International Journal of Enhanced Research in Educational Development (IJERED)
ISSN: 2320-8708, Vol. 13 Issue 2, Mar.-Apr,, 2025

Data Privacy Laws: Comparative Study India With Other Countries

Yash Chauhan[1], Dr. Shefali Raizada[2]

[1,2]Amity University, Noida

INTRODUCTION

In the absence of specific legislation for data protection in India, the knowledge Technology Act 2000 (the IT Act) and a set of other statutes substitute for this purpose. In 2017, the Indian Supreme Court ruled that Indian citizens have a fundamental right to privacy, guaranteed primarily under Article 21 of the Indian Constitution. The Court specified that this right includes, inter alia, the proper to informational privacy. Within the wake of this judgment, and so as to offer it meaning within the sort of comprehensive legislation, the govt empanelled a 10-member committee under the chairmanship of Justice BN Srikrishna, a former Supreme Court Justice. The Srikrishna committee was asked to compile an in-depth review of existing laws relevant to the topic. In 2018, the Srikrishna committee published a report running into over 200 pages. The Srikrishna report examined the present patchwork of relevant laws in India, studied the statutory approach to privacy and data protection in other jurisidctions and laid out detailed rationale for an improved legal framework. The report was amid the draft Personal Data Protection Bill 2018.

In December 2019, the private Data Protection Bill 2019 was tabled in parliament. This Bill finds basis within the Srikrishna Report and therefore the draft Personal Data Protection Bill 2018, and is modelled mainly on the GDPR. the private Data Protection Bill is rooted heavily within the notion of free, specific and consent of the individual. This aligns with the thrust of the Srikrishna Report, which states that:

To make [the right to privacy articulated by the Supreme Court] meaningful, it is the duty of the state to put in place a data protection framework which, while protecting citizens from dangers to informational privacy originating from state and non-state actors, serves the common good.

The Personal Data Protection Bill 2019 envisages the formation of a data protection authority for its enforcement, places heavy fiduciary duties on data controllers and processors and, if enacted, will apply to a wide range of actors and stakeholders across various sectors.

The executive scramble to mitigate the effects of the covid-19 crisis has brought various competing interests to the fore in the context of data privacy. The most conspicuous of these interests is the need for government surveillance in the form of contact tracing, large-scale testing and the maintenance of public health records (symptoms and quarantine regulation) for citizens and non-citizens across the country. India is a quasi-federal nation state. The centre and states are currently acting together through the Integrated Disease Surveillance Programme, which operates through a decentralised state-based surveillance system to monitor information flows on target diseases to compile and analyse data and organise an appropriate response. The centre has also developed and released a mobile application that relies largely on crowd-sourcing self-reported data to identify covid-19 hotspots. This collection and processing of data stands largely unregulated at this time.

REGULATORY FRAMEWORK

Privacy and data protection legislation and standards
The following statutes deal with data protection and privacy in India.

The Information Technology Act (2000) (IT Act) and the Information Technology (Amendment) Act 2008[1]The IT Act contains provisions for the protection of electronic data. The IT Act penalises 'cyber contraventions' (Section 43(a)–(h)), which attract civil prosecution, and 'cyber offences' (Sections 63–74), which attract criminal action.

The IT Act was originally passed to provide legal recognition for e-commerce and sanctions for computer misuse. However, it had no express provisions regarding data security. Breaches of data security could result in the prosecution

[1] "Links to pdf versions of the IT Act and Rules are available on the website of the Ministry of Electronics and Information Technology: meity.gov.in/content/cyber-laws."

of individuals who hacked into the system, under Sections 43 and 66 of the IT Act, but the Act did not provide other remedies such as, for instance, taking action against the organisation holding the data. Accordingly, the IT (Amendment) Act 2008 was passed, which, inter alia, incorporated two new sections into the IT Act, Section 43A and Section 72A, to provide a remedy to persons who have suffered or are likely to suffer a loss on account of their personal data not having been adequately protected.

The Information Technology Rules (the IT Rules)
Under various sections of the IT Act, the government routinely gives notice of sets of Information Technology Rules to broaden its scope. These IT Rules focus on and regulate specific areas of collection, transfer and processing of data, and include, most recently, the following:

- "The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules,[2] which require entities holding users' sensitive personal information to maintain certain specified security standards;"
- "The Information Technology (Intermediaries Guidelines) Rules,[3] Which Prohibit Content Of A Specific Nature On The Internet, And An Intermediary, Such As A Website Host, Is Required To Block Such Content;"
- "The Information Technology (Guidelines For Cyber Cafe) Rules,[4] Which Require Cybercafés To Register With A Registration Agency And Maintain A Log Of Users' Identities And Their Internet Usage; And"
- "The Information Technology (Electronic Service Delivery) Rules,[5] Which Allow The Government To Specify That Certain services, such as applications, certificates and licences, be delivered electronically."

The IT Rules are statutory law, and the four sets specified above were notified on 11 April 2011 under Section 43A of the IT Act. Any further references to the IT Rules in this chapter pertain specifically to the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, unless otherwise specified. Penalties for non-compliance are specified by Sections 43 and 72 of the IT Act.

Additional legislation
In addition to the legislation described above, data protection may also sometimes occur through the enforcement of property rights based on the Copyright Act (1957). Further, other legislation such as the Code of Criminal Procedure (1973), the Indian Telegraph Act 1885, the Companies Act (1956), the Competition Act (2002) and, in cases of unfair trade practices, the Consumer Protection Act (1986), would also be relevant. Finally, citizens may also make use of the common law right to privacy, at least in theory – there is no significant, recent jurisprudence on this.

Additionally, the Personal Data Protection Bill 2019, referred to above, may soon be passed into law, becoming India's first and most comprehensive cross-sectoral data protection legislation.

Compliance regulators
CERT-In
Under Section 70B of the IT (Amendment) Act 2008, the government constituted CERT-In, which the website of the Ministry of Electronics and Information Technology refers to as the 'Indian Computer Emergency Response Team'. CERT-In is a national nodal agency responding to computer security incidents as and when they occur. The Ministry of Electronics and Information Technology specifies the functions of the agency as follows:

- collection, analysis and dissemination of information on cybersecurity incidents;
- forecast and alerts of cybersecurity incidents;
- emergency measures for handling cybersecurity incidents;
- coordination of cybersecurity incident response activities; and
- issuance of guidelines, advisories, vulnerability notes and white papers relating to information security practices, procedures, prevention, response to and reporting of cybersecurity incidents.[6]

Cyber Regulations Appellate Tribunal (CRAT)
Under Section 48(1) of the IT Act 2000, the Ministry of Electronics and Information Technology established CRAT in October 2006. The IT (Amendment) Act 2008 renamed the tribunal Cyber Appellate Tribunal (CAT). Pursuant to the IT Act, any person aggrieved by an order made by the Controller of Certifying Authorities, or by an adjudicating

[2]meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf.
[3] Ibid
[4]Id
[5]Id
[6] "www.cert-in.org.in."

officer under this Act, may prefer an appeal before the CAT. The CAT is headed by a chairperson who is appointed by the central government by notification, as provided under Section 49 of the IT Act 2000.

Before the IT (Amendment) Act 2008, the chairperson was known as the presiding officer. Provisions have been made in the amended Act for CAT to comprise of a chairperson and such a number of other members as the central government may notify or appoint.[7]

Definitions
Current legislation does not contain a definition for 'personal data'. The IT Rules define personal information as any information that relates to a natural person that, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such a person.

Further, the IT Rules define 'sensitive personal data or information' as personal information consisting of information relating to:

- passwords;
- financial information, such as bank account, credit card, debit card or other payment instrument details;
- physical, physiological and mental health conditions;
- sexual orientation;
- medical records and history;
- biometric information;
- "any details relating to the above clauses as provided to a body corporate for the provision of services; and"
- "any information received under the above clauses by a body corporate for processing, or that has been stored or processed under lawful contract or otherwise."

"Provided that any information is freely available or accessible in the public domain, or furnished under the Right to Information Act 2005 or any other law for the time being in force, it shall not be regarded as sensitive personal data or information for the purposes of these rules."

"The Personal Data Protection Bill 2019 defines 'personal data' as 'data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling'."

The Bill also defines 'sensitive personal data' intrinsically personal data which will reveal, be associated with , or constitute, various sorts of information, including but not limited to financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe and non secular or political belief or affiliation. The Bill clarifies that this list isn't exhaustive, which the central government may notify further categories of knowledge as falling within the remit of sensitive personal data.

Unlike the IT Act and Rules, the private Data Protection Bill 2019 contains definitions for 'processing', 'data fiduciary', 'data processor', 'data principal' and 'consent'. Importantly, the Bill renames data subjects (i.e., the natural person to whom the private data relates) as data principals, and any entity that determines the aim and means of processing personal data is mentioned as a knowledge fiduciary. For the rest of the chapter, references to the provisions of the Bill will retain this new nomenclature according to the language of the Bill. References to existing legislation will employ only terms utilized in the present legislation.

General obligations for data handlers
Obligations for data processors, controllers and handlers
Transparency
The IT Rules state that each one data handlers must create a privacy policy to control the way they handle personal information. Further, the policy must be made available to the info subject who is providing this information under a lawful contract.

Lawful basis for processing
A body corporate (or a person or entity on its behalf) cannot use data for any purpose unless it receives consent in writing from the info subject to use it for that specific purpose. Consent must be obtained before collection of the info . The IT Rules also mandate that sensitive personal information might not be collected unless it's connected to the

[7]https://www.meity.gov.in/writereaddata/files/The%20Cyber%20Appellate%20Tribunal%28Chairperson_Members%29%20Rules%2C%202009.pdf.

function of the company entity collecting it, then as long as the gathering is important for that function. it's the responsibility of the body corporate to make sure that the sensitive personal information thus collected is employed for no other purpose than the one specified. the private Data Protection Bill 2019 defines 'consent' and 'explicit consent' and provides grounds, including the functions of the state, or compliance with a writ , for the lawful processing of private data also as sensitive personal data.

Purpose limitation

The IT Rules state that any information collected by a body corporate or an individual on its behalf shall be used for the aim that it's been collected. the private Data Protection Bill 2019 prescribes that private data be processed just for specific, clear and lawful purposes. It states that data shall be processed during a fair and reasonable manner that ensures the privacy of the info principal (the person to whom the info relates) and for the aim consented to by the info principal. Alternatively, the aim could also be accompanying or connected with such purpose, and that the info principal would reasonably expect that such personal data shall be used. It also limits the gathering of private data to such data that's necessary for the needs of processing.

Data retention

Section 67C of the IT Act requires that an intermediary preserve and retain information during a manner and format and for such period of your time as prescribed by the central government. the private Data Protection Bill 2019 states that a knowledge fiduciary might not retain personal data beyond the amount necessary to satisfy the aim that it's processed. It also states that such data must be deleted at the top of this era . However, the Bill also allows for extended periods of retention if required by compliance with legal obligations, or if the consent of the info principal has been obtained, and prescribes periodic reviews by data fiduciaries for an ongoing assessment of the continued necessity of the retention of private data.

Registration formalities

India currently doesn't have any legislative requirements with reference to registration or notification procedures for data controllers or processors. the private Data Protection Bill 2019 requires that supported certain criteria, the info protection authority envisaged by the bill shall notify certain data fiduciaries as being 'significant'. Significant data fiduciaries are going to be required to register with the authority during a manner specified by it, and can even be subject to data protection impact assessments, data audits, etc. The Bill also states that the info protection authority may require registration by other data fiduciaries at its discretion, albeit such entities aren't 'significant'.

Rights of people

Access to data

Rule 5, Subsection 6 of the IT Rules mandates that the body corporate or a person on its behalf must permit providers of data or data subjects to review the knowledge they'll have provided. the private Data Protection Bill 2019 teases out this right in additional detail, providing the choice for the info principal to get from the info fiduciary during a clear and concise manner, confirmation of whether its personal data is being (or has been) processed and a quick summary of processing activities. The Bill states that the info principal shall even have the proper to access in one place the identities of the info fiduciaries with whom their personal data has been shared, along side the categories of such personal data.

Correction and deletion

Rule 5, Subsection 6 of the IT Rules states that data subjects must be allowed access to the info provided by them and to make sure that any information found to be inaccurate or deficient shall be corrected or amended as feasible. Although the principles don't directly address deletion of knowledge , they state in Rule 5, Subsection 1 that corporate entities or persons representing them must obtain written consent from data subjects regarding the usage of the sensitive information they supply . Further, data subjects must be given the choice to not provide the info or information sought to be collected.

The Personal Data Protection Bill 2019 provides data principals with the proper to correction and erasure of private data. However, such correction or erasure is subject to the agreement of the info fiduciary. If there's a dispute between the 2 entities during this regard, the info principal may require the info fiduciary to point alongside the relevant personal data that it's been disputed by the info principal.

Objection to processing and marketing

Rule 5 of the IT Rules states that the info subject or provider of data shall have the choice to later withdraw consent which will are given to the company entity previously, and therefore the withdrawal of consent must be stated in writing to the body corporate. On withdrawal of consent, the company body is prohibited from processing the private information in question. Within the case of the info subject not providing consent, or later withdrawing consent, the company body shall have the choice to not provide the products or services that the knowledge was sought.

The Personal Data Protection Bill 2019 also envisages the proper to be forgotten, therein it provides for the info principal's right to limit or prevent continuing disclosure of private data by the info fiduciary. However, this right may only be enforced by order of an Adjudicating Officer.

The Supreme Court of India has also identified and clarified that citizens have the proper to be forgotten, which exists in physical and virtual spaces like the web , under the umbrella of informational privacy.

Right to limit processing
As mentioned above, the private Data protection Bill 2019 provides for a knowledge principal's right to limit or prevent continuing disclosure of private data by the info fiduciary, but as long as the info protection authority, through an adjudicating officer, determines that any of the listed grounds for restriction or prevention of disclosure are found.

Right to data portability
The IT Act and Rules don't contain provisions relevant to data portability. However, the private Data protection Bill 2019 provides data principals with this right where processing has been performed through automated means. Subject to certain restrictions, the info principal shall have the proper to receive during a structured, commonly used and machine-readable format, any personal data provided to the info fiduciary, the info that has been generated within the course of provision of services or use of products by such fiduciary, or the info that forms a part of the profile on the info principal, or that the info fiduciary has otherwise obtained.

Right to withdraw consent
The Personal Data Protection Bill 2019 envisages the proper to withdraw consent, having reference to whether the convenience of such withdrawal is like the convenience with which consent could also be given.

Disclosure of knowledge
Data subjects also possess rights with reference to disclosure of the knowledge they supply. Disclosure of sensitive personal information requires the provider's prior permission unless either disclosure has already been agreed to within the contract between the info subject and therefore the data controller; or disclosure is important for compliance with a legal obligation.

The exceptions to the present rule are if an order under law has been made, or if a disclosure must be made to government agencies mandated under the law to get information for the needs of verification of identity; prevention, detection and investigation of crime; or prosecution or punishment of offences. Recipients of this sensitive personal information are prohibited from further disclosing the knowledge.

Right to complain to the relevant data protection authority
Rule 5, subsection 9 of the IT Rules mandates that each one discrepancies or grievances reported to data controllers must be addressed during a timely manner. Corporate entities must designate grievance officers for this purpose, and therefore the names and details of said officers must be published on the web site of the body corporate. The grievance officer must redress respective grievances within a month from the date of receipt of said grievances.

The Personal Data Protection Bill 2019 states that the info fiduciary must provide all data principals with clear information on the procedure for grievance redressal under the Bill. Under the Bill, a knowledge principal may make a complaint of contravention of any provision of the Bill to the info protection officer (in the case of a big data fiduciary) or the other officer designated for this purpose (in the case of the other data fiduciary). Should such officer fail to resolve the complain expeditiously and within 30 day of receipt of the complaint, the info principal may file a complaint with the info protection authority.

Specific Regulatory Areas
Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act 1983[8]
Under this Act, public financial institutions are prohibited from divulging any information relating to the affairs of their clients except in accordance with laws of practice and usage.

The Prevention of Money Laundering Act 2002[9]
The Prevention of Money Laundering Act (PMLA) was passed in an attempt to curb money laundering and prescribes measures to monitor banking customers and their business relations, financial transactions, verification of new customers, and automatic tracking of suspicious transactions. The PMLA makes it mandatory for banking companies, financial institutions and intermediaries to furnish to the Director of the Financial Intelligence Unit (under the PMLA) information relating to prescribed transactions, and which can also be shared, in the public interest, with other

[8]http://legislative.gov.in/sites/default/files/A1983-48_0.pdf.
[9]Ibid

government institutions or foreign countries for enforcement of the provisions of the PMLA or through exchanges of information to prevent any offence under the PMLA.

Credit Information Companies (Regulation) Act 2005 and The Credit Information Companies Regulations 2006[10]

This legislation is essentially aimed at regulation of sharing and exchanging credit information by credit agencies with third parties. Disclosure of data received by a credit agency is prohibited, except in the case of its specified user and unless required by any law in force.

The regulations prescribe that the data collected must be adequate, relevant, and not excessive, up to date and complete, so that the collection does not intrude to an unreasonable extent on the personal affairs of the individual. The information collected and disseminated is retained for a period of seven years in the case of individuals. Information relating to criminal offences is maintained permanently while information relating to civil offences is retained for seven years from the first reporting of the offence. In fact, the regulations also prescribe that personal information that has become irrelevant may be destroyed, erased or made anonymous.

Credit information companies are required to obtain informed consent from individuals and entities before collecting their information. For the purpose of redressal, a complaint can be written to the Reserve Bank of India.

Payment and Settlement Systems Act 2007[11]

Under this Act, the Reserve Bank of India (RBI) is empowered to act as the overseeing authority for regulation and supervision of payment systems in India. The RBI is prohibited from disclosing the existence or contents of any document or any part of any information given to it by a system participant.

Foreign Contribution Regulation Act 2010[12]

This Act is aimed at regulating and prohibiting the acceptance and utilisation of foreign contributions or foreign hospitality by certain individuals, associations or companies for any activities detrimental to the national interest and, under the Act, the government is empowered to call for otherwise confidential financial information relating to foreign contributions of individuals and companies.

Workplace privacy

In the present scenario, employers are required to adopt security practices to protect sensitive personal data of employees in their possession, such as medical records, financial records and biometric information. In the event of a loss to an employee due to lack of adequate security practices, the employee would be entitled to compensation under Section 43A of the Information Technology Act 2000. Other than this piece of legislation, there is no specific legislation governing workplace privacy, although, in relation to the workplace, the effect of the Supreme Court judgment on privacy as a fundamental right remains to be seen.

Children's privacy

Section 74 of the Juvenile Justice (Care and Protection of Children) Act 2015 mandates that the name, address or school, or any other particular, that may lead to the identification of a child in conflict with the law or a child in need of care and protection or a child victim or witness of a crime shall not be disclosed in the media unless the disclosure or publication is in the child's best interest. The Personal Data Protection Bill 2019 provides for the protection of personal and sensitive data of children by requiring consent of a parent or guardian and imposing various restrictions on data fiduciaries processing such data.

Health and medical privacy

Under the Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations 2002 (Code of Ethics Regulations 2002)15 regulations, physicians are obliged to protect the confidentiality of patients during all stages of procedures, including information relating to their personal and domestic lives unless the law mandates otherwise or there is a serious and identifiable risk to a specific person or community of a notifiable disease.

Medical Termination of Pregnancy Act 1971

This Act prohibits the disclosure of matters relating to treatment for termination of pregnancy to anyone other than the Chief Medical Officer of the state. The register of women who have terminated their pregnancy, as maintained by the hospital, must be destroyed on the expiry of a period of five years from the date of the final entry.

[10]https://rbidocs.rbi.org.in/rdocs/Publications/PDFs/86706.pdf.
[11] Ibid
[12]https://fcraonline.nic.in/home/PDF_Doc/FC-RegulationAct-2010-C.pdf.

Ethical Guidelines for Biomedical Research on Human Subjects
These Guidelines require investigators to maintain confidentiality of epidemiological data. Data of individual participants can be disclosed in a court of law under the orders of the presiding judge if there is a threat to a person's life, allowing communication to the drug registration authority in cases of severe adverse reaction and communication to the health authority if there is risk to public health.

Technological innovation and privacy law
There are no marketing restrictions on the internet or through email. Because India has no comprehensive data protection regime, issues such as cookie consent have not yet been addressed by Indian legislation. The Personal Data Protection Bill 2019 does prohibit data fiduciaries from profiling, tracking or behaviourally monitoring, or generating targeted advertising at children.

The IT Rules provide reasonable security practices to follow as statutory security procedures for corporate entities that collect, handle and process data, and these also apply to the use of big data. Unfortunately, no specific guidelines exist for the use of big data and big-data analytics in India.

International data transfer and data localisation
India isn't yet a member of the Asia-Pacific Economic Cooperation (APEC), and its inclusion on the forum has thus far been limited to observer status. APEC rules therefore don't apply within the Indian jurisdiction so far.

In terms of restrictions on transfer of knowledge , Section 7 of the IT Rules states that bodies corporate can transfer sensitive personal data to the other body corporate or person within or outside India, provided the transferee ensures an equivalent level of knowledge protection that the body corporate maintained, as needed by the IT Rules. a knowledge transfer is merely allowed if it's required for the performance of a lawful contract between the info controller and therefore the data subjects; or the info subjects have consented to the transfer.

As worded, Section 7 of the IT Rules is already rather restrictive. However, in some ways this is often no different from EU data protection legislation, which restricts transfers of private data outside the EU unless certain measures are taken, like requiring the info importer to check in to EU Model Contract Clauses. additionally , the Ministry of data Technology clarified via a press note released on 24 August 2011 that the principles on sensitive data transfer described above are limited in jurisdiction to Indian bodies corporate and legal entities or persons, and don't apply to bodies corporate or legal entities abroad. As such, information technology industries and business process outsourcing companies may subscribe whichever secure methods of knowledge transfer they like , as long as the transfer in question doesn't violate any law either in India or within the country the info are being transferred to. Presumably litigation during this sector – thus far non-existent – will further clarify matters.

In general, data protection laws in India apply to businesses established in other jurisdictions also . Section 75 of the IT Act states that the provisions of the Act would apply to any offence or contravention thereunder committed outside India by a person (including companies), regardless of his or her nationality, if the act or conduct constituting the offence or contravention involves a computer, computing system or network located in India.

The draft Personal Data Protection Bill 2019 states that, subject to varied conditions, including the transfer being made pursuant to a contract or intra-group scheme approval (which makes provisions for cover of the info principal and liability of the info fiduciary), or the approval of the central government, sensitive personal data could also be transferred outside India. However, a replica of such data must still be stored in India.

Company policies and practices
The general obligations for data handlers elaborated above apply to all or any companies handling data, and their policies must reflect the maximum amount .additionally , the IT Rules contain specific legislation to affect best practices, particularly within the context of breach and security.

Rule 8 of the IT Rules describes reasonable security practices and procedures as follows:

1. A body corporate or an individual on its behalf shall be considered to possess complied with reasonable security practices and procedures, if they need implemented such security practices and standards and have a comprehensive documented information security programme and knowledge security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the knowledge assets being protected with the character of business. within the event of an information security breach, the body corporate or an individual on its behalf shall be required to demonstrate, as and when called upon to try to to so by the agency mandated under the law, that they need implemented security control measures as per their documented information security programme and knowledge security policies.
2. The international standard IS/ISO/IEC 27001 on 'Information Technology – Security Techniques – Information Security Management System – Requirements' is one such standard mentioned in sub-rule (1).

3. Any industry association or an entity formed by such an association, whose members are self-regulating by following aside from IS/ISO/IEC codes of best practices for data protection as per sub-rule (1), shall get its codes of best practices duly approved and notified by the Central Government for effective implementation.
4. The body corporate or an individual on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to possess complied with reasonable security practices and procedures as long as such standard or the codes of best practices are certified or audited on a daily basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be administered by an auditor a minimum of once a year or as and when the body corporate or an individual on its behalf undertake significant upgradation of its process and computer resources.

There are not any statutory registration or notification requirements for either data processors or data controllers. the private Data Protection Bill 2019 provides for various transparency and accountability measures to which the info fiduciary shall be subject. as an example , every data fiduciary uder the Bill shall prepare a privacy intentionally policy, take any steps necessary to take care of transparency in personal processing , implement necessary security safeguards, report breaches of private data to the info protection authority, conduct impact assessments when it contemplates the utilization of latest technology or large-scale profiling and have in situ effective procedures and grievance redressal mechanisms for data principals. additionally , if notified by the info protection authority as a big data fiduciary, such entity must register with the authority, appoint a knowledge processing officer with relevant qualifications and suitable experience, conduct annual audits of its policies and processing and maintain records of its activities, security measures, impact assessments and other aspects of knowledge processing.

Discovery and disclosure
If requests from foreign companies are supported an order from a court of law, and if the country in question features a reciprocal arrangement with India, then an Indian court is probably going to enforce the request in India. within the absence of a writ , however, no obligation exists against an Indian company to form any quite disclosure.

In a Ministry of Communications and knowledge Technology handout , the govt clarified that any Indian outsourcing service provider or organisation providing services concerning collection, storage, dealing or handling of sensitive personal information or personal information under contractual obligations with a legal entity located within or outside India isn't subject to the IT Rules requirements with reference to disclosure of data or consent, provided it doesn't have direct contact with the info subjects when providing services.

PUBLIC AND PERSONAL ENFORCEMENT

Enforcement agencies
In addition to the safety practices and policies outlined in Section V, the private Data Protection Bill 2019 envisages the creation of a knowledge protection authority for the enforcement of knowledge protection legislation and to oversee compliance with it. The Bill will likely become the principal data protection legislation if enacted, and therein event, provisions concerning the safety of private data that state specifically that each data fiduciary must set appropriate technological, organisational and physical standards for the safety of knowledge under its control also will inherit force.

Recent enforcement cases
As is clear from the above, India has no distinct legislative framework to support litigation within the areas of privacy, cybersecurity and data protection. There has been no significant litigation during this area within the recent past. With the passage of the private Data Protection Bill 2019 into law, perhaps a clearer definition of rights will emerge during this sector and therefore the enforcement of rights will become both more active and more stringent.

Private litigation
In 2017, as a results of a clutch of petitions within the public interest, the Supreme Court conducted a review of India's national unique biometric authentication system, which was found out (pursuant to the Aadhaar (Targeted Delivery of monetary and Other Subsidies, Benefits and Services) Act 2016) for the delivery of social subsidies and potentially greater state surveillance of the financial behaviours of Indian citizens.[13] In the process of delivering its judgment on the Aadhaar Act, a five-judge bench of the Supreme Court clarified that privacy is a fundamental right of the Indian citizen, guaranteed by the Constitution. There has been no subsequent litigation on questions relevant to data privacy and protection in India since 2017.

Considerations for foreign organisations
Unfortunately, Indian jurisprudence does not touch upon compliance requirements for organisations functioning outside India (see Section IV).

[13] *KS Puttaswamy&Ors v. Union of India &Ors* available at https://main.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf.

Cybersecurity and data breaches

See Sections V and VI for information on breaches and breach reporting requirements. In addition to the information given in those sections, it is pertinent to note that in the context of a legal requirement to report data breaches to individuals, while the law as it is contains no such provision, the Personal Data Protection Bill 2019 does. According to the Bill, on the report of a breach by the data fiduciary to the data protection authority as mandated, the authority shall determine whether or not the data fiduciary must also notify the data principal in question. This decision will depend on the severity of the harm caused to the data principal and the action required by the data fiduciary to mitigate such harm.

CONCLUSION

The several agencies performing cybersecurity operations in India, such as the National Technical Research Organisation, the National Intelligence Grid and the National Information Board, require robust policy and legislative and infrastructural support from the Ministry of Electronics and Information Technology, and from the courts, to enable them to do their jobs properly. The Personal Data Protection Bill 2019, as tabled in parliament, is a comprehensive framework for data protection in India. Notwithstanding concerns that the Bill does not perfectly balance the privacy of citizens with the need for occasional government intervention, the Bill, once it is passed into law, is likely to function as a much more effective means of data protection (and the protection of allied interests, such as free speech) than existing legislation.