Page 2000 - 2019 **DOI:** *https://doij.org/10.10000/IJLMH.115988*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 6 | Issue 5

2023

International Data Protection Laws

DR. GOWRI B CHANAL[1]

ABSTRACT

Immense concerns are already prevailing with respect to the protection of personal data and information, in essence the right to one's privacy. The right to privacy refers to the specific right of an individual to control the collection, use and disclosure of personal information. Personal information could be in the form of personal interests, habits and activities, family records, educational records, communication records including mail and telephone, medical records, financial records etc. The privacy rights have to be promoted and protected not only in the physical world but also in the virtual world like cyber space. Privacy if not properly protected faces the danger of being abused by other entities of the cyber space. This has generated a hot debate about the protection of privacy in cyber space.

***Keywords**: Privacy, Cyber Law, Information Technology, Data Protection Law, Conventions.*

I. INTRODUCTION

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.[2] The rapid advancement of network and computer technologies during the last sixty years has dramatically changed the ways in which personal information is created, stored, retrieved, and shared. Massive amount of personal information are stored in digital formats that are easy and cheap to access, duplicate, and transfer. The increasing reliance on digital and network communication often force citizens of modern societies to choose between not participating in some of the most basic social activities, such as staying in touch with family and friends, banking, and shopping, etc.

In a modern State, when means of communication and communication networks have undergone a radical change, the threat to the right of privacy is a weapon to ensure confidentiality in human affairs.[3] Confidentiality is one element in the panorama of rights covered by the right to privacy. The right of privacy extends over the entire gamut of collection, retention, use and disclosure of information. It stems out of the basic human desire for a secure

[1] Author is a Teaching Assistant at PG Dept. of Studies in Law, Karnatak University Dharwad, India.

[2] Shiv Shankar Singh, Privacy and Data Protection in India: A Critical Assessment, JILI, Vol.53, No.4 (Oct-Dec), pp.663-667

[3] Chander, Harish and Ors., Cyber Laws and it Protection 194 (PHI Learning Pvt.Ltd., Delhi, 2022)

 [ISSN 2581-5369]

identity of one's own and to that extent, cannot be denied.[4] The volume and varying nature of transactions carried out on the net are such that the right to privacy must exist at least to a limited extent. Volume and nature of transactions raise the issue of security concerns as to the political, social and economic health of the nation.[5] Internet privacy could be seen as economically important since it gives consumers an assurance that their personal particulars will not be released to unauthorized persons.[6]

Modern technological developments have made it possible for even the smallest of businesses to collect and analyse detailed information about identifiable individuals anywhere in the world. The internet is a rich source of information about online consumers. Websites collect much personal information. Through cookies and tracking software, website owners are able to follow consumer's online activities and gather information about personal interests and preferences. The data collected proves valuable to businesses because not only it is possible for them to target market products and services as well as selling advertising space on their websites. A new industry has emerged to market software products designed to assist websites in collecting and analyzing visitor data and serving useful purpose. Businesses have a great stake in protecting this private information as individuals do and online activities thrive only when there is trust in business practices and the electronic environment. There is a great concern about the use of information gathered and appreciate privacy concerns. The privacy of individual is certainly a concern of the law.[7]

Many US and European consumers have agitated the invasion of their privacy rights by suing e-commerce companies over their data collection practice. As a result thereof, most e-commerce websites now host privacy policies and terms of use on their websites. Internet has made it fairly simple to generate large quantities of personal information. Once the consumer information is collected it can be shared with marketers who may solicit business from them by targeted e-mail campaigns and advertisements. The banner ads and direct e-mail campaigns on the internet target specific individuals as well as specialized groups and internet advertisement companies.[8] In this article an attempt is made to examine at length various issues and new challenges which right to privacy faces in the era of information technology and a critical survey of International, British, America and Indian laws relating to data protection is also discussed.

[4] Yahya R. Kamalipour, Global Perspectives on Media, politics, Immigration, Advertising and Social Networking 166 (Cambridge Scholars Publishing, United Kingdom, 2019)
[5] S.P.Sharma, Business Law 178 (I.K. International Publishing House Pvt.Ltd., Dehradun, 2012)
[6] Dr. R.K. Chaubey, An Introduction to Cyber Crime and Cyber Law 889,890 (Kamal Law House, Kolkata 2009)
[7] *Ibid* p. 890
[8] Karnika Seth, Cyber Laws in the Information Technology Age 393 (Lexis Nexis Butterwoths Wadhwa, Nagpur ,2009)

 [ISSN 2581-5369]

II. INTERNATIONAL DATA PROTECTION LAWS

The data processing industry has an international character. Large amounts of data cross national borders every day, either electronically via cables or satellites or through the manual transfer of media such as magnetic tapes. The former will usually be transferred without control or supervision by any form of governmental authority. Such transfers thus pose a threat to individual privacy, since national laws can be circumvented by transferring data to a so-called 'data heaven' which lacks such legislation.[9] National laws governing privacy and data protection do exist in some countries.[10] But most countries in the world including India have no legislation at all. However, there exist some international legal instruments which help in providing the basis for development towards international harmonization of principles relating to data protection and right to privacy in the digital era i.e., the 1980 OECD Guidelines,[11] the 1981 Council of Europe Convention[12] and the 1995 European Commission Directive.[13]

(A) Organization for Economic Cooperation and Development (OECD)

As the importance of personal data privacy became understood several decades ago the OECD produced a set of guidelines. These guidelines have remained the touchstone of privacy discourse since then. The OECD is an organization focused predominantly on economic matters. The member countries are quite diverse and combined they produce approximately two-thirds of world goods and services. Consequently, concerns about the potential effects of the rise of the private enterprise were central to the OECD's interest in privacy.[14] The OECD was established in 1961 and currently comprises 30 of the leading industrial nations as its members.[15] In 1963, the OECD set up its 'Computer Utilization Group'. This Group's works associated with privacy was later entrusted to a sub-group called 'Data Bank Panel'.[16] This Data Bank Panel later became the 'Group of Government Experts on Tran border Data Barriers and

[9] Ian Walden, Data Protection, in Chris Reed (ed.) Computer Law 330 (Delhi: Universal Law Publishing Co. Pvt. Ltd., Delhi, 3rd edn., 1996)

[10] For instance, Australia has the Privacy Amendment (Private Sector) Act, 2000, Canada has the Personal Information Protection and Electronic Documents Act, 2000, New Zealand has the Privacy Act, 1993, and U.K. has the Data Protection Act, 1998.

[11] Organisation for Economic Cooperation and Development, "Recommendations of Concerning Guidelines Governing the Protection of Privacy and Trans-border Flow of Personal Data"

[12] Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data

[13] European Parliament and Council Directive on the Protection of Individuals with regard to the processing of Personal Data and the Free Movement of such Data

[14] Yee Fen LIM, Cyber Space Law: Commentaries and Materials 142 (Oxford University Press, New Delhi, 2nd edn., 2007)

[15] Australia, Austria, Belgium, Canada, the Czech, Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherland, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States.

[16] Dr. R.K. Chaubey, *supra note* 6, p. 903

 [ISSN 2581-5369]

the Protection of Privacy' with objectives 'to develop guidelines on the basis of rules governing the trans border flow and the protection of personal data and privacy, in order to facilitate the harmonization of national legislation'.[17] These guidelines were drafted in 1979 and adopted in 1980. These guidelines are basically recommendations to countries to adopt good data protection practices in order to prevent unnecessary restrictions on transborder data flows.[18] The OECD guidelines consist of eight basic principles which are as follows:

1) **Collection Limitation Principle:** There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.[19]

2) **Data Quality Principle:** Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.[20]

3) **Purpose Specification Principle:** The purposes for which personal data are collected should be specified not later than at the time of 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.[21]

4) **Use Limitation Principle:** Personal Data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Principle 3 except: (a) with the consent of the data subject or (b) by the authority of law.[22]

5) **Security Safeguards Principle:** Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.[23]

6) **Openness Principle:** There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available

[17] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, available at https://bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/oecd_fips.pdf, (last visited on 6/5/2023)
[18]Dr. R.K. Chaubey, *supra note* 6
[19] Paul De Hert, Ronald Leenes and Ors., Computers, Privacy and Data Protection: an Element of Choice, 150 (New York, Springer Netherlands, 2011)
[20] Robert Walters and Marko Novak, Cyber Security, Artificial Intelligence, Data Protection and the Law, 81 (Springer, Singapore, 2021)
[21] G.K.Gupta, Introduction to Data Mining with Case Studies 473 (PHI Learning, New Delhi, 2014)
[22] Daniel J.Solve and Paul M.Schwartz, Information Privacy Law 1173 (Wolters Kluwer, Netherland, 2022)
[23] Danierl J.Solve and Paul M.Schwartz, EU Data Protection and the GDPR 5 (Aspen Publishing, United States, 2020)

 [ISSN 2581-5369]

of establishing the existence and nature of personal data and the main purposes of their use, as well as the identity and usual residence of the data controller.[24]

7) **Individual Participation Principle:** An individual should have the right: (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; (b) to have communicated to him, data relating to him; (c) to be given reasons if a request made under sub-paragraphs (a) and (b) is denied and to be able to challenge such denial; and (d) to challenge data relating to him and if the challenge is successful. To have the data erased, rectified, completed or amended.[25]

8) **Accountability Principle:** A data controller should be accountable for complying with measures which give effect to the principles stated above.[26]

The OECD guidelines represent an attempt to balance the conflicting priorities of data protection and the free flow of information. The most fundamental limitation of these guidelines is that they have no legal force. They are not embedded in any Convention. Moreover, the open textured nature of the guidelines means that they can serve only as a loose framework for the harmonization of national laws.[27] Although electronic progress may have changed things substantially, it is difficult to argue with any of these eight principles. They have been set out by the OECD as guidelines for nations to legislate upon and achieve international harmony of principles.[28]

(B) Council of Europe Convention

Unlike the OECD, which is essentially concerned with the economic development of its member States, the Council of Europe has a broader political mandate. In 1968, the Parliamentary Assembly of the Council expressed concern over the adequacy of European Convention on Human Rights in securing privacy protection in the context of information technology.[29] In 1976, a Committee of Experts on Data Protection was established to prepare a Convention on the protection of privacy in relation to data processing abroad and trans frontier data processing. In April 1980, the text of the Convention was finalized, and opened for

[24] OECD, Privacy Online: OECD: OECD Guidance for Economic Co-Operation and Development 52 (OECD Publishing, Washington, 2003)
[25] Graham William Greenleaf, Asian Data Privacy Laws 504 (Oxford University Press, United Kingdom, 2014)
[26] Prof. Vimlendu Tayal, Cyber Law, Cyber Crime, Internet and E-commerce 34,35 (Bharat Law Publications, Jaipur, 2011)
[27] Faizan Mustafa, Emerging Jurisprudence of Right to Privacy in the Age of Internet, Collection and Transfer of Personal Data, KULR, Vol. 9, 2005, p. 53
[28] Nandan Kamat, Law Relating to Computers, Internet and E-Commerce: A Guide to Cyber laws and the Information Technology Act 306 (Universal Law Publishing Co., Delhi, 4th edn., 2009)
[29] Faizan Mustafa, *Supra Note* 27, p.53

 [ISSN 2581-5369]

signature on 28th January 1981. The Convention came into force in October 1985 upon ratification by five countries[30] and in total forty-one members of the Council of Europe have signed the Convention.[31] The Convention set forth the data subject's right to privacy, enumerates a series of basic principles for data protection, provides for transborder data flows and calls for mutual assistance between parties to treaty including the establishment of a consultation committee and a procedure for future amendment to the Convention. Two exceptions are permitted. One is where the first party gives special protection to a particular category of data and the second does not. The other is where the data are to be re-exported to a non-convention State.[32]

(C) European Union Directive

The European Parliament and the Council of the European Union passed the Data Protection Directive with an aim to establish a regulatory framework to protect privacy through meeting three stated objectives. The objectives include: protection of the rights of the rights and freedoms of individuals regarding the processing of personal data, harmonization of data protection standards throughout Europe and to limit movement of data to those countries outside Europe that do not have adequate levels of protection. The Directive aimed at facilitating the development of electronic commerce by fostering consumer confidence and minimising differences between member States data protection rules. The Directive requires EU member States to adopt national legislation ensuring privacy protection if they wish to participate in the free flow of information within the European Union. Under the Directive, data subjects are granted a number of important rights and may appeal to independent national authorities, if they consider their rights are not being respected.[33]

The E.U. Directive establishes strict rules about whether and how a controller may transfer personal data from the E.U. to a non-E.U. country. Art.25 states that E.U. Member States should prohibit the transfer of personal data that will undergo processing in a third country if that country fails to provide 'an adequate level of protection'.[34] The E.U. Directive does not define what constitutes an "adequate" level of protection, but it indicates that all circumstances surrounding the transfer, including the laws in force in the third country, must be considered by the supervising authority in making a determination about adequacy.[35] The E.U. Directive

[30] Sweden, Norway, France, Federal Republic of Germany and Spain
[31] S.K.Verma and Raman Mittal,, Legal Dimensions of Cyberspace 204 (Indian Law Institute, New Delhi, 2004)
[32] Faizan Mustafa, *Supra Note* 27, p. 54
[33] Dr.Vimlendu Tayal. *Supra Note* 26, p. 39
[34] Art.25 of the Directive is compatible with the General Agreement on Trade in Services (GATS, Art. XIV), which recognises the protection of personal data as a legitimate reason for restricting the free movement of services.
[35] Singh Dharamveer, The Oursourcing of Legal Services (Promoculture-Larcier, Luxembourg, 2015)

 [ISSN 2581-5369]

further enunciates a new concept called the "Safe Harbour", approach. The E.U. Directive states that in order to do business with E.U. Member States, a country should represent that it has in place an "adequate" level of data privacy protection. Any legislation passed by the said country will have to meet the E.U. standard. If there are no proper legislations in place, then the country will have to enter into a "Safe Harbour" agreement with the E.U. India also subsequently adopted this standard regarding other countries.[36]

(D) Protection of Privacy under British Data Protection Law

In recent years, in the UK several steps have been taken with regard to data protection. The Data Protection Act, 2018[37] (DPA) is a United Kingdom Act of Parliament. It is the main piece of legislation that governs protection of personal data in the U.K. The said Act seeks to empower individuals to take control of their personal data and to support organizations with their lawful processing of personal data.

But way back in 1961, a Right to Privacy Bill was introduced. This Bill marked the beginning of a 23 year history which finally led to the successful passage of the Data Protection Act, 1984. In May 1970, a Committee on Privacy was appointed under the Chairmanship of Kenneth Younger. The Younger Report was completed and presented to the Parliament in July 1972. In response to the Younger Report, the government promised a White Paper. However, it was three years before the White Paper, Computers and Privacy (Cmnd 6353) was presented to Parliament in December 1975. In it the government accepted the need for legislation to protect computer-based information. The government felt that computers posed a special threat to individual privacy. The government also issued a second White Paper, entitled Computers: Safeguards for Privacy (Cmnd 6354), which agreed with the comments made by the Younger Report. The creation of a Data Protection Authority was also proposed, to supervise the legislation and ensure that appropriate safeguards for individual privacy were implemented. The government came with a third White Paper (Cmnd 8539) in 1982 and the Data Protection Act of 1984 received Royal Assent on 12th July 1984. The Act became operational on 11th November 1987, to comply with its obligations to implement EU Directive 95/46/EC, the UK came out with the Data Protection Act, 1998, which received Royal Assent on 16th July 1998.[38] The Data Protection Act, 1998 was concerned with personal data.[39] Compliance with the Act is overseen

[36] *Ibid*

[37] The Act came into force on 25th May 2018. The Act updates data protection laws in the UK, supplementing the General Data Protection Regulation (EU) 2016/679 (GDPR), implementing the EU Law Enforcement Directive (LED), and extending data protection laws to areas which are not covered by the GDPR or the LED. It provides a comprehensive package to protect personal data and replaces the Data Protection Act, 1998.

[38] Dr. R.K.Chaubey, *supra note* 6, pp. 909,910

[39] 'Personal data' consists of data that relates to a 'living individual' who can be identified from that data, or

by an independent government authority, the Office of the Information Commissioner (OIC). The objective of the Act is to give individuals the right to know what information an organisation holds about them and to provide a framework to ensure personal information is handled properly.[40] The Act was enacted for implementing the European Union, Data Protection Directive. This is the key to the issue of internet privacy in Great Britain. This form of legislating has been backed up by court decisions in a number of sensitive matters.

But the U.K. government has entered the world of cyber-regulation with a tough stance. The Trade and Industry Regulations allow the bosses access to staff calls, e-mails and Internet activities without the employee's knowledge for a wide variety of reasons. 'Routine access to business communications' in the Regulations includes monitoring standards of service and training, combating crime and unauthorized use of company systems. Welcomed as a 'legitimate business need by the industries, it is the lack of consent and the vagueness of 'unauthorized usage' that have civil liberties groups and unions up in arms. They argue that these rules conflict with two things- a recent Data Protection Commission code on surveillance, which emphasizes consent and the guarantee in the new Human Rights Acts, according to which everyone has the right to privacy for correspondence. Other countries such as Germany and Austria, in this regard depend more on a workplace consensus and Scandinavian countries demand consent before undertaking electronic surveillance.[41]

(E) Data Protection Laws in United States

A series of major security breaches at companies with sensitive personal information has sparked significant attention to the problems with privacy protection in the United States. Currently, the privacy protections in the US are riddled with gaps and weak spots. Although most industrialized nations have comprehensive data protection laws, the US has maintained a sect oral approach where certain industries are covered and others are not. In particular, emerging companies known as 'commercial data brokers' have frequently slipped through the cracks of the US Privacy Law.[42]

Currently, the collection and use of personal data by business and government is spinning out of control. An entire industry devoted primarily to processing and disseminating personal

information in the possession of the data user. 'Data' includes information processed by computers, 'relevant filing systems' and 'accessible records'.

[40] Mike Caradi, Kemp Little LLP, Communications Law Hand Book 14 (Bloomsburg Profslo and Maxwelton Hunse, West Sussex, 2009)

[41] Bosses get key to staff e-mail boxes, available at https://edition.cnn.com/2000/TECH/computing/10/24/britain.regulation/index.html (last visited on 16/05/2023

[42] Daniel J. Solove and Chris Jay Hoofnogle, A Model Regime of Privacy Protection, Vol. 5, ICFAI Journal of Cyber Law, 2006, p. 8

information has arisen and this industry is not well-regulated. Many companies brokering in data have found ways to avoid being regulated by the Fair Credit Reporting Act (FCRA), a landmark law passed in 1970 to regulate consumer reporting agencies. Increasingly, the government is relying on data-broker companies to supply personal data for intelligence and law enforcement purposes. As a result, the government is navigating around the protections of the Privacy Act of 1974, a law passed to regulate the collection and use of data by government agencies. The FCRA and Privacy Act form the basic framework that regulates a large portion of the flow of personal data but this framework is riddled with exceptions and shunted with limitation.[43] Following are the some of the federal laws in United States which cover the collection and use of personal information and consumer data:

- **The Privacy Act, 1974**

The Privacy Act is a companion to and extension of Freedom of Information Act of 1966 (FOIA). The FOIA did exempt the disclosure of personal and medical files that would constitute, 'A clearly unwarranted invasion of personal privacy". This provision was initially used to deny access to people requesting their own records. So the Privacy Act was also adopted both to protect personal information in the federal data bases and to provide individuals with certain rights over information contained in those data bases. The Act set forth some basic principles of, "fair information practice" and provided individuals with the right of access to information about themselves and the right to challenge the contents of records. It required that personal information may only be disclosed with the individual's consent or for purposes announced in advance. The Act required federal agencies to publish an annual list of system maintained by the agency that contains personal information.[44]

- **The Electronic Communication Privacy Act, 1986 (ECPA)**

The ECPA was not enacted specifically for internet. However, it is most often used for internet privacy suits. The law prohibits the unauthorized interception or disclosure of many types of electronic communications, including telephone conversations and electronic mail, although disclosure by the one of the parties to the communication is permitted. It applies both to the government and private persons and entities. Violations are subject to civil and criminal penalties.[45]

- **The Computer Abuse and Fraud Act, 1986 (CAFA)**

[43] *Ibid*, p.9
[44] Faizan Mustafa, *supra Note* 27, pp. 58,59
[45] *Ibid*, p.59

 [ISSN 2581-5369]

The CAFA also known as the anti-hacking statute prohibits unauthorized access and also prohibits exceeding any authorization. Under the CAFA one may not access the computer with authorization and to use such access to obtain alter information in the computer that the access of is not entitled so to obtain or alter. 'Protecting computer' includes any computer used in interested commerce or communications. Paragraph (5A) of the statute also prohibits the transmission of virus with the intention of causing damage to a protected computer. The violation of this statute carries both criminal and civil penalties. The damages are limited to economic process and action must be brought within 2 years of the violation or within 2 years of the delivery of the damage. This statute is often relied on in internet privacy class action suits.[46]

- **The Children Online Privacy Protection Act, 1998 (COPPA)**

The COPPA is enacted to protect the privacy of children under the age of 13 while they are net surfing. The Act depicts the data that can be collected of a child, first and last name, home or other physical address, e-mail address, telephone numbers and social security number. The Federal Trade Commission (FTC) is authorised to add other categories for information that it determines. The COPPA requires each website operator to obtain verifiable parental consent before collecting, using and disseminating any of the above data. It also provides that the websites aimed at children may not condition the participation in a game or the receipt of a price on the child disclosing personal information.[47]

- **The Video Privacy Protection Act, 1988 (VPPA)**

The VPPA was enacted to protect the privacy of consumer rental and purchase of videos. Although the law did not contemplate the internet, its language is sufficiently broad to include internet video transaction also. The Act applies to any person, engaged in the business of rental, sale or delivery of pre-recorded video cassette tape or similar audio materials. The statute prohibits the disclosure of purchase or viewing history records of individual consumers without their informed written consent in advance of disclosure, with certain exceptions. The statute may create legal risk for companies streaming video for a fee over the internet. Disclosure of consumer data could leave these companies open to individual or class action law-suits. The Act provides for statutory and punitive damages.[48]

- **The Electronic Fund Transfer Act, 1978 (EFTA)**

[46] Karnika Seth, s*upra note* 8, pp. 396,397
[47] Vimlendu Tayal, *supra note* 26, p. 37
[48] Karnika Seth, *supra note* 8, p. 397

 [ISSN 2581-5369]

The EFTA requires institutions which deal with electronic banking services to inform their consumers of the circumstances under which automated bank account information will be disclosed to third parties in the ordinary course of business. The violators are subject to civil and/criminal penalties. The Act is enforced by the Federal Revenue Board.[49]

- **The Right to Financial Privacy Act, 1978 (RFPA)**

The REPA mandates that the federal government preset proper legal process of 'formal written request' to inspect an individual's financial records kept by a financial institution (including credit card companies) and gave simultaneous notice to the consumers to provide him/her with the opportunity to object. It provides for civil liability.[50]

- **The Federal Fair Credit Reporting Act, 1971 (FCRA)**

Enacted in 1970, FCRA limits the purposes for which a 'consumer credit report' covers a wide variety of information, including information relating to personal characteristics, mode of living and character. Failure to comply with the FCRA is made a violation of Sec. 5 of the FTC Act and can result in damages, civil penalties and in some cases, criminal liability.[51]

- **The Cable TV Privacy Act, 1984**

When the US Congress passed the Cable TV Privacy Act of 1984 to protect the viewing history of individual consumers, no one contemplated that people would receive internet access through their cable TV. Nevertheless, the Act provides that a 'cable operator cannot collect personally identifiable information without the prior written or electronic consent of the subscriber concerned. This prohibition is particularly strict, because, while other statutes limit disclosure of personal data, this statute prohibits the collection of any data whatsoever without prior written permission. The consumer must 'opt in' prior to any data collection. Further, even if the consumer consents to data collection, the cable company may not disclose the data to a third party without the consumer's express written consent. It is unclear how these restrictions will affect cable operators that supply internet access.[52]

- **The Health Insurance Portability and Accountability Act, 1996 (HIPAA)**

The HIPAA is an omnibus privacy Act for medical records that mandates the establishment of privacy protections for health care information. The HIPAA requires each person or entity who maintains or transmits heath information to maintain reasonable and appropriate administrative,

[49] Faizan Mustafa, *supra note* 27 p.59
[50] *Ibid*
[51] Karnika Seth, *supra note* 8, p. 398
[52] Rodney D. Ryder, Guide to Cyber Laws 460 (Wadhwa, Nagpur, 3rd edn., 2007)

 [ISSN 2581-5369]

technical and physical safeguards to (a) ensure the integrity and confidentiality of the information; (b) protect against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized uses or discloses of the information; and (c) ensure compliance by the officers and employees of such person or entity.[53]

In the US, apart from the protections provided by the Federal-States, State statutes protect an individual's informational privacy. A number of States have consumer protection and fraud laws which apply in many cases to breach of a privacy and wrong practices data-collection.[54] Identity theft is another serious privacy invasion in today's society. It covers when someone gathers enough personal information on some other individual to assume that person's identity. Often, the criminal will use internet to learn personally identifiable information about the victim, such as his/her name, address, social security number, mother's maiden name etc. With this information, the criminal will apply for credit cards using the victim's identity and purchase goods at will, leaving the victim to pay the bill. At present there are no significant laws against this form of identity theft. In view of the terrorist attacks of 11th Sept. 2001, the U.S. has introduced new stringent legislation to protect security.[55]

III. Privacy and Data Protection Law in India

Unlike the United States or the European Union, India has not yet enacted a separate legislation on privacy. There has been an increased concern in India about the impact of data protection laws enacted in other countries. Information technology has always been stalked by the perennial fear of invasion of privacy. This is primarily due to enormous potential of modern computer technology and its allied systems like internet to sneak into personal information. Affording protection to personal information as data at every step from collection, storage to dissemination brought in data protection laws. Data protection thus got intrinsically fused with the concept of cyber-privacy.[56] Protecting one's privacy means protection of right to control how personal information is collected and promulgated.[57] Protection of privacy also includes protection against identity theft or the use of an individual's personal information for fraudulent

[53] Karnika Seth, *supra note* 8, p. 399

[54] For instance, Virginia State has included the data collected over the internet in its Privacy Protection Act. Any company that collects data by way of internet may face liability in any jurisdiction wherein the internet is available under any or all of these rules.

[55] The Anti-Terrorism Act, 2001 broadens the power of law enforcement agencies. They only have to state to a judge that they are seeking information in connection with a terrorist investigation on order to obtain records. The Act however provided a Sunset clause for a review in Dec. 2005

[56] Aravind Menon, The C-Laws 359 (Swamy Law House, Kochi, 1st edn., 2011)

[57] S.K.Verma and Raman Mittal, *supra note* 31, pp. 209,210

 [ISSN 2581-5369]

purposes.[58]

The subject matter of data protection in India has been dealt with by the Information Technology Act, (ITA) 2000,[59] but not in an exclusive manner.[60] However, there are other statutes which provide some safeguards to the lack of explicit legislation. The Recovery of Debts Due to Banks and Financial Institutions Act, 1993, codifies India's tradition of maintaining confidentiality in bank transactions. Privacy in telecommunications is regulated by the Telecom Regulatory Authority of India (TRAI). The Common Charter of Telecom Services for adoption by all Telecom Service providers stipulates that "all Service Providers assure that the privacy of their subscribers (not affecting the national security) shall be scrupulously guarded".[61] Additionally, according to the Credit Information Companies (Regulation) Act, 2005, credit information pertaining to individuals in India has to be collected as per privacy norms enunciated in the applicable regulations. Certain older laws are also relevant. The Indian Contract Act, 1872, offers an alternative solution to protect data as Indian companies acting as 'data importers' may enter into contracts with 'data exporters' to adhere to a high standard of data protection. The Specific Relief Act, 1963, provides preventive relief in the form of temporary and perpetual injunctions in order to prevent the breach of an existent obligation, whether expressly or by implication. However, the outcomes, though, depend on judicial interpretation. The Indian Telegraph Act, 1885, recognizes privacy as a right but the government has the power to intercept communication for national security.[62]

The IT Act, 2000 talks about unauthorized access, damage to computer through computer contaminants, hacking, breach of privacy and confidentiality and publishing false digital signature certificate for fraudulent purposes.[63] An individual can do very little about these

[58] Robert Newman, Security and Access Control Using Biometric Technologies 324 (Cengage Learning, Boston, 2009)

[59] In order to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication and also to give effect to the Modern Law on Electronic Commerce adopted by the UN Commission on International Trade Law, Indian Parliament has passed the Information Technology Act, 2000

[60] The IT Act, 2000 provides for civil liability in case of data theft, computer database theft, and privacy violation. Sec.43 of the Act covers instances such as: (a) computer trespass, violation of privacy, etc.; (b) unauthorised digital copying, downloading and extraction of data, computer database or information and theft of data held or stored in any media; (c) unauthorised transmission of data or programme residing within a computer, computer system or computer network (cookies, spyware, GUID or digital profiling are not legally permissible); (d) data loss, data corruption, etc.; (e) computer data or computer database disruption, spamming, etc.; (f) denial of service attacks, data theft, fraud, forgery, etc.; (g) unauthorised access to computer data or computer databases; and (h) instances of data theft.

[61] Privacy and Human Rights Report, available at http://www.worldlii.org/int/journals/EPICPrivHR/2006/PHR2006-Republic-13.html (last visited on 10th April 2023)

[62] Subhajit Basu, Policy-Making, Technology and Privacy in India, Vol.6, Indian Journal of Law and Technology, 2010, p. 82

[63] S.K.Verma and Raman Mittal, *supra note* 31, pp. 209,210

offences. Sec.72 of the Act entitled "Penalty for breach of confidentiality and privacy" directly deals with 'confidentiality' and 'privacy' of individuals.[64] This section is narrow in scope as it is targeted only towards persons empowered under the Act. It means that provision of this section apply only to the officials who are authorised to collect data under this Act. In its application, this section would be extremely limited since it covers offences only by the authorities such as Adjudicating Officers, members of the Cyber Regulations Appellate Tribunal (CRAT)[65] or Certifying Authorities under the Act.[66]

Sec.43 also provided penalties for unauthorized access to a computer system, unauthorized extraction of information from a computer resource.[67] Although the IT Act, 2000 attempts to address the issue of protecting privacy rights, it fails to meet the breadth and depth of protection that the E.C. Directive mandates as it only protects privacy rights from government action. It is unclear whether such protection extends to private actions. Furthermore, unlike the E.C. Directive which imposes liability on each participant within the chain of command of the data who failed to protect the sanctity of the data, existing Indian laws only prosecute those individuals who directly violate laws related to computer systems. Companies or individuals are exempted from liability for breaches of data privacy unless such violations were made knowingly.[68] Moreover, unlike the E.C. Directive which protects against data breaches by limiting data collection and use, the Indian laws do not specify conditions under which data can be collected and used.[69]

It had become increasingly evident that the IT Act, 2000 did not have suitable privacy and data protection provisions, and so the Indian government had appointed an Expert Committee on Cyber Laws whose role was to suggest amendments. The Committee proposed the following: (i) a new Sec.43(2) relating to the handling of sensitive personal data or information with

[64] Sec.72 of ITA reads: "Save as otherwise provided in this Act or ay other law for the time being in force, if any person who in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such 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.

[65] Sec.48 of the ITA provides for the establishment of the Tribunal. The Central Government is authorised to issue a notification for the establishment of one or more appellant tribunals. The Central Government also lists all of the subjects and locations that come under the Tribunal's jurisdiction in the announcement.

[66] S.K.Verma and Raman Mittal, *Supra Note* 31, p. 210

[67] Sec.43 of the ITA states, if any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network (a) accesses or secures access to such computer, computer system or computer network or computer resource; (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 shall be liable to pay damages by way of compensation to the person so affected.

[68] Sec.79 of ITA provides for Exemption from liability of intermediary in certain cases

[69] Subhajit Basu, *supra note* 62, p. 83

 [ISSN 2581-5369]

reasonable security practices and procedures thereto; (ii) gradation of severity of computer related offences under Sec.66, committed dishonestly or fraudulently and punishment thereof; (iii) fine-tuning of Sec.72(1); (iv) additional Sec.72(2) in relation to breach of confidentiality with intent to cause injury to a subscriber; (v) language of Sec.66 pertaining to computer related offences to be revised in order to be in line with Sec.43 related to the penalty for damage to computer resources. The IT Amendment Act, 2008, was enacted to set the ball rolling in addressing the lacuna of data protection laws in the country through Sections 43A[70] and 72A.[71] The Amendment Act sought to rectify the many deficiencies which had been noticed with the enactment of the application of the enactment. The amendment sought to make the I.T. Act, 2000 a self sufficient Act with respect to internet behaviour.[72]

The Information Technology Act, 2000 (as amended) now requires companies to maintain reasonable security practices, and procedures as to sensitive personal data or information, but does not define the phrase 'reasonable security practices and procedures.' As understood from the section 43A, reasonable security practices and procedures are to be determined as per the following manner: "as defined between the parties by mutual agreement or as specified in any law for the time being in force or to be specified by the Central Government in consultation with such professional bodies or associations as it may deem fit". However, till date there is no law specifying reasonable security practices and procedures, nor has the Central government defined the security practices and procedures to be implemented in order to protect vital data. In the absence of such defined security practices and procedures, it is open for the parties to enter into agreements and lay down their own methods to protect their sensitive information and section 43A not only provides the freedom for doing so but also penalises any breach of

[70] Sec.43A reads as follows: 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. Explanation: For the purposes of this section (i) body corporate means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities; (ii) reasonable security practices and procedures means security practices and procedures designed to protect such information from unauthorised access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit; (iii) sensitive personal data or information means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

[71] Sec.72A states, "any person, including an intermediary, while rendering any services under a lawful contract, is required to act as per the terms of its contract and is under an obligation not to disclose any personal information that could cause wrongful loss or wrongful gain to any person. The breach of this duty is punishable with imprisonment for a term which may extend to three years or with fine upto five lakh rupees or both.

[72] Apar Gupta, Balancing Online Privacy in India, Vol.6, Indian Journal of Law and Technology, 2010, P. 54

 [ISSN 2581-5369]

such contractual obligations.[73]

With the advancement of technology, with every passing moment, even the new ITA seems obsolete. It is stated that sometimes the officials transgress their authority and enter the private domain of the people thus infringing their privacy. The Research and Analysis Wing (RAW) had access to bugging, surveillance and counter surveillance equipment. A variety of devices can be used by an investigating agency, like, E-Logger,[74] GSM Monitor,[75] Laser Ear,[76] E-mail interceptor,[77] Spy Cavities.[78] However, the increased use of these devices has definitely increased the vulnerability of a person, and the only check on this is the Controller appointed by the Government of India under the ITA. If the Controller is convinced himself that the interception is required then he may grant the permission for the same. The ITA also provides for a list of reasons, which are not exhaustive, under which the Controller can grant such permission.[79]

The IT Act has come out with the concepts of 'cryptography' and 'digital signature'. While cryptography is a science of encryption, the purpose of digital signature is to identify the originator of a message or electronic record. In the world of e-commerce, creating e-documents that are legally acceptable involves a high degree of technological perfection. For this it requires a hierarchically organised Public Key Infrastructure (PKI) where Trusted Third Parties (TTPs) or Certification Authorities (CAs) have to play a significant role. The concepts of cryptography and digital signatures measures ensure privacy over the internet, but to the government, it represents a legitimate security threat. The IT Act puts some restrictions on cryptography, through the Controller of Certifying Authorities (CCA), under Sec. 69(1) of the Act.[80]

The right to transmit an encrypted message is viewed as an integral part of right to privacy emanating from Art. 21 of the Constitution and in such cases privacy can be restricted only by

[73] Subhajit Basu, *supra note* 62, p. 84

[74] E-Logger is a computer come that is sent as an e-greeting to a target. It will pick up passwords, read all files and capture all key-strokes of targeted computer.

[75] GSM Monitor automatically tracks targeted cellular phones round-the-clock. Sophisticated GSM gateways track underworld callers whose voice samples are fed in systems.

[76] Laser Ear picks up vibrations created by speech and converts them into electric signals to reproduce conversations by hitting infra red rays on the window of a room.

[77] E-Mail interceptor: a special software allows intelligence agencies to capture e-mails and voice mails using about 2,00000 key words at India's Internet and telephone gateways. This is passive tracking with no human involvement.

[78] Spy Cavities are hidden cone shaped metal cavities in walls which pick up sounds which can be recreated.

[79] Sec. 69(1) of ITA provides that. "if the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

[80] *Ibid*

 [ISSN 2581-5369]

a "procedure established by law". But question arises, whether the procedure under Sec. 69 is similar to that to curb the right to privacy. The content of the Sec. 69 is similar to that of the Sec. 5(2) of the Telegraph Act, 1885[81], that came up for discussion in the PUCL[82] case. In this case, the safeguards formulated by the Supreme Court are remarkably similar to the safeguards devised by the OECD. The only exception that is found in the OECD guidelines is that the person who is the subject of investigation should be consulted before any kind of action is taken. All these procedures and safeguards provide a balance regarding exercising right to privacy and protection of national interest. But Sec. 69 of the IT Act leaves complete discretion in the hands of the Controller, hence, procedures in this section seems inadequate.[83]

Computer data changes moment by moment and is invisible to the eye. On the one hand the technologies of cryptography and steganography accord protection to privacy but on the other hand the same technologies can pose problems to law enforcement agencies when it comes to proceeding against subversive activists. Cryptography and steganography and recovery of deleted files are the challenges which law enforces will have to tackle. Proper guidelines have to be developed and prescribed for in these areas and for searches and seizure of information which make a balance between individual's right to privacy and the rights of law enforcement agencies.[84]

Sec. 69A also allows blocking of certain websites if their content is of such nature as described in Sec. 69. This provision is in conformity with the reasonable restrictions that are envisaged to be imposed on fundamental rights guaranteed under the public order, national security, sovereignty and allied interests. Further, Sec. 69B empowers Central Government to authorize any agency of the government to monitor and collect traffic data, or information generated, transmitted or received or stored in any computer resource in order to enhance cyber security and for identification, analysis and prevention of intrusion of computer contaminant. From the

[81] Sec. 5(2), Indian Telegraph Act, 1885 states: "On the occurrence of any public emergency, or in the interest of public safety, the Central or a State Government or any other officer specially authorized in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order".

[82] *People's Union for Civil Liberties v. Union of India* (1997) 1 SCC 301

[83] Shaymkrishna Balganesh and Neelanjan Maitra, Cryptography, Privacy and National Security Concerns, in Nandan Kamath (ed.) Law Relating to Computers, Internet and E-Commerce-A Guide to Cyber Laws and the IT Act, 2000 389-391 (Universal Law Publishing Co. Pvt. Ltd., New Delhi 2000)

[84] Dr. Neelotpal Deka, Cyber Privacy, available at https://www.academia.edu/7046569/Cyber_Privacy (last visited on 20th April 2023)

 [ISSN 2581-5369]

stand-point of data protection, the IT (Amendment) Act, 2008 introduces the distinction between 'contravention' and 'offence' by introduction of the element of mens rea for an offence.[85]

The fact that cannot be ignored here is that while in a case of privacy infringement by a State or an instrumentality of the State, an infringement action can be brought under Art. 21 of the Constitution, there is no remedy available if such an infringement is committed at the hands of a private individual. For such an infringement no expensive devices and equipments are required. As regards the friendly computers, it can infringe a person's privacy by sending out a lot of information about him to third parties. A software programme about the name of Spybot.gen downloaded on a computer's hard drive has the power to read MS Word documents and send contents back to its originator, or to an accomplice. Also hacking and spoofing are words not unknown to all. Sec. 66 of the ITA has defined hacking and the impact of such hacking can be best when a website is defaced.[86] The hacking can be committed only if the person has the intent or knowledge of committing the same.[87]

The foundation for a comprehensive legislation for the protection of data in India was laid down in the famous case *K.S.Puttaswamy v. Union of India*[88], in which the Supreme Court recognised 'privacy' as intrinsic to the right to life and liberty, guaranteed by Art.21 of the India Constitution. The Court held that, this case is not only the basis of establishing a prohibition against privacy-violative State action but also forms a basis for the State's mandate to regulate private contracts and private data sharing in the interest of individual privacy. Subsequent to the judgment, the Sri Krishna Committee was established and the said Committee came out with the Draft Personal Data Protection Bill, 2018. After incorporating the amendments pursuant to industry and stakeholder feedback, the Ministry of Electronics and Information Technology tabled the Personal Data Protection Bill 2019 (PDPB) in the Lok Sabha. On the same day, the Lok Sabha passed a motion to refer the PDP Bill, 2019 to Joint Committee of both the Houses of Parliament. Due to delays caused by the pandemic, the Joint Committee on the PDP Bill, 2019 submitted its report on the Bill after two years in December 2021. The report

[85] Secs. 43 and 66 as amended by the IT (Amendment) Act, 2008. Sec. 43 prescribes punishment by way of compensation for unauthorized access to a computer, downloading or extraction of data, introduction of contaminants, damage or disruption to a computer for deletion or alteration of data and Sec. 66 prescribes punishment upto three years of imprisonment and fine upto rupees five lakh if these activities are committed with mens rea.

[86] Sec. 66 of ITA states, "Whoever with the internet to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking".

[87] Rachika Agarwal, Privacy and Technology are Indian Laws catching UP?, Vol.19, Lawyers Collective, 2004, p. 18

[88] (2017) 10 SCC 1

 [ISSN 2581-5369]

was accompanied by a new draft Bill, namely, the Data Protection Bill, 2021 that incorporated the recommendations of the JPC. However, in August 2022, citing the report of the JPC and the extensive changes that the JPC had made to the 2019 Bill, the government withdrew the PDP Bill.

Thereafter, in November 2021, the JPC finally submitted its revised report and draft of the Bill. The PDPB was renamed as the Data Protection Bill 2021 (DPB) and it brought in various significant changes. An important change was the expansion of the scope of the law to cover not only personal data, but non-personal data as well. The DPB also introduced stringent data breach reporting requirements, regulation of hardware manufacturers, enabling a certification mechanism for all digital and devices to mitigate data breaches and the additional compliance measure of consulting the Central Government for cross border transfer of sensitive personal data. The DPB also provided for a phased implementation wherein the Central Government may notify different dates for enactment of different provisions. Unfortunately this new version of Bill attracted strong criticism and pushback from various stakeholders, including from JPC members as well as from domestic and international business houses for inter alia being more focused on the protection of State interests rather than being designed for the protection of data and privacy of individuals.

The Union Government has released a revised personal data protection bill viz., the Digital Personal Data Protection Bill, 2022. The new Bill will be tabled in the Monsoon Session of the Parliament in July 2023. The new Bill provides for significant concessions on cross-border data flows, in a departure from the previous Bill's contentious requirements of local storage of data within India's geography. Further, it offers a relatively soft stand on data localization requirements and permits data transfer to select a global destination which is likely to foster country to country trade agreements. The Bill also recognizes the data principal's right to postmortem privacy (Withdraw Consent) which was missing from the PDPB 2019 but has been recommended by the JPC.

IV. Conclusion

Thus it can be said that, the comprehensive European Union Directive on Data Privacy plays an important role in the protection of privacy. The E.U. Directive is a broad data protection law that instructs its member States to establish a legal framework to protect the fundamental right to privacy with respect to processing personal data that has extraterritorial. Privacy is individual as well as social value. It is undoubtedly invaded everywhere at every moment due to the application of scientific and technological advances. Invasion of privacy is more in cyber space

 [ISSN 2581-5369]

though it is invisible. It has become very difficult to keep confidential information, communications anonymity etc. In India the law lags behind the digital revolution.

*****

 [ISSN 2581-5369]