DATA SOVEREIGNTY: THE QUINTESSENTIAL MODEL FOR THE NEW WORLD ORDER

Aparajita Bhatt[*]

Abstract

The world is witnessing the start of a new world order. This new world order is expected to change the global operations as a result of the data-driven fast-technological advancements. Data, the new wealth, shall be even more precious now; and maintaining data governance and data sovereignty standards shall be even more challenging. This paper discusses the two most important global trends i.e. data governance and data sovereignty. The paper looks into the concept and significance of maintaining data sovereignty in the present challenging times, highlights the efforts of different nations to maintain data sovereignty requirements through legal lenses, identifies the shifting trend from digital colonialism to data sovereignty, discusses the threats of data extractivism, identifies sovereignty issues in the cloud and finally throws light on the Indian pursuit of data sovereignty, data governance and data localization. The paper argues that the new complex world order necessitates the digital ecosystem which is backed up by strong data sovereignty laws, while safeguarding fair competition and creating opportunities for the global digital trade to flourish.

Keywords*: data sovereignty, data localization, data colonialism, surveillance capitalism, data marketplace*

I. Introduction

WE ARE living in a data age rather than the data millennium! Two most important developments along with the discovery of data are its efficient governance and data sovereignty. Data governance and data sovereignty are relative concepts as data sovereignty cannot be achieved without proper data governance. The idea of data sovereignty conceptualizes that the data collected within the national borders from the data subjects or data

[*]Assistant Professor of Law, National Law University, Delhi.

owners is sovereign from outside control. The idea is that data has a national home.[1] It is subject to the laws and policies of the country within whose territorial limits it is collected and processed. Based on the concept of indigenous data sovereignty, it is the right of a nation to govern the collection, ownership, and application of its own data.[2] C Matthew Snipp (2016)[3] explains data sovereignty to mean managing information in a way that is consistent with the laws, practices and customs of the nation-state in which it is located. The recent appellate decision of the CJEU dismissing Facebook's appeal against the order made by Ireland's Data Protection Commissioner (hereinafter as DPC) suspending Facebook Ireland's transfer of data about European residents to the United States (hereinafter as US) is a recent example of how more and more countries are acknowledging the principle of data sovereignty.[4]

The sovereign nations reserve the right to adopt the data sovereignty requirement and put restrictions or prohibitions on the transfer of their data. As a consequence of this decision of CJEU, Facebook shall now have to store and process all the European users' data locally within Europe, and it can't be transferred to the US. This verdict of CJEU would go a long way to fortify the data sovereignty and data protection rights of the people of Europe. The European Union-United States Privacy Shield arrangement[5] which was evolved to protect cross-border transfer of personal data from the EU to the US has also been invalidated as a result of this judgment of the Court of Justice of the European Union.[6] The present times are witnessing a greater demand and call for indigenous data sovereignty which manifests the right of a nation to govern the collection, ownership and application of its own data.[7] In the present times of big data and its analysis by various state and non-state actors, it is imperative for nations to declare themselves as data sovereign entities where data shall be collected and governed as per their national governance structure. In India, recently the data sovereignty principle has started

---

[1] Sean Foley, "Data Sovereignty in the Cloud: the Nine-Step Solution", *available at:* https://www.cloudtp.com/doppler/data-sovereignty-in-the-cloud-the-nine-step-solution/ (last visited on March 18, 2021).

[2] Indigenous Data Sovereignty and Governance, *available at:* https://nni.arizona.edu/programs-projects/policy-analysis-research/indigenous-data-sovereignty-and-governance (last visited on March 17, 2021).

[3] C. Matthew Snipp, "What Does Data Sovereignty Imply-What Does it Look Like?", in Tahu Kukutai, John Taylor, Indigenous Data Sovereignty-Towards An Agenda, Australian National University Press, 2016

[4] *Data Protection Commissioner* v. *Facebook Ireland Limited and Maximillian Schrems*, *available at:* https://curia.europa.eu/juris/document/document.jsf;jsessionid=46E87F48268BA307E985E1680EC0677B?text=&docid=228677&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=9485381 (last visited on June 3, 2021).

[5] The EU-US Privacy Shield arrangement was passed under the Regulation 2016/679/EU of the European Parliament and of the Council of 27 April 2016.

[6] *Available at:* https://www.sap.com/documents/2020/08/2a0c01f7-a87d-0010-87a3-c30de2ffd8ff.html (last visited on June 3, 2021).

[7] International Indigenous Data Sovereignty IG, *available at:* https://www.rd-alliance.org/groups/international-indigenous-data-sovereignty-ig (last visited on March 17, 2021).

gaining importance and also being recognized under the newly framed IT Rules & policies and even the courts have started reflecting upon the need to maintain data sovereignty standards in the pursuit of protecting the data of the citizens. Data sovereignty has two elements: sovereignty in relation to control over data created within the territorial borders of a country; and sovereignty in relation to access to data stored in a foreign county. It includes the signing of executive agreements for foreign access to the data stored within the country. The US Cloud Act, 2018[8] has both elements of data sovereignty. Besides USA, many countries including Canada and Australia have framed their data governance laws to protect their data sovereignty. Hawaii and Sweden have undertaken similar initiatives to achieve data sovereignty. With all these developments around the globe in the field, it is evident that data sovereignty and data governance in the present times of insecure cyberspace is of supreme importance especially for developing nations like India. In the light of the developments in these nations, this paper seeks to analyse that to what extent India has been able to achieve data sovereignty and govern data most effectively. The basic premise drawn in this paper is that effective data governance by the state is concomitant to achieve and maintain data sovereignty. The paper discusses the shift from digital colonialism towards data sovereignty. Further, it discusses sovereignty issues in the cloud. Focussing on the need to maintain data sovereignty requirements by a state, the paper explains the Indian pursuit of data sovereignty requirements.

II From Digital Colonialism to Data Sovereignty

Digital colonialism is traditional colonialism revisited. Kimberly Anastácio (2016) holds that digital colonialism may be a new form of colonialism by deploying an internet model for the global periphery by the West.[9] Anastácio explains the paradox which lies at the heart of digital colonialism, that is, on the one hand, the Internet can democratize spaces and give voice to minorities, and on the other, it can reinforce inequalities and Western worldviews.[10] Whereas the internet is seen as a platform for true democratic discourse, digital colonialism exposes online freedom and democracy at the risk of being compromised. Digital colonialism also carries disadvantages for the subjects. Economic exploitation and geopolitical domination by the West over the East maybe its by-products. Nick Couldry and Ulises A. Mejias (2019) hold

[8] Clarifying Lawful Overseas Use of Data (CLOUD) Act, 2018, *available at:* https://epic.org/privacy/cloud-act/cloud-act-text.pdf (last visited on March 17, 2021).
[9] Kimberly Anastácio, "A view from the cheap seats: Internet and colonialism" *SSRN*, *available at:* ssrn.com/ SSRN-id2909369.pdf (last visited on March 31, 2021).
[10] *Ibid.*

that datafication is linked to capitalism.[11] Couldry and Mejias identify datafication or data quantification as a new social realm and the first step towards digital colonialism[12]. Data colonialism as a process makes human life itself a subject, which is being appropriated and is annexed towards capitalism.[13] Data colonialism is a far-fetched idea built upon the traditional concept of colonialism and this new norm is assumed to augment the fruits of capitalism to the West. Another variant of capitalism in this new age of technology is what Shoshana Zuboff calls surveillance capitalism[14]. According to Zuboff, the raw material for surveillance capitalism is human experience which can be transmitted into behavioural data.[15] Zuboff also holds that "surveillance capitalism has emerged as a leading version of information capitalism." This information capitalism is nothing but commercial exploitation of data. Surveillance capitalists, particularly the big hi-tech companies from the West have gained enormously from their surveillance mechanism over this targeted behavioural data of data principals or data subjects. Zuboff Considering the statistics of just one but the most used social media company, Facebook has 2.85 billion monthly users worldwide as of the first quarter of the year 2021 and India has the most Facebook users in the world with over 260 million, followed by the US (180 million), Indonesia(130 million), Brazil (120 million)[16]. This clearly shows the vastness & magnitude of the market and the population available to these companies to derive the benefits of surveillance capitalism. This surveillance capitalism has turned into a channel of digital colonialism through which the big tech giants from the West can not only exploit economic gains but also change the economic, political and social waves for their own interest. What Zuboff calls surveillance capitalism, Francesca Bria calls it platform capitalism. Bria compares the current platforms which are mostly online market places to the parasites as they ride on existing social and economic relations and public data.[17] Another interesting mechanism deployed by the big tech giants is digital extractivism. This mechanism is problematic as

[11] Nick Couldry and Ulises A. Mejias**, "**Making data colonialism liveable: how might data's social order be regulated?" 8 (2) *Internet Policy Review* 2019, *available at:* https://policyreview.info/articles/analysis/making-data-colonialism-liveable-how-might-datas-social-order-be-regulated (last visited on March 31, 2021).
[12] *Ibid.*
[13] *Ibid.*
[14] Shoshan Zuboff, "Big other: surveillance capitalism and the prospects of an information civilization", *Journal of Information Technology,* Palgrave Journals, *available at:* https://cryptome.org/2015/07/big-other.pdf (last visited on April 2, 2021).
[15] John Naughton, "The goal is to automate us: welcome to the age of surveillance capitalism" *The Guardian, available at:* https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook, (last visited on March 31, 2021).
[16] Facebook Demographic Statistics, *available at*: https://backlinko.com/facebook-users (last visited on June 3, 2021).
[17] Francesca Bria, "Public Policies for Digital Sovereignty", *available at:* https://www.academia.edu/19102224/Public_policies_for_digital_sovereignty (last visited on April 1, 2021).

although it promises development and convenience, it reinforces the same threats as posed by surveillance capitalism. It subjugates and exploits individuals, institutions and even states to the capitalist ideology of economic gains. Data extractivism tendency and capacity of the giant tech companies has tilted and led to the concentration of the economic benefits of the world into their favour.

The very idea of data sovereignty is anti-colonial. Data sovereignty ensures to safeguard the interest of the nation in relation to data access, data availability, data confidentiality and data integrity.[18] Realising the importance of data and digital sovereignty, the world is witnessing a new trend of a shift from digital colonialism to digital sovereignty, wherefrom it wants to have complete control and autonomy over its own data. Digital colonialism is the new type of colonialism, a channel used by the big tech companies such as Facebook, Google, Netflix to control the data of the global South. As most of the data centres are located in the western part of the globe, these big tech companies have easy access and control over data of the countries of their operation. This also has economic, political and such larger than thought implications which are suffered by the global South. The demand for data sovereignty and the urge of the global south to reign over its own data is thus not just out of bounds.

Data Sovereignty is expected to make the internet a decentralised platform for democratic discourse in its true sense. There are studies that indicate towards the constant conflict between the need to protect privacy, personal autonomy and democracy vis-à-vis the need to explore surveillance capitalism. Lukas Wohnhas (2019) in his research work has tried to explore the explanation for the failure of privacy to contest surveillance capitalism and further the implications of surveillance capitalism on democracy.[19] His findings suggest that surveillance capitalism has posed a threat to the democracy and personal autonomy of both nations and individuals. He argues that when surveillance capitalism interferes with personal autonomy, it has direct implications for democratic discourse and procedures; as personal autonomy is a *sin qua non* for effective democratic participation.[20] Surveillance capitalism is a catalyst for digital colonialism as it interferes with the data, privacy and autonomy of individuals having the potential to influence their behaviour and decision making. In this regard, it would not be wrong

[18] Yudhistira Nugraha, Kautsarina and Ashwin Sasongko Sastrosubroto, "Towards Data Sovereignty in Cyberspace" *SSRN*, *available at:* SSRN-id2610314.pdf (last visited on April 1, 2021).
[19] Lukas Wohnhas, "Surveillance Capitalism and Privacy- Exploring Explanations for the Failure of Privacy to Contest Surveillance Capitalism and the Implications for Democracy", *available at:* https://www.diva-portal.org/smash/get/diva2:1483285/FULLTEXT01.pdf (last visited on June 3, 2021).
[20] *Ibid.*

to expect and envision that the data sovereignty principle can liberate individuals from the ill effects of surveillance capitalism and also protect the personal autonomy as well as democratic participation of the people.

However, it goes without saying that the economic cost which the countries like India would have to bear for achieving and maintaining data sovereignty requirements can be quite high which includes the cost of setting up several data centres, local servers and adequate infrastructure, both hard and soft for aligning different data governance related activities such as data management, data cataloguing and data analysis for consumer benefit. For this purpose, the government can further liberalise its financial policies to attract more investment, and can provide different tax incentives to the companies investing to establish local data centres and related infrastructure.

Amidst the discussion on the clash between data sovereignty and data colonialism, few countries have adopted the protectionist approach. This digital protectionism which differs from data protection approach, challenges and creates barriers to the widely accepted way of internet governance. China has resorted to the practice of digital protectionism which creates barriers to cross border data flows. It has banned many foreign apps and digital platforms from competing and many others such as LinkedIn and Skype are allowed only on the condition of complying with the directions of the Government and giving direct access of data to the government. This, as Susan Ariel Aaronson holds, undermines human rights and scientific progress.[21] He explains how digital protectionism can lead to unanticipated side effects, including reduced internet stability, generativity and access to information.[22] A study conducted by Greenberg Centre for Geo-economics Studies shows that the main drivers of digital protectionism in Asia and Europe are web censorship, forced transfer of intellectual property, data localisation, and arduous privacy rules.[23] China's blocking of e-commerce sites such as Amazon and Rakuten, business apps such as SlideShare and Dropbox and chatting apps other than WeChat clearly indicates towards an over- protectionist approach adopted by the country.[24] Such an over-protectionist approach creates a direct threat to fair competition and

[21] Susan Ariel Aaronson, "What Are We Talking about When We Talk about Digital Protectionism?" *World Trade Review* (2018), *available at:* https://www2.gwu.edu/~iiep/assets/docs/papers/2018WP/AaronsonIIEP2018-13.pdf (last visited on March 18, 2021).
[22] *Ibid.*
[23] The Rise of Digital Protectionism-Insights From a CFR Workshop, *available at:* https://www.cfr.org/report/rise-digital-protectionism (last visited on June 6, 2021).
[24] China's digital protectionism puts the future of the global Internet at risk, *available at:* https://www.washingtonpost.com/outlook/2019/02/25/chinas-digital-protectionism-puts-future-global-internet-risk/ (last visited on June 6, 2021).

free trade. The Digital protectionist approach not only poses challenges for the digital economy; it also impend the traditional sectors such as agriculture, manufacturing and energy, as these sectors are also increasingly relying on data and are using digital technology.[25]

Digital trade has emerged as one of the most important components of the global trade and economy; and the digital protectionist tendency of the global east has become a major concern for the global west. This is clear from the fact that the contribution of digital trade and digital economy to the US GDP in the year 2017 has been accounted for 6.9%.[26] As a representative of the Global West, what the United States means by digital protectionism is "barriers or impediments to digital trade, including censorship, filtering, localization measures and regulations to protect privacy".[27] The United States International Trade Commission, in its report published in 2013 has factored digital protectionism, localisation measures, censorship measures and even the data privacy and protection laws of other countries as a notable barrier and impediment to digital trade.[28] On the other hand, China has holistically adopted and implemented the protectionist approach in the digital domain; more particularly to protect its political and state regime from the influence of the West, rather than protecting the privacy & data of the individuals.

There's a very thin line of difference between digital protectionism and adopting policies that protect data *i.e.*, data protection approach. In contrast to countries that favour digital protectionism, India has adopted an approach that seeks to protect data of individuals and also not give up on its data sovereignty. The digital protectionist approach not only creates trade barriers and threats to fair competition and innovation; it also takes away the freedom of choice from the consumers. Over protectionist approach by over regulating the digital domain and creating trade barriers for the global companies is expected to create a balkanized effect, resulting in restricting the consumers to avail benefits of the global digital economy.[29] This ideology in itself seems to be anti-democratic as not it restricts the choice of consumers; it also curtails healthy competition and fair trade.

---

[25] *Ibid.*
[26] Digital Trade and the US Trade Policy, Congressional Research Service, May 21, 2019, *available at:* https://fas.org/sgp/crs/misc/R44565.pdf (last visited on June 6, 2021).
[27] USITC, Digital Trade in the US and Global Economies, Part 1, Investigation No. 332-531 USITC Publication 4415, July 2013, *available at:* https://www.usitc.gov/publications/332/pub4415.pdf (last visited on June 6, 2021).
[28] *Ibid.*
[29] Ziyang Fan and Anil K Gupta, "The Dangers of Digital Protectionism" *Harvard Business Review*, 2018, *available at:* https://hbr.org/2018/08/the-dangers-of-digital-protectionism (last visited on June 6, 2021).

It is pertinent to note here that both digital colonialism and digital protectionism are extreme approaches, have led to unprecedented implications and have emerged as faulty approaches in dealing with data management, governance and its protection. Both of them are nowhere near the concept of digital sovereignty.

III. The Rise of Data Marketplace

Data has emerged as the most valuable and worthy resource of the present times and it would continue to hold such value even in the future. Big-tech companies already know the worth of data and are thriving on this very precious resource. Future businesses are being designed on the basis of data available with corporations. The idea that data as a resource can even be traded, has given rise to the data marketplaces. A Data marketplace is a platform where data can be bought and sold. It is a platform where data can not only be attributed to an individual, but where an individual can also have a relation of sovereignty to their personal data.[30] It provides the platform where an individual can move and deal with the data at his will. This has further strengthened the idea of data ownership and data sovereignty. Empowering citizens by giving them better or rather absolute control over their data is another facet of data sovereignty. The idea of data marketplace matches well with the idea of data sovereignty and digital empowerment of an individual. Elements of data sovereignty and the right of data portability (even in the restricted sense that is to move one's data in online spaces without loss) go together to protect the data protection rights of an individual. The rise of more data marketplace shall evolve such a mechanism which can discourage the global companies to collect data through unfair means without obtaining consumer's consent and rather create a more voluntary mechanism where data can be traded at the data principals' discretion.

There are two propositions with regard to data marketplaces. One, there is a strong correlation between data marketplace and data sovereignty. The conceptual structure of data marketplaces cannot be successful if it is not based on the foundation of data sovereignty. It has to be consciously agreed by all that the data owner, the data principal or the data subject is to be given the highest regard in the digital ecosystem. Second, data marketplaces, which may be categorized into individual, business or sensor/Internet of Things (IoT) based data need to be structured and regulated by the governments. However, the present regulatory and legal

[30] Michelle De Mooy, Center for Democracy and Technology, "Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data Considerations for Future Policy Regimes in the United States and the European Union", *available at:* https://cdt.org/wp-content/uploads/2017/04/Rethinking-Privacy_2017_final.pdf (last visited on Oct. 19, 2020).

framework and policies show significant gaps in the regulation of data marketplaces. Data marketplaces offer all kinds of data to be bought including demographic data, personal data, and consumer related data, commercial data *etc.* Proper regulation of the data marketplaces and acknowledgment of the sellers' rights at such marketplaces is expected to protect the rights of the data owners and provide them the real worth of their data with their free consent.

There are arguments against the concept of data marketplaces as it lacks transparency and accountability in the process of data collection and processing, obtaining free consent of the data principals or data owners and in the assessment of the fair valuation of data. There is a need for a unique model for the regulation of data marketplaces where both the State as well as the business sector has their own roles and responsibilities in pursuit of the best interest of the data principal. A hybrid model where the government can provide a broad regulatory and legislative framework to ensure transparency and better governance of data marketplaces or data exchange centres and corporations can provide for code of conduct for the buyer and the seller while trading with data. Such a model is expected to augment the data sovereignty rights of an individual as well as the government.

IV. Sovereignty Issues in the Cloud

The situation becomes more complex in the case of cloud computing. Users' privacy is more easily compromised in cases of cloud as they are giving away their rights for the sake of more personalised services including comfort, ease of share, accessibility of data, scalability of data and cost effectiveness.[31] However, the organisations operating in public clouds must be careful about following data protection and data sovereignty provisions. Protecting data sovereignty and creating a framework for effective data governance on the cloud has constantly been a challenge. The biggest challenge being that the laws and regulations relating to data collection, storage and management vary from country to country. The other challenge being that by its basic feature cloud facilitates data storage in different places which may create complex jurisdictional and governance issues. Due to this, the companies and organisations operating on the cloud may violate the data sovereignty regulations. In a range of data sovereignty laws across the countries ranging from China's cyber security laws, to Brazil's General Data Privacy Law, to Japan's Personal Information Protection Act, to Chile's Law for the Protection of Private Life, to more than a dozen regulations on this by the United States,[32] the organisations

[31] Primavera De Filippi, Smari McCarthy, "Cloud Computing: Centralization and Data Sovereignty", *available at:* SSRN-id2167372.pdf (last visited on March 18, 2021).
[32] *Supra* note 1 at 2.

may find it complex to adhere to the regulations in terms of transnational and cross border flow of data. The data sovereignty regulations of the countries are not uniform as they aim to protect their own data and have control over its collection, storage and processing. Some of them are difficult to interpret and follow. The data localisation requirements of each country may also be different. Given the way in which the SaaS and the cloud services work, its distributed mechanism may mean that the data hosted by the cloud service providers may be subject to the laws of the foreign countries.[33] This goes against the very idea of data sovereignty.

The technicalities may require the data to be stored in different locations outside the jurisdiction of the country of the data subject. It falls under the laws of different jurisdictions which might not be compatible with the laws of the country of the data subject. Moreover, the data and the data subject may be at the mercy of the laws of the country where the data resides. The data privacy laws of the other country may be less stringent and may not provide adequate protection to the data of the data subject from different jurisdictions. In EU, maintaining data sovereignty is the essence of the GDPR and is required to be followed strictly. If not followed, GDPR regime provides for a penalty up to 4% of the total worldwide annual turnover of a business or 20 Million Euros, whichever is greater.

V. The Pursuit of Indian Data Sovereignty

The new world order, triggered particularly by the pandemic, which has exalted the value of 'data' for businesses to a new level has necessitated the requirement to create a robust legal framework that can meet the standards of data sovereignty and data governance. The ongoing digitization and data revolution process where the consumer is no more the end user but is being seen as the product itself, requires an effective legal system which can empower the citizens and give them better control over their data. There is a need for such a legal system which does not allow digital colonialism to spread and pass on the monetary benefits of surveillance capitalism, behavioural targeting and datafication into the hands of few global companies based in the global West.

Needless to mention, the existing legal framework in the form of minimal to nil provisions under the Information Technology Act, 2000 towards maintaining requirements of data protection, data sovereignty and data governance are far from achieving the expectations in

[33] Data Sovereignty, *available at:* https://www.stratokey.com/solutions/data-sovereignty-and-the-cloud (last visited on March 18, 2021).

this regard. The pursuit of Indian data sovereignty; rather data protection has recently been extended with the enforcement of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. The new 2021 IT Rules which are in supersession of the 2011 intermediary guidelines are certainly a step up with regard to determining the role and liability of digital intermediaries including social media intermediary[34] and significant social media intermediaries.[35] The due diligence mechanism[36] under the Rules now requires the intermediaries to discharge several duties and obligations. The Rules require the significant social media intermediaries to observe additional due diligence[37] failing which they are liable for punishment under any other law for the time being in force including the Indian Penal Code.[38]

The recent controversies between foreign social media intermediaries such as WhatsApp, the microblogging site such as Twitter and the Government of India has again reinforced the demand to have an effective data protection law to protect not only the personal data of citizens, but also to ensure data sovereignty requirements. The relevant issue which arises in the context of data sovereignty is that the 2021Whats App privacy policy restricts the choice of the users with regard to sharing their data with Facebook owned apps and other third parties. As per the new policy, WhatsApp shall be free to share the data of the users with its parent company Facebook and other entities including their mobile phone number, profile name, phone model, screen resolution, IP address *etc*. This data can be stored and processed outside India; thus directly challenging the data sovereignty goals of the Government of India. The immediate implication of this would be an increase in the targeted advisements to the users' across all the Facebook owned platforms. Such a behavioural targeting is not only an issue of data protection, but it is also tantamount to surveillance capitalism and datafication of the lives of the users. Sans adequate and effective data sovereignty provisions, the nation may get subject to digital colonialism.

The adoption of the Indian Personal Data Protection Bill 2019 is expected to completely change the legal regime of data protection in India. The Personal Data Protection Bill 2019 is expected

[34] Rule 2(w) of the 2021 IT Rules defines a social media intermediary to mean an intermediary which primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services.
[35] Rule 2(v) of the 2021 IT Rules defines a significant social media intermediary to mean a social media intermediary having number of registered users in India above such threshold as notified by the Central Government.
[36] Rule 3, 2021 IT Rules – Due Diligence by an intermediary.
[37] Rule 4, 2021 IT Rules – Additional due diligence to be observed by significant social media intermediary.
[38] Rule 7, 2021 IT Rules - Non-Observance of Rules.

to be a game changer for all the stakeholders including the data owners, the data fiduciaries and the data processors. It is highly inspired by the GDPR and encompasses all measures to maintain the data sovereignty of the data which is collected and stored within the country. Unfortunately, India has already delayed its initiative to enact its own data protection legislation in the times when countries like Singapore, China, Canada, Japan and Malaysia have already joined the league of countries that have enacted their data protection laws much earlier than us. However, the expectation is that it turns out to be model legislation and the best legislation on data protection, data sovereignty and data governance, taking lessons and adopting best practices from the other best models around the world. The Bill seek to be applicable to the processing of personal data by data fiduciaries or data processors not present within the territory of India, in the following circumstances only[39] —

(a) If the processing is in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India; or

(b) If the processing is in connection with any activity which involves profiling of data principles within the territory of India.

An important way to achieve data sovereignty is data localisation which would require the companies to store data in servers located within the territorial borders of the country. India has been an active advocate of data localisation as by storing it within the servers located in the country, it would have better and effective control over its data. Contradictorily, data localisation would be averse to the very concept of cloud computing. The concept of cloud computing is based on data storage anywhere on the planet irrespective of fixed territorial location and its easy accessibility to the users. However, to some extent data localisation can be a panacea to the threats of data and privacy infringement of the citizens as well as the state. The data infringement case of Cambridge Analytica where this data-driven political consultancy[40] indulged in the unauthorised use of the data of millions of Facebook users for the purpose of election campaigning was an eye-opener for India and for the world. Data localisation simply mandates that companies and organisations collecting data from individuals within a territory must store and process within the country itself. The Reserve bank of India also provided clarification on the storage of payment system data ensuring that it is important to have unfettered supervisory access to data stored with these system providers as also with

[39] Personal Data Protection Bill 2018, s. 2(2).
[40] Understanding the data localisation debate in India, *available at:* https://www.investindia.gov.in/team-india-blogs/understanding-data-localisation-debate-india (last visited on March 30, 2021).

their service providers/intermediaries/ third party vendors and other entities in the payment ecosystem. The RBI required all service providers to ensure that the entire data relating to payment systems operated by them including the full end-to-end transaction details/information collected/carried/processed as part of the message/payment instruction are stored in a system only in India.[41] The Central Bank further issued a clarification that although there is no bar on the processing of payment transactions outside India, the PSOs will have to ensure the data is stored only in India after the processing.[42] This outstanding notification of the Central Bank sets forward that India is firm on the policy of data localisation and not allowing foreign companies and organisations to store and process data outside India. This would go a long way in maintaining the data sovereignty requirements by India.

The broad objective set out by the Personal Data Protection Bill 2019 is to maintain data sovereignty. However subject to certain conditions, the Bill allows the transfer of personal and sensitive personal data outside India. The data localisation provisions under the Bill impose restrictions on the cross-border transfer of personal data.[43] It requires every data fiduciary to ensure that at least one copy of the personal data must be stored on a server or data centre located in India. The Bill also emphasises on the importance of processing critical personal data only in India.[44] The fulfilment of these requirements would need more and more data centres or servers to be located in India. If at all data has to be transferred outside India, it would be subject to the conditions under the Bill.[45] These conditions include the explicit consent of the data principal, the transfer to be made subject to the standard contractual clauses and due prescription of the Central government that transfer to a particular country or international organisation is permissible.

The Committee of Experts to deliberate on data governance framework in India has acknowledged the significance of community data to understand public behaviour, preferences and making decisions for the benefit of the community.[46] The Committee in its report distinguished between community data and large scale data and seeks to facilitate collective

[41] RBI Notification dated April 6, 2018, RBI/2017-18/153 DPSS.CO.OD No.2785/06.08.005/2017-2018, *available at:* https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244 (last visited on March 31, 2021).
[42] *Ibid*.
[43] Personal Data Protection Bill 2019, s. 33.
[44] Personal Data Protection Bill 2019, s. 33(2).
[45] Personal Data Protection Bill 2019, s. 34.
[46] Office memorandum No 24(4) 2019/ - CLES available at https://meity.gov.in/writereaddata/files/constitution_of_committee_of_experts_to_deliberate_on_data_governance_framework.pdf (last visited on 1st April 2020).

protection of privacy by according protection to an identifiable community that has contributed to community data.[47]

The Indian judiciary has also been supportive of the data sovereignty requirements and this is well reflected through the recent judgments of various High Courts. In *Balu Gopalakrishnan* v. *State of Kerala*[48], the Kerala High Court passed an interim order directing the government of Kerala to undertake all necessary precautions and follow all the required protocols before handing over the health related sensitive personal data of the Covid-19 positive patients in the state of Kerala to the US based entity Sprinklr. As per the agreement between the Government of Kerala and Sprinklr, the patients' data which could be stored, processed and analysed outside India without any consent or knowledge of the data principles, is a direct breach of both data protection as well as data sovereignty norms. The Court pointed out the breach of confidentiality and highlighted that there should be no "data epidemic" after the pandemic is controlled. The Court specifically stated that no data can be handed over to a foreign entity without adhering with the requirements such as anonymization of data, obtaining specific consent of the data principals, clarity on return of data, no commercial exploitation etc. This decision of the Kerala High Court would have far reaching effects in shaping the digital ecosystem as well as in laying down strong data sovereignty norms.

VI. Data Sovereignty Requirements - Institutional and Policy Measures by India

Given that data localisation and data sovereignty are concomitant to each other, India, in pursuit of strong data sovereignty and data localisation requirements, has very recently taken several institutional and policy measures. One of the earliest attempts in this direction was made in the year 2012 with the launch of the National Data Sharing and Accessibility Policy of the Government of India. This policy is a significant measure that focuses on the requirement of data localisation. The Policy was brought out to increase the accessibility and easier sharing of non-sensitive data amongst the registered users and their availability for scientific, economic and social developmental purposes.[49]

[47] *Ibid.*
[48] *Balu Gopalakrishnan* v. *State of Kerala,* Kerala High Court, WP (C) Temp. no. 84 (2020), April 24, 2020.
[49] National Data Sharing and Accessibility Policy, *available at:* https://dst.gov.in/national-data-sharing-and-accessibility-policy-0 (last visited on April 2, 2021).

Another significant initiative towards this direction was the proposed Digital Information Security in the Healthcare Act, 2018 in order to protect the health data of the citizens. This Act aimed to provide for electronic health data privacy, confidentiality security and standardization and provide for the establishment of National Digital Health Authority and Health information Exchanges.[50] However, it does not expressly secure the data localisation or data sovereignty requirements.

Another measure was initiated in 2018 by the RBI when it notified the requirement of data localisation requirements with respect to the Payment System Operators (PSO) in India.[51] The Central Bank, well realising that all PSOs do not store the data in India and with a need to monitor the entire online payment mechanism in a better way, to have unfettered supervisory access to data which is stored with the system providers and other entities in the payment ecosystem, issued the directive[52] to all the system providers and required that "the entire data relating to payment systems operated by them are stored in a system only in India. The data must include the full end-to-end transaction details, information collected, carried, processed as part of the message or payment instruction."[53]

The recommendations of Srikrishna Committee headed by Justice B N Srikrishna which were adopted in the Data Protection Bill 2019 is another strong step towards mandating data localisation and data sovereignty requirements in India. The recommendations strongly put forward certain institutional mechanisms in the form of Data Protection Authority of India.[54] The DPA has been entrusted with vast powers to ensure compliance with the provisions of the Act including the provisions related to data sovereignty. However, many including the United States consider that through the 2019 draft Bill India seeks to adopt a protectionist approach rather than maintain data sovereignty requirements. The critics consider that by imposing restrictions on cross-border data transfer, requiring storing copies of data in India and by achieving data localisation, the Government of India seeks to create digital trade barriers similar to China.

---

[50] F.No Z-18015/23l2017-eGov, Government of India, Ministry of Health & Family welfare (eHealth Section) dated March 21, 2018, *available at:* https://www.nhp.gov.in/NHPfiles/R_4179_1521627488625_0.pdf (last visited on April 2, 2021).

[51] *Supra* note 36.

[52] Issued under section 10 (2) read with section 18 of Payment and Settlement Systems Act, 2007 (Act 51 of 2007).

[53] Storage of Payment System Data, RBI/2017-18/153 DPSS.CO.OD No.2785/06.08.005/2017-2018, *available at:* https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244 (last visited on June 6, 2021).

[54] Under section 41 of the Personal Data Protection Act, the Central government shall, by notification, establish the Data Protection Authority of India.

Another significant initiative by the government which mandates localisation and sovereignty requirements of government data stored on the cloud is the "Meghraj" initiative.[55] In May 2020, the invited applications for empanelment of cloud service offerings of cloud service providers lay down the requirements which are specific to the cloud deployment model for the government community cloud; and it confers the sole power on the government of India to control its data.[56] It mandates that Government Community Cloud shall only offer Cloud services to Govt. Departments / Ministries / Agencies / Autonomous Institutions / Statutory Bodies / Offices under Government of India or States or UTs or Local Governments or PSUs or Nationalized Banks within India.[57] Similarly, Cloud MeghRaj requires prior approval of the Government departments regarding the strategic control over the data and any change or modification to be introduced to solutions, database, data, configurations, security solutions, hosted infrastructure, etc. of the Government Community Cloud where such changes affect solutions of multiple Government Departments using the Government Community Cloud.[58]

Another institutional mechanism is the National Internet Exchange of India(NIXI), which was set up in 2003 for peering of ISPs among themselves for the purpose of routing the domestic traffic within the country, instead of taking it all the way to US/Abroad, thereby resulting in better quality of service (reduced latency) and reduced bandwidth charges for ISPs by saving on International Bandwidth.[59] NIXI promotes data sovereignty requirements by aiming to achieve the objectives such as[60]:

i) To set up, when needed, in select location(s)/parts/regions of India Internet Exchanges/Peering Points.

ii) To enable effective and efficient routing, peering, transit and exchange of the Internet traffic within India.

iii) To continuously work for enhancing and improving the quality of Internet and Broadband services.

[55] 'Meghraj' is the national GI cloud launched in 2014.
[56] Refer to 6.1.1 Inviting Application for Empanelment of Cloud Service Offerings of Cloud Service Providers, *available at:* https://meity.gov.in/writereaddata/files/tender_upload/Application_CSP.pdf (last visited on April 2, 2021).
[57] *Ibid.*
[58] *Ibid.*
[59] *Available at*: https://nixi.in/en/about-us (last visited April 2, 2021).
[60] *Ibid.*

VIII. Conclusion

There lies a strong connection between the new world order and sovereignty issues in the real space. In the light of the varied changes and challenges which the world is facing, the same connection can be seen even in the digital world. Sovereignty has different kinds- domestic sovereignty, international legal sovereignty, Westphalian sovereignty, interdependence sovereignty.[61] Digital sovereignty being the latest addition, is critical to the establishment and success of new world order. Sans adequate data governance and data sovereignty mandate, this new world order which is driven by technological complexities may lead to economic and human rights violation of digital have- nots, may intensify the problems related to digital colonialism and may also bring over half of the world being dominated under the neo-data-colonial practices by countries and corporate giants from the other half.

A nation has all the right to make any law and take any action in order to protect its sovereignty. The same holds true for data sovereignty as well. The common law act of state doctrine allows a nation to protect its sovereignty and its domestic actions cannot be questioned in the courts of other jurisdictions.[62] Even the United States Court of Appeals for the Ninth Circuit acknowledged this doctrine[63] stating that every foreign state is bound to respect the independence of every other sovereign state, and the court of one country will not sit in judgment on the acts of the government of another, done within its own territory.[64] The principle of sovereignty is applicable to even internet sovereignty and data sovereignty, wherein, any nation can enact data localisation laws to protect its digital sovereignty and minimize the threats of cross border digital colonialism.

However, achieving data sovereignty standards that are purely based on data localization is not an ideal situation for the global economy. Whereas data sovereignty laws have emerged as a response to the digital authoritarianism; excessive data localization is expected to lead to a balkanized digital world. Strict and excessive data localisation norms have their own demerits and can prove harmful to the global digital economy, fair competition, and fair trade. Data

---

[61] Anne-Marie Slaughter, Sovereignty and Power in a Networked World Order, *available at:* https://www.law.upenn.edu/live/files/1647-slaughter-annemarie-sovereignty-and-power-in-a (last visited on April 5, 2021).

[62] Act of State Doctrine, *available at:* https://definitions.uslegal.com/a/act-of-state-doctrine/ (last visited on April 5, 2021).

[63] *Yahoo! Inc., a Delaware Corporation, Plaintiff-appellee* v. *La Ligue Contre Le Racisme et L'antisemitisme, a French Association; L'union Des Etudiants Juifs De France, a French Association, Defendants-appellants*, 433 F.3d 1199 (9th Cir. 2006), *available at:* https://law.justia.com/cases/federal/appellate-courts/F3/433/1199/546158/#fn3-1_ref (last visited on April 5, 2021).

[64] *Ibid.*

localization norms are not only likely to create trade barriers, but in the long term, it is also likely to decrease investments in the corporate sector. This is certainly not what the government of any nation should intend to achieve. The nation states particularly the global east need to find a solution to the digital authoritarianism of the global west. There needs to be a balance between achieving digital sovereignty and yet keep away the harms caused by excessive data localization.

Apparently, data governance and data sovereignty requirements are aligned with the national interest and are quintessential to the new world order. Countries like China have already taken strong steps to protect their internet sovereignty. However, the Indian approach towards addressing the challenges of the new world order needs to be shaped up in a manner that neither our data sovereignty is compromised, nor the harmony between national and international trade is disturbed. The benefits of global digital trade must reach the consumers and individuals whose data is being subject to trade. We need to devise such a legal framework which provides a strong guard against the colonialist tendencies of the global west, while enabling only trusted cross border flow of data, which can't be misused or commercially exploited for their self-interests. Better harmonization between nation states, more accountability by global companies towards the customers, laying down the rights and obligations of all stakeholders in the digital business and stringent penal consequences for violating with the data protection provisions are some ways by which a balanced digital ecosystem can be created. In the Indian context, the rules of the game have not been drafted yet. Hence, the government should draft such new rules for the new world order which ensure data sovereignty, data protection as well as provides opportunities that allow global digital trade to flourish.