ISSUE BRIEF

INSTITUTE OF STRATEGIC STUDIES ISLAMABAD
Web: www.issi.org.pk
Phone: +92-51-9204423, 24
Fax: +92-51-9204658

INDIA'S G20 FRAMEWORK OF DIGITAL PUBLIC INFRASTRUCTURE: VULNERABILITIES AND MASS SURVEILLANCE

By
Maheen Shafeeq
Research Associate
India Study Centre (ISC), ISSI

Edited by
Dr. Khurram Abbas

January 2, 2024

(Views expressed in the brief are those of the author, and do not represent those of ISSI)

Introduction:

The G20 Leaders' Declaration welcomed the proposal of the 'G20 Framework for Systems of Digital Public Infrastructure (DPI)' by India.[1] The stated purpose of DPI framework is to minimize the digital divide and harness the potential of technology in low and middle-income countries, especially Africa. Though the DPI would bring services to society, it would have notable repercussions as well. It appears that India's proposal for DPI is to gather, control and govern global data, particularly from low and middle-income countries. Personal, financial, commercial, government, and defence information, which can be referred to as 'data,' is a critical strategic asset that exposes intricate details of the functioning of the state from the top (i.e. government) down to its basic unit, which is the individual. It exposes a society's information-processing, decision-making and problem-solving mechanisms, which would make the states adopting India's Framework of DPI vulnerable.

[1] Ministry of External Affairs India, "G20 New Delhi Leaders' Declaration," New Delhi, September 9-10, 2023, https://www.mea.gov.in/Images/CPV/G20-New-Delhi-Leaders-Declaration.pdf

India's DPI Ecosystem and its Vulnerabilities

The DPIs are digital applications or platforms that allow the exchange of data between different agencies which could either be government or businesses. DPIs function as Application Programming Interfaces (APIs), acting as messengers or connecting middle layers between applications, databases, software, or the internet-of-things.[2] In the case of global DPI, India aspires to be connecting layer.

The Indian government has introduced various digital platforms to harness India's DPI, such as for identification, digital payments, e-signature, healthcare, education and skills, to build a digital ecosystem. Famous digital platforms in India are CoWIN, Digilocker, Umang, IRCTC Rail Connect, MyGov and so on.[3] A commonly known digital platform in India is 'Aadhaar,' a unique digital identity connected to centrally stored basic demographic and biometric information. While the most promoted, especially among foreign visitors, is India's Unified Payments Interface (UPI) for the financial inclusion of citizens. However, UPI is also a highly vulnerable digital platform.[4]

As per India's Ministry of Finance, UPI fraud cases exceeded 95,000 in the year 2022-23, which is a notable increase from 84,000 cases reported in 2021-22. It is estimated that 55 percent of digital payment frauds in India are associated with UPI transactions.[5] Aadhaar identity is linked with UPI, which has led to theft of even property records and land ownership, among other financial frauds.[6] The G20 Leaders Declaration mentions the extension of such platforms beyond India. Particularly, it focuses on the inclusive use of financial digital technology by agri-tech startups, and small and medium-sized enterprises. It mentions of introduction and adoption of Central Bank Digital Currencies (CBDCs) particularly for cross-border payments. This would ultimately expand the scope of India's fraud market and widen the pool of potential targets. This shows that though the purpose of such a digital ecosystem would be to promote financial inclusion of citizens; however, it also exposes citizens of other countries to financial frauds, scams and cybercrimes.

[2] https://www.mailmodo.com/guides/api/

[3] Rohit KVN, Top 7 Indian government apps you should have on mobile, *Deccan Herald*, May 11, 2019, https://www.deccanherald.com/specials/top-7-indian-government-apps-you-should-have-on-mobile-732897.html

[4] "Renuka Kumar, Sreesh Kishore, Hao Lu and Atul Prakash, "Security Analysis of Unified Payments Interface and Payment Apps in India," *29th Usenix Security Symposium*, 2020, https://www.usenix.org/conference/usenixsecurity20/presentation/kumar

[5] Armaan Joshi, "Top Financial Scams In India For 2023," *Forbes*, December 20, 2023, https://www.forbes.com/advisor/in/personal-finance/financial-scams-in-india/#:~:text=In%20the%20fiscal%20year%202022,are%20associated%20with%20UPI%20transactions.

[6] Tanushree Dubey, "Aadhar Card Vulnerabilities: Understanding scams and protective measures," *Law Insider*, October 31, 2023, https://www.linkedin.com/pulse/aadhar-card-vulnerabilities-understanding-scams-protective-umi1f

Data Governance and Mass Surveillance

India’s DPI aspires to be the intermediary that would store, process, and transfer data between government agencies and citizens of other states, which can allow greater oversight of their activities. This becomes particularly concerning in India due to the practice of mass surveillance.[7] Through the proposal for the Framework of Systems of DPI, India could extend such activities globally, which is hinted in the G20 Leader’s Declaration as it mentions of cross-border data flow.

The G20 Leader’s Declaration mentioned the details of how they plan to build the DPI. For this purpose, the G20 leader agreed on the following:

1. “Welcome the G20 Framework for Systems of Digital Public Infrastructure, a voluntary and suggested framework for the development, deployment, and governance of DPI.

2. Welcome India’s plan to build and maintain a Global Digital Public Infrastructure Repository (GDPIR), a virtual repository of DPI, voluntarily shared by G20 members and beyond.

3. Take note of the Indian Presidency’s proposal of the One Future Alliance (OFA), a voluntary initiative aimed to build capacity, and provide technical assistance and adequate funding support for implementing DPI in LMICs.”[8]

Dissecting the plan, the DPI is a voluntary and suggestive framework for the development, deployment and governance of DPI. The first point does not indicate whether India would solely develop, deploy, and govern DPI or would it be a collective effort. However, it does highlight that India would be playing a prominent role in the governance of DPI, which is a crucial factor. If Indian researchers would develop and deploy the DPI, they can exercise greater leverage over the governance of DPI. Secondly, it shows Indian intent that how New Delhi plans to govern the global public data. It mentioned that India would build and maintain the repository of the global public data. This would imply that Indian laws would govern how, where and till how long the data is collected, stored, managed and processed. This could make the data susceptible to tampering by the Indian government and intelligence. Lastly, the third point highlights that the Indian government would train, build capacity, and provide financial support for building DPIs in low and middle-income countries. As India has welcomed the African Union into the G20 during its presidency, the DPI initiative is particularly targeted towards these states. Though this could help enhance technological integration and social mobility in Africa, it would

[7] Kamesh Shekar and Shefali Mehta, “The state of surveillance in India: National security at the cost of privacy?,” *ORF*, February 17, 2022, https://www.orfonline.org/expert-speak/the-state-of-surveillance-in-india

[8] Ministry of External Affairs India, “G20 New Delhi Leaders’ Declaration.”

expose the government data of African states, which may undermine their sovereignty. It is important to note that the Declaration mentioned India setting up DPI voluntarily, which implied that India views this as an investment into the information hub of an emerging market.

At present, there are no mechanisms for global governance of data or Artificial Intelligence. There are regulatory measures in place by various states such as the European Union's General Data Protection Regulation (GDPR), California's Consumer Privacy Act (CCPA), UK's Data Protection Act (DPA) and so on for digital media platforms that collect global data but these platforms are largely governed by their own rules and regulations rather than the states' regulations. It is also because usually state regulations lag behind the advancements and complex issues surrounding data. Moreover, some states do not have control over these social media platforms and how they store, use or sell data. What makes India's proposed DPI more vulnerable is that it would use the critical data of other states such as the identity of public, medical and financial records, which can have national security implications for low and middle-income countries.

While this may work for India and its public, it does create avenues of vulnerability for states opting for India's DPI framework. As the DPI maximizes openness and interoperable usage, it opens more avenues for people to engage with DPI, enhancing digital competition but also vulnerabilities. Though the G20 Leader's Declaration was cognizant of "safe, secure, trusted, accountable, inclusive, respectful of human rights, personal data, privacy and intellectual property rights," it does not mention how New Delhi would efficiently ensure its management. In order to guarantee data security, data privacy, and ethical and legal handling of private data, comprehensive laws and legislation must govern the data. However, a delicate balance needs to be ensured between regulations and digital freedom. Presently, the world is struggling to ensure the delicate and just balance on digital platforms, which shows that India would not be prepared to deliver this without malintent.

Conclusion

India's proposal of developing and deploying a global DPI has the potential to benefit its citizens. It would harness the potential of emerging technologies to deliver inclusive digital development. However, at present, India's DPI remains vulnerable even nationally. This exposes the low standards of digital safety and security of India's DPI. The proposed extension of India's DPI globally, especially in low and middle-income countries, appears as India attempts to increase its role in the development of global governance of data, AI and cybersecurity. It would enable India to try and control and administer the global data. This initiative will likely add vulnerabilities for the citizens of states adopting India's DPI, particularly mass surveillance and data exploitation. Though India's DPI plan mentions ensuring data privacy, trust and accountability, delivering these is only easier said than done.

India, at present, does not have a robust regulatory mechanism for the protection of digital platforms. Even India’s most used digital platforms such as Aadhaar and UPI remain vulnerable to fraud and cybercrimes, which shows weak mechanisms of cybersecurity and data protection. Understandably, ensuring cybersecurity in a highly digital fluid environment is a complex task. Due to this, it remains uncertain how trustworthy, inclusive and private India’s DPI would be. What principles and standards would govern and safeguard the cross-border data flow requires deeper deliberation and detailed inspection by the countries intending to voluntarily adopt India’s DPI.