RES MILITARIS
REVUE EUROPEENNE D ETUDES EUROPEAN JOURNAL OF MILITARY STUDIES
Social Science Journal

A Critical Analysis of National and International Legal Framework for Protection of the Right to Privacy and Data Protection

By

Ms. Sonal Rawal
Research Scholar at GLS University, Ahmedabad & Asst. Prof. at Faculty of Law, GLS University
Email: rawalsat@gmail.com

Dr. Hiren Patel
Principal in charge at M N Law College Ahmedabad
Email: patelhiren00@gmail.com

Abstract

The aim of this paper is to initiate a serious debate on right to privacy and data protection in the Indian perspective. Privacy though not expressly provided under the Constitution; it impliedly takes into it the right to privacy as personal liberty guaranteed under article 21. There is an inherent conflict between right to privacy and data protection. The data protection may include financial details, health information, business proposals, intellectual property and sensitive data. Data protection and privacy have been dealt within the Information Technology (Amendment) Act, 2008 but not in an exhaustive manner. The IT Act is not sufficient in protection of data and hence a separate legislation in this regard is required. This paper covers other international legal frame work for protecting privacy and also cover other international conventions for protection of privacy.

Keywords: Right to Privacy, Data Protection, Constitution of India, Article 21, Freedom of Speech

Introduction

The right to privacy is a multi-dimensional concept. In modern society right to privacy has been recognized both in eyes of 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 and 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 computerized data about him/her which is inaccurate or misleading and which could be transferred to an unauthorized third party at high speed and at very little cost. This growth in the use of personal data has many benefits but it could also lead to many 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 organizations should be protected in such a manner that their privacy rights are not compromised.

Concept of privacy

The term privacy and right to privacy cannot be easily conceptualized. It has been taken in different ways in different situations. Tom Gaiety opined that[1] _right to privacy is bound to include body 's inviolability and integrity and intimacy of personal identity including marital privacy. 'Jude Cooley[2] explained the law of privacy and has asserted that privacy is synonymous to _the right to be let alone'. Edward Shils[3] has also explained privacy as _zero relationship between two or more persons in the sense that there is no interaction or communication between them, if they so choose.' Warren and Brandeis[4] have very eloquently explained that _ once a civilization has made distinction between the ―outer‖ and ―inner‖ man, between the life of the soul and the life the body…the idea of a private sphere is in which man may become and remain himself.' In modern society privacy has been recognized both in the eyes of law and in common parlance. But it varies in different legal systems as they emphasize different aspects. Privacy is a neutral relationship between persons or groups or between groups and person. Privacy is a value, a cultural state or condition directed towards individual on collective self-realization varying from society to society.

The Indian Constitution provides a right to freedom of speech and expression,[5] which implies that a person is free to express his will about certain things.[6]A person has the freedom of life and personal liberty, which can be taken only by procedure established by law.[4]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,[5] the person is entitled to express his wishes regarding professing and propagating any religion.[6]The privacy of property is also secured unless the law so authorizes i.e. a person cannot be deprived of his property unlawfully.[7] The personal liberty mentioned in article 21 is of the widest amplitude and it covers a variety of rights which go to constitute the personal liberty[8] viz. secrecy,[9]autonomy,[10] human dignity,[11] human right,[15] self-evaluation,[12] limited and protected communication,[13] limiting exposure[14]of man etc. 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 rights and are 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 one's personal information.

[1] Tom Gaiety, ―Right to Privacy‖ 12 Harvard Civil Rights Civil Liberties Law Review 233.
[2] Thomas M Cooley, A Treatise on the Law of Torts 29 (2nd ed. 1888).
[3] Edward Shils, ―Privacy: Its Constitution and Vicissitudes‖ 31 Law & Contempt Problems 281 (1966). [4] Samuel Warren & Louis D. Brandeis, ―The Right to Privacy‖ Harvard Law Review 193 (1980). [5] Constitution of India, art. 19 (1)(a) [6] Id., art.19(2).
[4] Art 21
[5] Art 22
[6] Art 25
[7] Art 300A
[8] Kharak Singh v. State of U.P., AIR 1963 SC 1295 & Govind v. State of M.P., AIR 1975 SC 1378.
[9] Allgeyer v. Louision, 165 U.S. 578 (1897).
[10] Louis Henkin, ― Privacy and Autonomy‖74 Columbia Law Review 1410 (1974)
[11] Olmstead v. U.S., 277 U. S. 438, 478 (1928) & Menka Gandhi v. Union of India, AIR 1978 SC 597. [15] Universal Declaration of Human Rights, 1948, art. 12 & International Covenant on Civil and Political Rights, 1966, art. 17.
[12] Alan F Westin, ―Science, Privacy and Freedom‖ 66 Columbia Law Review 1003 (1966).
[13] Id. at 1027.
[14] Id. at 1040.

Judicial activism

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 recognized 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 case,[15]especially the minority judgment of Subba Rao J. In Govind v. State of M.P.,[20]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 the 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 one‘s data and ability to act freely.

Telephone tapping and privacy

Right to privacy is affected by new technologies. Right to privacy relating to a person‘s correspondence has become a debating issue due to the technological developments. There have been cases of intercepting mails and telephonic communication of political opponents as well as of job seekers. Section 5(2) of the Indian Post Office Act and section 26(1) the Indian Telegraph Act empower the central and state governments to intercept telegraphic and postal communications on the occurrence of public emergency in the interest of public safety. In R.M. Malkani v. State of Maharashtra,[16] the Supreme Court observed that the court will not tolerate safeguards for the protection of the citizen to be imperiled by permitting the police to proceed by unlawful or irregular methods. 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 articles 21 and 19(1)(a) of the Constitution. Kuldip Singh J opined in People ‘s Union for Civil Liberties v. Union of India[17]that right to hold a telephonic conversation in the privacy of one‘s home or office without interference can certainly be claimed as right to privacy. In this case Supreme Court laid down certain procedural guidelines to conduct legal interceptions, and provided for a high-level review committee to investigate the relevance of such interceptions. But such caution has been thrown to winds in recent directives from government bodies as is evident from phone tapping incidents that have come to light. In State of Maharashtra v. Bharat Shanti Lai Shah, [18]the Supreme Court said that interception of conversation though constitutes an invasion of an individual ‘s right to privacy it can be curtailed in accordance with procedure validly established by law. The court has to see that the procedure itself must be fair, just and reasonable and not arbitrary, fanciful or oppressive. An authority cannot be given an untrammeled power to infringe the right to privacy of any person.[19] In Neera Radia tape case[25] to use phone tapping as a method of investigation in a tax case seems to be an act of absurd overreaction. For so many journalists, politicians and industrialists to have their phone tapped without a rigorous process of oversight represents a gross violation of basic democratic principles.

Women ‘s liberty and privacy: The right to privacy implies the right not merely to prevent the incorrect portrayal of private life but the right to prevent it being depicted at all. Even a woman of easy virtue is entitled to privacy and no one can invade her privacy as and

[15] Supra note 11. [20] Ibid.
[16] AIR 1973 SC 157.
[17] AIR 1997 SC 568
[18] (2008) 13 SCC
[19] Directorate of Revenue v. Mohd. Nisar Holia (2008) 1 SCC (Cri) 415 [25] The Times of India, Allahabad Times December 8, 2010.

when he likes.[20]The modesty and self-respect may perhaps preclude the disclosure of such personal problems like whether her menstrual period is regular or painless etc. [27]The basic right of female is to be treated with decency and proper dignity. But if a person does not like marriage and lives with another it is entirely his or her choice which must be respected. Sense of dignity is a trait not belonging to society ladies only, but also to prostitutes.[21] he entire society.[22] As a victim of sex crime she would not blame anyone but the culprit. Rapist not only violates the victim 's privacy and personal integrity, but inevitably causes serious psychological as well as physical harm in the process. Rape is not merely assault- it is often destructive of the whole personality of the victim.[30]Right to privacy is an essential requisite of human personality embracing within it the high sense of morality, dignity, decency and value orientation. The question of relation between the right to privacy and conjugal rights arose for the first time in Sareetha v. Vankta Subbaih, [23]wherein the Andhra Pradesh High Court held the provisions of section 9 of the Hindu Marriage Act 1955 i.e., the restitution of conjugal rights, as unconstitutional as it is violative of article 21 of the Constitution of India vis-à-vis right to privacy. But in Harvinder Kaur v. Harmander Singh, [24]the Delhi High Court held that though sexual relations constitute most important attribute of the concept of marriage but they do not constitute its whole content. Sexual intercourse is one of elements that goes to make up the marriage but it is not summum bonum. In Saroj Rani v. Sudarshan Kumar Chandha,[25] the Supreme Court agreed with Delhi High Court and thereby upheld the constitutionality of section 9. This right is within the right to marry and it does not violate the right to privacy of wife. It has been generally felt that the Supreme Court in this case lost an ideal opportunity for changing law in this regard in accordance with the changing spirit of the times. The right of the husband or the right of wife to the society of the other is not a creation of statute. The Law Commission of India in its 71st report stated that the essence of marriage is the sharing of common life, the sharing of all the happiness that life has to offer and all the miseries that have to be faced in life, an experience of the joy that comes from enjoying the common things of the matter. Once the woman enters into the marriage relation, her right to privacy must be seen in the context of family life.

The other question that may be raised regarding the appropriateness of giving legislative judgment about abortion. The objective in prohibiting abortion is to protect the societal interest in procreation. If women were given the ultimate right of privacy to terminate pregnancy whenever they wish to do so, such right if exercised by the women could effectively threaten the life of the unborn child and the societal interest in procreation. The question is whether the right to privacy encompasses woman 's decision or not? A woman 's right to make reproductive choices is also a dimension of personal liberty as understood under article 21 of the Constitution. Reproductive choices can be exercised to procreate as well as to abstain from procreating. The crucial consideration is that a woman 's right to privacy, dignity and bodily integrity should be respected. Reproductive rights include a woman 's entitlement to carry pregnancy to its full term, to give birth and to subsequently raise children. [26]A woman 's right to terminate her pregnancy is not absolute and may to some extent be limited by the state's legitimate interests in safeguarding the woman's protecting potential human life. Recognizing that the sanctity of life has a supreme value in the hierarchy of values, it is nonetheless true that

[20] State of Maharastra v. Madhuker Narayan Markikar, AIR 1991 SC 207 [27] Neera Mathur v. LIC of India, AIR 1992 SC 392.
[21] State of Punjab v. Baldev Singh, AIR1999 SC 2378.
[22] Dinesh v. State of Rajasthan, AIR 2006 SC 1267 & State of Panjab v. Ramdev Singh, AIR 2004 SC 1290. [30] Rajinder v. State of H.P., (2009) 16 SCC 69.
[23] AIR 1983 AP 346.
[24] AIR1984 Del 66.
[25] AIR1984 SC 1562.
[26] Suchita Srivastava v. Chandigarh Admn. , (2009) 9 SCC 1.

the human fetuses cannot claim any rights superior to that of born persons because of the following reasons:[27]

a. A fetus is not a person;
b. The court does not know _when life begins ‘, it does know that _the unborn have never been recognized in the law as persons in the whole sense;
c. We do not agree that life begins at conception and is present throughout pregnancy.

Hence, many countries in the world have reformed their laws to allow abortion in a variety of circumstances, usually abnormality in the fetus, or the pregnancy being a result of rape or incest or danger to the life of the mother. In fact, an abortion decision involves competing interests of the society, that of the woman and that of the fetus. Abortion should not be recognized as a matter of personal privacy and must be prohibited unless there is an urgent necessity.

Press, e-media and privacy

The freedom of press has not been expressly mentioned in article 19 of the Constitution of India but has been interpreted that it is implied under it. In R Rajagopal v. State of Tamilnadu, [28] 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 authorization. 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. So, a female who is the victim of sexual assault, kidnapping, abduction or a like offence should not further be subject to the indignity of her name and the incident being published in press media.[29] The freedom of speech and expression as envisaged in article 19 (1)(a) of the Constitution also clothes a police officer to seize the infringing copies of the book, document or newspaper and to search places where they are reasonably suspected to be found, impinging upon the right to privacy.[30]Newspaper or a journalist or anybody has the duty to assist the state in detection of the crime and bringing criminal to justice. Withholding such information cannot be traced to right to privacy in itself and is not an absolute right.[31] Regarding protection of privacy vis-à-vis encroachment by press the judicial approach is not very clear. There is no specific legislation in India which directly protects right to privacy against excessive publicity by press. E-media includes television, radio, internet broadcast, and all electronic journalism which are used by today ‘s media. Main purpose of media is to bridge the gap between government policy and public grievances. In Destruction of Public & Private Properties v. State of A.P,[40] the Supreme Court held 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 very popular tool used by media nowadays which directly hammers the individual privacy. There is no guideline to handle this issue.

[27] . Roe v. Wade, 410 U.S. 113 (1973); 35 L.Ed. 2d. 147.
[28] AIR 1995 SC 264.
[29] R. Rajagopal v. State of Tamilnadu, AIR 1995 SC 264
[30] State of Maharashtra v. Sangharaj Damodar Rupawate, (2010) 7 SCC 398.
[31] People‘s Union for Civil Liberties (PUCL) v. Union of India, AIR. 2004 SC 456. [40] AIR 2009 SC 2266.

Information privacy

Information privacy or data privacy is the relationship between collection and dissemination of data technology, the public expectation of privacy, and the legal and political issues surrounding them. The extent to which confidentiality is to be protected could be understood from a few cases. In Union of India v. Association of Democratic Reforms,[32] the Supreme Court has put its stamp on the issue. The right to get information in a democracy is recognized all throughout and it is a natural right flowing from the concept of democracy. Article 21 confers on all persons a right to know which include a right to receive information. The ambit and scope of article 21 is much wider as compared to article 19(1) (a).[33] In People ‘s Union for Civil Liberties (PUCL) v. Union of India,[43] the Supreme Court observed that 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 to what extent a voter has a right to know about a candidate‘s privacy. The voter‘s right to know about a candidates privacy can be protected and flourished by removing the drawbacks of laws relating to voters 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. Thus, it ultimately requires a healthy and congenial inter-relationship between the social good and the individual liberty. Thus, it is concluded that one has to maintain a balance between the right to information of a citizen and the right of privacy of a candidate seeking election.

Health and privacy

Health sector is the important concern in privacy. Your health information includes any information collected about your health or disability, and any information collected in relation to a health service you have received. Many people consider their health information to be highly sensitive. The right to life is so important that it supersedes right to privacy. Under medical ethics, a doctor is required not to disclose the secret information about the patient as the disclosure will adversely affect or put in danger the life of other people.[34] In

Mr. _X‘ v. Hospital _Z‘ [45] the Supreme Court held that the 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 person ‘s right to be let alone with another person ‘s right to be informed. In another case the apex court said that[35] 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 appellant ‘s right was not affected in any manner in revealing his HIV-positive status to the relatives of his fiancée. In Selvi v. State of Karnataka[36] the Supreme Court held that narco-analysis, 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. If DNA test is eminently needed to reach the truth, the court must exercise the dissector of medical examination of a person. Therefore, the Supreme Court was of the view that[48] 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

[32] AIR 2002 SC 2112
[33] Reliance Petrochemicals Ltd. v. Proprietors of Indian Express Newspapers, AIR 1989 SC 190 [43] AIR 2003 SC 2363.
[34] Spring Meadows Hospital v. Hajot Ahluwalia, AIR 1998 SC 1801 [45] AIR 1999 SC 495.
[35] Mr. _X‘ v. Hospital _Z‘, AIR 2003 SC 664.
[36] See Bhabani Prasad Jena v. Orissa State Commission for Women, (2010) 8 SCC 633 [48] See Sarda v. Dharmpal, AIR 2003 SC 3450

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 enter relationship 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 organizations. 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 individual ‘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 web sites. 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 (Amendment) Act, 2008 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 is the only Act to date which covers the key issues of data protection, albeit not every matter. In fact, the Information Technology (Amendment) Act, 2008 enacted by the Indian Parliament is the first legislation, which contains provisions on data protection. According to section 2(1)(o) of the Act, ―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 or 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 ―data‖ 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,[37] Computer,[38] Computer network,[39]Computer resource,[40] Computer system,[41] Computer database,[42] Data,[55] Electronic form,[43] Electronic record,[44] Information,[45] Intermediary,[46] Secure system,[47]and Security procedure.[48] 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 concerned party. Third party information is defined to mean any information dealt with by an intermediary in his capacity as an intermediary and it may be arguable that this limitation also applies to data‘ and communication‘. Section 79 provides that an

[37] Information (Amendment) Technology Act, 2008, s. 2 (1) (a).
[38] Id., s.2 (1) (i)
[39] Id., s.2 (1) (j)
[40] Id., s.2 (1) (k)
[41] Id., s. 2 (1) (l)
[42] Id., s. 43, explanation (ii).
[43] Id., s. 2 (1) (r)
[44] Id., s. 2 (1) (t)
[45] s. 2 (1) (v)
[46] s. 2 (1) (w)
[47] s. 2 (1) (ze)
[48] s. 2 (1) (zf)

intermediary shall not be liable for any third-party information, data, or communication link made available or hasted 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 ―data‖ would be more relevant in 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 (Amendment) Act 2008 provides for civil liability in case of computer database theft, computer trespass, unauthorized 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 unauthorized access to computer, computer system, computer network or resources; (b) unauthorized digital copying, downloading and extraction of data, computer database or information, theft of data held or stored in any media; (c) introduced any computer contaminant or computer virus into any computer system or computer network; (d) unauthorized 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) unauthorized 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 ―a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalized 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 43A provides for compensation for failure to protect data‘, it provides: ―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 43A which provides for civil action for security breaches is based on the concept of sensitive personal information‘. Other than that, there is no special protection in Indian law for sensitive personal information. Section 43A 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 anyone 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 affected in different ways which justify compensation. It also provides that accessing data in an unauthorized way is a civil liability.

Criminal liability and data protection The Information Technology (Amendment) Act, 2008 provides for criminal liability in case of computer database theft, privacy violation etc. The Act also make wide ranging amendments in chapter XI enfacing sections 65-74 which

cover a wide range of cyber offences, including offences related to unauthorized tempering with computer source documents,[49] dishonestly or fraudulently doing any act referred to in section 43,[5051] sending offensive messages through communication service etc.,[64] dishonestly receiving stolen computer resource or communication device,[52] identity theft,[53] cheating by personation by using computer resource,[54] violation of privacy,[55] cyber terrorism,[56] transmitting obscene material in electronic form,[57] transmitting of material containing sexually explicit act, etc., in electronic form,[58] transmitting of material depicting children in sexually explicit act, etc., in electronic form,[72] 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 69B by refusing to provide technical assistance to the agency authorized 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 organizations to disclose details of the practices in handling personal information. Indian penal code provided remedies against defamatory act or an act outraging the modesty of women and the IT Act 2000 has provision to prevent publishing sexually explicit material, cyber stalking and violation of privacy[59].

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 whoever, 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. Section 66-E explanation (e) has also explained violation of privacy as circumstances in which a person can have a reasonable expectation that—(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.‘ Section 72 provides for penalty for breach of confidentiality and privacy as meaning any 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,

[49] S.65
[50] S.66
[51] S.66(a)
[52] S.66(b)
[53] S.66(c)
[54] S.66(d)
[55] S.66(e)
[56] S.66(f)
[57] S.67
[58] S.67A [72] S.67B
[59] Errakot, S., & VK, R. (2023). Cyber bullying: A Need for Separate Provision in Indian Law Saran. *GLS Law Journal* , *5*(1), 38 - 45. Retrieved from https://glslawjournal.in/index.php/glslawjournal/article/view/81

information, document or other material to any other person.‘ Section 72A also explains the law of privacy and asserts that 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‘ amounts to breach of privacy and provides for punishment for the same. Sections 66E, 72, and 72A require the consent of the concerned persons 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 Bank,84 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 amounts 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 unauthorized access to computer, computer system, computer network or resources, unauthorized 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 one can access any information related to anyone from anywhere at any time but this poses a new threat to private and confidential information. Globalization 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 the USA some special privacy laws exist for protecting student education records, children ‘s online privacy, individual ‘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 recognized in the Constitution but its growth and development is entirely left to the mercy of the judiciary. In today ‘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 within the Information Technology (Amendment) Act, 2008 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. To conclude it would suffice 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.

International legal frame work for protection of privacy Introduction:

The degree of intrusion into the private lives of individuals has been a topic of debate for years and has also featured prominently in literature for years. Kautilya‘s Arthashastra, an Indian epic dating from approximately 300 B.C. places great emphasis on the role of

knowledge gleaned from spies, both internally in a nation and outside it and in maintaining a grip on power, the echoes of which can be seen in Machiavelli's Prince written hundreds of years later. And as long as surveillance has been a part of human life so probably has opposition to its excesses. Due to the technology available a lot of our daily activities are recorded and either monitored in real time by someone for future reference. When you go to a bank to withdraw money from an ATM, you are being watched or when you go to a shop or a superstore, you come across a sign that reads ―This store is under surveillance‖, so you are forewarned. In Fresno, California, security measures included, for the first time in a United States airport, use of facial recognition technology to scan faces for terrorists as passengers entered security checkpoints. In addition to law enforcement, large companies and businesses use surveillance for a variety of other purposes. They use technology to monitor employee productivity, deter theft and fraud, and ensure safety in the workplace. Having seen the extent of surveillance in our lives it seems to be a given that we need to live with it and this paper explores the ways by which laws of various jurisdictions seek to achieve ―the preservation of basic human rights‖ i.e., Privacy. It must be kept in mind that the statutes and case laws analyzed in this paper are indicative and are not exhaustive.

Objectives

After studying this unit, you should be able to know:

- The concept of _privacy' in the legal sense;
- The international legal scenario as it stands today, for protection of privacy;
- Legal provisions that provide for protection of privacy in US; and
- Legal provisions that provide for protection of privacy in EU and UK.

The Position in the United States of America

American scholars as far back as the 1800s have debated the existence of the right to privacy. Samuel Warren and Louis Brandeis were pioneers in authoring "The Right to Privacy", which became the most important article recognizing a right of privacy.

Subsequently, President Woodrow Wilson appointed Brandeis to the United States Supreme

Court in 1916, where he endeavored to lay a foundation for the future privacy law. The United States Supreme Court has found a limited ―right to privacy stemming from a combination of the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments. The First Amendment provides: ―Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press, or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances. The Third Amendment provides: ―No soldier shall, in time of peace be quartered in any house, without consent of the owner, nor in time of war, but in a manner to be prescribed by law.‖ The Fourth Amendment provides that: ―The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.‖ The Fifth Amendment provides in relevant part that: ―No person shall ... be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law.... The Ninth Amendment retained rights clause

'provides: ―The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people. The Fourteenth Amendment provides in relevant part: ―No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws.‖ In Paul vs. Davis [(1976) 424 U.S. 693], the Court found that no privacy right existed when the police disclosed that the respondent was arrested on a shoplifting charge. The Court found that the activities detailed were very different from ordered liberty matters relating to marriage, procreation, contraception, family relationships, child rearing and education. The United States Constitution does not provide an explicit right to privacy but it is implied in the Fourth Amendment. That it protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected. In weighing these competing interests, American judges have expanded the principles that would guide all three branches of the federal government in the application of the Fourth Amendment to national security electronic surveillance. It has been noted that national security cases present a particularly prickly situation because of the tremendous governmental interest and the likelihood of both unreasonable invasions of privacy and jeopardy to free speech rights. Although judges have recognized the vital importance of protecting the national security, the primary concern is ensuring the sanctity of political dissent – both public and private – in determining the application of the Fourth Amendment to national security surveillance. The Fourth Amendment is to serve as ―an important working part of the machinery of government, operating . . . to check the well-intentioned but mistakenly over-zealous executive officers. This constitutional function cannot be guaranteed when domestic security surveillance is left entirely to the discretion of the executive: ―Unreviewed executive discretion may yield too readily to pressure of obtaining incriminating evidence and overlook potential invasions of privacy and protected speech‖. Thus, the Courts reiterated their assertion that some interposition of the judiciary between citizens and law enforcement must exist. The United States has a large number of narrowly-focused privacy laws consistent with its traditionally increment approach to legislation. This is in contrast to the trans sectoral approach of Europe. Whether the whole adds up to sufficiently comprehensive privacy protection in the US is in the eye of the beholder. It is clear that to understand completely US privacy protections, one must look at the various federal pieces, as well as at the matrix of state laws that adds to the national protections. Federal privacy (and privacy-affecting) laws include the following:

- Federal Trade Commission Act (1914)
- Fair Credit Reporting Act (1970)
- Privacy Act (1974)
- Freedom of Information Act (1974)
- Family Educational Rights and Privacy Act (1974
- Foreign Intelligence Surveillance Act (1978)
- Right to Financial Privacy Act (1978)
- Privacy Protection Act (1980)
- Cable Communications Policy Act (1984)
- Electronic Communications Privacy Act (1986)
- Video Privacy Protection Act (1988)
- Employee Polygraph Protection Act (1988)
- Telephone Consumer Protection Act (1991)
- Driver's Privacy Protection Act (1994)

- Health Insurance Portability and Accountability Act (1996)
- Telecommunications Act (1996)
- Children‘s Online Privacy Protection Act (1998)
- Financial Modernization Services Act (1999)
- USA Patriot Act (2001)

It is clear that the United States provides to its citizens an implied right to privacy through the Constitution as well through its various legislations. The concept of the rational test basis would imply that a balance would have to be struck between the rights of the individual on one hand and societal needs on the other.

The Position in the United Kingdom and the European Union

The European Convention on Human Right, 1950 (Convention) addresses the issue of privacy as under: ―8(1). Everyone has the right to respect for his private and family life, his home and his correspondence. 8(2). There shall be no interference by a public authority with the exercise of this right except if it is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. Article 8 provides a right to respect for private and family life, subject to the qualification in Art.8 (2) that interference may occur where it is ―in accordance with the law and is necessary in a democratic society in the interests of‖, the prevention of disorder or crime. The interrelationship between Arts.8 (1) and (2) is not one of balancing the legitimate interference against the right; the Art.8 (2) qualifications clearly represent exceptions to Art.8 (1). Article 13 of the Convention provides that ―everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity. In the face of considerable opposition, this provision was not incorporated in the Human Rights Act. In Convention terms, Art.13 requires an ―effective remedy whenever there is a breach of Art.8. Logically, the effectiveness of the available remedy must lie in its ability to secure the protection offered by the Article – in this context a respect for privacy. The fact that the Human Rights Act does not incorporate Art.13 does not negate domestic obligations to provide an effective remedy because the Convention must always be read as a whole. In the United Kingdom, until the passage of the Human Rights Act 1998 the concept of privacy was one that neither Parliament nor the courts had taken the initiative to develop.

In 1996, in R. v Brown [(1996) 1 All E.R. 545 at 556] Lord Hoffman stated that, ―English common law does not know a general right of privacy and Parliament has been reluctant to enact one‖. The House of Lords later that year in a case concerning covert police surveillance commented upon the ―continuing widespread concern at this apparent failure of the law‖ [R. v Khan (1997) A.C. 558 at 582]. Such a reluctance to develop the law has partly been a result of the inherent difficulties in defining such a nebulous concept. However, though ―privacy as a domestic legal term in England might be lacking clear parameters, the right to respect for private life under Art.8 of the Convention brings with it decades of developing jurisprudence. The European Court ‘s jurisprudence lays down a minimum set of values that must be respected in signatory states, and, even prior to the Human Rights Act, this had impacted UK law and practice indirectly. The Human Rights Act has brought about the development of a coherent and comprehensive system to ensure that all police action that might interfere with Art.8 is a Convention compliant. It has also ensured that the courts must address

directly the question of when a particular action interferes with the right to respect for private life. A number of general principles have derived from the interpretation of the exceptions to the general right. First, if the primary right is engaged in a particular case, then the restriction upon that right must be ―in accordance with the law‖. Regardless of the end to be achieved, no right guaranteed by the Convention should be interfered with, unless a citizen knows the basis for the interference through an ascertainable national law. That, law should be sufficiently clear and accessible to ensure that people can adequately determine with some degree of certainty when and how their rights might be affected. Secondly, any interference with the primary right must be directed towards a legitimate aim as stated in Art.8 (2). The restrictions on the primary right are numerous and widely drawn and it could be argued that it is not overly burdensome to require State conduct to remain within such boundaries. However, the list is intended to be exhaustive and there should be no capacity for the State to add to those grounds. In addition to being lawful, and for one of the prescribed purposes, the restriction must also be ―necessary in a democratic society. Necessity though not defined in the Convention itself, has been interpreted by the European Court as not synonymous with indispensable ‘but not as flexible as ordinary, useful, reasonable or desirable. Instead, what is required is that the interference with the primary right should be in response to a pressing social need. The Human Rights Act has brought the concept of proportionality directly into play in the United Kingdom. In the context of qualified rights, such as Art.8, proportionality has a special relevance. In Brown v Stott [(2001) 2 W.L.R. 817], Lord Steyn commented: ―... The fundamental rights of individuals are of supreme importance but those rights are not unlimited: we live in communities of (other) individuals who also have rights‖ Proportionality is a vital factor that attempts to find a balance between the interests of the individual and the interest of the wider community. Despite not explicitly appearing within the text of the Convention itself, it is said to be a defining characteristic of the way in which the courts seek to protect human rights. It is, according to the Court, ―inherent in the whole of the Convention‖ [Soering v United Kingdom (1989) 11 E.H.R.R. 439 at para 89]. There are numerous factors to be taken into account when considering the issue of proportionality. For example, if a measure, which restricts a right, does so in such a way as to impair the very essence of the right it will almost certainly be disproportionate. Furthermore, the need to have relevant and sufficient reasons provided in support of the particular measure has been emphasized: ―The Court will look at the interference complained of in light of the case as a whole and determine whether the reasons adduced by the national authorities to justify it are relevant and sufficient and whether the means employed were proportionate to the legitimate aim pursued. [Jersild v Denmark (1995) 19 E.H.R.R. 1 at para 31]. It should also be considered if there is a less restrictive alternative. A balancing exercise takes place that requires a consideration of whether the interference with the right is greater than it is necessary to achieve the aim. This is not an exercise in balancing the right against the interference, but instead balancing the nature and extent of the interference against the reasons for interfering. A further factor in the proportionality equation is to assess the adequacy of procedural fairness in the decision making process. Where a public body has exercised a discretion that restricts an individual ‘s Convention rights, the rights of the affected individual should have been taken into account. For example, the policy should not be arbitrary but should be based on relevant considerations. The guarantee against arbitrariness is one that lies at the heart of the Convention provisions. Proportionality can be more easily established where it could be shown that there are sufficient safeguards against abuse in place. This was expressed clearly in Klass vs Germany: ―One of the fundamental principles of a democratic society is the rule of law ... [which] implies, inter alia, that an interference by the executive authorities with an individual‘s rights should be subject to an effective control...‖[(1979-80) 2 E.H.R.R. 214 at para 55]. Given that most policing actions will have a basis in law and will invariably satisfy the requirement of being in pursuit of a legitimate objective (principally, the

prevention and detection of crime), the crux of a case will often be the proportionality of the action under scrutiny. In Ex p. Kebilene, Lord Hope commented: —... the Convention should be seen as an expression of fundamental principles rather than a set of mere rules. The questions which the courts will have to decide in the application of these principles will involve questions of balance between competing interests and issues of proportionality. ‖ [R v DPP Ex p. Kebilene (1999) 3 W.L.R. 972 at 994]. The European Court has never sought to give a conclusive definition of privacy, considering it neither necessary nor desirable. However, in Niemietz v Germany the Court stated: — Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of private life' should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest opportunity of developing relationships with the outside world.‖ [(1992) 16 E.H.H.R. 97 at para 29].

International Covenant on Civil and Political Rights and Other Conventions

Article17 of ICCPR provides for the 'right of privacy'. Article12 of the Universal

Declaration of Human Rights, 1948 (UDHR) is almost in similar terms Article 19(1) and 19(2) of the ICCPR declares that everyone shall have the right to hold opinions without interference, and everyone shall have the right to freedom of expression, and this right shall include freedom to seek, receive and impart information of ideas of all kinds regardless of frontiers, either orally, in writing or in print, in the form of art or through any other media of his choice. Similarly, Article 19 of UDHR provides that everyone has the right to freedom of opinion and expression and this right includes freedom to hold opinion without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers. India is a signatory to the International Covenant on Civil and Political Rights, 1966 (ICCPR). While interpreting the Constitutional provisions dealing with Fundamental Rights,

Indian Courts take into consideration the principles embodied in international conventions

And instruments and as far as possible give effect to the principles contained in those instruments.

Conclusion

Technology is making it increasingly possible to develop physically non-intrusive techniques. The use of satellites and other remote monitoring tools have lessened the need to physically intrude on a person's privacy.

- Technology cuts both ways and jurisprudence need to keep up with these changes to ensure that the use of technology does not spread unchecked.
- In areas other than national security, a system must be put in place so that the authority that wants to undertake surveillance does not also become the authority that takes a decision on whether the surveillance is permissible or not.

- Periodic reporting requirements to the authority that sanctioned the surveillance could be put in place so that the sanctioning authority is aware of whether the original premise under which the sanction was granted was correct or not.
- In the event a person finds out he/she is the subject of surveillance they need to have recourse to the courts of law if the surveillance is intruding on their privacy.
- The EU, UK and US have already enacted legislations to afford protection to their citizens.
- There is a need to ensure that the checks on the misuse of the system keep pace with change and thereby prevent unjustified intrusions on individuals' privacy.

References

Carole A. Lane. Naked in Cyberspace: How to find personal information online. University of Michigan, 2002.
Commonwealth Secretariat. Law in Cyberspace. Commonwealth Secretariat, 2001. 3. Guins De Angelis. Cyber Crimes. Chelsea House Publishers, 1999.
Serge Gutwirth. Privacy and the information age. Trans. Raf Casert. Rowman and Littlefield, 2002. 5. jspui › bitstream › 026_Privacy and D..
www.dbrau.org.in
www.researchgate.net