Personal Data Protection Bill, 2019: Looking at social media intermediaries and significant data fiduciaries

As the Joint Parliamentary Committee considers the Personal Data Protection Bill, 2019, MediaNama will publish a series of articles from legal experts focussing on the key aspects of the Bill and how they will affect users and companies. This is the fourth article in the series. Read our extensive coverage of the Bill here.

By Sajan Poovayya and Priyadarshi Banerjee

The story of internet penetration in India coinciding with the boom in mobile telephony implies that most users in India access internet only through smartphones. While no doubt, this may facilitate access to the internet at an unprecedented scale, it also calls for attention to the typical user behaviour whereby consumers unwittingly agree to submit their personal information to social media apps and other similar platforms, for free use of their services. This pattern of behaviour and its global exploitation have come to the fore in recent times raising concerns in terms of *inter alia* a data principal's privacy and larger societal concerns in terms of micro-targeting of users, utilising personal data shared on social media platforms and its effects on electoral democracy, etc.

Much of the public attention that the subject of data protection had received in this country stemmed from concerns of unauthorised and opaque sharing of personal data by data fiduciaries with third parties, without the knowledge or consent of the data principal. Further, recent controversies about distortion of electoral views through means of unauthorised and clandestine sharing and processing of personal data necessitates an analysis to see how the Personal Data Protection Bill, 2019 (the "2019 Bill"), measures up to such recent challenges.

Sharing of personal data by social media Intermediaries

The proposed law seeks to safeguard the personal data of users (or data principals) by creating a tiered regime of informed consent for collection and processing of personal data, in a bid to reduce the opacity in data flow. The legislative idea seems to be to put the data principal in the driving seat and guarantee her a degree of autonomy and control over her own personal data. Before embarking on examining whether the 2019 Bill is equipped to deal with a situation akin to the Cambridge Analytica fiasco, consider the following:

1. A class of intermediaries under the proposed legislation are classified as 'social media intermediaries' which are intermediaries who primarily and solely enable online interaction between two or more users and allow them to create, upload, share, disseminate, modify or access information using its services;

2. A subset of personal data is separately defined as 'sensitive personal data' [Section 3(36)] which is an enumerated class consisting of data relating to financial information, health, sexual privacy, caste/tribe status, religious or political belief or affiliation. Such sensitive personal data is subject to a heightened level of protection, safeguards or restrictions in terms of regulations which may be subsequently formulated by the Data Protection Authority of India, created under this statute; and
3. Under Section 26 of the 2019 Bill, certain thresholds in terms of volume of personal data processed, the sensitivity of personal data processed, risk of harm, etc., are specified, upon satisfaction of which, the Data Protection Authority may notify a data fiduciary as a 'significant data fiduciary'. The 2019 Bill further mandates that the Central Government 'shall' notify any social media intermediary as a significant data fiduciary if its actions have, or are likely to have a significant impact on electoral democracy, etc. Therefore, subject to any future notification by the Central Government, major social media intermediaries are as such liable to be notified as significant data fiduciaries which must comply with specific obligations under the proposed legislation.

How does the proposed law tackle the sharing of personal data by a social media intermediary with downstream data processors? Can a social media intermediary share personal data with a research company, which in turn may share it with a political party that uses it to micro-target voters?

Under the 2019 Bill, a data fiduciary (which would include a social media intermediary) is obligated to obtain consent for collection of data under Section 7, and consent for processing under Section 11. While seeking consent (by providing notice to a data principal at the time of collection of personal data) under Section 7, a data fiduciary must state the purposes for which the personal data is to be processed [Section 7(1)(a)], and inform a data principal about the individuals or entities including other data fiduciaries or data processors with whom such personal data may be shared [Section 7(1)(g)]. In this context, under Section 11(3), explicit consent is required for processing any sensitive personal data. The 'religious or political belief or affiliation' of a data principal is defined as sensitive personal data under Section 3(36)(xi) of the 2019 Bill.

> Therefore, **opaque unilateral sharing of personal data without intimation and consent of the data principal is ruled out under the proposed law.** A data principal must be made aware of sharing of any personal/sensitive personal data with a third party through a notice under Section 7(1)(g).

Now, the obligations on any such third-party recipient of personal data and what activities it may undertake thereon are governed by the provisions of Section 31 of the 2019 Bill. Under Section 31(1), the data fiduciary (including a social media intermediary) must enter into a contract with any data processor to engage it for processing personal data. Under Section 31(3), such data processor

who receives personal data under a contract from a data fiduciary may only process such data in accordance with the instructions of the data fiduciary and is further prohibited from sub-contracting with another data processor under Section 31(2) unless the principal data fiduciary has explicitly permitted so in its contract with the data processor. Also, the data processor receiving personal data from a data fiduciary under Section 31 is obligated to treat such data as confidential.

> Therefore, under the scheme of the proposed law, the data fiduciary at all times is in fiduciary control over the personal data and **no processing is permissible by a downstream data processor unless so explicitly permitted** under Section 31(2).

This, read with the data fiduciary's obligation to notify the data principal at the time of collection about the entities with whom personal data may be shared, implies that the data principal shall be transparently aware of the fate of any personal data which it reposes with such a data fiduciary.

The legal architecture as proposed in the 2019 Bill does not in essence prohibit the sharing of data by social media intermediaries with third parties. The proposed law requires that the user be furnished with notice of the possibility of such usage while her data was collected or subsequently processed. If the processing is that of sensitive personal data, then a specific consent is required from the data principal. Although it may seem, that a prohibitory framework (in terms of preventing sharing of personal data to third parties altogether) would have better served the interest of data principals, the proposed law seeks to create a consent-based framework which averts the crippling effect an all-or-none prohibitory framework may have had on the digital economy. The law seeks to strike a balance between the rights of the data principal and the business efficiencies which big data processing ushers in.

Remedies available to a data principal for breach of obligations

In light of the above, if a downstream data processor or data fiduciary unauthorizedly shares personal data with any other entity, it will fall foul of the proposed law, and an affected data principal may seek redressal under the provisions of Section 32. Redress under Section 32 may be sought from the data fiduciary itself, whereas under Section 32(4), if the data principal is dissatisfied with the response from a data fiduciary, she may file a complaint with the Data Protection Authority.

Further, an affected data principal may also invoke the jurisdiction of the Data Protection Authority under Section 53 for appropriate redress in case of any unauthorised sharing of data, seeking an inquiry by the Authority against the data fiduciary for conducting itself in a manner which is detrimental to the interest of data principals or for contravening the provisions of the law. Additionally, under Section 53, the Data Protection Authority has the power to *suo*

moto inquire into any activities of the data fiduciary if it has reasonable grounds to believe that certain processing of personal data is in contravention of the law or detrimentally affects the interest of the data principal.

In case of unauthorised profiling or micro-targeting of data principals which is in violation of the scheme as delineated above, leading to electoral distortions, even the Election Commission may initiate the process of inquiry by making a complaint to the Data Protection Authority as Section 53 does not stipulate any restrictions as regards who may initiate such a complaint. A recalcitrant data fiduciary or a data processor would be liable for compensation under Section 64.

Deterrent principle and its glaring omission

It is curious that the 2019 Bill deletes two significant provisions from its previous version as were proposed by the Justice B.N. Srikrishna Committee along with its 2018 version of the Bill. Two provisions from the older draft (Sections 90 and 91 of the 2018 Bill) — which had explicitly made obtaining, transferring or selling of personal data/sensitive personal data contrary to the provisions of the 2018 Bill an offence, — are now omitted. Inasmuch as the Justice Srikrishna Committee had adopted the deterrence principle as a necessary postulate for data protection, this glaring omission is a major departure therefrom.

The 2019 Bill falls seriously short of emancipating a data principal in terms of remedies afforded under it, when it proposes a truncated chapter on offences and simultaneously requires that no court shall take cognizance of any offence under this law unless the complaint in that regard is made by the Authority. The requirement to route the criminal process through the Data Protection Authority, in a manner, robs the data principal's agency to protect her personal data, which too, is a serious dilution of the deterrence principle adopted by the Justice Srikrishna Committee.

How does the proposed law deal with a political party that uses the data collected through its app to micro-target voters?

In connection with the data sharing fiasco surrounding Facebook and Cambridge Analytica, it is imperative to also consider the possibility of political parties themselves collecting data directly through some mobile applications for the purpose of micro-targeting voters. Possibly, surreptitiously. While it is possible that an application is facially innocuous (such as a meme-generator, a game, a pop quiz, etc.), the data collected in the process of using it may have a far reaching impact on the informational autonomy of a data principal. For instance, location data, cookies saved on a browser, search history, may, when aggregated or combined, create a profile of an individual for the purposes of micro-targeting.

Micro-targeting is a form of online targeted advertising which analyses personal data to identify the interests of a specific audience or individual in order to

influence their actions. It may be used to offer a personalised message to an individual or audience using an online service such as social media. It may determine what and how relevant content is delivered to an individual online and is sometimes used to market goods or services *and* for political marketing. For example, if you express an interest in a certain political party or ideology on a social network , personalised advertisements related to that party or ideology may be displayed to you; or, a political party may target propaganda material towards a data subject once it is aware of a particular political inclination of hers. There have been serious concerns of electoral manipulation through such means, the primary objection being that the data principal may not be even aware that she is being targeted.

Under the 2019 Bill, inasmuch as such a political party is collecting personal data of voters, it would be a data fiduciary under the 2019 Bill, as proposed. *Stricto sensu*, under the provisions of the proposed law, since political belief or affiliation is a sensitive personal data, such a data fiduciary (which in the present example is a political party) may also be notified by the Data Protection Authority as a 'significant data fiduciary' under Section 26 of the 2019 Bill. Therefore, such political party, being a data fiduciary, shall be required to issue notice of information (under Section 7) to the data principal at the time of collection of personal data specifying *inter alia*, the purposes for which such data may be processed. Also, under Section 11, the political party would need to obtain consent for processing the same from the data principal.

However, the status of a 'significant data fiduciary' is dependent on the affirmative act of notifying one as such, by the Data Protection Authority. Inasmuch as the appointment of the members of that Authority is at the hands of the Executive Government, its impartiality must be zealously maintained. In this regard, the legislative proposal of the Justice Srikrishna Committee was farsighted when it proposed a judicial member (the Chief Justice of India or her nominee) be in the selection committee to ensure transparency and fairness in such appointment. However, the 2019 Bill seeks to constitute the selection committee solely with bureaucrats as its members.

> Therefore, while in the minimum **such a political party has to comply with the requirements of informed consent for collection and processing of data under Sections 7 and 11 of the 2019 Bill, which itself provides a degree of safeguard to a data principal, such a political party may also be required to adhere to the additional obligations of a significant data fiduciary, if they are notified as such.** Once more, the legislative proposal seeks to usher in a regime of informed consent to provide a degree of informational autonomy to a data principal, which hitherto had been completely absent.

Conclusion

The development of a legal regime for data protection in India is presently in its nascency. Thus, it is fairly early to undertake a complete analysis of the data protection regime that is sought to be set up under the 2019 Bill. The Bill itself has multiple creases to be pressed out, some of which have been highlighted above. Additionally, contours of much of the protections are to be laid down through regulations once the law is operationalised. It is only when the Data Protection Authority is set up under the enacted statute that it shall commence the process of formulating Codes of Practices as required under the law. Therefore, weighing the efficacy of the entire process at present shall be no better than a soothsayer's chant. However, a robust framework has indeed been formulated after a herculean effort from both the Executive Government and the civil society participants in the process, which it is expected shall only be strengthened through parliamentary debate as this new regime is legislated.

*

Sajan Poovayya *is a Senior Advocate practising in the Supreme Court of India. He has a vast experience in technology laws and regularly appears before various judicial fora on issues pertaining to technology and its interface with domestic legal obligations, both statutory and constitutional.*

Priyadarshi Banerjee *is an advocate practicing before the courts in Delhi, and has represented multiple social media companies in myriad litigation revolving around issues of privacy, intermediary liability and digital rights.*

Edited by Aditi Agrawal