DATA -A SEA OF POSSIBILITIES AND A MIRAGE OF LEGAL CHALLENGES

Garima[*]

Salil Tripathy[**]

Abstract

The new oil and wealth in the current age is nothing else but data. The recent outcry for changes in India's data policy which is still in its formation stages aims at the transformation from data colonisation to data localisation and leading to data empowerment. The traditional ways of ensuring privacy are not adequate for a modernised technology of analytics like big data. This apprehension becomes more palpable as big data is a resource that can be used and reused. Data localisation becomes imperative due to the ever-growing threats of loss of private data to hackers or the same being misused by multinational companies when foreign storage solutions store it. What's more disturbing is that there's no segregation between personal and impersonal data done in big data which makes the ends of being anonymous open. It endangers the privacy of a user due to lack of access control management.

I. Introduction-A voyage to sea of data

INDIA A land of opportunities, it has always been the origin and abode of noble thoughts and ideas which disseminated into the world by some equally generous persons like Buddha and the highly revered *Gurus*. While in this era of technological evolvement, the conceptions in the virtual

[*] 5th Year, B.A. LL.B. (Hons.), University School of Law and Legal Studies, Guru Gobind Singh Indraprastha University, Delhi.

[**] 5th Year, B.A. LL.B. (Hons.), University School of Law and Legal Studies, Guru Gobind Singh Indraprastha University, Delhi.

world and the data footprints have already manifested the impending possibilities for body corporate worldwide whereas the function of *Gurus* as the channel has been seamlessly taken over by the internet.

Moreover, the only divergence is currently from that of the ancient times in terms of the channel is the internet has become more of a troublesome position for Indians. In contrast, the former helped Indians and others alike. With the advent of the internet and it's excellent unprecedented penetration into the rural areas, it's high time we try to redesign the plan of action concerning the digital footprint of Indians, its access and restructure our policies to envisage the country's digital journey giving it a much-needed direction to mitigate any issues that may have emanated from it inadvertently.

The influence of the internet on the lives of Indians can be understood from the very fact that its country accounts for 12% of internet users globally.[1] Further, the report elucidates that more than half of the population is enjoying access to the internet in the country. This has also encouraged the above argument for change in policy and governance concerning data footprints to counter the challenges and bag the opportunities in these changing times of the internet.

The risks are imminent and become even more pertinent given the semi and neo literacy prevalent in Indian population dwindling with the escalated unfortunate occurrences of fake news, there seems to be a lot at stake when weighing it against the positive prospects' internet brings with it nonetheless.

The paper discusses the path from digital divide to digital dividend riding upon the new-fangled epoch of data on a journey set out in the quest of finding the perfect balance, after examining all possible roads even if taken by none yet.

II. India and the Internet- the Sea of Possibilities

When we say, we are a country of 1.3 people, and we also say a digital market that's as massive as this where everyone has its unique identity. The same character and the unique behavioural pattern which needs to be safeguarded by the government to negate the possibility of any manipulation or wrongful gain by some techno-savvy individuals or groups through data analytics

[1] Mary Meeker, *Internet Trends 2019*, Bond Cap, *available at:* https://www.bondcap.com/report/itr19/, (last visited on May 1 2020).

and data breach. The *status quo* of Aadhar is linked with 877 million bank accounts which on the hindsight increases the benefits of direct money transfer from various government schemes and the transactional efficiency by eliminating the leakages.[2] However, many eyebrows rose in anticipation of a privacy breach and the apprehension of the database being a soft target for sophisticated cyber hackers and threats likewise.

The other prominent change that has come in India is in the transformation from cash or physical currency to hard money and from physical transactions to digital wallets. More so, India has a different array of multi-party payment systems like Google pay, Amazon pay, Phone pay, free charge, Paytm, Bharat Pay. This was unique in the fact that other countries have a monopoly of two or three players. Still, due to the efforts of National Pay Corporation of India (NPCI) and with the launch of UPI platform, it has strengthened this position. The platform recorded exceeded 1 billion marks this October.[3] Hence, the more significant issue is the transactions over these digital platforms also create a bulk amount of data. Even if it's hard cash like credit or debit cards, the payment intermediaries or agents store the data outside the country. So it puts sensitive data of millions of Indians transacting everyday vulnerable to data breach and severe privacy issues.

When we provide information or any sort of login credentials or social security, our data or our information is travelling at every kind of analytics, and we never know when it gets intercalated in others computer and is the most significant privacy issue which is faced by those practising the dark arts of big data analytics.

The United nation global pulse was an initiative done by the united nation for promoting big data for sustainable development as well as humanitarian actions.[4] This initiative was basically for the collective wellbeing of every individual, and even if it was started for welfare, still the members who were on behalf of this initiative complained in the world economic forum in 2011 regarding

[2]"87.79 crore bank accounts linked to Aadhar: Government", *The Economic Times*, *available at* https://economictimes.indiatimes.com/news/politics-and-nation/16-65-crore-pan-87-79-crore-bank-accounts-linked-to-aadhaar-government/articleshow/63233043.cms?from=mdr (last visited on May 20, 2020).

3 *Google, Walmart drive UPI payments past 1-billion transaction mark in Oct,* Business-Standard, *available at:* https://www.business-standard.com/article/companies/google-walmart-drive-upi-payments-past-1-billion-transaction-mark-in-oct-119110101606_1.html, (last visited on May 1, 2019).

[4]*United Nations Global Plus, available at:* https://www.unglobalpulse.org/, (last visited on May 10, 2019).

the ethical issues and privacy of an individual. One of them was Kirkpatrick who complained that this data was only available to the private sector, and there was no full access to data. He reiterated that the private players are taking it and even hiding data with limited access which indirectly facilitates breach of privacy of an individual. He suggested the notion of 'data philanthropy' with regards to sharing big data generated in the private sector in support of development causes, humanitarian aid, or policy development.[5]

There is a concept in e-contract, *i.e*., browse-wrap which without informing the user takes their consent for having access to data. It does not require the express permission of the user for terms and conditions, and without the knowledge of the users, every click is being analysed. It echoes the grey area when it comes to informed consent in the times of big data. It is still unregulated and unclear whether users' approval or non-approval or even the hidden consent is enough to justify using their data for research purposes and any other purpose even if for noble purposes. The rights that are inherent and provided by statutes can be analysed that these individual rights consist of four elements which are *viz.*, notice, Choice, Consent, Access. [6]

Notice and consent are tricky as big data target them. It is not accurate to state that at every occasion, there is a need for taking consent for using data. Still, also due diligence must be exercised by the body corporate while using the big data that is obtained fairly and legally. On the other hand, many a time people don't read privacy policies because they are so significant and lengthy, which makes them avoid it. It's in the best interest of everyone if privacy policies should be in a brief and concise form so that people can read them in just a minute. Even after ensuring that, the question of the authenticity of such policies is a matter of concern. This is a burning issue which needs to be addressed as soon as possible for the more significant benefit of society.

III Big data- A storm in the digital sea

Big data is defined as any data or any collection of data in huge size and in enormous volume, which is growing exponentially with time. This type of data is so vast and a labyrinth that none of the traditional data management tools can store it or process it efficiently. In routine life, this type of data is captured from various sites and various activities online that separate values from data,

[5] Annika Richterich, *The Big Data Agenda: Data Ethics and Critical Data Studies* (London: University of Westminster Press, 2018).
[6] *Davis* v. *United States*, 328 U.S 582 (1946).

enabling high-velocity capture, discovery and analysis". It can be in the form of structured and unstructured. Big data processing is complicated as traditional data processing applications are not enough. It is like standard data, but the difference comes in volume. In 2005 Roger Mougalas from O'Reilly Media coined the term big data for the first time, only a year after they created the term Web 2.0. It refers to a broad set of data that is almost impossible to manage and process using traditional business intelligence tools.[7]

Whenever we use any digital device, we are generating data, and that data is stored privately in our phone, which takes the shape of big data. Though it helps people in various ways by giving them some hints regarding the likes and dislikes of people, there is some scepticism surrounding the size of big data runs in quite a lot of gigabytes. So, it's colossal in volume which makes it difficult to analyse it. As more and more social sites and networks start appearing, and the Web 2.0 creates motion, more and more data is created daily. The creative start-ups slowly begin to dig into this massive amount of data, and even governments start working on big data projects. In 2009 the government decided to take an iris scan, fingerprint and photograph of all the 1.2 billion inhabitants. All these data are stored in the largest biometric database in the world. Some illustrations of Big Data are new stock exchanges which generate about one terabyte data per day regarding trade, other being Facebook and all other social networking platforms. The cue for such data is mainly produced from activities such as photo and video uploads, message exchanges, putting up comments etc.

The bigger the data is, the bigger the threat it inflicts, and the extent of the detrimental impact it causes is enormous. The adverse bearing is reflected in the field of confidential data, transparency and privacy of an individual. Meanwhile, these aspects have been projected as a trail in helping the economy, but the privacy of an individual is shelved. Is big data indispensable in the pursuit of the economic march that our citizens be deprived of their rights, and even if those are fundamental rights, how can it be treated secondary in this big data scenario? These questions need to be answered, and it is high time to think about our privacy.

[7] *A Short History of Big Data, available at:* https://datafloq.com/read/big-data-history/239, (last visited on May 20, 2020).

Big data is a kind of open data which can be accessed and exploited by organisations, governments, strangers and everyone alike in the world. The concept transcends from the fact that privacy and transparency as a principle applies not only to data as a product. It instead gets initiated to apply from the collection of data which is used or used by others in their research work and in other statistical issues which amounts to outright infringement of our privacy rights provided if due consent isn't obtained by legal means. The breach of right to privacy of a group somehow tantamount to infringing the rights of an individual since having similar ideas in terms of thoughts and its violation has an adverse impact on the wellbeing of an individual.

Freedom of speech, as well as the right to safety and privacy, have been underscored as rights and values countering individual privacy considerations. These all balancing acts, weighing individual rights against the public interest, are also characteristic of ethical debates concerning public health and surveillance. Some users are entirely clueless about how to protect or even use data securely, and hence, their data is vulnerable to be easily stolen. The need is to adopt a balanced approach concerning security and privacy. Even if a person has surfed the web for a little while yet his full personal information with the help of location and IP address can easily be tracked and revealing him and his data to the world. Generally, whenever any user wants to use any site, it is prompted by a pop up that they have to agree to the terms that their data can be used by companies and hence, are not having the leeway to use the services without providing their personal information. These practices have provoked several debates regarding biometrics and especially the messages that are being transferred on WhatsApp. It is entirely plausible that for the safety of the public and for combating terrorism, these steps have been taken. Still, there are grave concerns on the security and preservation of these data. These systems need to be transparent to build a credible system by gaining public confidence.

IV. Is the Sea of Data a High Sea? - Data Localisation

The RBI notification in April 2018 mandated payment service providers like *Visa, Amex* and *MasterCard* to ensure the entire data about payment must be stored in systems in India only.[8]

[8]*RBI, "Storage of Payment System Data"*, RBI, *available at:* https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0, (last visited on May 20, 2020).

However, this position retracted after India agreed to financial data transfer and foreign storage in negotiations held in Vietnam in late September this year of the commercial chapter for the agreement. They were thereby nullifying the notification partially.

On similar lines, Ministry Electronics and Information Technology has drafted the Personal data Protection Bill[9] and hence became the contact point. Apex body on matters related to data whereas the Ministry of Commerce and industry has designed the e-commerce policy where it advocates data localisation.[10] Hence, there seems to be some contradiction and lacks clarity with a standard procedure on data and for that matter data localisation in focus.

Closing the internet has never been a viable option as it would adversely affect the economy, and data localisation would also cost extra detrimentally concerning the business.

It is imperative to understand the fact that data localisation, when balanced with the concept of free internet, is done exceptionally well, only then the outcomes will be desirable for India. This can be achieved by proper coordination among the regulators of various nations under one umbrella treaty with clear demarcation to follow. The way forward lies in smart, sensible regulation and only regulation but nothing else.

The closed internet or limited data transfer is not economically viable in principle leave alone. It's practical implications. At the same time the idea of borderless data that has been carried from decades is fading with a belief of sovereign control of data with a specified territory to be a right possessed under the international law as another matter affecting its subjects this further got solidified with the rise in economic and geopolitical differences.

In the recent past, the Government of India has drafted and introduced several policies which stipulated that specific types of data must be stored in servers strategically stationed within the territory of India only. This diktat of localisation notifications has attracted a lot of criticism against the government and the regulatory bodies from all stakeholders such as civil society members, foreign investors, business houses and politicians among others who have categorically opposed this policy at all levels. At this point one has to understand all the dimensions of the data

[9]The Data Protection Bill, 2018, MeitY, *available at* : https://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill,2018.pdf, (last visited on May 20, 2020).
[10]*Draft National E-Commerce Policy,* DPIIT, *available at* https://dipp.gov.in/sites/default/files/DraftNational_e-commerce_Policy_23February2019.pdf, (last visited on May 5, 2020).

localisation and to begin with is the definition that it does provide legal limitation on the inability of data to be transported worldwide and hence, it's compelled to remain locally stored at local servers. There are different policy matters surrounding data localisation such as even if the data is transferred elsewhere it must leave a copy of the same in the source country, specific data are stipulated to be produced locally and cannot be outsourced. Also, this includes imposing strict terms and conditions on the transfer of data across borders.

The rights which have been recently established, such as the Right to be forgotten were introduced in Argentina and the EU, are closely related to the right to privacy. In a 2014 ruling, the Court of Justice of the European Union decided that 'individuals have the right – under certain conditions to ask search engines to remove links with personal information about them.' [11]

V. Data Protection and the present Legal Framework - An Indian Ship sinking in an Ocean of Data

In recent times the data consumption and usage have drastically increased rather exponentially. However, here it is important to note that unlike the west which has been reaping its benefits over a decade and its business models are based upon the purchasing parity of its population. The Indian market is new, and it's also pertinent to note that India's per capita income in the year 2018-19isRs, 1,26, 406 that's Rs 10,533 per month only, which is way below than 2,000 USD.[12]

Hence, the data footprint that is collected in the west can be analysed through data analytics to predict the purchasing patterns using big data and help in efficient advertising with more considerable influence on streamlined targets. It can't be said the same for India due to the underlying effect of poverty and illiteracy, which still holds back the significant chunk of the population. However, if data empowerment is emphasised upon to provide better healthcare and loans using data, then a lot of Indians and their small and medium enterprises can grow at a stellar rate. Though data protection through data localisation is an objective but going a step further

[11]European Commission (2014), *Google Spain SL, Google Inc*. v. *Agencia Española de Protección de Datos, Mario Costeja González Judgment* in case C-131/12, *available at:* https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf, (last visited on May 5, 2020).

[12]PTI *"India's per-capita income rises 10% to Rs 10,534 a month in FY19", The Times of India*, *available at:* https://timesofindia.indiatimes.com/business/india-business/indias-per-capita-income-rises-10-to-rs-10534-a-month-in-fy19/articleshow/69601770.cms, (last visited on May, 20, 2020).

endeavour must be to empower people rather than any government or private entities in a country like ours with vivid socio-economic classes. A blanket ban on data is not feasible but using the data for the benefit of individuals is always a viable option.

It is imperative to look at the statutory regulations that prevail concerning data protection in India and are in force since the data protection bill has been shelved for long. The enactments that presently govern directly or indirectly related to data protection and broadly on the principles of privacy are the Information Technology Act, 2000 (IT Act) and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules).

If any corporate body handles or has in its possession any data which can be termed as sensitive personal information like date of birth, medical records*, etc*. and it is revealed that such an entity is negligent in maintaining the same or fails to adopt adequate safeguard measures deliberately. Then under section 43A of the (Indian) Information Technology Act, 2000 the body corporate needs to pay reasonable compensation to the affected individuals who suffered huge losses due to unfair trade practices and breach of security. There is no bar to such payment that has to be paid and depends on the circumstances of each case differently.

Moreover, when a person gets access to any secured record, register, document. Book, correspondence, or any other information as may be conferred to him under the provision of the IT Act, he is expected to keep sensitive data secured. Hence, if any such confidential material is disclosed in the absence of the informed consent of the aggrieved individual or other words breach of privacy is caused by the person upon whom the access was provided. Then under the section 72 of the IT Act, he shall be liable with fine which may extend to INR 100,000 or with imprisonment for a term which may extend to two, or with both for the breach of privacy.

The inclusion of section 72 A in The IT Amendment Act, 2008 introduced a provision relating to disclosure of information intentionally and in full knowledge would invite imprisonment for a term extending to three years and fine extending to Rs. 5,00,000. This is applicable in the cases where any breach of contractual obligation takes place arising out of such disclosure which is made in the absence of legal consent from the concerned person. Thereby, we may conclude that any practice that is in derogation with the principle of data protection under the IT act can invite hefty

fines and possible imprisonment. Hence, both civil and criminal liabilities can be imposed under the IT Act.

However, the IT Act fails to accommodate the data processing phase while safeguarding the privacy of a person, and it lacks any specific provision regarding it.[13] In principle, the IT Act promulgates that data collection and processing must be legally undertaken to attain any lawfully sound purpose. However, the provisions in IT Act are limited to only the collection and use of data but misses out on processing of data. Hence, it has not adequately addressed the issue of the lawfulness of processing by any explicit provision.

The international enactments on the given subject like that of GDPR have not only included this aspect but also have recognised ethical issues such as data integrity, protection from unlawful processing, fairness, transparency, and accountability. As the principle of right to privacy has evolved with concepts like consent which is an integral part to it. However, the IT Act fails to define the terminology of consent and does not accommodate further the well-founded principles of International standards regarding the role of the data controller to regulate and monitor such consent. Further, the IT Act is also mum on child's consent.

The IT Act, in principle, covers internationally acclaimed rights such as the right to ratification and Right to be informed but not individually. However, it fails even to make a mention of the word Right.[14] Furthermore, principles such as right of access, right to restrict processing, right to erasure, right to data portability, right to object, rights about automated decision making and profiling is excluded from its purview. Though the IT act takes into consideration sensitive personal data that consists of biometric data, health records and sexual orientation,[15] hence, it can be said that security of confidential data is recognised in the present legal framework but is ineffective due to the vague and scattered provisions. The provisions also lack the inclusion of modern principles on data protection. The need of the hour is of a specific act such as the Personal Data Protection Act to help accommodate few additional safeguard measures like a data security officer, conducting privacy impact assessment and maintenance of records.

[13]Information Technology Act, 2000 s. 6.
[14]Information Technology Rules, 2011 r. 5(3), r. 5(6), r. 5 (7).
[15] *Id*., r. 4.

VI. The Justice Srikrishna Committee Report- An Anchor to a Sinking Ship

The recommendation made by the committee is majorly based upon three aspects that are imperative to data which are locating the boundaries of sensitive personal data, understanding data consent, and setting up of a data authority. Further, the concept of data localisation was dealt within the report. The committee was also of the view that recommendation when solidified as the law must only be prospectively applied.

The report recommends that personal data protection law will have the purview upon a personal data if any or all of the following functions such as use, shared, disclosed, collected or processing has been done in India. Furthermore, it also recommended that companies incorporated under the Indian law must be brought under its ambit. Hence, making them liable for all functions which may or may not have been processed within India or abroad. However, an exception was given to the Government of India for exempting such companies which may solely process the data of foreign nations who are presently residing outside.

The recommendations were also made in a stretch about data protection authority which was envisaged to be an independent regulatory body established for the effective implementation and enforcement of the personal data protection law. There was also mention of the constitution of an appellate for any further representation thereof against the orders of the body.

The recommendations also provided some relaxations for the government to exercise its power in furtherance of the objectives such as public safety and welfare, and it may process the data of the user without its explicit consent. However, the recommendations recognised the concept of consent and its significance as its lawful basis for the processing of personal data. The guidance also allowed for reasonable compensation to the user for any harm caused to her when the data processed without consent.

Furthermore, the recommendation enshrines the penalties as may be imposed in the occurrence of a violation to the data law to be fixed with an upper limit of a percentage of the worldwide turnover of the body corporate, the higher be considered in such a situation. The report efficiently defines

sensitive personal data to contain passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric and genetic data, and data that reveals transgender status, intersex status, caste, tribe, religious or political beliefs or affiliations of an individual. Lastly, the report also deals with cross border data transfers of personal data and offers to restrict it when critical data is involved. This is also popularly known as data localisation.[16]

VII. Policies, Notifications and Drafts Bills- A Quest for a Safe Harbour

In India at present, there are especially only four sectors in which data localisation specifications are mandated. These requirements are based upon the type of industry the data hovers upon such as in banking there was an RBI notification asking storage of payment system data to payment operating companies placed abroad such as *Amex, MasterCard and Visa*.

In telecom in 2017, the FDI policy had a mention of data localisation and the Unified access license and the Companies Act, 2013. The last but equally important policy matter relating to health care had mandated data localisation which dealt with the IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017 and the National M2M roadmap. If we look upon the timeline of events in 2017 and 2018, there are different instances where holistic, sector-oriented data localisation guidelines were tried to be introduced. These requirements categorised the data into groups. Hence, they were *viz.*, the draft e-commerce policy, Personal Data Protection Bill, 2018 and similar to them was the draft e-pharma regulations.

These policies as mentioned above carefully contemplate on the solutions of improved cyber security and safety, development in research and development for creating innovation, safeguarding Indians from foreign surveillance and thereby countering privacy concerns and eliminating any threats to national security. However, it's pertinent to note that the impact of such policy changes isn't limited only to one aspect like impacting national security. Still, it also leaves a mark upon other elements as well such as markets, international relations and individuals. Further, they even leave a deep impression on India's global and regional trade agreements. Hence, we must also reflect on these factors and take a conscious decision. Further, we must also take into

[16] Data protection committee, "Report on a free and fair digital economy; Protecting Privacy Empowering Indians (Ministry of Electronics and Information Technology), *available at:* https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last visited on Jul. 2, 2020).

note the possible implications of such a decision on digital trade where the General Agreement on Trade in Services (GATS) comes into play when negotiating with the powers like the US and the EU.

The Srikrishna Committee, the Bill and its provisions were opposed by most civil society organisations in India and abroad alike due to the generalised approach to data localisation as a blanket provision. Hence, it created many hues and cries at the international arena; companies like Facebook and Google were highly critical of such a decision. The politicians of countries like US Senators and few transnational groups such as US-India advocating free trade were also against India's stance on data localisation in its draft bills. They all cited the reason that for the global digital economy, it was necessary and would hinder that process of cross border transfer of data.

Another reason for MNCs complaining since they have to invest extra for costs incurred to comply with such provisions and store data at data centres in India if such a policy was successfully implemented. Hence, it was likely detrimental to their businesses.

The counter-narrative given by indigenous groups, civil society members, and politicians was that data localisation is the only remedy to free data from the Western world who still live upon the principle called 'data colonisation' and apprehending that it could be used to suppress the needs and voice of developing nations in recent future to come. Another argument that the Indian establishment relied upon was 'data sovereignty' wherein they and backed by other influential local companies such as Reliance that it should be the sole prerogative of a state with regards to its subject's data.

In these times when IT-BPM is booming providing high dividends when it boils down to the start-ups in the digital sector, there are some agencies like NASSCOM and Internet and Mobile Association of India (IAMAI). They have shown their reservations upon data localisation as according to them, it may slow down the growth in these sectors, adversely affecting the Indian economy. Their reservations are based on the reasoning that start-ups may not have adequate resources or capacity, making the compliance unviable for them due to the resulting upsurge in costs of doing so. On the contrary domestic players in the digital sector like *Paytm* and *Phone Pe*

believe that the data security of financial services would strengthen when the data is stored locally within the territory of India.

India isn't a country that has indulged in contemplation of data localisation, in the recent past, there are not less than 18 countries that have gone ahead in mandating data localisation but with varied levels of vigour and having different types of data in its ambit. Each model has a separate story and learning which might come handy for a newbie like India in this respect. There's only one issue that seems to be humongous standing tall that's of the openness and interconnection of the internet globally. However, in principle, a nation may assert the sovereignty of the data produced by its subjects. However, it still looks a distant dream where Indian corporations and the stakeholders control data locally given the fundamental nature of the internet.

The economic development of the nation and individual rights have acquired opposite poles and in every legislation, we provide exceptions with regards to integrity and security of the nation which deems right. However, we usually turn a blind eye towards human rights and as no attempts have been made to evaluate the study of various breaches in all such cases.

However, the justification behind every new policy matter kept on surveillance should be scrutinised under proper judicial supervision. It must also be mandated that the objective of such a policy matter needs to be clarified, the quality of the technology assessed in terms of its efficacy in achieving the concerned objects must be disclosed. The amount of intrusion and even its effect on the privacy sphere must be accounted for greater transparency.

VIII. Conclusion - A Mirage

The complexity of technology has for long assisted voices and also acted detrimental to the security of people. Still, it has been the way it is, which makes it unique and impactful. Also, this feature of the global interconnection of data flows has implications on the economy and political nuances which must be tailored accordingly for unique socio-political issues of the parent country implementing it. The Srikrishna Committee in his recommendations relied heavily upon the idea of upscaling an indigenous artificial intelligence ecosystem that would imbibe all such aspects like that of data localisation while assessing the prerequisites, then considering all possible consequences. The committee suggests that AI can be the key driver in economic growth and development, taking cues from strategies suggested by the Commerce Departments Task Force

and Niti Ayog. Also, they made a quick reference to the success of artificial intelligence in developed nations such as China and the US.

Moreover, the Srikrishna Committee white paper also recognised an unequal proportion of data is getting stored in the US, giving it an undue advantage. In contrast, the contrary can't be said right to the US. Further, the issue magnifies when we seek the alternative remedy which in turn is very slow and cumbersome due to the prevailing Mutual Legal Assistance Treaties process (MLATs) that assists Indian law enforcement agencies in requesting for data stored in the US.

The Srikrishna Committee made an important observation that localisation would help prevent and protect citizens of India against foreign surveillance as it stated that the data transmission by the undersea cable network from one country to another is subject to a plethora of risks emanating from external attack.

Further, the committee suggested for sector-based identification for data localisation rather than a blanket policy which may help gain benefit most from local storage than incurring extra costs and prove to be a loss affair. However, that localisation in that sector must be explicitly mandatory.

Another localisation which was suggested by the committee was based upon some conditions that must provide perquisites through being lenient must be developed. These conditions must give way for transfers to any jurisdiction of all kinds of data like countries in Latin America or EU. There are two vital factors identified by the committee. One is the equivalent privacy and security safeguards, meaning thereby, data transfer shall be allowed in those countries only where similar guarantees are upheld like those of India. For this to happen, India needs to initially enact a robust legal framework for keeping privacy and security protections at its core. The other approach was based upon the barter system where both nations amicably share data of Indian citizens when the authorities desire so and based upon some standard operating procedures.

Various new concepts have emerged with data localisation revolving on the core concept of making data a resident of India. Hence, when data with policies mandate its location in India evading the colonisation of developed nations, it came to be known as data nationalism with elements of nation and patriotism peeping into the umbrella issue of data protection and upholding privacy. Its pillars are based upon a national priority that is related to law enforcement, privacy, security which opposes the very idea of global internet in precise terms. The other thought that

runs parallel to the concept of data localisation is data exceptionalism that argues that territorial jurisdiction can be asserted over data since the territory is the foundation for any advocacy for localisation and not in isolation.

The basic premise of data localisation is the western world is banking upon the data produced in developing countries like India and using big data analytics to its best use for exploiting commercial opportunities and predicting consumer behaviour. This being an outright unethical act and always possessed a threat to data sovereignty and security over the data of its subjects. Hence, data localisation is imperative in such circumstances and precisely the cause of India's push. Therefore, the approach in which localisation will be enforced in India will determine how at least nationalism in data will pan out. The understanding of international agreements with various stakeholders and diplomatic obligations for free trade compels us to maintain a balanced view in which we must push for data localisation without compromising on our sovereignty but not go far enough to engage in excessive protectionism.