AN ANALYSIS OF DATA PROTECTION LAWS IN INDIA

Syamantak Sen & Antra Sisodiya

National Law Institute University, Bhopal

WHAT IS DATA PROTECTION?

The term "data" might be used to talk about information which –

a) is being processed by means of equipment that operates automatically,
b) is recorded with the intention that it should be processed using such equipment,
c) is either recorded as part of an information system or with the intention that it should form part of an information system,
d) is held on computer, or is intended to be held on computer,
e) is related to individuals to the extent that, although the information is not processed by means of such equipment, the record is structured, either by reference to such individuals or by reference to specific attributes related to such individuals, in such a way that specific information relating to a particular individual is easily accessible.
f) is recorded information held by a public authority[1].

'Data protection' can be defined as the process of protecting data and involves the relationship between the collection and distribution of data, the public's insight and expectation of privacy and the political and legal web that entangles data[2]. The context of 'data protection' varies and the methods and extent also vary according to one's capacity, for instance, there is data protection on the personal level, that of business or public entities, and that of data so highly classified that it should never fall into the hands of others aside from its owners — or in other words, top secret[3].

STATUES IN INDIA

There is no express legislation in India dealing with "Data Protection". However, the courts have read into related statutes to deal with "Data Protection" cases.[4]

Personal Data Protection Bill, 2006

[1] Roth, Alexander D. "DOCUMENTS ON DATA PROTECTION." International Legal Materials, vol. 19, no. 2, 1980.
[2] First Nations Information Governance Centre (FNIGC). "Pathways to First Nations' Data and Information Sovereignty." Indigenous Data Sovereignty: Toward an Agenda, edited by TAHU KUKUTAI and JOHN TAYLOR, vol. 38, ANU Press, Acton ACT, Australia, 2016.
[3] Wells, Nicholas D., et al. "Information Services, Technology, and Data Protection." The International Lawyer, vol. 44, no. 1, 2010.
[4] Raghavan, Radha & Ramchandran, Ramya, "Data Protection Law in India: An Overview" The Lex Warrier, January 29 2013.

The bill has been based upon and has further advanced the general framework of the European Union Data Privacy Directive, 1996. The bill aims to govern the collection, processing and distribution of personal data. However, the bill is only applicable to 'personal data' as defined in it. The bill can be applied to both government as well as private corporations engaged in data usage. "Personal Data" has been defined in the bill as,

"The personal data of any person collected for a particular purpose or obtained in connection with any transaction, whether by appropriate Government or by any private organization, shall not be put to processing without the consent of the person concerned: Provided that personal data of any person may be processed for any of the following purposes-

a) the prevention or detection of crime;
b) the prosecution of offenders; and
c) the assessment or collection of any tax or duty. Provided further that no consent of the individual shall be required if the personal data details of the individual are obtained through sources which have been made public."

Information Technology Act, 2000

Efforts have been made by the Indian Parliament to address data privacy issues under the purview of Information Technology Act, 2000. The act has also been amended to meet newer challenges in cybercrime. Two important provisions that have a strong bearing on the legal regime for data protection have been introduced through this amendment, they being sections 43A and 72A. However, it is reasonable to suggest that present provisions dealing with data security and confidentiality are grossly insufficient.

Law of Contract

In recent times, corporate houses have been relying on contracts to protect their data. Companies have inked several agreements with partner companies, clients as well as partners to control the privacy of their data according to their will. These agreements ensure a smooth running of their businesses.

The Copyright Act, 1957

Copyright over a database and data in general is protected by the Copyright Act, 1957. It has been held by Indian Courts that the Copyright Act, 1957 protects only slavish imitation of data. This principle was laid down in V.Govindan v. E.M Gopalkrishna[5] by the Madras High Court. However, this is not sufficient to check imitation of one's database with minor modifications.

Article 21, Indian Constitution

[5] V.Govindan v. E.M Gopalkrishna. AIR 1955 Mad 391.

Article 21 of the Indian Constitution guarantees the fundamental right to personal liberty which includes the right to privacy as well and thus by extension also includes private data that is not available in the public domain. Indian courts have extended this right to include electronic data as well.

JUDICIAL DECISIONS

1. People's Union for Civil Liberties v. Union of India[6]

The Supreme Court held that right to hold a telephonic conversation in the privacy of one's home or office without interference can certainly be claimed as right to privacy. In this case the Supreme Court had laid down certain procedural guidelines to conduct legal interceptions, and also provided for a high-level review committee to investigate the relevance for such interceptions but such caution has been thrown to winds in recent directives from the government bodies as is evident from phone tapping incidents that have come to light. Justice Kuldip Singh observed,

"Telephone-Tapping is a serious invasion of an individual's privacy. With the growth of highly sophisticated communication technology, the right to hold telephone conversation, in the privacy of one's home or office without interference, is increasingly susceptible to abuse. It is no doubt correct that every Government, howsoever democratic, exercises some degree of subrosa operation as a part of its intelligence out-fit but at the same time citizen's right to privacy has to be protected from being abused by the authorities of the day."

2. State of Maharashtra v. Bharat Shanti Lal Shah[7]

The Supreme Court said that interception of conversation though constitutes an invasion of an individual's right to privacy but it can be curtailed in accordance with procedure validly established by law. It also struck down the Maharashtra Control of Organized Crime Act, 1999 for being violative of Article 14 of the Constitution of India. The Act had special provisions that allowed the authorities to intercept wire, electronic and oral communications to control organized crime.

3. R. Rajagopal v. State of T.N.[8]

The Supreme Court held that the petitioners have a right to publish what they allege to be the life story/autobiography of Auto Shankar insofar as it appears from the public records, even without his consent or authorisation but if they go beyond that and publish his life story, they may be invading his right to privacy. The Constitution exhaustively enumerates the permissible grounds of restriction on the freedom of expression in Article 19(2). The Supreme Court noted that,

[6] People's Union for Civil Liberties v. Union of India, AIR 1997 SC 568.
[7] State of Maharashtra v. Bharat Shanti Lal Shah & Ors., 2008 SCC (13) 5.
[8] R.Rajagopal v. State of T.N., 1994 SCC (6) 632.

"(1) The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a "right to be let alone". A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child-bearing and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages. Position may, however, be different, if a person voluntarily thrusts himself into controversy or voluntarily invites or raises a controversy.

(2) The rule aforesaid is subject to the exception, that any publication concerning the aforesaid aspects becomes unobjectionable if such publication is based upon public records including court records. This is for the reason that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by press and media among others."

4. Destruction of Public & Private Properties v. State of A.P.[9]

The Supreme Court observed that the media should base upon the principles of impartiality and objectivity in reporting, ensuring neutrality, responsible reporting of sensitive issues, especially crime, violence, agitations and protests, sensitivity in reporting women and children and matters relating to national security and respect for privacy. Casting couch is a very popular tool used by media nowadays which directly hammers the individual privacy. There is no guideline to handle this issue.

5. Mr. X v. Hospital Z[10]

The Supreme Court held that the doctor-patient relationship though basically commercial, is professionally a matter of confidence and, therefore, doctors are morally and ethically bound to maintain confidentiality.

In such a situation, public disclosure of even true private facts may sometimes lead to the clash of one person's right to be let alone with another person's right to be informed.

6. Smt. Selvi & Ors. v. State of Karnataka[11]

The Court held that narcoanalysis, lie detection and BEAP tests in an involuntary manner violate prescribed boundaries of privacy. A medical examination cannot justify the dilution of constitutional rights such as right to privacy.

7. Bhabani Prasad Jena v. Convenor Secretary, Orissa State Commission for Women & Anr.[12]

[9] Destruction of Public & Private Properties v. State of A.P., 2009 SCC (5) 212
[10] Mr. X v. Hospital Z, 2000 SCC (9) 439
[11] Smt. Selvi & Ors. v. State of Karnataka, 2010 SCC (7) 263
[12] Bhabani Prasad Jena v. Convenor Secretary, Orissa State Commission for Women & Anr., SC CIVIL APPEAL NOS. 6222-6223 OF 2010

The Supreme Court held that if a DNA test is eminently needed to reach the truth, the court must exercise the discretion of medical examination of a person.

8. Sharda v. Dharmpal[13]

The Supreme Court held that though the right to personal liberty has been read into Article 21, it cannot be treated as an absolute right. To enable the court to arrive at a just conclusion a person could be subjected to a test even though it would invade his right to privacy. It concluded that one has to maintain a balance between the rights of a citizen and the right to privacy. It ultimately requires a healthy and congenial interrelationship between the social good and the individual liberty. The court laid down a definition for 'privacy' and noted, ""Privacy" is defined as "the state of being free from intrusion or disturbance in one's private life or affairs". mental health treatment involves disclosure of one's most private feelings. In sessions, therapists often encourage patients to identify "thoughts, fantasies, dreams, terrors, embarrassments, and wishes". To allow these private communications to be publicly disclosed abrogates the very fiber of an individual's right to privacy, the therapist-patient relationship and its rehabilitative goals. However, like any other privilege the psychotherapist-patient privilege is not absolute and may only be recognized if the benefit to society outweigh the costs of keeping the information private. Thus if a child's best interest is jeopardized by maintaining confidentiality the privilege may be limited."

9. District Registrar and Collector, Hyderabad and Ors. v. Canara Bank and Ors.[14]

The Supreme Court held that the disclosure of the contents of the private documents of its customers or copies of such private documents, by the bank would amount to a breach of confidentiality and would, therefore, be violative of privacy rights of its customers. The court noted, "Once we have accepted in Govind and in latter cases that the right to privacy deals with 'persons and not places', the documents or copies of documents of the customer which are in Bank, must continue to remain confidential vis-a'-vis the person, even if they are no longer at the customer's house and have been voluntarily sent to a Bank……Once that is so, then unless there is some probable or reasonable cause or reasonable basis or material before the Collector for reaching an opinion that the documents in the possession of the Bank tend, to secure any duty or to prove or to lead to the discovery of any fraud or omission in relation to any duty, the search or taking notes or extracts therefore, cannot be valid. The above safeguards must necessarily be read into the provision relating to search and inspection and seizure so as to save it from any unconstitutionality."

10. Kharak Singh v. State of U.P. & Others[15]

Kharak Singh, who was acquitted in a dacoity case due to lack of evidence, challenged police surveillance in this case before the Supreme Court of India. A six-judge bench, in a

[13] Sharda v. Dharmapal, AIR 2003 SC 3450
[14] District Registrar and Collector, Hyderabad and Ors. v. Canara Bank and Ors., 2005 SCC (1) 496
[15] Kharak Singh v. State of U.P. & Others, 1963 AIR 1295

majority judgment, held that "privacy was not a guaranteed constitutional right". It however, held that Article 21 was the repository of residuary personal rights and recognized the common law of right to privacy. The provision allowing domiciliary visits was struck down as unconstitutional. Dissenting judge Justice Subbarao, however, remarked that even though the right to privacy was not expressly recognized as a fundamental right, it was an essential ingredient of personal liberty under Article 21. He also held all surveillance measures to be unconstitutional.

CONCLUSION

With an ever-increasing number of organisations using computers to store and process personal information there is always an imminent danger that the information could be misused or fall into the wrong hands. A number of concerns arise due to this development, some of which include, access to the information, accuracy of the information, whether the information can be copied or not and whether there is a record of changes made to the information[16]. Post demonetisation, the Indian government has initiated a timely and much needed measure to increase digital payment options to weed out black money and corruption from public life. As an integral part of the government's move to take the country towards a total cashless economy, these measures would change the quality of life of citizens. One area that demands immediate attention is the need for a strong legal framework for privacy and protection of data shared by the individuals and entities. Legislative reforms are not as quick as technological innovations, and this leads to doubts regarding the enforceability of rights.

Hence, simultaneous legislative reforms would be required as part of the digitisation programme. The legal rights and liabilities arising out of handling of data of individuals and entities require a careful examination. With every innovation in technology, an innovation in the art of misuse and fraud, also takes place. India, unlike countries such as the UK, Australia and other European countries, does not have a dedicated Data Protection Law. Some of the recent decisions of the Supreme Court have expanded the contours of privacy to arrest the increasing assaults on the privacy rights of the citizens. If the courts further expand the scope of the fundamental rights to include privacy and data protection, then the existing framework of law may be insufficient to address the future legal challenges.

Hence, a comprehensive Data Protection Law is required for greater legal clarity and safe enforceability of rights by owners of the data. This could be achieved through a special legislation with the objective of affording protection to the data and information of the natural and legal persons. The focus on implementation of newer areas of innovations may get blurred when included as part of the general laws. Hence, a special law is needed. The following could be the broad features of such a legal framework: Personal data must be

[16] Roos, Anneliese. "Core Principles of Data Protection Law." The Comparative and International Law Journal of Southern Africa, vol. 39, no. 1, 2006.

clearly defined as any lack of clarity could expose the privacy rights to greater risks. There should be a process of registration of the data and data collectors. This would create a central registry for tracking the flow of information. The authorities could then timely intervene and initiate penal actions against offenders. A central authority should be constituted for monitoring the collection of information and data, registration of collectors, regulating the collection and dissemination of data and to initiate penal action against offenders. What constitutes "offence" under law must be clearly delineated. The punishments under this legislation should be made stringent. This will safeguard the interests of the citizens who participate in the space of digitised transactions against the misuse of their data. Knocking at the doors of justice in the ordinary course of time may prove to be expensive and a long-drawn affair for them. Hence, prescription of a stringent penal framework with a time bound implementation mechanism will act as a deterrent against misuse. Penal provisions should be exemplary. Penal provisions of fine, including issuance of disgorgement orders, non-compoundable offences, etc, should form part of such a law. Security measures required by the data collectors and controllers to prevent misuse should be stipulated. Collection, processing, usage and the grounds of exceptions from the provisions of this law should be clear. A comprehensive data protection legislation on the above lines will guarantee a sense of safety to the owners of the data.

