Privacy and Data Protection in India

What's Inside?

- Existing framework in India
- Proposed Framework
- Conclusion

CLA

Privacy and Data Protection in India

Big data's indispensable role in decision-making today has led to data being coined the oil of the digital era. Successful data mining has facilitated the growth of some of the largest companies in the world, allowing them to use data expertise to create products and services they can sell. Governments and large companies possess stores of private data collected from individuals. The manner in which this information is collected, stored, and shared, and whether it is vulnerable to unauthorized access, are concerns that must be addressed.

Privacy simply means the right to be left alone. Data privacy refers to the control an individual has over the collection, use and dissemination of information relating to them. Personal data is defined differently in different jurisdictions. Personally Identifiable Information (hereinafter PII) as used in North America, covers information that can be used to distinguish or trace an individual's identity (name, social security, biometrics, etc.), or such information combined with other personal or identifying information (place of birth, mother's maiden name, etc.) that is linked or linkable to a specific individual. In contrast to this, the EU's General Data Protection Regulation (hereinafter GDPR) defines personal data as any information relating to an identified or identifiable natural person, including, but not restricted to, identification numbers and physical, physiological, mental, economic, cultural or social identities. Personal data, in this context, covers a larger scope of information than PII.

Existing framework in India

India does not currently have a comprehensive privacy and data protection framework. It relies on certain statutory provisions and Supreme Court judgements to enforce limited privacy and data protection rights. The Information Technology Act, 2000 (hereinafter the IT Act), supplemented by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (hereinafter the SPDI Rules) and the Information Technology (Intermediary Guidelines) Rules, 2011 (hereinafter the Intermediary Guidelines), predominantly addresses issues involving misuse of lawfully collected data. Data protection, i.e., safeguards against unlawful access to private data by unauthorized persons is addressed in a very generic manner. Though the IT Act was not originally envisaged to address data privacy, subsequent amendments have attempted to add sensitive data to its purview to some extent.

Corporations and Privacy and Data Protection

The IT Act obligates a body corporate possessing, dealing or handling any sensitive personal data or information on a computer device it owns, controls or operates, to implement and maintain reasonable security practices and procedures.

The SPDI Rules define 'sensitive personal data or information' as:[1]

1. Passwords;
2. Financial information, such as bank account or credit card or debit card or other payment instrument details;
3. Physical, physiological, and mental health conditions;
4. Sexual orientation;
5. Medical records and history;
6. Biometric information;
7. Any detail relating to the above as provided to body corporate for providing services; and
8. Any information received under the above by body corporate for processing, stored or processed under lawful contract or otherwise

The SPDI Rules also describe reasonable security practices and procedures as those laid down in the International Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System - Requirements" or other such recognized standards. Other practices of self regulation may also be implemented after such codes of best practices have been certified or audited on a regular basis by entities through an independent auditor, duly approved and by the Central Government.[2] A body corporate failing to fulfil such obligations, and causing wrongful gain or loss to any person as a result, would attract liability in the form of compensation payable to the affected person.[3] The SPDI Rules place additional requirements on businesses and commercial entities in India in terms of data collection and disclosure of sensitive personal data or information. While body corporates are expected to have a privacy policy in place, and to obtain informed consent while collecting and transferring sensitive personal data, the only standard of protection expected from them is that which falls under the IT Act and SPDI Rules. When such data is transferred to a representative or another body corporate located in India or any other country, the receiving entity need only provide the same level of protection.[4]

1 Rule 3, The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

2 Rule 8, The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

3 Section 43A, The Information Technology Act, 2000.

4 Rule 7, The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

The Supreme Court, in *Justice KS Puttaswamy & Another v Union of India*[5] (hereinafter the *Puttaswamy* judgement), struck down a provision that allowed body corporates to use the 12-digit biometric based identification number, Aadhaar, for the authentication of an individual. Biometric information collected in pursuance of this Act is deemed to fall within the definition of "sensitive personal data or information" under the IT Act.[6] However, as many services of the government continue to be provided through public-private endeavours, complete prohibition against private sector access to Aadhar appears to be impossible. Entities in regulated sectors are required to fulfil obligations of confidentiality, and utilize accessed information only for prescribed purposes or in ways expressly consented to by the customer.

Intermediaries and Privacy

Under the Intermediary Guidelines, intermediaries are required to observe due diligence while discharging their duties. An 'intermediary' here refers to any person who on behalf of another person receives, stores or transmits an electronic record or provides any service with respect to that record. An example of an intermediary could be a telecom service provider, network service provider, search engine, internet service provider, or a cyber café.[7] The intermediary liability regime in India is governed by Section 79 of the IT Act and the Intermediary Guidelines, that were introduced to protect intermediaries from liability from user generated content.

Expanding upon the above, intermediaries are required to publish the rules and regulations, privacy policy, and user agreement for access or use of their resources. Such rules must prevent users from hosting, displaying, uploading, modifying, publishing, transmitting, updating or sharing certain specified types of content or information.

Further, an intermediary is exempted from liability provided they comply with requirements laid out by the IT Act and the Intermediary Guidelines. For example, the Act mandates that the intermediary removes content related to the restrictions placed in Article 19(2) of the Constitution upon receiving notice of such material from a court order or appropriate government agency. The need for a direct court order to inform the intermediary of offending content was clarified in *Shreya Singhal v. Union of India*[8] *("Shreya Singhal case")* after acknowledgement that intermediaries would have difficulty in judging the legitimacy of millions of requests alleging offending content. This is in contrast to the judgement of the Court of Justice of the European Union on the right to forget commonly called the 2014 *Google Spain*[9] case. In this ruling, the Court established that users themselves could ask search engines to hide certain URLs from search results when a search is conducted using their name and the content on the page the URL points to includes information that is "inadequate, irrelevant or no longer relevant, or excessive."

The Shreya Singhal case also proceeded to read down various provisions to address questions of the intermediary acting in accordance with takedown requests from non-judicial and non-governmental entities.

The Shreya Singhal case also proceeded to read down various provisions to address questions of the intermediary acting in accordance with takedown requests from non-judicial and non-governmental entities. Other compliances include the need to preserve the information pertaining to this 'offending content' to be preserved for ninety days for investigation purposes.

The Draft Information Technology [Intermediary Guidelines (Amendment) Rules] of 2018[10] that have since come out propose various changes to the Rules, mostly inclusive of amendments to timelines and mandatory compliance with these.

5 (2017) 10 SCC 1.

6 Section 30, The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

7 Section 2 (w), The Information Technology Act, 2000.

8 MANU/SC/0329/2015

9 C-131/12, Google Spain, S.L., Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja Gonzales

10 Information Technology [Intermediaries Guidelines (Amendment) Rules] 2018

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 have also been enacted since, and place accountability upon intermediaries by mandating them to perform due diligence with respect to certain information published on their platforms. This would involve informing users about the privacy policies and user agreements listing certain prohibited information that cannot be hosted, displayed, uploaded, modified, published, transmitted, stored, updated or shared. The latest rules empower a competent court and the government to direct any intermediary to take down certain information that is considered 'prohibitory'. If an SSMI removes any content of its own volition, it shall provide a reasonable opportunity to the offender and explain the reasons for such removal. In addition, it places additional responsibility upon Significant Social Media Intermediaries ("SSMIs") by mandating them to identify the first originator of information if the Court or government requires them to do so. An intermediary is considered to be an SSMI if it has more than 50 lakh registered users in India.

The Ministry can also require any other intermediary, not being an SSMI, to comply with any or all the conditions mentioned under Rule 4 if its operations pose a material risk of harm to the sovereignty of the country. A Code of Ethics has been put in place to reconcile the interests of digital media and the public. This Code is applicable to publishers of news and current affairs content and publishers of online curated content, provided that they have a physical presence in India and conduct their business activities in a planned manner. The Rules have now established ratings for online curated content.

Grievance Redressal

Intermediaries have been required under the most recent rules to appoint a Grievance Officer who can be approached for violation of any of the rules or other related matters, and publish details about them on their website,. The Grievance Officer shall be responsible to acknowledge a grievance if filed and ensure its disposal within a period of fifteen days from its receipt. If the complaint is about any material that displays nudity in any manner, the intermediary is obligated to remove such content within 24 hours from the receipt of the complaint. Apart from a 'Grievance Officer', in the case of SSMIs, a Chief Compliance Officer must be appointed. Such an officer must be a senior employee or Key Managerial Personnel of the SSMI. The Chief Compliance Officer so appointed would be liable in case the SSMI fails to comply with the rules.

The Intermediary Guidelines and Digital Media Ethics Rules, 2021 also provide for a hierarchical grievance redressal mechanism for publishers of online curated content and news and current affairs content. This hierarchy involves self-regulation by the publishers, self-regulation by the self-regulating bodies of the publishers, and an oversight mechanism by the Central Government. Appeals from these self-regulating bodies or violations that have been brought directly before the government will be heard by an Inter-Departmental Committee consisting of representatives from the ministries of Information and Broadcasting, Women and Child Development, Law and Justice etc. The Committee is allowed to make recommendations relating to examination of the complaints but no final order can be passed without the approval of the Secretary, Ministry of Information and Broadcasting.

If an intermediary fails to comply with any of the Rules applicable to it in, it will not be eligible for the exemptions provided under Section 79 of the Information Technology Act, 2000, thereby making it liable for any third party data or information posted.

Government Access to Citizens' Personal Data

While confirming the constitutional validity of Aadhaar in the *Puttaswamy* judgment, the Supreme Court also recognized the right to informational privacy as a fundamental right emanating from the right to life and personal liberty under Article 21 of the Constitution. According to the Court, the fundamental right to privacy includes the right to have control over the commercial use of one's identity or information, and determine when and how much of it is disseminated and for what purposes.

The fundamental right to privacy imposes a duty on the State to protect the privacy of individuals. This corresponds with the liability of the State in the event of a violation of the individual's right to life and personal liberty. The Puttaswamy judgment went further to state that the right to privacy could be restricted only if State action passes a three-limbed test:

(i) It must have a legislative mandate;
(ii) It must pursue a legitimate State purpose;
(iii) It must be proportionate.

The IT Act contains provisions that grant access to the government to personal data stored by private companies for use by law enforcement agencies for monitoring, interception, and decryption of online communications, for monitoring of internet traffic data, etc. for national security reasons, to prevent the commission of or incitement of cognizable offences, etc.[11] The provision also specifies that the government may not publish or share such information with a third party. In the *Puttaswamy* judgment, emphasis was laid on the need to protect information from the State. It noted that while interception may be desirable and permissible in order to ensure national security, such powers must not go unregulated. The Intermediary Guidelines and Digital Media Ethics Code, 2021, allow an Authorized Officer, not below the rank of Joint Secretary to the Government of India, to write to the Secretary, Ministry of Information and Broadcasting for blocking any information, provided it is within the grounds mentioned under Sec 69A of the IT Act. The latter, if satisfied, can do so without affording to the identified publisher or intermediary, an opportunity of hearing. The final order shall be passed by the Secretary, Ministry of Information and Broadcasting after considering the recommendations of the Committee. Rule 3 mandates an intermediary to implement the 'takedown order' within 36 hours without affording any opportunity of hearing to the alleged accused. There could be an issue of arbitrariness arising from this provision.

The Kerala High Court, in *Balu Gopalakrishnan & Another v State of Kerala & Others*,[12] struck down action by the state government at the onset of the COVID-19 outbreak, involving the grant of access to the data of patients for analysis and for the identification of vulnerable individuals, on the ground that no safeguards had been put in place against commercial and unauthorized exploitation of the data. A peremptory order was also passed, requiring that the private entity entrust back to the government any data remaining in its possession. The Court further observed that the prior informed consent of citizens would have to be obtained before such data could be handled by a third party service provider. Additionally, such information would have to be anonymized at the time access is granted to the entity, in order to safeguard the data protection rights of the individuals.

In furtherance of the same, the Karnataka High Court, on 25 January 2021, passed an interim order restraining the Central Government and the National Informatics Centre (NIC) from sharing data from Aarogya Setu, a COVID-19 contact tracing app developed by the NIC, to other government bodies not mentioned in the privacy policy of the app, without the informed consent of users.

The Aadhaar (Targeted Delivery of Financial and Other Subsidies) Act, 2016, also requires that authorities ensure the security and confidentiality of the identity information, and that such data is protected against access, use or disclosure not permitted by law. However, such information may be disclosed pursuant to an order by a Court not inferior to that of a District Judge, or in the interest

11 Section 69, The Information Technology Act, 2000.

12 Kerala High Court, WP (C) Temp. no. 84 (2020), April 24, 2020

of national security, in pursuance of a direction of an officer not below the rank of Joint Secretary to the Government of India, subject to review by an Oversight Company.

As is evident, provisions in the existing regulatory regime fail to address privacy concerns relating to non-sensitive personal data, thereby necessitating intervention by the Courts each time privacy concerns arise. Furthermore, the IT Act has a number of lacunae that remain unaddressed, such as aspects of the right to be forgotten, user rights to be notified of cookies and do-not track options, evidentiary value of social media content, and a number of other evolving issues unique to internet use.

The Intermediary Guidelines and Digital Media Ethics Code Rules, 2021 have been notified following these judgements, that may create circumstance warranting further challenges before the Courts. Under the Rules, an SSMI may be required, by way of a judicial order by a competent Court or an order passed by the competent authority under Sec 69 of the IT Act to identify the 'first originator' for certain electronic information which could have a bearing on the prosecution, prevention, investigation or punishment of an offence related to the sovereignty and integrity of India, its relationship with foreign states, rape, sexually explicit material or child sexual abuse etc. By virtue of the order so passed, the SSMI is obligated only to identify the 'first originator' of the electronic information as directed. It is not obligated to disclose the contents of any electronic message, any other information related to the first originator, or any information related to its other users. Even if the first originator of any such information is a foreigner, they will be considered to be within the territory of India for this purpose. The Rules, however, also specify that only the SSMIs providing messaging as their primary service might have to identify 'the 'first originator of information' in very specific cases like offences related to the integrity and sovereignty of India, incitement to an offence relating to rape, sexually explicit material or child sexual abuse, material etc. The purpose behind the said provision seems legitimate as identification of 'first originator of information' is mandated only when there is a judicial order passed by a competent court or an authorised agency under Section 69A of the IT Act. It will have to be seen how these provisions are implemented by law enforcement and whether actions under the new rules will pass the test of scrutiny for constitutional validity.

Data Localization

Data territoriality is an important part of the privacy and data protection framework. A large part of the information provided to foreign companies by customers in India is stored partly or completely outside India. Current legislation places no restrictions on such storage, which poses law enforcement and national security challenges, and there is limited judicial and regulatory guidance regarding data storage.

The Reserve Bank of India issued a circular in 2018,[13] directing payment system providers to ensure that data relating to their payment systems are stored in systems located within the territorial jurisdiction of India, to the exclusion of certain specified exemptions. Further to this circular, some other mandates for data localization have been noted in the New Guidelines for Other Service Providers,[14] the Companies (Accounts) Rules, 2014[15] and various draft legislations. The proposed Personal Data Protection Bill (hereinafter the Bill), in more detail below, also inserts provisions pertaining to the restriction on transfer of personal data outside India.

13 RBI/2017-18/153

14 Chapter 2, Clause 8, New Guidelines for Other Service Providers (OSPs) available at https://dot.gov.in/sites/default/files/2020_11_05%20OSP%20CS.pdf

15 Section 3, Companies (Accounts) Rules, 2014.

Proposed Framework

To address the gaps in existing legislation and to facilitate the enforcement of the fundamental right to privacy against private entities, the government has, in 2019, introduced the Personal Data Protection Bill (hereinafter the Bill), touched upon in the previous paragraph. This legislation is an attempt to streamline India's data protection laws with the EU's GDPR.

Some features of the Bill that are of interest are described hereunder.

Personal Data

Sensitive personal data has been defined as personal data revealing, related to, or constituting, as may be applicable, passwords, financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation, or any other data that may be categorized as sensitive personal data by the Data Protection Authority.[16]

Data Processing

Any person, including the State, a company, or a juristic entity, or any individual who alone or in conjunction with others, determines the purpose and means of processing personal data have been termed data fiduciaries.[17] Personal Data can be processed by data fiduciaries only with the consent of the individual,[18] except under specific circumstances under the Bill such as to respond to a medical emergency or to provide medical treatment, for the purpose of legal proceedings, or if the data is required by the State to provide benefits to the individual. Processing can include collection, recording, organization, structuring, storage, adaptation, alteration, retrieval, use, alignment or combination, indexing, disclosure by transmission, dissemination, or otherwise making available, restriction, erasure, or destruction.[19] Data processors are those who process data on behalf of data fiduciaries, but are not employees of the data fiduciary.[20] Data fiduciaries are required to notify the data principal of the other entities with whom personal data may be shared. No processing is permitted by a downstream data processor without a contract entered into by the data fiduciary and such data processor.[21]

Accountability and Governance

The Bill places an obligation on personal data processing entities to put in place measures for transparency and accountability by setting up grievance redressal mechanisms and implementing safeguards in security such as the appointment of a Data Protection Officer and regular data audits.[22] Other requirements include the need for these processing entities to prepare a privacy policy which discloses the business practices and technical systems put in place. This policy is also expected to contain information pertaining to the technology used in the processing of personal data, and the assurance that the interest of the individual whose data is involved is accounted for at every stage of processing of personal data. Significant data fiduciaries are also required to conduct a Data Protection Impact Assessment (DPIA) before processing personal data if the processing involves new technology, large-scale profiling or use of sensitive data, or any other activities that carry a significant risk of harm.

16 Section 3(36), The Personal Data Protection Bill, 2019.

17 Section 3(13), The Personal Data Protection Bill, 2019.

18 Section 12, The Personal Data Protection Bill, 2019.

19 Section 3(31), The Personal Data Protection Bill, 2019.

20 Section 3(15), The Personal Data Protection Bill, 2019.

21 Section 31, The Personal Data Protection Bill, 2019.

22 Section 30, The Personal Data Protection Bill, 2019.

Rights of Individuals

Individuals to whom the relevant data pertains have been termed data principals under the new framework.[23] Data principals, similar to 'data subjects' in the GDPR, have the right to know if their personal data has been processed. They also have the right to have their personal data transferred to a different data processing entity, or fiduciary, and to restrict further disclosure of their private information to a fiduciary at a later time.[24] The right to be forgotten has also been addressed in this framework. Data principals have the right to restrict or prevent the continuing disclosure of their personal data by a data fiduciary if such disclosure is no longer necessary as it has served its purpose, if the data principal has withdrawn consent, or if the disclosure was made contrary to the provisions of the Bill or any other law in force at the time. However, this right can only be enforced through an order by an Adjudicating Officer.[25]

Significant Data Fiduciaries

A significant data fiduciary is classified based on the volume and sensitivity of the personal data processed, the turnover of the data fiduciary, the risk of harm from processing undertaken by the fiduciary, the use of new technologies, and any other factors that might cause harm to a data principal.[26]

Social media intermediaries that facilitate online interaction between two or more users, that have a user base higher than a specified threshold, and which have the potential to impact elections or public order will be notified as significant data fiduciaries and will have to comply with specific obligations.[27] These entities are subject to obligations relating to data, and the appointment of a data protection officer.[28]

Another interesting aspect of the law is that political parties that collect personal data on voters may be categorized as significant data fiduciaries by the Data Protection Authority (hereinafter the DPA), as such data collection and processing could potentially impact the outcome of an electoral process. As such, if the DPA were to notify political parties as significant data fiduciaries, these bodies would have to obtain the consent of data principals prior to the collection of data, as well as comply with the additional requirements such as the need to conduct a data protection impact assessment.

Data Transfer

Sensitive personal data may be transferred outside India with the express consent of the data principal, provided that such personal data continues to be stored in India.[29] Data categorized as critical personal data can only be processed in India.[30] Critical personal data can only be transferred outside India to persons involved in the provision of health or emergency services, and to countries where sufficient regulatory safeguards exist, and such transfer does not affect the security and strategic interest of the State.[31] Additional conditions may also apply based on circumstances.

Government Access

The Government may access non-personal data or anonymized data from fiduciaries in order to better target services and government programs. Additionally, the central government can exempt its agencies from the provisions of the Act under certain circumstances laid down in Chapter VIII, involving:

(i) Security of the State;
(ii)Prevention, detection, investigation, and prosecution of contraventions of law.[32]

23 Section 3(14), The Personal Data Protection Bill, 2019.
24 Section 19, The Personal Data Protection Bill, 2019.
25 Section 20, The Personal Data Protection Bill, 2019.
26 Section 3(37), The Personal Data Protection Bill, 2019.
27 Section 26(4), The Personal Data Protection Bill, 2019.
28 Sections 27, 28, 29, and 30, The Personal Data Protection Bill, 2019.
29 Section 34(1), The Personal Data Protection Bill, 2019.
30 Section 33(2), The Personal Data Protection Bill, 2019.
31 Section 34(2), The Personal Data Protection Bill, 2019.

Exemption of Certain Provisions for Certain Processing of Personal Data

Other exemptions where personal data may be processed without the application of the provisions of the Bill include:[33]

(i) Processing for the purpose of legal proceedings;
(ii)Research, archiving, or statistical purposes, subject to specific conditions;
(iii) Personal or domestic purposes provided that this does not involve disclosure to the public and is not undertaken in connection with any professional or commercial activity;
(iv) Journalistic purposes, as long as such use is in compliance with the code of ethics of the Press Council of India and any other self-regulatory organization of the media;
(v) Manual processing by small entities, where personal data is being processed by means that are not automated.

Data Protection Authority of India

The Authority has the power to take steps necessary to protect the interests of individuals, prevent the misuse of data, and ensure general compliance with the provisions of the Bill.[34] Orders made by the DPA can be appealed to an Appellate Tribunal,[35] from which appeal will lie with the Supreme Court.[36]

Redressal

An individual can seek redressal from the data fiduciary itself at the first instance. If the response is dissatisfactory, the data principal can file a complaint with the DPA. The data principal is also free to approach the DPA at first instance, and seek an inquiry into the violation.[37] The DPA also has the power to look into breaches suo moto.

Offences

The Bill recognizes the processing of personal data in violation of the Bill as an offence punishable with fines. Re-identification and processing of de-identified data, i.e., data from which identifiers have been removed or masked, is deemed a criminal offence, punishable with a fine, imprisonment, or both.[38]

The Bill has been revised a number of times, losing certain provisions that existed in original versions. The 2018 draft of the law contained provisions that implemented the deterrent principle, found in data protection frameworks across the world. These provisions made obtaining, disclosing, transferring or selling personal data or sensitive personal data, contrary to the Bill, and punishable with imprisonment, or fine, or both. These deterrent penalties have been deleted in the 2019 draft. However, offences that have been retained in the new draft legislation continue to be cognizable and non-bailable.[39] The Bill takes away the jurisdiction of courts in matters falling under the scope of the legislation, providing that courts may only take cognizance of such matters if the complaint is made by the DPA.

The Non-Personal Data Governance Framework

The Non-Personal Data Governance Framework, proposed by the Justice B.N. Krishna Committee Report, meant to regulate the use of community data, is also of relevance here. Any data falling outside the meaning of personal data under the Personal Data Protection Bill would fall within the scope of this framework. This could include data never related to an identified or identifiable natural person, or data sourced from personal data. Non personal data can be further categorized as raw data, aggregate data, and inferred data.

The objective is to utilize data stripped of its identifying features, classified into three categories - Public (generated by the government in the course of publicly funded work), Community (originates or relates to a community), and Private Non-Personal Data (produced by persons or entities, not including the government) to:

33 Section 36, The Personal Data Protection Bill, 2019.
34 Section 49, The Personal Data Protection Bill, 2019.
35 Section 72, The Personal Data Protection Bill, 2019.
36 Section 75, The Personal Data Protection Bill, 2019.
37 Section 32, The Personal Data Protection Bill, 2019.
38 Section 82, The Personal Data Protection Bill, 2019.
39 Section 83, The Personal Data Protection Bill, 2019.

(i) generate economic, social, and public value for citizens and communities
(ii) incentivize innovation
(iii) address the concept of collective privacy and privacy concerns from processing non-personal data

Any data that is re-identified would fall within the scope of the Personal Data Protection law. This will also be the case for datasets where non personal data is inextricably linked to personal data. Data principals will be notified when their data is being anonymized, and will be given an option to opt-out.

Non-personal data that forms part of a high-value dataset is required to follow data localization requirements. The latest revised report remains silent on the data localization requirements for non-personal data derived from previously critical personal data as defined under the Personal Data Protection Bill.

Entities, including data processors, that meet specific thresholds requirements, and engage in activities involving collection, processing, storing, or otherwise managing data are to register with the National Data Protection Authority as a Data Business. Data Businesses are required to make all meta-data they collect available for open access through a directory that will be managed by the Authority. Entities collecting and processing non-personal data have been termed Data Custodians. These entities owe a duty of care to the community while handling such data, and are obligated to provide access to data when requests are made for specific purposes.

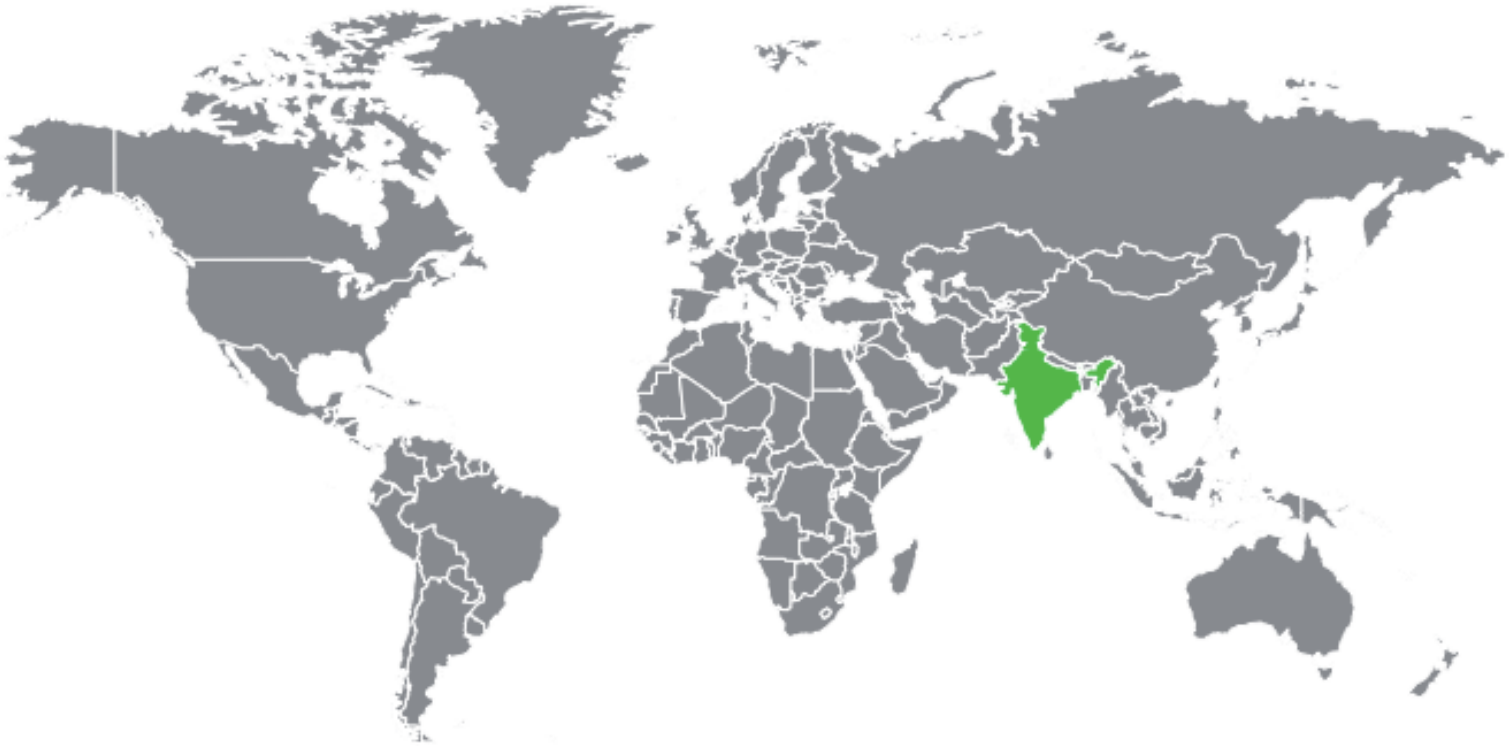
Since non-personal data is not linked to any one data principal, the framework provides for a group of people with common interests, i.e., a community, to derive value and eliminate harms through Data Custodians.

Conclusion

The existing law on data protection in India draws from a number of sources and addresses lacunae as concerns arise. The judgements create precedents for a strong data protection framework as an extension of the right to privacy as a fundamental right, and the amendments to legislations provide isolated remedies. The proposed new law remains under consideration, and is likely to undergo more changes following the standing committee report on the Bill. It would not be inaccurate to say that the framework is still in its nascent stages and requires some creases to be pressed out. The specifics of much of the law will become clear only once the regulations and rules falling under the legislation are notified.

As many countries around the world begin developing data governance regimes, the Bill will play an important role in shaping the global regulatory landscape. It is firmly based on the concept of consent, and individuals have increased control over how their data is utilized by private bodies. Redesigning policies to make consequences more transparent and predictable is likely to be beneficial to companies in the long term. The law places focus on curtailing instances of fake news and cyber attacks, issues that have become increasingly relevant in recent years.

At the same time, the new law is likely to result in an increase in economy-wide compliance costs for businesses in data collection, storage, and management practices. It could also indirectly lead to the stifling of innovation and productivity, unless implemented in a manner that contextually applies to India. Additionally, in its current form, the draft legislation facilitates increased State intervention, giving the State a greater role in the data economy. Not only does it lend legitimacy to State surveillance, it does so without making provisions for sufficient checks and balances.



Who we are

CLA is a law firm set up with an aim to provide specialized, sophisticated and top quality legal services.

CLA's head office is based out of Chennai with liaison offices in Hyderabad and Bangalore. The firm has three partners, a team of attorneys and of-counsels. Our philosophy is to maintain above par levels of integrity in our work and to add value to each client mandate. Our practice emphasis is to find resolution to intricate legal and business requirements, always keeping in mind commercial expectations of the client.

In addition, our professionals also have sector focus which include healthcare, technology, e-commerce, financial services, pharmaceutical, real-estate, power and energy. Given the experience and diversity in practice and sector focus amongst our professionals, we have the capability to support a wide spectrum of legal requirements. Our *Of-counsels* extend support in handling civil and commercial disputes.

Akshaya Suresh

Partner

Technology, Privacy and Start-ups

akshaya@cla-india.com

Akshaya has 14 years of experience. She focuses on transactions, mergers & acquisitions, technology laws, privacy & data security, corporate & commercial contracts, and corporate social responsibility.

In her previous role, she led the legal team at Freshworks and was a key member of the leadership there. She set up the legal team from scratch in a nascent start up environment and scaled the function to effectively manage go-to-market, M&A, capital raise, data privacy, compliance, contracts, IPR, litigation, governance & CSR. Prior to Freshworks she was with J Sagar Associates, a leading law firm in India.

Akshaya is an alumnus of ILS Law College, Pune. Akshaya has mentored many startups in setting up their legal and privacy functions and has presented at various industry events and forums like MCCI and IAPP.

Chennai

No. 6 Crystal Cove, 93/59
Satyadev Avenue,
MRC Nagar Main Road,
Chennai 600028.

Telephone: +91 44 48601672

www.cla-india.com

CLA