



International Journal of Emerging Technologies in Computational and Applied Sciences (IJETCAS)

www.iasir.net

Data Transfer and Privacy Protection Laws in India: An Overview

Dharmendra Kumar Singh¹, Ajay Kumar Singh²

¹Department of Law, Bareilly College, Bareilly, Uttar Pradesh, India-243005

²Department of Physics, Bareilly College, Bareilly, Uttar Pradesh, India-243005

Abstract: Computer and internet power has grown exponentially. Major problems arise with regard to protection of the citizen against the abuse of society data bank (information). There is the problem of trans-border data flow, that is the flow of data concerning citizens of a country which escape beyond national borders and thereafter remains free from the control of the country to which that individual belongs. A pooling of data contained in income tax records, custom records, police records, health records, credit records, bank records, motor registration records, insurance records and the like can give any government a vast dossier of information about each individual citizen. The lack of the necessary controls, in regard to the vast bulk of society data bank, poses grave human rights problems. Both governments and corporate establishments can be the entities which abuse such information power. The realization of three human rights norm i.e.- privacy, non-discrimination and consent is likely to be profoundly affected by the types of information systems that are developed and instituted, the manner in which access to the information they contain is regulated, and the way these data are used.

Keywords: security, data security, protection, access controls, information flow and IT Act.

I. Introduction

The rising abuse of computers and increasing threat to personal privacy through data banks has stimulated much interest in the technical safeguards for data. There are four kinds of safeguards, each related to but distinct from the others. Access controls regulate which users may enter the system and subsequently which data sets an active user may read or write. Flow controls regulate the dissemination of values among the data sets accessible to a user. Inference controls protect statistical databases by preventing questioners from deducing confidential information by posing carefully designed sequences of statistical queries and correlating the responses. Statistical data banks are much less secure than most people believe. Data encryption attempts to prevent unauthorized disclosure of confidential information in transit or in storage [1, 2].

The number of cross-border civil and commercial matters involving personal data issues are increasing as globalization and e-commerce continue to grow. As a result, the need for a consistent and predictable regime for the application of international data transfer rules is a recurrent issue at the domestic, regional and international levels. Cross-border data transfers are intrinsic to personal and professional relationships throughout the world, particularly when the omnipresent nature of the Internet is taken into account. The added convenience and efficiency resulting from global data flows also increases the risk to individuals' privacy. Protecting privacy in a global environment depends on cross-border co-operation. Although the need for effective enforcement and co-operation has been duly noted for many years, there is now renewed interest in working at the international level to address outstanding challenges in a world where trans-border data flows are widespread and continuous. Protection of privacy in an international context has become increasingly complex, and has become inherently linked with other important global issues, such as human rights, security, trade and development [3].

Technology has radically changed the manner in which information flows around the world. Global transfers of information are now a common and essential component of our daily lives. Sharing information allows businesses to provide consumers with enhanced services such as 24-hour customer hotlines as well as a greater choice of products and services at lower prices. At the same time, businesses are able to manage their operations in a more cost effective and efficient manner. Countries, in turn, benefit from increased global business investment and activity. All in all, consumers, businesses and governments receive enormous benefits from global data transfers [4].

The movement of information across national borders drives today's global economy. Cross-border data transfers allow businesses and consumers access to the best available technology and services, wherever those resources may be located around the world. The free-flow of data across borders benefits all industry sectors, from manufacturing to financial services, education, and health care and beyond. The seamless transfer of information is as critically important as it is inexorably linked to the growth and success of the global economy. To function in the international marketplace, businesses need reliable, continuous access to data, wherever they are located. Routine business activities, such as providing goods and services to customers, managing a global workforce, and maintaining supply chains, require the transfer of data among corporate locations and to service

providers, customers, and others situated around the world. In addition, as the Internet has facilitated the growth and success of micro-multinationals, these small businesses now have access to billions of potential customers beyond their borders and are able to compete based on the quality of their offerings, unconstrained by geographic limitations.

India does not currently have a general data protection statute. Nevertheless, the judiciary has derived a "right of privacy" from the rights available under Articles 19(1)(a) (the fundamental right to freedom of speech and expression) and 21 (the right to life and personal liberty) of the Constitution of India. However, all cases that deal with the right to privacy have been decided in the context of Government actions that resulted in private citizens being denied their right to personal privacy. No privacy judgment has granted private citizens a right of action against the breach of privacy by another private citizen. To that extent, the data protection and personal privacy jurisprudence in the country is not yet fully developed.

India is not a particularly private nation. Personal information is often shared freely and without thinking twice. Public life is organized without much thought to safeguarding personal data. In fact, the public dissemination of personal information has over time, become a way of demonstrating the transparent functioning of the government. Government collect personal data, this information is stored in silos with each agency of the government maintaining information using different fields and formats. Government databases do not talk to each other and given how differently they are organized, the information collected by different departments cannot be aggregated or unified.

Data privacy and the need to protect personal information is almost never a concern when data is stored in a decentralized manner. Data that is maintained in silos is largely useless outside that silo and consequently has a low likelihood of causing any damage. However, all this is likely to change with the implementation of the UID Project. One of the inevitable consequences of the

UID Project will be that the UID Number will unify multiple databases. As more and more agencies of the government sign on to the UID Project, the UID Number will become the common thread that links all those databases together. Over time, private enterprise could also adopt the UID Number as an identifier for the purposes of the delivery of their services or even for enrollment as a customer. Once this happens, the separation of data that currently exists between multiple databases will vanish. Such a vast interlinked public information database is unprecedented in India. It is imperative that appropriate steps be taken to protect personal data before the vast government storehouses of private data are linked up and the threat of data security breach becomes real.

Similarly, the private sector entities such as banks, telecom companies, hospitals etc are collecting vast amount of private or personal information about individuals. There is tremendous scope for both commercial exploitation of this information without the consent/ knowledge of the individual consent and also for embarrassing an individual whose personal particulars can be made public by any of these private entities. The IT Act does provide some safeguards against disclosure of data / information stored electronically, but there is no legislation for protecting the privacy of individuals for all information that may be available with private entities. In view of the above, privacy of individual is to be protected both with reference to the actions of Government as well as private sector entities.

As private data moves online, the need to secure it properly becomes increasingly urgent. The good news is that the same forces concentrating data in enormous datacenters will also aid in using collective security expertise more effectively. Adding protections to a single cloud platform can immediately benefit hundreds of thousands of applications and, by extension, hundreds of millions of users [5]

II. LAWS IN INDIA

There is no specific legislation on privacy and data protection in India. However, the Information Technology Act, 2000 (IT Act) contains specific provisions intended to protect electronic data (including non-electronic records or information that have been, are currently or are intended to be processed electronically). Section 43A of the IT Act provides for protection of sensitive personal data and information of individuals. A body corporate possessing, dealing with or handling sensitive personal data or information in a computer resource must implement and maintain reasonable security practices and procedures and as a result causes wrongful loss or wrongful gain to any person; it may be required to pay damages to the affected person.

The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rule 2011 (IT Rules) framed under section 43A of the IT Act, set out the reasonable security practices and procedures that must be implemented to protect sensitive personal data. While the IT Act and IT Rules regulate the collection and use of sensitive personal information, the government has proposed to enact a specific legislation on privacy (Privacy Bill) which will override the IT Rules. The Privacy Bill recognizes an individual's right to privacy and provides that it cannot be infringed except in certain circumstances, such as for reasons of:

- Protection of India's sovereignty or integrity.
- National security.
- Prevention of commission of crime.

- Public order.

Unauthorised collection, processing, storage and disclosure of personal information is treated as infringement of privacy under the Privacy Bill. Various sector specific regulators require banks and securities markets intermediaries (such as stock brokers, share transfer agents and bankers to a public issue, and depository participants) to maintain confidentiality of client data including personal data. These sector-specific regulators include the Reserve Bank of India (banking sector regulator) and the Securities and Exchange Board of India (securities markets regulator). These regulations apply in addition to the IT Rules [6].

The Privacy Rules define the term ‘personal information’ as any information that relates to a natural person, which either directly or indirectly, in combination with other information that is available or likely to be available to a corporate entity, is capable of identifying such person.

The Privacy Rules define ‘sensitive personal data or information’ to include the following information relating to password, financial information e.g. bank account/credit or debit card or other payment instrument details, physical, physiological and mental health condition, sexual orientation and medical records and history, biometric information, any detail relating to the above clauses as provided to a corporate entity for providing services, and any of the information received under the above clauses for storing or processing under lawful contract or otherwise.

Biometrics means the technologies that measure and analyse human body characteristics, such as ‘fingerprints’, ‘eye retinas and irises’, ‘voice patterns’, ‘facial patterns’, ‘hand measurements’ and ‘DNA’ for authentication purposes. However, any information that is freely available in the public domain is exempt from the above definition.

Every corporate entity collecting sensitive personal information must appoint a Grievance Officer to address complaints relating to the processing of such information, and to respond to data subject access and correction requests.

Under the Act, if a corporate entity that possesses, manages or handles any sensitive personal information in a computer resource that it owns, controls or operates, is negligent in implementing and maintaining compliance with the Privacy Rules, and its negligence causes wrongful loss or wrongful gain to any person, the corporate entity shall be liable for damages to the person(s) affected.

The Privacy Rules state that any corporate entity or any person acting on its behalf, which is collecting sensitive personal information, must obtain written consent (through letter, email or fax) from the providers of that information.

However, the August 2011 ‘Press Note’ issued by the IT Ministry clarifies that consent may be given by any mode of electronic communication. The Privacy Rules also mandate that any corporate entity (or any person, who on behalf of such entity) collects, receives, possess, stores, deals or handles information, shall provide a privacy policy that discloses its practices regarding the handling and disclosure of personal information including sensitive personal information and ensure that the policy is available for view, including on the website of the corporate entity (or the person acting on its behalf).

Specifically, the corporate entity must ensure that the person to whom the information relates is notified of the following

- at the time of collection of sensitive personal information or other personal information
- the fact that the information is being collected
- the purpose for which the information is being collected
- the intended recipients of the information, and
- the name and address of the agency that is collecting the information and the agency that will retain the information.

Further, sensitive personal information may only be collected for a lawful purpose connected with a function or purpose of the corporate entity and only if such collection is considered necessary for that purpose. The corporate entity must also ensure that it does not retain the sensitive personal information for longer than it is required, and should also ensure that the same is being used for the purpose for which it was collected.

A corporate entity or any person acting on its behalf is obligated to enable the providers of information to review the information they had so provided and also to ensure that any personal information or sensitive personal information that is found to be inaccurate or deficient is corrected upon request. Further, the provider of information has to be provided a right to opt out (i.e. she will be able to withdraw his/her consent) even after consent has been provided. However, the corporate entity will not be held responsible for the authenticity of the personal information or sensitive personal information given by the provider of information to such corporate entity or any other person acting on its behalf.

The data collector must obtain the consent of the provider of the information for any transfer of sensitive personal information to any other corporate entity or person in India, or in any other country that ensures the same level of data protection as provided for under the Privacy Rules. However, consent is not necessary for the transfer, if it is required for the performance of a lawful contract between the corporate entity (or any person acting on its behalf) and the provider of information or as otherwise specified in the Act.

A corporate entity may not transfer any sensitive personal information to another person or entity that does not maintain the same level of data protection as required in the Act. The contract regulating the data transfer should contain adequate indemnity provisions for a third party breach, should clearly specify the end purposes of the data processing (including who has access to such data) and should specify a mode of transfer that is adequately secured and safe.

Further, under the Act, it is an offence for any person who has pursuant to a contract gained access to any material containing personal information to disclose that information without the consent of the person concerned, and with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain. Thus, contracts should also specifically include provisions: entitling the data collector to distinguish between 'personal information' and 'sensitive personal information' that it wishes to collect/process representing that the consent of the person(s) concerned has been obtained for collection and disclosure of personal information or sensitive personal information, and outlining the liability of the third party.

A corporate entity possessing, dealing or handling any sensitive personal information in a computer resource which it owns, controls or operates is required to implement and maintain reasonable security practices and procedures to secure the sensitive personal information. The reasonable security practices and procedures may be specified in an agreement between the parties.

Further, the Privacy Rules provide that in the absence of such agreement 'reasonable security practices and procedures' to be adopted by any corporate entity to secure sensitive personal information are procedures that comply with the IS/ISO/IEC 27001 standard or with the codes of best practices for data protection as approved by the Federal Government.

The Government of India, has established and authorised the Computer Emergency Response Team (Cert-In), to collect, analyse and disseminate information on cyber incidents, provide forecast and alerts of cyber security incidents, provide emergency measures for handling cyber security incidents and coordinate cyber incident response activities.

The Information Technology (the Indian Computer Emergency Response Team and Manner of Performing Functions and Duties) Rules, 2013 (Cert-In Rules) impose mandatory notification requirements on service providers, intermediaries, data centers and corporate entities, upon the occurrence of certain 'cyber security incidents'.

Cyber security incidents have been defined to mean any real or suspected adverse events, in relation to cyber security, that violate any explicitly or implicitly applicable security policy, resulting in: unauthorised access, denial or disruption of service unauthorised use of a computer resource for processing or storage of information changes to data, information without authorisation.

The occurrence of the following types of cyber security incidents, trigger the notification requirements under the Cert-In Rules:

- Targeted scanning/ probing of critical networks/ systems
- Compromise of critical information/ system
- Unauthorized access of IT system/ data

Defacement of websites or intrusion into website & unauthorized changes such as inserting malicious codes, links to external websites Malicious code attacks such as spreading virus, worm/ Trojan/ Botnets/ Spyware Attacks on servers such as Database, Mail and DNS & Network devices such as Routers Identity theft, Spoofing and phishing attacks Denial of service (DoS) & Distributed Denial of service (DDoS) attacks, Attacks on critical infrastructure , SCADA systems and wireless networks, attacks on application such as E-governance and E-commerce etc.

Upon the occurrence of any of the aforementioned events, companies are required to notify the Cert-In within reasonable time, so as to leave scope for appropriate action by the authorities. The format and procedure for reporting of cyber security incidents have been provided by Cert-In on its.

Civil penalties of up to EUR 694,450 for failure to protect data including sensitive personal information may be imposed by an Adjudicating Officer; damages in a civil suit may exceed this amount. Criminal penalties of up to 3 years imprisonment or a fine up to EUR 6,950, or both for unlawful disclosure of information.

The Act does not refer to electronic marketing directly. However, sending false information (emails, SMS, MMS, etc.) persistently by means of a computer resource or a communication device for the purpose of causing annoyance, inconvenience, etc. is punishable under Indian law. Further, such emails, SMS, MMS etc. must not disguise or conceal the identity of the sender. The Privacy Rules also provide the right to 'opt out' of email marketing, and the company's privacy policy must address marketing and information collection practices.

There is no regulation of cookies, behavioural advertising or location data. However, the IT Act contains both civil and criminal offenses for a variety of computer crimes: Any person who introduces or causes to be introduced any computer contaminant into any computer, computer system or computer network may be fined up to EUR 694,450 (by an Adjudicating Officer); damages in a civil suit may exceed this amount. Under the IT Act, 'computer contaminant' is defined as any set of computer instructions that are designed: to modify, destroy, record, or transmit data or programmers' residing within a computer, computer system or computer network, or

by any means to usurp the normal operation of the computer, computer system or computer network Any person, who fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, is subject to a prison term of up to 3 years and fine up to EUR 1,390 [7].

III. Conclusion

It is important to ensure that the data is stored only till the time the purpose for which it was collected is achieved, unless the purpose is for archival purposes, national security purposes etc. To the extent possible the legislation must prescribe the measures to be taken by the data controllers to ensure the security of data under its control. Care should be taken to ensure that the measures prescribed should be technology neutral as it is likely that data security measures will only improve in the future. The emphasis should be on ensuring that appropriate measures are taken with a view to achieving a prescribed and stated result. There should be no attempt at prescribing the means to achieving that end.

The data must be protected against unauthorised access, deletion, disclosure and alteration. The onus to protect the data must be on the data controller. It may also be worth considering circumstances under which the data regulator could supervise the implementation of these measures.

In order to ensure that the database is accurate and up to date, specific provisions should be included to allow data subjects to rectify their own personal information. In fact, data subjects should always be allowed to review their personal information collected and stored in the database. It is important to consider whether legal heirs, guardians and authorised representatives of the data subject should be granted access to personal information of their guardians or wards. This would also be relevant to consider in the context of deceased data subjects – for instance, would it be possible to conclude, after the death of a person, that he ceases to be a natural person and therefore is no longer protected under the statute? In all these circumstances adequate verification procedures must be implemented to ensure that personal information does not fall into the hands of persons not authorised to collect it.

A strong data protection law will afford the opportunity for free flow of personal data from the European Economic Area to India. This would particularly benefit providers of outsourcing services located in India. However, there may not be a pressing need to enact data protection legislation as stringent as the European legislation in the Indian context. While there are many benefits in having a strong regime, the practical difficulties in implementing such provisions in a country of over a billion people with not prior experience in data protection would be challenging in the extreme.

However, it may be advisable to ensure appropriate measures to protect the data of Indian citizens that are processed outside the country. The legislation could include provisions that allow the regulator to proceed against data controllers not just for data protection violations committed within the country but also outside the country if the data concerned relates to an Indian citizen, or was collected by the data controller in India.

In the Indian context, it will be important to include exemptions on grounds of national security, discharge of statutory functions, protection of health and safety of citizens and such other circumstances as appropriate. However, in articulating exceptions care must be taken to ensure that the purpose for framing of the legislation is not diluted so much as to make it meaningless.

While there may not be an immediate need to include provisions relating to automated decisions into the data protection legislation (given the relatively few instances – if any – where data subjects have objected to such decisions having been taken against them), it is likely that as we grow more and more reliant on electronic databases this will become more of a problem. With that in mind it will probably be useful to include these provisions into the legislation.

Thus, while national security exemptions are necessary and recommended, they should be framed carefully to ensure that it is not possible for just anyone to claim that the provisions of the law are not applicable by citing some national security interest without substantiation. The persons who can claim the exemption and the circumstances should be carefully limited.

In the Indian context it is advisable to establish a regulator under the proposed data protection legislation. The role of the regulator would be to ensure that the legislation responds dynamically to the changing digital environment and fulfills the principles upon which the legislation was based. To this end the regulator should have the power to prescribe standards both technological and operational that could mould the manner in which the legislation is implemented. It is particularly important to develop the concept of accountability so that it should no longer be sufficient for organisations to meet applicable data protection requirements – they should demonstrate their willingness and ability to take on data responsibility and ensure compliance on an ongoing basis. The regulator should also have the power to require subsidiary regulators who operate under the provisions of legislations that include reference to data protection principles, to conform to the broad principles of the data protection legislation.

Since data protection and personal privacy are the other end of the spectrum from the right of citizens to access public information (as enshrined in the Right to Information Act), it may be appropriate to house the office of

the Data Regulator within the same executive framework as the chief information officers under the Right to Information Act[8].

Storage, virtualization, and networks are the biggest security concerns in Cloud Computing. Virtualization which allows multiple users to share a physical server is one of the major concerns for cloud users. Also, another challenge is that there are different types of virtualization technologies, and each type may approach security mechanisms in different ways. Virtual networks are also target for some at-tacks especially when communicating with remote virtual machines. However, new security techniques are needed as well as redesigned traditional solutions that can work with cloud architectures. Traditional security mechanisms may not work well in cloud environments because it is a complex architecture that is composed of a combination of different technologies [9].

Cross-border data transfers are indispensable to the growth of the digitized global economy. The global economy simply cannot afford to revert to digital isolationism. The question is whether governments will implement legal regimes to promote a beneficial expansion of the data economy, or if the cumbersome systems currently in place will continue in force, hindering innovation and slowing progress. The path forward must include cooperation between regulators and businesses working together to determine how best to address important concerns about privacy and data security without crippling economic growth. In India cross-border transfers are permitted where (1) the recipient jurisdiction provides an equivalent level of data protection to that contained in India's Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules; (2) the transfer is necessary for the performance of a contract between the data recipient and the individual; or (3) the transfer is made with the individual's consent. Prior written consent is required to transfer sensitive personal data. [10].

References

- [1] Dorothy E. Denning & Peter J. Denin, Data Security, Computing Surveys, Vol.11 (3) 1979,227.
- [2] "The Data Deluge: Businesses, governments and society are only starting to tap its vast potential", The Economist (25 February 2010), p. 11.
- [3] "A special report on managing information: Data, data everywhere", The Economist (25 February 2010), p. 16.
- [4] Miriyam Wugmeister, Karinretzer & Cynthiarich, Georgetown Journal of International Law, 2007,449.
- [5] Dawn Song, Elaine Shi, Ian Fischer and Umesh Shankar, Cloud Data Protection for Masses, Published by the IEEE Computer Society, 2012, 39.
- [6] Kosturi Ghosh & Suvojit Halder, Data Protection in India: Overview, global.practicallaw.com/1-505-9607.
- [7] *Data Protection Laws of the World*, 140. <http://www.dlapiperdataprotection.com>.
- [8] Approach Paper For Legislation on Privacy, No-17/1/201-IR, Government of India, Ministry of Personnel, P G & Pensions, Department of Personal Training.
- [9] Keiko Hashizume, David G Rosado, Eduardo Fernández-Medina and Eduardo B Fernandez, *Journal of Internet Services and Applications*, 4(5), 2013, 1.
- [10] Hunton and Williams, *Business without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity*, U S Chamber of commerce, 2014.