CSS | ISSUE BRIEF

MAPPING INDIA'S DATA SECURITY AND SOVEREIGNTY

Jahnavi Pande *

INTRODUCTION

The clash between Indian and Chinese troops in the Galwan Valley, located in the Eastern sector of India's Union Territory of Ladakh led to the cumulative banning of over 200 Chinese apps by India's Central government,[1] citing 'national security' as the reason for the ban. For all intents and purposes, we can assume this was a retaliatory action by the Government of India, looking to punch above its weight in signaling to China that it was willing to stand up to its attempts at transgressing India's sovereignty.

By all means, the ban on apps was unlikely to cause a significant dent in India's trade deficit with China, nor was it likely to cause any major setback to China's economic prowess as a whole. The move nonetheless, is more than mere symbolism as China today, is among the leading producers of cutting edge technology in the world.[2] The ban on Chinese apps must be read in the context of India's emergent data security concerns as the number of internet users in the country continue to swell and new disruptive yet strategically important technologies required to harness for India's socio-economic and political ambition continue to mushroom.

If data is the new oil then its use has larger national security implications- a fact apparently recognized by several countries around the world, many of whom, such as the EU have strong data protection regimes already[3], and are now looking rather tentatively at the integration of China's 5G network into their systems. It is against this backdrop that India's data security situation must be assessed.

DATA SECURITY REGIME IN INDIA: AN OVERVIEW

1. Creation of NEST in the MEA

Earlier in 2020, the Ministry of External Affairs created the 'NEST' (New, Emerging and Strategic Technologies) Division. The immediate consideration for this development, was presumably due to the debate surrounding the entry of China's 5G under Huawei but even as

[1]* ***The Author is a student at the Jindal School of International Affairs and Research Intern at the Centre for Security Studies, JSIA.***

[1] Press Information Bureau, "Government Blocks 118 Mobile Apps Which Are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order," accessed December 30, 2020, pib.gov.in/Pressreleaseshare.aspx?PRID=1650669.

[2]Bob Savic, "China's New Digital Industrial Transformation," accessed December 30, 2020, https://thediplomat.com/2020/06/chinas-new-digital-industrial-transformation/.

[3] "General Data Protection Regulation (GDPR) – Official Legal Text," General Data Protection Regulation (GDPR), accessed December 30, 2020, https://gdpr-info.eu/.

that possibility phased out, tensions with China at the disputed boundary made the creation of this new division a timely step in the right direction.

The general idea behind the NEST division is a three-pronged approach to diplomacy in strategic technologies such as Artificial Intelligence (AI) or 5G. This entails policy guidance in shaping of international rules; navigating competition over strategic supply chains and aligning India's tech policy with international regimes.[4] A successful NEST will also mean greater diplomatic muscle on the part of India in shaping the rules of international engagement with such technologies. The challenge however, will be to first align India's diplomatic policy with its domestic policy, for which the MEA will have to work in consort with other ministries in arriving at a cohesive strategy.

2. Legislative Framework

Beyond diplomatic developments, India also has certain legislative frameworks dealing with data security in different sectors such a banking and telecommunications. These include the SPDI rules of 2011 to the IT Act, the Credit Information Companies (Regulation) Act of 2005 along with Credit Information Companies Regulations 2006 and circulars issued by the Reserve Bank of India. Other statutes governing the financial sector also contain provisions on data protection, particularly on customer confidentiality.[5] The Telecom Regulatory Authority of India (TRAI) through its regulations and the Unified License Agreement issued by the Department of Telecommunications also contain certain rules governing data protection although not very comprehensive by nature.[6]

3. Ad-hoc mechanisms

On the specific issue of India's national security and the protection of its critical infrastructure, India was, to its credit, quick in recognize the threats, by establishing the Computer Emergency Response Team (or CERT-in) as early as 2004 under the IT Act, 2000. CERT-In is essentially the "first responder" to any threat or use of cyberspace for unlawful activities. And while the agency has been effective, the violators of India's cyberspace have frequently managed to hoodwink its scrutiny.

IDENTIFYING EXISTING AND POTENTIAL THREATS

While criticism from some quarters on the Indian government using excess regulation to clamp down protests and other forms of dissent hold merit,[7] it is equally true that India faces a

[4]Trisha Ray and Akhil Deo, "Priorities for a Technology Foreign Policy for India," ORF, accessed December 30, 2020, https://www.orfonline.org/research/priorities-for-a-technology-foreign-policy-for-india/.

[5]Ministry of Electronics and Information Technology, "White Paper on the Committee of Experts on a Data Protection Framework for India," White Paper, 2017.

[6] Ibid at 30.

[7] *K.S. Puttaswamy (Retd.) v. Union of India & Ors.* 2017 (10) SCALE 1.

complex security environment, replete with both, traditional and non-traditional security threats. India has been fighting a largely asymmetric war in its conflict zones, the contours of which keep evolving as new technologies are being incorporated into the modus operandi of the various belligerents.

Broadly, India's security threats can be classified into left-wing extremism in certain areas, an international (ized) armed conflict in Jammu and Kashmir and other insurgencies in the North East.[8] Externally, India now has two heavily militarized borderlands on its Eastern and Northern flanks. And regionally, the country now stares at an increasingly contested maritime geography. All of these traditional security threats today, have underlying non-traditional features. In the aftermath of Burhan Wani's killing in 2016 for instance, India faced a spate of cyber-attacks clearly originating from outside its borders amidst escalating tensions with Pakistan.[9] With countries like China whose capabilities are even more formidable, the threat to India's critical infrastructure has only exacerbated and it is estimated that India faces over 300 cyber-attacks on a daily basis.[10]

All of these factors contribute to an understanding of national security that has now come to encompass a wide variety of forms. Moreover, the app ban by India also demonstrates that technology and data can be used, not only for surveillance and attack but also in the form of sanctions or coercion, thus rendering data security itself, with a punitive character. India has to be mindful of the fact that it too could be on the receiving end of such sanctions in the future.

IDENTIFYING "DATA SOVEREIGNTY" IN THE INDIAN CONTEXT

The debate on data sovereignty in India is rather murky with very few official positions being taken on the subject, and the government preferring an *ad hoc* approach to dealing with security challenges as they emerge. This does not mean that India has not made efforts to safeguard whatever connotation of sovereignty that may be understood by the state, but that no homogenous position has been articulated by official sources, detailing just what it would mean for India's digital sovereignty to be violated. Nonetheless, India's overall position on data localization and cross-border transfers of data does offer an indicative albeit inadequate understanding of India's broad position on the matter which, on at least a preliminary reading, appears to be fairly stringent.

[8] Utsav Mittal, "A New Framework for a Secure Digital India," ORF, accessed December 31, 2020, https://www.orfonline.org/research/a-new-framework-for-a-secure-digital-india/.

[9] "Government Sites Sit Defenceless as Pakistan Steps up Cyber Attacks - The Economic Times," accessed December 31, 2020, https://economictimes.indiatimes.com/news/economy/policy/government-sites-sit-defenceless-as-pakistan-steps-up-cyber-attacks/articleshow/54744534.cms.

[10] "'India Sees 375 Cyberattacks Everyday,'" *The Hindu*, November 17, 2020, sec. Business, https://www.thehindu.com/business/india-sees-375-cyberattacks-everyday/article33110725.ece.

Data Localization

While Indian laws do not per se define 'data sovereignty', India has been among the strong votaries of 'data localization' along with other Asian countries like Vietnam and Indonesia[11] even though the United States has forced a dialing down of the demand for such localization.[12] The proposed Personal Data Protection Bill of 2019 (PDP) requires all "critical personal data" to be stored locally (Section 33). The Bill at present does not define critical personal data, subjecting it instead, to Central Government notifications. RBI guidelines already mandated sensitive information to be stored locally in 2018.[13]

On its own, no Indian statute defines 'data localization'. But in a general sense, the term may be understood as "government requirements that control the storage and flow of data to keep it within a particular jurisdiction.[14]" Data localization laws are also often alternatively understood to denote 'data sovereignty' itself[15] since they denote both, the ability of a government to store and access data locally.

Cross-Border Data Access

Different countries have different standards when it comes to cross-border sharing of data. Jurisdictions such as the EU can be particularly strict about allowing access to user information, requiring that the country making the request have a strong data protection regime in place, of its own. This can prove to be a challenge for countries like India which have data protection provisions scattered across multiple legislations in various sectors. India's own stand on data access to external agencies is rather unclear even in the new Bill introduced in 2019[16].

As it happens, India is also not party to any of the direct access agreements that are being negotiated between some countries- particularly in Europe and North America, leaving it out

[11]Arindrajit Basu, Elonnai Hickok, and Aditya Singh Chawla,"The-Localisation-Gambit.Pdf," accessed December 31, 2020, https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf.

[12] Arindrajit Basu, "The Retreat of the Data Localization Brigade: India, Indonesia and Vietnam," accessed December 31, 2020, https://thediplomat.com/2020/01/the-retreat-of-the-data-localization-brigade-india-indonesia-and-vietnam/.

[13]Bavadharini KS, "All You Wanted to Know about Data Localisation," @businessline, accessed December 31, 2020, https://www.thehindubusinessline.com/opinion/columns/slate/all-you-wanted-to-know-about-data-localisation/article25363062.ece.

[14] Internet Society, "Internet Way of Networking Use Case: Data Localization," *Data Localisation* (blog), September 2020, http://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/use-case-data-localization/.

[15] Ibid.

[16] Smriti Parsheera Jha Prateek, "Cross-Border Data Access for Law Enforcement: What Are India's Strategic Options?," Carnegie India, accessed December 31, 2020, https://carnegieindia.org/2020/11/23/cross-border-data-access-for-law-enforcement-what-are-india-s-strategic-options-pub-83197.

of the simpler modes of accessing data for criminal investigations. It has to rely instead on the much slower and less simple Mutual Legal Assistance Treaties or MLATs which can take up to 10 months of processing time.[17] Indeed, India's unofficially cited reasons for not being a part of an agreement like the Budapest Convention include concerns around its sovereignty.[18]

CONCERNS SURROUNDING INDIA'S DATA SECURITY

China's presence in India Tech

While it has been evident for some time now, the recent clashes with China at the Line of Actual Control have made the possibility of China's targeting of India's critical infrastructure more imminent than ever before. Add to this the fact that the Chinese invest heavily in Indian technological start-ups[19] and have a large consumer base for their products and it becomes evident that India also faces a high level of risk of Chinese espionage activities that pose a larger regional security threat. Indeed, some of the banned Chinese apps such as Smart App Lock demanded highly intrusive access to users' location, fingerprint and network usage history.[20] The access to biometric data is particularly worrisome given the ways in which it may be used to profile users.

A recent three-part series of articles on Foreign Policy have also shed light on the extremely sophisticated network of China's intelligence units and their workings vis-à-vis the United States. With India-US ties getting stronger, India is already likely to have been exposed to considerable Chinese surveillance. The challenge before India therefore, is to firewall key strategic sectors to Chinese presence since it cannot forego the economic relationship with latter altogether.

India's absence from international frameworks

As indicated earlier, India is not a party to the Budapest Convention although it also hasn't officially outlined its position on why it finds it necessary to keep away from the arrangement. It is also not a party to the ongoing plurilateral negotiations on e-commerce under the aegis of the WTO (World Trade Organisation) which could very well see the conclusion of provisions relating to data security.[21] Given the growth of the e-commerce sector and the country's sheer market size, India choosing to stay away from the negotiations implies that if it were to decide

[17] Ibid

[18] Alexander Seger, "India and the Budapest Convention: Why Not?," ORF, accessed December 31, 2020, https://www.orfonline.org/expert-speak/india-and-the-budapest-convention-why-not/.

[19] Trisha Ray and Akhil Deo, Note 4.

[20] Utsav Mittal, Note 8.

[21]D. Ravi Kanth, "India Boycotts 'Osaka Track' at G20 Summit," mint, June 30, 2019, https://www.livemint.com/news/world/india-boycotts-osaka-track-at-g20-summit-1561897592466.html.

to become party to the outcome of such negotiations, it will have to abide by the terms set by other countries.

At the same time, while the ASEAN[22] nations have come out with a framework on Digital Data Governance which regulates data localization and promotes domestic oversight over data, India is not a party to any such regional arrangement governing data flows nor has it initiated negotiations on the matter. Of course, part of the reason for India's immobility is also a generally defunct character of the SAARC[23]. But India's own Act East policy has evidently not included within its purview, questions surrounding data governance.

Pitfalls of excess regulation

It has been evident for some time now that India's growth is going to be digitally driven. Indeed, this has been recognized by the government itself when it launched the Digital India program and initiated the use of Aadhar for delivery of services, among other things.[24]

India's own homegrown businesses too, have quickly adapted to the changing business environment in which internet and data has become an imperative-be artificial intelligence or data labelling.[25] India's growth story on the whole, has been propelled by the services sector which, in the presence of excessive regulation and intrusive government demands for data access, will suffer considerably in its day-to-day operations.

Moreover, there are concerns that excess constraints over the use of Internet are likely to diminish its value to users as an efficient network "allowing people everywhere the widest range of opportunities.[26]" It is only in authoritarian models such as Russia and China that a tightly regulated Internet including restrictions on "in transit data"[27] along nationalistic lines can hope to survive.

POLICY RECOMMENDATIONS

No recommendation on any issue concerning India's national security can proceed without addressing the elephant in the room-a lack of overarching defense strategy or a White Paper as is commonly published by other global powers.[28] Even China's authoritarian ruling party known for its opacity has managed to articulate the country's position on matters of national

[22] Association of Southeast Asian Nations.

[23] South Asian Association for Regional Cooperation.

[24] White Paper on Data Protection, Note 5.

[25] Trisha Ray and Akhil Deo Note 4.

[26] Note 14.

[27] Ibid.

[28] M. k Narayanan, "The Missing Piece in India's Defence Jigsaw Puzzle," *The Hindu*, February 20, 2020, sec. Lead, https://www.thehindu.com/opinion/lead/the-missing-piece-in-indias-defence-jigsaw-puzzle/article30863880.ece.

security ranging from piracy to nuclear non-proliferation to cyber security.[29] Its position on what it considers to be its core national interests, howsoever contradictory to International Law is at least recorded.

For India to proceed to data governance in the realm of security it must first clearly articulate its overall conception of national security and clearly state the red lines that it expects to be respected.

On the specific issue of cyber security a number of propositions have been advanced both, by former members of the defense established affiliated to defense-centric think tanks and industry bodies such as the Data Security Council of India.[30] The first of course is the need for a comprehensive strategy for cyber security. With over 76 countries having already published their cyber-security policies, India is already behind the curve on that front. On the upside, it now has plenty of references to come up with a strategy that is customized to suit domestic demand and can be implemented effectively.

Some of the policy suggestions in this regard include provision of a greater role for India's private sector in managing cyber-security infrastructure; reducing dependence on foreign technologies (the pitfalls of which have already been outlined above); and providing for an implementing authority whose role and powers are clearly defined. It is also important that India demonstrate the gumption to respond to cyber-attacks so that the strategy does not look like a soft policy instrument but as a legal position on the back of which the Indian government would be willing respond to any 'use of force' in the cyberspace.

Finally, if Digital India is to drive India's future growth, then the country cannot afford to abdicate individual rights in the domain of privacy in favor of unfettered access to state authorities in the name of national security. At the very least, an independent authority with security of tenure in order to grant approval to data access is a policy imperative for any effective architecture on data security to survive.

CONCLUSION

On technology, India has very little time to catch up with the world despite the pandemic-induced slump. The future of global power today, largely rests on the ability to develop and control critically important technologies and despite the calls for self-reliance, India has a long way to go, not only in terms of indigenization but also in terms of adopting a legal framework

[29] "China's New 2019 Defense White Paper," accessed December 31, 2020, https://www.csis.org/analysis/chinas-new-2019-defense-white-paper.

[30] Maj Gen P. K. Mallick, "India's National Cyber Security Strategy : How to Go About It – Center For Land Warfare Studies (CLAWS)," accessed December 31, 2020, https://www.claws.in/publication/indias-national-cyber-security-strategy-how-to-go-about-it/.

"National Cyber Security Strategy 2020 DSCI Submission.Pdf," accessed December 31, 2020, https://www.dsci.in/sites/default/files/documents/resource_centre/National%20Cyber%20Security%20Strategy%202020%20DSCI%20submission.pdf.

that can both, enhance its security prerogatives as well as protect individual rights in the digital space.

This brief looked at the broad range of issues surrounding India's data security structures and the possible solutions to some of the more outstanding problems that pertain to data governance in the country. In themselves however, these issues-be it data sovereignty; or data sharing and access; or the conversation around 5G, are rather complex and have attracted independent analysis from technology and cyber policy experts. For India to get its data governance right, it is crucial that its lawmakers cover the nuances so that a cohesive, clear and compliance-friendly architecture can emerge.