Privacy and Data Protection in India

Privacy and Data Protection in India

By Dr. Shiv Shankar Singh*

Cite as: (2012) PL February S-2 Introduction

The right to privacy is a multidimensional concept. In modern society right to privacy has been recognised both in the eye of the law and in common parlance. Article 21 protects the right to privacy and promotes the dignity of the individual. In recent years there has been a growing fear about the large amount of information about individuals held in computer files. The right to privacy refers to the specific right of an individual to control the collection, use and disclosure of personal information. Personal information could be in the form of personal interests, habits and activities, family records, educational records, communications (including mail and telephone) records, medical records and financial records, to name a few. An individual could easily be harmed by the existence of computerised data about him/her which is inaccurate or misleading and which could be transferred to an unauthorised third party at high speed and very little cost. This growth in the use of personal data has many benefits but it could also lead to problems.

Further, the convergence of technologies has spawned a different set of issues concerning privacy rights and data protection. Innovative technologies make personal data easily accessible and communicable. There is an inherent conflict between right to privacy and data protection. Data protection should primarily reconcile these conflicting interests to information. But, the data of individuals and organisations should be protected in such a manner that their privacy rights are not compromised. This article aims to initiate a serious debate on right to privacy and data protection and to deal with the privacy and data protection issue in Indian perspective keeping in view the ongoing multidimensional development.

Concept of privacy The terms privacy and right to privacy cannot be easily conceptualised. It has been taken in different ways in different situations. Warren and Brandeis1 has very eloquently explained that â€œonce a civilization has made distinction between the â€˜outerâ€™ and â€˜innerâ€™ man, between the life of the soul and the life of the body â€¦ the idea of a sphere in which man may become and remain himself.â€• In modern society privacy has been recognised both in the eye of the law and in common parlance. But it varies in different legal systems as they emphasise different aspects. Privacy is a neutral relationship between persons or groups or between groups and persons. Privacy is a value, a cultural state or condition directed towards individual on collective self-realisation varying from society to society.

The Indian Constitution in Article 19(1)(a) provides the right to freedom of speech and expression, which implies that a person is free to express his will about certain things. A person has the freedom of life and personal liberty, which can be taken only by procedure established by law under Article 21. These provisions improvably provide right to privacy to individuals and/or groups of persons. The privacy of a person is further secured from unreasonable arrests under Article 22 and under Article 25 the person is entitled to express his wishes regarding professing and propagating any religion. The privacy of property is also secured unless the law so authorises i.e. a person cannot be deprived of his property unlawfully under Article 300-A. The personal liberty in Article 21 is of the widest amplitude and it covers a variety of rights which constitute the personal liberty2, secrecy3, autonomy4, human dignity5, human right6, self-evaluation7, limited and protected communication8, limiting exposure9 of man and some of them have been raised to the status of fundamental right viz. life and personal liberty, right to move freely, freedom of speech and expression, individual and societal right and given protection under Article 19. Article 21 as such protects the right to privacy and promotes the dignity of the individual. Privacy relates to ability to control the dissemination and use of oneâ€™s personal information.

Judicial activism: The right to privacy Judicial activism has brought the right to privacy within the realm of fundamental rights by interpreting Articles 19 and 21. The judiciary has recognised right to privacy as a necessary ingredient of the right to life and personal liberty. The Supreme Court of India has interpreted the right to life to mean right to dignified life in Kharak Singh case10, especially the minority judgment of Subba Rao, J. In Gobind v. State of M.P.11, Mathew J., delivering the majority judgment asserted that the right to privacy was itself a fundamental right, but subject to some restrictions on the basis of compelling public interest. Privacy as such interpreted by our Apex Court in its various judgments means different things to different people. Privacy is a desire to be left alone, the desire to be paid for oneâ€™s data and ability to act freely.

Right to privacy relating to a personâ€™s correspondence has become a debating issue due to the technological developments. In R.M. Malkani v. State of Maharashtra12, the Supreme Court observed that, â€œthe Court will not tolerate safeguards for the protection of the citizen to be imperilled by permitting the police to proceed by unlawful or irregular methodsâ€•. Telephone tapping is an invasion of right to privacy and freedom of speech and expression and also Government cannot impose prior restraint on publication of defamatory materials against its officials and if it does so, it would be violative of Article 21 and Article 19(1)(a) of the Constitution. In Peopleâ€™s Union for Civil Liberties v. Union of India13 the Supreme Court held that right to hold a telephonic conversation in the privacy of oneâ€™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. In State of Maharashtra v. Bharat Shanti Lai Shah14, the

Supreme Court said that interception of conversation though constitutes an invasion of an individualâ€™s right to privacy but it can be curtailed in accordance with procedure validly established by law.

In R. Rajagopal v. State of T.N.15, 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); it would be quite difficult for courts to add privacy as one more ground for imposing reasonable restriction.

In Destruction of Public & Private Properties v. State of A.P.16, the Supreme Court said that 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 hammer the individual privacy. There is no guideline to handle this issue. Privacy frame will provide solution to solve this problem.

In Peopleâ€™s Union for Civil Liberties (PUCL) v. Union of India17, the Supreme Court observed that by calling upon contesting candidate to disclose the assets and liabilities of his/her spouse the fundamental right to information of a voter or citizen is thereby promoted. When there is a competition between the right to privacy of an individual and the right to information of the citizens, the former right has to be subordinated to the latter right as it serves larger public interest. The question arises as to what extent a voter has a right to know about a candidateâ€™s privacy. The voterâ€™s right to know abou a candidateâ€™s privacy can be protected and flourished by removing the drawbacks of laws relating to voterâ€™s right to information. Privacy means the right to control the communication of personally identifiable information about any person. It requires a balancing attitude; a balancing interest.

In Mr. â€˜Xâ€™ v. Hospital â€˜Zâ€™18 the Supreme Court held that 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 personâ€™s right to be let alone with another personâ€™s right to be informed. In another case the Apex Court said that19 the hospital or doctor was open to reveal such information to persons related to the girl whom he intended to marry and she had a right to know about the HIV-positive status of the appellant. The Court also held that the appellantâ€™s right was not affected in any manner in revealing his HIV-positive status to the relatives of his fiancÃ©e. In matrimonial cases the petitioner would always insist on medical examination. In Selvi v. State of Karnataka20, 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. In Bhabani Prasad Jena v. Orissa State Commission for Women21, the Supreme Court said that if DNA test is eminently needed to reach the truth, the court must exercise the discretion of medical examination of a person.

In Sharda v. Dharmpal22 the Supreme Court said 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 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.

Privacy and data protection Privacy and data protection require that information about individuals should not be automatically made available to other individuals and organisations. Each person must be able to exercise a substantial degree of control over that data and its use. Data protection is legal safeguard to prevent misuse of information about individual person on a medium including computers. It is adoption of administrative, technical, or physical deterrents to safeguard personal data. Privacy is closely connected to data protection. An individualâ€™s data like his name, address, telephone numbers, profession, family, choices, etc. are often available at various places like schools, colleges, banks, directories, surveys and on various websites. Passing of such information to interested parties can lead to intrusion in privacy like incessant marketing calls. The main principles on privacy and data protection enumerated under the Information Technology Act, 2000 are defining data, civil and criminal liability in case of breach of data protection and violation of confidentiality and privacy.

Concept of data protection The Information Technology Act which came into force in the year 2000 and is the only Act to date which covers the key issues of data protection, albeit not every matter. In fact, the Information Technology Act, 2000 enacted by the Indian Parliament is the first legislation, which contains provisions on data protection.

According to Section 2(1)(o) of the Act,
2. (1)(o) â€˜dataâ€™ means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer;

The IT Act does not provide for any definition of personal data and the definition of â€œdataâ€• would be more relevant in the field of cyber crime. Further, the IT Act defines certain key terms with respect to data protection, like access, computer, computer network, computer resource, computer system, computer database, data, electronic form, electronic record, information, intermediary, secure system and security procedure. The idea behind the aforesaid section is that the person who has secured access to any such information shall not take unfair advantage of it by disclosing it to the third party without obtaining the consent of the party concerned. â€œThirdÓparty informationâ€• is defined to mean â€œany informati dealt with by an intermediary in his capacity as an intermediaryâ€•, and it may be arguable that this limitation also applies to â€œdataâ€• and â€œcommunicationâ€•. Section 79 provides that an intermediary shall not be liable for any third-party informati or communication link made available or hosted by him except in the conditions provided in sub-section (2) and (3) thereof.

The IT Act does not provide any definition of personal data. Furthermore, the definition of â€œdataâ€• would be more relevant i the field of cyber crime. Data protection consists of a technical framework of security measures designed to guarantee that data are handled in such a manner as to ensure that they are safe from unforeseen, unintended, unwanted or malevolent use.

Civil liability and data protection The Information Technology Act, 2000 provides for civil liability in case of computer database theft, computer trespass, unauthorised digital copying, downloading and extraction of data, privacy violation, etc. Furthermore Section 43 provides for penalty for a wide range of cyber contraventions such as: (a) related to unauthorised access to computer, computer system, computer network or resources; (b) unauthorised digital copying, downloading and extraction of data, computer database or information, theft of data held or stored in any media; (c) introduction of any computer contaminant or computer virus into any computer system or computer network; (d) unauthorised transmission of data or programme residing within a computer, computer system or computer network; (e) computer data/database disruption, spamming, etc.; (f) denial of service attacks, data theft, fraud, forgery, etc.; (g) unauthorised access to computer data/computer databases; (h) instances of data theft (passwords, login IDs), etc.; (i) destroys, deletes or alters any information residing in a computer resource, etc. and (j) steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage.

Explanation (ii) of Section 43 provisions definition of computer database as,
43. (ii) a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
Section 43ÓA provides for â€œcompensation for failure to protect dataâ€•, it provides:
43-A. Compensation for failure to protect data.â€”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.

There is no limitation imposed on the compensation that can be awarded. Section 43ÓA which provides for civil action for security breaches is based on the concept of â€œsensitive personal informationâ€•. Other than that, there is no special protection in Indian law for sensitive personal information. Section 43ÓA provides for compensation to an aggrieved person whose personal data including sensitive personal data may be compromised by a company, during the time it was under processing with the company, for failure to protect such data whether because of negligence in implementing or maintaining reasonable security practices. This provision, therefore, provides a right of compensation against any one other than the person in charge of the computer facilities concerned, effectively giving a person a right not to have their personal information disclosed to third parties, or damaged or changed by those third parties. The section is equally able to be used by data controllers or the subjects of personal information against third parties. It is only that they will be â€œaffectedâ€• in different ways which justify compensation. It also provides that accessing data in an unauthorised way is a civil liability.

Criminal liability and data protection The Information Technology Act, 2000 provides for criminal liability in case of computer database theft, privacy violation, etc. The Information Technology (Amendment) Act, 2008 makes wide ranging amendments in Chapter XI enfacing Sections 65 to 74 which cover a wide range of cyber offences, including offences related to unauthorised tampering with computer source documents, dishonestly or fraudulently doing any act referred to in Section 43, sending offensive messages through communication service, etc., dishonestly receiving stolen computer resource or communication device, identity theft, cheating by personation by using computer resource, violation of privacy, cyber terrorism, transmitting obscene material in electronic form, transmitting of material containing sexually explicit act, etc. in electronic form, transmitting of material depicting children in sexually explicit act, etc. in electronic form, any intermediary intentionally or knowingly contravening the provisions of sub-section (1) of Section 43, any person intentionally or knowingly failing to comply with any order of controller, interception or monitoring or decryption of any information through any computer resource, blocking for public access of any information through any computer resource, intermediary contravening the provisions of sub-section (2) of Section 69ÓB by refusing to provide technical assistance to the agency authorised by the Central Government to monitor and collect traffic data or information through any computer for cyber security, securing access or attempting to secure access to any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, any misrepresentation to or suppressing any material

fact from the Controller or the Certifying Authority, breach of confidentiality and privacy, disclosure of information in breach of lawful contract, publishing electronic signature certificate false in certain particulars and electronic signature certificate for any fraudulent or unlawful purpose.

India does not have specific data protection legislation, other than the IT Act, which may give the authorities sweeping power to monitor and collect traffic data, and possibly other data. The IT Act does not impose data quality obligations in relation to personal information and does not impose obligations on private sector organisations to disclose details of the practices in handling personal information.

Violation of confidentiality and privacy The terms violation of confidentiality and privacy are described under the IT Act. Section 66-E very eloquently explains violation of privacy as â€œwhoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person.â€• Section 66-E Explanation (e) has also explained violation of privacy as â€œcircumstances in which a person can have a reasonable expectation thatâ€”(i) he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or (ii) any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.â€•

Section 72 provides for penalty for breach of confidentiality and privacy as meaning â€œany person securing 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.â€• Section 72ÓA also explains the law of privacy and asserts that disclosure of information in breach of lawful contract:
72-A. Punishment for disclosure of information in breach of lawful contract.â€”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 personâ€¦. amounts to breach of privacy and provides for punishment for the same.

Sections 66ÓE, 72 and 72ÓA require the consent of the persons concerned but within limited scope as it would be difficult to consider that it could provide a sufficient level of personal data protection. Indeed, these sections confine themselves to the acts and omissions of those persons who have been conferred powers under the Act. These sections provide for monitoring violation of privacy, breach of confidentiality and privacy, and disclosure of information in breach of lawful contract. Breach of confidentiality and privacy is aimed at public and private authorities, which have been granted power under the Act. In District Registrar and Collector v. Canara Bank23, the Supreme Court said 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.

Conclusion Privacy is a basic human right and computer systems contain large amount of data that may be sensitive. Chapters IX and XI of the Information Technology Act define liabilities for violation of data confidentiality and privacy related to unauthorised access to computer, computer system, computer network or resources, unauthorised alteration, deletion, addition, modification, destruction, duplication or transmission of data, computer database, etc. The data protection may include financial details, health information, business proposals, intellectual property and sensitive data.

However, today we can access any information related to anyone from anywhere at any time but this poses a new threat to private and confidential information. Globalisation has given acceptance to technology in the whole world. As per growing requirement different countries have introduced different legal framework like DPA (Data Protection Act), 1998 UK, ECPA (Electronic Communications Privacy Act of 1986) USA, etc. from time to time. In USA some special privacy laws exist for protecting student education records, childrenâ€™s online privacy, individualâ€™s medical records and private financial information. In both countries self-regulatory efforts are facilitating to define improved privacy surroundings.

The right to privacy is recognised in Indian Constitution but its growth and development is entirely left at the mercy of the judiciary. In todayâ€™s connected world it is very difficult to prevent information to escape into the public domain if someone is determined to put it out without using extremely repressive methods. Data protection and privacy has been dealt with in the Information Technology Act, 2000 but not in an exhaustive manner. The IT Act needs to establish setting of specific standards relating to the methods and purpose of assimilation of right to privacy and personal data. We may conclude by saying that the IT Act is facing the problem of protection of data and a separate legislation is much needed for data protection striking an effective balance between personal liberties and privacy.

*. Assistant Professor of Law, C.M.P Degree College, University of Allahabad, Allahabad, email: ss_singh_2008@yahoo.com.
- Samuel Warren & Louis D. Brandeis, â€œThe Right to Privacyâ€• (1890) 4 no. 5 Harv L Rev 193.
- Kharak Singh v. State of U.P., AIR 1963 SC 1295 : (1963) 2 Cri LJ 329; Gobind v. State of M.P., (1975) 2 SCC 148 : 1975 SCC (Cri) 468.
- Allgeyer v. State of Louisiana, 41 L Ed 832 : 165 US 578 (1896).

- Louis Henkin, â€œPrivacy and Autonomyâ€• (1974) 74 Columbia Law Review 1410.
- Olmstead v. United States, 72 L Ed 944 : 277 US 438, 478 (1927); Maneka Gandhi v. Union of India, (1978) 1 SCC 248.
- Article 12 of the Universal Declaration of Human Rights, 1948 & Article 17 of the International Covenant of Civil and Political Rights, 1966.
- Westin, Alan F., â€œScience, Privacy and Freedomâ€• (1966) 66 Columbia Law Review 1003.
- (1966) 66 Columbia Law Review 1003, 1027.
- (1966) 66 Columbia Law Review 1003, 1040.
- AIR 1963 SC 1295 : (1963) 2 Cri LJ 329.
- (1975) 2 SCC 148 : 1975 SCC (Cri) 468.
- (1973) 1 SCC 471 : 1973 SCC (Cri) 399.
- (1997) 1 SCC 301.
- (2008) 13 SCC 5.
- (1994) 6 SCC 632.
- (2009) 5 SCC 212 : (2009) 2 SCC (Cri) 629 : (2009) 2 SCC (Civ) 451.
- (2003) 4 SCC 399.
- (1998) 8 SCC 296.
- Mr. â€˜Xâ€™ v. Hospital â€˜Zâ€™, (2003) 1 SCC 500.
- (2010) 7 SCC 263 : (2010) 3 SCC (Cri) 1.
- (2010) 8 SCC 633 : (2010) 3 SCC (Cri) 1053 : (2010) 3 SCC (Civ) 501.
- (2003) 4 SCC 493.
- (2005) 1 SCC 496.