local private-sector companies.

registration (CR) ecosystems that increase access to services, improve economic opportunities, and empower people' (World Bank 2023). The other is Digitising Government-to-Person Payments, which aids 35 countries in digitising G2P payments with a focus on inclusion, efficiency, and empowerment.

These two initiatives seek to help countries develop digital IDs and public infrastructure and to address risks related to exclusion, digital security, and personal data protection. By promoting thought leadership and providing guidance and tools for practitioners, they can enhance the global DPI agenda by raising awareness, building partnerships, developing digital public goods, and facilitating peer-to-peer learning. Additionally, they offer technical and financial assistance to countries for inclusive and secure DPI.

Other initiatives have been launched by international organisations in partnership with leading countries on the development of DPI. Among them, **GovStack** is a joint initiative between Germany, Estonia, the ITU, and the Digital Impact Alliance. GovStack supports countries and organisations by building cost-effective and efficient digital public services that are easy to scale so that people can seamlessly access health records, manage identity documents, make digital payments, and utilise other government services. The GovStack approach is rooted in the SDGs and works with over 20 countries across four pillars (GovSpecs, GovTest, GovLearn, and GovMarket).

The appeal of the GovStack approach is that the initiative has compiled best practices from international DPI champions such as Estonia, India, and Singapore and translated them into an open source whole-of-government stack for the digitisation of public services. This building-blocks approach entails interoperable software code, platforms, and applications which can provide a basic digital service at scale and be reused in various use cases and contexts. GovStack is part of the Digital Public Goods Alliance, a 'multi-stakeholder initiative with a mission to accelerate the attainment of sustainable development goals in LMICs by facilitating the discovery, development, use of, and investment in digital public goods'.

Among private donors, the **Gates Foundation** massively supports the deployment of DPIs. Initiatives include the Modular Open-Source Identity Platform (MOSIP), which helps governments adopt digital identity systems while retaining sovereignty over their digital infrastructure. Mojaloop is an open-source digital payment system serving as a core technology for DPI in countries like Malawi and Rwanda. The cooperation between 11 'first-mover countries', the UNDP, the Gates Foundation, and other international organisations (including GovStack) recently led to the launch of the 50-in-5 campaign. These 11 countries span different geographies and income levels (Bangladesh, Estonia, Ethiopia, Guatemala, Moldova, Norway, Senegal, Sierra Leone, Singapore, Sri Lanka, and

Togo). By 2028, the campaign aims to help 50 countries design, launch, and scale the components of their DPI.

3.1. INDIASTACK: THE QUINTESSENTIAL DPI?

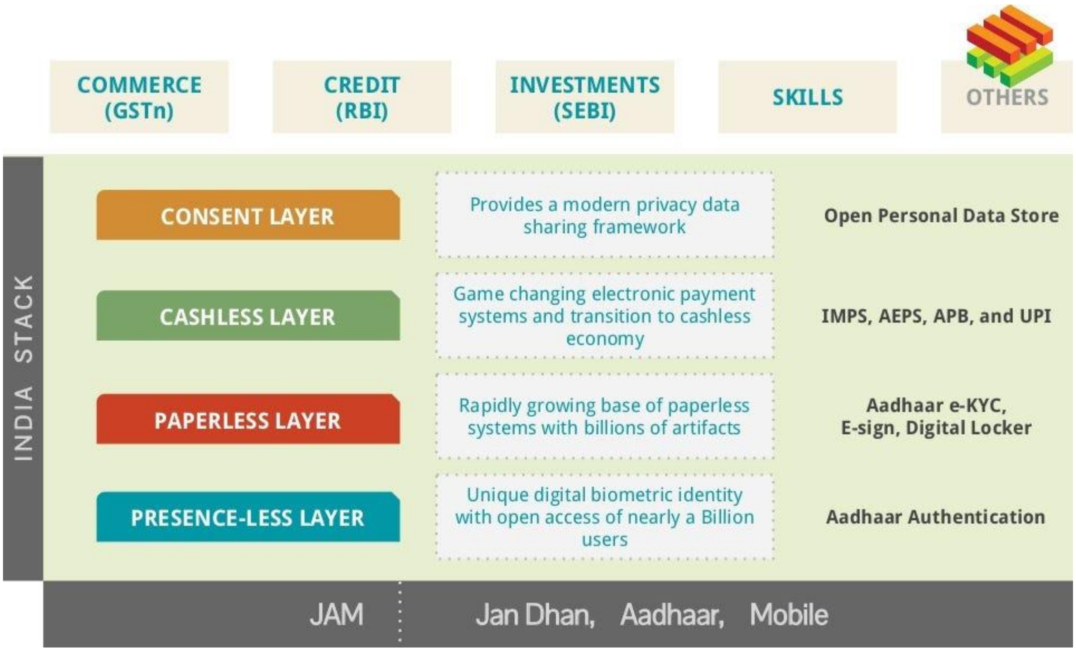
IndiaStack is a government-backed collection of application programming interfaces (APIs) that enables third parties to build software with access to government IDs, payment networks, and data. This digital infrastructure is interoperable and 'stacked', allowing private companies to develop apps integrated with state services. The vision behind IndiaStack is to provide a comprehensive digital infrastructure to enhance efficiency, transparency, and inclusion across various sectors.

IndiaStack began with the Aadhaar digital identity scheme, launched in 2009, and now covers nearly the entire adult population. Indian citizens and foreign residents enrolled in Aadhaar receive a 12-digit identity number linked to their photographs, fingerprints, and iris scans, managed by the Unique Identification Authority of India. This ID, which can be linked to a mobile phone, allows banks, telecom companies, and others to verify identities instantly, reducing fraud and verification costs. The government has also made Aadhaar a key part of social service provision, including a monthly ration that over 800 million people get. However, the security of Aadhaar has been a topic of debate and concern.

The Unified Payments Interface (UPI) and Data Empowerment and Protection Architecture (DEPA) add two other layers to India's digital infrastructure, complementing the Aadhaar system within the broader IndiaStack framework:

- **UPI,** introduced in 2016, is a real-time payment system that enables instant fund transfers between bank accounts using smartphones. It allows users to link multiple bank accounts to a single mobile application, facilitating seamless transactions. Its integration with Aadhaar further enhances the ease of transactions.
- **DEPA, the data layer** launched in 2020, allows users to securely share their financial data with third-party service providers through consent-based mechanisms. DEPA leverages Aadhaar for user authentication and authorisation, enabling individuals to access a wide range of financial services and products while maintaining data privacy and security.

Figure 2 – The IndiaStack: main layers and solutions


COMMERCE (GSTn)
CREDIT (RBI)
INVESTMENTS (SEBI)
SKILLS
OTHERS
INDIA STACK
CONSENT LAYER
Provides a modern privacy data sharing framework
Open Personal Data Store
CASHLESS LAYER
Game changing electronic payment systems and transition to cashless economy
IMPS, AEPS, APB, and UPI
PAPERLESS LAYER
Rapidly growing base of paperless systems with billions of artifacts
Aadhaar e-KYC, E-sign, Digital Locker
PRESENCE-LESS LAYER
Unique digital biometric identity with open access of nearly a Billion users
Aadhaar Authentication
JAM
Jan Dhan, Aadhaar, Mobile

Source: Pramod Varma.

IndiaStack also includes components like eKYC (electronic Know Your Customer), eSign, and DigiLocker. eKYC simplifies the customer verification process, eSign enables the digital signing of documents, and DigiLocker provides a secure cloud-based platform for storing and sharing official documents.

By integrating all these components within IndiaStack, the Indian government has created a robust digital infrastructure that facilitates efficient and secure transactions, fosters financial inclusion, and empowers people to control their personal data.

All the same, IndiaStack has also faced problems and criticism, mostly for three reasons. First, the **security** of the system has been questioned. There have been multiple reports of data breaches and unauthorised access to Aadhaar data. For instance, in 2018, a breach reportedly allowed access to the personal data of over a billion people for a small fee. There have been instances where the implementation of Aadhaar has led to exclusion errors, denying people access to essential services due to authentication failures or data mismatches. Likewise, ensuring the security and privacy of the data exchanged through UPI and DEPA remains a priority to address concerns and build trust among users and stakeholders.

Second, the system has been criticised for being prone to **privacy violations and mass surveillance**. This is mostly due to the fact that Aadhaar stores sensitive biometric data (fingerprints and iris scans) linked to personal details, creating a centralised database. Being linked to a wide variety of services, from banking to healthcare, welfare, and taxation, centralised data storage can be converted into rather intrusive tracking by the government, even if most of the applications running on IndiaStack are formally separate from the underlying infrastructure and can exhibit varying levels of safeguards against government monitoring. In any event, the concern related to surveillance is exacerbated by the lack of comprehensive, robust, and well-implemented legislation on privacy related to both private and public surveillance.

A third concern is that IndiaStack is **not fully open source**. Rather, it is a mix of open APIs and controlled core infrastructure. For example, in the case of Aadhaar, the APIs are open, but the system's backend is proprietary and controlled by the Indian government. Similarly, the National Payment Corporation of India operates and controls the core UPI infrastructure, and while APIs are open for use, the system itself is not open source. Although developers can use and integrate many of the stack's APIs, the underlying systems and codebases are not fully open source. This hybrid approach ensures accessibility for developers while maintaining centralised control over critical national infrastructure for security and policy considerations.

Since New Delhi hosted the G20 presidency last year, the nation's DPI has become central to Prime Minister Narenda Modi's strategy, with the aim of positioning India as an emerging economic superpower, an attractive alternative investment destination for China, and a leading voice for the Global South. The DPI featured prominently in the sixth Quad Leaders' Summit in September 2024, marking the continuation of a high-level dialogue between India and the US, Australia, and Japan. During the G20 Digital Economy Working Group meetings in 2024, several countries (inter alia, Armenia, Sierra Leone, Suriname, Antigua, and Barbuda) signed Memorandums of Understanding with India to adopt IndiaStack's digital solutions.

3.2. BRAZIL'S PIX: A REVOLUTION IN DIGITAL PAYMENTS

The Brazilian Pix system is a real-time payment platform developed and managed by the Central Bank of Brazil (BCB). It is a highly efficient and inclusive payment system designed to facilitate instant, secure, and cost-effective transactions for individuals and businesses. Launched in November 2020, Pix has quickly transformed Brazil's financial landscape – attracting millions of users and bringing to the surface many transactions that had previously occurred in the informal economy.

At the same time, Pix has faced criticism similar to that of IndiaStack, particularly for its homologous UPI. Notably, Pix is operated centrally by the BCB, which has direct access to all transaction data. Such access could potentially be used for profiling, monitoring, or surveillance, since Pix is integrated with other public systems, including tax collection and government benefits. Pix transactions are also directly tied to the user's tax ID or phone number, which ends up leaving a digital trail. Yet unlike India, Brazil has enacted a comprehensive General Data Protection Law, although the effectiveness of this law in preventing the abuse of Pix-related data is still questioned.

Importantly, like IndiaStack, Pix is not a fully open source. On the one hand, the BCB made the communication protocols open source and the API specifications publicly available, allowing financial institutions, payment service providers, and developers to create interoperable solutions. It hosts an official GitHub repository where Pix-related resources (including API documentation and integration guides) are published. On the other hand, Pix's central infrastructure, including its operational framework and implementation, is managed exclusively by the BCB and is not open. The backend systems and centralised settlement mechanisms are not open source, a decision that is reportedly motivated by the need to ensure security, reliability, and regulatory compliance.

3.3. A fork in the road to DPI? Emerging alternative models for rollout

The entry of the G7 in the DPI dialogue signals a significant shift in global digital governance. While the G7 emphasises DPI's role in enhancing people's access to public services, the G20 envisages a broader scope where DPI facilitates equitable access to both public and private services. This difference reflects the varying perspectives on the purpose of DPI and its potential impact on market structures and competition policies.

Furthermore, the motivations for deploying DPI differ between the G7 and G20. The G7 focuses on public service delivery, leaving the task of fostering competitive markets to national regulators. By contrast, the G20 sees DPI as a means to disrupt incumbent positions, increase state capacity in digital service provision, and promote competition in digital ecosystems. The debate extends to design principles, with the G7 emphasising private sector involvement in building DPI components and the G20 advocating for open source technology and standards. Despite these disparities, both groups recognise the importance of engagement in global DPI discussions to shape future governance frameworks and outcomes.

The Global DPI Summit 2024 in Cairo emphasised seven key priorities for 2025: knowledge sharing, universal safeguards, inclusive innovation, thriving local digital ecosystems, sustainability, financing, and interoperability. These priorities aim to foster collaboration, ensure equitable access, promote sustainability, and establish global standards for DPI to drive inclusive and secure digital transformation worldwide. In practice, these priorities should sustainable digital ecosystems, enabling individuals to access essential services, governments to deliver better public services, and nations to collaborate on global challenges like climate change and economic inequality. However, they do not specify the exact approach for deploying DPI models.

DPI can be implemented using various models, each with distinct characteristics that impact governance, security, inclusivity, and innovation. These models range from decentralised and open-source approaches to centralised and proprietary systems, as well as hybrid models that combine elements of both.

3.3.1. Decentralised models

Decentralised and open-source models emphasise transparency, community-driven development, and distributed control, aiming to avoid reliance on single entities and promote inclusivity and resilience. These systems often utilise open standards and protocols, allowing different systems to interact seamlessly and foster innovation by enabling diverse stakeholders to develop applications and services. For example, Estonia's X-Road, an open-source data exchange layer, allows secure and decentralised sharing of data between government agencies. This system ensures that no single entity has complete control over data, enabling interoperability between public and private services. Similarly, the Signal Protocol, which powers the Signal messaging app, is open source, allowing anyone to verify its encryption methods. This transparency has made Signal a trusted platform for secure communication.

- **Open protocols for data exchange and interoperability** are key to ensuring access to different systems and promoting seamless interaction. For instance, the Open Network for Digital Commerce in India promotes a decentralised and interoperable framework to encourage participation from both large and small retail players.

- **Decentralised data storage** distributes data across multiple nodes, enhancing security and privacy by eliminating single points of failure. Examples include Estonia's data embassies, which operate in foreign territories with full legal protection and maintain the integrity and availability of the country's data.

- **Open-source software** allows countries to use existing work without relying on external vendors, reducing geopolitical risks and promoting collaboration and transparency. Open-source AI models, such as those on platforms like Hugging Face and Meta's Llama, provide alternatives to proprietary AI systems.

- **Cost-effectiveness is another major advantage of open-source systems**. Where a system is built on open APIs, developers and private companies can freely access and integrate its services into their applications. This approach has significantly reduced costs for developers and enabled widespread adoption, making it a cornerstone of India's digital public infrastructure. Additionally, decentralised systems are often more resilient to failure. For example, Bitcoin and other blockchain-based systems distribute control across multiple nodes, making them resistant to single points of failure or censorship.

Despite their benefits, decentralised systems can face challenges in scalability and coordination complexity, and require specialised knowledge for deployment and maintenance. For instance, while open source is intended to level the playing field, the scale of computing power needed to run large language models limits accessibility to well-endowed organisations and countries, perpetuating inequalities.

3.3.2. Centralised models

Centralised and proprietary models, by contrast, are characterised by centralised control and ownership. These systems are often chosen for their scalability, ease of use, and streamlined management. For example, Microsoft Azure provides ready-to-use cloud services, making it easy for governments and businesses to deploy infrastructure without building it from scratch.

- **Scalability is a significant strength of centralised systems**. For instance, **Aadhaar**, India's centralised digital identity system (with some open-source components), has successfully scaled to over 1.4 billion users, enabling efficient delivery of government services such as subsidies and welfare programmes. In the financial sector, **Visa** processes over 65 000 transactions per second, far outpacing decentralised payment systems like Bitcoin, which can only handle around 7 transactions per second. This makes centralised systems ideal for large-scale, time-sensitive projects.

- **Another advantage of proprietary systems is the dedicated support and maintenance they offer.** For example, Oracle provides proprietary database solutions with robust support, making it a popular choice for mission-critical systems like banking. During the COVID-19 pandemic, governments turned to centralised platforms like Salesforce for vaccine management systems because of their quick deployment capabilities and reliable support. Vaccine Cloud helped public health authorities and healthcare providers to quickly scale vaccine operations, such as recipient registration and public health outreach.

However, centralised systems come with their own set of challenges. Vendor lock-in[3] is a common issue, as organisations become dependent on a single provider. For example, many governments using Microsoft Office 365 face high switching costs if they want to

[3] This refers to a situation where the cost of switching to a different vendor is so high that the customer is essentially stuck with the original vendor.

migrate to open source alternatives like LibreOffice. Centralised systems are also vulnerable to single points of failure. For example, Amazon Web Services outages have disrupted major websites and services globally, highlighting the risks of relying on a single cloud provider. Government-led initiatives, while ensuring regulatory frameworks, may stifle innovation and limit private sector participation. Centralised systems also raise concerns about transparency and accountability, as their operation is often a 'black box'. For example, a third-party service provider developed Pakistan's Asaan Mobile Account scheme, whereas Singapore's PayNow was developed by the Association of Banks in Singapore, indicating different approaches to private sector involvement in DPI.

3.3.3. Hybrid Models

To balance the strengths and weaknesses of both models, many governments and organisations are adopting **hybrid approaches**. For example, Android is an open-source operating system at its core, but Google adds proprietary services like the Play Store and Google Maps to enhance its functionality. Similarly, India's UPI is an open API-based system that allows private companies like Google Pay to build proprietary apps on top of it. This approach ensures that the core infrastructure remains open and accessible, whereas private companies can innovate and provide user-friendly services.

The EU's eIDAS Regulation on electronic identification and trust services is another example of a hybrid solution. It combines centralised national identity systems (managed by individual EU Member States) with decentralised digital wallets (controlled by individuals). The amended Digital Identity Framework Regulation will be fully implemented by 2026, including its new solution of the EU Digital Identity (EUDI) Wallet from each Member State for its residents to use according to approved specifications (see more about the EUDI Wallet in Section 5.2).

Table 2 – Comparison of different aspects of decentralised and open-source vs centralised and proprietary models

Aspect	Decentralised/Open Source	Centralised/Proprietary
Control	Distributed among participants	Centralised under a single entity
Transparency	High, due to open standards and community involvement	Can be low, as systems often operate as 'black boxes'
Scalability	Can face challenges in scaling to meet large-scale demands	Generally easier to scale rapidly
Security	Enhanced by distributed data storage and decentralised control, reducing single points of failure	Can be robust due to enhanced control, but vulnerable to single points of failure
Innovation	Fostered through open standards and community-driven development	May be limited due to vendor lock-in and proprietary restrictions
Vendor lock-in	Low, due to open standards and open source software	High, can lead to dependence on a single vendor
Cost	Can be lower due to community contributions and open source	Can be higher due to licensing fees and reliance on proprietary technology
Interoperability	High, due to the use of open standards and protocols	May be limited by proprietary systems
Data ownership	Individuals have greater control and can monetise their data	Data are typically controlled by the central entity
Governance	Decentralised governance mechanisms, often using DAOs	Centralised governance by government or private entity

Source: Authors' own elaboration

Notably, for countries with a relatively small population (up to a million people), there is an emerging consensus on a possible way to roll out DPIs with less friction — DPI as a packaged Solution (DaaS) model. It is a comprehensive solution that is easy to adopt, cloud-ready (deployable in both private and public cloud environments), well-packaged, and ideal for all countries, particularly for those with small populations. DaaS has been suggested as a pilot for DPI deployment. DaaS pilots can start within three to six months after identifying a use case and securing a sponsor.

This approach, presented at the Global Technology Summit 2023 and positively received by DPI experts from 25 countries, offers an alternative to high-risk, capital-intensive traditional models. The Centre for Digital Public Infrastructure (CDPI), in collaboration with the EkStep Foundation, was set to launch a DaaS pilot last summer, with several countries already expressing interest. Through this innovative approach, DPI is presented as a cloud-ready 'plug-and-play' solution accessible to any country, significantly reducing the lengthy procurement and implementation processes. Housed at India's International Institute of Information Technology, the CDPI comprises a compact team of DPI architects from various parts of the world. Their mission is to offer pro bono technical architecture guidance, aiding countries in co-designing scalable localised solutions.

4. The DPI landscape in Europe: exploring pioneering initiatives

European countries have been trailblazers in the digital transformation of government, from relatively simple solutions all the way to Government-as-a-Platform (GaaP). Countries like Estonia, Finland, and Ukraine have made their digital ecosystem a source of competitiveness and a distinctive trait of the government's relationship with the public and businesses. Many of these initiatives have, in one way or another, revolved around the creation of a DPI, or layers thereof, with widely diverging modalities and governance arrangements.

4.1. Estonia's X-Road: the blueprint for DPIs

Estonia's digital transformation began in the early 2000s, when the government adopted a digital-by-default policy, aiming to make digital solutions the standard for public services. Today, 99 % of Estonia's public services are available online, and 98 % of Estonians use electronic IDs. A critical component of this transformation is *X-Road*, an open-source platform that facilitates secure data exchanges between public and private sector organisations. This system significantly enhances efficiency, saving the Estonian administration approximately 804 working years annually and contributing an estimated 2 % to the national GDP through the use of electronic signatures. More than 20 countries, including Cambodia, Brazil, Finland, and Namibia, have taken action to adapt X-Road through open source to suit their local needs.

Most importantly, X-Road is free, open source, and decentralised. Each participating organisation maintains its own data, reducing the risk of a single point of failure and enhancing the system's overall resilience and security. Data held by the Estonian administration are decentralised and duplicated through the use of 'data embassies', i.e. data centres that, despite sitting outside Estonia's borders, remain fully under Estonia's control and have the same rights as physical embassies, such as immunity.

The key principles underpinning X-Road, as well as the overall Estonian strategy, include:

(i) the 'once-only principle', based on which people and businesses provide information to the government only once, and the X-Road data exchange layer makes this information available to all other government actors;

(ii) the 'no legacy principle', which caps the technologies used in the DPI to a maximum of 13 years; and

(iii) the 'build versus buy' principle, which prioritises open-source systems built from scratch to off-the-shelf systems provided by ICT vendors.

Table 3 provides a non-exhaustive list of Estonia's initiatives in the DPI domain. Examples of the country's progress towards a DPI include the Estonian Government Cloud, the e-Identity system (e-ID), and the virtual assistant Bürokratt, compared with a 'Siri of digital public services'.

Table 3 – Estonia: selected DPI initiatives

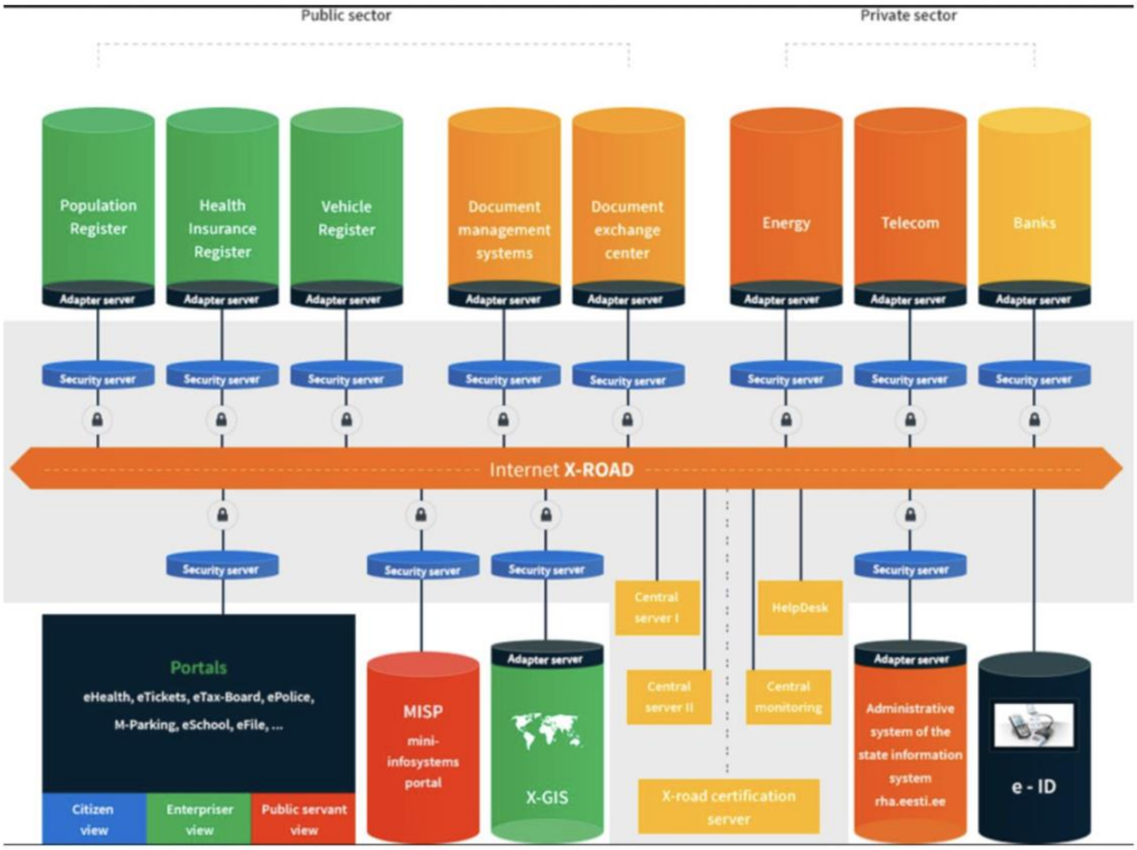
DPI Element	Estonia
Digital identity	- e-ID System: Estonia's digital identity system, known as e-ID, is mandatory for all citizens and residents. It is used for secure authentication and digital signatures. e-ID is used for a wide range of services. The chip on the card carries embedded files, and with 384-bit ECC public key encryption, it can be used as definitive proof of ID in an electronic environment. It is used for digital signatures, i-Voting, checks of medical records, submission of tax claims, and e-Prescriptions. - ID Cards: physical and mobile ID cards (Mobile-ID and Smart-ID) allow users to authenticate their identity online and provide legally binding electronic signatures. - Security: two-factor authentication and cryptographic technologies ensure high levels of security.
Digital payments	- Digital Banking: Estonia has a highly digitised banking sector where most transactions are conducted online or via mobile apps. - e-ID Integration: e-ID supports secure online payments and banking transactions, providing identity verification and authentication.
Data governance and interoperability	- X-Road Platform: Estonia's X-Road is an advanced data exchange platform that enables secure and standardised data exchange between public and private sector entities. It operates on a decentralised architecture, reducing the risk of single points of failure and enhancing resilience. It acts as a platform for application development and helps the state to extend its physical services through electronic ones. - Interoperability: promotes seamless interoperability, allowing different systems to communicate and share data efficiently.
APIs for public services	- API Ecosystem: Estonia provides a comprehensive set of APIs for public services, enabling secure and efficient access to various government databases and services. Open APIs are available for third-party developers to build applications that integrate with government systems, fostering innovation and service improvements. - Service Delivery: APIs facilitate automated and real-time access to services such as tax filings, business registrations, and health records. APIs are

	designed with strict security protocols and compliance with data protection regulations.
Other notable elements of DPI	- E-Residency Programme: Allows non-residents to establish and manage businesses in Estonia, access Estonian services, and benefit from the country's digital infrastructure remotely. - E-Estonia Initiative: This comprehensive national initiative aims at promoting digital innovation, improving public services, and fostering international collaboration in digital governance. - Virtual Assistant Bürokratt: This AI-powered virtual assistant is designed to streamline public services and improve their accessibility. - The Estonian State eService portal (eesti.ee) has been used by citizens to access over 800 services since 2003. The platform features an audit trail that allows users to see who accessed their data and why. Personal details such as a unique identifier, name, date of birth, sex, address history, citizenship, and legal relationships are stored in a single system, enhancing data protection by avoiding centralised storage.

Source: Authors' own elaboration

All in all, through these and other initiatives, Estonia has managed to build a fairly complete, free, open, and decentralised middleware, which is now becoming a global resource, especially for LMICs. X-Road is highly relevant to the future of the European DPI, as explained in Section 3. Unsurprisingly, X-Road has become an ally of the federated cloud project launched by France and Germany, known as Gaia-X, and is the basis for implementing sectoral data spaces.

Figure 3 – Schematic structure of X-Road



Source: X-Road.eu.

4.2. GERMANY'S DIGITAL STRATEGY 2025 AND THE SOVEREIGN TECH FUND

Recognising that Germany needed a comprehensive digital transformation, the German government adopted a digital strategy in 2016, setting out a series of goals to be achieved by 2025. In particular, the strategy structures the government's digitalisation policy priorities around three action areas: 'connected and digitally sovereign society', 'innovative economy, jobs, science and research' and 'digital learning and government'. To achieve these goals, the strategy prioritises projects that are expected to have the greatest multiplier effect across all government departments in the areas of efficient and sustainable networks, data availability, uniform international standards, and secure and user-friendly digital identities.

Table 4 – Germany: selected DPI initiatives

DPI Element	Germany
Digital identity	Since 2010, German ID cards have contained a chip with the electronic identification (eID) to ensure for secure, easy, and privacy-friendly electronic identity verification. The eID chip is also available for electronic residence permits, and the eID card for citizens of the EU and the European Economic Area. The eID is used for identification and authentication in digital administrative services that require a high level of security. Until 2017, online identification required a card reader, but since then it can be done with a smartphone (and a suitable app, such as the AusweisApp).
Digital payments	Germany is home to different fintech companies leading innovations in digital payments, like N26, Vivid Money and Trade Republic.
Data governance and interoperability	Germany launched a data strategy in 2023 aiming to strengthen data interoperability and contribute to the country's competitiveness through future-proof data use for business, civil society, science, and public administration.
APIs for public services	- Administrative Services Directory: this 'serves as an interdisciplinary and cross-administrative infrastructure, [providing] secure and reliable automation of services and procedures for communication between, and with, public entities'.
Other notable elements of DPI	- Plattform Industrie 4.0: this initiative involves collaboration between the government, research institutions, and the private sector to enhance digital transformation in manufacturing. This includes developing interoperable systems and standards for data exchange within industrial processes. 'Plattform Industrie 4.0 has a number of working groups that develop practical solutions and recommendations for action in the areas of standards and standardisation, technology and application scenarios, security of networked systems, legal frameworks, work and training, and business models.' 'In [the] 2030 Vision, the stakeholders of Plattform Industrie 4.0 present a holistic approach to the shaping of digital ecosystems, [aiming] to create a framework for a future data economy in line with the requirements of a social market economy: emphasising open ecosystems, diversity and plurality and supporting competition between all the stakeholders on the market.' - Smart cities: various smart city projects across Germany focus on using data to improve urban living. These projects emphasise data interoperability between different urban systems (e.g. transportation, energy, and public services) to create integrated and efficient city management solutions.

Source: Authors' own elaboration

Notably, with regard to funding for digital public infrastructure, the German government launched the Sovereign Tech Fund in October 2022 to strengthen the open-source ecosystem through the development, improvement, and maintenance of open digital infrastructure. The Federal Ministry for Economic Affairs and Climate Action finances it, with a budget of EUR 11.5 million in 2023, which increased to EUR 25 million in 2024. It is currently being incubated at the Federal Agency for Disruptive Innovation (SPRIN-D)[4]. The Sovereign Tech Fund has three active areas of work: general funding for open-source digital infrastructure, the Bug Resilience Programme, and Contribute Back Challenges.

Since its establishment in 2022, the Sovereign Tech Fund has supported 60 technology projects, with EUR 23.5 million allocated so far and plans to increase funding to EUR 29 million in 2025. The initiative aims to professionalise open-source development (addressing the reliance on unpaid developers) and strengthen global digital infrastructure through open technologies and public-interest digital resources. Currently, it has investments in various technologies, including FFmpeg, the OpenJS Foundation, the Python Package Index, and the Yocto Project.

The Sovereign Tech Fund was initially a state-owned company under SPRIN-D. Last year, the German government established the Sovereign Tech Agency, which is now the home of the fund. This better reflects its expanded scope, institutionalisation, and long-term commitment to supporting open-source technologies. While the Sovereign Tech Fund primarily focuses on providing financial support for open-source projects, the Sovereign Tech Agency has a broader mission. It not only funds projects but also invests in resilience programmes, fellowships, and structural improvements to strengthen the open-source ecosystem as a whole.

[4] At present, the Sovereign Tech Fund is no longer accepting applications as it is transitioning to a permanent organisation within SPRIN-D.

Table 5 – Germany's Sovereign Tech Fund: main areas of work

Area	Description
General funding	Applications were sought to invest in open digital base technologies 'that are vital to the development of other software or enable digital networking' with a focus on strengthening the open-source ecosystem. The Fund explicitly noted that it only supports 'technologies with societal relevance, i.e., technologies from which a broad public benefits or on which particularly vulnerable groups depend'.
Bug Resilience Programme	'Proactively increases the resilience of open source software infrastructure and empower[s] small and medium-sized open source projects.'
Contribute Back Challenges	These involved applications from developers using open source and seeking to give back to the ecosystem they leveraged. Three workstreams were established: Improve Free and Open Source Software (FOSS) Developer Tooling, Securing FOSS Software Production, and FOSS Infrastructure Documentation.

Source: Authors' own elaboration

Overall, the German approach to the DPI appears to be very different from Estonia's, in that the level of centralisation is much greater, and the commitment to open-source software is only partial.

4.3. The Netherlands

The Netherlands has developed a robust digital infrastructure over the past several decades, with a dedicated Dutch Digitalisation Strategy first released in 2018 and updated in 2019 and 2021. In 2022, the Netherlands ranked 3rd overall in comparison with other EU countries and 4th in the Digital Public Services category. On a global scale, the Netherlands ranked 9th in the UN's e-government development index in 2022 (EGDI).

Overall, the Dutch government is actively implementing digitalisation across its ministries – the Ministry of Interior and Kingdom Relations and the Ministry of Justice and Security bear the main responsibility for the implementation of NL Digibeter (the Digital Government Agenda). They are further supported by administrative consultations and advised by the Digital Netherlands Council. The government also collaborates closely with several coalitions, including the AI Coalition, the Digital Society Alliance, and the Data Sharing Coalition. Of particular note is the Data Sharing Coalition, through which the government is 'facilitating voluntary data sharing between sectors ... in order to utilise data capabilities for the benefit of the economy and society in a responsible way'.

In addition to the Digitalisation Strategy, the Netherlands presented in late 2022 the 'Values-Driven Digitalisation Work Agenda' to the Dutch House of Representatives. The agenda has five 'tracks': participation, trust, control over digital lives, a value-driven and transparent digital government, and strengthening the digital society in the Dutch Caribbean. In December 2023, a review was conducted of the initial round of initiatives.

Table 6 – The Netherlands: selected DPI initiatives

DPI Element	Netherlands
Digital identity	**DigID:** A digital authentication system used by residents to access government services online. It provides a secure and standardised method for people to verify their identity and perform various online transactions, such as tax filings, healthcare services, and social benefits.
Digital payments	**DigID:** Though DigID itself is not a payment system, it can serve as a secure authentication for accessing certain financial services. As such, Dutch citizens have access to tax services, social benefits, pensions, municipal services (taxes, fines, and fees), healthcare-related payments, student finance, and housing allowances.
Data governance and interoperability	• **Data Overheid:** Data Overheid is an open data initiative that promotes transparency and innovation by making government data freely available to the public. This initiative supports the development of data-driven applications and services, fostering economic growth and enabling informed decision-making by people and businesses. • **NORA (Nederlandse Overheid Referentie Architectuur):** NORA provides a framework for designing and implementing interoperable public services. It includes guidelines, standards, and best practices for data exchange and system integration. • **StUF (Standard Uitwisseling Formaat):** This is a set of standards for data exchange between Dutch government entities. It ensures that data can be shared consistently and efficiently across different systems. • **eHerkenning:** This digital authentication tool is designed for businesses. It allows companies to securely access government and semi-public services online. By standardising the authentication process, eHerkenning simplifies administrative procedures and enhances security for business transactions with the government. • **Common Ground**: This initiative aims to modernise the Dutch public sector's IT infrastructure by creating a modular and interoperable system architecture. It separates data from applications, allowing for more flexible and efficient data sharing and system integration.

	• Basic Data Infrastructure (BDI): Decentralised data sharing takes place between companies and authorities for all forms of transport. • National Mobility Data Access Point (NTM): Data on road traffic and multimodal travel information come together and are made accessible to all parties. • DEFLog (Data Exchange Facility for logistics): Enables logistics service providers to digitally incorporate road closures, roadworks, and other infrastructure 'disruptions' into their planning.
APIs for public services	The Dutch government offers a range of APIs for public services, including: • Kadaster API (property and real estate) • RDW API (vehicle registration data) • BRP API (Dutch Personal Records Database) • KvP API (business registration data) • Belastingdienst API (tax-related data) • DigID • Data Overheid (open data APIs) • MijnOverheid (MyGovernment) • DUO API (educational services, data, and student finance) • SVB API (social insurance and benefits data).
Other notable elements of DPI	• Data Sharing Coalition • Basisregistraties (Key Registers): These are central databases that hold essential information such as personal records, business information, and addresses. They ensure that all public sector entities use the same authoritative data, reducing redundancy and improving accuracy. • MijnOverheid: Provides access to a personal dashboard for citizens, aggregating their interactions with different government agencies. • Omgevingsloket Online (OLO): OLO is an online environmental permit system that streamlines the application process for permits related to construction, the environment, and spatial planning. It provides a single point of access for individuals and businesses to submit applications and track their progress, improving transparency and efficiency in the permitting process.

Source: Authors' own elaboration

In 2017, the 5 largest Dutch cities (the 'G5') and 32 medium-sized to large cities (the 'G32') took part in the NL Smart City Strategy, which was developed in partnership with the private sector and other institutions. The G5 comprises Amsterdam, Rotterdam, The Hague, Utrecht, and Eindhoven. These initiatives are aimed at leveraging technology and data to enhance the quality of life in urban areas, improve sustainability, and increase efficiency in public services.

Table 7 – Smart City DPI initiatives in the Netherlands

Cities	Smart City Initiatives-- Examples
Amsterdam	• **Energy Transition**: Projects like the Smart Energy Grid and energy-neutral buildings aim to reduce the city's carbon footprint. • **The Marineterrein Living Lab:** To transform the historic Marineterrein area into a living lab for sustainable urban development and innovation, initiatives include smart energy solutions, sustainability mobility and an innovation hub.
Rotterdam	• **Climate Adaptation**: As a city prone to flooding, Rotterdam has implemented smart water management systems, green roofs, and water plazas to manage excess rainwater. • **Port of Rotterdam**: Digital technologies are used to enhance the efficiency and sustainability of port operations, including automated logistics and real-time data sharing.
Eindhoven	• **Living Lab Stratumseind**: This project involves the installation of sensors in the city's nightlife district to monitor and improve public safety and manage crowd behaviour. • **Brainport Smart District**: A neighbourhood is being developed as a living lab for smart technologies, focusing on energy-neutral homes, smart mobility, and community engagement.
Utrecht	• **Utrecht Central Station**: A major transportation hub seeks to integrate smart technologies to manage passenger flow and enhance the user experience. • **Smart Solar Charging:** This project involves installing solar panels on rooftops and using the generated energy to charge electric vehicles. The smart charging stations can also feed excess energy back into the grid, optimising the use of renewable energy.
The Hague	• **Urban Data Center:** The Urban Data Center in The Hague collaborates with Statistics Netherlands (CBS) to analyse and use urban data effectively. This

	helps the city to address challenges like housing, transportation, and public health through data insights. • **Air Quality Monitoring:** The city has installed a network of sensors to monitor air quality in real time. Data from these sensors is used to inform policies and actions to reduce pollution and improve air quality.

Source: Authors' own elaboration

In 2018, several Dutch public institutions came together to set up PublicSpaces, with the stated ambition of 'providing a digital social platform that serves the common interest and does not seek profit'. The coalition aims 'to orient public institutions to invest their resources into digital solutions that reflect a set of key values based on their Public Interest Missions'. Their five core values are solutions that are open, transparent, accountable, sovereign, and user-centric (European Public Digital Infrastructure Fund). Over 35 public institutions have joined the coalition since 2018, and PublicSpaces claims to reach more than 70 % of the Dutch population through those institutions.

4.4. Italy's journey to digital government

Italy had an epiphany with its Digital Transformation team, which worked from 2016 to 2019 and stated their intention to 'build the "operating system of the country", a series of fundamental components on top of which we can build simpler and more efficient services for the citizens, the public administration and businesses, through innovative digital products'. In 2019, the team was jointly replaced by the Department for Digital Transformation (the Italian government body for promoting and coordinating efforts to establish a unified strategy for digital transformation through digital technologies) and the pagoPA company.

pagoPA is wholly owned by the state through the Ministry of Economy and Finance and is subject to the supervision of the Prime Minister. Its mission is to design and build infrastructure and technological solutions to promote the diffusion of digital public services that are accessible to people and businesses in the simplest possible way. pagoPA does that via mobile devices and according to the 'once-only' principle, with secure, scalable, highly reliable architectures based on clearly defined APIs.

PagoPA acts as an intermediary between the public sector and the market. It is entrusted with the development of the national electronic payment system pagoPA and the public services app 'IO', as well as the National Digital Data Platform (PDND), launched in October 2022 and the Digital Notification Service (SEND) launched in July 2023. In 2024, IO was reportedly used by an average of 5 million monthly users to transact with a population of approximately 18 000 public administrations. As of March 2024, there were 410 payment service providers connected to the pagoPA platform. The 182.5 million transactions handled by pagoPA in 2021, for a value of approximately EUR 4 billion, grew to 422 million in 2024, for a value of over EUR 93.5 billion.

This already well-developed part of the Italian DPI is likely to be further boosted by the National Recovery and Resilience Plan, which allocates 25.1 % of total funds to the digital transition (EUR 191.5 billion). Of this, nearly EUR 900 million is devoted to implementing digital infrastructure, encompassing investment in digital infrastructures and ultra-wideband connectivity. It also covers initiatives to advance the digitalisation of public administration systems. This entails ensuring that they are hosted in secure, reliable data centres, with rigorous standards for quality, security, and efficiency.

The strategy involves (i) establishing a national hybrid infrastructure utilising cloud technology, referred to as the 'National Strategic Hub' or certifying secure public clouds; (ii) completely digitalising the national population register (already achieved); (iii) boosting the uptake of e-Identity (possibly moving from an externally assigned ID or 'SPID' to embedding digital identity in national ID cards); and (iv) diffusing the IO app (World Bank, 2023, p. 28).

The approval of Law decree no. 19 of 2 March 2024 established the Italian Digital Wallet System (IT-Wallet), entrusting the implementation and management of the technical and organisational infrastructure to pagoPA and to the State Mint and Polygraphic Institute.

Table 8 – Italy: selected DPI initiatives

DPI Element	Italy
Digital identity	**SPID** (Public Digital Identity System) and CIE (Electronic Identity Card). Both systems are currently used to access the online services of public administration for identification purposes. The main difference is their level of security (CIE is more in line with the EU standard). The current Italian government announced its intention to give higher priority to CIE in the future.
Digital payments	**pagoPA:** This platform enables people to pay their taxes, fees, or charges to the public administration, either online via the IO app or via their preferred payment service provider and/or other channels (bank, payment app, etc.).
Data governance and interoperability	**IO app:** On this unified platform, all local and national authorities (like municipalities, regions, and central agencies) can deliver their services to citizens in an easy manner, according to the user's needs and preferences, accessible directly on smartphones or tablets. **IT-Wallet:** Established in February 2024, this service began working in October 2024. In its first phase, important documents like driving

	licences, health cards and European disability card-specific documents were made digitally storable and accessible on the IO app. Selection during the initial phases will be randomised, ensuring compliance with privacy and data protection regulations. Since December 2024, all citizens have been able to access digital versions of key documents through the IO app. As of December 2024, there were 3 069 253 active eIDs, 2 438 350 active driving licences, 2 671 171 active Health Cards, and 43 243 active disability cards. This initiative is a precursor to the full implementation of the IT-Wallet, scheduled for 2025. **PDND Interoperability:** This platform enables the exchange of information between entities. Each entity on the PDND can exchange information in a simple and secure way, publishing the e-services it manages in the catalogue and requesting the use of those it needs.
APIs for public services	**The IO app manages APIs for most public services** (national digital identity system, the platform for electronic payments (pagoPA), and the single national registry). The app enables people to receive messages, alerts, and communications from any public entity in one place.
Other notable elements of DPI	In April 2020, Italy launched its **National Coalition for Digital Skills and Jobs** (built on 'Repubblica Digitale'), the national strategic initiative designed to address the cultural digital gap among the Italian population, enhance digital inclusivity, and promote education on future technologies.

Source: Authors' own elaboration

Italian public administration has traditionally been extremely fragmented, with over 23 000 entities, each with distinct communication channels, procedures, and touchpoints for public services. In this framework, pagoPA has played an important role in strengthening a unified ecosystem of interoperable, user-friendly digital platforms to streamline and enhance interactions between the state, its citizens, and businesses. As remarked in Section 5, pagoPA is participating in two of the four Large-Scale Pilots initiated by the European Commission to test EUDI Wallet applications. These pilots, called Potential and Nobid, began their activities in April 2023, and are scheduled to conclude in May 2025.

The IO app, which will host the upcoming IT-Wallet, is also intended to host the EUDI Wallet developed within the Large-Scale Pilot Potential project. This dual hosting strategy ensures ongoing alignment with EU regulations and technological developments for interoperability. Therefore, people will be able to access all digital infrastructures by pagoPA and public services (including communications, payments, and documents) thanks to a unique channel. For example, via the IO app, notifications sent near deadlines keep users informed, and payments for services or taxes can be completed within the app directly from received messages. Each communication includes references to the relevant entity and offers quick access to specific contact channels for further information. The IT-Wallet is scheduled for launch in 2025, ahead of the European roadmap for EUDI Wallet implementation. This early launch positions Italy as a frontrunner in digital identity solutions and allows for valuable insights and experience to be gained before the broader EU rollout.

In the fulfilment of its mission, pagoPA has also launched other platforms and services that add to the richness of the Italian DPI. One is Piattaforma Welfare (welfare platform), designed to streamline and simplify access to welfare benefits. It leverages the IO app's functionalities, such as user accounts, notification systems, and QR code-scanning capabilities, to provide a comprehensive and user-friendly experience for managing and accessing welfare benefits. The platform aims to consolidate various welfare programmes, making it easier for beneficiaries to access and use their benefits. The platform promises to benefit both the public and institutions, with advantages such as faster processing times, reduced costs, improved transparency, and increased accessibility.

Finally, pagoPA has recently established an Open Source Programme Office (OSPO), a multidisciplinary working group tasked with the 'systematic implementation of best practices in the company's open project management' and fostering transparency in the service of the public[5]. The Italian OSPO's activities cover various areas, as described in Table 9. This initiative represents a model that can be replicated in both the public and private sectors, in Italy and abroad.

[5] It must be noted that the European Commission and some agencies of the UN already have OSPOs (the latter in line with the achievement of the SDGs).

Table 9 – Areas of activity of the Italian OSPO

Area	Key Tasks
Tech area	This area offers expert consulting services to spread specialised knowledge and foster a robust open-source culture among the product teams. This entails creating informational materials tailored to communicate effectively with the developers at pagoPA. Additionally, it involves identifying, maintaining, and integrating the technical tools necessary to support and enhance this engineering culture.
Legal area	This area is dedicated to building an ecosystem within the company that aligns seamlessly with the principles of the open-source community. This involves formulating company policies that facilitate contributions to third-party projects or carefully selecting appropriate licences for the company's repositories.
Communication and institutional relations	Experts in this field manage relationships with institutional entities such as the European Community and universities, as well as with the external developer community. Tasks include developing tools, channels, and best practices that enable efficient communication between developers and the community, ensuring easy and clear access to code and documentation.

Source: Authors' own elaboration

In summary, Italy's journey towards building a full-scale DPI is well advanced and largely reliant on secure, open-source solutions. The IO app's source code is publicly available on GitHub under the European Union Public Licence (EUPL-1.2), which ensures that the app can be freely used, modified, and distributed as long as the derivative works comply with the same licence terms. In the future, progress in digital literacy and further improvements in the app's coverage of public services are likely to lead to a fuller scale-up of the Italian DPI.

4.5. UKRAINE'S DPI

One country that has made important progress towards DPI is Ukraine. Despite not yet being part of the EU, it is worth mentioning some of its DPI-related solutions, as these have already been partly implemented in other countries, including EU Member States.

Ukraine's digital development began in 2012 with support from the Organization for Security and Co-operation in Europe and Estonia's e-Governance Academy. This effort was further strengthened in 2014, which helped establish key components of Ukraine's digital government. Ukraine introduced two complementary e-government instruments. The first was the e-procurement platform Prozorro. Designed to enhance efficiency, transparency, and competitiveness in government procurement, Prozorro began with small procurements and expanded to larger ones. The system aims to streamline procurement and reduce corruption, targeting an annual public procurement loss of USD 2.2 billion due to limited competition and corruption (Ingram and Vora 2024).

Prozorro's platform, based on open-source code and open standards, provides a central and standardised process for tender notices, bid submissions, and contract awards. It operates on three principles: openness, transparency, and a 'golden triangle' partnership between the state, business, and civil society. Key features include the disclosure of all procurement information, a two-stage bid process, and oversight by civil society organisations like Dozorro, which monitors procurement and identifies high-risk tenders.

Table 10 – Ukraine: selected DPI initiatives

DPI Element	Ukraine
Digital identity	- **Diia**: Ukraine's primary digital identity system is integrated into the Diia app. The Diia app provides access to digital passports, driving licences, and other documents. - **Security**: Utilises advanced encryption and authentication methods to ensure secure identity verification.
Digital payments	- **Cashless Society Initiative**: Ukraine is actively promoting cashless transactions to enhance financial inclusion and reduce corruption. - **Integration with Diia**: The Diia app supports digital payments for government services, taxes, and fines.
Data governance and interoperability	- **Trembita**: Ukraine's equivalent of Estonia's X-Road facilitates secure data exchange between government institutions. - **Interoperability**: Ensures seamless communication between different government systems and databases. - **Data Protection**: Complies with the GDPR and national data protection laws to safeguard personal information.
APIs for public services	- **Open APIs**: Ukraine offers open APIs to facilitate the development of public and private sector applications. - **Diia APIs**: The Diia platform provides APIs for accessing various e-government services. - **Developer Engagement**: Encourages developers to create innovative solutions that integrate with government services.

	- **Efficiency:** APIs streamline processes such as business registration, tax filing, and public service access.
Other notable elements of DPI	- **Diia City**: This special legal and tax framework aims at boosting the IT sector and digital economy. - **E-Governance**: These comprehensive e-governance initiatives seek to digitalise public services and reduce corruption. - **Digital Education**: Programmes to improve digital literacy and skills among citizens help ensure widespread adoption of digital services.

Source: Authors' own elaboration

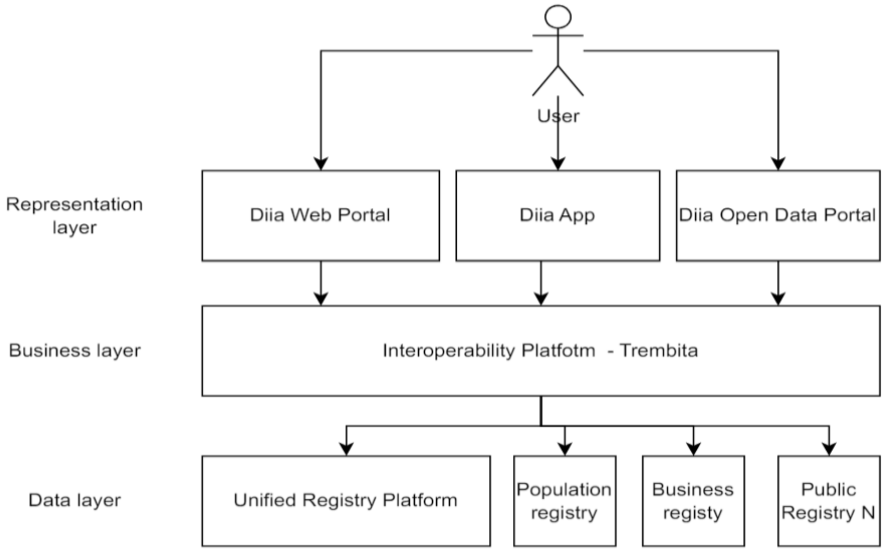
Three years later, e-services for people and businesses were launched on the platform, Trembita. It is an interoperable, decentralised platform modelled on Estonia's X-Road but tailored to Ukraine's needs. Utilising cryptography standards conforming to Ukrainian regulations, Trembita was developed with licenced technology from Estonia-based Cybernetica. Key security features include encrypted data transmission and storage, digital signatures for data modification, and secure logging and backup. Trembita has significantly improved transparency and efficiency by facilitating information exchange across hundreds of government registries.

Among the most prominent services, the most notable example is Diia, launched in April 2020. Powered by the Trembita system, Diia is a mobile application and web portal that simplifies citizen–government transactions. Key features include the legal storage of digital documents in secure registers, verification linked to the registry, and credential storage that only keeps depersonalised data for operational needs while displaying information from state registers without storing personally identifiable information. Users can access personal documents such as IDs, driving licences, passports, social security numbers, and student IDs. Ukraine became the first country in the world with a digital passport that served as a full legal analogy of ordinary physical documents.

Before the full-scale Russian invasion, Diia had approximately 14.5 million users; now, it boasts over 20 million. Diia has become essential since the start of the war in 2022 for displaced Ukrainians and those abroad, offering digital ID, document management, and access to social benefits in other countries. This digital tool has enabled direct applications for monthly cash assistance, which is crucial for meeting humanitarian needs at a time when documentation is often lacking. As the war has progressed, Diia has expanded its range of e-services. New features include buying military bonds, contributing military and medical equipment funds, providing financial aid to entrepreneurs and employees in conflict areas, and offering assistance to displaced people. Additionally, users can apply for property damage compensation, access news, use eDocuments for identification, obtain e-pension certificates, manage car registration and driving licence renewals, receive court decisions, and change residency.

Diia has facilitated border crossings and access to social services in Poland and has enabled the issuance of Canadian driving licences in some locations. Some of the key current developments include the launch of the electronic Diia.Signature, which is compliant with EU standards and enables Ukrainians to sign European contracts and documents. Diia facilitates communication with government offices, allowing users to submit requests and track application statuses. It integrates with payment systems for paying government and private service fees. Furthermore, it enables the digital creation, signing, storage, and sharing of documents, including the transfer of document copies.

Figure 4 – High-level architecture of e-Gov in Ukraine



Source: Ingram and Vora (2024).

4.6. A COMPARATIVE OVERVIEW OF SELECTED NATIONAL DPI INITIATIVES

Table 11 provides a comparative analysis of the key elements and initiatives of DPI across Estonia, Ukraine, Germany, the Netherlands, and Italy based on the analysis in the previous subsections. What emerges is a relative fragmentation of the DPI landscape in Europe, with varying features in terms of coverage, degree of centralisation, security, transparency, and commitment to open source. As a result, Europe's journey towards an integrated DPI appears to be fundamentally hampered by the lack of genuinely interoperable, if not common, pan-European approaches and solutions for the DPI. As observed in Section 5, this fragmentation also constrains Europe's ambition to achieve technological sovereignty and competitiveness by unleashing the macroeconomic benefits that a fully fledged DPI can offer.

Table 11 – Comparative overview of national DPI initiatives

DPI Element	Estonia	Ukraine	Germany	Netherlands	Italy
Digital identity	e-ID System: Mandatory for all citizens and residents. Used for authentication and digital signatures.	Diia: Integrated into the Diia app, providing digital passports, driving licences, and other documents.	eID: Chip-enabled ID cards for secure electronic identity verification.	DigID: A digital authentication system used by residents to access government services online.	SPID (Public Digital Identity System) and CIE (Electronic Identity Card).
Digital payments	e-ID Integration: Supports secure online payments and banking transactions.	Cashless Society Initiative: Promotes cashless transactions and integrates with Diia for digital payments.	Leading fintech companies like N26 and Vivid Money.	DigID: Used for secure authentication in accessing financial services.	pagoPA: Platform for paying taxes, fees, and charges to the public administration.
Data governance and interoperability	X-Road Platform: Secure and standardised data exchange between public and private entities.	Trembita: Facilitates secure data exchange between government institutions, ensuring seamless communication.	Data Strategy: Strengthens data interoperability and contributes to competitiveness through future-proof data use.	Data Overheid: Promotes transparency and innovation by making government data freely available.	IO app: A unified platform for delivering services to citizens via smartphones or tablets.
Open-source commitment	Global leader in open source use; X-Road components are shared internationally, adoption by other nations encouraged.	High use of open-source components, with international collaborations promoting scalability and transparency.	Limited open-source adoption; reliance on proprietary systems with some recent government pushes towards transparency.	Moderate open-source use; open standards encouraged, but there is reliance on proprietary systems for critical components.	High commitment to open-source solutions like the IO app and pagoPA, promoting transparency and collaboration.
Other notable elements	E-Residency Programme: Allows non-residents to manage businesses in Estonia.	Diia City: Special framework to boost the IT sector and digital economy.	Plattform Industry 4.0: Enhances digital transformation in manufacturing through	Common Ground: Modernises IT infrastructure with a modular and	National Coalition for Digital Skills and Jobs: Addresses the cultural digital gap and promotes

	Virtual Assistant Bürokratt: AI-powered assistant for public services.	Digital education programmes for improving digital literacy.	collaboration. Smart City projects for integrated and efficient urban management.	interoperable system architecture. Basisregistraties: Central databases holding essential information.	education on future technologies.

Source: Authors’ own elaboration

5. The EU DPI: a brick in the EuroStack wall

In the early 2010s, the EU started to realise the potential for tension between the rise of the World Wide Web and consolidated EU policies such as the 1995 Data Protection Directive, which is deeply rooted in national law. Competition law, with its *ex post* approach requiring proof of abuse of dominance and consumer harm, began to suffer with the decision by the European Commission in 2004 in the *Microsoft client-server interoperability and Windows Media Player case.* This continued in the 2010s with the Google search case, which took almost a decade for the Commission and is still pending before the Court of Justice of the European Union.

The fast-paced development of cyberspace has at once created enormous opportunities but almost insurmountable obstacles for EU policymakers. Tech giants were the only market players able to really tap the potential of the single market, leveraging their enormous resources to serve customers across borders. The rest, including both public and private services, remain on hold. In a recent study, Scott Marcus found that reliance on cross-border e-commerce in the EU has plateaued and even fallen in the past few years.

Importantly, the gradual reintermediation of the internet by 'gatekeepers' (using the terminology of the EU Digital Markets Act) has led to the rise of platforms that largely reproduce, in private form, the functioning of a digital infrastructure, yet in private hands. For example, both Google and Apple have managed to create mobile environments in which electronic identity, very well-developed wallets, secure data storage, and e-payments have become part of a single, conglomerate offer that is hard for any competitors to match. In the future, national governments wishing to launch a DPI may have to mandate the interoperability of public services and DPI layers with private conglomerate business models or (for security purposes) impose the integration of secure elements related to digital identity, secure data exchanges, and e-payments into commercially available devices.

Building a European DPI requires a plethora of reforms and initiatives, many of which have already been launched by EU institutions but would need a further boost in the coming years. These include, inter alia:

- the modernisation and digital transformation of administrations in Member States;
- the development of a common framework for digital identity, at least to enable cross-border transactions and document exchanges;

- the definition of standards and a reference architecture for identity and credentials verification and data exchanges;
- the standardisation of public-to-private exchanges to enable the fruition of private services through public infrastructure; and
- ensured interoperability with a decentralised model and standardised access token.

More recently, the European Commission has started working on a comprehensive and self-sovereign data layer that includes the federated cloud and the deployment of thousands of edge nodes throughout the territory of the EU.

Accomplishing all this amounts to a herculean task and almost an uphill battle if one considers the fragmentation and heterogeneity of national DPI initiatives, as described in Section 3. Below, we briefly take stock of the making of the European DPI, starting with the identity and wallet layers and then discussing the data and edge/cloud layers. Importantly, we also describe how recent EU legislation can become an ally for DPI.

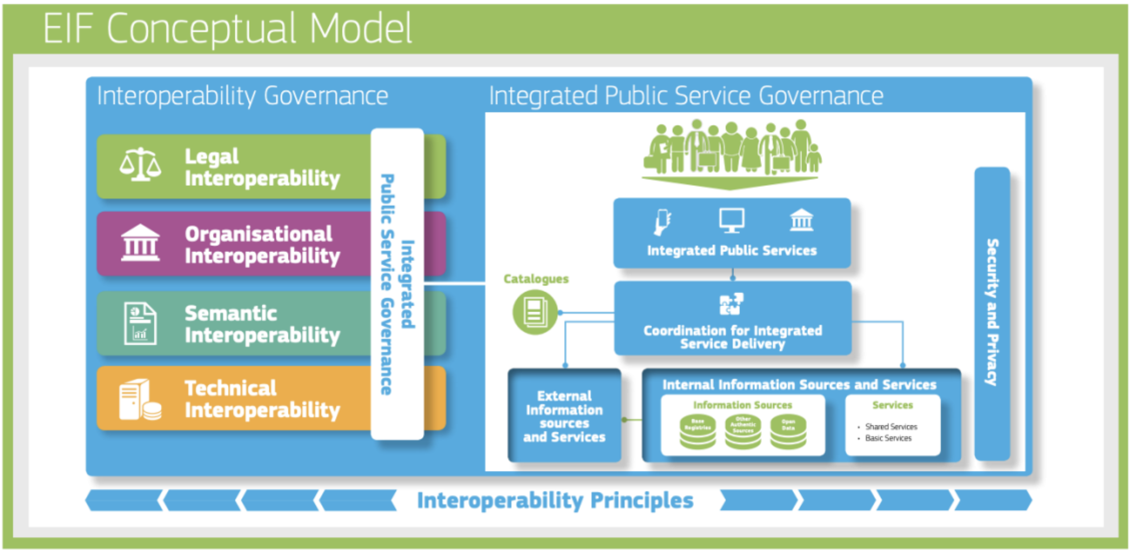
5.1. MODERNISING AND CONNECTING PUBLIC ADMINISTRATION: A LONG AND WINDING ROAD FROM CROSS-BORDER TO BORDERLESS PUBLIC SERVICES

As explained above, one of the key preconditions for building an integrated EU DPI is the modernisation and digitalisation of administrations in Member States, a process that the EU has tried to stimulate for over 25 years, particularly since 2010. It is still a work in progress in some countries despite a clear focus placed on this aspect by the national Resilience and Recovery Strategies after COVID-19.

Member States have tried to speed up the development of eGovernment, particularly with the Tallinn Declaration in 2017, followed by the Berlin Declaration in 2020, which takes the user-centricity tenets one step further by committing to a digital transformation in Europe firmly based on democratic values and ethical principles. The 2020 Berlin Declaration also clarifies the overall direction that Member States want to take, based on a 'human-centred digital transformation and interoperability as a key enabler for digital public services in the EU'. It sets the ambitious target of 100 % online provision of key public services in the EU by 2030.

Over the years, the European Commission has tried to stimulate a modular approach to solutions for public administration in what was initially called the European Interoperability Framework (EIF). In particular, the ISA2 project on interoperability for public administrations developed dozens of applications, which were kept voluntary for any Member State that wished to make use of them. This approach, still primarily focused on making national frameworks interoperable, ended up only partly successful in terms of uptake (CEPS, 2020). It was instrumental in promoting principles that, while established in certain Member States, were still far from widely endorsed in others. These included user-centricity, transparency, and reusability of public services, as well as the preference for open-source solutions and open data policies.

Figure 5 – Conceptual model of the European Interoperability Framework


EIF Conceptual Model
Interoperability Governance
Integrated Public Service Governance
Legal Interoperability
Organisational Interoperability
Semantic Interoperability
Technical Interoperability
Integrated Public Service Governance
Integrated Public Services
Catalogues
Coordination for Integrated Service Delivery
External Information sources and Services
Internal Information Sources and Services
Information Sources
Base Registries
Other Authentic Sources
Open Data
Services
Shared Services
Basic Services
Security and Privacy
Interoperability Principles

Source: European Commission (2017)

From the outset of the first von der Leyen Commission, DG DIGIT, a directorate that plays a coordinating role in the development of information technology and ICT systems for the European Commission, has driven a gradual transformation of the EIF into a more binding convergence process. In February 2020, the European Commission adopted the Communication 'Shaping Europe's digital future' (COM(2020) 67). Under the headline ambition of 'Europe fit for the digital age', the Communication sets out as a key action the development of a 'reinforced EU governments interoperability strategy' by 2021, aiming to foster coordination and the adoption of common standards for public services and data flows. Throughout the rest of the year, the need for action in the field of interoperability became even clearer as a result of the COVID-19 crisis.

Since then, a flurry of new initiatives has been launched, including:

- the Single Digital Gateway (which carved in stone the once-only principle as of 2023)[6];
- the Regulation on the free flow of non-personal data in 2018;
- the EU Cybersecurity Act and the Open Data Directive in 2019;
- proposals for a framework for a European Digital Identity (on which, see Section 5.2) and the EU Digital COVID Certificate Regulation in 2020; and
- the Proposal for the 2030 Policy Programme 'Path to the Digital Decade' in 2021.

In addition, the legislative framework was significantly enhanced by the adoption of new measures aimed at creating a more competitive and trustworthy market for data exchanges, as explained in Section 5.6.

In November 2022, the European Commission adopted the Interoperable Europe Act proposal to strengthen cross-border interoperability and cooperation in the public sector across the EU. In its impact assessment, the Commission took stock of the EIF and related initiatives. It concluded that 'the EIF, as a communication therefore not binding, has only supported voluntary implementation of interoperability. This is not sufficient to help remove cross-border and cross-sector barriers for the EU public sector and has led to persistent limited interoperability of public services in Europe.' The problem was caused, in the Commission's analysis, by three main obstacles:

(i) inefficient governance of interoperability efforts between EU policies and between the European Commission and Member States for all administrative levels (national, regional, and local) and sectors;

(ii) lack of common minimum interoperability specifications, shared solutions, and standards; and

(iii) lack of an 'interoperability by default' approach in the design and implementation of EU policies.

[6] The once-only principle will, from 2023, allow public administrations to reuse and share data and documents that people have already supplied in a transparent and secure way. (See Article 14 of Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services, OJ L 295, 21.11.2018).

The Commission set, among the specific objectives of the initiative, that of establishing 'interoperability governance designed to enable public administrations from all levels and sectors as well as private stakeholders to work together – with a clear mandate to agree on shared interoperability resources (e.g. IT solutions, specifications, standards or guidelines)'. It also sought the 'co-creation of an ecosystem of interoperability resources (solutions, open standards, data and services) for the EU's public sector, so that public administrations at all levels in the EU and other stakeholders can contribute to and re-use such resources, create public value and innovate together'.

At the time of choosing the preferred option, however, the European Commission eventually discarded the possibility of moving towards a more deeply integrated and coordinated approach to interoperability on the grounds that it would create frictions in the short term, especially in terms of compatibility with legislation already in the implementation phase (the Digital Services Act, Data Governance Act, and Data Act, among others). This was motivated also by the belief that the most ambitious option would imply 'a "standardisation" oriented approach which does not seem appropriate considering the differences in levels of digitalisation of the Member States'.

The Interoperable Europe Act eventually entered into force in March 2024. Among the key novelties introduced is the launch of structured EU cooperation, where public administrations come together in the framework of projects co-owned by Member States, as well as regions and cities. It features a multilevel governance framework steered by an 'Interoperable Europe Board'. It also offers the possibility of sharing and reusing interoperability solutions powered by a one-stop shop for solutions and community cooperation (Interoperable Europe portal).

Box 1 – The European Digital Infrastructure Consortium and ComPAct: a new focus on public administration

Two fairly recent additions to the future European DPI are the European Digital Infrastructure Consortium (EDIC) and the ComPAct programme.

The former is a rather innovative legal instrument launched under the Digital Decade policy programme and envisages multi-country projects (a minimum of three Member States) seeking to contribute to key areas selected by the European Commission. These include, among others, European common data infrastructure and services, compute infrastructure, connectivity solutions (e.g. 5G corridors), quantum- and space-based infrastructure, European blockchain services infrastructure, European innovation hubs, and cybersecurity solutions. The first EDICs currently being set up are the Alliance for Language Technologies EDIC (ALT-EDIC), which aims to create a large language model of European regional and official languages, and CitiVerse, which seeks to connect existing local digital twins across the EU. CitiVerse focuses on advanced generative AI applications in smart cities. The EDIC structure intends to deliver large-scale interventions by pooling resources across Member States[7].

One of the areas selected by the Commission is connected public administration. In that context, the EU is fostering shared digital infrastructures within the EU. Moving from the existing European Research Infrastructure Consortia, EDICs are being created to support multi-country projects that promote common standards and interoperability. These include training to foster a digitally skilled workforce with highly skilled digital professionals; establishing secure, efficient, and sustainable digital infrastructures; transforming companies digitally; and digitising public services.

An even more recent development is the ComPAct, a strategic set of actions aimed not only at supporting the public administrations in Member States to become more resilient, innovative, and skilled, but also at strengthening the administrative cooperation between them, thereby closing existing gaps in policies and services at the European level. With the ComPAct, the Commission is committed to enhancing the European Administrative Space by promoting a common set of overarching principles underpinning the quality of public administration and reinforcing its support for the administrative modernisation of the Member States. The ComPAct will help Member States address the EU Skills Agenda and actions under the European Year of Skills, deliver on the targets of the Digital Decade to have 100 % of key public services accessible online by 2030, and shape the conditions for economies and societies to deliver on the ambitious 2030 climate and energy targets. The ComPAct will also help EU enlargement countries on their path to building better public administration.

The most DPI-related pillar of ComPAct is Pillar 2, which is related to the Digital Decade. The Commission Communication focuses on, e.g. ‘digitalising administrative procedures, engaging in technical preparations for providing EU Digital Identity Wallets by 2026, increasing the automated exchange of evidence and information to deliver user-centric digital public services and improving the digital skills of staff’. It estimates that ‘[p]ublic administrations can generate efficiency gains amounting between EUR 439 million and EUR 1.3 billion a year by increasing the use of digital public services by up to 80 % by 2030’. Furthermore, ‘improving cross-border interoperability of digital public services could lead to efficiency gains [of] up to EUR 6.3 million for people and between EUR 5.7 and EUR 19.2 billion for businesses’.

ComPAct is still in its infancy but promises to provide a significant contribution to the shaping of the European DPI. For this to fully happen, however, a clear link and coherent connection to the emerging EuroStack would be needed to prevent separate EU initiatives from failing to contribute to a coherent vision of the European DPI.

[7] https://digital-strategy.ec.europa.eu/en/policies/edic

Against this highly complex background of emerging initiatives, we argue that a more ambitious approach is needed for a fully fledged DPI to emerge in Europe. This would require, inter alia, abandoning the focus on 'cross-border' interoperable services to embrace a borderless model grounded in a deeply user-centric redesign of public administrations at all levels of government in the EU.

5.2. The digital identity and payments layer: towards the European wallet

Nowhere has the European Commission tried to push for a decentralised, user-centric approach more than in the digital identity layer. The quest for a pan-European digital identity framework started early and met the first milestone with the first eIDAS Regulation in 2014. The eIDAS framework became a reference for countries around the world, even forming the basis for what would later become the Model Law on the Use and Cross-Border Recognition of Identity Management and Trust Services by the UN's trade commission, UNCITRAL. It was, however, essentially proposing a framework for the interoperability of national digital identity schemes without moving in the direction of a fully coordinated and integrated system.

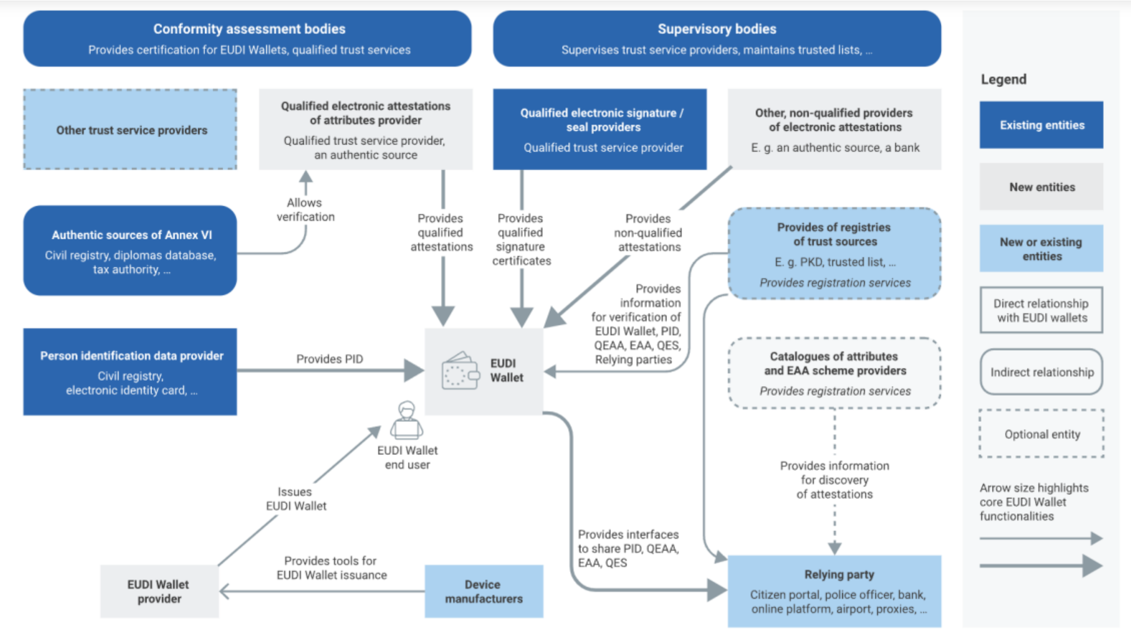
The process of developing a more integrated framework, which would go beyond pure cross-border interoperability, relied on cases of cooperation between Member States. For example, in the case of Estonia's digital identity scheme (eID), the country adopted the initial technical part from Finland and the legal part from Germany. Later, Finland used parts of the secure data exchange developed in Estonia (World Economic Forum). Today, Estonia actively cooperates with Ukraine in digitalisation towards public participation, and in 2023 launched its pilot version of mRiik, an app largely inspired by the Ukrainian Diia.

In 2021, the European Commission proposed revising eIDAS with the idea that every user should have full control of their digital identity. The European Commission and Parliament largely endorsed the proposal all the way to its adoption in March 2024, strengthening some of its user-centric aspects to protect users' rights. The revised eIDAS 2.0 entered into force on 20 May 2024. A key aspect of the new framework is its extension to the private sector, which significantly broadens its reach and prospective impact. The new EUDI Wallet will feature a dashboard of all transactions accessible to its holder both online and offline, offer the possibility of reporting possible violations of data protection, and allow interaction between wallets. Moreover, citizens will be able to onboard the wallet with existing national eID schemes and benefit from free e-signatures for non-professional use.

Based on the new EUDI Wallet framework, by 2026, each Member State must make a digital identity wallet available to its citizens and accept EUDI Wallets from other Member

States. Issuance, use, and revocation will be free of charge for all natural persons. Furthermore, Member States will also be required to provide free-of-charge validation mechanisms to verify the authenticity and validity of the wallet and of the relying parties' identity. Importantly, the application software components will be open source, but Member States are granted leeway so that, for justified reasons, specific components other than those installed on user devices need not be disclosed.

Figure 6 – European Digital Identity architecture and reference framework


Conformity assessment bodies
Provides certification for EUDI Wallets, qualified trust services
Supervisory bodies
Supervises trust service providers, maintains trusted lists, ...
Legend
Other trust service providers
Qualified electronic attestations of attributes provider
Qualified trust service provider, an authentic source
Qualified electronic signature / seal providers
Qualified trust service provider
Other, non-qualified providers of electronic attestations
E. g. an authentic source, a bank
Existing entities
New entities
New or existing entities
Direct relationship with EUDI wallets
Indirect relationship
Optional entity
Arrow size highlights core EUDI Wallet functionalities
Allows verification
Provides qualified attestations
Provides qualified signature certificates
Provides non-qualified attestations
Authentic sources of Annex VI
Civil registry, diplomas database, tax authority, ...
Provides of registries of trust sources
E. g. PKD, trusted list, ...
Provides registration services
Provides information for verification of EUDI Wallet, PID, QEAA, EAA, QES, Relying parties
Person identification data provider
Civil registry, electronic identity card, ...
Provides PID
EUDI Wallet
Catalogues of attributes and EAA scheme providers
Provides registration services
EUDI Wallet end user
Issues EUDI Wallet
Provides information for discovery of attestations
Provides interfaces to share PID, QEAA, EAA, QES
Provides tools for EUDI Wallet issuance
EUDI Wallet provider
Device manufacturers
Relying party
Citizen portal, police officer, bank, online platform, airport, proxies, ...

Source: European Commission.

The European Commission recently published a technical architecture reference framework (ARF) and a toolbox for the EUDI Wallet, specifying, among others, the role of intermediaries and key actors in the ecosystem, as well as the main protocols and conditions for the ecosystem to fully function. Importantly, the EUDI Wallet will not involve any centralised data storage as a condition to give end users full control of their data. However, ARFs are not specifications, and the specifics of their implementation are left open to interpretation – so they must be supplemented with detailed technical standards to ensure clarity and interoperability.

On top of that, the development of open-source libraries can support the creation of digital identity wallets by offering the required tools and guidelines. The Open Wallet Foundation is a good example of an initiative that aims to establish the best practices for digital wallet technology using standards-based open-source components. The Commission will provide a prototype of the EUDI Wallet that conforms to the requirements of the regulation. The prototype has been procured under the Digital Europe Programme, including code libraries and a sample application.

To ensure EUDI Wallet's proper implementation, since April 2023, four Large-Scale Pilot projects have been underway to test the wallet in a number of everyday use cases before deploying it in Member States. They are testing the technical specifications for the common Toolbox that will be the base of EUDI Wallets. These pilots involve approximately 360 entities, including private companies and public authorities from 26 Member States, Norway, Iceland, and Ukraine. These projects (described in Table 12) are scheduled to continue throughout 2025.

Table 12 – Consortia currently piloting the EUDI Wallet

Name	Description
Potential for European Digital Identity	The project tests six pilots aimed at being suitable to work with a digital ID: (i) eGov Services, (ii) SIM Card Registration, (iii) Mobile Driving Licence, (iv) Qualified eSignature, (v) ePrescription, and (vi) Bank Account Opening. It is the largest of the pilots involving over 50 public entities and over 80 private organisations. 'POTENTIAL aims to foster innovation, collaboration and growth in six digital identity sectors — governmental services, banking, telecommunications, mobile driving licences, electronic signatures, and health.'
EU Digital Wallet Consortium (EWC)	'The EWC is a joint effort to successfully leverage the benefits of the proposed EU digital identity in the form of Digital Travel Credentials across the Member States. The EWC intends to build on the reference wallet application to enable a use case focused on Digital Travel Credentials.' By using travel as an example, the EWC demonstrates how eIDAS will revolutionise many other e-commerce use cases, capturing the imagination of citizens, businesses and governments. The EWC will create two common building blocks that will support the travel use case. The first is payments and the second is organisational digital identity.
Digital Credentials for Europe (DC4EU)	The project's main objective is testing interoperability and scalability in the national domain and multiple cross-border contexts. The process will allow for comprehensive wallet testing using qualified electronic attestations of attributes, electronic attestations of attributes and credentials, and their national and cross-border functionalities in a pre-production environment and correspondent use cases.

	DC4EU will focus on identifying and applying all these aspects in the education field, focusing on the issuance of educational credentials and professional qualifications, and in the social security field by engaging in the execution of the Portable Document A1 and the European Health Insurance Card. 'DC4EU provides tangible support to the public and private sectors in the educational and social security sectors by deploying and accessing state-of-the-art trans-European interoperable digital service infrastructures and their integration in a cross-border trust framework.'
Nordic-Baltic eID (NOBID) Consortium	NOBID is a set of Nordic and Baltic countries that, together with Italy and Germany, will pilot use of the EUDI Wallet for the authorisation of payments for products and services by the wallet user. NOBID addresses two issues in particular: (i) online users should be able to utilize an eID from their home country to identify also for digital services in other countries; and (ii) there should be access to civil registration numbers for citizens of the other countries when appropriate for provision of digital cross-border service.

Source: Authors' own elaboration

The implementation of the EUDI Wallet promises very significant benefits and is likely to become a cornerstone of the future EU DPI. This is because of the conflation of public and private services in a user-centric federated environment maintained by a properly defined reference architecture. The prevalence of open-source solutions can also speed up the reuse of modules across countries, thus leading to the gradual integration of national e-ID systems into a coherent framework. Experts have listed possible benefits by referring to better cross-border transactions, better business conditions, and faster and easier access to services in any Member State.

At the same time, there is a concern that the high security standards mandated by the EU could make the digital wallet cumbersome, deterring widespread use. This, coupled with the limited level of trust in digital systems observed in some Member States, where people fear for their privacy, may jeopardise the success of the initiative in the coming years[8]. Ultimately, the success of the EUDI Wallet will depend on its ability to balance security, user experience, and practical implementation.

In summary, while the EUDI Wallet initiative holds promise for enhancing European integration and digital sovereignty, its success hinges on overcoming multifaceted challenges. These include technical interoperability, regional fragmentation, regulatory alignment, user acceptance, and privacy protection. If effectively implemented, the EUDI Wallet could catalyse a profound transformation, offering citizens and businesses a seamless, secure, and efficient means to engage with services within their countries and across borders.

5.3. Data governance and data spaces

Another very important layer of the DPI relates to data governance and exchange. Absent a well-developed set of interoperability protocols, sharing rules, and practices for data, the potential of open standards and digital identity/wallet layers to deliver value-added services to citizens and businesses is inevitably compromised. Over the past decades, the lack of an articulate framework for data governance has led the EU to gradually surrender to the superior ability of US-based technology giants to develop cloud-based business models, eventually capturing over 90 % of the data originated by Europeans. This came with privatised governance, often obscure patterns of data reuse, and an overall lack of collaborative pooling of data for the development of public services.

The von der Leyen Commission tried to shift gear by proposing an ambitious data strategy in February 2020. The strategy would couple legislative intervention (particularly the Data Governance Act and the Data Act, on which see Section 5.4) with the creation of cross-cutting and sectoral data spaces, alongside the launch of a European federated cloud initiative. The overarching goal was to enable more collaborative and inclusive management of data for specific purposes, as well as to empower sectoral players vis-à-vis larger conglomerate technology corporations. In fact, during the COVID-19 pandemic, the development of the EU Digital COVID Certificate (EUDCC) became a game changer in data exchange (Gambardella and Zagari 2024).

[8] Recent research by Visa from the last year demonstrated that while mobile wallet penetration and usage differs by country, a majority of Europeans (72 %) actively engage with mobile wallets, indicating their widespread adoption. Among Norwegian consumers, 94 % actively use mobile wallets, marking the highest market penetration. By contrast, 54 % of German consumers still actively use cash, the highest among surveyed markets. Additionally, only 39 % of Italians indicated they planned to use mobile wallets for all purchases next year. uk-visa-mobile-wallets-paper-nov-2023-final.pdf

Box 2 – The EU Digital COVID Certificate: a game changer for the data exchange layer

The pandemic underscored the critical role of digital communications, prompting unprecedented collaboration among European states to create tools like national contact tracing apps and the EUDCC, launched in February 2021. The EUDCC allowed travellers to move freely across the EU and EEA countries without quarantine, while also being compatible with systems in 51 third countries. By enabling countries to verify travellers' health status, it minimised risks during reopening and established a regional framework for safe mobility. Although the EUDCC Regulation expired in 2023, the European Commission and World Health Organization have partnered to build on its success by developing a global digital health credential to facilitate mobility during future public health crises.

Beyond enabling safe movement, the EUDCC laid the foundation for an interoperable European framework and a universal digital identity model, allowing people to access public services across the EU. The pandemic also highlighted the need for advanced digital infrastructures to support essential services like vaccine distribution, social assistance, identity management, medical data sharing, and payments, which will continue to provide long-term societal benefits.

In essence, the common European Data Spaces and the DPI are complementary elements of the EU's digital strategy. DPI provides the necessary digital architecture upon which data spaces are built and operated, ensuring that data can be shared and utilised efficiently, securely, and in a manner that respects individual rights and freedoms. Common European Data Spaces are currently being developed across 14 sectors. These include energy, finance, health, and mobility, among others. All European Data Spaces use the same data infrastructures and governance frameworks, which facilitate data pooling, access, and sharing. In addition, the common European Data Spaces feature:

- open participation for all organisations and individuals;
- a secure and privacy-preserving infrastructure to pool, access, share, process, and use data;
- a clear and practical structure for accessing and using data – common European Data Spaces have fair, transparent, proportionate, and non-discriminatory access rules, due to well-defined and trustworthy data governance mechanisms;
- respect for EU rules and values, especially personal data, consumer protection, and competition law;
- the ability of data holders to grant access to or share certain personal or non-personal data;

- the option for data holders to make their data available for reuse for free or against compensation.

Still, the implementation of the 14 data spaces has proceeded more slowly than expected. The first attempt was adoption of the proposal for a regulation on the European Health Data Space, which faced several obstacles during the debate in the European Parliament, where the original idea of moving towards an opt-out system for the collection of individual health data was heavily questioned. Eventually, a political agreement was reached in March 2024 with reinforced provisions to safeguard the privacy of natural persons. The difficulties encountered during this process raise concerns about the viability of swiftly adopting similar data spaces for cross-cutting purposes (such as skills or public administration) and for the other 13 sectors.

Most importantly, there still seems to be limited availability of a common framework for governing a data space: some sectors (e.g. automotive, with Catena-X) have so far moved towards a data space that is fully privately governed, whereas others (health and tourism) are essentially large-scale public–private partnerships. Even in the latter case, the role of intermediaries and the degree of institutionalisation still appear to be undefined. The relationship between the data spaces and the rest of the DPI seems rather obscure at the moment and deserves further clarification. Moreover, the management of data spaces would benefit from the promotion of data stewardship skills and competences, but this area of policy continues to be in its infancy, despite repeated calls by scholars.

Finally, the relationships among the different data spaces and their integration under the common umbrella of a federated cloud architecture are still a work in progress, despite expectations that results would be reached during the five years of the first von der Leyen Commission. That said, one would expect the new European Commission, which started its work at the end of 2024, to take action to speed up the development of data spaces for their integration into a pan-European DPI. Absent this step, it is highly unlikely that European citizens will ever reap the full benefits of the EUDI Wallet.

5.4. The federated cloud architecture: a dead end or a concrete plan?

Similar to the case of data spaces, the plan for a federated European cloud architecture has proceeded much more slowly than originally envisaged. The Franco-German project Gaia-X was supposed to offer a blueprint for such an architecture, yet its implementation is proceeding in a rather cumbersome and patchy way. Launched in 2019, Gaia-X is 'an initiative that develops, based on European values, a digital governance that can be applied to any existing cloud/edge technology stack to obtain transparency, controllability, portability and interoperability across data and services'.

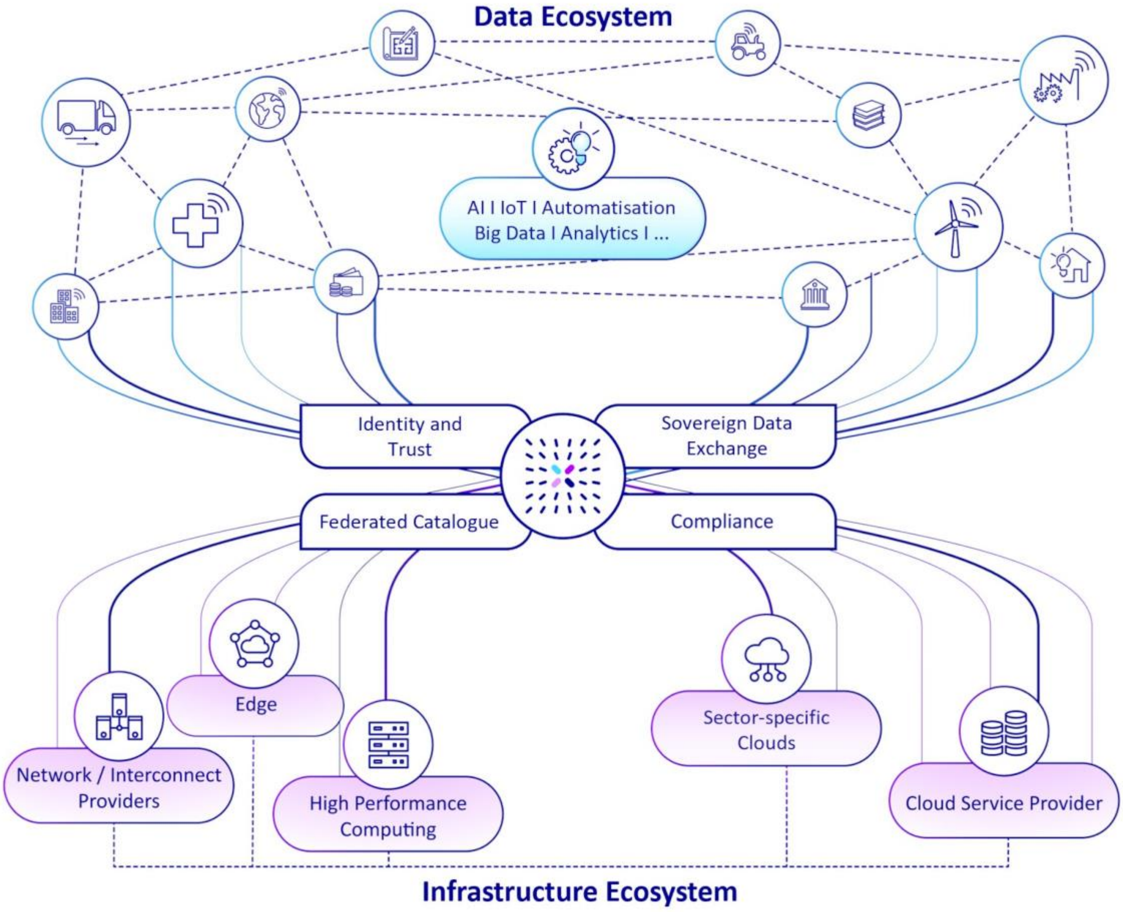
Gaia-X primarily targets companies seeking to share and create value from their data while leveraging a 'common framework for access and transport protocols, services and policies' that has been built with respect for European regulations and values. The emphasis of Gaia-X is on transparency, data security, privacy, interoperability, and scalability. The project does not aim for a new cloud infrastructure but rather seeks to create a 'federated' form of European data infrastructure which facilitates sharing and accessing data. Key principles in Gaia-X are self-sovereignty, interoperability, and decentralisation. The consortium has a vision in which data remain under the control of the businesses and people generating them, and interoperability and trustless or trust-enhancing solutions allow for a competitive and flourishing service ecosystem.

Gaia-X consists of an association and a decentralised structure with 21 hubs. The association is the non-profit arm of Gaia-X, established in Belgium in 2020 to develop the overarching strategic direction of the project at the European level. Hubs are 'the central contact points for interested parties in each country' and serve as 'think tanks' and 'grass root supporters' for the overall project. Currently, there are Gaia-X hubs in 21 cities in Europe, North America, and Asia. For those hubs in the EU, one of the objectives is to collaborate to create pan-European data spaces where possible.

Since its launch, the Gaia-X project has been the subject of political attention. The project responds in part to growing European concerns about the dominance of large US technology companies in the cloud sector. This reliance on foreign companies, whose treatment of commercial and personal data does not necessarily fall in line with European regulations and values, spurred the development of this 'sovereign cloud'. However, non-European firms such as Microsoft, Google, and Huawei have been incorporated into the cloud alliance, which calls into question whether these entities have watered down existing projects. One area of recurring concern is the US CLOUD Act, which permits the US government to request data stored by US communications service providers located in foreign jurisdictions and raises concerns over the extraterritorial application of US law in the EU.

At the time of writing, several lighthouse data spaces and projects are active within Gaia-X, including Agdatahub for agriculture, Catena-X for the automotive sector, OMEGA-X for energy, and many more. The Gaia-X infrastructure ecosystem is in principle dependent on a technology stack that includes sovereign data exchanges and an integrated identity and trust-enhancing layer of solutions.

Figure 7 – Gaia-X infrastructure and data ecosystem



Source: Gaia-X Germany.

5.5. HOW OTHER EU DIGITAL LEGISLATION FACILITATES THE EMERGENCE OF DPI

Some of the most remarkable efforts by the von der Leyen Commission towards the creation of a more pluralistic, decentralised, and self-sovereign digital ecosystem can be found in several legislative initiatives launched over the past few years. Without going into fine detail, it bears recalling that the future European DPI will significantly depend on the successful implementation of several new pieces of legislation – including most notably the Data Act, the Data Governance Act, the Digital Markets Act and the Interoperable Europe Act.

More specifically, the Data Act seeks to improve and clarify the environment for data sharing in the EU, with emphasis on the fairness of B2B data sharing and the conditions for government access to privately held data (B2G data sharing). On the former, the Data Act introduces a key principle: no device should be placed on the market under the assumption that the data collected will be managed by the device producer. In other words, users should be empowered to unbundle data from the device and choose a third-party public or private data intermediary. The same principle is found in the Digital Markets Act for specific large-scale players known as 'gatekeepers', where all core platform services (including e-identity and app stores) can be unbundled to allow end users to choose competing public or private offers.

Yet, these provisions will remain only theoretical possibilities if a flourishing market for alternative providers does not emerge. This is where the Data Governance Act becomes relevant, as it is essentially aimed at creating the preconditions for data intermediaries to emerge. The concrete implementation of this piece of legislation is still surrounded by a veil of uncertainty, since the new intermediaries are heavily regulated in the Data Governance Act, a feature that may discourage many players from investing in this new role.

The Data Act also contains provisions on B2G data sharing, as mentioned. This promises to become an especially important area for governments willing to collect data to develop services of general interest, thereby leveraging DPI to its fullest potential. Even so, the conditions for governments to access such data (also called fair, reasonable, and non-discriminatory conditions, or FRAND), as well as the obligations of the private sector regarding the format and interoperability of the data, are still to be fully developed, and this generates uncertainty in the market.

Finally, the Interoperable Europe Act entered into force on 11 April 2024. As mentioned in Section 5.1, this provision capitalises on previous efforts in the context of the European Interoperability Framework, possibly taking public services interoperability and user-centricity to a new level.

CONCLUSION: A DECALOGUE TO BUILD A FULL-SCALE EUROPEAN DPI

Europe needs a well-functioning, deeply embedded, seamlessly interoperable, open digital public infrastructure to realise its ambition within and beyond the digital realm. Such an achievement would promote efficiency in citizen–government interactions. It would boost competitiveness by cutting red tape for businesses dealing with administrations within and across borders, as advocated by the Draghi report, among others. Transaction costs would fall through fee-free instant payments, while bringing the informal economy to the surface. It would also help Europe build resilience and technological sovereignty, which are key goals of the current legislative bodies, as clearly mentioned in Executive Vice-President Henna Virkkunen's Mission Letter (Gambardella and Zagari 2024).

Thus, in this report we have shown that the effects of a European DPI would be huge, but the challenges are equally daunting, as outlined below.

- **The landscape of DPIs around the world is evolving in a way that is not fully in line with Europe's ambitions** in terms of openness, trustworthiness, and privacy preservation. This means that the world itself would benefit from a DPI based on European values. At the moment, as discussed in Section 3, emerging options are far from self-sovereign, but rather converge towards offering proprietary, off-the-shelf solutions, or are so complex that they require reliance on system integrators.

- **Within Europe, approaches to the DPI vary significantly**, with marked divergence in terms of scope, commitment to open-source software, approaches to data storage and collection, security, and uptake.

- **Over the past 10 years, the European Commission has struggled to build sufficient consensus around the DPI in Member States**. It was initially forced to rely on purely voluntary frameworks (ISA2) and then started to gradually build bridges between completely independent national frameworks (as in the case of eIDAS). Key initiatives on payments, such as the Second Payment Services Directive, ended up failing due to the fragmentation of APIs at the national level. The attempt to give birth to data spaces has been frustrated by significant resistance to an opt-out regime for relevant personal data.

- **Recent initiatives** such as the EUDI Wallet, the Interoperable Europe Act, the ComPAct programme, and the data strategy have the potential to ramp up Europe's progress on the DPI. Yet, they also depend on the successful implementation of legislative provisions such as the Data Act, Data Governance Act, and Digital Markets Act (among others); the further shaping of Gaia-X and data spaces into a coherent canvas; and the translation of the current EUDI Wallet pilots into a seamlessly interoperable framework and architecture for digital identity and public–private service provision.

Against this background, many obstacles appear to stand in the way of achieving a fully fledged DPI. They can be overcome if the European Commission targets a number of reforms, such as the following ones.

1. **Facilitate a concrete, multistakeholder standardisation effort** to create more legal certainty on data quality and management, and to define the standards that will shape data flows, digital identity and wallets, and full data interoperability in the years to come. Beyond technical interoperability, semantic interoperability is essential to ensure that the data exchanged between systems are understood in the same way by all parties. This requires the development of common data models, ontologies, and vocabularies that enable seamless communication and understanding across different systems, sectors, and Member States.

2. **Launch a specific initiative on data stewardship** aimed at fostering the needed skills and competences for collecting, storing, reusing, and protecting data as it flows among stakeholders and leverages service provision in the territory of the EU. Alongside this initiative, it would be important to promote actions aimed at establishing a 'social licence' for the privacy-preserving circulation of data within the single market, also given the review of the GDPR (Verhulst et al. 2023).

3. **Reiterate Europe's commitment to secure, user-centric, open-source solutions**. As already mentioned, commitment to open source is uneven across Member States. The need for enhanced security of open-source solutions is triggering important changes in the community of developers, away from unmanaged products and towards secure, containerised applications.

4. **Consolidate and upgrade the European federated cloud.** Gaia-X has progressed too slowly yet has given life to a myriad of initiatives that need to be brought into a coherent framework, oriented towards European values and policy goals – not least those nested in the Digital Decade communication.

5. **Speed up the implementation of key EU legislation,** including the Data Act, Data Governance Act, and Data Spaces, to ensure the emergence of intermediaries and regulatory certainty on data exchanges.

6. **Invest in the integration of DPI solutions with established private platforms**, including through the embedding of 'secure elements' in existing hardware–software platforms. For example, Apple recently announced that any third-party wallet will be able to build on its Near Field Communication and Secure Element architecture. Storing private

keys in the embedded components of hardware can lead to a much more user-friendly development of DPI solutions. It will also be key for the Digital Euro, as access to the Secure Elements is critical for mobile device-based offline payments.

7. **Move from asynchronous to allowing synchronous payment solutions as well.** As it stands, given the complexity of achieving interoperability between various national systems that differ in degrees of openness, API specifications, and protocols for authentication, the EUDI Wallet can at best aim at achieving asynchronous transactions. This is despite the fact that the EU model for data exchange layers supports both asynchronous and synchronous communication. Enabling real-time operations would be crucial for services like eID validation or eHealth.

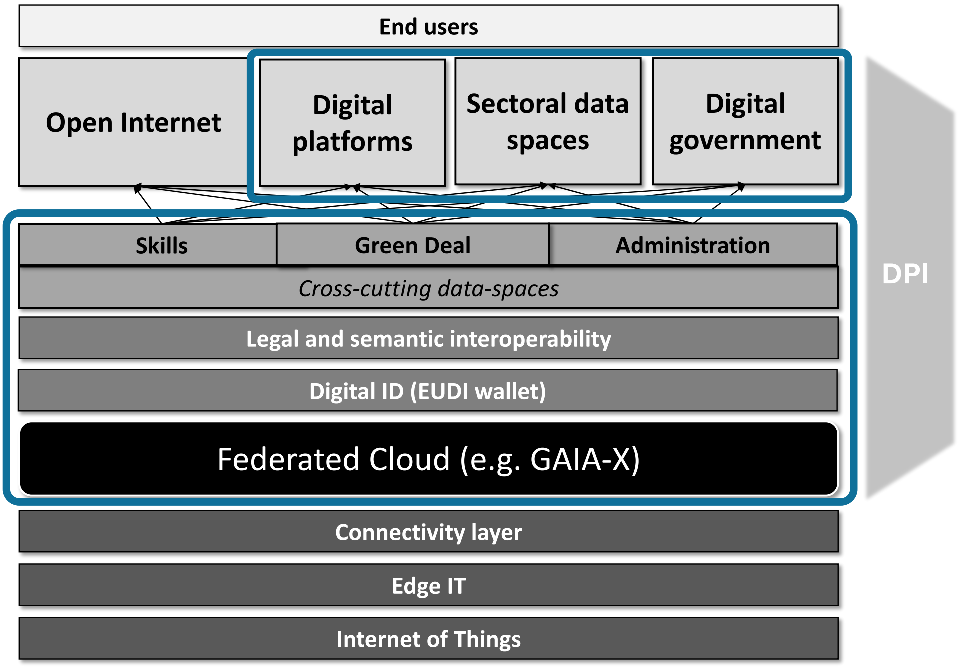
8. **Embed the DPI in Europe's global digital offer**. The deployment of a European DPI would be a perfect way to project Europe's approach to digital markets around the world and offer self-sovereign solutions to partner countries, for example, as part of the Global Gateway (see Renda et al. 2023). An investment in the European DPI would therefore also become an investment in Europe's 'actorness' in the global governance of digital technologies, as well as in the future of digitally enabled democracy and public services. This compelling vision requires further stewardship and investment by the Commission yet promises far-reaching returns and rewards for the EU, its society, and businesses.

9. **Launch an ambitious investment plan for the whole EuroStack**. This means testing the interplay of digital identity and the wallet, data governance and intermediaries, self-sovereignty, and data space interoperability across a multitude of layers in the technology stack (see Figure 8). It also means going further and tackling all the dependencies in critical layers that threaten Europe's present and future technological sovereignty. The reason is simple: the DPI is certainly an essential, but not sufficient, condition for recovering digital sovereignty. Even when national DPIs are well developed, as in the case of X-road, Suomi, or pagoPA, they often have to rely on traditional commercial cloud providers – a market dominated by less than a fistful of non-European companies – and they lack sufficient applications, which leading commercial offers can provide.

   That is why authors have advocated the setup of a European DPI fund (Keller 2023; Siewicz 2023) or have gone beyond this by proposing investment in a broader EuroStack, which includes compute, cloud, and federated AI solutions (Bria et al.). Or they have even proposed the launch of a moonshot on AI with the objective of developing, inter alia, trustworthy, open-source, user-centric AI-driven public services (Renda 2024). The EuroStack must be designed with long-term financial viability in mind. This includes the creation of funding mechanisms to support its development, maintenance, and evolution over time.

10. **Enable a third-party market for complementary services on the DPI.** A DPI should be designed as an open ecosystem that allows third-party providers to build and offer complementary services. This would foster innovation, competition, and diversity in the services available to society and businesses. For example, third-party developers could create specialised applications for eHealth, education, or local government services that integrate seamlessly with the DPI. Clear rules and standards for third-party participation would be necessary to ensure security, privacy, and interoperability while encouraging a vibrant market for value-added services.

Figure 8 – The European DPI in the new digital technology stack



Source: Authors' elaboration

This, after all, is the real challenge and opportunity for the new European Commission. Realising what is at stake, the 'size of the prize', as well as the extent of the challenge, can lead EU policymakers to take actions with the necessary sense of urgency. A push is needed for pragmatic solutions without compromising on EU standards for the DPI, which lays the foundations for a more European approach to several layers of the emerging tech stack. A flourishing DPI requires a well-developed EuroStack, and this future EuroStack will have to rely on a European DPI.

CEPS
PLACE DU CONGRES 1
B-1000 BRUSSELS