

CROSS BORDER DATA PROTECTION AND E-COMMERCE

Mayank Singhal*

ABSTRACT

There has been a consistent increase in e-commerce transactions all across the world and India is not an exception to it. These transactions generate huge amount of data. Such data involves personal as well as the financial data like bank account details. E-commerce industry in India has presence of foreign enterprises like Amazon, e-bay etc. It is a genuine concern for a developing country like India to regulate the cross border data flows with a balanced approach towards the issue. A balance between the privacy of individuals and economic concerns of the stakeholders involved. The Department for Promotion of Industry and Internal Trade released a draft e-commerce policy to address the issue of data protection along with other issues relating to e-commerce. The policy terms data as a new oil and emphasizes upon the need to prevent misuse and regulate the data flows. It places a restriction upon the cross border data flows, seeks to nationalise data and rest the control in hands of the government to utilise the economic benefit derived for the larger public benefit. The draft policy may be termed as extremely protectionist in nature. The method of data localisation adopted to achieve the objective of the policy, suffers from major deficiencies. The cost and risks of hacking involved in local storage of data has been overlooked by the policy. Another aspect of the policy, which favours domestic enterprises over the

* Student, B.A. LL.B. (Hons.) FYIC, 3rd Year, Rajiv Gandhi National University of Law, Punjab, Patiala (mayanksinghal@rgnul.ac.in).

foreign counterparts is devoid of reasons and may be a ground of challenge under the WTO Agreement for discriminating between local and foreign enterprises. The draft e-commerce policy has been formulated to regulate the e-commerce sector, but has widened its scope by inclusion of an unidentified term like 'digital economy' which may include all others aspect relating to information technology like cloud computing services, internet service providers etc. These aspects form a separate field altogether and cannot be regulated along with the e-commerce. The policy must define its scope with clarity so as to avoid uncertainty.

1. INTRODUCTION

“Data is the new oil. Therefore, just like oil or any other natural resource, it is important to protect data, prevent its misuse, regulate the use and processing of data and address the concerns related to privacy and security.”¹ The increasing use of information technology services including e-commerce has raised concerns regarding the protection of data generated by the consumers while they enter into transactions. The data so generated is surely a valuable resource; it is monetized by business enterprises for purposes like user – based advertisement. Many foreign companies like Amazon, E-bay, etc. operated in India, thus the need arises for cross- border data protection.

2. NEED FOR CROSS BORDER DATA PROTECTION

The importance of data protection has been increasing due to an increase in the number of economic activities taking place online. There is

¹ *Draft National E-Commerce Policy: India's Data for India's Development*, DEPT. FOR PROMOTION OF INDUS. & INTERNAL TRADE (May 25, 2019), https://dipp.gov.in/sites/default/files/DraftNational_ecommerce_Policy_23February2019.pdf.

a huge amount of information being generated, stored and transmitted across the globe. The data flows needs to be regulated so as to address concerns of consumer confidence as well as the privacy of the individuals. Right to privacy has been recognised as a Fundamental Right enshrined under Article 21 of the Indian Constitution.² In the judgment delivered by the Supreme Court in *Justice K.S. Puttaswamy*,³ the Court emphasized upon the regime of data protection in following words, “Formulation of a regime for data protection is a complex exercise which needs to be undertaken by the State after a careful balancing of the requirements of privacy coupled with other values which the protection of data sub-serves together with the legitimate concerns of the State.” The data protection regime must necessarily be balanced. An imbalanced approach would lead to a breach of privacy of the individuals. An excessively stringent regime, on the other hand, would seriously hamper the trade flows. E-Commerce has been a growing phenomenon, with more and more people becoming digitally educated. There has been consistent growth in the e-commerce market. The Indian B2C e-commerce market was valued at USD 38.5 billion in 2017 and is estimated to rise to USD 200 billion in 2026.⁴ Activities undertaken by the consumer during e-commerce transactions generated an unprecedented amount of data.

3. DRAFT E-COMMERCE POLICY AND DATA PROTECTION

The Department for Promotion of Industry and Internal Trade (DPIIT) released the draft e-commerce policy (“draft policy”) on February 23, 2019. The policy, in light of increasing importance of data protection

² Justice K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.

³ *Id.*

⁴ *Indian Ecommerce Industry Analysis*, INDIAN BRAND EQUITY FOUNDATION (May 25, 2019), <https://www.ibef.org/industry/ecommerce-presentation>.

and privacy, aims at regulation of cross border data flows. The term ‘data’ has been broadly defined by the draft policy. It defines ‘data’ as any type of information converted into a binary digital form that is efficient to store, process and transfer across different devices, platforms, servers and borders. Data includes both standalone personal data as well a financial data.⁵

The data generated may be monetized by the corporations in various ways by analysing, processing and utilizing it. The online advertisements nowadays are based upon activities of the user. The draft policy, asserts that “An Individual owns the right to his data”, thereby granting the right to an individual over the data generated by him. It further states that “the data that is generated in India belongs to Indians, as do the derivatives there from”.⁶ Thus, draft policy terms data as a “national asset” and that it must be held by the government in ‘trust’.⁷

The draft policy restricts the cross border transfer of data generated by way of e-commerce and social media activities. The policy aims to restrict the sharing of data with business entities outside India even with the consent of the customer. The data cannot be made available to the foreign government, without prior permission of Indian authorities. The government by way of the draft policy, seeks to exercise sovereignty over the data generated in the country.

The draft policy, however, exempts cross-border flow in the case where (a) data that is not collected in India (b) B2B data is sent to India as part of a commercial contract (c) data flows relating to cloud computing

⁵ *supra* note 1, at 10.

⁶ *Id.* at 15.

⁷ *Id.* at 14.

services, have no personal or community implications; which and (d) MNCs moving internal data of company.

4. ANALYSIS OF THE DRAFT POLICY

The draft policy may be termed as an extremely protectionist measure taken by the government as it restricts the cross border data flows in a stringent manner. The government seeks to justify the stringency of the measures in the guise of India being a developing nation and there being consequential need to develop and boost the domestic digital infrastructure.

4.1 EXCESSIVELY WIDE SCOPE

The draft e-commerce policy has been formulated to regulate data transfers in the e-commerce sector. But usage of the term ‘digital economy’, expands the coverage to all network related communications like search engines, ISPs, OTT services providers, content ecosystem and the larger Indian IT industry which processes data on behalf of clients. NASSCOM recommends that “DPIIT should avoid placing conflicting or significant views in the e-commerce policy on matters which are core to other ministries. Placing them in the policy causes anxiety for the industry as it generates avoidable uncertainty.”⁸ The recommendations by the NASSCOM are relevant to address the issue of defining the scope of the draft policy. If the policy has been formulated with an aim to regulate the e-commerce sector, then it must regulate the only e-commerce sector and not beyond. The vagueness in defining the scope causes uncertainty.

⁸ Ashish Aggarwal, *NASSCOM's comments on the draft e-commerce policy*, NASSCOM (May 26, 2019), <https://community.nasscom.in/communities/policy-advocacy/nasscoms-comments-on-the-draft-e-commerce-policy.html>.

4.2 EXCESSIVE PROTECTIONISM

The draft policy addresses the genuine concerns of a developing nation like India in the global digital regime, which is dominated by developed nations. Treating individual data, as a national resource and its transfer being controlled by the government, is unjustified. The individual has a right over the data generated by his activity and transfer of such data may be allowed with his consent. The draft policy, does not allow transfer with consent of customer.⁹ The policy intends to nationalize the data and transfers the control of transfer in the hands of the government. The government is attempting to adopt an excessive protectionist regime. The government intends to treat the data as community asset and derive economic benefit as public trust. The approach suffers from a few deficiencies. First, it fails to address how such data shall be utilised by the government for the benefit of public. Second, the approach is based upon data localization and restriction upon the cross border data flow. The draft policy does not take into consideration the rationale and efficiency of these methods. Moreover, for ensuring public benefit it assumes that domestic enterprises are more beneficial than the foreign counterparts. This approach is devoid of reasons as it may be possible that a foreign enterprise may handle data more effectively than a domestic one. Government cannot escape from its obligation to ensure privacy of the citizens by way of restricting cross border data flows. The draft policy provides for discriminatory provisions in favour of the domestic players by restricting data flows with foreign enterprises which may be challenged before WTO for violation of principle of National Treatment found in Article 3 of GATT. All e-commerce sites or apps are required to have a

⁹ *supra* note 1, at 16.

registered entity in India.¹⁰ This reduces competition for Indian enterprises because the small and medium foreign enterprises might not be able to comply with the requirements.

4.3 PROBLEM WITH DATA LOCALIZATION

The draft policy suggests localisation of data generated in India. Such restriction may act as a barrier to trade and raise the costs of handling data. The US Trade Representative's 2019 National Trade Estimate Report on Foreign Trade Barriers state, "India has recently promulgated a number of data localisation requirements that would serve as significant barriers to digital trade between the US and India, the US strongly encourages India to reconsider the most discriminatory and trade-distortive aspects of this draft policy and the other measures described above."¹¹ Data localisation has been a measure to protect privacy. But, the viability of such measure may be a concern owing to lack of sufficient infrastructure in India.

4.4 OVERLAPPING WITH DATA PROTECTION BILL, 2018

The draft e-commerce policy prepared by the Department for Promotion of Industry and Industrial Trade contains six categories – Data, Infrastructure Development, E-commerce marketplaces, Regulatory issues, Stimulating the domestic digital economy and Export promotion through e-commerce. In regard to data protection, it overlaps with the Personal Data Protection Bill, 2018 (draft bill) which is based on Justice Shrikirishna committee report. The bill is prepared by the Ministry of

¹⁰ *Id.*, at 20.

¹¹ *US criticises India's data localisation norms, draft ecommerce policy*, CNBC TV- 18 (May 27, 2019), <https://www.cnbc18.com/economy/us-criticises-indias-data-localisation-norms-draft-ecommerce-policy-2891051.htm>.

Electronics and Information Technology (MeitY). The Bill is wide in scope and it covers the e-commerce sector. It allows data – sharing with the consent of the user, while the same is not allowed under the draft e-commerce policy. There may be a situation where conflict may arise between both the draft bill and the e-commerce policy. Such situations may cause uncertainty. Data protection measures should be done away with the draft e-commerce policy and should be solely governed by the Data Protection Act, eventually. It was suggested by the Ministry of Finance, a government official said “The draft data protection bill, which is being dealt by the information technology (IT) ministry, is not restricted to e-commerce companies but is applicable for every industry and sector. It is best if the issue is not a part of the e-commerce policy,”¹² The suggestions by the Finance Ministry must be incorporated so as to ensure that there is no overlapping and uncertainty which may arise due to parallel laws governing the same domain.

5. SUGGESTIONS

A few suggestions are provided for the draft policy in respect to cross border data transfers. First, the draft policy must restrict the regulations in respect to data generated by way of e-commerce transactions only as the personal data is being dealt under the Personal Data Protection Bill. The overlap between both may become an unwanted cause for legal uncertainty. Second, there is need to define the scope of community data with clarity and a need to provide a due process to enable its sharing. The policy needs to address the manner in which data shall be

¹² Shreya Nandi, *FinMin wants data protection provisions out of e-commerce policy*, LIVEMINT (May 26, 2019, 7:30 PM), <https://www.livemint.com/politics/policy/finmin-wants-data-protection-provisions-out-of-e-commerce-policy-1557773284732.html>.

utilised for the benefit of public in general and domestic enterprises. Third, the draft policy has adopted an excessive protectionist regime for cross border data flows. Data localisation method used to restrict data flow will create unnecessary expenditure and it may become hurdle in global trade. In alternate, the government can provide for free data flow but ensure high level protection for data generated by way of e-commerce transactions taking place in the country.

6. CONCLUSION

The draft policy addresses the major concerns which have been raised due to the increasing growth of the e-commerce sector in the India. The policy terms data as the new oil and has adopted an extreme protectionist approach towards the cross – border data flows. Such an approach has been adopted in an attempt to address the legitimate grievances of developing nation like India. The government must also consider the alternative approaches to data localisation and restriction upon the cross border data flows. Data localisation requires storage of data in India. Such storages may be an expensive affair and also expose the data to the risk of being hacked. In such cases, the costs may outweigh the benefits. The future impact of such a policy has to be kept in mind before it is to be implemented. The policy must comprehensively define its scope and lay down the provisions with clarity so as to avoid unfavourable consequences.