Amrut Joshi Founder
amrut@gamechangerlaw.com
Namrata Bhagwatula Senior Associate
namrata@gamechangerlaw.com
GameChanger Law Advisors

State of the nation: Examining India's current and future data protection regime

Image: Bruno Nascimento / Unsplash.com

With Moore's law reaching its saturation, and almost all objects around us slowly coming to life with the Internet of Things, we have reached that stage of human civilisation where we are leaving our digital footprints and transmitting data at a rate faster than the human ability to process such data. This progress in the rate of exchange, transmission, storage and processing of data has also called for lawmakers around the world to protect and secure such data as well as to protect the privacy of individuals, including in India. Amrut Joshi and Namrata Bhagwatula, Founder and Senior Associate respectively at GameChanger Law Advisors provide an overview of the existing data protection framework in India and look ahead to the future in light of recent jurisprudence and legislative proposals.

Scattered data protection regime

Currently the data protection regime in India comprises of a multitude of legislation, both general and sector-specific, including:

(a) The Information Technology Act, 2000 ('the IT Act'), which represented India's first legislative attempt to regulate transactions on the information highway. However, this legislation was designed at a point in time which can best be described as 'Web 1.0.' During the last 18 years, while the IT Act has granted legal recognition to electronic transactions, it has not really served as an effective policing mechanism against fraudulent and other undesirable transactions.

(b) The Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011 ('the SPI Rules') issued under the IT Act, which only apply to private entities. The SPI Rules mandate certain requirements to be fulfilled by such private entities for collection of sensitive personal information ('SPI'), and restrict the sharing of SPI without the subject's consent. It is pertinent to note, however, that SPI only refers to a very specific class of information like sexual orientation, medical records and history, biometric information, and financial information, etc. Since large swathes of information (for example, email addresses, phone numbers, locations etc.) are not considered as SPI, the ambit of these SPI Rules is constricted in nature. Further, this restriction on sharing of SPI is only limited to non-state parties, and such non-state parties do not require the consent of the data subject before sharing such information with any governmental authority or agency.

(c) The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 ('the Aadhaar Act') permits the Government of India to collect identity information, including biometrics, from its citizens, in order to issue a unique identification number on the basis of such biometric information. The Aadhaar Act and the regulations thereunder provide for various data protection principles to be followed by the Unique Identification Authority of India to protect such information collected under the Aadhaar Act. A constitutional challenge to the Aadhaar Act is currently pending in the Supreme Court of India. While the security of the information collected under the Aadhaar Act is under severe public and judicial scrutiny as of now,

it will be interesting to analyse how the Aadhaar Act will be juxtaposed *vis-à-vis* the data protection framework being currently contemplated by the Committee (examined further below).

(d) The Credit Information Companies (Regulation) Act, 2005 ('the CIC Act') and the regulations framed thereunder govern the protection of data in the financial sector. The Reserve Bank of India ('RBI') is the regulatory body that oversees the implementation of the CIC Act. The CIC Act particularly deals with credit information companies and recognises them as collectors of information. The CIC Act requires the collectors of financial information to comply with various internationally accepted data protection principles like data collection limitation, data use limitation, data accuracy, and data retention and access.

(e) The RBI has also issued various regulations, notifications and master directions, including the Know Your Customer ('KYC') norms, which specify the categories of information which may be collected by banks and financial institutions from their customers. It also imposes on such collectors of information, the obligation to keep such information confidential.

(f) While there are various regulations governing the telecommunication sector, the data protection norms in the telecom sector are primarily governed by the Unified License Agreement ('ULA') issued to telecommunications service providers by the Department of Telecommunications ('DoT'). The DoT, through such ULAs, prescribes the formats for collection of information as well as the necessary steps to be taken to safeguard the privacy and confidentiality of the collected information.

Proposal of a new framework

On a review of the various pieces of legislation described above, it was felt by a number of judicial experts that principles of data protection were incorporated in a haphazard manner by different regulatory authorities operating in their respective silos. Given that the issue of data protection is all-encompassing, as the data of individuals is gathered on a day-to-day basis by a multitude of service providers and government agencies, the Government of India initiated the process of codifying principles of data protection under one overarching legislation.

The efforts to legislate a new data protection law gathered steam in the aftermath of the landmark judgment passed by the Supreme Court in the case of *Justice K. S. Puttaswamy (Retd.) and Anr. v. Union of India And Ors.*[1] ('the Right to Privacy Judgement'). While the Right to Privacy Judgement was a landmark case confirming the fundamental right to privacy available to Indian citizens, it did not address in detail a protection regime for informational privacy and the rights available to its citizens with respect to protection of their personal data. However, Justice Sanjay Kishan Kaul, one of the nine judges of the Supreme Court who delivered the judgement, made a cursory reference as regards the need to regulate the extent to which personal information can be stored, processed and used by non-state parties. The Government of India responded by appointing an eight-member committee of experts, led by Justice B. N. Srikrishna, a former Judge of the Supreme Court of India ('the Committee') to recommend a new framework for regulation of data protection in India.

The Committee released the White Paper of the Committee of Experts on a Data Protection Framework for India[2] ('the White Paper') in November 2017. The White Paper called for responses and suggestions from the public and the stakeholders.

The White Paper recommends that the data protection framework to be devised must be based on seven principles:

1. technology agnosticism: the law must be versatile enough to address dynamic technologies and standards of compliance;
2. holistic application: the law must apply both to state and non-state parties, though state parties may have certain differential rights to protect legitimate state interests;
3. informed and meaningful consent;
4. data minimisation: the data being processed ought to be minimal and necessary for the purposes for which it is sought and other compatible purposes beneficial for the data subject;
5. controller accountability: a data controller shall be held accountable for any processing of data whether by itself or by other third parties which it may have shared the data with;
6. structured enforcement of the data protection framework by a high-powered statutory agency with sufficient authority; and
7. deterrent penalties.

The Committee sought responses from various stakeholders on various issues concerning the proposed data protection legislation including definitions of the terms 'data' and 'information'; definition of the term 'personal data'; definition of the term 'identifiable information'; and definition of the term 'sensitive personal data.'

Image: Mikael Kristenson / Unsplash.com

1. https://supremecourtofindia.nic.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf
2. http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf
3. https://www.washingtonpost.com/world/asia_pacific/whistleblower-claims-cambridge-analyticas-partners-in-india-worked-on-elections-raising-privacy-fears/2018/03/28/1168c04c-328a-11e8-b6bd-
4. https://www.thehindu.com/news/national/nothing-but-lies-fake-videos-rumour-set-off-the-lynch-mobs/article24361988.ece

In the White Paper, the Committee sought to incorporate the principle of technological agnosticism within the proposed data protection framework and argued that any such framework should be designed in a manner that not only covers the technology of the day, but is also broad enough to include future technologies which may or may not be anticipated.

The Committee has also recommended that the terms 'data controller' and 'data processer' be defined to ensure accountability of parties who control and process the data. The principle, however, remains that the data controller shall be responsible for processing data. Such an obligation will also extend to a situation where the data controller has provided data to a third party for processing it.

In addition, the White Paper considers excluding storing/processing of information for personal or household purposes; journalistic/artistic/literary purposes; research/historical and statistical purposes; the purpose of investigation of a crime, and apprehension or prosecution of offenders; and the purpose of maintaining national security and public order, from the purview of the data protection regime.

The White Paper also discusses the concepts of the cross border flow of data and data localisation. There is an apprehension that the draft data regulation framework may require tech giants such as Google and Facebook to store and process data of Indian data subjects in India.

The White Paper even discusses certain grounds, including consent and the processing of data for a specific pre-determined purpose to be specified as permitted grounds for data processing, as well as obligation on entities and rights of individuals. Furthermore, the White Paper considers enforcement models and penalties and compensations for non-compliance. The Committee has sought responses from the public on what would serve as an effective deterrent for persons who are held to be in breach of the proposed data protection framework.

The Committee has received the responses of the public and stakeholders, and is expected to release its final report with recommendations and a draft framework for data protection regulation imminently. The provisions pertaining to enforcement mechanisms and penalties would be watched with great interest by non-state actors as well as lawyers from different parts of the world.

It will be interesting to see whether the lawmakers utilise the recommendations of the Committee while framing the data protection legislation to come up with a comprehensive data protection regime to ensure protection of data and informational privacy in India.

Curiously, while the Committee was in the midst of its deliberations on the contours of the proposed data protection law, the Ministry of Health and Family Welfare also released a draft of a Digital Information Security in Healthcare, Act ('DISHA') and invited comments from stakeholders. DISHA aims to regulate collection, storage, transmission and use of digital health data. Considering that the Committee had been tasked with the responsibility of recommending a sector-agnostic and overarching data protection law, this move by the Government of India appears to dilute the efforts of the Committee. Consequently, we do believe that there is a significant potential for conflict between the proposed data protection law and DISHA.

Conclusion

Over the last couple of years, the issue of data protection has consumed reams of paper as well as a significant amount of time of multiple stakeholders, including central and state governments, the judiciary, different sector-specific regulatory authorities and private players. The issue of data protection has manifested itself in various forms, be it the issues surrounding Aadhaar, the Cambridge Analytica scandal[3], a general upsurge in fake news which has led to tragic consequences[4], or the responsibilities of private actors such as Facebook, WhatsApp, Google etc. being debated by governments all over the world.

Earlier this year, the EU's General Data Protection Regulation (Regulation (EU) 2016/679) ('GDPR') came into effect and has changed the way private business players can now transact with residents of the EU.

While it will be prudent for India to adopt several of the fundamental principles incorporated in the GDPR, we do believe that lawmakers in India must (a) be cognizant of the political, economic, legal and social context that will underpin the proposed data protection legislation, and (b) ensure that any such legislation complies with the principles enshrined in the Right to Privacy Judgement.

At the same time, it is incumbent on the lawmakers to ensure an appropriate balance between the rights of the individuals with respect to their personal data, and the rights of both state agencies as well as non-state actors in complying with such obligations while providing services and products using technology for the benefit of a large population.