DATA PROTECTION - EMERGING TRENDS AND ITS HUMAN RIGHTS PERSPECTIVES

Prof (Dr.) V.L. Mony, Dean, School of Law

Data protection is a significant area, which is focussed in modern times. The significance of the data largely increased largely due to its use and advancement of technology and the purposes for which it can be put. The regulations and protection of the data is largely a matter of human right and liberty. The protection is envisaged in various nations based on their respective rules and regulations. This article analyses the various aspects of data protection and its impact in the society

Key words: Data, Data Privacy, Data Protection, Regulations and Human rights aspects.

Introduction

Data are characteristics or information, usually numerical, that are collected through observation. In a more technical sense, data is a set of values of qualitative or quantitative variables about one or more persons or objects, while a datum (singular of data) is a single value of a single variable.

The data relates to various aspects and might relate to scientific data, social data, professional data, and research data and so on. The data are also being collected by Satellites, and other scientific equipments for the purpose of Research. Human ingenuity is such that such data are processed analysed and concluded for various findings.

The importance of data protection comes, when it relates to the confidential nature which is collected by agencies and has social interest. Data relating to the individuals are private since they relate to protection of individual aspects of humans and is subject to human rights protection. The data is used by different agencies for their advantageous of inventions, marketing, analysis, for scientific purposes and a host of other uses based on the purposes for which they are used.

In India, the private data is protected and it is a personal right affecting the liberty of a person protected under Indian Constitution. This relates to the element or liberty and privacy protected under the Constitution as an individual right.

The data is protected under different ways globally. In Europe, there is European Code for the protection of Data and Privacy. In USA, the protection is considered as a part of Civil Right granted to a citizen. Any Violation relating to the above protection is a violation of human right.

In India, the data protection is a matter of individual liberty and can be challenged as a violation of Fundamental Right.

In the Covid days, data protection has more relevance. Government of Kerala entrusted an agency styled Springler, during the year 2020, which is incorporated in Europe for the purposes

of compilation, analysis and storage of data of patients who were affected with Covid 19. The agreement was such that they were giving a software application, which can process the data and make analysis as to its impact, how it can go ahead in pandemic spreading and the total facilities and other requirements for the treatment of the patients. The understanding was that data will be stored by the Company in USA in their Server and for any disputes law in USA shall apply to them.

The matter was brought before the High Court of Kerala, as a writ challenging the jurisdiction of US Courts, and for expressing the lack of confidentiality in protecting the personal data of t he patients and citizens of India. The High Court was analysing whether there is privacy of data? And made an Obiter, stating that the data relating to the patients in India is a matter of privacy and need to be protected. Based on the above, Government of Kerala severed its services with the Company Springler and entrusted the work to the CDAT owned by Kerala, but using the application of Springler. It was also provided that the data shall be served only in the servers hired by CDAT.

Justice K S Puttaswamy (Retd.) & Anr. vs. Union of India and Ors., The constitution bench of the Hon'ble Supreme Court has held Right to Privacy as a fundamental right, subject to certain reasonable restrictions.

The relevant protection for data in India is available only in Information Technology Act, 2000 and under Indian Contract Act, 1857. No specific enactment is existing to protect the Data. According to Information Technology Act. 2000, if anyone is using personal data with a gain and making loss for another, such activity can be punished under the Act.

The Government has notified the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011. The Rules only deals with protection of "Sensitive personal data or information of a person", which includes such personal information which consists of information relating to:-

- Passwords;
- Financial information such as bank account or credit card or debit card or other payment instrument details;
- Physical, physiological and mental health condition;
- Sexual orientation;
- Medical records and history;
- Biometric information.

The rules provide the reasonable security practices and procedures, which the body corporate or any person who on behalf of body corporate collects, receives, possess, store, deals or handle information is required to follow while dealing with "Personal sensitive data or information". In case of any breach, the body corporate or any other person acting on behalf of body corporate, the body corporate may be held liable to pay damages to the person so affected.

The disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years and fine extending to Rs 5,00,000 (approx. US$ 8,000).

Under 69 of the Act, which is an exception to the general rule of maintenance of privacy and secrecy of the information, provides that where the Government is satisfied that it is necessary in the interest of:

- the sovereignty or integrity of India,
- defence of India,
- security of the State,
- friendly relations with foreign States or
- public order or
- for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, if there is any violations.

It may by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource. This section empowers the Government to intercept, monitor or decrypt any information including information of personal nature in any computer resource.

Under section 69 of the IT Act, any person, authorised by the Government or any of its officer specially authorised by the Government, if satisfied that it is necessary or expedient so to do in the interest of sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, for reasons to be recorded in writing, by order, can direct any agency of the Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource. The scope of section 69 of the IT Act includes both interception and monitoring along with decryption for the purpose of investigation of cyber-crimes. The Government has also notified the Information Technology (Procedures and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, under the above section.

The Government has also notified the Information Technology (Procedures and Safeguards for Blocking for Access of Information) Rules, 2009, under section 69A of the IT Act, which deals with the blocking of websites. The Government has blocked the access of various websites.

Penalty for Damage to Computer, Computer Systems, etc. under the IT Act

Section 43 of the IT Act, imposes a penalty without prescribing any upper limit, doing any of the following acts:

- accesses or secures access to such computer, computer system or computer network;

- 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;
- introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
- 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;
- disrupts or causes disruption of any computer, computer system or computer network;
- 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;
- 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 to the person so affected.
- destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
- steal, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage.

Tampering with Computer Source Documents as provided for under the IT Act, 2000

Section 65 of the IT Act lays down that whoever knowingly or intentionally conceals, destroys, or alters 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 Rs 2,00,000 (approx. US$3,000), or with both.

Computer related offences

Section 66 provides that if any person, dishonestly or fraudulently does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to Rs 5,00,000 (approx. US$ 8,000)) or with both.

Penalty for Breach of Confidentiality and Privacy

Section 72 of the IT Act provides for penalty for breach of confidentiality and privacy. The Section provides that any person who, in pursuance of any of the powers conferred under the IT 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 material to any other person, shall be punishable with imprisonment for a term which may extend to two years, or with fine which may extend to Rs 1,00,000, (approx. US$ 3,000) or with both.

Amendments as introduced by the IT Amendment Act, 2008

Section 10A was inserted in the IT Act which deals with the validity of contracts formed through electronic means which lays down that contracts formed through electronic means "shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose".

The following important sections have been substituted and inserted by the IT Amendment Act, 2008:

1. Section 43A – Compensation for failure to protect data.

2. Section 66 – Computer Related Offences

3. Section 66A – Punishment for sending offensive messages through communication service, etc. (This provision had been struck down by the Hon'ble Supreme Court as unconstitutional on 24th March 2015 in Shreya Singhal vs. Union of India)

4. Section 66B – Punishment for dishonestly receiving stolen computer resource or communication device.

5. Section 66C – Punishment for identity theft.

6. Section 66D – Punishment for cheating by personation by using computer resource.

7. Section 66E – Punishment for violation for privacy.

8. Section 66F – Punishment for cyber terrorism.

9. Section 67 – Punishment for publishing or transmitting obscene material in electronic form.

10. Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act, etc, in electronic form.

11. Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc, in electronic form.

12. Section 67C – Preservation and Retention of information by intermediaries.

13. Section 69 – Powers to issue directions for interception or monitoring or decryption of any information through any computer resource.

14. Section 69A – Power to issue directions for blocking for public access of any information through any computer resource.

15. Section 69B – Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security.

16. Section 72A – Punishment for disclosure of information in breach of lawful contract.

17. Section 79 – Exemption from liability of intermediary in certain cases.

18. Section 84A –Modes or methods for encryption.

19. Section 84B –Punishment for abetment of offences.

20. Section 84C –Punishment for attempt to commit offences.

Thus, the data protection is an emerging area of law and needs more amendments ahead for the protection of data. It is considered as a private right of every citizen, under Article 19 and 21 of the Indian Constitution, which can be relooked by the Courts of Laws in India for proper protection and enforcement. It is generally, provided that the law need more stricter enactment and enforcement provisions.

Article 19 and 21 of the Indian Constitution

Part III of the Constitution of India

Centre for developed and Advanced Technology- CDAT

Sec 43 A of the IT Act, 2000

Under section 72A of the (Indian) Information Technology Act, 2000,