International Journal of Law Research, Education and Social Sciences

Open Access Journal – Copyright © 2026 – ISSN 3048-7501
Editor-in-Chief – Prof. (Dr.) Vageshwari Deswal; Publisher – Sakshi Batham

Cloud Sovereignty in India: How to Develop Effective Mechanisms to Establish Cloud Sovereignty?

Sania[a]

[a]University Institute of Legal Studies, Panjab University, Chandigarh, India

Received 10 March 2026; Accepted 09 April 2026; Published 13 April 2026

The integration of cloud computing into commercial and governmental infrastructures has caused a major shift in the meaning and concept of sovereignty. Cloud environments owned by private tech giants are highly scalable, cost-effective and remotely operated. However, they come with significant risks not only to privacy and security but also to sovereign state structures as a whole. Sovereignty is no longer decided by territory but by who controls the data integral to the governance of a state. This paper specifically highlights India's dependence on privately operated cloud providers and the risks it poses to the country. It also studies India's regulatory and policy landscape to argue that existing legal frameworks are insufficient to reclaim digital sovereignty in India. It conducts a doctrinal analysis of IT, 2000 and DPDP, 2023, along with an analysis of technical measures by the government of India, including the Meghraj GI-Cloud and the National Infographics Centre's National Cloud initiative, to understand the attempts of the Indian government and also suggests further techno-legal advancements to pave the way towards achieving cloud sovereignty in India.

Keywords: *digital sovereignty, cloud computing, cloud sovereignty, national infographics centre.*

INTRODUCTION

The concept of sovereignty has evolved dramatically with the advancement of technology. Today's societies rely on technology more than ever, and this is true for governments as well. The elements of sovereignty, such as territory and institutions, have shifted to a vast digital infrastructure controlled by technological giants. While debates on this shift were going on, another paradigm of digital sovereignty emerged-cloud sovereignty. Cloud computing services emerged as a revolutionary technology which provided heavily scalable services worldwide. It transcends borders and is highly scalable while being remotely operated.

Today, these Cloud Service providers offer service for a minimal cost, but the unseen price that the customers pay along with it is their privacy. The idea that if the tech giants control our data, they control us, resulted in escalated tensions between the traditional sovereign authorities-governments and these tech giants who became the de facto sovereigns.

Historically, sovereignty has always been defined as the supreme authority of the state to govern its territory while being free from external control. However, the shift of governmental functions and data storage to cloud environments challenges this classical theory of sovereignty. Cloud computing technology decentralises computational resources while concentrating infrastructural power in a limited number of global providers. The operational mechanism of cloud systems makes state control over its digital economy subordinate to the big tech companies. In the Indian context, it is paired with dependence on foreign cloud service providers, which further aggravates the situation as data integral to the state is hosted by foreign tech giants.

Digital India's adoption of e-governance frameworks aimed at expanding digital identification systems and online citizen-centric services has increased its dependence on foreign cloud technologies. Despite the benefits of cloud computing, associated sovereignty risks must also be taken into account while we move further towards our Digital India mission.

The debates on cloud sovereignty extend beyond data localisation and legitimacy. India's innovative measures, like the Government of India Cloud initiative (MeghRaj) and the development of the NIC National Cloud, reflect attempts to reclaim sovereign control over cloud technologies. As of now, no specific statute has been designed to address this issue.

This paper studies relevant legal and technological frameworks to examine India's position in the digital sovereignty race. In doing so, it seeks to contribute to emerging debates on how constitutional governance adapts to technological advancements in the digital era.

RESEARCH METHODOLOGY

This paper adopts doctrinal and analytical research methods relying on both primary and secondary sources. Primary sources include bare acts for analysing statutes, official government portals, policy documents and publicly available government reports. Secondary sources include journal articles and published research papers for analysing various aspects of the topic. In addition, online news articles and credible media reports were also used for tracing recent developments, debates and concerns. These sources offer a systematic analysis of the relationship between technology and sovereignty.

SHIFT IN THE CONCEPT OF SOVEREIGNTY

Traditional Sovereignty: We all have read the same thing about sovereignty in political science- "Sovereignty is the Supreme Rule of the Sovereign."[1] If a state is sovereign, it means it is free from all external controls and the sovereign rules every aspect of the state. Earlier, the sovereigns were kings.[2] Today, it's our political heads- whether democratically elected leaders or dictators. However, when the definitions of sovereignty were being given, the thinkers did not comprehend the possibility of a vast technological revolution which would permanently alter its meaning in the future. We cannot say that sovereignty means something entirely different today. However, there has been an undeniable expansion in the meaning of this term, and the entire concept of sovereignty has broadened. Today, we come across newer terms like digital sovereignty and many of us feel intimidated for the right reason of not knowing what it is. The following two sections elaborate on these terms.

Digital Sovereignty: When the internet was invented in the late 1900s, no one could have predicted the ways in which it would be used today. Today, we use the internet for almost everything- from tiny Google searches to streaming a movie online, from making online payments to putting out an entire estate for sale. Not surprisingly, it is not just the public but

[1] Francis Harry Hinsley, *Sovereignty* (2nd edn, CUP Archive 1986)
[2] Daniel Philpott, 'Sovereignty' in George Klosko (ed), *The Oxford Handbook of the History of Political Philosophy* (OUP 2011)

also the government that uses the internet. Not so long ago, something called E-governance[3] started taking shape. We all know the role played by the COVID-19 pandemic in drastically increasing the use of the internet worldwide. It also skyrocketed the use of the internet for governance. We have had online government websites and portals for a long time. However, after the pandemic, governments worldwide began setting up platforms for online healthcare, education and overall governance as well.

Almost everything on the internet is owned by big tech companies. You can say that you own a website, but the platform on which your website runs is entirely controlled by a tech giant that you have no control over. But, if we say we live in a sovereign state, shouldn't this aspect also be controlled by our government? The answer is- yes, it should be. In fact, it has to be. This is what we mean by digital sovereignty. It means the ability of a state to maintain control over its entire digital ecosystem.[4] To put it simply, Digital Sovereignty means sovereignty over the digital world, and the digital world includes everything that is on or connected to the internet. Digital sovereignty is really about having control over your digital world.[5]

Data Sovereignty: A narrower concept of digital sovereignty is data sovereignty.[6] which means control over data within a specific jurisdiction. Basically, it refers to the idea of information being governed by the laws and systems of the government of a specific state.[7] Different states have different data sovereignty rules and frameworks.

At this point, we must understand the difference between data sovereignty and data localisation. When we talk about data sovereignty, we are talking about a legal concept by which we mean that data is subject to the law of a specific state, no matter where it is stored or processed. However, data localisation is a physical concept, which means that data is processed and stored within a specific state.

---

[3] Muhammad Ali, 'E-governance and E-democracy: A Digital Revolution' (2023) SSRN <https://ssrn.com/abstract=4623414> accessed 11 February 2026

[4] Victor Angelier, 'From Sovereign Cloud to Data-Centric Sovereignty: A Framework for Digital Sovereignty' (2026) SSRN <https://ssrn.com/abstract=6172067> accessed 10 February 2026
accessed 10 February 2026

[5] 'Digital sovereignty 101: Everything you wanted to know (and needed to ask)' (*Google Cloud,* 02 October 2025) <https://cloud.google.com/transform/digital-sovereignty-101-your-questions-answered/> accessed 11 February 2026

[6] *Data Sovereignty, Data Residency, and Data Localization: An Introduction* (Scale Computing 2023)

[7] Prateek Singh, 'How Data Sovereignty Matters: Secure Your Cloud Now' (*ESDS*, 20 August 2025) <https://www.esds.co.in/blog/data-sovereignty-matters-secure-your-cloud-now/> accessed 10 February 2026

Cloud Sovereignty: Another aspect of digital sovereignty, which is central to this paper, is Cloud sovereignty. For this, we must first understand what the cloud means. A cloud is not just something we see in the sky. Today, it is a much more complex technological concept. A cloud is a platform which offers on-demand delivery of Information Technology (IT) Services with pay-as-you-go pricing.[8]

Cloud computing means the delivery of computing services like servers, software, artificial intelligence (AI), etc., over the internet. Today, there are many cloud providers in the market - Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, etc.[9]

It shifts the way we think about IT. There is no need for huge in-house servers anymore. We can just pay a cloud provider for the services we want and avail them. It is cost-effective, fast and globally scalable.[10] All of this makes cloud computing the new way of doing things online. It is mainly being used in running businesses, but many states, including India, are increasingly using it for e-governance.[11]

However, as with any other technology, there comes a risk along with its benefits. The very idea of using cloud technology suggests privacy risks because of its "no responsibility" nature. To put this into perspective, if we pay someone else to store or process our data, we are willingly giving them control over our data. This is the main disadvantage of cloud computing against traditional or on-premise IT- we lose control of our own data.[12]

We are already developing laws and other frameworks to ensure security and privacy in the older and "less risky" IT environment, so it is an obvious conclusion that when we use cloud technology, the laws need to be more robust and comprehensive. The following section

[8] 'What is cloud computing?' (*Amazon Web Services*) <https://aws.amazon.com/what-is-cloud-computing/> accessed 11 February 2026
[9] Prajwal, 'Top 15+ Private Cloud Providers Dominating 2026' (*Sprintzeal,* 24 February 2025) https://www.sprintzeal.com/blog/private-cloud-providers accessed 11 February 2026
[10] 'Advantages and disadvantages of cloud computing' (*Google Cloud*) <https://cloud.google.com/learn/advantages-of-cloud-computing> accessed 11 February 2026
[11] C Vijai and D Joyce, 'Cloud-Based E-Governance in India' (2020) 8(2) Shanlax International Journal of Management <https://doi.org/10.34293/management.v8i2.3334> accessed 11 February 2026
[12] Ajith, 'Major Cloud Computing Problems Facing Businesses' (*Digit Defence*, 09 November 2024) <https://digitdefence.com/blog/major-cloud-computing-problems-facing-businesses> accessed 11 February 2026

elaborates on these risks and emphasises the need to develop stronger frameworks to maintain privacy and security in cloud environments.

THE NEED FOR STRONGER PRIVACY AND SECURITY FRAMEWORK TO ESTABLISH CLOUD SOVEREIGNTY

To have a clear understanding, we must study this section by dividing it into two parts: firstly, the risks associated with cloud computing and secondly, the insufficiency of the current legal frameworks in establishing cloud sovereignty.

Risks Associated with the Use of Cloud Computing Services: Unlike traditional ICT, one cloud platform can extend to multiple jurisdictions with no limits whatsoever. Every country wants to advance in technology, and the benefits of using cloud services seem to overshadow their flaws. However, not every country is equally advanced in technology, especially developing countries like India that still rely on foreign technology.

The majority of the Cloud Service Providers (CSPs) are based in America and are owned by the tech giants like Amazon, Microsoft, Adobe, etc. According to Digit Defence, "The cloud market is majorly dominated by three main CSPs, and they are- Amazon Web Services (AWS), Microsoft Azure, and Google Cloud (GCP). Together, these three companies capture over 65% of the global cloud infrastructure market. In India, they account for approximately 33% of all public cloud revenue." Many other countries, especially developing nations, avail their services for various purposes, including E-governance. This clearly means that they are sharing critical governance data with companies based in a foreign country.

Besides, the US CLOUD (Clarifying Lawful Overseas Use of Data) Act, 2018[13] mandates that every CSP based in the US must disclose information to the US government whenever required, irrespective of where the data was stored or processed. This means that the US government can request access to information of any other country, if it is available on a CSP based in the US. This poses a clear threat to digital sovereignty. According to Swiss reporter Craige Hail, "Data protection officers from Switzerland have warned government not to use cloud services from Microsoft, Amazon, and Google, due to a lack of true end-to-end encryption. This comes as

[13] Clarifying Lawful Overseas Use of Data (CLOUD) Act 2018 (US)

many SaaS (Software as a Service) vendors, especially those that come under the US Cloud Act, could be required to hand over data to US authorities, even if it is stored in Switzerland."[14]

US cloud providers, such as AWS, have attempted to reassure international clients by stating that the CLOUD Act "does not give any government unlimited or automatic access to data" and that, since 2020, they "have not disclosed any enterprise or government content data stored outside the U.S. to the U.S. government." However, this is a carefully worded statement of past performance, not a legal guarantee of future immunity.

The act also allows the US to sign bilateral agreements with other countries to access information stores in US clouds for the purpose of easing the transfer of data. The UK and Australia have already signed such agreements under the Act. India does not yet have any agreement with the US under this act. However, there is a possibility of future agreements.[15]

Another problem is that the tech companies are private entities and do not have a "social contract" with the citizens, unlike the states. So, there exists a "legitimacy gap" as they have no responsibility to ensure that the citizen data remains secure, and there are high chances of data being used against the public interest.[16]

Data breaches are a significant risk in cloud environments. A data breach means unauthorised access to data stored in a system. In particular, public clouds are prone to hacking and other cyberattacks. According to the Federal Bureau of Investigation, cyber crimes went up by 69% year-over-year and half of the attacks in 2022 came via cloud applications.[17] This shows that data stored in the cloud is more prone to being breached.

---

[14] Craig Hale, 'Swiss government urges people to ditch Microsoft 365 and others due to lack of proper encryption' (*Tech Radar*, 02 December 2025) <https://www.techradar.com/pro/security/swiss-government-urges-people-to-ditch-microsoft-365-and-others-due-to-lack-of-proper-encryption/> accessed 10 February 2026

[15] 'CLOUD Act Resources' (*United States Department of Justice*) <https://www.justice.gov/criminal/cloud-act-resources> accessed 11 February 2026

[16] Huw Roberts, 'Digital sovereignty and artificial intelligence: a normative approach' (2024) 26(4) Ethics and Information Technology <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4699167> accessed 10 February 2026

[17] Brett Deemer, 'What Are the Security Risks of Cloud Computing?' (*Optro*, 17 July 2024) <https://auditboard.com/blog/what-are-the-security-risks-of-cloud-computing/> accessed 10 February 2026

ANALYSIS OF RELEVANT LEGAL FRAMEWORKS IN INDIA

As of now, there is no specific law that aims for cloud sovereignty in India. However, some frameworks might play scattered roles towards achieving it.

Information and Technology Act, 2000: Section 69 of the act is a very important provision in this respect as it authorises the Central/State Government to intercept, monitor, decrypt information on grounds of sovereignty and integrity of India, security of the State, maintaining public order, etc.[18] Section 69A allows the government to block access to information for sovereignty, defence, security, etc.[19] The issue here is that the IT Act is primarily a data protection law and not designed with any thought of sovereignty. There are not many provisions of this act that can be moulded for this purpose.

Digital Personal Data Protection Act, 2023: One of the best things about the DPDP Act is its extent; it applies not only to the processing of personal data inside the territory of India, but also outside, as long as it is related to Indian Data Principals. This is key because, as we have already discussed, CSPs are international, and India does not have its own cloud. However, one thing we come across while reading this act is that it majorly ensures an individual's sovereignty over personal data, which lowers its relevance for other types of data that might be non-personal in nature.

Section 2(k) defines Data Processor as an entity processing personal data on behalf of a Data Fiduciary. CSPs fall under the definition as they process data on behalf of the customers.[20] Section 10 allows the government to classify certain data fiduciaries as "Significant Data Fiduciaries" (SDFs)[21] based on multiple factors, including volume and sensitivity of data and the amount of associated risk. Once classified, the significant data fiduciary has to appoint a Data Protection Officer based in India, and an Independent Data Auditor in accordance with the provisions of the act. CSPs easily qualify as SDFs. However, as of now, the government has not notified any CSP as SDF.

[18] Information Technology Act 2000, s 69
[19] Information Technology Act 2000, s 69A
[20] Digital Personal Data Protection Act 2023, s 2(k)
[21] Digital Personal Data Protection Act 2023, s 10

Section 12 allows the data principal to request complete erasure of personal data held by a data fiduciary. This is another key provision for ensuring individual sovereignty over personal data.[22] The problem with the DPDP act, which many seem to miss, is that it applies only to "personal data" and the data stored and processed by government agencies on foreign cloud platforms may not qualify as "personal data". If the act is amended in future to include all forms of data, it might become complex. Therefore, a newer and more specific law is required for this purpose.

Cloud Service Contracts (CSC): As of now, the privacy and security of non-personal government data are based on Cloud Service Contracts. Cloud Computing Contracts, or Cloud Service Contracts, or simply Cloud Contracts, are a non-statutory way of ensuring privacy. Government agencies can design cloud contracts in a way that focuses on data security. However, contracts are private law instruments and have little to no significance in deciding sovereign authority. The ultimate authority rests with the CSPs and not the government.

In the absence of relevant statutes, contractual provisions become crucial in expressing the parties' understanding of how to divide risks and responsibilities between them. However, Laws and regulations are required for auditing, penetration tests and physical inspection of data centres involved in cloud computing services to ensure arbitrary terms and conditions.[23]

Another issue is that the most common form of cloud computing contracts in India is drafted in the international standard form of contracts with fixed terms. India does not have its own standard for cloud computing contracts. Besides, under Indian laws, parties to a contract have the right to choose the governing law. Even if parties are contracting in India, and the customer of CSP, which is a party to the contract, is based in India, the parties may choose not to be governed by Indian Law. Not just that, even the terms and conditions of most cloud contracts in India are similar to terms that are commonly used in large markets, such as the US and the UK.[24]

---

[22] Digital Personal Data Protection Act 2023, s 12
[23] 'Notes on the Main Issues of Cloud Computing Contracts (prepared by the secretariat of the United Nations Commission on International Trade Law, 2019)' (*United Nations Commission on International Trade Law*) <https://uncitral.un.org/en/cloud/pre-contract> accessed 10 February 2026
[24] Samuel Mani, 'Cloud Computing Contracts in India' (*Lexology*, 18 November 2019) <https://www.lexology.com/library/detail.aspx?g=ae7a1ac9-bb2c-47cc-b4e0-36ce46e077a0> accessed 11 February 2026

Besides, it is also argued that CSCs are not as effective as they are proposed to be, even in ensuring privacy, as they are being used by CSPs as a shield to escape liability. This is largely due to the absence of any statutory provisions that mandate certain requirements in the terms and conditions of the cloud contracts.

MEGHRAJ- INDIA'S TECHNO-LEGAL INITIATIVE TOWARDS ACHIEVING CLOUD SOVEREIGNTY

The Indian Government's Ministry of Electronics and Information Technology launched its very own GI (Government of India) Cloud initiative in 2014.[25] "National Informatics Centre (NIC) has been providing cloud services to the Government at the Central and State levels to ensure Government services internally and for citizens. Under NIC cloud services, more than 21,000 virtual servers have been allocated for various e-Governance applications to more than 1470 Ministries/ users, and over 5000 websites of the Government are being served through NIC cloud."[26]

The Meghraj initiative is a national-level cloud management service which integrates various cloud computing services on a single platform. The main aim of this initiative is to regulate the effective implementation of e-governance services.[27] It also includes NIC (National Infographics Centre) Cloud Infrastructure, which is India's first and only state-run Cloud platform. This paves the way towards India's Cloud Sovereignty, being India's first-ever state-run cloud, a crucial step for cloud sovereignty.

Basically, as the government realised the importance and efficacy of cloud computing models, it sought to use them for implementing citizen-centric services and government schemes. However, instead of using a single cloud service, it sought to integrate multiple CSPs like Microsoft Corporation (India) Private Limited, IBM India Private Limited, Tata Communications Limited, Bharat Sanchar Nigam Limited (BSNL), ESDS Software Solutions Private Limited, Net Magic IT Services Private Limited, Sify Technologies Limited, CtrlS Data

[25] 'About Us' (*NIC Cloud*) <https://cloud.gov.in/user/about.php> accessed 11 February 2026
[26] *Annual Report 2024-25* (Ministry of Electronics & Information Technology 2025)
[27] 'National Cloud' (*National Informatics Centre*) <https://www.nic.gov.in/service/national-cloud/> accessed 10 February 2026

Centres Limited, Cyfuture India Private Limited, Web Werks India Private Limited, AMAZON Internet Services Pvt. Limited, NXTRA Data Limited and Reliance Corporate IT Park Ltd.[28]

The Meghraj initiative is indeed a commendably big step towards India's journey of achieving cloud sovereignty. However, one major problem remains- dependence on private CSPs. This challenges the practicality of this initiative in achieving digital sovereignty. As of today, India does not have its own cloud which is on par with the international competitors. However, that is not even required. What India needs is a fully state-run cloud instead of a compilation of CSPs in the name of GI cloud. The national cloud by NIC must be developed, and the dependence on foreign and domestic private CSPs must be reduced.

IS ABSOLUTE CLOUD SOVEREIGNTY ACHIEVABLE MERELY BY LAW?

Cloud sovereignty cannot be understood merely as a legal concept. Even though laws and regulations do play a crucial role in establishing sovereign authority, the cloud computing technology extends beyond the boundaries where the sovereign law prevails. Besides, Cloud as a technology is inherently complex in nature, and the governance challenges that come with it are not just rooted in statutory insufficiencies, but also in technological ones.

In the Indian context, the bigger problem is not the absence of targeted laws or frameworks. Such steps are easier to take. The real problem is India's dependence on foreign technologies. Besides, the state-run cloud in India is still in early development stages. Therefore, achieving cloud sovereignty requires looking at the challenges from a techno-legal perspective rather than simply a legal one.

The complexity of cloud environments complicates traditional understandings and assumptions of sovereignty. What India requires is a hybrid governance model that focuses on fixing both the legal and technical insufficiencies in this respect. The development of the National Informatics Centre (NIC) Cloud marks the start of this approach. The NIC Cloud represents more than a technological initiative; it reflects a governance strategy aimed at reinforcing sovereign control through a state-run cloud. This also aligns with the objectives of national security.

[28] National Policy on Software Products 2019

PROPOSED TECHNO-LEGAL DEVELOPMENTS TOWARDS ACHIEVING CLOUD SOVEREIGNTY IN INDIA- SUGGESTIONS AND RECOMMENDATIONS

There must be newer, stronger, advanced and more specific laws that aim at ensuring privacy and security in private CSPs. Such laws must increase the liability of CSPs in handling citizen data. Privacy is the first step of digital sovereignty. Firstly, we must design privacy and security laws specific to cloud computing technology. Secondly, we design comprehensive mechanisms, including statutes, contracts, guidelines, etc. The main aim of such laws should be to bring tech giants under the umbrella of the Indian Government so that the government can exercise more control over citizen data.

There can also be laws that specify the required terms and conditions of Cloud Service Contracts so that CSPs do not use contracts as a shield to escape liability. Including such conditions which increase the responsibility of private CSPs in handling data. There can also be executive mechanisms, such as designated officers or committees, to examine each such contract to ensure compliance with the provisions of the act. The law may also mandate that Indian laws shall apply to the parties to the contract.

Set up fully state-run clouds and designate them as “protected systems” under Section 70 of the IT Act, 2000, for enhanced security. This classification criminalises unauthorised access and imposes stricter safeguards. Even though this provision is for cybersecurity protection, it can function as an important provision for shielding sovereign cloud infrastructures from external interference.

Seek to advance the NIC cloud instead of integrating more private CSPs under the Meghraj Initiative. Dependence on private CSPs comes with long-term risks. Focus should be on reducing this dependence and advancing in state-run clouds.

Set up a designated interdisciplinary committee to examine the strategic dimensions of the issue and make recommendations. There can also be separate committees- technical and legal, to handle different aspects and work together to evolve hybrid governance models.

Launch the Digital Swaraj (Self-Governance) initiative.[29] India's heavy dependence on foreign technologies is not just harmful for sovereignty but also for its economy. The Digital Swaraj mission must be given due importance, and indigenous technologies must be developed and scaled throughout the nation.

CONCLUSION

With the rapid adoption of cloud computing services in businesses and governance, cloud sovereignty has become one of the most important legal issues in today's digital world. It has not only expanded the meaning of sovereignty, but has also started debates worldwide on how to achieve digital sovereignty. India's position in the digital sovereignty race is not as behind as we imagine. However, we still have a long way to go. Since cloud sovereignty is not achievable merely by law, digital India must adopt a hybrid governance model with advanced legal mechanisms and secure technical solutions to ensure privacy, security and digital sovereignty. The proposed ways are inculcating state-run CSPs and scaling them pan-India, along with more robust laws to enhance sovereignty in private CSPs. Setting up national-level interdisciplinary committees can also help with in-depth research and better solutions. India must put a lot of thought into where it is headed with its level of dependence on foreign and private domestic technology. Realising and reversing it is the only true way of achieving cloud Sovereignty in India.

[29] "Digital Swaraj Mission': GTRI flags risks of US tech dependence; calls for India's cloud and OS self-reliance by 2030' *The Times of India* (14 September 2025) <https://timesofindia.indiatimes.com/business/india-business/digital-swaraj-mission-gtri-flags-risks-of-us-tech-dependence-calls-for-indias-cloud-and-os-self-reliance-by-2030/articleshow/123880429.cms> accessed 11 February 2026