Q&A: the data protection legal framework in India

India | August 28 2020

Law and the regulatory authority

Legislative framework

Summarise the legislative framework for the protection of personally identifiable information (PII). Does your jurisdiction have a dedicated data protection law? Is the data protection law in your jurisdiction based on any international instruments on privacy or data protection?

India does not have a dedicated law on data protection and privacy. India has also not adopted any international instruments on privacy or data protection. Specific provisions on privacy are found in the Information Technology Act 2000 (IT Act). The IT Act is based on the United Nations Model Law on Electronic Commerce adopted by the United Nations Commissions on Internal Trade law on 30 January 1997 vide resolution A/RES/51/162. A plethora of laws in areas such as banking, telecoms and the medical field prescribe obligations of confidentiality. Banking regulations deal with when financial institutions can transfer data overseas and the types of data that cannot be transferred overseas. Telecom regulations, by and large, prevent the transfer of customer information overseas. The code of conduct of medical practitioners prevents disclosure of patient information. The insurance regulations restrict the transfer of claims-related data overseas.

The IT Act contains three provisions on data protection and privacy. Section 43A provides for compensation in the event one is negligent in using reasonable security practices and procedures (RSPP) in protecting sensitive personal data and information (SPDI) and this results in a wrongful gain or wrongful loss. It should be noted that this law provides only compensation, and only when a wrongful gain or loss results from the failure to observe RSPP. It can be argued that this is nothing but a codification of the law of negligence. This means that there is no negative consequence arising merely from the failure to observe RSPP. Further, RSPP is defined to mean such procedures stated by a law in force or as agreed to by the parties, and in the absence of both, the rules framed by the government. There is no statute that prescribes RSPP. This means that if parties – for example, an employer and an employee – agree on the RSPP to be adopted, the rules of the government would not apply.

In the guise of prescribing what constitutes RSPP, the government has issued basic and not very well-written privacy rules. As stated above, these rules apply only if the concerned parties have not agreed on the RSPP that would apply. These rules contain basic principles of privacy such as when SPDI can be collected, requirements of notice and consent, when SPDI can be transferred, among others.

Section 72A provides for criminal punishment if, in the course of performing a contract, a service provider discloses personal information without the consent of the person concerned or in breach of a lawful contract and he or she does so with the intention to cause, or knowing he or she is likely to cause, wrongful loss or wrongful gain.

Section 72 prescribes criminal punishment if a government official discloses records and information accessed by him or her in the course of his or her duties without the consent of the concerned person or unless permitted by other laws.

Data protection authority

Which authority is responsible for overseeing the data protection law? Describe the investigative powers of the authority.

There is no specific data protection authority in India. The IT Act provides for an adjudicating officer to be appointed to adjudicate whether a person has contravened the IT Act or its rules where the claim of injury or damages does not exceed 50 million rupees. If the claim exceeds 50 million rupees, the adjudicating authority would be the civil court. The Secretary to the Ministry of Information Technology in each state government has been appointed as the adjudicating officer. The adjudicating officer has all powers of a civil court. These include summoning the attendance of persons and examining them on oath, requiring the discovery or production of documents and other electronic records, receiving evidence on affidavits and issuing commissions for the examination of witnesses or documents.

The police have the power to investigate offences under the IT Act such as under section 72 and section 72A.

Under specialised statutes relating to banking, telecom and in the medical field, the relevant sectoral regulator has powers.

Cooperation with other data protection authorities

Are there legal obligations on the data protection authority to cooperate with other data protection authorities, or is there a mechanism to resolve different approaches?

There is no data protection authority in India.

Breaches of data protection

Can breaches of data protection law lead to administrative sanctions or orders, or criminal penalties? How would such breaches be handled?

Under section 43A, if a breach results in a wrongful gain or wrongful loss, the adjudicating officer can order compensation to be paid. The law does not prescribe what the maximum compensation is. Under section 72, the punishment is imprisonment of up to two years or a fine of up to 100,000 rupees, or both. Under section 72A, the punishment is imprisonment of up to three years or a fine of up to 500,000 rupees, or both. Other laws provide for penalties under those statutes for breach of confidentiality provisions.

Scope

Exempt sectors and institutions

Does the data protection law cover all sectors and types of organisation or are some areas of activity outside its scope?

The provisions under the Information Technology Act 2000 (IT Act) apply to all sectors, though laws specific to particular sectors would apply concurrently. Section 43A of the IT Act relates to a body corporate and the rules issued thereunder exclude the government from the meaning of ‘a body corporate’. Section 72A covers all types of organisations. Section 72 relates only to a government officer.

It should be noted that under section 43A, the parties concerned can agree among themselves on the reasonable security practices and procedures (RSPP) to be adopted. If they do so, then the privacy rules passed by the Indian government would be excluded.

Since section 72 dealing with breach of confidentiality by a government officer is subject to other laws, if another law permits the disclosure of the information by a government officer, such disclosure would not be a violation of section 72.

Other sector-specific laws provide for exceptions relating to those sectors. For example, a doctor could disclose information in circumstances where there is a serious and identified risk to a specific person or community. Banking laws refer to the duty of confidentiality in the context of other laws, practices and usages customary among bankers.

Communications, marketing and surveillance laws

Does the data protection law cover interception of communications, electronic marketing or monitoring and surveillance of individuals? If not, list other relevant laws in this regard.

Yes, the Indian Telegraph Act 1885 and the Information Technology Act 2000 permit the government to engage in surveillance based on certain criteria that is in the interests of the sovereignty and integrity of India, security of the state, friendly relations with foreign states, public order or for prevention of incitement of the commission of an offence. These grounds are based on reasonable restrictions to free speech contained in the Constitution of India.

All surveillance has to be approved in writing by the home secretary of the central government or the relevant state government as the case may be. The home secretary is the most senior of bureaucrats tasked with maintaining law and order. Indian law does not require the permission of a court to engage in surveillance.

Other laws

Identify any further laws or regulations that provide specific data protection rules for related areas.

Many laws impose a duty on service providers to maintain the confidentiality of customer information. For example, medical laws deal with maintaining the confidentiality of patient information. Such laws, for example, relate to medical termination of pregnancy and mental health. The codes of ethics for medical professionals also prescribes that doctors must maintain the confidentiality of patient information.

Banking laws also deal with the protection of confidentiality of customer information. This is provided both in statutes relating to banks and payment systems as well as regulations passed by India's central bank, the Reserve Bank of India (RBI), on customer servicing, credit card operations of banks, among others.

A statute dealing with credit information companies requires credit information companies and credit institutions (banks, etc) to adopt principles relating to the collection of information, processing of such information, protection of data and the manner of access and sharing of data. The principles are not prescribed by the law or by the regulator but have to be framed by the concerned credit information companies and institutions.

The RBI has prescribed detailed guidelines on information security, electronic banking, technology risk management and cyber frauds. In particular, the guidelines mention that banks must report breaches to the RBI and require the use of encryption technology of at least 128-bit SSL and implementation of ISO/IEC 27001 and ISO/IEC 27002. Further, the banking regulations require banks to appoint a chief information security officer who will be responsible for articulating and enforcing the policies that banks use to protect their information assets apart from coordinating security-related issues.

RBI regulations on outsourcing also deal with the ability of banks to transfer data outside India. This is permitted, provided that:

- the offshore regulator will not obstruct the arrangement or prevent inspections by the RBI or auditors;
- the availability of records to the management and RBI would withstand the liquidation of the offshore provider or the bank in India;
- the offshore regulator does not have access to the data simply because the data is being processed overseas; and
- the jurisdiction of the courts in the offshore location would not extend to the operations of the bank in India.

The outsourcing regulations also require customer data to be isolated and clearly identified, and there can be no comingling of data. Telecom laws, by and large, prohibit the transfer of customer accounting and user information outside of India except with regard to roaming information and remote access to such data from outside India. A recent notification issued by the RBI imposes restrictions on overseas transfers of payment system data by payment system operators.

PII formats

What forms of PII are covered by the law?

While section 72A of the IT Act covers personal information, section 43A covers sensitive personal data and information (SPDI). 'Personal information' means information that relates to a natural person, which either directly or indirectly in combination with other information available or likely to be available with a body corporate is capable of identifying such person. SPDI covers the following:

- passwords;
- financial information such as bank account or credit card or debit card or other payment instrument details;

- physical, physiological and mental health conditions;
- sexual orientation; medical records and history; and
- biometric information.

The law does not distinguish personal information on the basis of the format of the information, such as electronic as opposed to physical records. However, the laws on SPDI are applicable only to SPDI in electronic form.

Extraterritoriality

Is the reach of the law limited to PII owners and processors of PII established or operating in the jurisdiction?

The law does not specify whether it applies only to personally identifiable information (PII) owners or processors of PII established or operating in the jurisdiction. After the privacy rules were notified, there was some concern that they would apply to the SPDI of foreign nationals that was being processed in India by the many business process outsourcing businesses to India. The government then issued a press note to clarify that it relates only to a body corporate or person located within India. Further, data processing as a result of a contract between two entities is not covered by the privacy rules. While the clarification is not entirely clear, the accepted view is that this does not apply to foreign personal information being processed in India.

The law does allow transfer of SPDI out of India only if the recipient ensures the same level of data protection.

Covered uses of PII

Is all processing or use of PII covered? Is a distinction made between those who control or own PII and those who provide PII processing services to owners? Do owners', controllers' and processors' duties differ?

The law is not entirely clear on this point, though there is a clarification that appears to suggest that the privacy rules relate to a party that collects the data directly from the providers of the information and does not relate directly to a situation where the processor of the information receives the information from another body corporate. At the same time, the law allows transfer of SPDI only if the recipient ensures the same level of data protection. The two provisions are somewhat contradictory as one exempts onward transfers and the other appears to apply the rules to onward transfers.

Law stated date

Correct on

Give the date on which the information above is accurate.

4 May 2020

Kochhar & Co - Naqeeb Ahmed Kazia and Stephen Mathias