DATA PROTECTION, PRIVACY AND CORPORATE COMPLIANCE: THE LAW AND EMERGING TRENDS IN INDIA

Rodney D Ryder & Ashwin Madhavan

Introduction – Welcome to the Back Office of the World!

Outsourcing to India is one of the best ways for CIOs to cut application development and maintenance costs, deal effectively with the immense growth and demand of softwares, and focus on more strategic work. Nearly two thirds of the Fortune 500 companies are outsourcing work to India be it voice or non voice.[1]

One of the primary areas of concern is the absence of a privacy culture and little privacy and data protection regulation in India. The importance of the outsourcing business in India must certainly be taken in consideration given the quantity of processed data that can potentially increase the degree of risk that a misuse could pose for data-subjects. It is because of a lack of data privacy regulation that has hampered many Indian firms from gaining lucrative contracts in key segments of the BPO industry. [2]

The Data Protection Regime in India: Analysing the Context

The Constitution of India does not provide for a fundamental right to privacy explicitly. However, the Constitution of India embodies the Fundamental Rights in Part III, which are enumerated in Article 14-30. Judicial activism has then brought the Right to Privacy within the realm of Fundamental Rights. The Supreme Court deduced that right from the Right to Life and Personal Liberty enshrined in Article 21 of the Constitution through an extensive interpretation of the phrase.[3] The right to privacy has derived itself from two sources: one being common law of torts and the other being constitutional.[4]

No specific legislation pertaining to data protection has been enacted in India.[5] However, one could claim that other statutes provide some safeguards to the lack of explicit legislation in that field. These statutes must be examined even if they cannot provide adequate protection on their own accord.

The 'IT Act' – The Indian Information Technology Act, 2000

---

[1] Fortune 500 Companies Simply love India, 7th July 2005, available at <http://economictimes.indiatimes.com/archivelist.cms?year=2005&month=7&starttime=38540>

[2] *R P Srikanth*, 'Indian BPO firms constrained by lack of data protection laws', 26th April 2004 available at *<http://www.expresscomputeronline.com/20040426/coverstory01.shtml>* **(accessed on 25th July 2008)**

[3] *R. Rajagopal v. State of T.N.*, (1994) 6 SCC 632; also See *Gobind* v. *State of M.P., (1975) 2 SCC 148*

[4] *Madhavi Divan*, 'The Right to Privacy in the Age of Information and Communications' **(2002) 4 SCC (Jour) 12,** also available online at *<http://www.ebc-india.com/lawyer/articles/2002v4a3.htm>* **(accessed on 27th July 2008)**

[5] ibid

The IT Act doesn't provide for any definition of personal data. Besides, provisions regarded as providing rules pertaining to data protection include Chapters IX and XI that define cyber contraventions related to unauthorized access to computer, computer system, computer network or resources, unauthorized alteration, deletion, addition, modification, alteration, destruction, duplication or transmission of data, computer database. Some sections of Chapters IX and XI are viewed in India as the "backbone" of the data protection regime.

The sections which form the backbone of data protection are S.43[6], S.65[7] and S.72.[8] However, over the last six years, since the act was first enforced, it has increasingly become evident that the current IT Act does not contain sufficient privacy and data protection provisions.[9] The Indian

government, aware of the lack of regulation in this field, appointed an Expert Committee on Cyber Laws whose role was to suggest amendments to the IT Act. **They have proposed the following Amendments**:

---

[6] Section 43 of the IT Act 2000 reads as follows - 'Penalty for damage to computer, computer system, etc. If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, — (a) accesses or secures access to such computer, computer system or computer network; (b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium; (c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network; (d) damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network; (e) disrupts or causes disruption of any computer, computer system or computer network; (f) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder; (h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.'

[7] Section 65 of the IT Act 2000 reads as follows – 'Tampering with computer source documents. Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may
extend up to two lakh rupees, or with both.'

[8] Section 72 of the IT Act reads as follows – 'Penalty for breach of confidentiality and privacy.Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book. register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

[9] First Analysis of the Personal Data protection Law in India, Final Report, CRID – University of Namur, Report delivered in the framework of contract JLS/C4/2005/15 between CRID and the Directorate General Justice, Freedom and Security. Available at ..... **contd on page 3.**

..... *http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/final_report_india_en.pdf>* **(accessed on 28th August 2008)**

A new Section 43(2) related to handling of **sensitive personal data** or information with reasonable security practices and procedures thereto; (ii) Gradation of severity of computer related offences under Section 66, committed dishonestly or fraudulently and punishment thereof; (iii) fine-tuning of Section 72(1); (iv) additional Section 72 (2) for breach of confidentiality with intent to cause injury to a subscriber; (v) Language of Section 66 related to computer related offences has been revised to be in lines with Section 43 related to penalty for damage to computer resource. These have been graded with the degree of severity of offence when committed by any person, dishonestly or fraudulently without the permission of the owner. "Keeping in line with the principles in EC Directive 2000/31/EC, Section 79 has been revised to bring-out explicitly the extent of liability of intermediary in certain cases.[10]"

The proposed amendments are more or less reaction of the government to the data thefts and other cyber crime related incidents. The provisions purportedly for 'data protection' are an ugly patch on the IT Act and do not offer any comprehensive protection to personal data in India.[11]

Enforcement mechanisms

The Information Technology Act, 2000 has legislated the setting up of three authorities to provide a mechanism for arbitration or adjudication and settlement of civil disputes under the Act. These are:

a. Controller of Certifying Authorities,

b. Adjudicating Officer, and

c. Presiding Officer of the Cyber Regulations Appellate Tribunal

An affected party under Section 43 (a) – (h) has a right to seek damages from the wrongdoer by compelling him to pay for the damage done upto rupees one crore. The remedy lies in approaching and filing the complaint before the Adjudicating Officer under Section 46 of the Act. The adjudicating officer under the Act is a quasi-judicial authority powers limited to the determination of contraventions and imposition of penalties under S. 43, 44 and 45 of the Act only. The Central Government as per the Gazette Notification for Information Technology Rules, 2003 has notified 'Scope and Manner of Holding Inquiry' [Rule 4]. Moreover, S.46 (5) provides that the adjudicating officer has the same powers as are vested in a Civil Court under the Code of Civil procedure, 1908. Cyber Regulations Appellate Tribunal (CRAT) has appellate jurisdiction and power to examine the correctness, legality or propriety of the decision or order passed by the Controller of Certifying Authorities or the Adjudicating Officer under the Information Technology Act, 2000 is absolute.

This impliedly bars the jurisdiction of civil courts to hear such appeals. The Act further provides a second forum of appeal in the form of the High Court (the first being the Cyber Regulations Appellate Tribunal) to any person aggrieved by any decision or order of the Cyber Regulations Appellate Tribunal.

Contracts as 'alternative': The Indian Contract Act, 1872

[10] Does India need a separate data protection law?, available at *<http://www.knspartners.com/files/BNA%20Article-180106.pdf>* **(accessed on 28th July 2008)**

[11] ibid

The Indian Contract Act offers an alternative solution to protect data under Article 366(10). The Indian companies acting as 'data importers' may enter into contracts with 'data exporters' to adhere to a high standard of data protection. These contracts are binding and may fulfil the requirements of overseas customer(s) national legislations. Hence, Indian IT companies active in the IT/ BPO sector presently have a very stringent policy dealing with protection of their client's information and all the employees are contractually bound to protect the confidential information which may be processed. The employment contracts clearly specify that the employees have to maintain as secret and confidential all such information, which the company specifies from time to time.

Specific Relief Act

The Specific Relief Act provides preventive relief in the form of temporary and perpetual injunctions[12] to the plaintiff to prevent the breach of an obligation existing in his favour, whether expressly or by implication or award damages which has been provided under section 40 of the Act

Judicial Interpretation

The Supreme Court of India has construed a general Right to Privacy from Article 21 of the Constitution. However, this right is not absolute as it can be curtained according to a procedure established by law or when there is a superior countervailing interest and is also limited to the first generation of rights (the first cases of the Supreme Court only involve domiciliary visits).

No general right relating to personal data protection has been developed so far. The Indian conception of privacy is rather different from the European one. Although the Information Technology Act, 2000 is based on the Model Law on Electronic Commerce earlier adopted by the United Nations Commission on International Trade Law (UNCITRAL), it is often quoted in India as an Act containing provisions pertaining to data protection.

The research has analyzed several provisions but, in our opinion, none of them seems to offer an adequate protection. The concept of "personal data" is not even defined. Moreover, the contractor

[12] *Section 37* of the Specific Relief Act - Temporary and perpetual injunctions.- (1) Temporary injunctions are such as are to continue until a specified time, or until the further order of the court, and they may be granted at any stage of a suit, and are regulated by the Code of Civil Procedure, 1908 (5 of 1908). (2) A perpetual injunction can only be granted by the decree made at the hearing and upon the merits of the suit; the defendant is thereby perpetually enjoined from the assertion of a right, or from the commission of an act, which would be contrary to the rights of the plaintiff.

And *Section 38* - Perpetual injunction when granted.-(1) Subject to the other provisions contained in or referred to by this Chapter, a perpetual injunction may be granted to the plaintiff to prevent the breach of an obligation existing in his favour, whether expressly or by implication. (2) When any such obligation arises from contract, the court shall be guided by the rules and provisions contained in Chapter II.

(3) When the defendant invades or threatens to invade the plaintiff's right to, or enjoyment of, property, the court may grant a perpetual injunction in the following cases, namely:- (a) where the defendant is trustee of the property for the plaintiff; (b) where there exists no standard for ascertaining the actual damage caused, or likely to be caused, by the invasion; (c) where the invasion is such that compensation in money would not afford adequate relief; (d) where the injunction is necessary to prevent a multiplicity of judicial proceedings.

considers that the proposed amendments to this Act which have not been adopted so far will not be sufficient to ensure an adequate protection within the meaning of Directive 95/46/EC.[13]

"In general, the IT Act is more an Act related to e-commerce and cyber crime than a data protection Act. The Indian Contract Act provides for an alternative solution for European data exporters Nevertheless, this remains a subsidiary solution. The Credit Information Companies (Regulation) Act, 2005 contains certain provisions ensuring data protection but it is limited in its scope. It only imposes duties on credit information companies, credit institutions and specified users while processing credit information. Moreover, no specific authority has been established to ensure the implementation of these provisions under this Act. Nevertheless, Rules and Regulations that could be adopted under Article 20(f) of this Act could provide for an adequate protection in the field of credit information. Regarding the procedural and enforcement mechanisms, the research has analyzed the different ways of enforcement: general ones (courts and tribunals system) as well as specific ones (under the IT Act, Rules and Regulations that could be adopted under the Credit Information Companies Act, etc…). Given the absence of any general data protection Act, no Data Protection Authority has been established in India. However, Regulations made by the Reserve Bank of India –still not adopted- foresees, in Section 19, that the Reserve Bank is empowered to impose penalty or reprimand any credit information company, credit institution or specified user having contravened the Act. On this ground, the Reserve Bank could be considered as a specific Data Protection Authority in the field of credit information."[14]

SELF REGULATION AND 'INDUSTRY CODES' AS AN ALTERNATIVE

The National Association of Software and Service Companies [NASSCOM]

NASSCOM acts as an advisor, consultant and coordinating body for the software and services industry in India. In 2000, NASSCOM urged the government to pass a data protection law to ensure the privacy of information supplied over computer networks and to meet European data protection standards.

NASSCOM has been proactive in ensuring that the Indian Information Security environment benchmarks with the best across the globe. As a part of its Trusted Sourcing initiative, it is in the process of setting up the Data Security Council of India (DSCI) as a Self Regulatory Organization (SRO) to establish, popularize, monitor and enforce privacy and data protection standards for India's ITeS-BPO industry. The authors of this article are advisors to the Data Security Council of India.[15]

DSCI shall be based on the following five guidelines:

- Self regulation
- Adoption of best global practices
- Independent oversight
- Focused mission
- Enforcement mechanism

[13] 'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data' available at < *http://www.cdt.org/privacy/eudirective/EU_Directive_.html*> **(accessed on 28th 2008)**

[14] Supra Note 9
[15] ibid

The initiative is aimed at enabling Indian IT/ITES organisations to provide high standard of security and data protection, build capacity to provide security certification to organisations, common platform for promoting knowledge about information security and foster a community of security professionals/firms and create awareness among industry professionals and other stakeholders

The Indian Government finally steps in: The Indian Personal Data Protection Bill, 2006

The Personal Data Protection Bill, 2006 has been drafted to provide for protection of personal data and information of an individual collected for a particular purpose by one organization, and to prevent its usage by other organization for commercial or other purposes and entitle the individual to claim compensation or damages due to disclosure of personal data or information of any individual without his consent.

It defines personal data as information or data which relate to a living individual who can be identified from that information or data whether collected by any Government or any private organization or agency.

The Bill intends to protect personal data of individuals and states that 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.

The Bill states the following exemptions to the abovementioned prohibition on processing of data without the consent of the person concerned:

- The prevention or detection of crime;
- The prosecution of offenders; and
- The assessment or collection of any tax or duty.

The bill imposes sanctions if the personal data of any person collected by an organization whether government or private, is disclosed to any other organization for the purposes of direct marketing or for any commercial gain and states every person whose personal data or details have been processed or disclosed for direct marketing or for any commercial gain without consent shall be entitled to compensation for damages in such manner as may be prescribed. However the personal data of any person may be disclosed to charity and voluntary organizations after obtaining prior consent of the person.

For the implementation of the same the appropriate Government shall, by notification in the Official Gazette, appoint as many 'Data Controllers' [a familiar term but with an entirely different meaning] as may be necessary (not be more than three Data Controllers in a State or a Union Territory) and number of officers and staff as may be necessary efficient functioning of the Data Controller for over viewing the complaints relating to processing and disclosing of personal data and claim for compensation. The appropriate Government shall, after due appropriation made in this behalf, provide such sums of money as it may think fit for being utilized for the purpose of this Act.

The bill imposes certain duties on every organization, whether Government or private, engaged in the commercial transaction and collection of personal data of persons shall: —

- Report to the Data Controller the type of personal data and information being collected by them and the purpose for which it is being or proposed to be used;
- Take adequate measures to maintain confidentiality and security in the handling of personal data and information; and
- Collect only such information that is essential for completion of any transaction with the individual.

The contravention or attempts to contravene or abets the contravention of the provisions of this Bill shall be punishable with imprisonment for a term, which may extend to three years or with fine, which may extend upto ten lakh rupees or with both and this can be in addition to the compensation for damages claimed for disclosure of personal data. Where such contravention is made by a company, every person who, at the time the contravention was committed, was in charge of, and was responsible to, the company for the conduct of business of the company, shall be guilty of the contravention and shall be liable to be proceeded against and punished accordingly however if such a person proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention, he shall not be held liable for the same.

All offences under this Bill shall be tried summarily in the manner prescribed for summary trial under the Code of Criminal Procedure, 1973.

In order to give effect to the provisions of this Act, the Central Government may, by order published in the Official Gazette within a period of three years from the date of commencement of this Act, make such provisions not inconsistent with the provisions of this Act, as appear to it to be necessary or expedient for removing the difficulty.

An exhaustive study of the present scenario in relation to privacy and data protection, reveals that currently the industry is concentrating mainly on trying to satisfy their clients through contractual agreements with regards to data protection and privacy, however this approach is only a peace meal effort in comforting the overall challenge. A more appropriate and long-term approach, which is also the need of the hour especially after the recent data thefts cases, is to build a '*culture of privacy and data protection'*. This could not only act as a means of reducing the concerns and the risks associated with process of client confidential and personal data, but also offers through the adoption of a proper and effective education policy, save the reputation of a critical industry, in the fastest growing economy of the world. In this regard the steps taken recently by some of the banks and IT industry majors in partnership with the authors firm, with regard to introducing training modules on privacy law, data processing and handling procedures, can be taken into consideration to develop a self-regulatory industry standard.

Similar recommendations on formally introducing industry wide, Privacy and data protection training as part of the induction training would go a long way in inculcating proper data handling and data usage values as maintaining secrecy of personal information, adopt correct data processing patterns and seek advice and help from qualified expert attorney in case of a data breach. Much work needs to be done specially in terms of making the users aware of the issues involved, communicating and educating them regarding the proper usage and adoption of the proper handling procedures so that the society at large can reap the benefits a new revolution.

<Rodney D. Ryder> is partner with Preconcept. He is an advisor to the Ministry of Communications and Information Technology, the Technology Law Committee of the Indian Parliament and the Data Security Council of India [DSCI]. He has authored publications such as Intellectual Property and the Internet; Guide to Cyber Laws: The Information Technology Act, 2000; Data Protection and the Internet; Right to Information – Law Policy and Practice. Mr. Ryder has been nominated as a 'Leading Lawyer' in his areas of practice by Asia Law, Who'sWhoLegal amongst other International publications. He also conducts education and training programmes on Corporate Due Diligence and Audits, Information Technology and Intellectual Property. He is the Founder of Scriboard Knowledge Solutions and also part of the Founding Team of Law Wire and its Editorial Board. He can be reached at rodney@scriboard.com

<Ashwin Madhavan> is an IVth Year law student of Gujarat National Law University. He has written an article on Outsourcing Legal Services in India which has been published in the Indian Journal of International Law. He is part of the Founding Team at Scriboard and Law Wire. He has written several articles which have been published in various national and international journals. He has also co authored an article with Mr Ryder on Protecting IP in India which has been published in the Halsbury's Law Monthly [published by Lexis Nexis Butterworths Wadhwa Nagpur India]. He has also authored an article on Domain Names and Cybersquatting which has been published in India Law Journal. He can be reached at ashwin@scriboard.com