LEGAL ALERT

An Indian Outline on Database Protection

Contributed by: Dipak Rao and Nishi Shabana

One Business Processing Outsourcing company of India was in the eye of storm when one of its employees sold confidential financial information relating to customers of few British banks to an undercover reporter from the British tabloid 'The Sun'. The incident sparked off a debate among the offshore industry circles, media and the legal world for the need of specific legislation for the protection for personal data in India which is absent currently. With the growing dependence on technology and e-commerce the problem relating to same is growing by leaps and bounds. India being one of the preferred destinations for outsourcing industry requires well formulated regulations for dealing with such cybercrimes. Data in the current scenario have become largest corporate asset for the industry. Due to the importance of data in this new era, its security has become a major issue with industry.

The primary legislation dealing with cyber security in Indian is the Information Technology Act, 2000 ("IT Act"). The nodal agency dealing with Cyber Security in India is Indian Computer Emergency Response Team [CERT-In]. This is the national agency for responding to computer security incidents as and when they require. However, since there isn't any Data Protection Authority in India, the system of courts is the main vector by which individuals can obtain a remedy. There are a host of laws which can protect and enforce the private and property rights of a person namely the law of the land – Constitution of India, Indian Contract Act, 1872; Copyright Act, 1957; Information Technology Act, 2000; Indian Penal Code, 1860; Specific Relief Act; Indian Telegraph Act, 1885; The Credit Information Companies (Regulation) Act, 2005; Public Financial Institutions Act of 1993.

A Brief Overview of Current Legislations

Before engaging in the core analysis of regulation provided by the subject Act, it would be relevant to evaluate the perception of privacy in India. While 89% of US subjects disagree with the statement that "Data security and privacy are not really a problem because I have nothing to hide", only 21% of Indian disagree.

Constitution of India

One of the basic features of the Constitution of India is its supremacy and the overriding effect it renders on all the rest of the statutes. It's another significant feature is that it guarantees civil liberties to the citizens of India in the form of certain rights which include Right to Privacy. Now, the horizon of right to life in our Constitution encompasses two organs, i.e., right to livelihood and right to personal liberty. Property in form of commercial database is covered in the means of livelihood and the same cannot be taken away except due process of law. In case of its violation by any person, compensation can be duly claimed. Besides, under the constitution one can also enforce his right on his property in case of any conflict or dispute. It's been stated that no person can be deprived of his/her property.

The State is not only under an obligation to respect the fundamental rights of the citizens, but also equally under an obligation to ensure conditions under which the right can be meaningfully and effectively be enjoyed by one and all. Thus, data protection rights may be pitted

against freedom of information in a given case and the facts and circumstances of each case will govern the position.

The continuous demand on the part of multinational corporations (MNCs) has made it essential to assure that a proper mechanism for protection of their valuable data exists in India. An indifferent attitude towards this demand may cost valuable foreign exchange and numerous job opportunities.

Indian Penal Code, 1860

The Indian Penal Code, 1860 (IPC) can be used as an effective means to prevent data theft. The IPC gives an inclusive definition of the term 'movable property' which includes all the corporal properties. The word 'include' indicates that information stored in the form of data on papers and in the computer can be conveniently and safely regarded as movable property, since it is capable of moving from one place to another. Thus, there is nothing that excludes the data property from the definition of property under IPC. Therefore, offences such as misappropriation of property, theft or criminal breach of trust attract imprisonment and fine under IPC.

Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act) was enacted primarily for facilitating the development of a secure regulatory environment for electronic commerce by providing a legal infrastructure governing electronic contracting, security and integrity of electronic transactions and to showcase India's growing IT prowess and the role of Government in safeguarding and promoting IT sector. Though, it is pertinent to note that the subject Act do not supply us with any concept of 'personal data'. It is defined as a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed or has been processed in a computer system or computer network, and may be in any form or stored in the memory of the computer.

Some of the sections of this Act are viewed in India as the 'backbone' of the data protection despite of which it runs short of appropriate remedies sometimes. Any misappropriation of the computer network, system, resources, database is termed as cyber contraventions and the person indulging in the same is heavily penalized. It facilitates us with an exoteric or long arm jurisdiction, meaning thereby, if any person contravenes the data and privacy rights of an individual by means of computer, computer system or computer network locates in India, he would be liable under provisions of the Act. Any nature of unauthorized use which leads to damage, tampering with computer source documents, hacking with computer system and access to electronic record, register, book, correspondence, information, and document without consent of the person concerned is liable to punished under the Act. Hence, it further ropes in the network service provider for violating the privacy right of third party. But all these offences are subjected to one exception, that of, if the person charged proves that the contravention took place without his knowledge or that he exercised all due diligence to prevent such contravention.

Section 43 A of the Information technology Act explicitly provides that "Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to

pay damages by way of compensation to the person so affected"

Further Section 72 A provides that "Punishment for disclosure of information in breach of lawful contract. -Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both"

It is apparent that both the sections mentioned above are not dealing with data security directly. Prior to 2011 the situation of the laws related to data protection was very vague and ambiguous, as there was no law which dealt directly and explicitly with this issue.

Later in 2011, new set of rules named the "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011" came into picture. These rules have provisions for three groups- Body Incorporates, Information Providers (Data Subjects) and the Government. The key features of the Rules are as follows-

- *Rule 3* mentions the list of things which will be treated as "sensitive personal data "under the Act. It includes passwords, credit or debits card information, medical and biometric records etc.

- *Rule 4* casts a duty upon the Body Corporate to provide a privacy policy for dealing with personal information and sensitive data and it also requires that the policy should be available on the website of the body corporate. The policy shall include all the necessary details for e.g. type of personal data collected, statements of practices, purpose of collection, provisions related to disclosure and security practices etc.

- *Rule 5* states various provisions which govern the collection of information by the Body Corporate. The main clauses are as follows

    i. Body Corporate shall not collect sensitive personal data without obtaining consent in writing or by fax or e-mail form the provider regarding the purpose for which the data is being collected.

    ii. Any personal information or sensitive data shall not be collected unless and until it is for a lawful purpose and the collection is necessary for the fulfillment of that particular purpose.

    iii. The provider shall be made aware of the facts as to the information collected, its purpose, its recipients and the agencies that are collecting and retaining the information.

    iv. The information collected shall be used only for the purpose for which it is collected and shall not be retained for a period longer than which is required.

    v. However, the Body Incorporate shall not be responsible for the authenticity and reliability of any

personal data or sensitive information.

vi. The provider shall be given an option to opt out of providing such information along with an option to withdraw his consent to the collection at any later stage as well.

vii. The Body Corporate shall keep the data secured and it shall designate a grievance redressing body for any discrepancies arising in future.

- Rule 6 requires that the Body Corporate shall seek the consent of the concerned provider before disclosing the sensitive data to a third party, unless such disclosure was agreed by the parties through any contract. However, such information can be shared without any prior consent with government agencies mandated under law or any other third party by an order under the law, who shall be under a duty not to disclose it further.

- Rule 8 clarifies that a body corporate shall be considered to have complied with reasonable security practices if they have implemented and documented the standards of these security practices. Rule 8 (2) mentions the name of one such ISO security standard for data protection. However, any person or agency that are following any code of best practice other than that mentioned in rule 8(2) shall get their code duly approved by the Central Government. Body Corporate and agencies who have implemented either ISO standards or any other standard duly approved by the central government shall be considered to have implemented security measures provided that such codes have been audited on a yearly basis by independent auditors approved by the government.

Therefore, we can say that the new law being in place now would tighten its grip on mishandling of data and any crime related to same.

Copyright Act, 1957

Under the Copyright Act, 'Computer database' is included in the definition of 'literary work'. Therefore, copying a computer database, or copying and disturbing a database amounts to infringement of copyright for which civil and criminal remedies can be initiated.

However, to obtain copyright protection for a compilation, it must exhibit some creativity of originality in selection or arrangement of contents of the compilation. There has been no clear pronouncement by the Indian courts on the concept of originality and each case is decided on the basis of its peculiar, 'facts and circumstances.' Nonetheless, the Indian courts seem to uphold the 'sweat of the brow' theory or the skill, labor and judgment test in deciding copyright infringement of databases, which states that creativity is a concept that is alien to the requirements of 'originality'. A database is 'original' merely by reason of the fact that the author has invested time, money, labor or skill in its creation. There has been renunciation of the 'sweat of the brow' doctrine (Eastern Book company v Desai, AIR 2001 (Delhi) 185) which is a result of some inherent defects in its applicability in the context of copyright law and it is only a matter of time before the Indian Courts realize the same and apply 'modicum of creativity' doctrine which requires a minimum degree of creativity.

Indian Contract Act, 1872

Further, business entities seek data protection under contract law and common law, by incorporating confidentiality and data protection clauses in contracts. According to this Act, when a party commits a breach of contract, the other party is entitled to receive compensation for any loss or damage caused to it, in exceptional cases, the court may direct the "specific performance" of the contract against the party in default. Hence, 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 fulfill the requirements of overseas customer(s) national legislations. In the event of a breach the contract should provide for remedies available. Moreover, increasingly, outsourcing/BPO contracts are also incorporating clauses(s) on alternative dispute resolution like international arbitration, mediation and conciliation for dispute resolution. They are also submitting themselves to the exclusive jurisdiction of customer's national courts and forums. Further, most of the BPOs follow European Union's data protection provisions on their agreements after learning it the hard way.

Considering the current scenario of India, it is left open for debate whether the quantity of legislations will further the objective of obtaining data security or the quality of legislations will clarify the doubts arising every now and then. Proposing amendments and modifying the law with progressive time will definitely lead to the eradication of ambiguity in a statute but the burning need of the hour should be to consolidate the remedies available. Adequate protection is a relative term and floats with the facts and circumstances of the case. In such a prevailing global environment it is obligatory for India to enact a law clearly stating the protections enjoyed by databases. TRIPS Agreement, the Copyright Act, 1957 and the IT Act provide sufficient safeguards for preventing violations of electronic and paper bases databases of MNCs. The brightest and the positive aspect of this situation is that even non-data items are also protected, both under the TRIPS Agreement and the Copyright Act, 1957.

In the same breath, it is also pertinent to note that the 'sweat of the brow' doctrine has been proven to be jurisprudentially incorrect in its application to copyright law and it is time that the Indian Courts took note of its innate defects. The 'modicum of creativity' rule lends more value to a copyright and is well aligned in its analytical underpinnings. Further, another issue that needs to be dealt with is the protection of non-creative/non-original databases. Without additional protection for non-creative databases, Indian economy will suffer. Only clearly defined copyright and database rights will cultivate a legal environment from which the investment necessary to construct and disseminate a variety of on-line and off-line database services so vital to the development of electronic commerce may flow. A limited right on data needs to be created in favor of database owners. This right must, however, be only an exception to the general rule of free access to data by the public and not vice-versa. Such an approach would strike a correct balance between the rights of a database owner and the general right of the pubic to access public domain information.

Dipak Rao
Senior Partner
dipak@singhania.in

Nishi Shabana
Principal Associate
nishi@singhania.in