Probability of Protection of Data and Basic Principles for Personal Data Protection under National and International Legal Instruments

Vishal Mahalwar
Assistant Professor of Law National Law University Sector- 14, Dwarka New Delhi-110078, India

Abstract

In the present scenario, in the name of "Free flow of information" and "Right to information", privacy of individuals has been encroached. Either government or any private organization, the accountability of both in regard to personal data process has to be established. "Free flow of Information" especially the personal data has to be concern of check. Ironically, India stands far behind the European countries in the context of protection of personal data. Few provisions in regard to data protection have been symbolically incorporated in the Information Technology Act, 2000. Any personal data must be abided by certain principles. Social, cultural and different legal backgrounds are the reasons behind the lack of uniform model personal data protection legislation. As an international instrument, EU Data Protection Directives lay down the certain standards for the protection of personal data. This paper will elucidate protection of data under various law and common principles pertaining to the personal data protection generally adopted by the various countries.

KEY WORDS: Data, Protection of Data, Personal Data, Principles of Personal Data, Constitution, Indian Penal Code, Copy Right Act, Trade Secrets, Right to Information Act, 2005, Data Protection Directives, Trans border Data, Data Quality Principle

Introduction

In the present economic scenario, Knowledge or information plays a very important role in generating wealth. For the protection of corporeal property, numerous specific laws have been enacted. As far as incorporeal property i.e. intellectual property is concerned, Intellectual property laws have been enacted like Patent law, Copyright law etc. Information is an effective tool for creating capital. Though, all efforts have been made for the protection of knowledge or information, enactment of legislations alone does not seem to be sufficient enough. "Data" is such a notion for which no relevant *sui generis* law has been enacted and implemented. A democratic country demands every thing transparent and accountable. In the age of information, information is supposed to be freely available and accessible to all irrespective of territorial boundaries. At the same time, Right to privacy of individual should not be compromised.

Space under Constitution

In the pre constitutional era in India, we had a close door administration wherein no one was supposed to get even important informations pertaining to the administration of various departments. Britishers introduced the Official Secrets Act, 1923. This Act restricted the free flow of official information to the public.[1] The second Administrative Reforms Commission[2] had suggested that the Official Secrets Act (OSA) of 1923 should be repealed, saying it is incongruous with the regime of transparency in a democratic

society.[3] The Constitution of India does not contain a specific right pertaining to the right to information. However, The Supreme Court has held in several decisions that the citizen's right to know accrues from two fundamental rights guaranteed by the Constitution – The right to freedom of speech and expression, guaranteed by Article 19(1) and The right to life, guaranteed by Article 21.[4]Grund norm of the land i.e. The Constitution of India also validates the right to privacy under Art. 21. Though, no direct right to information has been expressed under this Art 21. In fact Supreme Court of India has interpreted the Art 21in several cases and has clearly stated that it embodies right to privacy.[5] Every one has a right to information and be informed. But it doesn't mean it is an exhaustive right. Right to information is also subject to right to privacy. The major issue is right to privacy which should not be encroached upon in the name of free flow of information and right to information. Further, Right to life under Article 21 includes right to livelihood.[6] It means if any one's business depends upon the personal data or information of others, in order to earn his or her livelihood, such data can be prevented from disclosure under Article 21 of the Constitution. Apart from Article 21 and 19, Article 300A also sounds relevant with regard to personal data. Article 300A talks about the property Right whether tangible or intangible property.[7] This Article would be appropriate law for the protection of data property of any individual. Right to property includes right to use the same in accordance with the law. Misappropriation of data property of an individual would be considered as violation of Article 300A. Hence, Constitution of India gives appropriate and adequate protection to the data property of an individual subject to right to privacy.

Probabilities under Indian Penal Code

Protection od Data seems possible under the Indian Penal Code 1860 also. One of the chapters of IPC deals with the provisions regarding the offences related to property. Here, property means movable property which has been defined under Section 22 of IPC. Definition of movable property is inclusive in nature which includes all corporeal property.[8] The probability of inclusion of data property in movable property increases further. Data would be eligible or qualify to get the protection under the Code, if data is in tangible form. Stealing or theft of the data which is not in tangible form shall not come within ambit of the definition of movable property. Unless and until you keeping the data in fixation form like keep the data saved in pen drive or C.D., it can not get the protection under the IPC.

Copy Right Act & Respective International Instruments

As far as protectability of data is concerned under intellectual property laws, Copy Right Act, 1957 provides the protection to databases under the definition of literary work.[9] In order to get the protection under copyright law, subject matter is supposed to be *Original*.[10]It is not easy to establish the Intellectual property Right protection in data, that's why TRIPS provides the protection to the compilation of data rather than data itself.[11] Expressions are copyrightable and protected whereas idea in neither copyrightable nor protected. Similarly, Data can not get the protection under Copyright law. In fact, the way of expression or way of presentation of data would be copyrightable under the Intellectual property laws.[12] Lack of originality in compilation of data would be the matter of denial of protection under the concerned law.[13] According to TRIPS,

compilation of data would be eligible to get protection under copyright since it reflects the intellectual capabilities of selection or arrangement of data employed by the compiler, which is the pre-requisite of copyright.

Protection under Trade Secrets

Data can also be protected under the Trade Secrets with certain limitations because of lack of statutory protection. To get protection under trade secret, data holder has to comply with specific parameters. Firstly, data must be secret. Secondly, Data must have commercial value. Thirdly, Data holder must have taken precaution to prevent disclosure of secret information.[14] Delhi High court has held that list of customers qualifies for protection under trade secret in addition to copyright law.[15]

Right to Information Act, 2005

With a view of accountability, transparency and good governance towards every individual of the society, major step has been taken by the Government by enacting Right to Information Act, 2005. Though, right to information has been given to all citizens, but this right is not exhaustive in nature. Section 8 of the Act provides the list of informations which are exempted from disclosure. [16] Constitutionality of this Act has been derived from Art. 19 of the constitution and Art 19 (2) allows the State to impose reasonable restrictions on the exercise of rights.[17] Right to Information Act sets a fine example of a balance between "free flow of information" and "interest of sovereignty and integrity", "morality" and "right to privacy".

Information Technology Act, 2000

As on today we don't have any specific law for the protection of Data. Split provisions in various statutes are the only law pertaining to the data protection among which Information technology Act is also one of them which carries certain provisions in this regard. For the first time, the term "data" has been defined under the Information Technology Act as under:

> *"Data" means 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, 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*[18]

The Act talks about the civil and criminal liabilities in case of extracting data, damage or causing damage to data without the permission of the owner.

According to *Section 43* of Information Technology Act, 2000,

> *If any person without permission of the owner or any other person who is in charge of a 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;*

> *(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;*
> *He shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected.*

In the absence of permission of owner of the computer, computer system; downloads, copies or extraction of the data from computer, computer system or computer network including information or data held or stored in any removable storage medium, shall make the culprit liable to pay damages by way of compensation. Similarly, damage or cause to damage any data residing in such computer, computer system or computer network is also a ground to get compensation under the provisions of the Act.

Further more, According to Section 43 A of Information Technology Act, 2000,

> *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, not exceeding five crore rupees, to the person so affected.*[19]

This section clearly talks about the body corporate's liability when they possess, deal or handle any sensitive data which is in control of body corporate and due to the negligence in implementing and maintaining reasonable security practice and procedures, wrongful loss or wrongful gain occurs. Iin such circumstances, body corporate shall be liable to pay damages to the person so affected. Plain reading of this section reveals that the nature of the liability under this section is not strict or absolute. In fact, either wrongful loss or wrongful gain has to be proved to get the compensation under this section.

Apart from this section, The Act indirectly emphasizes on the right to confidentiality and privacy in addition to data protection. Section 72 further provides as under;

> *Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuant of any of the powers conferred under this Act, rules or regulations made there under, 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.*

According to this provision, if any person has secured access to any information without the consent of person concerned and discloses the same to another person, shall be punished with imprisonment, fine or both. The Act has given very wider meaning to the term "data" which includes information. From incorporation of word "information" it is apparent that this section also provides the protection to privacy of data holder. Apart from this section, section 72 A prescribes the punishment for disclosure of information in breach of lawful contract.[20] Protection of privacy, secrecy or confidentiality of the information is

not exhaustive in nature. In fact, Government in the interest of the sovereignty or integrity of India, defense 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, 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 transmitted received or stored through any computer resource.[21] Section 69 B also carves out an exception to the section 72, in which central government may authorize any agency of the Government to monitor and collect traffic data or information generated, transmitted, received or stored in any computer resource, in order to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country.

Above mentioned provisions make it abundantly clear that the Act provides certain steps in order to provide the protection to "Data". Simultaneously, right to privacy pertaining to data holder has also been ensured by this Act. Some time, access or downloading the data without owner's permission, even if no wrongful loss or wrongful gain occurs, make the culprit liable to pay damages in the shape of compensation.[22] These provisions provide teeth to the Act and make it more stringent.

International Instruments for Data Protection

Basic idea behind the enactment of the statute pertaining to the data protection is to provide protection from *mal processing* of personal data by the organization whether Government or private players. Data protection Act could be the only possible way to impose obligation on part of organizations which process personal data relating to privacy and data quality. Individual rights can also be granted in relation to their data through such enactment. Ironically, India lacks such a law which is available in the countries who are providing protection to data for the last two decades. India stands far behind the European countries in the context of protection of personal data.

In fact, no Asian countries have international instrument with regard to personal data protection. As far as Europe is concerned, In the year of 1980, Council for the Organization for economic Co-operation and Development [23] adopted non binding *Guidelines governing the protection of privacy and transborder flows of personal data*. For the first time, The meaning of "*personal data*" was elucidated in the guidelines. According to it "Personal data" means any information relating to an identified or identifiable individual. Subsequently, in 1981, "Council of Europe" [24] issued a *Convention on the Protection of individuals with regard to the automatic processing of Personal Data,* (Convention 108 or COE Treaty) which was open for signature. The convention covered all the key principles of data protection which were set out in the OECD Guidelines. In 1995, European Union adopted *The Data Protection Directive*[25] to harmonize and bring Uniformity among the data protection laws through out the Europe. The scope of Directive's protection is widened by giving the new definition to "personal data". According to the Directives, "personal data" shall mean any information relating to an identified or identifiable natural person ("data subject"); and an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;.[26] All the European countries have followed the principles laid down in the above mentioned Guidelines, Convention or Directive.

European countries or Asian countries, in spite of lack of international instrument among Asian countries, both have the common principles which are regarding the data collection, data processing and use of data.

Model Principles of Personal Data Protection & Indian Law

Protection of personal data must be guided by certain principles. Social, cultural and different legal backgrounds are the reasons behind the lack of uniform model personal data protection legislation. In spite of above facts, most of the countries are governed by the common principles which have become indispensable for inclusion in the data protection laws regarding data collection, data processing and use of data without ignoring the right to privacy. Though, In India, no *sui generis* law is there pertaining to personal data protection, still for the personal data protection, Central government of India has framed few Rules which are in consonance with the commonly observed principles in the laws of the world countries.

The Social Justification Principle

The social justification principle indicates about such data collection, data processing and use of data which are socially accepted by public at large. It is difficult to determine the social acceptability and non acceptability of data for collection, process and use. COE treaty talks about the special categories of data which illustrate the social justification principle. According to Article 6, "Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions." All the subject matters mentioned in the Article are socially sensitive that's why restriction has been imposed with certain conditions. EU Directive also prohibits the processing of personal data which reveals the racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.[27]Again, this provision is not exhaustive in nature.[28] In India, In exercise of the powers conferred by clause (ob) of sub-section (2) of section 87 read with section 43A of the Information Technology Act, 2000 (21 of 2000), the Central Government has made the Rules namely Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. In these Rules, the term "sensitive personal data" has been elaborated which includes password[29]; 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[30] information etc. Those information or data which is freely available and accessible in public domain or furnished under Right to information Act, 2005 shall not come within the ambit of the definition of "sensitive personal data".[31] These Rules are regarding the data collection, data processing and use of data which is sensitive personal data. There can not be a uniform exhaustive list of "sensitive personal data" in all the countries. It varies from one state to another state. Those data which are not covered within the definition of "sensitive personal data" in India, may be covered in Muslim dominated countries like Pakistan, Afghanistan etc. Countries like India which has diversity in culture, religion,

political opinions have a big challenge to comply with social justification principle pertaining to the personal data protection.

The Collection Limitation Principle

The collection limitation principle restricts processing of personal data except fairly and lawfully.[32] This principle was propounded for the first time in the OECD Guidelines. According to these guideline, "There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, with the knowledge or consent of the data subject." COE Treaty also advocates the fairly and lawfully obtaining and processing the personal data.[33] At the time of obtaining or collecting the personal data, consent has to be taken from the data subject. Data may be processed only if; data subject has unambiguously given his consent.[34] If data collector obtains the data by trick, then processing would be unfair. Consent supposes to be free consent. The term "consent" has not been elaborated in any Convention or Guidelines. In a reasonably prudent persons understanding, consent is unfair and unlawful if Consent has been taken by fraud, misrepresentation Coercion, undue influence, mistake etc. In India, Body corporate[35] or any person on its behalf shall obtain consent in writing through letter or Fax or email from the provider of the sensitive personal data or information regarding purpose of usage before collection of such information.[36] Precisely, it can be stated that data should be collected and processed without going beyond the law of the land.

The Data Quality Principle

OECD Guidelines of 1980 elucidate the data quality principle. According to Paragraph 8 of the same, Personal data should be relevant to the purpose for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date. Personal data processing shall be adequate, relevant and not excessive in relation to the purposes for which they are stored.[37] In addition to this, Personal data processing shall be accurate and, where necessary, kept up to date.[38]Data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;[39] Data must be accurate and, be kept up to date. Every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.[40]In view of these mentioned provisions and guidelines, it is clear that the main idea behind the quality principle is to keep or collect the relevant data which are required for the purpose. Some where, the obligation of keeping the personal data up dated is on the shoulder of the data collector rather than data subject. In India, the data collector which is a body corporate shall not be responsible for authenticity of personal data or information supplied by the provider of information to such body corporate.[41] The provider of information can make a request to review the information which they had provided is found to be inaccurate or deficient. It shall be corrected or amended.[42]

The Purpose Specification Principle

According to this principle, data collector must inform the data subject, before data collection, about his intention and purpose for which he is collecting the data. The

purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.[43] COE also emphasizes on this principle.[44] The Directive also makes it mandatory that, the controller or his representative must provide the information of the purposes of the processing for which the data are intended[45] According to the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, While collecting information directly from the person concerned, the body corporate or any person on its behalf shall take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of the purpose for which the information is being collected.[46] Further, information collected shall be used for the purpose for which personal data has been collected.[47] Data collector is bound to not to use information otherwise than the purpose for which it has been collected. Almost all the countries, who have the data protection law, apply the purpose specification principle at the time of collection, obtaining and processing of personal data.

The Disclosure Limitation Principle

Article 5 (b) of the COE Treaty clearly states that personal data shall be stored for specified and legitimate purposes and not used in a way incompatible with those purposes. Without the prior permission of data subject or by authority of law, no data is supposed to be disclosed or made available, to any other person.[48] This principle has also been applied in Indian. The Rules provide that without prior permission of provider of information, no sensitive personal data shall be disclosed to the third party except such disclosure has been agreed to in the contract between the body corporate and provider of information, or where the disclosure is necessary for compliance of a legal obligation.[49] Further it says that the information shall be shared, without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences.[50] Obligation has also been imposed on body corporate or any person on its behalf to not to publish the sensitive data.[51] Third party who receives data also must not disclose it further.[52]

The Security Safeguard Principle

According to paragraph 11 of OECD Guidelines, Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data. Once, data has been transferred from data subject then it is an obligation on the part of data collector to take appropriate security measures for the protection of personal data. COE treaty also talks about the security safeguard principle. It says that appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorized destruction or accidental loss as well as against unauthorized access, alteration or dissemination.[53] This principle is strictly indispensable in order to safeguard the right of privacy and right to integrity of any data subject. The Rules enumerate the safeguard principle. According to it, A body corporate or a person on its behalf shall be

considered to have complied with reasonable security practices and procedures, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. In the event of an information security breach, the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies.[54]

The Openness Principle

Openness principle refers to a general policy of openness about developments, practices and policies with respect to personal data.[55] This principle has been adopted in the Rules. According to the Rules, "Such policy shall be published on website of body corporate or any person on its behalf and shall provide for Clear and easily accessible statements of its practices and policies; type of personal or sensitive personal data or information collected under rule 3; purpose of collection and usage of such information; disclosure of information including sensitive personal data or information as provided in rule 6; reasonable security practices and procedures as provided under rule 8."[56] In addition to this, while collecting information directly from the person concerned, the body corporate or any person on its behalf shall take such steps as are, in the circumstances, reasonable to ensure that the person concerned is having the knowledge of the name and address of the agency that is collecting the information; and the agency that will retain the information.[57]

The Time Limitation Principle

The time limitation principle advocates that the personal data shall be preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.[58] The Directive also enumerates that Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.[59] The Rules also do not allow the body corporate or any person on its behalf to retain the sensitive personal data for longer than is required for the purposes.[60]

The Individual Participation & Accountability Principle

OECD Guidelines are the first one to provide these principles. Both the principles are co-related with each other. First principle encompasses the data subject's right to challenge data relating to him. If challenge is successful, he shall have the right to get data erased, rectified, completed or amended. As far as the E U directive is concerned, Article 12 talks about the right of access to data by data subject. This principle encourages the data subject to participate with regard to data collection, data processing and use of data. Accountability principle is equally important to implement the previous principles. OECD Guidelines, Paragraph 14, talks about the accountability principle. This principle makes the data controller accountable. COE Treaty doesn't have any provision in regarding accountability. The Rule also doesn't convey anything

specific pertaining to accountability principle. But according to the Rules, Body corporate shall address any discrepancies and grievances of their provider of the information with respect to processing of information in a time bound manner. For this purpose, the body corporate shall designate a Grievance Officer and publish his name and contact details on its website. The Grievance Officer shall redress the grievances or provider of information expeditiously but within one month ' from the date of receipt of grievance.[61] This rule is sufficient enough to bring the accountability among the data collectors.

The Transborder Data flow Principle

OECD Guidelines elucidate Transborder data flow principle which is international principle. According to guidelines, "A Member country should refrain from restricting transborder flow of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines."[62] Apart from this, legitimate restriction can be imposed in relation to the transborder flow of data which should be in proportion to the risk presented, taking into account the sensitivity of the data, and the purpose and context of the processing.[63] Article 12 of COE Treaty also talks about the transborder flow of personal data. In India, The Rules also regulate the transborder flows of personal data by body corporate or any person on its behalf. A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules.[64] The transfer of data may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.[65] The main criteria of transfer are to ensure the same level of protection and consent by the data subject. Almost all the European countries have this principle in their respective laws due to the international obligations.

Epilogue

Unlike European countries, India lacks appropriate and adequate legislation for the protection of personal data including sensitive personal data. Until and unless, we provide and strongly recognize the right to privacy specifically, we can not achieve the goal of protection of data. Right to privacy and data protection are co related with each other. In fact, right to information has been emphasized extremely instead of causing a balance between personal data protection and right to privacy. This is the right time for Asian countries to evolve or create a new uniform jurisprudence at the international level for personal data protection. Those principles which have been adopted by the EU countries, seem adequate enough for the data protection. All these principles would be helpful for developing and third world countries to draft an effective model law pertaining to the data protection. Till the time, we don't have *sui generis* law in this regard; courts have to perform in the light of existing laws. In India, right of data protection could be enforced

in the accordance with the existing laws. In fact, urgent amendments in the concerned laws are also required for ensuring data protection.

---

[1] Section 5 of The Official Secrets Act, 1923

[2] The Administrative Reforms Commission or ARC is the committee appointed by the Government of India for giving recommendations for reviewing the public administration system of India. The Second Administrative Reforms Commission (ARC) was constituted on 31.08,2005, as a Commission of Inquiry, under the Chairmanship of Veerappa Moily for preparing a detailed blueprint for revamping the public administrative system.

[3] Refer to http://right2information.wordpress.com (Last visited May 27, 2014)

[4] Vishal Mahalwar, "Evolving Jurisprudence of Information Right", International Conference on Transparency and Accountability in Governance: Issues and Challenges, Vol. 2, 2012, p. 120.

[5] See *Govind v. State of Madhya Pradesh (1975) 2 SCC148; Rayala M. Bhubaneswari v Nagaphanender Rayala, AIR 2008 AP 98*

[6] See *Narendra Kumar v. State of Haryana (1994) 4 SCC 460, State of Himachal Pradesh v. Raja Mahendra Pal, (1999) 4 SCC 43*

[7] Article 300A of Constitution of India says, "*No person shall be deprived of his property save by authority of law*". Before 44th Amendment, right to property was fundamental right. But now, it is constitutional right.

[8] Section 22 of IPC says

"Movable property".-The words "movable property" are intended to include corporeal property of every description, except land and things attached to the earth or permanently fastened to anything which is attached to the earth.

[9] Section 2(o) of Copyright Act 1957 says

"literary work" includes computer programmes, tables and compilations including computer data bases

[10] Section 13 of Copy Right Act says;

Works in which copyright subsists.- (1) Subject to the provisions of this section and the other provisions of this Act, copyright shall subsist throughout India in the following classes of works, that is to say,-

(a) *original* literary, dramatic, musical and artistic works;

[11] According to Article 10(2) of TRIPS,. "Compilations of data or other material, whether in machine readable or other form, which by reason of the selection or arrangement of their contents constitute intellectual creations shall be protected as such. Such protection, which shall not extend to the data or material itself, shall be without prejudice to any copyright subsisting in the data or material itself."

[12] Refer to, Vishal Mahalwar, "Idea and Expression Dichotomy: A Conspicuous Demarcation" ,OIIRJ,Vol-III, Nov 2013, p. 405

[13] *Fiest Publications, Inc. v. Rural Telephone Service Company, Inc, 499 U.S. 340 (1991)*

[14] Article 39 (2) of TRIPS says

Natural and legal persons shall have the possibility of preventing information lawfully within their control from being disclosed to, acquired by, or used by others without their

consent in a manner contrary to honest commercial practices10 so long as such information:
(a) is secret in the sense that it is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons within the circles that normally deal with the kind of information in question;
(b) has commercial value because it is secret; and
(c) has been subject to reasonable steps under the circumstances, by the person lawfully in control of the information, to keep it secret.

[15] *Burlington Home Shopping Pvt. Ltd. v. Rajnish Chibber, 1995 PTC (15) 278*

[16] Section 8. Exemption from disclosure of information. (1) Notwithstanding anything contained in this Act, there shall be no obligation to give any citizen,—
(a) information, disclosure of which would prejudicially affect the sovereignty and integrity of India, the security, strategic, scientific or economic interests of the State, relation with foreign State or lead to incitement of an offence;
(b) information which has been expressly forbidden to be published by any court of law or tribunal or the disclosure of which may constitute contempt of court;
(c) information, the disclosure of which would cause a breach of privilege of Parliament or the State Legislature;
(d) information including commercial confidence, trade secrets or intellectual property, the disclosure of which would harm the competitive position of a third party, unless the competent authority is satisfied that larger public interest warrants the disclosure of such information;
(e) information available to a person in his fiduciary relationship, unless the competent authority is satisfied that the larger public interest warrants the disclosure of such information;
(f) information received in confidence from foreign Government;
(g) information, the disclosure of which would endanger the life or physical safety of any person or identify the source of information or assistance given in confidence for law enforcement or security purposes;
(h) information which would impede the process of investigation or apprehension or prosecution of offenders;
(i) cabinet papers including records of deliberations of the Council of Ministers, Secretaries and other officers:
Provided that the decisions of Council of Ministers, the reasons thereof, and the material on the basis of which the decisions were taken shall be made public after the decision has been taken, and the matter is complete, or over:
Provided figther that those matters which come under the exemptions specified in this section shall not be disclosed;
(j) information which relates to personal information the disclosure of which has no relationship to any public activity or interest, or which would cause unwarranted invasion of the privacy of the individual unless the Central Public Information Officer or the State Public Information Officer or the appellate authority, as the case may be, is satisfied that the larger public interest justifies the disclosure of such information:

[17] Article 19(2) Nothing in sub-clause (*a*) of clause (1) shall affect the operation of any existing law, or prevent the State from making any law, in so far as such law imposes

reasonable restrictions on the exercise of the right conferred by the said sub-clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence.

[18] Section 2(1) (o), Information Technology Act, 2000

[19] Ins, by Act 2009, sec. 22

[20] Section 72 A of IT Act says:

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 a fine which may extend to five lakh rupees, or with both.

[21] Section 69(1) of Information Technology Act, 2000

[22] Section 43 (b) of Information Technology Act, 2000

[23] The Organisation for Economic Co-operation and Development (OECD) is an international economic organisation of 34 countries founded in 1961 to stimulate economic progress and world trade. OECD was originated as Organisation for European Economic Co-operation, in the year of 1984. It is a forum of countries committed to democracy and the market economy, providing a platform to compare policy experiences, seek answers to common problems, identify good practices and coordinate domestic and international policies of its members. Refer http://en.wikipedia.org/wiki/Organisation_for_Economic_Co-operation_and_Development (Last visited May 29, 2014)

[24] The Council of Europe is an international organisation promoting co-operation between all countries of Europe in the areas of legal standards, human rights, democratic development, the rule of law and cultural co-operation. It was founded in 1949, has 47 member states with some 800 million citizens, and is an entirely separate body from the European Union (EU), which has 28 member states. Unlike the EU, the Council of Europe cannot make binding laws. The two do however share certain symbols such as the flag and the anthem. Refer to http://en.wikipedia.org/wiki/Council_of_Europe(Last visited May 29, 2014)

[25] Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[26] Article 2(a) of The Data Protection Directive

[27] Article 8, para. 1

[28] See, Article 8, para. 2 & 3

[29] Rule 2 (h)"Password",means a secret word or phrase or code or passphrase or secret key, or encryption or decryption keys that one uses to gain admittance or access to information

[30]Rule 2(b)"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

[31] Rule 3, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
[32] Article 6 (1) (a), E U The Data Protection Directive
[33] Article 5(a), COE Treaty
[34] Article 7 (a), E U The Data Protection Directive
[35] Explanation (ii) of Section 43 A of IT Act, 2000: "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities
[36] Rule 5 (1) Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
[37] Article 5 (c), COE Treaty
[38] Article 5 (d), COE Treaty
[39] Article 6 (c), E U The Data Protection Directive
[40] Article 6 (d), E U The Data Protection Directive
[41] Rule 6, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
[42] Ibid.
[43] Para. 9, OECD Guideline
[44] See, Article 5 (b), COE
[45] Article 10 (b), E U The Data Protection Directive
[46] Rule 5 (3), , Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
[47] Rule 5 (5), , Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
[48] Para. 10, OECD Guideline
[49] Rule 6 (1), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
[50] Ibid
[51] Rule 6 (3), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
[52] Rule 6 (4), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
[53] Article 7, COE Treaty
[54] Rule 8 (1), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
[55] Para.12, OECD Guideline
[56] Rule 4 (1), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
[57] Rule 5 (3)(d) , Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
[58] Article 5 (e) COE
[59] Article 6 (e), E U The Data Protection Directive
[60] Rule 5 (4), Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011

[61] Rule 5 (9) Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
[62] Para. 17, OECD Guidelines
[63] Para. 18, OECD Guidelines
[64] Rule 7, Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011
[65] Ibid