TAKSHASHILA INSTITUTION

Takshashila Policy Advisory

Comments to the Draft Personal Data Protection Bill, 2018

Takshashila Policy Advisory 2018-02

28 September 2018

By Ajay Patri | Manasa Venkataraman

This paper can be cited as "Patri A, Venkataraman M, *Comments to the Draft Personal Data Protection Bill*, Takshashila Policy Advisory, 2018-02"

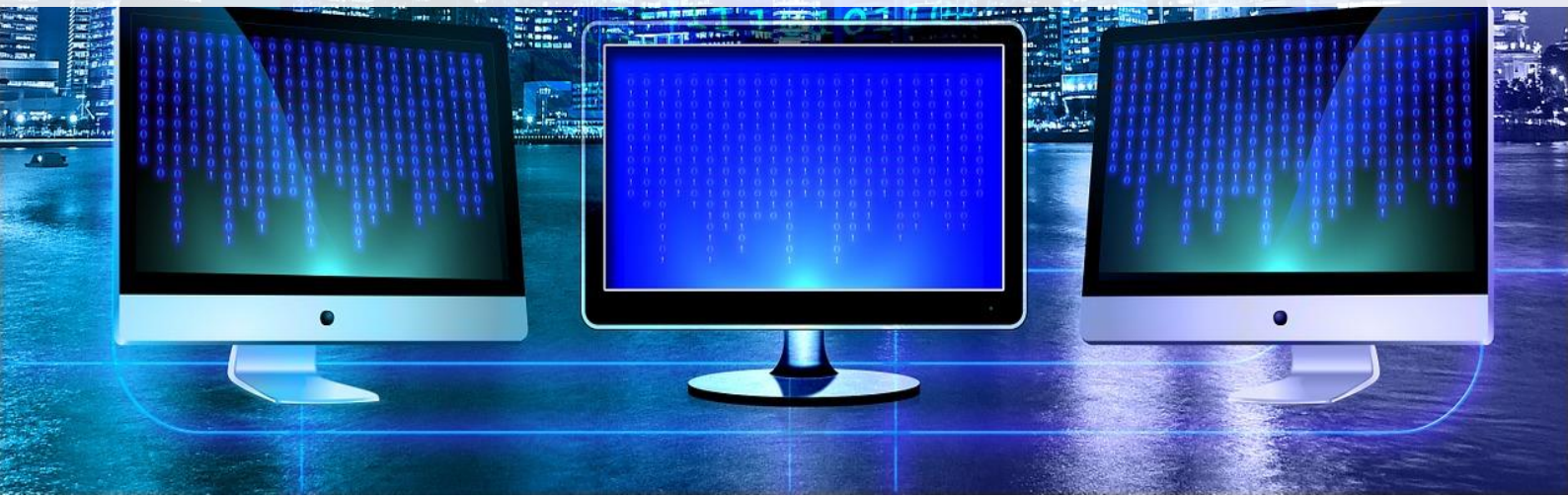

TABLE OF CONTENTS

Executive Summary

This document contains recommendations and comments in response to the draft Personal Data Protection Bill, 2018 (***Bill***) released by the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna (***Justice Srikrishna Committee***) in July 2018.

At the outset, we welcome the release of the Bill and the call for comments, however, we note that some aspects of the draft legislation demand further scrutiny. Our comments to the Bill focus on four distinct areas of the proposed legislation: (i) the exemptions granted to the State; (ii) restrictions on cross-border flows of personal data; (iii) the capacity of the proposed Data Protection Authority (**DPA**)*; and (iv) the excessive discretion allowed to the Union government and the DPA in certain circumstances.*

After examining the Bill's positions on these four aspects, we make the following recommendations:

1. ***Exemptions*** – The continued applicability of the fair and reasonable processing standard to the exempted scenarios under the proposed law is a step in the right direction. While it would have been prudent to extend additional safeguards of purpose limitation, collection limitation, and storage limitation to the exempted scenarios, the presence of S. 4 in the Bill should act as a safety blanket against unfair and unreasonable intrusions into the privacy of individuals. It is recommended, however, that the Bill expressly mention the need for appropriate judicial oversight as a necessary precondition for availing the exemptions by the State.

2. ***Restrictions on Cross-Border Flows of Data*** — We recommend that personal data and sensitive personal data be capable of easy transfer across Indian boundaries. In order to curtail the risk of this law being a deterrent for data fiduciaries servicing Indian customers, we recommend that "critical personal data" be defined narrowly and exhaustively in the law. We also recommend that localisation be mandated only for such data.

3. ***Capacity of the DPA*** – The DPA performs both a monitoring as well as adjudication function under the Bill and we anticipate that it is likely to soon be overburdened. We recommend that the DPA establish regional offices to function more efficiently. Data auditors should also be an independent and professional body.

4. ***Discretion to the Union Government and the DPA in Certain Scenarios*** – We recommend that the discretionary powers extended to the State be narrow. Owing to the unique position and responsibilities of the State as a data fiduciary, specific provisions must be made in the Bill with respect to penalties, qualifying as a

significant fiduciary, as well as limitations on the State's power to circumvent consent for the collection of personal data in some circumstances.

Introduction

On 27 July 2018, the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna released the report titled *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*[1] (the Report) and the draft *Personal Data Protection Bill, 2018*[2] (the Bill). Together, these documents outlined a framework to govern the protection of personal data in India. On 14 August 2018, comments were invited from the general public to the Bill. This paper sets out the Takshashila Institution's views on the Bill.

The publication of the Report and the Bill is a positive development. They represent the next logical step to the Puttaswamy decision from 2017 that recognised privacy as a fundamental right under the Indian Constitution.[3] The documents are comprehensive and provide the perfect starting point for a nuanced conversation around the data protection framework India must adopt.

This paper focuses on the following aspects of the Bill:

1. The exemptions granted for data processing in the interests of security of the State and to facilitate actions of law enforcement agencies.

2. The restrictions on cross-border flows of personal data.

3. The capacity of the proposed Data Protection Authority (the DPA).

4. The excessive discretion granted to the Union government and the DPA under certain scenarios.

Exemptions

Position Under the Bill

Chapter IX of the Bill outlines scenarios in which safeguards provided under the Bill are not applicable. In particular, S. 42(1) provides an exemption for the processing of personal data if it is done "*in the interests of the security of the State.*" Similarly, S. 43(1) provides an exemption for the processing of personal data if it is done "*in the interests of prevention, detection, investigation, and prosecution of any offence or any other contravention of law.*"

It is encouraging that these exemptions are only available if they are authorised by a statute. The provisions also expressly mention that the exemptions can be availed only if the standards of necessity and proportionality are satisfied. As commented elsewhere, these safeguards strike at the heart of any mass surveillance programme conducted by the State as well as any surveillance that acts in the absence of a legislative backing.[4]

The exemptions under S. 42 and S. 43 are also not absolute. The processing under these provisions is still subject to certain safeguards under the Bill. This includes S. 4, which mandates that any processing of personal data must be done in a fair and reasonable manner, and S. 31, which obliges data fiduciaries to ensure that adequate security safeguards are in place when they process personal data.

Critical Analysis

There are two issues of note in the position established in the Bill with regard to exemptions. One, the wide-ranging scope of fair and reasonable processing as provided for under the Report is a positive measure. Two, the lack of any enumeration of judicial oversight in the Bill for the activities under S. 42 and S. 43 is a cause for concern and must be addressed.

Scope of Fair and Reasonable Processing

The Bill does not define what fair and reasonable processing entails, except to say that it should respect the privacy of the data principal. However, the Report addresses this matter at some length:

"*The obligation to process fairly implies that the data fiduciary must act in a manner that upholds the best interest of the privacy of the principal. Further, the obligation to process reasonably also implies that the processing must be of such a nature that it would not go beyond the reasonable expectations of the data principal.*"

The high standard set by this explanation of the terms fair and reasonable is a positive measure.

At the same time, the Bill excludes certain protections from the purview of S. 42 and S. 43. This includes the following:

1. *Purpose limitation under* S. 5: Data should be processed for specified purposes only.

2. *Collection limitation under* S. 6: Data collected should be limited to that which is necessary for the purpose of processing.

3. *Data storage limitation under* S. 10: Data should be stored for only as long as it is necessary for the purpose for which it is collected.

There is merit in the argument that these protections must continue to apply in scenarios where the State seeks the exemptions under S. 42 and S. 43.

The Report provides an explanation for their inapplicability to S. 42 by stating that since the activity in question is covert and there is no question of consent being taken, principles such as purpose limitation and storage limitation can be done away with. However, the issue of consent not being taken should not prevent the State entity from adhering to these obligations. In fact, there are several non-consensual grounds under the Bill where these obligations are still applicable. The same standard can be extended to S. 42 as well.

Similarly, the explanation provided for S. 43 states that a strict standard of purpose specification will hinder investigations where enforcement agencies are unaware of what direction their investigations will take and how they will conclude. It follows this up by stating that investigations might still have a broad purpose but that this *may* not meet the standard of purpose specification under the law. This argument is not clear enough to justify the exclusion of the safeguards mentioned above.

It is also odd that S. 43(4) does impose a degree of storage limitation by stating that personal data should not be retained after the purpose of prevention, detection, investigation, and prosecution of any offence or any other contravention of law is complete, unless such retention is required to deal with future offences. It is unclear why a similar protection is not extended to the processing under S. 42.

Having said that, the scope of fair and reasonable processing as defined above is wide enough to account for some of the protections outlined above. The way it has been framed in the Report is akin to an accountability model that requires an entity that is processing data to ensure that it does so while keeping the best interests of the individual in mind.[5]

Judicial Oversight

While the Bill provides the exemptions as discussed above, it leaves the exact contours of the State's actions thereunder to be governed by subsequent legislation. The Report mentions that any such legislation should incorporate both judicial and parliamentary

oversight over the State's actions. However, the Bill itself does not expressly mention the requirement of such oversight.

The Report is not a binding document by itself. On the other hand, the Bill, if passed, will be. Given this, the lack of any mention of judicial oversight in the Bill leaves the door ajar for a future law on surveillance to ignore the recommendation from the Report.

Comments and Recommendations

The effectiveness of a law on data protection will be affected by the position it takes on the subject of surveillance.[6] Given this, and after accounting for the preceding discussion, this paper makes the following comments and recommendations:

1. *On the scope of fair and reasonable processing*

   The continued applicability of the fair and reasonable processing standard to exempted scenarios is a step in the right direction. While it would have been prudent to extend the additional safeguards under S. 6 (purpose limitation), S. 7 (collection limitation), and S. 10 (storage limitation) to the exemptions granted under S. 42 and S. 43, the presence of S. 4 should act as a safety blanket against unfair and unreasonable intrusions into the privacy of individuals.

2. *On judicial oversight*

   In addition to the requirement of necessity and proportionality, and the need for legislative backing, the Bill must expressly mention the existence of appropriate judicial oversight as a precondition for the granting of an exemption under S. 42 and S. 43.

Restrictions on Cross Border Flows of Personal Data

Position Under the Bill

Chapter VIII lays down the conditions on which personal data, sensitive personal data and "critical personal data" can be transferred out of Indian borders. S. 40, while introducing the data localisation framework that will underscore most processing of personal data, proscribes "critical personal data" from travelling outside the country.

The other contours of S. 40 and S. 41 are examined in greater detail in this paper.

Critical Analysis

Data Localisation as an Excessive Burden on Businesses

Localisation of personal data is mandated by requiring the data fiduciary to store a serving copy of the data in India. The fiduciary must also establish a server or data centre in India which stores all personal data collected or processed falling within the purview of this law. These requirements are significant cost burdens.

The DPA is established as the gate-keeper for cross border flow of data, especially sensitive and critical personal data. Additionally, the Union Government is empowered to notify: (i) the conditions upon which fiduciaries may transfer data across Indian borders; and (ii) restrain the flow of certain kinds of data as it deems fit.

Given the speed at which data trades hands in a technologically advancing world, these provisions might handicap businesses considerably. The DPA should have been burdened with fewer responsibilities vis-à-vis the transfer of personal data in the course of regular business.

As notifications, rules and other subordinate legislations by the Union/State Government do not fall within the meaning of "law", the powers allowed to the Union Government to notify conditions of cross border flow under this Chapter might go unchecked.

The immense compliance burden introduced in Chapter VIII is likely to disincentivise innovation within the country [as well as the provision of services from businesses outside India].

Data localisation is also likely to disincentivise foreign businesses from serving Indian data principals. Aside from the compliance burden, the inability to share customer data

within the organisation, albeit across borders, is clearly discouraging to these fiduciaries. Localisation creates entry barriers and hinders a free economy.

It is submitted that the fiduciary's duty to be fair and reasonable while processing any kind of personal data is sufficient to ensure their compliance. Therefore, cross-border transfers that happen in the normal course of business of a data fiduciary must not be subject to the additional minute scrutiny by the DPA.

The lack of clarity on the scope of "critical personal data"

S. 40(2) proscribes "critical personal data" from being transferred outside the country, i.e., it is to be processed only within India and stored on a server also located within India. There are very limited circumstances (as envisaged in S. 41(3)) under which such data can travel outside India, and even then, with the specific permission of the Union Government.

For a provision that imposes such a blanket restriction on a category of data, neither the Bill nor the Report provide much clarity on the scope of this term. In fact, the Report indicates that the term refers to any kind of data critical to India's national interest. It goes on to state that the term, because of its reference to India's national interest, will include government services, infrastructure and any other kind of data relevant to the functioning of the Indian economy.

Such broad premises for the interpretation of critical personal data will be detrimental, and will in fact allow the State to adopt protectionist interpretations of the term. Owing to the limitations imposed on the flow of such data, the term should be defined and interpreted narrowly, so that it is only invoked where necessary. Most importantly, this term must not be defined by the Union Government through a notification – it must be defined in the statute. This will operate as an effective check on the Government's discretion to expand the scope of this term at will. By being defined in the statute the term falls within the meaning of "law", and will have to abide by the conditions imposed by the Puttaswamy judgment (i.e., privacy may only be circumvented, inter alia, by an authority of the law).

Comments and Recommendations

1. *On the definition of critical personal data*

   The term "critical personal data" should be defined to include only that data which is crucial to the Indian national interest. This term should also be defined in the statute so that it mitigates the risk of state overreach.

2. *On limiting the scope of data localisation*

It is crucial that data localisation be restricted only to critical personal data – this will enable the localisation requirement to be restricted to only that data which is directly linked to the security of the state. The threat of a localisation provision in the Bill has already prompted protectionist e-commerce and pharmacy policies. Mandating data localisation in the Bill will only translate into more and more stringent embodiments of this requirement in subsequent regulation – making India an increasingly unfriendly business environment.

3. *On restricting the DPA's powers to regulate data transfers*

Taking the DPA's approval before every data transfer is also a deterrent for data fiduciaries. This requirement should be lifted, except in cases of a merger or restructuring of an Indian data fiduciary with a foreign fiduciary, or in cases where it is critical personal data that is to be transferred out of India.

Capacity of the DPA

Position Under the Bill

The Bill outlines the creation of an independent DPA, comprising a Chairperson and six whole-time members. The functions of the DPA are provided for under S. 60 of the Bill, which contains a list of 24 functions. This includes the following:

1. S. 60(2)(i), which authorises the DPA to specify "*the requisite qualifications, code of conduct, practical training and functions to be performed*" by data auditors.

2. S. 60(2)(k), which empowers the DPA to monitor cross-border transfers of personal data.

Critical Analysis

The DPA has a vital role to play in the overall data protection framework as set out in the Bill. It is important, therefore, that the DPA possess the requisite capacity to perform all tasks assigned to it in a time-bound manner. A failure to do so will have negative repercussions on the functioning of data fiduciaries in the country, who would face uncertainty in their day to day operations. This, in turn, would have a knock-on effect on data principals.

Given this, the current strength of the DPA may not be sufficient for the volume of work that such a body will encounter once the law is in place. It would be prudent to conduct a capacity assessment exercise to determine the adequate capacity of the DPA. The Report does recommend that such an exercise be undertaken by the Union government to determine the number of Adjudicating Officers who would be a part of the Adjudication Wing under the Bill. We recommend that a similar exercise be conducted for the DPA as well. This exercise must also consider the possibility of establishing regional offices of the DPA. While this has been envisaged under S. 49(4) of the Bill, the final decision to do so is left to the DPA itself.

Aside from having an adequate number of members, the capacity of the DPA must also be examined in light of whether it is best-placed for carrying out certain functions, particularly the two highlighted above.

Data Auditors

Like the DPA, data auditors perform an important function under the Bill. They help data fiduciaries ensure compliance with the law and facilitate the adoption of processes that safeguard the privacy of data principals. Their function can be likened to that of professionals such as lawyers and financial auditors.

The regulation of data auditors as provided for in the Bill, including the determination of their qualifications, code of conduct, practical training, etc., is a massive undertaking. It

would be a function that would best done by a specialised organisation rather than the DPA, which has a broader mandate.

Given this, it would be prudent to explore the possibility of data auditors being classified as a professional class with its own distinct set of rules and regulations. This could take the form of setting up a statutory body that regulates the profession, similar to the function the Bar Council of India performs with lawyers and the Institute of Chartered Accountants of India with chartered accountants.

Monitoring Cross-Border Transfers of Personal Data

The Bill should, to the extent possible, lower the restrictions on cross-border transfers of personal data. One of the means of achieving this is by examining the role played by the DPA in such transfers.

S. 41(1)(a) empowers the DPA to approve standard contractual clauses and intra-group schemes that govern data transfers. While the intent behind this provision is to pre-empt any harm that might be caused to data principals, its implementation might be an undue burden on the DPA. The Report does not rely on any studies that can suitably anticipate the number of such applications for approval that the DPA is likely to face.

Similarly, S. 41(1)(b) permits transfers to such jurisdictions which ensure an adequate level of data protection. The Union government is expected to consult the DPA before arriving at a decision in this regard. The capacity of the DPA to render effective advice in such situations must also be examined.

A better alternative to these measures would be to subject cross-border transfers of personal data to mandatory audits. This would provide data fiduciaries the ability to incorporate changes in their data transfer policies that are in the best interests of data principals as well as understand the scope of data protection available in other jurisdictions.

Comments and Recommendations

This paper makes the following recommendations with regard to the capacity of the DPA:

1. *On the composition of the DPA*

   A capacity assessment exercise must be undertaken to determine the strength of the DPA and the possibility of establishing regional offices.

2. *On data auditors*

   The Bill should not entrust the DPA with the responsibility of regulating data auditors. This task must be fulfilled by a separate professional body.

Similar to the oversight bodies for other professionals such as chartered accountants and company secretaries, the oversight body for data auditors should also be independent. This will enable it to set the industry standards for qualification and practice, establish codes of conduct, and allow for a new body of professionals to emerge in a systematic manner.

3. *On the monitoring of cross-border data transfers*

The Bill should refrain from providing the DPA with the power to approve contractual provisions of entities or engage in an exercise to determine the robustness of data protection frameworks in other jurisdictions. Instead, it must mandate that the data fiduciaries who seek to transfer personal data outside Indian territory must subject their processes to audits under the law.

Discretion to the Union Government and the DPA under certain scenarios

Position Under the Bill

The Bill carves out discretionary powers to the Union Government in two ways: (i) by allowing some exemptions to the collection, processing and storage of personal data by the Government; and (ii) by enabling it to perform some actions not necessarily in keeping with other similar provisions in the Bill.

The following provisions are examined in detail:

1. Section 13, Chapter III;
2. Section 19, Chapter IV;
3. Chapter VII – Transparency and Accountability Measures;
4. Chapter XI – Penalties and Remedies;
5. Chapter XIII – Offences.

Critical Analysis

Processing by the State

The first example of this discretion is in S. 13 and S. 19 of the Bill. The State is allowed to process personal data (S. 13(1)) and sensitive personal data (S. 19(1)) when it is necessary for the functioning of the Parliament or a State Legislature. Further, the State may also process personal or sensitive personal data where it is necessary for the provision of any service or benefit by the State, as authorised by law.

It is unclear why this provision has been carved out specifically with reference to the State's legislative and service provision wings. Additionally, upon closer examination of these sections, a few other inconsistencies emerge. It appears that the State is not required to obtain consent for the processing of personal data. Secondly, while S. 13 contains the requirement of "necessity" and S. 19 requires the State to process personal data where "strictly necessary", these might not be sufficient protections to the individual data principal.

S. 13 and S. 19 also do not consider subordinate legislation. Much of the legal framework for the processing of personal data will be through rules and regulations drafted under a

statute, and also through executive notifications by sectoral regulators (such as the Reserve Bank of India, the Telecom Regulatory Authority of India, etc.). In fact, it is more likely that the State will need to process personal data in these capacities than when exercising its Parliamentary function. It is, therefore, not only difficult to determine the intent behind S. 13(1) and S. 19(1), but also its relevance.

Transparency and Accountability Measures

Chapter VII sets out several checks and balances for entities that can be classified as "significant data fiduciaries." These measures include conducting impact assessments, appointing a data protection officer, carrying out periodic audits, etc. One of the criteria for being classified as a significant data fiduciary is turnover. It is unclear how this qualifying feature will be applied to State entities.

Penalties on State Entities

A difference is apparent between the provisions pertaining to penalties and those setting out remedies for offences. Unlike the liability for an offence committed by the State, for which the head of the concerned department will be held accountable, there is no penalty provision carved out for harm caused by improper processing of personal data by the State.

S. 69(2) states that a contravening data fiduciary will be liable to pay a penalty of either Rs. 5 crores or up to 4% of its total worldwide turnover. It is unclear how the State will be penalised for any processing in contravention of the Bill.[7]

Comments and Recommendations

1. *Penalty provisions should be designed for data fiduciaries that are state entities*

   The penalties imposed on a non-compliant data fiduciary under the statute are tied to its worldwide turnover. This would make these penalties difficult to calculate where the State is the data fiduciary. The penalties for state entities that are data fiduciaries should therefore be put in place in the Bill.

2. *It is possible that a data fiduciary that has a wealth of principals' data does not meet the turnover criteria set out in the Bill.*

   This limitation becomes more apparent where the data fiduciary is a State entity. The Bill should, therefore, not restrict itself to the turnover of a data fiduciary alone to determine whether it is a significant fiduciary or not. Other criteria, such as the number of individuals whose data is collected and processed by the fiduciary, should be computed to determine if an entity is a significant data fiduciary.

3. *The principles of purpose limitation and necessity should apply to Ss. 13 and 19*

The liberty given to the State to access and utilise personal data for Parliamentary purposes as well as for the purposes of providing a service should be removed. The State should take the principals' consent when data is collected for these purposes.

Additional Comments

The list of comments in this paper addresses some of the most pressing concerns with the Bill in its current iteration. There have also been several efforts in the weeks since the documents were released to conduct discussions with experts and stakeholders on the potential impact of the Bill.

The Takshashila Institution organised one such roundtable on 10 August 2018 to provide a platform for more discussions on the Bill and the Report. The output of this exercise was a Blue Paper that collated the main points of discussion and analysis.[8] The comments in the Blue Paper form a useful collection of comments that the Committee can examine for further feedback on the Bill.

References

[1] *A Free and Fair Digital Economy: Protecting Privacy, Empowering Indians*, Report of the Committee of Experts under the Chairmanship of Justice B. N. Srikrishna. Last accessed 3 September 2018. http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf
[2] *The Personal Data Protection Bill, 2018*. Last accessed 3 September 2018. http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf
[3] Justice K. S. Puttaswamy (Retd.) v Union of India, (2017) 10 SCC 1.
[4] Vrinda Bhandari, "Data Protection Bill: Missed Opportunity for Surveillance Reform," Bloomberg Quint, 29 July 2018. Last accessed 3 September 2018. https://www.bloombergquint.com/quint/2018/07/29/personal-data-protection-bill-2018-draft-srikrishna-committee-loopholes-surveillance#gs.f=_awWk
[5] Rahul Matthan, *Beyond Consent – A New Paradigm for Data Protection*, Takshashila Discussion Document, 2017-03. Last accessed 19 September 2018. http://takshashila.org.in/wp-content/uploads/2017/07/TDD-Beyond-Consent-Data-Protection-RM-2017-03.pdf
[6] Gautam Bhatia, "Gautam Bhatia dreams of genuine data protection in India," Livemint, 11 August 2018. Last accessed 3 September 2018. https://www.livemint.com/Leisure/RuHOGczbrpt33v5ijP987M/Gautam-Bhatia-dreams-of-genuine-data-protection-in-India.html
[7] Rahul Matthan, "The Achilles heel of the draft personal data Bill," Livemint, 31 July 2018. Last accessed 7 September 2018. https://www.livemint.com/Opinion/sgjyNwQ6yBTBsKz1LAYVuJ/The-Achilles-heel-of-the-draft-personal-data-Bill.html
[8] Blue Paper: Justice Srikrishna Committee Documents on Data Protection, published by the Takshashila Institution. Last accessed 5 September 2018. http://takshashila.org.in/takshashila-policy-research/takshashila-blue-paper-roundtable-on-justice-srikrishna-committee-documents/
[9] Vinay Kesari, "Data Localisation and the Danger of a Splinternet". Last accessed 19 September 2018. https://factordaily.com/data-localisation-and-the-danger-of-splinternet/
[10] Saritha Rai and Archana Chaudhary, "India reviews draft e-commerce policy after criticism". Last accessed 19 September 2018. https://www.livemint.com/Industry/EyPAfhcNV8wAXONlIDq8sI/India-reviews-draft-ecommerce-policy-after-criticism.html