P: ISSN NO.: 2321-290X RNI : UPBIL/2013/55327 VOL-6* ISSUE-9* May- 2019
E: ISSN NO.: 2349-980X **Shrinkhla Ek Shodhparak Vaicharik Patrika**

Data Security and Data Localisation in The Context of India's National Security

A.M. Tripathi
Associate Professor & Head,
Deptt. of Defence Studies,
K.G.K College,
Moradabad, U.P., India

Abstract

Nowadays, the cyberspace is a focal domain that has great potential for good or an equal potential for immense destruction. Data threats can manifest in many ways and affect millions of people through cybercrimes, data theft, and data breaches. There is an even greater danger if hostile powers target our critical infrastructure like communication links, transportation, energy and financial institutions, literally bringing the country to a halt. Hence, Data Security is very important for India's National Security. Dealing with this threat will require robust countermeasures, major challenge lies in the use of social media as a weaponised platform.

This is a form of warfare that does not require any use of force, and due to its nature, can continue to be pursued even during peace. Tracing the source of the attack is not easy, and we can neither be sure about the exact capability of the adversary nor accurately assess our chances of success if we launch a cyber counterstrike. Notwithstanding these limitations, we must have a clearly stated policy.

The dangers to our social fabric and our Nation are absolutely clear, and it is well known that our laws can only be enforced in our territorial jurisdiction. These are the primary drivers that automatically point us towards adopting a data localisation policy. The enormous economic potential that can accrue by utilisation of this data gives an added impetus to adopt such a policy.

Keywords: Data Security, Data Localisation, National Security, Data Breaches, Right to Privacy.

Introduction

In today's world, privacy is security. To protect ourselves, we need to take steps to protect our privacy and the security of our data. In August, 2017, the Supreme Court of India recognised that there exists a Fundamental Right to Privacy under the Indian Constitution (Puttaswamy v. Union of India, 2017). The Court, in a wide ranging declaratory judgment, found privacy to be an integral component of numerous fundamental rights, notably rights to equality (Articles 14-18), speech and expression (Articles 19(1)(a)), and the protection of life and liberty (Article 21). While recognising that the right could have multiple facets (informational privacy, freedom from unwarranted stimuli, autonomy to take decisions, etc.), the court noted, that as with other fundamental rights, the right to privacy is not an absolute right, and can be restricted on certain overriding grounds. However, there was consensus on the point that any interference in the right to privacy should satisfy the requirement of a "fair, just and reasonable" procedure established by law.[1]

Importance of Data Security

Data security is the process of securing any data. It is also termed as information or IT Security. Data can be secured using numerous software and hardware technologies. Encryption, antivirus, firewalls, two-factor authentication, software patches, updates, etc. are some tools that can be used for this purpose. There have been many data security scares in the headlines over the past few years. Companies around the world have been victims to hacks and data breaches and have had customer information compromised. There is a common misconception that only the big organizations, governments, and businesses get targeted by cyber-perpetrators. Data security is important for businesses, governments and common users who get targeted equally by attackers for their sensitive information, such as their credit card details, banking details, passwords, etc.

Data security should be thorough and seamless for everyone, irrespective of whether you are an individual or a business. According to estimates by the Center for Strategic and International Studies, cybercrimes cost the global economy over 400 billion USD per year. Undoubtedly, data breaches and cyber-attacks have increased in due time as computer networks are getting bigger and better every day. A report revealed that hackers made over one trillion cyber attack attempts within a year. Automated attacks are consistently being initiated without the hacker having to lift a finger. Researchers have predicted that "burst bot attacks" will be the fastest growing type of cyber attack in coming years.[2]

Data Localisation

Localisation generally refers to requirements for the physical storage of data within a country's national boundaries although it is sometimes used more broadly to mean any restrictions on cross border data flows. There's a massive explosion in data being generated by connected internet users in India and data breaches are an unfortunate consequence of it.

According to a report by real estate and infrastructure consultancy Cushman and Wakefield, the size of the digital population in India presents a huge potential demand for data centre infrastructure. Digital data in India was around 40,000 petabytes in 2010; it is likely to shoot up to 2.3 million petabytes by 2020 — twice as fast as the global rate. If India houses all this data, it will become the second-largest investor in the data centre market and the fifth-largest data centre market by 2050, the consultancy has forecast.[3]

Due to the transient and pervasive nature of data on the internet, its security is constantly threatened and indeed been breached at several instances. Data localization is a measure adopted to give countries increased control over the data belonging to their citizens and residents in the interest of enforcing data protection regime set by the country and to secure the critical interests of the nation state. This is achieved by encumbering the transfer of data across national borders – including through rules preventing transmission of data outside the country, requiring a copy of the data to be stored within the country or tax on export of data, and enforcing applicable laws of the country vis-à-vis data security.

Objective of The Study

The objective of this study is to asses the emerging challenges in the field of Data Security and its impact on India's National Security. Also to determine the efficacy of Data Localisation in this context. This paper classifies the arguments around data localisation into three broad categories - the civil liberties perspective; the government functions perspective and the economic perspective. We examine the likely costs and benefits under each of these heads and come to the conclusion that it would be premature to adopt any sweeping localisation norms in India. At the same time, India must not will away its ability to adopt such measures in future by agreeing to sweeping 'free flow of data' provisions in trade agreements. The identification of cases where narrowly tailored localisation requirements might be an appropriate response should be done through a transparent and consultative process. Where an assessment of the overall costs and benefits justifies a case for localisation, it should be adopted in its least intrusive form.

Review of Literature

Data Scandals and Breaches across the World

A major political scandal in early 2018 was the Facebook-Cambridge Analytica scandal. It was revealed that Cambridge Analytica had harvested the personal data of millions of people's Facebook profiles without their consent and used it for political purposes. It has been described as a watershed moment in the public understanding of personal data and precipitated a massive fall in Facebook's stock price and calls for tighter regulation of tech companies' use of data.

Harry Davies, a journalist for "The Guardian" was the first to report the illicit harvesting of personal data by Cambridge Analytica. He alleged that Cambridge Analytica was working for United States Senator Ted Cruz and harvesting data from millions of people's Facebook profiles without any consent. Further reports followed in the Swiss publication 'Das Magazin' by Hannes Grasseger and Mikael Krogerus, Carole Cadwalladr in The Guardian and Matthias Schwartz in The Intercept.

The scandal erupted in March 2018 with the emergence of a whistleblower, Christopher Wylie, an ex-Cambridge Analytica employee. Three news organisations published simultaneously on March 17, 2018, and caused a huge public outcry. More than $100 billion was knocked off Facebook's share price in days and politicians in the US and UK demanded answers from Facebook CEO Mark Zuckerberg. The scandal eventually led to him agreeing to testify in front of the United States Congress.

The scandal was significant for inciting public discussion on ethical standards for social media companies, political consulting organizations, and politicians. Consumer advocates called for greater consumer protection in online media and the right to privacy as well as curbs on misinformation and propaganda. This scandal ignited the debate on data security across the world.

In September 2016, the once dominant Internet giant Yahoo, while in negotiations to sell itself to Verizon, announced it had been the victim of the biggest data breach in history, likely by "a state-sponsored actor," in 2014. The attack compromised the real names, email addresses, dates of birth and telephone numbers of 500 million users.

The online auction giant, ebay, reported a cyberattack in May 2014 that it said exposed names, addresses, dates of birth and encrypted passwords of all of its 145 million users. The company said hackers got into the company network using the credentials of three corporate employees, and had complete inside access for 229 days, during which time they were able to make their way to the user database. In late 2016, Uber learned that two hackers were able to get names, email addresses, and mobile phone numbers of 57 million

users of the Uber app. They also got the driver license numbers of 600,000 Uber drivers.

Breaches in India

In 2016, 3.2 million debit cards were compromised in what emerged as one of the biggest ever breaches of financial data in India. Several victims reported unauthorised usage from locations in China. Of the cards, 2.6 million were said to be on the Visa and Master-Card platform and 600,000 on the RuPay platform. The worst-hit of the card-issuing banks were State Bank of India, HDFC Bank, ICICI Bank, YES Bank and Axis Bank.[4] The breach was said to have originated in malware introduced in systems of Hitachi Payment Services, enabling fraudsters to steal information allowing them to steal funds. Hitachi provides ATM, point of sale (PoS) and other services in India.

In Feb, 2018, Cyber Security firm, Cloudsek, found details of over 10,000 credit and debit cards of customers of the embattled Punjab National Bank up for sale for $ 4-5 per card on the internet for the last three months. The country's second largest public sector bank blocked the cards soon after the breach was reported by Cloudsek. These breaches point us towards adopting a clearly data localisation policy to have proper monetering and control of data.

Data Localisation Debate in India

Data Localisation has become one of the most debated subjects in India in light of recent policy moves towards the localisation of payment sector data and personal data. Yet, this is not a debate that is entirely new, or even unique, to India. Equally, it's not a debate that can be understood in isolation. Calls for localisation must be placed in the broader context of the growing economic, strategic and political relevance of the digital economy and ensuing demands for State control and "sovereignty" in this space. Demands for increased regulation are also playing out in other fields like data protection, cyber security, surveillance, digital taxation and platform regulation, with localisation often seen as a tool to assert control in these other areas. This motivates a deeper exploration of the justifications and challenges of data localisation.[5]

Recent Developments in Data Security Policy in The Context of India

There have been major policy decisions, bills and judiciary decision in this regard in the last few years. Firstly, in August, 2017, the Supreme Court of India recognised that there exists a fundamental right to privacy under the Indian Constitution (Puttaswamy v. Union of India, 2017). The second was the issuance of the draft Digital Information Security in Healthcare Act, 2018 (DISHA) published by the Government of India on 21 March 2018, which seeks to empower the proposed National Electronic Health Authority to impose localisation requirements with respect to digital health data. The draft statute itself, however, does not mandate localisation of data.

A recent report issued by the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna and the Personal Data Protection Bill, 2018 have set the topic sizzling in India again. The Data Protection Bill presently proposes (a) all personal data to which the law applies must have at least one serving copy stored in India, (b) in respect of certain categories of personal data that are critical to the nation's interests, a mandate is intended to be made to store and process such personal data only in India such that no transfer abroad is permitted, and (c) the Central Government will be vested with the power to exempt transfers on the basis of strategic or practical considerations. This article seeks to understand the various arguments extended by the proponents and opponents of 'data localization' with the aim to understand the implications of the provisions on restrictions on cross-border transfer of personal data proposed under the Data Protection Bill.

The Reserve Bank of India (RBI) issued a directive on 6 April, 2018 imposing stringent data localisation requirements on all players in the Indian payments ecosystem. The directive, simply put, requires all payment system providers and their suppliers and intermediaries to store the entire data related to payment transactions only in India.[6]

The aim of this data localisation move is, as the directive explains, to ensure "better monitoring" and "unfettered supervisory access" to data stored with payment system providers. The directive creates obligations for payment processors to maintain 'full end-to-end transaction details', 'payment instructions' and other information collected, processed, carried in India within the country. This claim overlooks the fact that the central bank retains access by requiring payment processors to store a superset of all transactions data processed by them which is at all times available to RBI. This is equally true for both a centralised domestic payment network like Unified Payments Interface (UPI) used by PhonePe and PayTm, and foreign card networks or banks in India, like Visa, Mastercard and American Express.

When data is held in other jurisdictions, officials depend on the mutual legal assistance treaties (MLATs) processes to obtain access. The MLAT process has been envisaged as a cooperation mechanism of criminal investigations by law enforcement agencies (LEAs) in exceptional circumstances. Over a period of time, MLATs have proven to be ill-suited to handle large number of requests or provide immediate or time-bound access to critical information. Hence, India's law enforcement agencies security agencies are backing the RBI's push for data localisation citing difficulties in carrying out cross-border probes, investigative and intelligence agencies' are of the firm view that "the practice of what they referred to as colonisation of Indian data has to end due to national security concerns that are getting sharpened amid the government's growing push for Digital India".

Also, the Directive also does not appear to have taken into account the fact that most financial entities maintain their data in an encrypted form. The RBI itself requires banks and other entities to utilise 128-bit encryption to se-cure online communications and to protect sensitive personal data while at rest.

Similarly, the National Payments Corporation of India also mandates the use of encryption to store customer data. Encryption renders the data illegible without assistance from the relevant payment entity or a significant effort being made to crack the encryption. Given that the premise behind mandatory localisation of data is to ensure unfettered supervisory access to the data, the Directive fails to consider that regulatory authorities will still have to request the payment entity to decrypt the data, in line with legal processes, before it can be accessed and used. Therefore, the RBI would presumably still need to follow other processes to ensure "unfettered supervisory access" to the data, even though it may be stored in the country. This highlights the shortcoming of imposing localisation requirements without considering the broader technological environment – merely mandating localisation is unlikely to meet the stated regulatory ends. Perhaps near real-time reporting requirements for certain kinds of data could have achieved the regulatory objective without micromanaging the exact location of the data.

Global Developments

In 2013 when Edward Snowden, a former contractor with CIA, leaked to the media details of extensive internet and phone surveillance by American intelligence agency, establishing border control provisions on the internet gained an impetus. China, Russia, Australia, Canada and several other countries have already adopted data localization provisions. In fact, Russia has already set an example of enforcement of its 'data border control' provisions against LinkedIn in 2016, and last year the Russian Data Protection Authority, Roskomnadzor, published its 2018 plans for conducting inspections of local companies' compliance with Russian privacy requirements including data localization requirement. The European Union's General Data Protection Regulation doesn't have a specific data regulation rule, only stressing that cross-border data movement can happen if the other country has stringent rules to secure information.

Many other countries have implemented various shades of data localisation. Nigeria requires all subscriber and consumer data of tech and telecom firms and government data to be located locally, since 2013. Germany mandates that telecom and internet service providers store data locally. Turkey requires banks and payment systems operators to have their information systems within the national territory, countries such as Australia prohibit personal electronic health information from being held or processed outside of the country.

In China, the broad data localization restrictions introduced since 2017 by the Cyber Security law and the subsequent regulations and rules cannot be easily categorized. The law requires that personal data and "important data" held by "critical information infrastructure operators" are stored within the country. Although the offshore processing of this data is not explicitly forbidden, international transfers are only allowed if there is a "genuine need for reasons of operational necessity" and they are subject to security assessments, prior regulatory approval and informed customer consent.[7]

Objectives and Side Effects of Data Localisation

India introduced data localization restrictions for a combination of public policy objectives. The protection of their citizens' personal data, the safeguarding of national security, and the access to data for regulatory supervision or law enforcement purposes are generally the most claimed reasons. However, other more underlying goals may include economic protectionism, national sovereignty or even Government control (and surveillance) over the Internet. Below we discuss some of these intended goals as well as the negative side effects that data localization restrictions may have on a country's access to financial services and markets as well as for cyber security, risk management, fraud or financial crime.[8]

Personal Data Protection

The explosion in the collection and processing of personal data has raised concerns over the risks for consumers if their information is not adequately used by companies and safeguarded against potential security breaches. As a result, countries around the world are developing more comprehensive data protection regulations that set the legal basis for processing personal data, grant citizens certain rights over their own information (e.g. access, rectification or erasure) and introduce security and transparency obligations for data controllers and processors. In this context, it is not only legitimate but reasonable that governments aim to make sure that these protections are not weakened when their citizens' data is moved to foreign locations with different regulatory regimes and levels of protection. Therefore, some form of conditional restrictions to the international transfer of data may be necessary and are generally recognized and supported by financial institutions, who have a common interest to protect their clients' personal information. However, stricter, unconditional restrictions are hardly justifiable on the grounds of personal data protection.

National Security

On the one hand, access to sensitive information by foreign governments (or para-governmental institutions) can be a threat to national security. The sensitivity of a particular category or set of data is not only something relative, but increasingly difficult to assess given how new technologies such as Artificial Intelligence and Machine Learning can generate unforeseen insights from the combination of different sources of data. In some countries, government agencies might gain relatively easy access to any information stored within their territory, even if there is no a clear law enforcement justification. Therefore, it is reasonable that other governments aim to prevent the transfer of data to those countries that do not offer sufficient guarantees. However, as in the case of personal data protection, this can be achieved by making use of conditional and proportionate restrictions.[9]

On the other hand, but closely linked to the former, Governments regard some data processing centers and organizations, including financial

institutions, as critical infrastructures for their national security and sovereignty. Certainly, the interruption of some data processing and networking activities — such as those linked to the provision of communication or financial services — can severely damage the functioning of a country, which justifies special resilience, recovery and continuity requirements for those infrastructures. However, it is questionable that requiring that those are located exclusively within the national territory makes them safer, particularly in the case of financial services, which are connected to the global economy.

Companies and organisations faced with localization restrictions may end up using local data processing services that are not best-in-class in cybersecurity — which is always a function of technical, financial, physical, and personnel resources — instead of global cloud-based solutions that may improve resilience and redundancy by relying on a distributed network of computing power. This means that, in cases where a natural or hostile government or hacktivist-engineered disaster disrupts the functioning and reliability of a local data center, workloads can be rebalanced to run on alternate data centers (e.g. in the case of natural disaster, located far away from it), and addressed quickly by provisioning readily-available resources. In addition, data localization restrictions hinder the sharing of information about cyber-incidents within a company and between industry peers and regulators. Timely access to relevant information is key to effectively responding to cyber-attacks, limiting their impact, as well as preventing future threats.

Regulatory Supervision and Law Enforcement

Supervising compliance with national laws and regulations, and enforcing them when necessary, requires that public authorities such as. financial supervisors, tax agencies, Anti-Money Laundering bodies or criminal prosecutors can obtain access to relevant data on citizens and corporations, under appropriate restrictions and safeguards that balance the rights of the data subjects. When that relevant information is located offshore, national public authorities fear that their capacity to access data may be weakened due to the territorial limit of their powers and potential discrepancies with the laws and authorities of the host countries. Legal access to data may ultimately depend on bilateral or multi-lateral international agreements that can restrict, delay or make costlier the access to information. Therefore, some countries see the requirement of a local copy of data as a way of ensuring that they keep full control over access to data for regulatory supervision or law enforcement.

This argument has been particularly relevant for a highly regulated industry such as financial services, subject to a number of different regulations (prudential, market integrity or AML/CFT) that are enforced through active ongoing supervision. As an example, the Reserve Bank of India (RBI) justified its recent data localization requirement for payment service providers on the grounds of “ensuring better monitoring of the growing and highly technology dependent payment ecosystem in the country.” In some jurisdictions, concerns are especially related to the monitoring of market activity by securities regulators, for instance if a small hedge fund stores data on a public cloud located outside of the country and the regulator needs information for an investigation into rogue trading practices. It is important to understand that modern methods of virtualized data storage mean that data is no longer physically stored such that an authority could seize it without assistance from the data controller. The cooperation of financial institutions and/or their vendors is always necessary for authorities to gain access to information, no matter where a data center is located. This means data localization is irrelevant from a technical perspective and only matters when, absent voluntary cooperation by an institution, authorities need to legally force it. For this, increased and improved cross-border cooperation and mutual assistance between authorities is necessary.

Introducing data localization restrictions instead is counterproductive precisely for some of the ultimate goals of regulatory supervision and law enforcement. By limiting the internal sharing of information across jurisdictions, data localization requirements may undermine the ability of financial institutions to have a “golden source of data” and comprehensive risk management systems, for example, if exposure to international clients cannot be aggregated across borders. Similarly, data silos may result in suspicious activities not being identified in a timely manner, or missed altogether, undermining the prevention of and reaction to cyber-attacks, fraud, money laundering or terrorist financing. It is also worth considering whether the supervision of those global institutions may also be affected if the competent authorities in the different jurisdictions where the firms operate cannot share timely and detailed information between them.

Economic Protectionism

Finally, but not least important, some countries introduce strict data localization restrictions with the aim of developing or boosting their national Information Technology sectors. The political argument is quite simple: if companies are required to locally store and process data, they (and/or their service providers) will have to invest in servers and data centers located within the country, which will generate economic activity, employment opportunities and other spillovers associated with high-tech sectors. However, as it is always the case with international trade barriers, the economic consequences are complex and not at all straightforward. Companies may be forced to use local data processing solutions that are less efficient than those available abroad, such as public cloud solutions that leverage greater economies of scale and provide more flexibility. The increased data processing costs will likely be passed on to other companies and in the end, to consumers in the form of higher prices, or even reduced access to services if some data-intensive ones are no longer viable. As argued by the OECD, restrictive data localization requirements “affect firms’ ability to adopt the most efficient technologies, influence investment and employment decisions, increase the cost of

innovation and lead to missed business opportunities." [11]

The impact may be particularly negative for the attractiveness of a country for multinational corporations, including financial institutions. Data localization restrictions reduce their ability to benefit from scale-related efficiency gains, make more complex the already difficult task of managing IT infrastructures and data repositories across a global organization, complicate the servicing of clients with presence in multiple geographies, such as in corporate and investment banking, and limit the possibility of combining different sources of data to extract value with artificial intelligence techniques. As a consequence, financial institutions might take a step back in countries that introduce burdensome data localization restrictions, and local economies may lose or have reduced access to global financial services and markets.

It is true that data localization restrictions may reduce competition for local companies, but they will also be less prepared to compete internationally if they cannot access state-of-the-art, more efficient global technologies, as well as financial services and other intermediary inputs.

Conclusion

Some of the aforementioned public policy goals are not only reasonable but desirable: protecting personal data against breaches or inappropriate uses, preserving national security interests or ensuring access to data for regulatory supervision and law enforcement purposes. However, these objectives can be achieved through proportionate and conditional requirements that minimize the downside effects of data localization restrictions, such as increased exposure to cyber threats and reduced ability to manage risks, including preventing and responding to fraud and financial crime. Ultimately, these downside effects have the potential to impact the stability and the integrity of the financial system.

Following an assessment of every perspective we find that the costs of introducing broad and sweeping data localisation norms are likely to outweigh its benefits, from a rights-based perspective as well as an economic one. Yet, this is not to suggest that data localisation can never qualify as a justified measure. There may indeed be circumstances where local storage and even processing of the data can be justified, particularly on certain normative grounds.

To minimize the cross-border restrictions to the flow of data, international cooperation is essential, particularly to address the challenges related to privacy, security, regulatory supervision, and law enforcement. International cooperation is currently taking place, and should be reinforced, on three different fronts: trade agreements, which increasingly incorporate free flow of data provisions; cooperation agreements for regulatory supervision or law enforcement; and data protection and privacy, with the mutual recognition of national standards or the development of specific cross-border frameworks. Since free-flow-of-data provisions in trade agreements are always limited by the prevalence of other public policy goals, such as the privacy of individuals or the access to information for law enforcement, those three fronts of international cooperation are necessarily complementary.

References

1. *Bhandari, V., Kak, A., Parsheera, S. & Rahman, F. (2017). An analysis of puttaswamy: The Supreme Court's Privacy Verdict. The Leap Blog. Retrieved from https://blog.theleapjournal.org/2017/09/an-analysis-of-puttaswamysupreme.html*
2. *Ahmed, U. & Chander, A. (2016). Information goes global: Protecting privacy, security, and the new economy in a world of cross-border data flows. UC Davis Legal Studies Research Paper Series Research Paper No. 480. Retrieved from http://ssrn.com/abstract=2731888*
3. *Cushman & Wakefield. (2016). Data center risk index. Cushman & Wakefield. Retrieved from http : / / www . cushmanwakefield . com / en / research - and - insight/2016/data-centre-risk-index-2016*
4. *Saloni Shukla (2016). The Economic Times. Retrieved From https://economictimes.indiatimes.com/industry/banking/finance/banking/3-2-million-debit-cards-compromised-sbi-hdfc-bank-icici-yes-bank-and-axis-worst-hit/articleshow/54945561.cms*
5. *Cohen, B., Hall, B. & Wood, C. (2017). Data localisation laws and their impact on privacy, data security and the global economy. Antitrust, Vol. 32, No. 1, Fall. Retrieved from https://www.americanbar.org/content/dam/aba/publications/antitrust magazine/anti fall2017 cohen.authcheckdam.pdf*
6. *Hetavkar, N. (2018). RBI firm on data localisation; 80% of firms to comply by Oct 15 deadline. Business Standard. Retrieved from https://www.businessstandard.com/article/economy-policy/rbi-firm-on-data-localisation-80-offirms-to-comply-by-oct-15-deadline-118101101302 1.html*
7. *Chin, M., Goodell, A., Liu, C. & Zhang, X. (2018). China's cybersecurity law. Reed Smith. Retrieved from https://www.reedsmith.com/ - /media/files/perspectives/2018/chinas-cybersecurity-law-002.pdf*
8. *Ashi Bhat, Suneeth Katarki. (2018). The Debate – Data Localization And Its Efficacy. Retrieved http://www.mondaq.com/india/x/736934/Data+Protection+Privacy/The+Debate+Data+Localization+And+Its+Efficacy*
9. *Ferracane, M. F. (2017). Restrictions on cross-border data flows: A taxonomy. European Centre for International Political Economy. Retrieved from http:// ecipe.org/publications/restrictions-to-cross-border-data-flows-a-taxonomy/ ?chapter=3*
10. *India's National Security Strategy, retd. Gen. Hooda, March 2019. Public document published by INC in April 2019.*
11. *Rahul Sachitanand. (2018). All about India's data localisation policy. The Economic Times. https://economictimes.indiatimes.com/tech/ites/all-about-indias-data-localisation-policy/articleshow/66297596.cms*