VOLUME 6 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

DIGITAL PUBLIC INFRASTRUCTURE AND THE CONSTITUTIONAL STATE: A COMPARATIVE ANALYSIS OF INDIA AND ESTONIA

- Anushka Vasishth[1]

A. ABSTRACT

This article aims to assess how Digital Public Infrastructure (DPI) impacts the efficiency of the state while balancing the protection of individual rights, by examining the contrasting models of India and Estonia. On one hand there is Aadhaar which represents a very centralised approach and does welfare delivery using a single biometric database, whereas on the other end there is Estonia's X-Road framework which demonstrates a decentralised system which is based on interoperability, user control, and minimal data. At the core of the study lies the exploration of the digital architectural choices and how they influence fundamental rights like privacy and dignity. The hypothesis advanced is that *while India's centralised digital architecture has expanded the administration, it has an increased risk of exclusion and surveillance, whereas Estonia's decentralised design represents that technological efficiency can coexist with privacy protections.*

B. INTRODUCTION

What is Digital Public Infrastructure?

Digital Public Infrastructure (DPI) is a network of interoperable digital systems that provide tools for various foundational purposes such as, creating digital identities, making electronic payments, and securing data exchange, for government as well as private service delivery. All of such systems are viewed as highly essential components of modern governance because they enable financial inclusion, efficient welfare distribution, and enhance overall state capacity. Institutions like the G20 have recognised DPI as a key

[1]PGIP-LLM In Insolvency, National Law University, Delhi & Advocate enrolled with the Bar Council of Delhi.

driver of digital transformation, also pointing out the need to operate within a system that protects human rights and ensures public trust.[2]

Objectives of this Article

The objective is to undertake a comparative public law analysis of DPI models of two countries that diverge sharply in their technical design: India's Aadhaar and Estonia's e-ID system supported by their X-Road platform. And the purpose is to evaluate how the system of the two countries affects the questions of accountability, privacy, and inclusion.

Core Challenge

The fundamental question lies at the heart of digital governance, i.e., *can the state pursue administrative efficiency without compromising constitutional rights?* And in order to answer the same, this study applies comparative public law methods by focusing on the response of each country's constitutional and regulatory frameworks towards the risk of these technological designs.

C. INDIA: CENTRALISED EFFICIENCY AND CONSTITUTIONAL CONFLICT

Scope of the Aadhaar System

Aadhaar is India's flagship national identification project which was launched in 2009 and was designed to assign a unique 12-digit number to every resident which would be linked to their biometric and demographic data. This program is managed by the Unique Identification Authority of India (UIDAI)[3], and was adopted in order to be able to authenticate and streamline welfare delivery and also to prevent leakages in the said welfare distribution. The process to enrol for this program involves the collection of fingerprints, retina scans, and facial photos. More than 1.4 billion people are enrolled in this program, making it the world's largest biometric ID system.[4]The single, centralised database for Aadhar is called the Central Identities Data Repository (CIDR), and it stores all the biometric and demographic data in one place. The goal of such a centralised

[2]G20 India Presidency, *G20 Framework for Systems of Digital Public Infrastructure* (Aug. 2023), https://g7g20-documents.org/fileadmin/G7G20_documents/2023/G20/India/Sherpa-Track/Digital%20Economy%20Ministers/2%20Ministers%27%20Annex/G20_Digital%20Economy%20Ministers%20Meeting_Annex1_19082023.pdf.
[3]Unique Identification Authority of India (UIDAI), *About UIDAI*, https://uidai.gov.in/en/.
[4]Unique Identification Authority of India (UIDAI), *Aadhaar Dashboard*,https://uidai.gov.in/aadhaar_dashboard/india.php.

system was efficiency and inclusion, however this centralisation has instead raised questions regarding data security, surveillance, and autonomy of the individual. This choice of design does prioritise administrative scale over distributed control, but also ends up creating a concern with regards to privacy.

Data Privacy and Security Vulnerabilities

A centralisation of data is a risk to privacy and cybersecurity, which can be well understood by the fact that Aadhaar's database can potentially correlate multiple transactions by using a common unique identifier across contexts, enabling the creation of detailed behavioural profiles. In practice also, the record of Aadhar's safety has been patchy, several government portals have inadvertently published citizen's personal data, revealing their names, addresses, and Aadhaar numbers. One investigation revealed that nearly 200 government websites had displayed Aadhar information publicly, while unauthorised access of those websites had also come to light.[5]

A major example of this security gap in India's DPI was the CoWIN data breach back in 2023, in which, sensitive vaccination and identification details were exposed on platforms like Telegram.[6] Even apart from such breaches, other concerns that have emerged out of the potential use of Aadhaar data include surveillance driven by Artificial Intelligence (AI). With AI applications being expanded in law enforcement, there is an increased possibility of linking biometric data to predictive policing or facial recognition tools, which has been criticised as undermining democratic accountability. [7]

Exclusion and Right Based Challenges

One of the most serious problems that can be caused because of Aadhaar is exclusion, i.e., the denial of welfare benefits that will be caused as a result of authentication failures like biometric mismatches, connectivity issues, or other technical problems, which can prevent people from getting food rations or other social advantages. Evidences show that such failures have gone up to 12% in the Public Distribution System (PDS), eventually

[5]Jackson School of International Studies, University of Washington, *The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment*, https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/#_ftn11.
[6]The Legal School, *CoWIN Data Breach: A Wake-Up Call for India's Digital Infrastructure*, https://thelegalschool.in/blog/cowin-data-breach.
[7]Jackson School of Int'l Studies, *The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment*, supra note 4.

affecting the elderly, the poor, manual labourers and others whose fingerprints are often worn because of the nature of activities they perform.[8] Such exclusion hits right at the heart of the constitutional right to dignity. Welfare becomes excessively dependent upon technology when access to entitlements depends on algorithms rather than the discretion of a human.

Judicial Scrutiny: The Puttaswamy Judgement

The legislative foundation of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, itself was controversial procedurally, why? Because the Act[9] was passed as a Money Bill which appeared as a manoeuvre to allow the Lok Sabha to pass it, without being constrained by the recommendations of the Rajya Sabha. And it was being argued that it did not qualify to be a Money Bill in the first place because of there being no relation to government taxation or expenditure, and hence, it bypassed the necessary comprehensive legislative scrutiny required for such a foundational identity system. Therefore, it led to increasing concern with regard to prioritisation of rapid statutory implementation over deliberation on the impact on fundamental rights.

The case of Justice K.S. Puttaswamy (Retd.) v. Union of India[10] in 2018 proved to be a turning point for the legality of Aadhaar. In this case, the Hon'ble Supreme Court upheld the constitutionality of the Aadhaar Act, 2016[11] but limited its scope through a four-prong proportionality test (legality, legitimate state aim, proportionality, procedural guarantees). The legitimacy of Aadhaar was accepted by the court specifically for schemes financed by the Consolidated Fund of India, but was struck down for its mandatory use for private contracts and "earned benefits" like pension and insurance. Section 57 of the Aadhaar Act[12] had permitted private entities to demand Aadhaar authentication, and this was declared unconstitutional. The reasoning given by the Apex Court reflected two main deficiencies in India's DPI system:

[8]The Quint, *UIDAI CEO Admits Aadhaar Authentication Failure Rate up to 12%*, https://www.thequint.com/news/india/uidai-ceo-admits-aadhaar-authentication-failure-rate-12.
[9] Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
[10]K.S. Puttaswamy (Privacy-9J.) v. Union of India, (2017) 10 SCC 1.
[11]Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
[12]Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016, §57.

1. The government failed to show that mandatory biometric authentication was the "Least Reactive Measure" available to prevent fraud, and there were other alternatives like smart cards or offline ID verifications that were being widely used in states like Tamil Nadu and could have been adequately considered by the government.
2. Additionally, there was no "Balancing of Competing Interests", since exclusion and violations of rights weighed more than unverified claims of fiscal savings through benefit transfers.

Thus, this judgement validated the use of Aadhaar in a limited welfare context but also highlighted its constitutional fragility in private and commercial contexts.

Policy Implications and Continuing Risks

Reforms post the Puttaswamy Judgement[13] have been attempting to integrate the data protection principles, but still there is a lack of robust data protection regime that can be said to be rights oriented or could be considered equivalent to the European Union's General Data Protection Regulation (GDPR)[14]. However, the Digital Personal Data Protection Act, 2023[15] can be considered a significant step, but it gives wide exemptions to state entities, which raises concerns about potential misuse and limited judicial oversight.

Besides, the expansion of Aadhaar beyond welfare, such as SIM verification, linking bank accounts, and e-KYC for financial services shows a "functional creep", illustrating a welfare or identification system which eventually permeates into various aspects of life, acting as a functional overreach, which, if left unchecked, will transform Aadhaar into a pervasive tool of surveillance and not just a social inclusion mechanism which it was originally intended to be.

Analytical Reflection

India's experience demonstrates that a centralised DPI, although administratively convenient, increases the scale and risk of error or abuse of extremely sensitive data, since a single breach can compromise millions, and lead to a deprivation of rights. From the perspective of public law, the Aadhaar program reveals a stark dilemma, which is, that

[13] K.S. Puttaswamy (Privacy-9J.) v. Union of India, (2017) 10 SCC 1.
[14] GDPR, Regulation (EU) 2016/679.
[15] Digital Personal Data Protection Act, 2023.

the pursuit of administrative efficiency often collides with constitutional guarantees of dignity, privacy, and autonomy. While it cannot be disagreed that the Puttaswamy judgement[16] is a vital judicial intervention but it alone also would not be sufficient to safeguard the right of the citizens in the absence of a systemic regime which itself embeds privacy and accountability into the infrastructure.

D. ESTONIA: DECENTRALISATION AND INTEROPERABILITY

Estonia's digital Public Infrastructure

Estonia is known as the pioneer of digital governance because it transformed its administrative structure since the early 2000s through technology and in contrast to India, Estonia's DPI operates on a decentralised and interoperable framework which is designed to balance efficiency, transparency, and privacy, all at once. The e-ID system, which is a mandatory identity mechanism for citizens, lies at the heart of Estonia's digital state, as it functions as a legal identification tool, as well as a secure means of online authentication. Also, this e-ID can be accessed through various mediums, like, the physical card, Mobile-ID, and Smart-ID, and each being secured via advanced cryptographic systems employing Public Key Infrastructure (PKI). Such systems enable citizens to sign legally binding documents, access government services, everything completely online.

The guiding principle of the small European country of Estonia is that a citizen's digital identity should empower her, more than the state, and this philosophy, is reflected in the policy documents of the country, and its constitutional culture situates digitisation within the broader framework of human dignity and democratic participation.

Decentralised Data Management

X-Road[17] is a data exchange platform which connects hundreds of independent public and private databases through secured interfaces, and is considered the backbone of Estonia's DPI. This is system is very different from the India's Central Identities Data Repository (CIDR), which consolidates data in a central repository, unlike Estonia's architecture which distributes information across multiple databases which are in turn managed by different entities. Also, X-Road functions not just as a storage system, but also as a layer

[16]K.S. Puttaswamy (Privacy-9J.) v. Union of India, (2017) 10 SCC 1.
[17]e-Estonia, *X-Road: Secure Data Exchange Between Organisations*, https://e-estonia.com/solutions/interoperability-services/x-road/.

of communication, since it enables databases to exchange data in real time while at the same time, keeping the control of the information with the original holder. Besides, each transaction is digitally signed, encrypted, and logged, which ensures traceability and accountability of each transaction. The data is only collected once in this system and further different agencies reuse it securely rather than collecting it again and again, for instance, at the time of the birth of a child, the national population registry is automatically updated by the hospital records, and thereby trigger eligibility for social benefits. Such automation increases administrative efficiency manifold and gets rid of redundancy. Studies estimate that X-Road saves approximately more than 820 years of working time for the Estonian state and citizens annually.[18]This system has an open software which is maintained by the Nordic Institute for Interoperability Solutions (NIIS)[19]and ensures transparency and more importantly international replicability, therefore, it aligns digital governance with the rule of law and public accountability.

Privacy and Cybersecurity

Privacy by design is the central commitment to the resilience of DPIin Estonia, which can be witnessed by the fact that all of the X-Road data exchanges are encrypted and digitally signed, which prevents unauthorised access and tampering of data. Additionally, Estonia also integrates blockchain based solutions through the Keyless Signature Infrastructure (KSI), which timestamps and secures data transactions without revealing their content.[20] The design of such framework limits overreach of the state, by storing data in different databases, where the citizens themselves can view who and when accessed their data, hence reinforcing a culture of trust and transparency. “Data Embassies” have been established by Estonia, which are backup servers hosted abroad, notably in Luxembourg, to ensure continuity and resilience, and to safeguard national data against potential cyberattacks.[21]

It can be agreed that the Estonian DPI system is robust, but it can also not be denied that it is not completely immune to challenges, as was seen in 2017, when security

[18]e-Estonia, *How Estonia Saves Annually 820 Years of Work*, https://e-estonia.com/how-save-annually-820-years-of-work/.
[19]Nordic Institute for Interoperability Solutions (NIIS), *About NIIS*, https://www.niis.org/.
[20]e-Estonia, *KSI Blockchain: Ensuring the Integrity of Data and Systems*, https://e-estonia.com/solutions/cyber-security/ksi-blockchain/.
[21]e-Estonia, *Data Embassy: Ensuring Digital Continuity Beyond Borders*, https://e-estonia.com/solutions/e-governance/data-embassy/.

vulnerabilities were discovered in approximately 7,50,000 ID card chips that were supplied by a private contractor.[22] Although no breach of data had taken place, but still the incident highlighted the risks that are associated with technological outsourcing and called for Estonia to strengthen its certification and auditing processes.

Legal and Institutional Frameworks

Estonia's DPI functions under a well-defined legal and regulatory regime which integrates both national and EU law. There is an Identity Documents Act, 1999[23] which provides the domestic framework and makes the e-ID mandatory for all the Estonian residents aged 15 and above, and has also designated an issuing authority, called the Police and Border Guard Board (PBGB)[24]. The national law is also complemented by the broader European regulatory framework:

- eIDAS Regulation, 2014[25]- it establishes mutual recognition of electronic identities and signatures across the EU, which is a standard that was shaped with the help of Estonia, additionally, the regulation assigned a "high" assurance level to Estonia's e-ID and Smart-ID.
- The General Data Protection Regulation (GDPR)[26]- Estonia implemented this regulation through its Personal Data Protection Act[27], which enforces strict principles of data minimisation, consent, and purpose limitation, in order to ensure that the processing of data by the public bodies remains lawful as well as proportionate.

Such double layered regime demonstrates a legislative model which is proactive and, where the technological design evolves within legal boundaries that are predetermined, contrasting India's reactive, litigation driven approach. Estonia has embedded rights based norms, from the outset, into its system's architecture, as a result many conflicts are prevented that India's judiciary later had to resolve.

[22]*Postimees, Cyber Lollygagging Cost the State Millions*, https://news.postimees.ee/6383968/cyber-lollygagging-cost-the-state-millions.
[23]Identity Documents Act, RT I 1999, 25, 365.
[24]Police and Border Guard Board (PPA), Republic of Estonia, *About the Police and Border Guard Board*, https://www.politsei.ee/en.
[25]Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, 2014.
[26]GDPR, Regulation (EU) 2016/679.
[27]Personal Data Protection Act, RT I, 26.06.2019, 32 (Est.).

Efficiency, Adoption, and Trust

Estonia's DPI has been able to achieve great adoption and public trust, as data reveals that close to 98% of residents have an e-ID, and more than 90% are regular users of the digital services like e-voting, filing of tax, and management of prescription.[28] The digital signature, which is considered to be a legal equivalent to a handwritten signature, has now become a part of daily routine of the citizens and saves them five working days annually.[29] Estonia sustains public trust because of such transparency, security safeguards, and a narrative that is completely rights based and treats digital participation as an extension of citizenship rather than an obligation by the state. Contrary to India's experience of pushing mandatory enrolment despite repeated data breach, Estonia's system fosters trust.

Analytical Reflection

The DPI of Estonia presents a public law model that is grounded in technological humility, which recognises that digitisation must not become a weapon of domination but remain an instrument of governance, because ultimately, its success comes from treating privacy, autonomy, and efficiency as co-dependent principles and not as competing goals. Estonia also minimises the potential for misuse and abuse of data by decentralising it and building transparency across mechanisms while maintaining administrative agility at the same time.

E. COMPARATIVE PUBLIC LAW ANALYSIS

Centralisation v. Decentralisation

The DPI of India has a centralised database of biometric as well as demographic information, with the Central Identities Data Repository (CIDR) which is under the control of the state. While this model prioritises administrative efficiency, it also creates a point of failure, which is, the constitutional risk of the state or the potentially unauthorised actors transferring data across multiple domains.

[28]e-Estonia, *Estonia Introduced a New ID Card*, https://e-estonia.com/estonia-introduced-a-new-id-card/.
[29]e-Estonia, *ID-Card: The Cornerstone of Estonia's Digital Society*, https://e-estonia.com/solutions/estonian-e-identity/id-card/.

Whereas the DPI of Estonia in contrast, functions on a decentralised structure which is built on the X-Road platform, and in place of collating the information, it instead connects numerous autonomous databases through a secured exchange layer, across the public and private sectors. Such a mechanism diffuses threat of failure, enhances resilience and also reduces the potential for mass surveillance. The X-Road being an open source further incubates transparency and the trust of the public.

This distinction, places the two models at the opposite ends of the spectrum of digital statehood, i.e., *India's state efficiency centric model, where citizens later adapt to the technological systems developed,* and, *Estonia's citizen right centric model, where technology adapts to these right based principles.*

Privacy, Surveillance, and State Power

The centralised system of India facilitates the convergence of data across various public services, which in turn enables cross linkages that could eventually lead to surveillance of the people of the country. Despite the Hon'ble Supreme Court holding that Aadhaar was not a tool of surveillance[30],repeated data breaches have been witnessed, and the opaque protocols regarding access have undermined that assurance. Also a possibility of Aadhaar with AI based tracking or predictive policing systems raises concerns with respect to unchecked executive power.

On the other hand, the approach of Estonia to privacy is in fact, remedial, since its DPI already embeds safeguards like encryption, digital signatures, and user access logs into the system itself. The individual can trace every instance of their data being accessed, along with this, they can also view which agency retrieved their information, shifting privacy protection from a legal defence to a technical guarantee.

Inclusion, Dignity, and Access to Welfare

The failure of biometric authentication in the Indian welfare schemes like the Public Distribution System (PDS), has excluded vulnerable citizens from rations and other benefits. Studies have recorded such failure rates of upto 12%.[31] These accidents are real

[30]K.S. Puttaswamy (Privacy-9J.) v. Union of India, (2017) 10 SCC 1.
[31]The Quint, *UIDAI CEO Admits Aadhaar Authentication Failure Rate up to 12%,* https://www.thequint.com/news/india/uidai-ceo-admits-aadhaar-authentication-failure-rate-12.

constitutional injuries to the right to life and dignity under Article 21[32]. While the court accepted Aadhaar for welfare schemes, but struck it down for private uses, this only addressed the issue partially, because the problem of technological errors still persists.

Whereas Estonia's framework has reversed this relationship of technology and dignity. Its "once only" principle reduces redundant procedures of repeated verification, and the digital inclusion being built into the system minimises human error and bureaucratic delay, demonstrating how inclusion can be engineered into governance without depending on judicial enforcement in case of failures.

Legal Philosophy: Reactive v. Proactive

The trajectory of India can be labelled to be a *reactive* one, in which the constitutional limits were imposed after the rights were violated. The proportionality analysis done by the Supreme Court in the Puttaswamy Case[33] is a testament to this approach. The reliance on post-facto judicial review limits the effectiveness of protection of rights.

On the flip side of this, Estonia or rather the EU show a more of a *proactive* regulatory approach with norms like the GDPR[34] and eIDAS Regulation[35] which define privacy, consent, and interoperability requirements before the technologies are deployed. Estonia makes sure that the safeguards of the fundamental rights of the citizens are not left to judicial interpretation by programming those safeguards into the architecture of the system.

F. CONCLUSION

This comparative study of India and Estonia illustrates how a DPI architecture choice can inadvertently become a constitutional choice and shows how, a state is structuring its digital identity system, is concurrently shaping the balance between efficiency, rights, and accountability.

Aadhar's centralised database presents the risks of rapid digitisation in the absence of appropriate legal safeguards. Having improved the administrative efficiency to a great

[32]India Const. art. 21.
[33]K.S. Puttaswamy (Privacy-9J.) v. Union of India, (2017) 10 SCC 1.
[34]Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, 2014.
[35]GDPR, Regulation (EU) 2016/679.

extent, the system is not able to completely curb exclusion and also represents vulnerabilities to privacy, along with the fear of state surveillance. The Puttaswamy Judgement was an attempt to reduce these tensions through the proportionality test, still the architecture itself appears to be the stem of recurring constitutional conflicts.

Talking of Estonia's X-Road and e-ID systems, they integrate privacy and proportionality into their design itself, leaving no room for constitutional conflicts. Management of data in a decentralised manner, encrypted exchanges, and transparent access logs prevents any single institution from monopolising personal information. Then again, the legal frameworks of GDPR[36] and eIDAS[37] which institutionalise privacy before technological deployment transform the constitutional guarantees into operational realities.

The comparison done presents three principal findings:

- Technological architectural choices have corresponding constitutional impacts: a centralised architecture increases the magnitude of power asymmetries, whereas a decentralised system distributes control and responsibility.
- Legal sequencing: technological design should be guided by rights and not vice versa, where rights have to be confirmed by carving out the technological design.
- Trust arises from transparency and not compulsion: legal regimes that are open and auditable foster trust of the subjects, as opposed to the ones that rely on mandatory participation.

Charting the path forward

While Estonia's DPI sets a commendable example of privacy encrusted into the design, we cannot ignore the geographic, demographic, and administrative scale at which India operates, with a population of over 1.4 billion, that the government of Estonia dealing with a population of just over a million cannot even begin to fathom.What happens to be working seamlessly for Estonia cannot be transplanted to India's diverse and federal framework.

However, at the same time, the goal of this study was to learn lessons from Estonia's system. But also, the exceptional journey of India with respect to Aadhaar and Universal

[36]GDPR, Regulation (EU) 2016/679.
[37]Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, 2014.

Payment Interface (UPI) has already shown that DPI at such a large scale can transform governance. The paper does not suggest adopting Estonia's DPI architecture but merely the principles behind it, to inspire India's future infrastructure projects, especially as it expands into areas like health, education, and data governance.

G. REFERENCES

Primary Legal Sources

1. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.
2. Constitution of India.
3. Digital Personal Data Protection Act, 2023.
4. GDPR, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), 2016.
5. Identity Documents Act, RT I 1999, 25, 365.
6. Personal Data Protection Act, RT I, 26.06.2019, 32 (Est.).
7. Regulation (EU) No. 910/2014 of the European Parliament and of the Council of 23 July 2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation), 2014.

Case Law

1. K.S. Puttaswamy (Privacy-9J.) v. Union of India, (2017) 10 SCC 1 (India).

Government & Institutional Reports

1. G20 India Presidency, G20 Framework for Systems of Digital Public Infrastructure (Aug. 2023), https://g7g20-documents.org/fileadmin/G7G20_documents/2023/G20/India/Sherpa-Track/Digital%20Economy%20Ministers/2%20Ministers%27%20Annex/G20_Digital%20Economy%20Ministers%20Meeting_Annex1_19082023.pdf.
2. Nordic Institute for Interoperability Solutions (NIIS), About NIIS, https://www.niis.org/.

3. Police and Border Guard Board (PPA), Republic of Estonia, About the Police and Border Guard Board, https://www.politsei.ee/en.
4. Unique Identification Authority of India (UIDAI), About UIDAI, https://uidai.gov.in/en/.

Academic & Policy Literature

1. Jackson School of International Studies, University of Washington, The Aadhaar Card: Cybersecurity Issues with India's Biometric Experiment, https://jsis.washington.edu/news/the-aadhaar-card-cybersecurity-issues-with-indias-biometric-experiment/#_ftn11.
2. Postimees, Cyber Lollygagging Cost the State Millions, https://news.postimees.ee/6383968/cyber-lollygagging-cost-the-state-millions.
3. The Legal School, CoWIN Data Breach: A Wake-Up Call for India's Digital Infrastructure, https://thelegalschool.in/blog/cowin-data-breach.

News Articles

1. The Quint, UIDAI CEO Admits Aadhaar Authentication Failure Rate up to 12%, https://www.thequint.com/news/india/uidai-ceo-admits-aadhaar-authentication-failure-rate-12.

Official Digital Governance Platforms

1. e-Estonia, *Data Embassy: Ensuring Digital Continuity Beyond Borders*, https://e-estonia.com/solutions/e-governance/data-embassy/.
2. e-Estonia, *Estonia Introduced a New ID Card*, https://e-estonia.com/estonia-introduced-a-new-id-card/.
3. e-Estonia, *How Estonia Saves Annually 820 Years of Work*, https://e-estonia.com/how-save-annually-820-years-of-work/.
4. e-Estonia, *ID-Card: The Cornerstone of Estonia's Digital Society*, https://e-estonia.com/solutions/estonian-e-identity/id-card/.
5. e-Estonia, *KSI Blockchain: Ensuring the Integrity of Data and Systems*, https://e-estonia.com/solutions/cyber-security/ksi-blockchain/.

6. e-Estonia, *X-Road: Secure Data Exchange Between Organisations*, https://e-estonia.com/solutions/interoperability-services/x-road/.