Page 1060 - 1159 **DOI:** *https://doij.org/10.10000/IJLMH.117592*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 7 | Issue 3

2024

Right to Privacy in Digital Era: The Privacy Concern Surrounding AI and it's Potential Impact on Personal Data

HARSHITA SINGH[1]

ABSTRACT

Even with the adoption of legal and protection, violation of privacy remains a concern. Privacy denotes a state of life, free from unreasonable interference. It ensures everyone a life to live with one's own choice. The desire for privacy is a common criterion among human beings. Hence, privacy is not simply an absence of information about us in the mind of others; rather it is the control we have over the information about ourselves! The demand for privacy is the basic human right by virtue of being human and has continued for ages since the inception of human civilization. In the present state-of-art development, the level of consciousness and awareness of people has increased a lot and hence the protection of privacy has become a major concern with the advancement of technology. With the advent of globalization, information and communication technology has reached great heights. Nonetheless, the world has turned into a smaller place where people can gather any information around the world by sitting in one place. On one hand, it can never be denied that the internet and communication development has made our lives much easier, but on the other hand, they carry a great threat to our privacy. . As has been already mentioned above, the quest for privacy among the people began since early societies. The right to privacy gained prominence during the development of the Common law period. During that time, the concept of privacy was considered only in terms of property. As such, violation of privacy resulted in simple torts such as, trespass, nuisance, etc., which were to be remedied by paying compensation to the injured as it is continued till today. In addition to that, privacy was dealt in accordance with the provisions of law which either dealt with land or tax, etc., in almost every country. The paper focuses upon the Right to privacy in indian perspectives as well as In the international Perspective and ends with the various dimential measures to ensuring individuals privacy at digital platforms or with usage of AI.

***Keywords**: Privacy, Human Rights, tort, Information, Common Law.*

[1] Author is a student at Amity University, Lucknow Campus, India.

 [ISSN 2581-5369]

I. INTRODUCTION

The recognition of Privacy' is deeply rooted in history and religion. Several religious Scriptures, texts, and classical write-ups recognize the importance of Privacy. There is recognition of Privacy in the Quran and in the saying of Prophet Mohammed. The Bible has numerous references to Privacy and the Jewish law has long recognized the concept of _freedom from being watched*. Fifty years ago, George Orwell, the English writer, whose fears for the loss of individual liberty dominated his novels, imagined a totalitarian state where advanced technologies would be used to monitor the people in all their endeavors. -Big Brother' would be watching us and privacy would be a thing of the paste. Orwell's fears have come true in this era of Information and Communication Revolution (ICR).

Privacy is a fundamental human right recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in many other international and regional treaties. Privacy underpins human dignity and other key values such as freedom of association and freedom of speech. It has become one of the most important human rights issues of the modem age.

Nearly every country in the world recognizes a right of privacy explicitly in their Constitution. At a minimum, these provisions include rights of inviolability of the home and secrecy of communications. Most recently-written Constitutions such as South Africa's and Hungary's include specific rights to access and control one's personal information.

(A) Statement of the Problem

Even with the adoption of legal and other protections, violations of privacy remain a concern. In many countries, laws have not kept up with the technology, leaving significant gaps in protections. In other countries, law enforcement and intelligence agencies have been given significant exemptions. Finally, in the absence of adequate oversight and enforcement, the mere presence of a law may not provide adequate protection.

There are widespread violations of laws relating to surveillance of communications, even in the most democratic of countries. The U.S. State Department's annual review of human rights violations finds that over 90 countries engage in illegally monitoring the communications of political opponents, human rights workers, journalists and labor organizers. In France, a

government commission estimated in 1996 that there were over 100,000 wiretaps conducted by private parties, many on behalf of government agencies. In Japan, police were recently fined 2.5 million yen for illegally wiretapping members of the Communist party.

 [ISSN 2581-5369]

(B) Objectives of the Study

The Primary objective of the study is to analyze the serious threat to right to privacy of individual by the Information Technology and the effectiveness of the present legal mechanism to deal with it. More specifically the objectives of the study were:

1) To make a conceptual analysis of Right to Privacy;
2) To analyze the legal protection of right to privacy at national and International level;
3) To evaluate the provisions of Information Technology Law via-a-via Right to Privacy;
4) To determine the liability of Internet Service Providers at national and International Level; 5) To examine the Cloud Computing implications on the Right to Privacy;
5) To examine the National and International Standards on Data Protection;
6) To focus on remedies against violation of Right to Privacy;
7) Lastly, to present the major findings of the study and to offer pertinent suggestions to strengthen the legal system.

(C) Significance of the Study

Although modem telecommunications technologies, such as computers, the Internet, and wireless communications provide tremendous convenience and tools for productivity they also raise numerous concerns and legal issues. These concerns and issues generate new responsibilities for system managers, new challenges for law enforcement, and new questions for individuals. One of the most critical of these legal issues is privacy.

(D) Research Methodology

The methodology adopted for the study is purely doctrinal. Various books, journals, magazines, International materials, treaties and conventions etc., have been studied for the collection of the data. Materials from various websites have been visited& used to get the latest information in analyzing the problem. Secondary data available from various sources have been used to support some conclusions and findings.

II. PRIVACY: INTRODUCTION, CLASSIFICATION, FUNCTION AND PHILOSOPHICAL BASIS

According to etymological meaning, privacy has been taken from Latin term privatus' which

 [ISSN 2581-5369]

means 'separated from the rest'. deprived of something, esp. office, participation in the government', and from 'privo ' which means 'to deprive', is the ability of an individual or group to seclude themselves or information about themselves and thereby reveal themselves or information about themselves and thereby reveal themselves selectively. 'Privacy' is concerned with a man's dignity and liberty. It is a fundamental human right guaranteed by International Laws. It has been an inalienable and integral part of human life since long. Initially, it had a very narrower scope as such thought to be included only 'right to be let alone. Later. the increasing, maturity levels of the democratic systems, rapid strides in science and technology, made its scope wider. Now the right to privacy covers many aspects such as, freedom of thought, control over one's body, identity, solitude in one's home, control over self information, freedom from surveillance. protection of one's reputation, and freedom from searches and seizures etc. The USA is the motherland of right to privacy. Privacy's origin can be traced back to an article written by Warren and Brandy published in 'Harvard Law Review' in 1890, in which the concept of Right to Privacy was discussed in detail for the first time. The concept was first proposed in December, 1890, in a Harvard Law Review article written by two young lawyers who had roomed together in Cambridge - Samuel Warren and Louis Brandeis. Brandeis would later become one of the legendary justices of the U.S. Supreme Court. Warren's family was prominent in Boston society. They threw lavish parties. Press gossips constantly festered the family and tried to spy on their parties. Warren and Brandeis published their novel idea in a Harvard Law Review essay. "Instantaneous photographs and newspaper enterprise," they wrote, "have invaded the sacred precincts and domestic life."

Once a civilization has made a distinction between the 'outer' and Inner man, between the life of the soul and the life of the body, between the viritual and the material, between the sacred and profane, between the realm of God and the realm of Ceaser, between the church and the State, between rights inherent and inalienable and the rights that are in the power of goverment to give and take away, between publi and private, between society and solitude, it becomes impossible to avoid the idea of privacy by whatever name it may be called- the idea of a private space and remain himself[2].

Privacy is the claim of individuals, groups or institution to determine for themselves when, how and to what extent information about is to be communicated to others. Right to privacy is more of an implied obligation. It is the 'right to be let alone'!. Hence, 'Right to life[3], "the Right to be

[2] Milton R. Konvitz. “Privacy and the Law : A Philosophical Preclude”, Law and the Contemporary Problems(1966).p.no 273

[3] Westin AF; Privacy and Freedom, London,1967 visited at www.privacysummersymposium.com/reading/ westin.pdf

let Alone" has emerged[4].

The concern for the Right to privacy was shown by Thomas M. Cooley at the end of the nineteenth century when the observed that privacy was synonymous with the right to be let alone. Therefore, privacy as right is the right to be left alone[5] without unwarranted intrusion by government, media or other institutions or individuals.

Thus, In common legal parlance, the right of privacy has one meaning i.e. a legal right to be left alone; the right to live life free from unwarranted publicity. In wider sense, privacy is the ability of a person to control the availability of information about and exposure of him or herself. It is related to bang able to function in society anonymously (including Pseudonymous or blind credential identification).

In the United Kingdom, The Justice Report, 1970 and The Younger committee Report, 1972 pointed out the difficulty of finding a precise and loeical formula which could either circumscribe the meaning of the word 'privacy, or define it exclusively. Each however suggested a working definition. Justice Report defines privacy as 'that area of man's life which in any circumstances, a reasonable man with an understanding of the legitimate needs of the community would think it wrong to invade.

(A) Definition of Privacy

The term "privacy" has been described as "the rightful claim of the individual to determine the extent to which he wishes to share of himself with others and his control over the time, place and Circumstances to communicate others.[6]

It means his right to withdraw or to participate as he sees fir. It also means the individual's right to control dissemination of information about himself, it is his own personal possession"[7].

In another view, privacy is a "Zero Relationship between two or more persons in the sense that there is no interaction or communication between them if they so choose"%. Right of Privacy, the right of a person to be free from intrusion into or publicity concerning matters of a personal nature called right to privacy.

Privacy is the ability of an individual or a group to keep their lives and personal affairs out of public view, or to control the flow of information about them. Privacy is sometimes related to anonymity although it is often most highly valued by people who are publicly known them.

[4] Samuel D. Warren and Louis D. Brandies, “The Right to Privacy” 4 Harvard Law Review (1890),p.no193
[5] The phrase was coined by Thomas M. Cooley in his Treastise, The Law Of Torts (2” Ed. 1888)
[6] Adam Carlyle Brenckenridge : “The Right to Privacy”(1971), Quoted in Mandhavi Divam, “The Right to Privacy in the Age of Information and Communication”(2002) 4SCC(J) 12.
[7] lbid

 [ISSN 2581-5369]

Privacy is sometimes related to anonymity although it is often most highly valued by people who are publicly known.

The simplest definition of privacy was given by Judge Thomas Cooley in Olmstead v. United States[8], he called it, "the right to be let alone". Invasion of privacy means "an unjustified exploitation of one's personality or intrusion into one's personal activity, actionable under tort law and sometimes under Constitutional law[9]"

Rubenfield defines privacy as "the right to make choices and decisions" which forms "the 'Kernel' of autonomy"[10] . However, going a step further, he introduces the concept of personhood into the doctrine by stating: "Some acts, faculties, or qualities are so important to our identity as persons and as human beings that they must remain inviolable, at least as against the State the right to privacy is a right to self definition." Thus, "where our identity or self definition is at stake, the state may not interfere" [11]

The privacy can be defined further as 'As autonomy or control over intimacies of personal identity. It can also be described as 'The Rightful claim of the individual to determine the extent to which he wishes to share of himself with other and his control over the time, place and circumstance to communicate with other. It also means the individual's right to control dissemination of information about him, it is his own personal possession'. Another author defines privacy as a "Zero relationship between two or more persons in the sense that there is no interaction or communication between them if they so choose" Judge Cooley calls it 'the right to be let alone. According to Charles Fried, 'Privacy is not simply an absence of information about other; rather it is the control we have over information about ourselves... The person who enjoys privacy is able to grant or deny access to others. Privacy, thus, is control over knowledge about oneself.' Another Miller defines privacy as a control over information. Privacy is the individual's ability to control the circulation of information relating to him. a power that often is essential to maintaining social relationship and personal freedom.

As a young Boston lawyer in 1890, U.S. Supreme Court Justice Louis d. Brandeis co wrote a landmark Harvard Law Review article titled " The Right to Privacy," advocating that "the right to life has come to mean the right to enjoy the life- the right to be let alone.""

No one shall be subjected to arbitrary interference with his privacy, family, home or

[8] Edward Shills; “Privacy : Its Constitution and Vicissitudes, Law and Contemporary Problems”,(Spring 1996) vol2 ,p.no31.
[9] 277 U.S. 438 (1928)
[10] Black’s Law Dictionary, 7th Ed. Garner Bryan visited at www.bamesandnoble.com/.../blacks-law-dictionary-bryan-garner/1 1192 accessed on 21/04/16
[11] Jeb,rubenfield-“the right to privacy”,vol.102 yale law journl,February,1989

correspondence or to attack upon his honour and reputation. Everyone to the protection of the law against such interference or attack.[12]" The recognition to Right to privacy under Universal Declaration of Human Rights set forth the basic human requirement regarding the privacy about the =lan of one's personality & for preservation of one's self respect. Therefore are certain arenas of person's life which he wish no to be interfered by anyone Lord Denning has forcefully argued for the recognition of a right to thus [13]:

(B) Classification of Privacy:

a. Intimate Privacy

According to the western view "intimacy is the sharing of information. one's action, beliefs, or emotions, which one does not share with me. This would include sexual relations, the performance of bodily Aims. family relations, and the like[14]

The individual sharing these intimate information actions, beliefs, etc. mid not favour any leakage, disclosure or exposure to their privacy. The intimate privacy generally covers the grounds of sexual intimacies, personal beliefs and such other things the society would not approve.

b. Family Privacy

A concept of family privacy can cover a wide area beginning from the privacy between a married couple, extend to a joint family living together and ending with all the blood relations of the family though they may not be living together. The social customs and the cultural background were such that the families were such that the families were auto adjusted to certain kinds of privacy and the individuals never even felt the need of intervention of law or that of any court. The safeguards were in built in the very customs themselves. There was segregation of males and females and unwritten social rules automatically created and granted privacy.

c. Social Privacy

This privacy can further be sub-divided into three categories-

i. **Political/Legal Privacy**:- In this privacy the intrusions by the government are regulated by means of law and the law in turn either gives or takes away rights to aeration liberties which will have considerable bearing on privacy. Examples-Procedure of search and seizure; Publications of news; wire-tapping; taking photography. Public nudity, sexual

[12] Cozic, "Civil Liberties, Opposing Viewpoints", Greenhaven Press, U.S.A. 1994 12 of Universal Declaration of
[13] Article 12 of Human Rights, 1948 Resolution 217A (III) of 10 er 1948
[14] De shta Kiran; "Right to Privacy under Indian law", New Delhi, deep and Deep Publication Pvt. Lail(2(111).p.35

 [ISSN 2581-5369]

relationship beyond marriage; Privacy of court proceedings etc.

ii. **Professional Privacy**:- In the case of professionals safe ground to privacy may become essentials on two scores: first is own professional privacy, and secondly, the professional privates of his clients.

General in India, lawyer, doctor, charted accountants, consultants etc. are the professionals who have the opportunity to posses knowledge about the privacy of their patrons.

In R.M. Malkanis v. State of Maharashtra, [15] the coroner's attempts to extract bribe from Dr. Adatia has been a typical case of an attempt to violate professional privacy.

In the context of modern living, professionalism has come to stay in a long and important way and hence it would adequately need and deserve all legal safeguards. By protecting professional privacy, we will be in a position to protect right to life and personal liberty.

iii. **Community Privacy**:- The concept of community privacy has a very limited field because a society is composed of conglomeration of communities and social laws general govern major aspect. But there are certain community privacy which may need intervention of law for their safeguard. A Hindu Brahmin community would not approve of a slaughter house he beef in the midst and cluster of their business and residential colony. Nor would Christians and Muslims approve of a ban on cow slaughter for them beef eating is their privacy of food and dietary habit and they would not wish to surrender this community privacy. Similarly every community can have some peculiar customs and rituals private to their own community, which they would not like to expose to public gaze or interference[16].

d. Individual Privacy

The most susceptible area is the privacy of individuals. An individual by nature at some time or the other in his doily existence craves for brief periods of privacy for mental peace, quiet, mediation, enjoyment of hobbies, cultivation of personality, both by cosmetically means as well as by rehearsals and practices such as well as by rehearsals and practices such as speech modulation, physical exercise, etc.

e. Information privacy

Data privacy refers to the evolving relationship between technology and the legal right to, or

[15] AIR 1973 SC 157

[16] MeLaren John, "An Alternative Approach to community Privacy and Open Space", Washington, University of Washington, Third Edn. (2001),p. 281

 [ISSN 2581-5369]

public expectation of privacy in the collection and sharing of data about one's self. Privacy concerns exist wherever uniquely identifiable data relating to a person or persons are collected and stored, in digital form or otherwise. In some cases these concerns refer to how data is collected, stored, and associated. It can further be divided into-

i. Financial privacy

In which information about a person's financial transactions is guarded, is important for the avoidance of fraud or identity theft. Information about a person's purchases can also reveal a great deal about that person's history, such as places they have visited, whom they have had contact With, products they use, their activities and habits, or medications they have used.

ii. Internet privacy

Is the ability to control what information one reveals about oneself over the Internet, and to control who can access that information. These concerns include whether email can be stored or read by third parties without consent, or whether third parties can track the web sites someone has Visited. Another concern is whether websites which are visited collect, store, and possibly share personally indentifiable information about users. Tools used to protect privacy on the Internet include encryption tools and anonymizing services.

(C) Genesis of Right to Privacy: Indian Scenario

The distance from the biblical garden to the statutory wilderness may have taken thousands of statutory wilderness may have taken thousands of year to traverse because it is necessary to a secure relationship between man and wife; it concretizes interpersonal relationship of love, friendship and trust. Privacy is one of the concepts which is closely connected with human dignity. There are several recent which establish it beyond doubt that disturbing mediation was considered a wrong or a sin. Lord Shiva, while in meditation, is said to have been disturbed by *Kamdev' the god of love and sex in the Indian mythology, who was burnt as punishment there of when Lord Shiva opened his third eye[17].

In matters of religious and spiritual pursuits interference or disturbance of any kind was prohibited. The following text of Rigeda clearly established the concern and awareness of privacy in the ancient India society. (one ought to build such house which may sustain and protect the inmates in all seasons and be comfortable. The passaers- by may not see the inmates not the inmates see them.)

[17] Kalidas Kumarasambhavam, 3/17,as cited in “the right to privacy: concept and evolution ”by Gaurav Goyal and ravinder kumar, Partridge publication ed. Lg 2015 p.no35

 [ISSN 2581-5369]

The Griha sutras, Arthashashtra and the epics of the Ramayan and the Mahabharata contain elaborate rules for the construction of a house so that privacy is prominently preserved. Since privacy is the essence of human beings its history begins with the history of human beings.

Historical, evidence shows that it was prevailing as a social value in every civilization. Our ancient law of Dharmashashatra also recognized the concept of privacy.

i. Privacy in Hindu Period

India has essentially been gregarious society wherein cooperation and not competition,. Society and solitude have been dominant themes of its culture and civilization.

Privacy is a value of human relation in India. The ancient law giver of the Hindus declares "Sarvas Swe Swe Griha Rajya". Which means every man is a king of his own house. The king were bound to uphold Dharma and to respect the privacy of the citizens[18]. Ancient Indian theory the privacy of knowledge based on Upanishads mind from external things and direct it inward- to make him more and more introspective so that he may get rid of his dependence on the objective world.

ii. Privacy under Islamic Law

Islamic law is a divinely ordained comprehensive system regulating public and personal matters as well. It is called "Shariah' which mean the right path. The world Islam itself means total submission and surrender to God alone. The Quran, the holy book of God revealed to the Prophet Mohammad and traditions of Prophet Mohammad are the principal sources of Islamic law[19].

Islamic law explicitly protects privacy of home a fundamental human right. The home thrives its importance as a sanctuary for the family and carries with it associations and meanings which make it particularly important. The peculiar immunity that law has thrown around the dwelling house is explicitly expressed in the famous maxim "a man's home is castle." Is a supreme and valid truth which is valued in all cultures and civilizations? The prophet Mohammed stated, if a person loose at you, without your permission and pelt with a stone and put on his eye, no guilt will be on you. In Colonial era, in India right to privacy is protected from various statutes, such as the Indian Telegraph Act, 1885, Indian Penal Code, 1860, etc. through various provisions. After the Post-Independent in India, The Constitution does not grant in specific and express terms any right to privacy as such, right to privacy is not enumerated as a fundamental right in

[18] Rigveda, Mandal 7, sukta 55, hymn 6
[19] Deshta Kiran, "Right To Privacy under Indian Law", New Delhi, Deep and Deep publication Pvt. Ltd. (2011), P.98

the constitution. However, such a right has been culled by the Supreme Court from Article-21 and several other provisions of the Constitution read with the Directive principles of State Policy. The right to privacy has now become established in India, but as part of Article 21.

III. RIGHT TO PRIVACY IN INTERNATIONAL PERSPECTIVE

In recent years right to privacy has gain much importance in international legal world. The united nation and other agency working for the protection of human rights has worked for the protection of right to privacy in digital world. Due to technological advancements the right to privacy has emerged significantly, but also due to changes in the way people, markets, and our societies function. The advancements of systems of communications for instance permits continual tracking and enable always available communications habits. Advances in information communication technology are dramatically improving real-time communication and information-sharing. By improving access to information and facilitating global debate, they foster democratic participation.

But at the same time it has become clear that these new technologies are vulnerable to electronic surveillance and interception.Recent discoveries have revealed how new technologies are being developed covertly, often to facilitate these practices, with chilling efficiency. As the UN High Commissioner has cautioned in her recent statements [September 2013 and February 2014], such surveillance threatens individual rights-including to privacy and to freedom of expression and association-and inhibits the free functioning of a vibrant civil society.[20]

(A) Privacy and Human Rights at International Level

Privacy is a human rights recognized in the UN Declaration of Human Rights, the International Covenant on Civil and Political rights and many other international and regional treaties.

Privacy underpins human dignity and other key blues such as freedom of association and freedom of speech. It has become one of the most important human rights issued in the technological era. Many countries in the world recognized a right of privacy explicitly in their constitutions. At a minimum these provisions include rights of inviolability of the home and secrecy of communication.

The Legal protections of the right to privacy in General and of data privacy in particular have various issues around the world and have different directives on data privacy. The basic right to protect an individual's privacy has been enshrined in the Universal Declaration of Human

[20] www.un.documents.net/a6 l r l 06.hitm,accessed on 08-02-16

Rights. 1948 (UDHR. 1948)[21] as follows:-

"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence. or to attacks upon his honour and regulation. Everyone has the right to protection of the law against such interference or attacks." This has also been articulated in various other International covenant and treaties under which privacy is specifically mentioned as a right[22].

1. International Covenant on Civil and Political Rights, 1966[23]

This covenant has also said about right to privacy in the above language adopted by the UDHR, 1948. It says in its Article 17 as under:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to the protection of the law against such interference or attacks. In addition, General Comment No. 16 to the ICCPR provides further specification data protection requirements under Article 17. It states, among other things, that
    - The collection and storage of personal information on computers, in data bases or other devices, whether by public or private bodies, must be regulated by law;
    - States must take effective measures to ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it;
    - Uses of this information for purposes incompatible with the Covenant must be prevented;
    - Individuals should have the right to determine what information is being held about them and for what purposes and to request rectification or elimination of incorrect information:
    - Any "interference" with these rights must only take place on the basis or law which must comply with the Covenant.

2. Convention on the Rights of the Child 1989[24]

[21] Article 12;India is a signatory to the UDHR, 1948.resso no. ail-es/3/217A
[22] Chandra umesh, "Human rights", Allahabad law agency ,I,ed. 2018 p.no 124
[23] Jaya Wickrama, Nihal, "The Judicial Application of Human Rights Law", Cambridge University Press (2002) p. 597
[24] Adopted and opened for signature, ratification and accession by United Nation General Assembly resolution 14/25 of 20 November 1989

 [ISSN 2581-5369]

Article 16-

i. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.

ii. The child has the right to the protection of the law against such interference or attacks.

3. Convention on the Rights of Persons with Disabilities, 2006[25]

Article 22 Respect for Privacy

i. No person with disabilities, regardless of place of residence or living arrangements, shall for subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence or other types of communication or to unlawful attacks on his or her honour and reputation. Persons with disabilities have the right to the protection of the law against such interference or attacks.

ii. States Parties shall protect the privacy of personal, health and rehabilitation information of persons with disabilities on an equal basis with others.

(B) Regional Level

1. American Declaration of the Rights and Duties of Man 1948[26]

Article 5. Every person has the right to the protection of the law against abusive attacks upon his honour, his reputation, and his private and family life.

Article 9 Every person has the right to the inviolability of his home.

Article 10. Every person has the right to the inviolability and transmission of his correspondence.

2. American Convention on Human Rights 1969[27]

Article 11. Right to Privacy

i. Everyone has the right to have his honor respected and his dignity recognized

ii. . 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.

iii. Everyone has the right to the protection of the law against such interference or attacks.

[25] U.N. General Assembly Resolution 61/106 (2006)
[26] Adopted by the Ninth International Conference of American States, Biogota, Colombia, 1948
[27] www.hrcr.org access on 20/11/13 at 9:50 p.m.

3. European Convention for the protection of Human Right and fundamental Freedoms, 1950 (ECHR) Article 8[28]-states

i. Everyone has the right to respect for his private and family life, his home and his correspondence.

ii. There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and freedoms of other.

iii. The convention created the European Commission of Human Rights and the European Court of Human Rights to oversee enforcement of privacy rights and have consistently and restrictions expansively and interpreted and restrictions narrowly. The Commission found in 1976.

4. Arab Charter on Human Rights 2004 [29]

i. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, or to unlawful attacks on his honour and reputation.

ii. Everyone has a right to the protection of the law against such interference or attacks. The concept of privacy differs from nation to nation in terms of the impact of culture on interpersonal relation. Indeed, the law of a nation reflects and recognizes its fundamental norms. Obviously the right of privacy has been developing in many countries of the world to meet the needs to protect the individual from unreasonable intrusions into areas of intimate concern.

The right to privacy as an independent and distinctive concept originated in the field of tort law, under which a new cause of action for damages resulting from unlawful invasion of privacy was recognized. The constitutional recognition of right of personal privacy, or more accurately, a guarantee of certain 'zones of privacy', was developed by the courts as an extension of constitutionally guaranteed rights of life, liberty and security of person[30] .

The United Nations has only focused on the human rights aspects of the use of computer technology comparatively recently. In 1989, the United Nations General Assembly (UNGA)

[28] Council of Europe Convention for the protection of Human rights and fundamental freedom (ETSNOOO5).en for signature November 4, 1950.
[29] 22 may reprinted in 12 International Human Rights Reports 893 (2005)
[30] Jaya Wickrama, Nihal, "The Judicial Application of Human Rights Law"Cambridge University Press,:02) p. 598

adopted a set of drafts guidelines for the regulation of computerized personal data files[31]. These drafts guidelines were subsequently referred to the commission of Human Right's Special Rapporteur, Mr. Louis Joint, for redrafting based on the comments and suggestions received from member government and other interested international organizations. A revised version of the guidelines were presented and adopted in 1990[32]. The guidelines are divided into two sections. The first section of these covers principle concerning the minimum guarantees that should be provided in the national legislation'. These 'principles' echo these put forward by both the council of Europe Convention and the OECD guidelines added three additional terms:

a) Principle of non-discrimination-sensitive data, such as racial or ethnic origin, should not be compiled at all.

b) 'Power to make exceptions' - justified only for reasons of national security, public order, public health and morality.

c) Supervision and sanctions'-the data protection authority shall offer guarantees of impartiality, independence vis-à-vis person of agencies responsible for processing and technical competence[33].

5. The organization for economic cooperation and development Principles

The Organization for Economic Cooperation and Development (OCED) was established in 1961, and currently comprises 30 leading industrial nations as its member. The nature of the organization has meant that interest in data protection has centered primarily on the promotion of trade and economic advancement of Members States, rather than 'privacy' concerns.

In 1963, a Computer Utilization Group was set up by the third Ministerial Meeting. Aspects of the Group's work concerned with privacy went to a subgroup, the Data Bank Panel. This body issued a set of principles in 1977. In the same year, the working Party of Information

Computers and Communications policy (ICCP), was created out of the Computer Utilization and scientific and technical policy groups. Within this body, the Data bank of Panel became the 'Groups of Government Experts on trans border Data Barriers and the Protection of 'Privacy'.

Its remit was to develop guidelines on basic rules governing the Trans border flow and the protection of personal data and privacy, in order to facilitate the harmonization of national legislation. The OECD guidelines on the protection of privacy and Trans border Flows of

[31] Resolution 44/132, on 15 December, 1969

[32] Adopted by the Commission on Human Rights, Resolution 1990/42 (6 March 1990); subsequent by the UN Economic and Social Council, Resolution 1990/38, 14th Plenary session (25 may 1990) and finally the UN General Assembly, Resolution 45/95, 68th Plenary session (14 December 19900

[33] Ian walden, "Data Protector", in Chris Reed & John Angel (eds.),Computer Law, 447-448 4th ed.,2002

personal information were drafted in 1979 and adopted in September 1980[34]. The guidelines are based, as with the council of Europe Convention, upon eight, self-explanatory, principles of good data protection practices. The guidelines are simply recommendations to countries to adopt good data protections practices in order to prevent unnecessary restrictions on Trans border data flows and have no formal authority. However, some companies and trade associations, particularly in the United States and Canada, have formally supported the guidelines.

The OECD guidelines consist of eight basic principles which are as follows:

- **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.
- **Data Quality Principle:** Personal data should be relevant to the purpose for which they are to be used, and, to the extent necessary for those purpose, should be accurate, compete and kept up-to-date.
- **Purpose Specification Principle**: The purpose 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 purpose or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- **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.
- **Security Safeguards Principle:** Personal data should be protected by reasonable security safeguards against such risk as loss or unauthorized access, destruction, use modification or disclosure of data.
- **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 of establishing existence and nature of personal data, and the main purpose of their use, as well as the identity and usual residence of the data controller.

[34] Organization for Economic Cooperation and Development , Guidelines on the Protection of Privacy and the Trans Border Flows of Personal Data, Paris. OOCED, 1980.www.oecd.org/sti/ieconomy/37626097.pdf.

A. **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

i. Within a reasonable time;

ii. At a charge, if any, that is not excessive;

iii. In a reasonable manner; and

iv. In a form that is readily intelligible to him;

(c) To be given reasons if a request made under sub-para 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.

B. **Accountability Principles**: A data controller should be accountable for complying with measures which give effect to the principles stated above. The OECD guidelines were developed to harmonize national privacy legislations and, at the same time, have much relevance and the directions may be taken by states for privacy protection.

6. European Convention on Human Rights

The council of Europe has been the major international force in the area of protection of privacy since 1968. The Council discussed in its forum whether domestic laws gave adequate protection for personal privacy in the light of modern s.cientific and technical developments and it saw insufficient protection in this area through domestic legislations.

A specialist Committee of Experts on the Protection of Privacy was subsequently asked to draft appropriate resolutions for the Committee of Ministers to adopt. In 1976, a Committee of Experts on Data Protection of privacy in petition to data processing broad and Trans frontier data processing. In April 1980, text of the Conventions was finalized. and opened for signature on 28th January 1981.

The Convention came into force of in October 1985 upon ratification by five countries, namely Sweden, Norway, France, Federal Republic of Germany ad Spain and in total forty-one members of the Council of Europe has signed the & Convention.

The right to data privacy is heavily regulated and rigidly enforced in Europe. Article 8 of the European Convention on Human Rights (ECHR) provides right to respect for one's "Private and

 [ISSN 2581-5369]

family life, his home and his correspondence", subject to certain restrictions. The European Court of Human Rights has given this Article a very broad interpretation in its jurisprudence. According to the Court's case law the collection of information by officials of the gate about an individual without his consent always falls within the scope of Articles of the state about an information for the official census, recording timerprints and photographs in a policy register. collecting medical data or details of personal identification have been judged to raise date privacy issues.

Any state interference with a person's privacy is only acceptable for the Court if three conditions are fulfilled.

1. The interference is in accordance with the law.
2. The interference pursues a legitimate goal.
3. The interference is necessary in a democratic society.

The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, the European Commission was concerned that deserving data protection legislation would emerge and impede the free flow of dista within the EU zone. Therefore the European Commission decided to harmonize data protection regulation and proposed the Directive on the protection of personal data, which member states had to transpose into law the end of 1998.

The directive contains a number of key principles which must be complied with. Anyone processing personal data must comply with the eight enforceable Principles of good practice.

They state that the data must:

- Fairly and lawfully processed
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate. Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure
- Not transferred to countries without adequate protection.

7. **The European Union**

In 1976, the European parliament's adopted a resolution calling for a directive to ensure that

Community citizens enjoy maximum protection against abuses of failures of data processing' as well as 'to avoid the development of conflicting legislation'[35]. In 1977 the Legal Affairs Committee established the Subcommittee on Data Processing and the Rights of the individual. The subcommittee, produced the 'Bayer 1 Reports' in May 1979.

The result debate in the European Parliament led or recommendations being made to the Commission and the council of Ministers concerning the Principles that should form the basis of community's attitude to data protection18. These recommendations called on the European commission to draft a directive to complement a common communications system, to harmonized the data protection laws and secure the privacy of information on individual in computer files. In July 1981, the European commission recommended that all Members should sign the council of Europe convention and seek to ratify it by the end of 1982.

A second parliament report, the 'Sieglerschidt' Report, was published in 198238. The report noted 'that data transmission in general should be placed on a legal footing and not to be determined merely by technical reason'. In July 1990, the European Commission finally published a proposed Directive on data protection. It was published as part of a package of proposal, which included a recommendation that the European Community adheres to the Council of Europe Convention on data protection 39 , a declaration applying data protection principles to Community institutions, a draft directive addressing data protection issued in the telecommunications sector!, and a draft council decision to adopt a two-year plan in the area of security for information systems. After considerable controversy and political debate at all stages of the legislative process, the general framework Directive on data protection was finally adopted by the European Parliament and council on 24 October 199543. Members states had to implement the directive by 24 October 1998. although only five managed to adopt legislation by that date.

In 1990 only eight of the (then) twelve Members states have passed data protection legislation.

(C) National level

1. United States of America

The US supreme court said that although the constitution of the USA does not explicitly mention any right of privacy, the united states courts recognized that a right of personal privacy, or a guarantee of certain 'zones of privacy' does exist under the constitution and that the roots of that

[35] Resolution on the protection of the rights of individuals in constitution with data processing ajc100, 3may 1976, p. 27 . Report on the protection of the individual in the face of the technical developments in data processing, 1979-1980 EUR. Parl. Doc (no 100) 13 (1979)

right may be found in the first amendment, in the fourth and fifth amendments, in the penumbras of the bill of rights, in the ninth amendment, and in the concept of liberty guaranteed by the first section of the fourteenth amendment and that the right to privacy is not absolute.

The need for a law to protect privacy was articulated as early as 1890 when an article titled "The Right to Privacy" was published by Warren and Brandeis this articles laid the intellectual foundations (jurisprudence) for the law on privacy.

"Recent inventions and business method call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley Calles 'the right to be let alone. Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of the home private devices threaten to make good the prediction that 'what is whispered in the closed shall be proclaimed form the house tops'. The press is overstepping in every direction the obvious bounds of propriety and of decency. Gossip is no longer the resource of the idle and of the vicious, but has become a trade, which is pursued with industry as well as effrontery. The intensity and complexity of life attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have through invasions upon his privacy, subjected him to metal pain and distress, far greater than could by inflicted by bodily injury. It is our purpose to consider whether the existing law affords a principle which can properly be invoked to protect the privacy of an individual; and, if it does, what the nature and extent of such protection is.

In this case the constitutionality of a law which prohibited the use of contraceptives was challenged. Upholding the notion of privacy, Justice Douglas held:

"Governmental purpose to control or prevent activities constitutionally subject to State regulation may not be achieved by means which sweep unnecessarily broadly and thereby invade the area of protected freedoms'46.

Roe v. Wade[36]

In this case it has been dealt that the right of an unmarried pregnant woman to an abortion. Upholding the woman's right to make that choice which affected her private life, the Supreme Court held that although the American Constitution did not explicitly mention any right of privacy, the Supreme Court itself recognized such a right as a guarantee of certain "zones or

[36] 410 US 113 (1973)

 [ISSN 2581-5369]

areas of privacy" and "that the roots of that right may be found in the First Amendment, in the Fourth and Fifth Amendments, in the penumbras of the Bill of Rights and in the concept of liberty guaranteed by the Fourteenth Amendment". The Commission also expressed its desire to protects the right of individual data subject, 'and in particular their right to privacy' (Art 1 (1). 46 Griswoldv. "Perhaps the most salient characteristic of legal protection of information privacy in the united states is its ad hoc nature, some types of information transfers are heavily regulated, while other types, seemingly no less significant to individual privacy interests, are unregulated and left to the mercies of the marketplace48.

The issue of privacy in the area of communication started to develop in the US Legislations since the late 1960s. In 1968, the US congress enacted the omnibus crime control and safe streets act, primarily focused on telephone wiretaps. Later, it was broadened to include digital electronic communication. The Electronic Communication Privacy Act, 1968 (ECPA) in the US makes it illegal to intercept or disclose private communications and provide victims of such conduct, a right to sue anyone violating his mandate.

At the same time, several legislations were enabled dealing with the online environment. Some of these Legislations are, the Fair Credit Reporting Act, 1970, the Family Education Rights and Privacy Act, 1974, the Driver's Privacy Protection, 1974, the Fair Debt Collection Practices Act, the Right to Financial Privacy Protection Act, 1980, the Computer Fraud and Abuse Act, 1986, the Telephone Consumer Protection Act 1991, the Privacy Act, 1994 and the National Information Infrastructure Protection Act, 1996.

The Federal Trade Commission (FTC) in the USA has been playing an important role in the development of a federal legal system towards the issue of information privacy. In June 1998, the FTC submitted a report to the congress, on which basis Online Privacy Protection act came into effect from April 2000. Now, intrusion into the privacy of children is allowed only after obtaining consent of parents.

The US senate judiciary committee approved hacker's bill in October 2001. It clarifies federal law enforcement authority's power to prosecute hackers. The US federal laws basically protect the privacy of financial information transmitted via telecommunications system, and in recent years, its laws deal with the online privacy.

2. **United Kingdom**

In recent years, in the U.K., several steps have been taken with regarded to Data protection. But way back in 1961, Lord Mancroft introduced a right of privacy bill, this bill marked the beginning of a 23-year history which finally led to the successful passage of 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. 10 However, it was three years before the white paper on Computers and Privacy (cmnd6353) 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 (cmnd6354), 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 (emnd 8539) in 1982 and the Data Protection Act of 1984 received royal assent on 12 July 1984. To comply with its obligations to implement EU directive 95/46/EC, the U.K. came out with the Data Protection Act, 1998, which received royal assent on 16 July 1998.

In case of Albert v. Stranges° Involved the unauthorized copying of etchings made by Queen Victoria and her husband for their private amusement. The etchings, which represented members of the Royal family and matters of personal interest, were entrusted to a printer for making impressions. An employee of the printer made unauthorized copies and sold them to the defendant who in turn proposed to exhibit them publicly. Prince Albert succeeded in obtaining an injunction to prevent the exhibition. The court's reasoning was based on both the enforcement of the Prince's property rights as well as the employee's breach of confidence. This case is widely regarded as having inspired the development of the law of privacy in the United States.

Even as late as 1991, the law in England was found to be inadequate in protecting privacy. In that year, the Court of appeal in case of Kaye v. Robertson"!

The case concerned a well-known actor who had to be hospitalized after sustaining serious head injuries in a car accident. At a time when the actor was in no condition to be interviewed, a reporter and a photographer from the Sunday Sport newspaper unauthorized gained access to his hospital room, took photographs and attempted to conduct an interview with the actor.

An interlocutory injunction was sought on behalf of the actor to prevent the paper from publishing the article which claimed that Kaye had agreed to give an exclusive interview to the

 [ISSN 2581-5369]

paper. There being no right to privacy under the English law, the plaintiff could not maintain an action for breach of privacy. In the absence of such a right, the claim was based on other rights of action such as libel, malicious falsehood and trespass to the person, in the hope that one or the other would help him protect his privacy. Eventually, he was granted an injunction to restrain publication of the malicious falsehood. The publication of the story and some less objectionable photographs were, however, allowed on the condition that it was not claimed that the plaintiff had given his consent. The remedy was clearly inadequate since it failed to protect the plaintiff from preserving his personal space and from public glare. The court expressed its inability to protect the privacy of the individual and blamed the failure of common law and statute to protect this rights.

The Data Protection Act, 1998 is concerned with personal data. Personal data' consists of data that relates to a 'living individual' who can be identified from that data, or information in the possession of the data user. 'Data' includes information processed by computers, 'relevant filing system' and 'accessible records'.

This legislation was backed up by several court decisions and the U.K. government has entered the world of cyber regulation with comprehensive guidelines.

3. **Japan**

The Japanese Constitution enshrines freedom of speech, assembly and association. The 1988 Act for the Protection of Computer Processed Personal Data held by administrative organs and 1990 Protection of Computer Processed Personal Data (based on the OECD guidelines) provide partial regulation for national government agencies vis-à-vis data protection and privacy.

The national government has emphasized self-regulation by the private sector, especially regarding privacy aspect of electronic commerce, with a series of inspirational guidelines from the ministry of international trade & industry (MITI) and other agencies. The Personal Data Protection Act, passed in May 2003, has established some general restrictions on the use and sharing of personal data, also giving individuals the right to obtain 52 Hopefully, the Human Rights Act in 1998 which imposes a positive obligation to act in accordance with Ewopean Convention on Human Rights will have a positive effect on the development of the law in the UK 29 information collected by some private sector bodies.

4. Bangladesh

The Bangladesh Constitution recognizes the right of privacy to home and correspondence. Article 43 states that: Every citizen shall have the rights, subject to any reasonable restrictions imposed by law in the interests of the security of the state, public order public morality or public

 [ISSN 2581-5369]

health.

- To be secured in his home against entry, search and seizure and
- To the privacy of his correspondence and other means of communication.

In 2006 the Parliament of Bangladesh enacted the Information and Communication Technology Act 2006. The ICTA 2006 touches on the issue of privacy in sections 78 and 79, which approximate section 72 of the Indian I.T. Act 2000.

5. Pakistan

Article 4 of the 1973 Constitution recognizes the right of every citizen and of every other person for the time being within the Country to be protected and treated in accordance with the law. Article 4 (2) disallows any action detrimental to the life, liberty, body, reputation, or property of any person to be taken except in accordance with the law.

The Prevention of Electronic Crimes Ordinance 2008 (Ordinance No. IX of 2008) was approved in November 2008. The Penal Code limited protection of privacy. Pakistan Pena Code (Act XLV of 1860) : The Pakistan Penal Code (PPC) is the primary law for all offences charged in Pakistan. It is applicable across the country and has been in force since the birth of the nation, with a few modifications as per Islamic principles. Though there are some sections that are related to individual privacy, these are far from sufficient to guarantee the comprehensive protection of privacy. One explicitly mention of privacy occurs in Section 509 as substituted by Act 1 of 2010.

- Intending to insult the modesty of any woman, utters any word, makes any sound or gesture, or exhibits any object, intending that such word or sound shall be heard, or that such gesture or object shall be seen, by such woman, or intrudes upon the privacy of such woman;
- Conducts sexual advances or demands sexual favours or uses written or verbal communications or physical conduct of a sexual nature which intends to annoy, insult, intimidate or threaten the other person or commits such acts at the premises of workplace or makes submission to such conduct either explicitly or implicitly, shall be punished with simple imprisonment for a term which may extend to one year, or with fine, or with both.

6. Malaysia

Malaysia also proposed a Personal Data Protection Act recently in 2003. It breaks new ground in law making for cyber-privacy. According to the Malaysian soy ernment, the legislation is

 [ISSN 2581-5369]

envisaged to be a world-class leading edge cyber bv. that provides for higher level of personal data protection. This Act seeks to

(a) Provide adequate security and privacy in handling personal information;

(b) Create confidence among consumers and user of both networked and non networked industries;

(c) Accelerate uptake of e-commerce; and

(d) Promote a secured electronic environment in line with multimedia super corridor (MSC) objectives.

The rationale, the government said, is to promote Malaysia as a communization and multimedia hub where the national adoption of e-based transactions is expected to be high».

7. China

The China's Internet law as well as the related information technology legal infrastructure as a whole is still not well developed. However, the China has got various types of measures to the protection of privacy.[37]

Article 38 of Constitution provides that human dignity of citizens should not be infringed. Article 39 provides that he premises should not be trespassed. Article 40 stipulates that the freedom and privacy of correspondence of citizens are protected by law. These are the parts of the privacy of citizens and general principles set out by the Constitution as the basic law. Moreover, these provisions may provide the basis for the protection of privacy by other laws and regulations".

In Civil Law, there are no explicit provisions identifying the right of privacy as the right of personality of citizens in the General Principles of Civil Law. 1986.

The opinions of the Supreme People's Court of China on several issues, concerning the implementation of the General Principles of Civil Law of the People's Republic of China does not treat the right of privacy as a separate right of personality.

The Criminal Law of China provides that whoever conceals destroys or unlawfully opens another person's letter thereby infringing upon the citizen's right to freedom of correspondence, if the circumstances are serious, shall be sentenced to fixed term imprisonment of not more than one year of criminal detentions.

The Criminal Law of China also provides that any postal worker who opens without

[37] Internet Business Law Services, Inc. (2001-2208). Visited at www.ibls.com accessed on 13/3/16

 [ISSN 2581-5369]

authorization or conceals or destroys mail or telegrams shall be sentenced to fixed term imprisonment of not more than two years of criminal detentions?. The infringement is not convicted of the crime of invasion of privacy, but the crime of violation of freedom of communication and the crime of opening, accealing and destroying mails and telegrams.

A. Internet and Legal Protection to Privacy in China

In China, the provisions on the Technical Measures the Protection of the Security of the Internet were promulgated by the Ministry of Public Security on March 1, 2006. It requires that the provider of the Internet services and entity users network should be responsible for carrying into effect the technical for the protection of the Internet security and should guarantee normal functioning of the technical measures for the protection of the Internet security.

The providers of the Internet services and entity users of the network should establish corresponding administration system. The information as registered by users should not be publicized or divulged without the approval of tic users unless it is provided for by any law or regulation.

The Measures for Security Protection Administration of the international Networking of Computer Information Networks in People's Republic of China provides that user's freedom of communication and communication secrecy are provided by law40. No unit or individual shall use the international networking to infringe on user's freedom of communication and communication secrecy in violation of the provisions of law.

Article 18 of the Implementations Rules for Provisional Regulations of the Administration of the International Networking of Computer Information in the People's Republic of China provides that it is prohibited to infringe on the privacy of others by accessing computer systems without authorization, tampering with the information of others or sending information in the name of others.

B. The Asia-Pacific Economic Cooperation (APEC) privacy initiatives

The 21 APEC economic (Asia-pacific Economic Cooperation) commenced development in 2003 of an Asia-pacific privacy standard. This may become the most significant international privacy initiative since the European Union's Data Protection Directive of the mid-1990s on February 2003, Australia put forward a proposal for the development of APEC Privacy Principles using the 20 years old OECD guidelines ont eh protection of privacy and trans border flows of personal data 1980) as starting point. A privacy sub group was set up comprising Australia, Canada, China, Hog Kong, Japan, Korea, Malaysia, New Zealand, Thailand and the United States. In March 2004 version 9 of the APEC privacy principles was released as a public

 [ISSN 2581-5369]

consultation draft. The history to date of the APEC initiative shows that the dangers are as outcome for privacy protection is still possible.

C. Warsaw declaration Warsaw, Poland-24 September 2013[38]

Nowadays, mobile applications (apps) are ubiquitous. On our smart phones and tablets, in cars, in and around the house: a growing number of items have user interfaces connected to the internet. Currently, over 6 million apps are available in both the public and private sector.

This number is growing by over 30.000 a day. Apps are making many parts of our day-to-day lives easier and more fun. At the same time, apps also collect large amounts of personal data. This allows for continuous digital monitoring, often without the users being aware that this happens and what their data are used for.

App developers are often unaware of the privacy implications of their work and unfamiliar with concepts like privacy by design and default. The main operating systems and app platforms do offer some privacy settings, but do not allow for full control by the users to protect their personal data and verify what information is collected for which purpose.

During their 35th International Conference held on 23 and 24 September 2013 in Warsaw, It is essential that users are and will remain in charge in charge of their own data. They should be able to decide what information to share with whom and for what purposes. To this end, clear and intelligible information should be available including within an app-about data collections taking place before the actual collection starts. Users should be given the option to allow access to specific information life location data or address book entries on a case-by-case basis. Most importantly, apps should be developed on the basis of surprise minimization: no hidden features, nor unverifiable background data collection.

(D) Summery

- The recognition of privacy as a fundamental constitutional value is part of India's commitment to a global human rights regime. Article 51 of the Constitution, which forms part of the Directive Principles, requires the State to Endeavour to "foster respect for international law and treaty obligations in the dealings of organized peoples with one another".[16]
- Article 12 of the Universal Declaration of Human Rights, recognizes the right to privacy. Similarly, Article 17 of the ICCPR, the International Covenant on Civil and Political

[38] "35" international conference on data protection and privacy commissioners : a compass In turbulent world : warsaw ,"23-26 september 2013 available at www. Oas.org/en/sla/dil/docs/data-protection-confereces-warsaw-2013-declaration. Pdf. Access 13/4/16

Rights was adopted on 16 December 1979 and came into effect on 23 March 1976. India ratified it on 11Dec. 1977, also provides prohibition against such interferences and attacks as well as to the protection of the right. The Protection of Human Rights Act, 1993 which has been enacted by Parliament refers to the ICCPR as a human rights instrument. Section 2(1) (d) defines human rights. Under Section 12(f) of the Protection of Human Rights Act, 1993, the National Human Rights Commission: "is entrusted with the function of studying treaties and other international instruments on human rights and make recommendations for their effective implementation." The ICCPR casts an obligation on states to respect, protect and fulfill its norms.

- On 30 June 2014, a report of UN High Commissioner for Human Rights said that: "there is universal recognition of the fundamental importance, and enduring relevance, of the right to privacy and of the need to ensure that it is safeguarded, in law and in practice".[17] "The Right to privacy in the Digital age".[18]

IV. LEGAL FRAMEWORK OF THE RIGHT TO PRIVACY IN INDIA

Privacy is inherent in human behavior. It is a natural need of a man to establish individual boundaries and to restrict the entry of other into that area. There are few moments in the life of every one when he does not want interference of others and desires to be alone. The autonomy is an essential element for the development of one's personality. These areas may, in relation to a person, be the family, marriage, sex or other matters. Which requires, closed chamber treatment. In such areas an individual requires to be at liberty to do he likes.[39]

Advances in information technology and tele-communication networks have radically increased the amount of information and data that can be stored, retrieved, accessed and collated almost instantaneously. Technology blurs the boundaries and move towards convergence of techniques ensure that every bit of information is extracted and logged.

The Internet has facilitated this in an unprecedented manner as an information revolution in present scenario. The growth of technology in the modern world can be viewed as an irresistible drive for efficiency, a relentless urge to achieve the maximum production of goods and services with minimum of human effort.

An element of technological injury appears as an inevitable consequence of this advancement, against which the benefits that flow from the technology have to be balanced. A society is a modern society which exploits computer techniques and where the flow of information is

[39] Singhvi LM., "Constitution of India Protection of Life and Personal Liberty" New Delhi Volume-1 Second edn. (2008) p. 1071

greater and easily collected, recorded, evaluated and transmitted.

Thus a society in which the boundaries created to limit the flow of information may be superseded to the detriment of the privacy of the individual. The life of the individual in a society has to strike a balance between freedom and restrictions. It is inevitable that if any society governed by law, there must be a degree of control of control depending upon the information regarding the past, present and predicted behavior of the individuals and groups in a particular system.

(A) Right to Privacy-Constitutional Perspective

In most of common law constitutions right to privacy is not given expressly to their citizens, but derived from judicial review and court decisions. The right to privacy in India has derived itself from essentially two sources-the common law of torts and the constitutional law. 6 However, this lacuna has not prevented the courts from carving out a constitutional right to privacy by a creative interpretation of the right to life and the right to freedom of movement.

In common law, a private faction for damages for unlawful invasion of privacy is maintainable. The printers and publishers of a journal, magazine or book are liable for damages if they publish any matter concerning the private life of the individual without such person's consent.

The constitution does not grant in specific and express terms any right to privacy such, right to privacy is not enumerated as a fundamental right in the constitution. However, such a right has been culled by the Supreme Court from Article-21 and several other provisions of the Constitution read with the Directive Principles of State Policy.[40]

Competence of Central and state legislatures to enact legislation is derived from the Indian Constitution. The Seventh schedule of constitution of India has three lists-i.e. List I- Union list, List II- State list, List, List II- Concurrent list. These lists contain various entries, which can be subject matters of legislation. But, Privacy is not a subject in any of the three lists of Schedule VII of Constitution of India. Parliament has power to make law on subjects which are mentioned in any of three lists. But no legislative competence is found for subject of privacy. Under the constitutional law, the right to privacy is implicit in the fundamental right to life and liberty guaranteed by Article 21 of the Constitution. This has been interpreted to include the "right to be let alone". The constitutional right to privacy flowing from Article 21 must, however, be read together with the constitutional right to publish any matter of public interest, subject to reasonable restrictions.

[40] Jain M.P., Indian Constitutional Law. Nagpur, Lexis Nexis Butterworth Wahwa, Sixth Edn. (2018). P. 1236

 [ISSN 2581-5369]

The Constitutional Assembly Debates on 'Fraternity clause' of the Preamble project the importance of the dignity of the individual. A few members, namely, B. Pattabhi, Sitaramayya, Srimati Durga Bai, Thakurdas Bhargava, B.V. Keskar, T.T. Krishnamuriti, M. Anathasyanam and K. Santanam of the Constituent Assembly moved an amendment which sought to change the drafting of the clause to the following form: "Fraternity assuring unity of nation and the dignity of the individual". The purposed amendment was negative. The reason for putting 61 There are also a few statutory provisions contained in The Code of Criminal Procedure (Section 327 (1), The Indecent Representation of Women (Prohibition) Act, 1980 (Sections 3 and 4), the Medical Termination of Pregnancy Act, 1971 Section 7 (1)c), The Hindu Marriage Act, 1955 (Section 22), The* Special Marriages Act, 1954 (Section 33), The Children Act, 1960 (Section 36), and The Juvenile Justice Ihrz. 1986 (Section 36), all of which seek to protect women and children from unwarranted publicity.

"dignity of the individual" first was that unless the dignity of the individual is assured, the nation cannot be united. Further, in the Constituent Assembly fourth an amendment on the lines of the United States constitution was moved by Kazi Karimuddin and it was also supported by Dr. B.R. Ambedkar, Mr. Karimuddin had proposed addition of a clause to the Draft article 14 (now article 20) which was intended to serve the purpose of the right of privacy. The resolution provide "The right of the people to be secured in their persons. houses, papers, and effects against unreasonable searches and seizers shall not be violated and no warrant 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.[41]

Though there was nothing novel in Karimuddin suggestion as the Cr.P.C. as a law of the land contained such procedural safeguard, yet Dr. Ambedkar, as the chairman of the Drafting Committee, has expressed his concurrence to the desirability of its incorporation 4. But the constituent assembly after a postponement of this question, issue of a party whip and tow calls division voted against the adoption of Karimuddin's resolution. 65 Therefore the right to privacy akin to the Fourth Amendment was denied, the constitution guaranteed the second right akin to the Fifth Amendment i.e. right against self-incrimination in clause (3) of Article 20 of the constitution. Therefore the right to privacy against the arbitrary arrest, search and seizure of a person by the police or by any agency of the state having similarly with the fourth amendment could not become part and parcel of the person's fundamental rights. Therefore the constituent assembly has failed to rise to the occasion.

[41] Cad Vo.-vii p.794

 [ISSN 2581-5369]

Privacy as one of the necessary ingredient of personal liberty suffered heavily on that account. Whereas the Constitution does not mention expressly the right to privacy, Article 21 miraculously has been playing a major role in the safeguard of privacy as an essential ingredient of personal liberty. Article 21 by self has not been a potent enough weapon in the defense of privacy until it is harpened and made effective by judicial activism. Whether the word privacy implies positive or negative meaning depends upon the social and cultural background in which the concept of privacy has developed. It would be said that privacy is a dynamic concept. It starts with life and protects human dignity. It is skin to the concept of natural justice which is in accordance with natural human one will agree to the privacy of a married couple in their conjugation. By ranting this privacy in our intellectual perception what is in fact we are doing granting the right to privacy to the couple. In other words, imanimously recognize the right to privacy as inherent in human society. Privacy s a concept involves what privacy entails and how it is to be valued. Privacy as a right involves the extent to which privacy is, -The law does not determine what privacy is, but only what situations of privacy will be afforded legal protection.

The Constitution of India, in its Preamble, inter alia, secures equality of status to all citizens and assures their dignity. Dignity of an individual has been adjudged as an essential feature of the constitution. Article 21 protects the right to privacy and promotes the individual dignity mentioned in the Preamble to our Constitution®. The Preambular purpose of our constitution is that it promises to assure the dignity of the individual, while stressing the right to privacy as a basis for the assurance of the dignity of the individual and its autonomy.

a. **Right to Information vis-a-vis Right to Privacy**

The concept of an open government is the direct emanation from the right to know which seems to be implicit in the right of freedom of speech and expression conferred under Article 19 (1) (a) of the Constitution of India.

b. Right to Privacy under Art 19 (1) (a)

Article 19 reads as follows: "19 (1) (a)-All citizens shall have the right-to freedom of speech and expression; (2) Northing in sub-clause (a) of clause (1) shall affect the operation of any existing law, or prevent the State from making an law, insofar as such law imposes reasonable restrictions of the exercise of the right conferred by the said sub-clause in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality or in relation to contempt of court. defamation or incitement to an offence:.

The result of the restrictions being exhaustively enumerated is that unless a publication that

 [ISSN 2581-5369]

invades the individual's privacy is "immoral- or "indecent" it does not fall foul of Article 19(2). Even the fundamental right "to freedom of speech and Expression" as enumerated in Article 19 (1) (a) of Constitution comes with reasonable restriction imposed by State relating to

i. Defamation
ii. Contempt of Court
iii. Decency or Morality
iv. Security of State
v. Friendly relations with foreign states
vi. Incitement to an offence
vii. Public order

However, in India, the right to privacy is not a specific fundamental right but has gained Constitutional recognition. Unfortunately, the infringement of right. to privacy is not covered by the expression "reasonable restrictions"68 to the right to freedom of speech and expression under Article 19 (1) (a). The result of the restrictions being exhaustively enumerated in, that unless a publication that invades the individual's privacy is "immoral" or "indecent", it is not contrary to Article 19 (2). But this has not restricted the activism of the Courts from carving out a Constitutional right to privacy by a creative interpretation of the right to life as enshrined under Article 21 of the Constitution of India.

Coinciding with these legal implications and technological developments a public spirited i.e. a participatory and meaningful law was enacted in India on freedom of information, namely, the Freedom of Information Act, 2002 was enacted to provide for freedom to every citizen to secure access to information under the control of the public authorities, consistent with public interest, in order to promote openness, transparency, and accountability in administration and related matters, though it never came into force?.

Thereafter, on the recommendations made by the National Advisory ouncil, a more comprehensive law ensuring greater and more effective access to information was envisaged. As a result, the Right to Information a Act, 2005 was -acted by the Indian Parliament and it received the President's assent on 6.2005.71 68 Constitution of India, Article 19 (2): "Nothing in sub-clause (a) of clause (1) shall affect the operation existing law, or prevent the state from making any law, in so far as such law imposes reasonable restrictions of the exercise of the right conferred by the said sub clause in the interests of the sovereignty and integrity of India the security of state friendly rations with foreign state, public order, decency or morality or in

 [ISSN 2581-5369]

relation to contempt of court, defamation or incitment of an offence. 69 See Government of India, Report of the Working Group on Right to Information and Promotion of Open Transparent Government, May 1997.

At the same time, it has also brought into confrontation between the right of public to know and the right of the individual to be left alone (right to privacy) 2. The right to information act exempt to disclose the information which effects life and personal liberty of the person.

c. **Right to Privacy under Art. 21**

The existing law just affords a principle which if properly invoked may protect privacy of the individual and Indian judiciary has been using Judicial Activism to widen ambit of the constitution of India Article 21. Where seeds of the privacy right may be found and extending protection granted by it. There are no express words in the Constitution of India about the right to privacy and it is not to be found in any other statue, though interests similar to that were protected both under the civil law.

Article 21 Protection of life and personal liberty "No person's hall be deprived of his life or personal liberty according to procedure established by law".

In, India judiciary has been playing a vital role in interpreting the concept of privacy as a fundamental right. High Court of Allahabad in case of Nihal Chand v. Bhawan Dei took the first step in recognizing the right to privacy in India.

After the independence of India the first case in which the issues of the right to privacy came specifically before Supreme Court was in M.P. Sharma v. Satish Chandra, where the question involved was, whether the state power of search and seizure authorized by section 96 of the Cr. P.C. was violate of individuals of individuals right of privacy, particularly enshrined in Article 19 (1) (f) and Article 20 of the Constitution of India. Kharak Singh v. State of Uttar Pradesh? is an important decision given by the Supreme Court of India on right to Privacy. In this case a question was raised whether the right to privacy could be implied from the existing Fundamental rights, such as Arts. 19 (1) (d), 19 (1) (e) and 21.

The majority of judges participating in the decision said of the Right to Privacy that "our Constitution does not in terms confer like constitutional guarantee. On the other hand, Justice Subba Rao, who gave his minority opinion, was in favour of inferring the right to privacy from the expression 'personal liberty' in Article 21. In the words of J. Subba Rao: "Further, the right to personal liberty, takes is not only a right to free from restriction placed on his movement, but also free from encroachments on his life. It is true our constitution does not declare a right to privacy as a fundamental right but the said right is an essential ingredient of personal liberty.

 [ISSN 2581-5369]

Every country sacrifices domestic life.

" In Govind v. State of Madhya Pradesh, the Supreme Court under took a more elaborate appraised of the right to privacy. In this case the court considered the constitutional validity of a regulation. The court upheld the regulation by ruling that article 21 was not violated as the regulation in question was "procedure established by law", in terms of Article 21.

The court also accepted a limited fundamental right to privacy "as an emanation" from Arts. 19 0) (a), (d) and 21. The right to privacy is not, however, absolute reasonable restriction can be placed thereon in public interest article 19 (5). Thus Justice Mathew observed that "The right to privacy in any event will necessary have to go through a process of case by case development. Therefore even assuming that the right to personal liberty, the right to move freely through ought the territory of India and the freedom of speech creates an independent right of privacy as an emanation from them which one can characterize as a fundamental right, we do not think that the right is absolute." In this case he also formulated a dominant test known as the compelling state interest through which the state may have control over the man's privacy. Justice Mathew said "Assuring that the fundamental right explicitly guaranteed to to citizen have penumbral zones and that the right of privacy itself a fundamental right the fundamental right must be subject to restriction on the basis of compelling public interest".

This shows that Justice Mathew has displayed his best judicial craft-man ship by holding the 'right to privacy' as a part of personal liberty in Article 21 Justice Mathew has in articulated manner determined a brand nature and scope of the right to privacy. But the learned judge has not declared it an absolute right as no right can be has legitimately and clearly advocated that the right to privacy may be trammel led by the compelling public interest he further emphasized the need of the reasonable restrictions legitimately required to be put in the enjoyment of the right of privacy.

The right to privacy has been held as an integral part of the fundamental right to life and personal liberty under Article 21 of the Constitution. In Maneka Gandhi ease Supreme Court accepted J. Subba Rao's view in Kharak Singh that the right to privacy is fundamental right.

In Maneka Gandhi vs Union of India, 80 in a seven-judge bench decision, Justice P.N. Bhagwati, held that he expression "personal liberty" in Article 21 is of the widest amplitude and covers a variety of rights which constitute the personal liberty of man. Some of them have been raised to the status of distinct fundamental rights and given additional protection under Article 19. The court ruled: "Any law interfering with personal liberty of a person must satisfy a triple test: i) it must prescribe a procedure ii) the procedure must withstand the test of one or more of

 [ISSN 2581-5369]

the fundamental rights conferred under Article 19 which may be applicable in a given situation, and iii) it must also be liable to be tested with reference to Article 14 (the guarantee of equality). As the test propounded by Article 14 pervades Article 21 as well the law and procedure authorizing interference with personal liberty and right of privacy must also be right and just and fair and not arbitrary, fanciful or oppressive. If the procedure prescribed does not satisfy the requirement of Article 14 it would be no procedure at all within the meaning of Article 21". The net result is that he fundamental right to "personal liberty", embodied in Article 21, covers the right to privacy as well.

1. State of Maharashtra V. Madhukar Naravan Mardikar[42]

In this case a police Inspector visited the house of one banubai in uniform and demanded to have sexual inter course with her. On refusing he tried to have her by force. She raised a hue and cry. He is as prosecuted he told the court that she was a lady of easy virtue and therefore her evidence was not to be relied. The court rejected the arguments of the applicant and held him liable for violation her right to privacy.

It was also held that right to privacy is available even to a woman of easy virtue and no one can invade her privacy. In R. Raj Gopal v. State of Tamil Nadu® in this case Supreme Court has asserted that intimes the right to privacy has acquired constitutional status, it is implicit in the right to life and liberty guaranteed to the citizens by Art-21. It is a "right to be alone."

In people's Union for Civil Liberties v. Union of India® in this case SC has deserved that, " We have therefore; no hesitation in holding that right to privacy is a part of the right to "life" and "personal liberty" enshrined under Article 21 is attracted the said right cannot be curtailed 'except according to procedure established by law'.

For first time Supreme Court articulated on sensitive data related to health. In this case the Appellant's blood test was conducted at respondent's hospital and he was found to be HIV (+). His marriage which was already settled was called off after this revelation the appellant field a writ petition in High Court of Bombay. He contended that

i. His prestige among his family members was damaged and

ii. Respondents were under a duty to maintain confidentiality on account of medical ethics formulated by Indian Medical Council.

iii. His right to privacy has been infringed by respondents by disclosing that the appellant was HIV (+) and therefore they are liable in damages.

[42] AIR 1991 SC 207

 [ISSN 2581-5369]

Supreme Court has held that although the right to privacy is a fundamental right under Art 21 but it is not an absolute right and restrictions may be impose on it for prevention of crime, disorder or protection of health or morals or protection of right and freedom of others 86.

Ms. X.V. Mr. Z87 In this case, the wife filed a petition for dissolution of Marriage on ground of cruelty and adultery against husband under section 10 of Divorce Act. Husband also asserted that his wife has adulterous affairs with one person which resulted in family way. Pregnancy of wife was terminated at all Indian Institute of Medical Sciences and records and slides of tabular gestation were preserved in hospital. Husband filed an application for seeking DNA test of said slide with a view to ascertain if husband is father of foetus.

The Court held that the right to privacy though a fundamental right forming part of right to life enshrined under Art 21 is not on absolute right. When right to privacy has become a part of public document, in that case a person cannot insist that such DNA test would infringe his or her right to privacy. The foetus was no longer a part of body and when it has been preserved in AIIVIS, the wife who has already discharged same cannot claim that it affects her right of privacy. When adultery has been alleged to be one of the grounds of divorce in such circumstances application of husband seeking DNA test of said slides can be allowed.

2. District Registrar and Collector V. Canara Bank[43]

In this Court was held that "exclusion of illegitimate intrusions into privacy depends on nature of the right being asserted and the way in which it is brought into play, it is at this point that context becomes crucial, to inform substantive judgment. If these factors are relevant for defining the right to privacy. They are quite relevant whenever there is invasion of that right by way of searches and seizures on the instance of the state.

If one follows the judgment given by Hon'ble, Supreme Court, three themes emerge

i. Individual's right to privacy exists and any unlawful invasion of privacy would make offender liable for consequences in accordance with law.

ii. That there is constitutional recognition given to right of privacy which protects personals privacy against unlawful governmental invasion.

iii. That person's "right to be let alone" is not an absolute right and may be lawfully for prevention of crime, disorder or protection of health or morals or protection or rights and freedom of others.

All these rights are grouped in Part III of the Constitution as Fundamental right which can be

[43] AIR 2005 SC 186

 [ISSN 2581-5369]

remedied under Article 32 & 226 of the Constitution of India. As a safeguard the Supreme Court of India and other High Courts exercise wide powers for enforcing these rights by issuing writs. Article 13 of the Constitution forbids the State from making any law or regulation in contravention of these rights may be declared void. Constitutional right of privacy is emanated under these provisions of the Constitution®. The right to privacy has now become established in India, but as part of Article 21. It is well established that is an essential human rights. Certain norms of privacy should be determined and measured to a common standard, because a right without description is a right without protection. Conceptual basis of privacy and its protection should be removed immediately°°

(B) Right to Privacy- Legal Framework

Several existing legislations in India as well as many proposed ones have rave privacy implications that are scarcely recognized. India is a very close-knit society with strong ties of kinship, where the intensely private and personal affairs of an individual may, more often than not, become the 'public' affairs of all. There is a fact, a lack of awareness among the people in general about these most fundamental rights concerning personal liberty and freedom. This is reflected in the absence of any comprehensive, all-encompassing legislation dealing with all aspects of the law in relation to a person's right to privacy". However, the legislators in India have not been completely obvious to the necessity of such a right. They have therefore, from time to time, included provisions relating to the right of privacy in various pieces of legislations, which govern or deal with special circumstances and or special classes of people.

1. **Information Technology Act, 2000 (as Amended 2008) : vis-a-vis Right to Privacy**

The Act provides for a set of laws intended to provide comprehensive regulatory environment for electronic commerce. The Act also addresses the question of computer crimes, hacking, and damage to computer source code, breach of confidentiality and viewing of pornography, protection of privacy.

Section 43

This section provides protection against unauthorized access of the computer system by imposing heavy penalty up to one crore. The unauthorized downloading, extraction and copying of data are also covered under the same Penalty. Clause 'c' of this section imposes penalty for unauthorized introduction of computer viruses of contaminants. Clause g' provides penalties for assisting the unauthorized access. If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network

i. Access such computer, computer system or computer network or computer resource;

ii. Downloads, copies or extracts of any data, computer data base or information;

iii. Introduces or causes to be introduced any computer contaminant or computer virus;

iv. Damages or causes to be damaged any computer, computer system or computer network data, computer data base or any other programmes;

v. Disrupts or causes disruption;

vi. Denies or causes the denial of access to any person authorize to access;

vii. Provides any assistance to any person to facilitate access in contravention of the provisions of this act;

viii. Charges the services availed of by a person to the account of another person by tempering with or manipulating any computer, computer system or computer network.

ix. Destroys deletes or alters any information residing in a computer recourse or diminishes its value or utility or affects it injuriously by any means;

x. Steal, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code with intention to cause damage*?;

He shall be liable to pay damages by way f compensation to the person so affected.

Section 43A is a proactive provision with the sole objective to protect personal data and privacy. Though the Act, has not defined the term "data subject", but by default this section has articulated the term "data subject". It creates onus on "body corporate" to implement and maintain "reasonable security practices and procedures" in order to protect sensitive personal data of an individual. The aforesaid section has identified "body corporate" as "data processor" and "data controllers" which would be possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates.

In fact, this section has provided a redressal mechanism to any affected person to seek compensation from a body corporate, which has been negligent in implementing and maintain reasonable security practices and procedures vis-à-vis 'any personal data and information' and thus caused wrongful loss or wrongful gain to any such person.

Liability for Body-Corporate under Section 43A

Sec.43A of the Information Technology Act, 2000 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

 [ISSN 2581-5369]

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 unauthorized access, damage, use, 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's bodies or associations as it may deem fit.

Data Protection: Currently the strongest legal protection of personal information in India is through section 43A of the Information Technology (Reasonable security practices and procedures and sensitive personal data information) Rules 2011.

The newly inserted section 43A4 makes a start at introducing a mandatory data protection regime in Indian law. The section obliges corporate bodies who 'possess, deal or handle' an 'sensitive personal data' to implement and maintain 'reasonable' security practices, failing which they would be liable to compensate those affected by any negligence attributable or professional activities' that are the targets of this section. Thus government agencies and nonprofit organizations are entirely excluded from the ambit of this section. "Sensitive personal data or information" is any information that the Central Government may designate as such, when it sees fit to. The "reasonable security practices" which the section obliges body corporate to observe are restricted to such measures as may be specified either "in an agreement between the parties" or in any law in force or as prescribed by the Central Government. By defining both "sensitive personal data" and "reasonable security practice" in terms that require executive elaboration, the section in effect pre-empts the courts from evolving an iterative, contextual definition of these terms.

Under Section 43A% in order to define "sensitive personal information" and to prescribed

 [ISSN 2581-5369]

reasonable security practices" that body corporate must observe in relation to the information they hold. Central Government of India draft rules, The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

Sensitive Personal Information

Rule 3 of these Draft Rules designates the following types of information as sensitive personal information".

a) Password;

b) User details as provided at the time of registration or thereafter, information related to financial information such as Bank account/credit card/debit card/other payment instrument details of the users;

c) Physical, physiological and mental health condition;

d) Sexual orientation;

e) Medical records and history;

f) Biometric information;

g) Information received by body corporate for processing stored or processed under lawful contract or otherwise; call data records;

This however, does not apply to -any information that is freely available or accessible in public domain or accessible under the Right to Information Act, 2005".

Mandatory Privacy Policies for Body Corporate

Rule 439 of the draft rules enjoins a body corporate or its representative who "collects, receives, possess, stores, deals or handles" data to provide a privacy policy "for handling of or dealing in user information including sensitive personal information". This policy is to be made available for view by such "providers of information". The policy must provide for

i. And easily accessible of its practices and policies;

ii. Type of personal or sensitive data or information collected under rule 3; ili,

iii. Purpose, means and modes of usage of such information;

iv. Disclosure of information including sensitive personal data or information as provided in rule 6;

v. Reasonable security practices and procedures as provided under rule 8.

Prior Consent and Use Limitation during Data Collection

 [ISSN 2581-5369]

In addition to the restrictions on collective sensitive personal information, body corporate must obtain prior consent form the "provider of information" regarding "purpose, means and modes of use of the information". The body corporate is required to "take such steps as are, in the circumstances, reasonable" to ensure that the individual from whom data is collected is aware of:

a. The fact that the information is being collected;

b. The purpose for which the information is being collected;

c. The intended recipients of the information; and

d. The name and address of

    (i) The agency that is collecting the information; and

    (ii) The agency that will hold the information.

During data collection, body corporate is required to give individuals the option to opt-in or opt-out from data collection. They must also permit individuals to review and modify the information they provide "wherever necessary". Information collected is to be kept securely, used only for the stated purpose and any grievances must be addressed by the body corporate "in a time bound manner".

Section 65

This section provides for computer source code. If anyone knowingly or intentionally conceals, destroys, alters or causes another to do as such shall have to suffer a penalty of imprisonment of fine up to 2 lakh rupees. Thus protection has been provided against tampering of computer source documents.

Section 66

Protection against hacking has been provided under this section. As per this section hacking is defined as any act with an intention to cause wrongful loss or damage to any person or with the knowledge that wrongful loss of damage will be caused to any person and information residing in a computer resource must be either destroyed, deleted, altered or its value and utility get diminished. This section imposes the penalty of imprisonment of three years or fine up to two lakh rupees or both on the hacker.

Section 66C

This section provides punishment for identity theft whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other

 [ISSN 2581-5369]

person. This section imposes the penalty of imprisonment of three years of fine up to one lakh rupees. This section protects the identity of a user in the online medium. The purpose of the section is to protect the privacy of all or any web users, including their personal information or data

Section 66E

Sec. 66E of The Information Technology Act, 2000 reads as follows, Punishment for violation of Privacy-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, shall be punished with imprisonment which may extended to three years or with fine not exceeding two rupees, or with both.

In this section world use 'private area' is define under Explanation-"Private area" means the naked or undergarment clad genitals. public area, buttocks or female breast.

Under circumstances violating privacy means circumstances in which a person can have a reasonable expectation that

- He or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or
- 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.

Voyeurism: Whoever intentionally or knowingly captures, publishes or transmits the image of a private of area of any person under circumstances violating the privacy of that person. and without consent is held criminally liable with imprisonment for up to three years and/or witha fine not exceeding two lakh rupees. Though it is important that an individual is protected from the transmitting of invasive images without his/her consent, the provision is unclear if this applies to any other person, in other words, it is not clear if an individual can voluntarily transmit an image of his or genitals. Violation of privacy such as installation of spy cameras, hidden cameras, communication devices inside washrooms, bedrooms, changing rooms, hotel rooms, etc. for the purpose of violating bodily privacy of any users/occupant of such places.

Section 67C

In this section liability imposes on intermediary for preservation and retention of information collected during transaction in the manner of Central Government may prescribe. In order to prescribe such duration and in such manner and format Central government draft The Information Technology (Intermediary Guidelines) Rules 2011.

 [ISSN 2581-5369]

Intermediary due diligence: The Information Technology (Intermediary Guidelines) Rule 2011 provides regulations for intermediaries to follow concerning the content that passes through their systems. The rules also establish what content is an is not allowed to be posted by individuals, and holds intermediaries responsible for ensuring that websites are in compliance with the provisions. Aspects of the rules that are relevant to privacy include: provide regulations for intermediaries to follow concerning the content that passes through their systems. The rules also establish what content is and is not allowed to be posted by individuals, and holds intermediaries responsible for ensuring that websites are in compliance with the provisions.

Section 70

This section provides protection to the data stored in the protected system. Protected systems are those computers, computer system or computer network to which the appropriate government, by issuing gazette information in the official gazette, declared it as a protected system. Any access or attempt to secure access of that system in contravention of the provision of this section will make the person accessed liable for punishment of imprisonment which may extend to ten years and shall also be liable to fine.

Section 72-Penalty for breach of confidentiality and Privacy

This section provides protection against breach of confidentiality and privacy of the data. As per this, any person upon whom powers have been conferred under IT Act and allied rules to secure access to any electronic record, book, register, correspondence, information document of other material discloses it to any other person, shall be punished with imprisonment which may extend to two years or with fine which may extend to one lakh rupees or both. The purpose behind this section is that he person who has secured access to my any such information shall not take unfair advantage of it by disclosing party. An obligation of confidence arises between the 'data collectors/data controller' and data subject.

Section 72A-Punishment for discloser of information in breach of lawful contract

This section creates liabilities for service providers, including an intermediary. It is in fact a Kind of data protection measure, wherein a service provider who has secured access to any material containing personal information about a person, discloses such information with the consent of the person concerned or in breach of a lawful contract, with the intent to cause or knowing that the is likely to cause wrongful loss or wrongful gain to such person. The issue of confidentiality and privacy as enumerated in section 72 and section 72A of the Act should be read along with the eight reasonable restrictions imposed by article 19 (2) on right "to freedom of speech and expression" as enumerated in article 19 (I) (a) of the constitution of India. If need

 [ISSN 2581-5369]

be, ata subject' may take advantage of Article 2lwhich states that "no person shall be deprived of his life or personal liberty except according to procedures established by law"'[44].

After going through the discussion it is clear that the provisions contained in The Information Technology Act, 2000 (as amended 2008) it is does not contained adequate provisions for checking the violation of privacy in technological advancements age. In spite of this Act contains some novel provisions for protection of privacy in technological advancements era-like Sec. 72, 72A, 66E of I. T. Act 2000.

Internet Services License

In India interception powers are also given to the government through the Internet Services License Agreement and the Unified Access Services Agreement for service providers. In practice, both licensed afford the government expansive access to communication data held by an accessible to ISPs.

Protection of Privacy

There is a responsibility on the ISP to protect the privacy of its communications transferred over its network. This includes securing the information and protecting against unauthorized interception, unauthorized disclosure, ensure the confidentiality of information, and protect against over disclosure of information -except when consent has been given. In order to protect the privacy of voice and data, monitoring shall only be by the Union, Home Secretary of Home Secretaries of the States/Union Territories.

2. The Indian Contract Act, 1872

These days companies are relying on the contract law as a useful means to protet thei information. The corporate houses enters into several agreements with other companies, clients, agencies or partners to keep their information secured to the extent they want to secure it. Agreements such as 'non circumvention and non-disclosure' agreements, 'user license' agreements, 'referral partner' agreements ete. are entered into by them which contains confidentiality and privacy clauses and also arbitration clauses for the purpose of resolving the dispute if arises. These agreements help them in smooth running of business. BPO companies have implemented processes like BS 7799 and the ISO 17799 standards of information security management, which restrict the quantity of data that can be made available to employees of BPO and call centres.

[44] Sharma Vakul, Information Technology Law and Practices, New Delhi, Universal Law Publishing Co. Pvt. Ltd. Third Edn. 2011, p. 258

3. The Indian Penal Code 1861

It imposes punishment for the wrongs were expected to occur till the last decade. But if failed to incorporate within itself the punishment for crimes related to data which has become the order of the day. A section 292 dealt with sales, hire, distributes of obscene books etc. and section 293 provides sale of obscene objects to young persons. Both sections punish who violates these provisions. Some other provisions are also deals with privacy like provisions related house trespass and house breaking. [45]

Provision for Sexual Voyeurism: Section 345C of the IPC provides as follows-Whoever watches, or captures the image of, a woman engaging in a private act in circumstances where she would usually have the expectation of not being observed either by the perpetrator or by any other person at the behest of the trpetrator shall be punished on first conviction with imprisonment of either description for a term which shall not be less than one year, but which may extend to three years, and shall also be liable to fine, and be punished on a second or Rthsequent conviction, with imprisonment of either description for a term which shall not be less than three years, but which may extend to seven years, and shall also be liable to fine".

Explanation 1: For the purposes of this section, "private act" includes an act of watching carried out in a place which, in the circumstances, would reasonably be expected to provide privacy, and where the victim's genitals, buttocks or breasts are exposed or covered only in underwear; or the victim is using a lavatory; or the person is doing a sexual act that is not of a kind ordinarily done in public

Explanation 2: Where the victim consents to the capture of images or any act, but not to their disemination to third persons and where such image or act is disseminated, such dissemination shall be considered an offence under this section! This provision seeks to protect victims of voyeurism, from being watched, or recorded, without their consent under circumstances where the victim could reasonably expect privacy. A reasonable expectation of privacy implies to both public and private places where the victim has a reasonable expectation that she is not being observed engaging in private acts such as disrobing or sexual acts. Similar provisions can be found in voyeurism laws across the world, and section 66E of the IT Act. It is particularly important because voyeurism also takes place in public spaces where there is generally an expectation that exposed body parts are not being watched.

Provision for Stalking: Section 354D of Indian Penal Code, 1860 as follows

[45] Section 442, 443, 444, 445 and 446, The Indian Penal Code. 1860

 [ISSN 2581-5369]

(1) Any man who

i. a woman and contracts, or attempts to contacts such woman to foster personal interaction repeatedly despite a clear indication of disinterest by such woman: or

ii. Monitors the use by a woman of the internet, email or any other form of electronic communication, Commits the offence of stalking.

Provided that such conduct shall not amount to stalking if the man who pursued it proves that

i. Was pursued for the purpose of preventing or detecting crime and the man accused of stalking had been entrusted with the responsibility of prevention and detention of crime by the state; or

ii. It was pursued under any law or to comply with any condition or requirement imposed by any person under any law; 49or

iii. In the particular circumstances such conduct was reasonable and justified.

(2) Whoever commits the offence of stalking shall be punished on first conviction with imprisonment of either description for a term which may extend to three years, and shall also be liable to fine; and be punished on a second or subsequent conviction, with imprisonment of either description for a term which may extend to five years, and shall also be liable to fine.

Cyber stalking:-"Cyber stalking" is one of the most widespread and overlapping forms or personal online harassment. A simple definition of "cyber staking" is: " the use of electronic comnunication emails and the internet to bully, threaten, harass, and intimidate a vicim "Cyber stalking" can be perpetuated through email, online websites, social networking sites, message forums, and online gaming. Harassment is defined as nay behavior that causes the victim distress, whether intentional or not. Social networking sites provide an example of online applications, with otherwise legitimate purposes, that can be used to facilitate direct and indirect cyber stalking. Social networking sites are vulnerable to abuse by cyber stalkers because of the ease with which the sites enable subscribers, and sometimes non-subscribers, to access large amounts of personal information, usually voluntarily posted by a victim on its "profile". A "cyber stalker" may use social networking sites to follow a victim's actions, gain contact information, or to enact abuse on the person's identity.

4. Code of Criminal Procedure, 1973[46]

Section 327 (1) provides that the place in which any criminal court is held for the purpose of

[46] The Code came into force with effect from 25 January 1974

 [ISSN 2581-5369]

inquiring into or trying any offence shall be an open court but the second sub-clause provides that any inquiry into, trial and punishment for an offence of rape 07, or an offence involving intercourse by a man with his wife during separation, or an offence involving intercourse by a public servant with women in his custody or an offence involving intercourse by a superintendent of jail, remand home, etc. shall be conducted in camera, and only with the special permission of the presiding judge can any person be allowed to have access to, or be or remain in, the room or building used by the court. Further, in any proceedings under this subsection it shall not be lawful for any person to print or publish any matter in relation to any such proceedings except with the prior permission of the court los.

Thus code of criminal procedure, 1973 is through this provisions protecting privacy of the victims or accused, in the court rooms trial.

5. The Hindu Marriage Act, 1955[47]

Section 22-Every proceeding under this Act, shall be conducted in camera and it shall not be lawful for any person to print or publish any matter in relation to any such proceeding except a judgment of the High Court or of the Supreme Court printed or published with the previous permission of the court. If any person prints or publishers any matter in contravention of the provisions this shall be punishable by a fine which may extended to 1000, rupees. The provisions of this Act are applicable to marriages where both the parties are Hindus by religions.

Setion 33 of the Special Mariages Act, 1954 though on the same ters as section 22 of The Kindu Mariage Act, 1955 is less restricive as it provides that a proceeding under that act shal be conducted in camera if either party thereto, desires or if the District Court desires to do so.

6. The Juvenile Justice Act, 1986

This act is applies to a juvenile who is defined as a boy under the age of 16 years and a girl under the age of 18 years. Section 36 of the Act provides that no report in any newspaper, magazine or news-sheet of any inquiry regarding a juvenile under this act shall disclose the name, address or school or any other particular calculated to lead to the identification of the juvenile, nor shall any picture of any such juvenile be published. Any person contravening the provisions of this section shall be punishable with fine, which may extend ti one thousands rupees. This sections with the intention of safeguarding the image of a child and or juvenile who is particularly vulnerable to acquiring any stigma or disrepute which would jeopardize their chances of leading a normal life.

[47] The Hindu Marriage Act came into force on 18 May 1955

 [ISSN 2581-5369]

7. The Indecent Representation of Women (Prohibition) Act, 1986

Section 3- "No person shall publish, or cause to be published or arrange or take part in the publication or exhibition of any advertisement which contains indecent representation of women in any form".

Section 4- "No person shall produce or cause to be produced, sell let for hire, distribute, circulate, or send by post any book, pamphlet, paper, slide, film, writing, drawing, painting, photograph, representation or figure which contains indecent representation of women in any form, except if the said book etc. is in the interest of science, literature, art or learning or other objects of general concern or for religious purpose".

Indecent representation of women is defined in section 2 (c) of the Act to mean, the depiction in any manner of the figure of a women, her form or body or any thereof in such a way as to have the effect of being indecent, or derogatory to, or denigrating, women, or is likely to deprave, corrupt, or injure the public morality or morals. Therefore this Act meant to protect bodily privacy of women through its provisions.

8. The Telegraph Act, 1885 (as amended) 2003, 2006

The Indian Telegraph Act was passed to govern telegraphy, phones, communication, radio, telex and fax in India. The Act allows any authorized public official to intercept communication. in 2007 Telegraph Act (Interception) Rules 2007 were issued. Unauthorized interetion of communications is punishable by imprisonment for up to one year and a fine of IN 500. The Interception Rules further hold service providers responsible for the actions of their employees, who can be held criminally liable under the act. The following provisions relating to interception exist under the act:"[48]

Lawful Interception: Communications can be intercepted under the Telegraph Act during public emergencies or in the interest of public sofily, provided hat certain other grounds also apply, namely, the sovereignty and integrity of India, the security of the State, friendly relations with foreign states. public order, and the prevention of the incitement of offences.

9. The Medical Termination of Pregnancy Act, 1971

Section 7 (1) (c) of this Act, the State Government are empowered to make regulations prohibiting the disclosures, except to such persons and for such purposes as may be specified in such regulations, of any information regarding the particulars of a women having undergone termination of any pregnancy under the act. Any person who willfully contravenes or willfully

[48] Indian Telegram Rules 2007s. 15

 [ISSN 2581-5369]

fails to comply with the any such regulations shall be liable to be punished with fine which may extend to 1,000 rupees. It is evident that these special provisions were enacted to essentially safeguard the special interests of women and children in extraordinary circumstances .

10. The Right to Information Act, 2005

In many countries citizens are able to hold government transparent and accountable through Freedom of Information laws, Access to Information laws, and Public Information laws. In India, the Right to Information Act works to promote transparency, contain corruption, and hold the Government accountable to the people. The RTI establishes a responsibility on public bodies to disclose pre identified information, the right of citizens to request information held by public authorities from public information officers, and creates a Central Information commissioner responsible for hearing/investigating individual complaints when information is denied. In the context of the RTI Act, every public authority must provide information relating to workings of public authorities as listed under section 4 (I(b)) to the public on a suo motu basis at regular intervals. Section & of the Act lists specific types of information that are exempted from public disclosure in order to protect privacy. In this way privacy is the narrow exception fo the right to information, When contested, the Information Commisioners will use a pubic interest test to determine whether the individual's right to privacy should be trumped by the publi's right to information. There exist more than 400 cases where the Central Information Commissioner has pronounced on the balance between privacy and transparency.

11. TRAI Regulations on Unsolicited Marketing Calls

In India, the Telecom Regulatory Authority of India (TRAI) is responsible for establishing Regulations for unsolicited marking calls. The first Regulation regarding unsolicited commercial marketing calls from telemarketers emerged in 2007, but were repealed and replaced in 2010 by the Telecom Commercial Communications Customer Preference Regulations 2010. Since their enactment, the Regulations have been amended eight times. They work to regulate 'unsolicited commercial communications", which have been defined as any message which is transmitted for the purpose of informing, soliciting, or promoting any commercial transaction in relation to goods, investments or services etc. Excluded from this definition are 'transactional messages', which relate to: Information pertaining to the account of a customer and sent by a licensee, bank, insurance company, credit card company, or depositories registered with Securities and Exchange Board of India, or Direct to Home Operators; any information given by airlines or Indian Railways or its authorized agencies to its passengers regarding travel schedules, ticket booking, and reservation; information from

 [ISSN 2581-5369]

registered educational institutions to parents or guardians of its students; any other message as may be specified by the Authority from time to time as a "transactional message".

12. The Personal Data Protection Bill, 2006

Upon the footprints of the foreign laws, this bill has been introduced in the Upper House of Indian Parliament Rajya Sabha on December 08, 2006. The purpose of this bill is to provide protection of personal data and information of an individual collected for a particular purpose by one organization, and to prevent its usage by other organization for commercial or other purposes and entitle the individual to claim compensation or damages due to disclosure of personal data or information of any individual without his consent and for matters connected with the Act or incidental to the Act. Provisions contained in this Act are relating to naluc of data to be obtained for the specific purpose and the quantum of data to be obtained for the purpose. Data controllers have been proposed to be appointed to look upon the matters relating to violation of the proposed Act.

On comparing the Indian law with the law of developed countries the proper requirement for the Indian law can be analyzed. Data are not of same utility and importance; it varies from one another on the basis of utility. So, we require framing separate categories of data having different utility values, as the U.S. have. Moreover, the provisions of Information Technology Act, 2000 deals basically with extraction of data, destruction of data.

Organizations cannot get full protection of data through that which ultimately forced them to enter into separate agreements to keep their data secured. These agreements have the same enforceability as the general contract.

Despite the effort being made for having a data protection law as a separate discipline, the Indian legislatures have left some lacuna in framing the bill of 2006. The bill has been drafted wholly on the structure of the UK Data Protection Law'14 whereas today's requirement is of a comprehensive Act. Thus it can be suggested that a compiled drafting on the basis of US laws relating to data protection would be more favourable to current legal requirements.

Being one of the most concerned topics of discussion in the modern era, legislatures are required to frame more stringent and comprehensive law for the protection of data which requires a qualitative effort rather than quantitative in modern context of developing technologies.

13. The Privacy Protection Bill (2013)

As the bill says that it is a bill "to establish an effective regime to protect the privacy of all persons and their personal data from Governments, public authorities, private entities and

others, to set out conditions upon which surveillance of persons and interception and monitoring of communications may be conducted, to constitute a Privacy Commission, and for matters connected therewith and incidental thereto".

Following are the chapters of the privacy protection bill (2013):

- Preliminary
- Right to Privacy
- Protection of Personal Data
- Interception of Communications
- Surveillance
- The Privacy Commission
- Offences and Penalties

This bill deals with all the major aspects of the privacy concern. It states that no person shall collect, store, process, disclose or otherwise handle any personal data of another person, intercept any communication on another person or carry out surveillance of another person except as provided in the act. 16 It also put a bar on collecting data or personal information of individuals without obtaining prior consent of the person whom it pertains. If made applicable privacy commission would be formed so that no one can carry out any surveillance of any person without taking permission from the privacy commission though it has some exceptions too.

14. National Cyber Security Policy 2013

For secure computing environment and adequate trust & confidence in electronic transactions and spread awareness regarding protection from cyber-attacks.

Cyber Security and Cyber Defense: Cyber security is the activity of protecting information and information systems (networks, computers, data bases, date centres and applications) with appropriate procedural and technological security measures. In that sense, the notion of cyber security is quite generic and encompasses all protection activities. Cyber defense relates to a much more specialized activity linked to particular aspects and organizations. The distinguishing factors between cyber security and cyber defense in a network environment are the nature of the threat, the assets that need to be protected and the mechanisms applied to ensure that protection. Cyber defense relates to defensive actions against activities primarily originating from hostile actors that have political, quasi-political or economic motivation that

 [ISSN 2581-5369]

have an impact on national security, public safety or economic wellbeing of the society. The cyber defense environment requires deployment of technologies and capabilities for real-time protection and incident response. Generally, cyber defense is driven by intelligence on the threat to achieve the kind of defense that directs, collects, analysis and disseminates the relevant actionable intelligence information to the stakeholders concerned for necessary proactive, preventive and protective measures. The effectiveness of cyber defense lies in the proactive nature of security counter measures as well as in ensuring resilience and continuity of operations, despite the possibilities of successful attacks.

Some other Acts and Bills which deals with privacy protections as follows-

- The National Security Act, 1980 The Indian Evidence Act, 1872
- National Investigation Agency Act, 2008
- The Unlawful Activities (Prevention) Act, 2002
- UASL License,
- Medical Council of India's Code of Ethics Regulations, 2002
- Pre-Natal Diagnostic Techniques Act, 1994
- The Official Secrets Act, 1923
- The Prevention of Corruption Act, 1988
- The Securities and Exchange Board of India act, 1992
- The Monopolies and Restrictive Trade Practices Act, 1969
- The Lok Pal and Lokayuktas Act, 2013
- The Public Interest Disclosure and Protection to Persons Making Disclosures Bill, 2011, etc.

These all are Acts and Bills which provide for protection of privacy in various modes through there provisions.

(C) Complaint Procedure to combat privacy violation

Section 46 and the rules framed under that section provide elaborate guidelines on the procedure that is to be followed by the adjudicating officer. Thus, the adjudicating officer is required to give the accused person "a reasonable opportunity for making representation in the matter". Thereafter, if, on an inquiry, -he is satisfied that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the

provisions of that section.

In order to carry out their duties adjudicating officer have been invested with the powers of a civil court which are conferred on the cyber appellate tribunal. Additionally, they have the power to punish for their contempt under the Code of Criminal Procedure. 117 The Information Technology Act 2000

Rules framed under the section provide further details on the procedure that must be followed compounding of offences, etc!. and provide for the issuance of a "show cause notice", manner of holding enquiry.

Section 47 provides that in adjudging the quantum of compensation, the adjudicating officer shall have due regard to the following factors, namely:-

- The amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;
- The amount of loss caused to any person as a result of the default;
- The repetitive nature of the default.

The complaint must be made to the adjudicating officer of the state or union territory on the basis of location of computer system, computer network. The complaint must be made on a plain paper in the format provided in the Performa attached to the rules.

In case the offender or computer resource is located abroad, it would be deemed, for the purpose of prosecution to be located in India .

The Rules direct that the whole matter should be heard and decided "as far as possible" within a period of six months.

1. Appeals to the Cyber Appellate Tribunal and the High Court

The act provides for the constitution of a cyber appellate tribunal to hear appeals from cases decided by the adjudicating officer. Within 25 days of the copy of the decision being made available by the adjudicating officer, the aggrieved party may file an appeal before the cyber appellate tribunal. Section 57 provides that the appeal filled before the cyber appellate tribunal shall be dealt with by it as expeditiously as possible and endeavor shall be made by it to dispose of the appeal finally within six months from the date of receipt of the appeal. Section 62 gives the right of appeal to a high court to any person aggrieved by any decision or order of the cyber appellate tribunal on any question of fact or law arising out of such order. Such an appeal must be filed within 60 days from the date of communication of the decision or order of the cyber

appellate tribunal.

2. Criminal Penalties

The process described above applies to "contraventions" under Chapter X of the Act. In adition to being liable to pay compensation, in the cases falling under section 3, such offenders may also be liable for criminal penalties such as imprisonment and fines, 12

3. Cognizance of offences and investigation

Section 78 of the IT Act empowers police officers of the rank of Inspectors and above to investigate offences under the IT Act.

Manystates have set up dedicated cyber crime police stations to investigate offence under this Act. Thus, for example, the State of Karnataka has set up a special cyber crime police station responsible for investigating all offences under the IT Act with respect to the entire territory of Karnataka.

Although there is no time limit prescribed by the IT Act or the Code of Criminal Procedure with respect to when an FIR must be filed, in general, courts tend to take an adverse view when a significant delay has occurred between the time of occurrence of an offence and it's reporting to the nearest police station.

The Code of Criminal Procedure forbids courts from taking cognizance of cases after three years "if the offence is punishable with imprisonment for a term exceeding one year but not exceeding three years". Where either the commission of the offence was not known to the person aggrieved, or where it is not known by whom the offence committed, this period is computed from the date on which respectively the offence or the identity of the offender comes to the knowledge of the person aggrieved

No special procedure is prescribed for the trial of cyber offences and hence the general provisions of criminal procedure would apply with respect to investigation, charge sheet, trial, decision, sentencing and appeal.

4. International Obligations Pertaining to Privacy

India is a signatory to the International Covenant on Civil and Political Rights which explicity individuals to approach the National Human Rights Commission or any of the State Human Rights Commissions for redress of human rights infringed under this convention.

Apart from this, there are no regional conventions that deal specifically with privacy. India has signed and ratified the international Convention for the Suppression of Terrorist Bombings and the International Convention for the Suppression of the Financing of Terrorism. India is a

 [ISSN 2581-5369]

signatory to the SAARC Convention on Mutual Assistance in Criminal Matters as well as several bilateral treaties on mutual legal assistance. These treaties typically requires signatory states to provide mutual assistance in criminal matters, including, inter alia, "providing information, documents and records. -providing objects, including lending exhibits", "search and seizure", "taking evidence an obtaining statements;" etc.[49]

India is a signatory to 85 agreements (81 DTAAs and 4 TTEA agreements) on exchange of tax information. For instance. India has reportedly signed four tax Information Exchange Agreements (TIEAs) on the OECD Model each with the Governments of the Bahamas, Bermuda, Cayman Islands and the Isle of Mann-popular 'tax havens. These agreements enjoin the competent authorities' of each country to provide information 'upon request' about a variety of financial details including bank records and corporate information. The request must be made on the basis of evidence and fishing expeditions are not usually permitted. These agreements include standard Confidentiality clauses which require that the information only be disclosed to appropriate tax authorities for purposes of tax proceedings. They also exempt information disclosed to an attorney under attorney client privilege form being disclosed.

In addition, India has signed a number of Double Taxation avoidance Agreements which include information-sharing clauses. In June 2010, the Government approached the govermment of 65 countries to "specifically" provide for the sharing of bank-related information 26 Pursuant to this, most notably, in June 2011, the Indian Government entered revised DTAA with the Swiss government allowing India to "gain aces to the details of Indians' money, which is not accounted for, stashed in Swiss banks. Similarly, in the same amount, the government of Mauritius agreed to renegotiate is tax treaty with India. Mauritius agreed for more than 40% of total foreign direct investments (FDIs) to India most of which one suspected to be nothing more than treaty shopping arrangement to avoid paying tax. An OECD report on India current DT A with Mauritius points to vast gaps in the treaty including provisions requiring disclosure of information to the persons in respect to whom information or document had been sought and that Mauritius has not exchanged information over the last three years.

These treaties seem to have resulted in some information being shared. In October 2011, Pranab Mukherjee, the Finance Minister reported that, pursuant to these treaties, "Specific requests in 333 cases have been made by Indian authorities for obtaining information from foreign jurisdictions. Over 9,900 pieces of information regarding suspicious transactions by Indian citizens from several countries have been obtained which are now under different stages of

[49] SAARC Convention on mutual Assistance in Criminal Matters (2008)

 [ISSN 2581-5369]

investigation.

Although information obtained under DTAASs cannot be used for purposes other than tax proceedings, in June 2011, the Income Tax Department announced that it would re-negotiate this clause in its agreements to enable it to share information with other law enforcement agencies like the Central Bureau of Investigation and the Enforcement Directorate.

(D) Privacy Needs To Be Added As A Ground For Reasonable Restriction Under Article 19(2) Of The Constitution Of India

Privacy, in its simplest sense, allows each human being to be left alone in a core which is inviolable. Yet the autonomy of the individual is conditioned by her relationships with the rest of society. The overarching presence of state and non-state entities regulates aspects of social existence which bear upon the freedom of the individual. The preservation of constitutional liberty is, so to speak, work in progress. Challenges have to be addressed to existing problems. Equally, new challenges have to be dealt with in terms of a constitutional understanding of where liberty places an individual in the context of a social order.

The Indian constitution guarantees a fundamental right to privacy. This was upheld in a decision of a nine-judge constitutional bench of the Supreme Court in August 2017. This case was brought to the Supreme Court after the claim in the 2015 by Mukul Rohatgi, the then Attorney General stated that there is no constitutionally guaranteed right to privacy. This claim was denied by the nine-judge bench of the court, which found that the constitution does guarantee a right to privacy. Importantly, the case strikes down ***M.P Sharma*** and ***Kharak Singh***, to the extent that the 2017 judgment holds that Indian Constitution does uphold a right to privacy.

The Supreme Court Judgment also upholds the decisions made after Kharak Singh on privacy, subject to the above conditions. Thus it is important to understand the contours of the right to privacy and its restrictions in India from the other case law that exists;The right to privacy can be restricted by procedure established by law and this procedure would have to be just, fair and reasonable (***Maneka Gandhi v.Union of India***);Reasonable restrictions can be imposed on the right to privacy in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence; (Article 19(2) of the Constitution of India, 1950). The right to privacy can be restricted if there is an important countervailing interest which is superior to it. The right to privacy can be restricted if there is a compelling state interest to be served. (***Govind v. State of M.P. & Anr***.);

1. The rule aforesaid is subject to the exception, that any publication concerning the

aforesaid aspects becomes unobjectionable if such publication is based upon public records including court records. This is for the reason that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment by press and media among others. We are, however, of the opinion that in the interests of decency [Article 19(2)] an exception must be carved out to this rule, viz., a female who is the victim of a sexual assault, kidnap, abduction or a like offence should not further be subjected to the indignity of her name and the incident being publicised in press/media. The protection available under the right to privacy may not be available to a person who voluntarily introduces him- or herself into controversy. ***(R.rajagopal v.Union of India***).

2. No doubt the expression "*personal liberty*" is a comprehensive one and the right to move freely is an attribute of personal liberty. It is said that the freedom to move freely is carved out of personal liberty and, therefore, the expression "*personal liberty*" in Article 21 excludes that attribute. In our view, this is not the correct approach. Both are independent fundamental rights, though there is overlapping. There is no question of one being carved out of another. The fundamental right of life and personal liberty have many attributes and some of them are found in Article 19. If a person's fundamental right under Article 21 is infringed, the State can rely upon a law to sustain the action; but that cannot be a complete answer unless the said law satisfies the test laid down in Article 19(2) so far as the attributes covered by Article 19(1) are concerned. In other words, the State must satisfy that both the fundamental rights are not infringed by showing that there is a law and that it does amount to a reasonable restriction within the meaning of Article 19(2) of the Constitution. Similarly, Right to Privacy is carved out from Personal Liberty but is also subject to adhere restrictions under Article 19(2).

3. In the case of ***R.C. Cooper***, it was held that any law which deprives any person of the liberty guaranteed under Article 21 must not only be just, fair and reasonable, but must also satisfy that it does not at the same time violate one or some of the other fundamental rights enumerated under Article 19, by demonstrating that the law is strictly in compliance with one of the corresponding clauses 2 to 6 of Article 19.

4. The importance which the Court ascribes to privacy is evident from the fact that it did not await the eventual formulation of rules by Parliament and prescribed that in the meantime, certain procedural safeguards which it envisaged should be put into place.

 [ISSN 2581-5369]

5. It goes without saying that no legal right can be absolute. Every right has limitations. This aspect of the matter is conceded at the bar. Therefore, even a fundamental right to privacy has limitations. The limitations are to be identified on a case-to-case basis depending upon the nature of the privacy interest claimed. There are different standards of review to test infractions of fundamental rights. While the concept of reasonableness overarches Part III, it operates differently across Articles. Having emphatically interpreted the Constitution's liberty guarantee to contain a fundamental right of privacy, it is necessary to outline the manner in which such a right to privacy can be limited.

6. The options canvassed for limiting the right to privacy include an Article 14 type reasonableness enquiry55; limitation as per the express provisions of Article 19; a just, fair and reasonable basis (that is, substantive due process) for limitation per Article 21; and finally, a just, fair and reasonable standard per Article 21 plus the amorphous standard of 'compelling state interest'. The last of these four options is the highest standard of scrutiny56 that a court can adopt. It is from this menu that a standard of review for limiting the right of privacy needs to be chosen.

7. Another aspect of this is the right to pseudonymous speech where again the author of the information does not give his correct identity. In order for a person to express his/her thoughts and ideas, political, ethical, or otherwise a person requires a safe private sphere free from State or private interference. Therefore, the right to privacy which would protect one's privacy actually goes hand in hand with the right to freedom of information and transparency. Thus, the relationship between the freedom of expression and privacy does not have to be a zero sum game but rather can be a positive sum game where both rights exist not only to not diminish each other but actively support and enhance each other.

8. The court has to balance the rights of the person whose privacy has been invaded against the freedom of press and the right of public to disclosure of newsworthy information. The standard to be adopted for assessing as to whether the published material infracts the right to privacy of any individual is that of an ordinary man of common sense and prudence and not an out of ordinary or hyper-sensitive man.

9. The internet never forgets! This single line encapsulates one of the gravest concerns for privacy advocates vis-à-vis the internet and the online world. In what circumstances can an individual require the deletion of information pertaining to them

that has been circulated in the public domain. Although the right to privacy in the non online world has been described as the 'right to be left alone' that may not exactly translate into a right to be forgotten. In Spain there was a case where a person was arrested and the fact that he had a criminal record was publicized on the internet as well. In this case the court ruled that he had a right to be forgotten. The new draft EU Regulations have expressly talked about the right to be forgotten by including a right to demand the deletion of data no longer required for the purpose for which it was collected. However in India, the debate on data retention and the right to privacy has not yet reached such a level and data retention and verification requirements are still governed more by national security requirements rather than privacy issues.

(E) Restrictions imposed to protect right to privacy

1. The provisions in the Official Secrets Act, 1923 which speak to what material is protected from disclosure are binding to the press.
2. While reporting a crime such as rape or abduction, the name and photographs of the victims or other particulars related to their identity should not be published.60 Minor children and infants who are the offspring of sexual abuse or forcible marriage should not be identified or photographed A.I is so advanced that the photo are converted and are used in Adult websites and in other dangerous activities.
3. Newspapers should not publish or comment on evidence collected through investigative journalism when, after the accused is arrested and charged, the court takes up the case. This in effect gives a blessing to sting operations which would infringe the privacy of individuals in the public interest as using Ai the photo and voices can be formed as exact as real once.
4. Caste identification of a person or a particular class should be avoided.
5. If information is received from a confidential source, the confidence should be respected. The journalist cannot be compelled by the Press Council to disclose the source, but he/she will not be penalized if they choose to voluntarily disclose the source by leaking the data on online platforms.
6. Newspapers should exercise caution in representing news, comments, or information which has the potential to jeopardize, endanger, or harm the interests of the state, society, or the individual in order to ensure that reasonable restrictions may be imposed by law on the right to freedom of speech and expression to be adhered to.

 [ISSN 2581-5369]

7. It is an offense for the media or other such person to disclose the names, addresses or schools, or pictures of juveniles who are involved in a legal proceeding under the Act which would lead to their identification, unless permitted by the authority in charge of the inquiry.
8. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child-bearing and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned and would be liable in an action for damages.[63]
9. There are three exceptions to the above Rule:
    a. Position may, however, be different, if a person voluntarily thrusts himself into controversy or voluntarily invites or raises a controversy.
    b. Any publication concerning the aforesaid aspects becomes unobjectionable if such publication is based upon public records including court records. This is for the reason that once a matter becomes a matter of public record, the right to privacy no longer subsists and it becomes a legitimate subject for comment

(F) Summery

The freedom of expression and privacy in many ways support each other, as the right to express an opinion or thought freely often is protected by providing the individual the privacy to do so. In the context of the media, the right to privacy can be violated by press coverage both online and offline. There are many new ways in which the right to privacy and the freedom of expression relate to each other which have not been addressed strongly in Indian legislation, policy, or case law. For example the taking of photographs by individuals (not the press) has not been addressed, the ability for individuals to issue comments anonymously offline, and the 'right to be forgotten' online and offline have not been addressed. These issues are being addressed by many countries and at an international level. For example, the EU has proposed an amendment to the EU directive that would require companies holding data to allow users to withdraw the information from websites. The amendment, known as the "Right to be forgotten"[64] would give users the power to tell websites to permanently delete all personal data held about them. Websites would be held legally accountable and would face sanctions if they did not comply.

V. INDIAN JUDICIARY AND RIGHT TO PRIVACY

Judiciary plays a vital role in interpreting law and administering justice in a country. Judiciary is the final interpreter of the Constitution and watchdog of the Constitutional provisions in India. In a country where there is a Written Constitution, the judiciary is under obligation to maintain the rule of law.

Under a federal Constitution, where the power has been divided between Centre and State, the judiciary is assigned with the duty of arbitrator to resolve the disputes between two States inter se as well as between Centre and State or States. It is the duty of the court to keep constant vigilance over the exercise of legislative domain allotted to each Legislature and in case of any encroachment of either side, the decision of the court is final.

In India, the judicial hierarchy consists of the Supreme Court followed by High Courts and some sub-ordinate courts. Supreme Court is situated at the apex of the judicial hierarchy. The Constitution of India ensures an independent and impartial judiciary for the sake of larger public interest. An independent and impartial judiciary is an essential part of the efficient functioning of a democracy and moreover, it is the essence of a federal government too. Under the Constitution, it is also assigned with an additional duty to protect and safeguard the fundamental rights of the citizens of India.

In the case of ***Union of India v. Sankalchand Himatlal Seth***, Justice Untwalia has compared the judiciary to "a watching tower above all the big structures of the other limbs of the State the other limbs of the State as to whether they are working in accordance with the law and the Constitution, the Constitution being the supreme". With the passage of time, the judiciary has adopted different new techniques in order to carry out the faith of the common people over it. The dynamic approach of the judiciary at different times is able to raise the status of this machinery.

The power of judicial review is implicit in a Written Constitution and unless expressly excluded by a provision of the Constitution.. Dr. B. R. Ambedkar also supported strongly the absolute necessity of judicial review. According to him, 'the provision for judicial review and particularly for writ jurisdiction that gave a quick relief against the abridgement of fundamental rights constituted the heart of the Constitution, the very soul of it'. In the early 1980s, the role of the higher judiciary in India underwent a radical transformation. A new and radically different kind of litigation came into existence. Instead of being asked to resolved private disputes, the Supreme Court and High Courts were asked to deal with public grievances over flagrant human rights violations by State or to vindicate the public policies embodied in Statutes

 [ISSN 2581-5369]

or Constitutional provisions. This new type of judicial business is collectively called the "Public Interest Litigation". This new trend works as a wakeup call amongst the judges to take an active role to impart justice, where statutory law is not enough to meet all challenges, arises in a society where legislation has left ample scope for judges to traverse beyond the limits set forth because of the uncertainty of the law. This is termed as judicial activism.

Due to the deficiencies in the Executive's response to public apathy, the Supreme Court has used its interim directions to influence the quality of administration, making it more responsive than before to the Constitutional Ethics and Law. Prof. Upendra Baxi describes this gradual judicial takeover of the direction of administration in a particular area from the Executive as 'Creeping Jurisdiction'.

Law-making has assumed a new dimension through judicial activism. Judiciary has adopted a healthy trend of interpreting the law in the social context. It has proved to be the most effective instrument in protecting the basic human rights of the people including the right to privacy.

Right to privacy and the judiciary have a very close connection since ages. Judiciary is the pacesetter of privacy right in India. It is only because of the goodwill of the judiciary right to privacy is able to achieve present status in India. The decision of ***Maneka Gandhi's case*** has brought a revolutionary change after a wider interpretation of the term "life and liberty" under Art. 21 which eventually added various dimensions to the provision. Along with others, right to privacy is also included as an important element of life and personal liberty under Art. 21 of the Constitution. Since then, the judiciary has been eloquently interpreted right to privacy as an essential ingredient of the right to life and liberty.

Although, right to privacy has acquired constitutional status with the pace of time, yet, this right is not an absolute right. Reasonable restriction can be imposed if there is an issue of larger public interests. Moreover, when there is any conflict between right to privacy and public interest, the later prevails over the previous one.

Right to privacy evoked as an individual right long before ***Maneka Gandhi's case***. But this right did not receive any positive response. Even the judiciary also took very narrow views regarding the existence of privacy rights. Some of the judges in their minority opinion accepted the very existence of the right to privacy. However, in the present day, while interpreting right to privacy as a basic human right, many a time, the judiciary cites the examples of international conventions like the Universal Declaration of Human Rights, International Covenant on Civil and Political Rights, European Convention on Human Rights, etc., of which India is a signatory. Sometimes, Courts also take precedence of foreign judgment while dealing with cases relating

 [ISSN 2581-5369]

to right to privacy.

The Indian judiciary from time to time makes complete effort to establish the very existence of right to privacy of individuals under different aspects. The researcher while analyzing the various judgments of the Supreme Court has tentatively categorized right to privacy under the following heads –

- Right to privacy and Search and seizure
- Right to Information and Right to the privacy of patients
- Right to Privacy and Telephone Tapping
- Right to Know and Right to Privacy of Undertrials
- Right to Publication and Right to privacy
- Right to Privacy and Matrimonial Rights
- Right to privacy and Right to reputation
- Right to privacy and Right to live with dignity
- Right to privacy and Protection of the identity of rape victims
- Right to privacy and Easement right
- Freedom of Press and Right to Privacy

(A) Recent Developments On Right To Privacy

Very recently, the Supreme Court in ***K. S. Puttaswamy v. Union of India*** has given a very wider interpretation to the right to privacy and established the right as a fundamental right under the Constitution. In the instant case, a writ petition was filed challenging the Aadhar scheme on the ground of violation of fundamental rights of the innumerable citizen of India, namely, right to privacy falling under Art. 21 of the Constitution. The petitioner raised questions as to the constitutionality of the Aadhar project which aims at building a huge database of personal identity and biometric information covering every Indian. In this project, the government of India decided to provide all its citizens a unique identity called Aadhar card containing a 12-digit Aadhar number. The registration for this card was made mandatory so as to enable the people to file tax returns, opening bank accounts, etc. As a result of which all those who do not want to register themselves, are not left with any option. It is pertinent to mention that at the time when the petition was filed Aadhar scheme was not under the legislative parameters.

The question of whether or not privacy is a fundamental right considering the constitutional

challenge to the Aadhaar framework first arose in 2015 before a three-judge bench of the Supreme Court. The Attorney General had then argued that although bench of smaller strength in the ***case of Govind Singh, R. Rajagopal and PUCL*** affirms the existence of a constitutionally protected right to privacy, but larger benches of the Court in ***M.P Sharma (8 judge bench) and Kharak Singh (6 judge bench***) had refused to accept that the right to privacy was constitutionally protected, hence, Part -III of the Constitution does not guarantee such a fundamental right. Consequently, this bench referred the matter to a five-judge bench to ensure "institutional integrity and judicial discipline". Thereafter, the five-judge bench referred the constitutional question to an even larger bench of nine judges to pronounce authoritatively on the status of the right to privacy.

The Supreme Court overruled its earlier decision in ***M.P. Sharma and Kharak Singh's case***, but decided to scrutinize the reason for the decision in these cases while determining a much larger question, i.e., whether right to privacy is a constitutionally protected right or not. In order to understand the concept of privacy, the Court has been addressed on various aspects of privacy, international conventions and the origin and evolution of privacy.

The majority judgment authored by Dr. D.Y. Chandrachud, J.86 (on behalf of three other Judges) and five concurring judgments of the other five Judges have declared, in no uncertain terms and most authoritatively, right to privacy to be a fundamental right. The scope and ambit of right to privacy can be summarized from this judgment into the following features,

i. Privacy has always been a natural right: The correct position in this behalf has been established by a number of judgments starting from Govind Singh's case.

Various opinions conclude that:

a) privacy is a concomitant of the right of the individual to exercise control over his or her personality.

b) Privacy is the necessary condition precedent to the enjoyment of any of the guarantees in Part -III.

c) The fundamental right to privacy would cover at least three aspects

- intrusion with an individual's physical body,
- informational privacy, and
- privacy of choice.

d) One aspect of privacy is the right to control the dissemination of personal

information. And that every individual should have a right to be able to control exercise over his/her own life and image as portrayed in the world and to control commercial use of his/her identity.

ii. The sanctity of privacy lies in its functional relationship with dignity: Privacy ensures that a human being can lead a life of dignity by securing the inner recesses of the human personality from unwanted intrusions. While the legitimate expectation of privacy may vary from intimate zone to the private zone and from the private to the public arena, it is important to underscore that privacy is not lost or surrendered merely because the individual is in a public place. Further, privacy is a postulate of dignity itself. Also, privacy concerns arise when the State seeks to intrude into the body and the mind of the citizen.

iii. Privacy is intrinsic to freedom, liberty, and dignity: The right to privacy is inherent to the liberties guaranteed by Part-III of the Constitution and privacy is an element of human dignity. The fundamental right to privacy derives from Part-III of the Constitution and recognition of this right does not require a constitutional amendment. Privacy is more than merely a derivative constitutional right. It is the necessary basis of rights guaranteed in the text of the Constitution.

iv. Privacy has both positive and negative content: The negative content restrains the State from committing an intrusion upon the life and personal liberty of a citizen. Its positive content imposes an obligation on the State to take all necessary measures to protect the privacy of the individual.

v. Informational Privacy is a facet of right to privacy: The old adage that knowledge is power has stark implications for the position of individual where data is ubiquitous, an all-encompassing presence. Every transaction of an individual user leaves electronic tracks without her knowledge. Individually these information silos may seem inconsequential. In aggregation, information provides a picture of the beings. The challenges which big data poses to privacy emanate from both State and non-State entities.

vi. Right to privacy cannot be impinged without a just, fair and reasonable law: It has to fulfill the test of proportionality i.e.

- existence of a law;

 [ISSN 2581-5369]

- must serve a legitimate State aim; and
- proportionality.

Further, privacy is considered as a subset of personal liberty thereby accepting the minority opinion in ***Kharak Singh v. State of U.P. & Ors.*** Another significant jurisprudential development of this judgment is that right to privacy as a fundamental right is not limited to Art. 21. On the contrary, privacy resonates through the entirety of fundamental rights pertains to Part III of the Constitution particularly, Art.s 14, 19 and 21. Therefore, privacy as a right is intrinsic to freedom, liberty, and dignity. Privacy is also recognized as a natural right which inheres in individuals and is, thus, inalienable. In developing the aforesaid concepts, the Court has been receptive to the principles in international law and international instruments. It is a recognition of the fact that certain human rights cannot be confined within the bounds of the geographical location of a nation but have universal application. In the process, the Court accepts the concept of universalization of human rights, including the right to privacy as a human right and the good practices in developing and understanding such rights in other countries have been welcomed. In this hue, it can also be remarked that comparative law has played a very significant role in shaping the aforesaid judgment on privacy in Indian context, notwithstanding the fact that such comparative law has only a persuasive value.

(B) Summery

The contribution of the judiciary in anchoring right to privacy as a fundamental right is not exhaustive, but inclusive. Right to privacy has been marked as a significant right under the constitutional regime on account of countless efforts of the judiciary. In the above discussion, although it seems to us that initially Indian courts were reluctant to recognise right to privacy as an essential personal right, broad head of right to property, gradually, the courts' attitude has been changed towards the right and consequently, Indian courts in due course of time recognise right to privacy as an important human right.

Moreover, under the present communication and technological development, civilians hold a strong opinion to protect their personal information namely, private life, financial details, day-to-day transaction from being public. In addition to that recent trend of social networking, following cookies in online transactions, etc., including numerous reasons induces the courts to established right to privacy as a fundamental right within the spirit of the letter of Art. 21 of the Constitution. ***Justice Puttaswamy's case*** and ***Navtej Singh Johar's case*** set the milestone in rejuvenating privacy right as an important personal right.

VI. THE PERSONAL DATA PROTECTION BILL AND RIGHT TO PRIVACY

 [ISSN 2581-5369]

After a long decade of waiting the Government of India has brought about some ray of hope concerning the protection of data privacy through the Personal Data Protection Bill, 2018. The Union Government, on 31 July 2017, had constituted a committee chaired by Retd. Justice B N Srikrishna, former Judge of the Supreme Court of India to review data protection norms in the country and to make recommendations. The Committee recently released its report and the first draft of the Personal Data Protection Bill, 2018 which comprehensively addresses the processing of personal data where such data has been collected, disclosed, shared or otherwise processed within the territory of India. The bill has incorporated provisions and principles from Europe's General Data Protection Regulation (EUGDPR). The Draft Bill replaces the traditional concepts of data controller i.e. the entity which processes data and data subject.

The Bill has viewed the growth of the digital economy and the critical way of communication as a crucial point to the protection of information privacy. It signifies the right to privacy as the fundamental right and makes provision to protect the autonomy of individuals in relation to their personal data which is an important facet of informational privacy. The Bill tries to emphasize collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation of usage of personal data.

The Bill has inserted some provisions on data protection obligation in Chapter-II. Sec. 4 mandates the person who processes the personal data to respect the privacy of data principal. Under the Bill, purposes are made limited for the processing of personal data. Sec. 5 specifies that personal data can be processed only for clear, specific and lawful purposes as well as incidental purposes that a data principal reasonably expects to protect. It is pertinent to mention that data principal is a natural person to whom personal data relates to an individual or a Hindu undivided family or a company or a firm or an association of persons or a body of individuals or the State, and every artificial juridical person. Sec. 6 imposes limitations on the collection of personal data for processing. Not only that Sec. 7 also mandated on lawful processing of the personal data as per the provisions of the Bill. It is the duty of a data fiduciary to provide necessary information to the data principal during the collection of personal data. It also owes the duty of a data fiduciary to maintain data quality while processing the data of the data principal. No personal data can be retained by the data fiduciary more than the reasonable periods which is necessary to fulfill the purpose unless excessive periods to comply with the obligation.

The right to protect privacy of an individual is enumerated in the Universal Declaration of Human Rights, 1948 (UDHR) "*No one shall be subjected to arbitrary interference with his*

 [ISSN 2581-5369]

privacy, family, home or correspondence, or to attacks upon his honour and reputation Everyone has the right to the protection of the law against such interference or attacks."

The principle of Right to Privacy is also contained in International Covenant on Civil and Political Rights, 1976. The requirements under both the international treaty are that the state shall implement certain legislations to protect the right of privacy and attacks o reputation. As India is signatory to both the treaties, it is the mandate duty of India to pass such legislation but still India has not passed any separate and independent legislation dealing with the subject matter.

The Constitution of India does not explicitly guarantee fundamental right to Privacy though Judicial Activism has bought it within the realm of Fundamental rights. Article 21 states "no person shall be deprived of his life or personal liberty except the procedures established by law." The Supreme Court of India deduced the Right to Privacy from Article 21 wherein the court held that "personal liberty" means life free from any encroachments that is unsustainable in law. The court in a landmark judgment held that "the concept of liberty in Article 21 was comprehensive enough to include privacy and an unauthorized intrusion in to an individual's home and thus disturbance caused violates his personal liberty." In People's Union for ***Civil Liberties (PUCL) v Union of India***, the court explained right to privacy to be under Article 21 in consonance with Article 17 of International Covenant on Civil and Political Rights, 1968.10 The gross violations of the right to privacy encouraged the Judiciary to take a pro-active role in protecting the right and providing the affected person adequate compensation and damages.

It is important to note that for processing personal data the consent of the data principal is compulsory. As per Sec. 12(2) consent of the data principal to be valid, it must be free, informed, clear, specific and capable of withdrawn by him. However, personal data may be processed for any function of the Parliament or State Legislature or any function authorized by law for the benefit of the data principal. To comply with any order or judgment of court or tribunal or for any other reasonable purposes including the public interest, personal data may be processed.

Under the Act, for processing sensitive personal data express consent of the data principal is necessary. However, consent will be considered express consent only if it is clear and specifically made after the data principal is informed of the purpose of use. Very usually, personal sensitive data may be processed if is necessary for the function of the Parliament or State Legislature or if it is authorized by law for the exercise of any state function for the benefit of the data principal. Sensitive personal data may also be processed to comply with the order or judgment of any court or tribunal or to meet any medical emergency during an epidemic or

 [ISSN 2581-5369]

outbreak of disease.

In addition to the above, Sec. 23 of the Act directs the data fiduciary to ensure that personal data and sensitive personal data of children must be processed only to protect and advances the rights and best interests of the child. For processing the data belongs to a child, it is necessary to verify his age through appropriate mechanisms and express consent of the parent. There will be a guardian data fiduciary who operates commercial websites or online services directed at children or who process large volumes of personal data of children. A guardian data fiduciary will not be required to obtain parental consent if he provides counselling or child protection services to a child.

Data fiduciary shall ensure privacy while he implements policies and measures. It is the duty of the data fiduciary to design any organizational, managerial or technical system in such a way that does not cause harm to the data principal. Privacy of data principal should be protected throughout the processing of data collection to deletion and in achieving any legitimate interests of business. However, processing of personal data should be carried out in a transparent manner and the interest of the data principal shall also be accounted for at every stage of processing of personal data. Under the Act, there are some security safeguards having regard to the risks associated with such processing, and the likelihood and severity of the harm that may result from such processing. Accordingly, the data fiduciary and the data processor shall implement appropriate security safeguards including the use of methods such as, deidentification and encryption, steps necessary to protect the integrity of personal data and steps necessary to prevent misuse, unauthorized access to, modification, disclosure or destruction of personal data. The data fiduciary as well as data principal shall also take a review of such security measures periodically to ensure appropriate safeguards.

The Act made complete efforts to ensure the protection of the informational privacy of an individual by incorporating several provisions in it. Sec. 32 of the Act is one such example which deals with breach of personal data and relative measures to meet such breach. As per the provision, whenever there is any breach of personal data during processing, the data fiduciary shall notify the data principal nature, number of such breaches as well as possible harm and remedy for the harm. It is the duty of the data fiduciary to inform such breach of personal data to the Data Protection Authority as early as possible with a view to adopt some urgent measures to remedy the harm. Besides, the Authority shall require the data fiduciary to report the personal data breach to the data principal and direct the data fiduciary to take appropriate measures. The Data Authority shall display the details of the breach on its websites and also direct the data fiduciary to do the same. Moreover, the data fiduciary is under a duty to take a data protection

 [ISSN 2581-5369]

impact assessment in view of the risk of harm to the data principal where the data fiduciary intends to undertake any processing involving new technologies or large scale profiling or use of sensitive personal data such as genetic data or biometric data, etc. There is also some restriction over the cross-border transfer of personal data for which the data fiduciary has to ensure that one serving copy of personal data has been stored on a server or data center located in India.

The law of Personal Data Protection also inserts some penalty provisions for any kind of contravention or failure to comply with the provision in processing the personal data by the data fiduciary. Thus, it can be inferred that in the age of information and communication technology, this piece of social legislation is a sigh of relief against unwanted intrusion into personal data. If this legislation works properly, this is probably the first law with regard to the protection of privacy rights.

In United States, statutory protection towards right to privacy is available since long under different provisions. After the worldwide recognition of right to privacy under the UDHR as well as the European Convention of Human Rights, there has been great awakens on the right in U.S. Immediately preceding this, the U.S. Congress has enacted several legislations in order to protect right to privacy on different dimensions like, family, finance, trade and commerce, health and online, etc. Moreover, in 1974 a more specific Act, namely, the Privacy Act, 1974 was passed to suppress the growing violation of privacy rights and to regulate unwarranted intervention by certain agencies into personal affairs as well. Besides, there are several Acts which directly does not deal with privacy right but they ensure the protection of privacy rights on specific issues. The COPPA denotes here a special mention because this is the first privacy law for internet privacy which regulates the internet marketers that operates Web sites and collect personal information from children below the age of 13.

(A) The Privacy Act, 1974

The Privacy Act, 1974 is undoubtedly an important piece of legislation in United States and is very popularly recognised as “code of fair information practices”. The Act of 1974 was enacted with a purpose to balance the government’s need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasion of privacy stemming from federal agencies’ collection, maintenance, use and disclosure of personal information about them. Besides, four basic policy objectives of the Act are –

i. To restrict the disclosure of personally identifiable records maintained by agencies.

ii. To grant individuals increased right to access to agency records maintained on themselves.

iii. To grant individual's right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely or complete.

iv. To establish a code of "fair information practices" which require agencies to comply with statutory norms for collection, maintenance and dissemination of record.

The Privacy Act contains the provisions are as follows –

1. Conditions of disclosure to third parties:

This provision consists of two rule

A. The "No Disclosure Without Consent" Rule:

As per the rule, no agency shall disclose by any means any record which is contained in a system of record to any person or to any agency except a written request and also with the prior written consent of the individuals to whom the records pertain.

B. Twelve exceptions to the "No Disclosure Without Consent" Rule:

i. Disclosure to the officers and employees of the agency.

ii. Disclosing any records required by the Freedom of Information Act.

iii. For the routine use of records.

iv. Disclosure to Bureau of census.

v. For the statistical research.

vi. To the National Archives and Records Administration as a record.

vii. To any agency or instrumentality of any government jurisdiction under the control of United States for civil and criminal law enforcement activity.

viii. To any person pursuant to a showing of compelling situation affecting health or safety of an individual.

ix. To the either House of Congress or to the extent of any matter within its jurisdiction or any committee or sub-committee etc., of Congress.

x. To the Comptroller General or any authorised representatives in the course of performance of the duties of the Government Accountability Office.

 [ISSN 2581-5369]

xi. In pursuant to the order of a court of competent jurisdiction.

xii. To a consumer reporting agency under the Debt Collection Act.

2. Accounting of Certain Disclosures:

Under this provision, each agency must keep a record of the date, nature and purpose of each disclosure of a record to any person or agency. This accounting of disclosures must be kept for five years or the life of the record whichever is longer.

3. Individual's right to access:

Every individual may access to his records or any information about him to review the record and also have a copy of the record from the agency that maintains a system of records.

Thus, it can be simply inferred that the Privacy Act applies to the records of every individual held by an agency. The Act while prohibits disclosure of information without the written consent of the individual, but also keeps some exceptional grounds to it. Moreover, the Act also provides individuals with the right to access to and amendment their records. The Privacy Act mandates each United States Government agencies which are in the administrative and physical security systems to prevent the unauthorised release of personal information.

(B) Summery

Undoubtedly, right to privacy took the long run to get the constitutional status. It has been nurtured under the aegis of right to personal life and liberty in Art. 21 of the Constitution of India. Moreover, right to privacy has been regarded as an important component to restrict the freedom of speech and expression in Art. 19(1)(a). However, freedom of press and right to know which are two important emanations of freedom of speech and expression very often comes in conflict with right to privacy. Especially, trends of aggressive journalism like media trial and intrusive journalism like sting operation, etc., set an argumentative status for right to privacy. In the absence of sui generis legislation on privacy, it is very difficult to meet such a situation. However, ***K. S. Puttaswamy's case*** and the Personal Data Protection Bill bring some hope to the people and recognize this right as a significant personal right inherent in every human being, be it a child or an adult.

The lack of comprehensive legislation related to Privacy and data protection is in great demand as the foreign companies that are doing business in India are concerned for the transmission of confidential data into the country. The need for the law on data protection is paramount. Though data protection is not specifically mentioned in the statutes still after amendment in 2008 in IT Act and the new privacy bill is a huge step towards privacy norms. The only point to be noticed

is that the Bill shall be implemented as soon as possible with proper amendment to the last bill published in public domain. The Privacy Bill must be enacted with sound and effective provisions to ensure adequate safeguards to the collected data and its usage.

VII. RIGHT TO PRIVACY UNDER THE REGIME OF CRIMINAL JURISPRUDENCE

The law of crimes has drawn immense importance to mankind since the ages of civilization to curb the menace from society. All the civilization leads to a common goal of protecting human rights so that there would be a peaceful co-existence and every individual can live with dignity. The protection of human rights through the criminal justice system is the most cherished goal under the doctrine of rule of law in every democracy. The criminal jurisprudence in India is highly developed as supported by the judiciary. Indian penal laws are primarily governed by three Acts:

1. Code of Criminal Procedure, 1973
2. Indian Penal Code, 1960, and
3. Indian Evidence Act, 1872.

Where the interest is affected or likely to be affected by the act or omission of a man, criminal jurisprudence arises. It assures peaceful living of the member of society with dignity. The objects of criminal law are to protect the citizen from what is offensive or injurious, to provide a safeguard against exploitation, etc., and to preserve the public order or decency. Criminal law is the branch of public law which defines crimes, treats their nature and provides for their punishment.

Although, promotion and enlargement of human rights are one of the most valued goals of the criminal justice delivery system, under certain cases, criminal proceedings may raise serious privacy concerns of the individuals. Nevertheless, there is statutory protection of privacy during the judicial proceeding of a criminal trial, but, some of the investigation procedures such as, search and seizure, forensic tests, surveillance, etc., pose a serious threat to individual privacy.

(A) Right To Privacy v. Surveillance

Surveillance is watching over or monitoring of behaviour or activities especially the one who is under suspicion. Surveillance can be done by various means either by electronic equipment (such as, CCTV cameras, etc.) or through traditional way without technological methods (such as, human intelligence agents, etc.). It is a very purposeful method for both government and law enforcement agencies to monitor as well as investigat criminal activity in order to maintain social control.

 [ISSN 2581-5369]

Surveillance is a useful technique to establish a corpus delicti modus operandi linkage between crime and criminal, etc. It may be done in various ways –

1. Surveillance by law enforcement agencies
2. CCTV system or surveillance cameras
3. Computerised monitoring
4. Wire tapping or telephone tapping
5. Biometric surveillance
6. Aerial surveillance

Surveillance be whatever it is, may stand as a potential threat to civil liberties by breach of privacy on many occasions.

(B) Surveillance by law enforcement agencies

Surveillance is the most common process of investigation used by law enforcement agencies or the State against the suspected criminals. Surveillance by law enforcement agencies is the traditional method sustained in criminal cases. There have been many questions raises on the issue of surveillance by law enforcement agencies be it authorised or unauthorised. One of the core issues is – the invasion of right to privacy of a person. Although, right to privacy has not been explicitly endowed in the Constitution of India, the said right has been recognised as an integral part of right to life and personal liberty under Art. 21 of the Constitution.

One of the most controversial uses of AI technology is in the area of surveillance. AI-based surveillance systems have the potential to revolutionise law enforcement and security, but they also pose significant risks to privacy and civil liberties.

AI-based surveillance systems use algorithms to analyse vast amounts of data from a range of sources, including cameras, social media, and other online sources. This allows law enforcement and security agencies to monitor individuals and predict criminal activity before it occurs. While the use of AI-based surveillance systems may seem like a valuable tool in the fight against crime and terrorism, it raises concerns about privacy and civil liberties. Critics argue that these systems can be used to monitor and control individuals, potentially losing freedom and civil liberties.To make matters worse, the use of AI-based surveillance systems is not always transparent. It can be difficult for individuals to know when they are being monitored or for what purpose. This lack of transparency can erode trust in law enforcement and security agencies and create a sense of unease in the general public.To address these concerns, the use of AI-based surveillance systems must be subject to strict regulation and oversight. This

 [ISSN 2581-5369]

includes the development of clear policies and procedures for the use of these systems, as well as the establishment of independent oversight and review mechanisms.

The Supreme Court in its majority opinion did not agree on the constitutional safeguard to the right to privacy. In view of Justice Ayyangar, majority observed that there is a lack of privacy provision under the Constitution of India congruent to the Fourth Amendment to the American Constitution. While relying on the common law maxim, et domus suacuique est tutissimum refugium struck down the Regulation 236(b) as unconstitutional which authorises domiciliary visits at night. However, Justice Subba Rao in his dissenting minority opinion argued in favour of the right to privacy by holding that the breach of personal data does not include only right to free from the restriction on movement, but also free from encroachment on one's private data. He further said that although the Constitution does not expressly declare right to privacy as a fundamental right, the said right is an essential ingredient of personal liberty. He defined privacy as the right to be free from restriction or encroachments on his persons whether those restrictions are directly imposed or indirectly brought about by calculative measures and accordingly held all surveillance unconstitutional.

Law enforcement and security agencies must be transparent about when and how these systems are used, and individuals must be able to access information about how their data is being collected and used. The integration of AI-based surveillance systems has undoubtedly brought significant advantages to law enforcement and security agencies. However, it is crucial to acknowledge these systems' potential risks to our fundamental rights and freedoms. The lack of transparency and the potential for discrimination are just some of the concerns that must be addressed by regulatory bodies to ensure the protection of individual privacy and civil liberties.

The implementation of strict regulations and oversight mechanisms is a vital step towards creating a future where AI technologies are used to benefit society without compromising individual rights and freedoms. It is important to establish clear policies and procedures to govern the use of AI-based surveillance systems and ensure transparency in their application. Additionally, independent oversight and review mechanisms must be put in place to ensure accountability.

A few years later, similar question of surveillance vis-a-vis right to privacy again came before the Supreme Court in ***Govind Singh v. State of M. P.,*** regarding the validity of M.

P. Police Regulations 855 and 856 framed under Sec. 46(2) (e) of the Police Act authorising domiciliary visits by the police against whom reasonable material exists were violative of the fundamental right guaranteed in Art. 21 which also includes right to privacy.

 [ISSN 2581-5369]

Unlike ***Kharak Singh***, however, the Supreme Court held that the Regulation has the force of law which allows the State Government to make notifications giving effect to the provisions of the Act and therefore, it is valid. The Court undertook a more comprehensive analysis of right to privacy in the instant case by accepting a limited fundamental right to privacy as an emanation from Art.s 19(1) (a), (d) and 21. The Court further held that right to privacy is a part of life under Art. 21 of the Constitution.

Recently, The European Union (EU) Parliament has taken a significant step towards protecting individual privacy in the age of AI. A majority of the EU Parliament is now in favour of a proposal to ban the use of AI surveillance in public spaces. This proposal would prohibit the use of facial recognition and other forms of AI surveillance in public areas, except in cases where there is a specific public security threat. This decision reflects the growing concern about the potential for AI technology to be used in a way that infringes on individual privacy and other fundamental rights. By banning the use of AI surveillance in public, the EU Parliament is taking a strong stance toward ensuring that AI technology is developed and used in a way that respects individual privacy and other ethical considerations.

In my opinion, the use of AI technology in surveillance can only be justified if it is carried out in a responsible and ethical manner. By prioritising individual privacy and civil liberties, we can build a future where AI technologies are harnessed to enhance security and protect society, without sacrificing the values that define us as a free and democratic society.

(C) Technical data of forensic science v. Right to privacy

With the advancement of science and technology, many sophisticated tools of investigation have been developed. The high climbing graph of crime rate necessitates the state authority to use different scientific interrogation techniques to extract the truth where the offender leaves no physical evidence the data recorded or saved are leaked or fabrigated. The data test, lab-mapping test and narco-analysis test are the often-used forensic tools of interrogation. These are three main psycho-analytical tests are also at risk of data leakage.

(D) Summery

Prevention as well as punishment of the crime is an indispensable feature of every criminal justice system, at the same time, protection of human rights is also an important facet of every system governed by the rule of law. Criminal law has played a vital role in evolving many of our fundamental and inalienable rights. However, the implementation of these rights may vary in jurisdiction amongst the nations. The rights of suspects, or under-trials, or detainees, or convicts are equally important to that of a law-abiding citizen in every democratic society. But

 [ISSN 2581-5369]

it seems that many a time some inalienable rights, such as, right to privacy of the victims or undertrials got endangered in due course of criminal proceedings. It is significant to note that right to privacy is an important aspect under the criminal justice delivery system which is also recognised by many International Human Rights documents. Protection of various categories of human rights during as well as after investigation of a criminal trial is the basic pillar upon which every democracy is founded.

VIII. ISSUE AND FINDINGS

1. Privacy Challenges in the Age of AI

AI presents a challenge to the privacy of individuals and organisations because of the complexity of the algorithms used in AI systems. As AI becomes more advanced, it can make decisions based on subtle patterns in data that are difficult for humans to discern. This means that individuals may not even be aware that their personal data is being used to make decisions that affect them.

2. The Issue of Violation of Privacy

While AI technology offers many potential benefits, there are also several significant challenges posed by its use. One of the primary challenges is the potential for AI to be used to violate privacy. AI systems require vast amounts of (personal) data, and if this data falls into the wrong hands it can be used for nefarious purposes, such as identity theft or cyber bullying.

3. The Issue of Bias and Discrimination

Another challenge posed by AI technology is the potential for bias and discrimination. AI systems are only as unbiased as the data they are trained on; if that data is biased, the resulting system will be too. This can lead to discriminatory decisions that affect individuals based on factors such as race, gender, or socioeconomic status. It is essential to ensure that AI systems are trained on diverse data and regularly audited to prevent bias.

At first glance, the link between bias and discrimination in AI and privacy may not be immediately apparent. After all, privacy is often thought of as a separate issue related to the protection of personal information and the right to be left alone. However, the reality is that the two issues are intimately connected, and here's why.

To start with, it is important to note that many AI systems rely on data to make decisions. This data can come from a variety of sources, such as online activity, social media posts, and public records. While this data may seem innocuous at first, it can reveal a lot about a person's life, including their race, gender, religion, and political beliefs. As a result, if an AI system is biased

 [ISSN 2581-5369]

or discriminatory, it can use this data to perpetuate these biases, leading to unfair or even harmful outcomes for individuals.

For example, imagine an AI system used by a hiring company to screen job applications. If the system is biased against women or people of colour, it may use data about a candidate's gender or race to unfairly exclude them from consideration. This harms the individual applicant and perpetuates systemic inequalities in the workforce.

4. The Issue of Job Displacements for Workers

A third challenge posed by AI technology is the potential for job loss and economic disruption. As AI systems become more advanced, they are increasingly capable of performing tasks that were previously done by humans. This can lead to job displacement, economic disruption in certain industries, and the need for individuals to retrain for new roles But the issue of job loss is also connected to privacy in a number of important ways. For one thing, the economic disruption caused by AI technology can lead to increased financial insecurity for workers. This, in turn, can lead to a situation where individuals are forced to sacrifice their privacy to make ends meet.

For example, Imagine a worker has lost their job due to automation. They are struggling to pay their bills and make ends meet and are forced to turn to the gig economy to make money. In order to find work, they may be required to provide personal information to a platform, such as their location, work history, and ratings from previous clients. While this may be necessary to find work, it also raises serious concerns about privacy, as this data may be shared with third parties or used to target ads. However, the issue of privacy and job loss is not just about the gig economy. It also relates to the ways in which AI technology is used in the hiring process. For example, some companies use AI algorithms to screen job applicants, analyzing their social media activity or online behaviour to make decisions about their suitability for a particular role. This raises concerns about the accuracy of the data being used and questions about privacy, as job applicants may not be aware that this data is being collected and used in this way. Ultimately, the issue of job loss and economic disruption caused by AI technology is closely tied to privacy because it can lead to situations where individuals are forced to sacrifice their privacy in order to survive in a changing economy**.**

5. The Issue of Data Abuse Practices

Finally, another significant challenge posed by AI technology is the potential for misuse by bad actors. AI can be used to create convincing fake images and videos, which can be used to spread misinformation or even manipulate public opinion. Additionally, AI can be used to create highly

 [ISSN 2581-5369]

sophisticated phishing attacks, which can trick individuals into revealing sensitive information or clicking on malicious links.

The creation and dissemination of fake videos and images can have serious privacy implications. This is because these fabricated media often feature real people who may not have consented to their image being used in this way. This can lead to situations where individuals are harmed by the dissemination of fake media, either because it is used to spread false or damaging information about them or because it is used in a way that violates their privacy.

For example, Consider a case in which an evil actor uses artificial intelligence to create a fake video showing a politician engaging in illegal or immoral behaviour. Even if the video is clearly fake, it may still be shared widely on social media, leading to serious reputational harm for the politician in question. This not only violates their privacy but also has the potential to cause real-world harm.The most recent AI technology presents many challenges that must be addressed to ensure that it is used ethically and responsibly. One reason why recent AI software has been associated with these challenges is that it often relies on machine learning algorithms, which are trained on large amounts of data. If that data contains biases, the algorithms will also be biased, leading to situations where AI perpetuates existing inequalities and discrimination. As AI continues to evolve, it is essential that we remain vigilant in addressing these challenges to ensure that AI is used for the greater good rather than for nefarious purposes that negatively affect our rights to privacy.

(A) Summary of the concept: right to privacy

Privacy thus can be conceived what Edward Shils defines as a "zero-relationship" between two persons or groups or between a group and a person. By the phrase "zerorelationship" he meant – the absence of interaction or communication or perception within contexts in which such interaction, communication, or perception is practicable, i.e., within a common ecological situation, such as that arising from spatial contiguity or membership in a single embracing collectivity such as a family, a working group, and ultimately a whole society.

There is no hard and fast definition of privacy, as such, legal scholars attempt to explain the concept of privacy as per their own perception. Privacy is a multi-dimensional concept that involves various interests; hence, it is a difficult task to arrive at a satisfactory definition. Till date, the simplest and most appreciable definition of right to privacy is what Warren and Brandeis called 'a right to be let alone.' Undoubtedly, Warren and Brandeis were the persons who invoked the right to privacy in the late nineteenth century when common people were not very concern about the right. This endeavour of the duo author led to the development of the

right to privacy intending to give a new parameter to the right to life. However, Warren and Brandeis's analysis of right to privacy was not only confined to the protection against physical interference, it means to include the right to enjoy life – the right to be let alone.

Of late, Dean Prosser in 1960 widens up the concept of privacy as propounded by Warren and Brandeis. For Prosser, privacy was defined by Warren and Brandeis in terms of tort remedy which was limited and inadequate in scope. He, therefore, put forward 'four distinct torts' which evolve as a result of the violation of four different interests and these four interests becomes distinctive interests in privacy, such as,

- Intrusion upon the user's seclusion or solitude, or into his private affairs.
- Public disclosure of embarrassing facts about the user.
- Publicity which places the user into a false light in the public eye.
- Appropriation of user's name or likeliness for defendant's advantage.

In the modern context, privacy acquires significant importance from the instances of intrusiveness in society. Privacy violation arises either from the state action or from human activities. Right to privacy stands as a shield against all such intrusion and obstacles into personal life. In contemporary society, people fond of using the internet and

Under the situation, some sorts of autonomy are indispensable for every individual in society. Everyday every person losing sensitive personal information in different contexts whether meaningfully or unknowingly. Right to privacy assures the secluded zone free from any kind of unwarranted interference.

Thus, by analyzing the concept of privacy, the researcher achieves that

'right to privacy is that privilege which allows us to build our own space of individuality, self-realization and dignity; it creates an intimate shell where one's ethical, spiritual and personal affairs are safe from any kinds of interruption; it is the ability to decide as to what extent you may expose yourself to the world.'

(B) Findings

The need for recognition of privacy as a fundamental human right is a recent phenomenon and is the outcome of the transformation of the society from group to individual. Moreover, technological development has significantly contributed to the rising concern for the protection of privacy interests. At a minimum, privacy denotes not only the private domain of an individual but includes right to be free from governmental surveillance and intrusion.

 [ISSN 2581-5369]

Passion for privacy is an old phenomenon since ages among human society. Privacy was cited during ancient times in terms of enjoyment of property, not as a personal right. Henceforth, Edward Coke proclaims that "a man's house is his castle." The phrase has been interpreted based on the idea that house being a place of safety and refuge into a place where a man has central importance. Likewise, William Pitt, a Parliamentarian from England opined that a man within his house has the boldness against anything even against the King.

It is pertinent to mention the contribution of the Universal Declaration of Human Rights, 1948 in the emergence of right to privacy as a significant human right. Since then this right never looks back for want of recognition. UDHR recognition becomes a turning point for the right, because, thereafter many conventions on the international sphere came forward to recognise the right. The Convention on Rights of the Child draws a special mention as it ensures the privacy of children which encourage many countries to enact special laws on the protection of identity of child who are the victim of sexual offences. With the emergence of these conventions, the interpretation and scope of privacy as a right has been expanded to include various aspects of life and eventually receive the constitutional status.

The need for right to privacy becomes obvious every day. The constant governmental intercession in public life and the development of new technology which helps in digging out and monitoring everyone's personal affairs, make life miserable. Now-a-days, the use of CCTV in public places, institutions, private places become a common practice, but it threats to privacy when such gazettes are misused. Using biometric technology for surveillance of physiological and behavioural features of human beings again raises serious human rights concerns, more particularly privacy interests. Taking such serious threats to privacy into consideration, in the judgment of ***K. S. Puttswamy case***, it was suggested that although the government tries to create robust administration of data protection, such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state which includes, for instance, protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge.

In the age of AI, privacy has become an increasingly complex issue. With the vast amount of data being collected and analysed by companies and governments, individuals' private information is at greater risk than ever before.Some of these issues include invasive surveillance, which can erode individual autonomy and exacerbate power imbalances, and unauthorised data collection, which can compromise sensitive personal information and leave individuals vulnerable to cyber attacks. These problems are often compounded by the power of BigTech companies, which have vast amounts of data at their disposal and significant influence

 [ISSN 2581-5369]

over how that data is collected, analysed and used.

Let's take a closer look at the implications of each of these problems.

The Power of Big Tech on Data Big Tech companies have become some of the most powerful entities in the world, with enormous amounts of influence over the global economy and society as a whole. With the rise of AI and the coming shift to the metaverse, their power is only set to increase even further. Today, Big Tech companies like Google, Amazon, and Meta have access to vast amounts of data, giving them unprecedented power to influence consumer behaviour and shape the global economy. They are also increasingly involved in politics, as they have the ability to influence public opinion and shape government policy. As we move towards the metaverse, where people will live, work, and interact in a virtual environment, BigTech companies are likely to become even more powerful. The metaverse will generate the usage of data twenty times more than the internet today, creating even more opportunities for BigTech companies to leverage their data and influence. The metaverse will also allow BigTech companies to create entirely new virtual ecosystems, where they will have even more control over the user experience. This could create new opportunities for BigTech companies to monetise their platforms and exert even greater influence over society. However, with this power comes great responsibility. BigTech companies must be transparent about their data practices and ensure that the data they collect is used ethically and responsibly. They must also work to ensure that their platforms are inclusive and accessible to all rather than being controlled by a small group of powerful players. The rise of BigTech has given these companies unprecedented power, and their influence is only set to increase with the coming shift to the immersive internet. While this presents many exciting opportunities, Big Tech companies must take proactive measures to ensure that their power is used ethically and responsibly. By doing so, they can build a future where technology is used to benefit society as a whole rather than just a select few. Of course, it may be naive to think that Big Tech will do so voluntarily, so regulation will likely have to force Big Tech to take a different approach.

Data Collection and Use by AI Technologies One of the most significant impacts of AI technology is the way it collects and uses data. AI systems are designed to learn and improve through the analysis of vast amounts of data. As a result, the amount of personal data collected by AI systems continues to grow, raising concerns about privacy and data protection. We only have to look at the various generative AI tools, such as ChatGPT, Stable Diffusion or any of the other tools currently being developed, to see how our data (articles, images, videos, etc.) are being used, often without our consent. More importantly, the use of personal data by AI systems is not always transparent. The algorithms used in AI systems can be complex, and it can be

 [ISSN 2581-5369]

difficult for individuals to understand how their data is being used to make decisions that affect them. Lack of transparency can lead to distrust of AI systems and a feeling of unease.To address these concerns, it is essential that organisations and companies that use AI technology take proactive measures to protect individuals' privacy. This includes implementing strong data security protocols, ensuring that data is only used for the intended purpose, and designing AI systems that adhere to ethical principles. Needless to say, transparency in the use of personal data by AI systems is critical. Individuals must be able to understand how their data is being used and have the ability to control the use of their data. This includes the ability to opt out of data collection and to request that their data be deleted. By doing so, we can build a future where AI technologies are used to benefit society while protecting individuals' privacy and data protection.

IX. AI RELATED PRIVACY CONCERN: REAL- LIFE EXAMPLES

In the age of AI, our personal data is becoming increasingly valuable to organisations and businesses, and it is being used in ways that were once unimaginable. From facial recognition to predictive algorithms, AI is being used to collect, process, and analyse our personal information, often without our knowledge or consent.For instance, generative AI, such as text and image generation tools, has become increasingly popular in recent years, enabling individuals to create content that mimics human-produced media. However, the use of generative AI raises significant privacy concerns, as companies that develop these tools may collect and analyse the data entered by users as prompts.

Users may enter a wide range of information as prompts, including personal information, images, and other sensitive data. This information can be used to train and improve the generative AI models, but it also raises questions about data security and privacy. Companies must ensure that they have adequate safeguards in place to protect this data, such as implementing robust data security measures and encryption protocols and complying with relevant privacy laws and regulations.

At the same time, users should be aware of the risks associated with sharing personal information when using generative AI tools. They should carefully consider what information they enter as prompts and be aware of the data protection policies and practices of the companies that develop these tools.

Ultimately, it is important that both companies and individuals take steps to ensure that privacy is protected in the age of generative AI so that the benefits of these technologies can be realised in a safe and responsible way.

 [ISSN 2581-5369]

In the next section, we'll take a closer look at other pressing examples of privacy concerns in the age of AI and discuss their potential impact on individuals and society as a whole.

CASE 1. Google's Location Tracking

Due to privacy concerns, Google's location-tracking practices have come under intense scrutiny in recent years. The company tracks the location of its users, even when they have not given explicit permission for their location to be shared. This revelation came to light in 2018 when an Associated Press investigation found that Google services continued to store location data, even when users turned off location tracking. This was a clear breach of user trust and privacy, and Google faced significant backlash from users and privacy advocates. Since 2018, Google has changed its location tracking policies and improved transparency regarding how it collects and uses location data. However, concerns remain regarding the extent of data collected, how it is used, and who has access to it. As one of the world's largest tech companies, Google's actions have far-reaching implications for individuals and society at large. One of the biggest issues with Google's location tracking practices is the potential for the misuse of personal data. Location data is incredibly sensitive, and if it falls into the wrong hands, it can be used to track individuals' movements, monitor their behaviour, and even be used for criminal activities. The implications of location data being leaked or hacked can be dire, and it is essential for companies like Google to ensure that they have robust security measures in place to protect user data. Also, there is the issue of third-party access to user data, which can be used for advertising purposes or even sold to other companies for profit.

CASE 2. AI-Powered Recommendations: My Personal Experience with Google's Suggestion Engine

An example of privacy concerns in the age of AI is the invasive nature of Big Tech companies. I recently shared a personal experience I had about watching a show on Amazon Prime on Apple TV. Two days after finishing the show, I received news recommendations related to the show on a Google app on an iPhone, while I never watched that show on my iPhone. An alarming practice and it begs the question: does Google have full access to all of our apps and activities?

As someone who has been working with big data for over a decade, I know it is technically possible, but it is concerning that it is allowed. For this level of personalised recommendation to be made, Google would need to access information from other apps on the iPad (even with my privacy settings preventing this practice) or eavesdropping on my conversations using the microphone of my iPhone or iPad and connect it to the my Google account. Both are not allowed and are a massive breach of privacy.

 [ISSN 2581-5369]

The example of Google's suggestive algorithm highlights the significant privacy concerns in the age of AI. The fact that Google is able to make personalised recommendations based on seemingly unrelated activities raises questions about the company's access to our private data. While this level of personalisation is technically possible, it is important to consider the ethical implications of such practices. As we continue relying more on AI and big data, it is critical to ensure privacy is respected and protected. It is vital that companies and policymakers take the necessary steps to establish clear guidelines and regulations to ensure that AI technology is developed and used in a way that upholds fundamental human rights and values.

CASE 3. The Use of AI in Law Enforcement

One example of the use of AI in law enforcement is the deployment of predictive policing software. This software uses data analysis and machine learning algorithms to predict where crimes are most likely to occur and who is most likely to commit them. While this technology may sound promising, it has come under scrutiny for perpetuating biases and reinforcing existing prejudices. For example, some predictive policing systems have been found to unfairly target minority communities, leading to allegations of racial profiling and discrimination.

Another example of the use of AI in law enforcement is facial recognition technology. This technology uses algorithms to match images of people's faces to a database of known individuals, allowing law enforcement to identify and track individuals in real time. While facial recognition technology has the potential to help law enforcement solve crimes, it also raises concerns about privacy and civil liberties. In some cases, facial recognition systems have been found to misidentify individuals, leading to false accusations and wrongful arrests.

As law enforcement agencies integrate AI technologies, there is a risk that these systems may perpetuate and even exacerbate existing societal biases and injustices. Also, the use of AI in law enforcement raises questions about transparency and accountability. It can be difficult to understand how these systems operate and make decisions, making it crucial to develop regulations and oversight mechanisms to ensure that the use of AI is transparent, ethical, and respects individual rights and freedoms.

CASE 4. The Use of AI in Hiring and Recruitment

The use of AI in hiring and recruitment has become increasingly popular in recent years. Companies are turning to AI-powered tools to screen and select job candidates, citing benefits such as increased efficiency and objectivity. However, these tools can also raise significant concerns about fairness and bias. One notable example is the case of Amazon's AI-powered recruiting tool, which was found to discriminate against women because the system was trained

 [ISSN 2581-5369]

on resumes from mostly male candidates.

This highlights the potential for AI to perpetuate existing biases and discrimination, and the need for careful consideration and testing of these tools to ensure they are not inadvertently perpetuating unfair practices. As the use of AI in hiring and recruitment continues to grow, it is crucial that we prioritise transparency and accountability to prevent discrimination and ensure fairness in the workplace.

X. SUGGESTION AND RECOMMENDATION

From the findings of the in-depth study on right to privacy, the researcher prefers the following recommendation –

1. The concept of privacy is itself misleading and vague one. It is a multidimensional concept, so, many difficulties arise to lend it in an accurate definition. Therefore, appropriate interpretation of the term "right to privacy" is the essential requirement to get into a right perspective.
2. As right to privacy is a multi-faceted right, its extent is unlimited. Moreover, with the development of technology and sophistication of life, privacy concerns are also increasing under various dimensions. So, the magnitude of the right to privacy for different dimensions should be made clearer and more distinct so that the essence of the right to privacy is preserved.
3. As we continue to integrate AI into various aspects of our lives, it is clear that privacy and ethical considerations are becoming increasingly important. The potential benefits of AI are vast, but so are the risks associated with its use. As a society, we must take a proactive approach to address these challenges to protect individual privacy and ensure that AI is used ethically and responsibly.
4. Organisations and companies that use AI must prioritise privacy and ethical considerations in their AI systems' design and implementation. This includes being transparent about data collection and usage, ensuring data security, regularly auditing for bias and discrimination, and designing AI systems that adhere to ethical principles. Companies that prioritise these considerations are more likely to build trust with their customers, avoid reputational damage, and build stronger relationships with their stakeholders.
5. As AI continues to advance and transform the world, it is crucial that we do not lose sight of the importance of privacy and ethical considerations. By prioritising privacy

 [ISSN 2581-5369]

and adopting strong data protection policies, we can help ensure that AI technology is developed and used in a way that respects individual privacy and other ethical considerations.

6. Initiative must be taken to make the common people aware who are still unaware of what constitutes right to privacy so that they can make a justifiable claim to establish their right.
7. Possible consequences for the violation of privacy must be defined as well as available remedies so that one must think twice before interfering with other's personal matters.
8. The right to privacy comes into effect only in the event of a violation of the rights in the majority cases. Even in the present situation right to privacy is balanced against other competing interests, such as, 'societal interest' or 'public interest' and 'compelling state interest', etc. Therefore, there must be a reasonable proportionality test to reconcile the conflicting interests. That is to say, such a test would determine the balance as to secure the ends of justice and public interest at large at the same time.
9. Privacy is a fundamental human right, and as AI technology continues to advance, it is criticalthat we prioritise privacy and ensure that individuals' rights are protected. This requires a multifaceted approach that involves the cooperation of governments, organisations, and individuals. Governments should implement regulations to ensure that AI is developed and used in a way that respects individual privacy and other ethical considerations. Organisations should prioritise privacy as a core value and adopt strong data protection policies that respect individual privacy.
10. India is still in the infant stage of developing personal data protection laws. The Personal Data Protection Bill, 2018 which is pending due to some lacuna, must be made more specific and stringent so as to ensure the protection of data at all levels.
11. The Government of India may take initiative to comply with its international rectification as defined under the UDHR, ECHR, ICCPR, etc., for the protection and promotion of the right to privacy.
12. . It is also suggested to abide by the privacy principles defined by the Report of the Experts on Privacy by the A. P. Shah Committee and recommendation made therein while drafting the legislation.
13. Legislations that would be developed for the violation of the right to privacy should also contain penal provisions within it which should be distinguished according to the

degree of infringement of the right to privacy. In addition to that appropriate provisions should be incorporated for sanctions dealing with the non- implementation of the stated provisions.

14. Now-a-days people often are misguided regarding the fact that individuals data privacy and privacy of data domain are the same and can be claimed on equal grounds. So appropriate steps should be taken to make the common people aware of the limitations of privacy in the public domain and individual privacy. Both of these concepts should not be intermingled.

15. Though it cannot be denied that privacy laws are being developed for various aspects but they are not being able to keep pace with the advancement of technology. So, many a times they are not able to cater to the needs of certain technical issues that might arise. Hence, the privacy laws should be updated so that they can keep in touch with the present state-of-art development in the country.

16. Finally, individuals should be empowered with transparency and control over their personal data. By prioritising privacy and adopting strong data protection policies, we can help ensure that AI technology is developed and used in a way that is both effective and privacy-respecting, ultimately leading to a future where individuals can benefit from the transformative power of AI without sacrificing their fundamental right to privacy.

(A) Global Approaches to Protecting Privacy in the Age of AI

The issue of AI and privacy is a global concern, and countries around the world have taken various measures to protect their citizens' privacy. In the USA, the California Consumer Privacy Act (CCPA) is the most comprehensive privacy law, giving Californians the right to know what personal information companies collect and request deletion. The US government has also introduced several bills, such as the Consumer Online Privacy Rights Act (COPRA) and the SAFE DATA Act.

In **Europe**, the General Data Protection Regulation (GDPR) is the most significant privacy regulation, setting a global standard for privacy regulations. It provides a set of rules to protect the personal data of EU citizens and applies to all companies operating within the EU. For example, in 2020, the French data protection regulator fined Google 50 million euros for violating the GDPR. The European Union has also proposed a new regulation called the Digital Services Act, which aims to strengthen online privacy and give users more control over their data.

 [ISSN 2581-5369]

China has implemented several measures to protect citizens' privacy, including the Cybersecurity Law, which requires companies to protect personal information and gives citizens the right to know how their data is being used. However, the Chinese government has been criticised for using AI to monitor citizens' activities and suppress dissent. In 2020, the National People's Congress passed a new personal information protection law, which took effect in November 2021. The new law imposes stricter rules on companies collecting and processing personal information and introduces penalties for violations.

Australia has enacted laws such as the Privacy Act 1988, which regulates the handling of personal information by government agencies and private organisations and gives citizens the right to access and correct their personal information. However, critics argue that the Privacy Act is outdated and needs to be updated to address emerging privacy concerns posed by AI. In fact, in late 2022, the Australian government released a discussion paper outlining proposed reforms to the Privacy Act, including stronger penalties for breaches and a requirement for companies to conduct privacy impact assessments.Many other countries are taking different approaches to protecting their citizens' privacy in the age of AI, and the development of privacy laws is an ongoing process with changes and updates likely to happen in the future.While the responsibility of protecting privacy falls on many parties, including governments, companies, and individuals, it is essential for consumers to take an active role in protecting their personal information. By staying informed, utilising privacy tools and settings, and being mindful of their online activities, consumers can help safeguard their privacy in the age of AI.

XI. CONCLUSION

The Future of Privacy in the Age of AI. As AI technologies continue to advance and become more integrated into our daily lives, the future of privacy is at a critical crossroads. With the rise of the metaverse and the increasing amount of data we generate, it is essential that we begin to consider the future implications of these technologies for the security and privacy of our data.

The decisions we make today will have far-reaching consequences for future generations, and it is up to us to ensure that we build a future where AI technologies are used in a way that benefits society as a whole while also respecting and protecting individual rights and freedoms. In this section, we'll explore some of the potential opportunities for privacy in the age of AI and what steps we can take to shape a more positive future.

(A) The Need for Regulation

As AI systems become more sophisticated and are able to process and analyse vast amounts of data, the potential for misuse and abuse of this technology grows.

 [ISSN 2581-5369]

In order to ensure that AI technology is developed and used in a way that respects individual rights and freedoms, it is essential that it be subject to effective regulation and oversight. This includes not only the collection and use of data by AI systems but also the design and development of these systems to ensure that they are transparent, explainable, and unbiased.

Effective Regulation will require collaboration between governments, industry, and civil society to establish clear standards and guidelines for the ethical use of AI. This will also require ongoing monitoring and enforcement to ensure these standards are upheld.

Without proper regulation, there is a risk that the increasing use of AI technology will lead to further erosion of privacy and civil liberties, as well as exacerbating existing inequalities and biases in society. By establishing a regulatory framework for AI, we can help ensure that this powerful technology is used for the greater good while protecting individual rights and freedoms.

(B) The Importance of Data Security and Encryption

Data breaches and cyber-attacks can have severe consequences, such as identity theft, financial loss, and reputational damage. In recent years, several shigh profile databse breach have highlighted the importance of data security, and the use of encryption to protect sensitive information has become increasingly important.

Encryption is the process of converting information into an unreadable format to prevent unauthorised access. It provides a way to protect data both in storage and during transmission. Encryption is essential for protecting sensitive data, such as personal information, financial data, and trade secrets. As AI technology advances, the need for robust data security and encryption becomes even more critical. The vast amount of data that AI relies on means that any breach can have far-reaching consequences, making it essential to implement security measures to safeguard against data loss or theft.

For example, consider a healthcare organisation that uses AI technologies to analyse patient data. This data may include sensitive information such as medical histories, diagnoses, and treatment plans. If this data were to be stolen or accessed by unauthorised parties, it could have serious consequences for the patients involved. By using strong encryption to protect this data, the healthcare organisation can ensure that it remains confidential and secure.

Another example is a financial institution that uses AI to analyse customer data for fraud detection. The data collected by the institution may include personal and financial information, such as account numbers and transaction histories. If this data were to fall into the wrong hands, it could be used for identity theft or other fraudulent activities. By using encryption to protect

 [ISSN 2581-5369]

this data, the financial institution can prevent unauthorised access and keep its customers' information safe.

Both of these examples make the importance of data security and encryption clear. Organisations that use AI must take data security seriously and implement robust encryption measures to protect the sensitive data they collect. Failure to do so could result in serious consequences for both the organisation and the individuals whose data has been compromised.

(C) The Correlation with Quantum Computing

The rise of quantum computing poses a significant threat to data security and encryption and underscores the need for increased investment in advanced encryption techniques.

Quantum computers can break traditional encryption algorithms currently used to secure sensitive data, such as financial transactions, medical records, and personal information. This is because quantum computers can perform calculations much faster than classical computers, allowing them to crack encryption keys and reveal the underlying data.

To address this threat, researchers and industry experts are developing new encryption techniques that are specifically designed to resist quantum computing attacks. These include post-quantum cryptography, which uses mathematical problems that are believed to be resistant to quantum computers, and quantum key distribution, which enables the secure exchange of cryptographic keys over long distances.

As the development of quantum computing technology continues, it is essential that organisations and governments take steps to ensure the security of their sensitive data. This includes investing in advanced encryption techniques specifically designed to resist quantum computing attacks and implementing robust data security measures to prevent unauthorised access and data breaches.

(D) The Role of Consumers in Protecting their Privacy

Protecting our privacy is more important than ever. While regulations and data security measures can provide some level of protection, individuals also play a vital role in protecting their own privacy. Consumers can take several steps to safeguard their personal information.

First, it is essential to understand what data is being collected and how it is being used. This information can usually be found in privacy policies and terms of service agreements. Consumers should take the time to read and understand these documents before using any products or services that collect their data.

Second, individuals can take advantage of privacy tools and settings that are often available

 [ISSN 2581-5369]

within software and social media platforms. For example, many websites offer the option to opt out of targeted advertising or limit data sharing with third-party companies. Similarly, social media platforms often provide privacy settings to control who can view or access personal information.

Lastly, consumers should be mindful of their online activities and the information they choose to share. Social media posts, online purchases, and even simple web searches can reveal personal information that could be used to compromise privacy. Being aware of the information that is being shared and taking steps to limit its dissemination can go a long way in protecting personal privacy.

(E) The Possibility of Decentralised AI Technologies

The rise of blockchain technology has opened up new possibilities for decentralised AI technologies. Decentralised AI refers to a system where artificial intelligence algorithms are distributed across a network of devices rather than being centrally located on a server. This allows for greater privacy and security, as well as more efficient processing power.

One potential application of decentralised AI is in healthcare. Currently, many healthcare organisations struggle to share patient data securely and efficiently due to privacy concerns and data protection regulations. Decentralised AI could enable healthcare providers to securely share patient data while also protecting patient privacy. For example, a patient's medical records could be stored on a blockchain, and AI algorithms could be used to analyse the data and provide personalised treatment recommendations without compromising the patient's privacy.

Another potential application of decentralised AI is in the development of autonomous vehicles. Decentralised AI could enable vehicles to communicate with each other in real time, making it possible for them to coordinate and navigate without the need for a central server. This would increase the efficiency and safety of autonomous vehicles while also reducing the risk of cyber attacks.

The following are some applications and use cases paving the way for a more secure and decentralised future for AI technologies.

a. Ocean Protocol

Ocean Protocol is a decentralised data exchange platform that enables secure and private data sharing for artificial intelligence and other applications. It is built on blockchain technology and uses smart contracts to facilitate data exchange and ensure that data providers are fairly compensated for their contributions. The platform enables data scientists, developers, and

researchers to access and use data from various sources, including individuals, companies, and public institutions, while ensuring the data's privacy and security.

Ocean Protocol is an example of decentralised AI technology because it operates on a decentralised network of nodes rather than relying on a central server. This means that the data and AI algorithms are distributed across a network of devices, making it more difficult for cyber attacks to compromise the system. In addition, because the data is decentralised, no single entity has control over the data or the algorithms, which can provide greater transparency and accountability.

Another key feature of Ocean Protocol is its focus on data privacy. The platform enables data providers to share their data without compromising their privacy, as the data can be stored on a blockchain and accessed only by those who have been granted permission. This makes it possible for individuals and companies to share their data in a secure, transparent, and fair way.

b. SingularityNET

SingularityNET is a decentralised platform that enables the creation and sharing of AI algorithms and services. It allows developers, data scientists, and researchers to create and collaborate on AI services, which can then be accessed and used by others through a decentralised network of nodes. The platform is built on blockchain technology, ensuring data and algorithms' security and privacy.

As a decentralised technology, SingularityNET is focused on democratising AI. The platform allows anyone to access and use AI algorithms and services, regardless of their technical expertise or financial resources. This makes it possible for individuals and companies to create and deploy AI solutions that might not otherwise be feasible, which can help drive innovation and promote social and economic progress.

c. DeepBrain Chain

DeepBrain Chain is a blockchain-based platform that enables secure and private AI computing. The platform allows AI developers and data scientists to rent computing resources from a decentralised network of nodes rather than having to rely on a central server. By using the power of blockchain technology, DeepBrain Chain provides a more cost-effective and efficient way for developers to access the computing power they need to build and run AI algorithms and applications.

One of the key features of DeepBrain Chain is its focus on privacy and security. The platform allows users to rent computing resources without having to reveal the details of their algorithms

or data, which can help protect their intellectual property and ensure the security of their projects.

This makes DeepBrain Chain a popular choice for companies and individuals who are working on sensitive or confidential projects.

Another important aspect of DeepBrain Chain is its cost-effectiveness. Because the platform operates through a decentralised network of nodes, it can offer computing resources at a lower cost compared to traditional cloud computing services. This can help reduce the barriers to entry for AI developers and data scientists, making it easier for them to create and deploy AI solutions.

The rise of decentralised AI technologies represents a major shift in the development and deployment of artificial intelligence. By leveraging blockchain technology, these platforms enable the creation, sharing, and access of AI algorithms and services in a more secure, transparent, and cost-effective manner.

Decentralised AI technologies also promote greater democratisation and accessibility to AI solutions, which can drive innovation and promote social and economic progress. As such, the rise of decentralised AI technologies is poised to revolutionise the way AI is developed, deployed, and used, and holds great promise for the future of the field.

(F) Final Thoughts

Protecting privacy in the age of AI is an issue that affects all of us as individuals and as members of society. It is critical that we take a multifaceted approach to this challenge, one that involves both technological and regulatory solutions. Decentralised AI technologies offer a promising way forward by enabling secure, transparent, and accessible AI services and algorithms. By leveraging these platforms, we can reduce the risks associated with centralised systems while promoting greater democratisation and accessibility of AI solutions.

At the same time, it is important that governments and regulatory bodies take an active role in overseeing the development and deployment of AI technologies. This includes the establishment of regulations, standards, and oversight bodies that can ensure the responsible and ethical use of AI while also protecting individual privacy rights.

Ultimately, protecting privacy in the age of AI requires collaboration and cooperation across a range of stakeholders, including government, industry, and civil society. By working together to develop and implement strategies that promote privacy and security, we can help ensure that AI's benefits are realised in a manner that is ethical, responsible, and sustainable and respects

 [ISSN 2581-5369]

the privacy and dignity of all individuals.

*****

 [ISSN 2581-5369]

XII. BIBLIOGRAPHY

(A) Books

- Basil S. Markesinis 1999.
- Bing Juris Jon, Data Protection in Norway" 1996.
- Chopra Deepti and Merrill Keith, -Cyber Cops, Cyber Criminals and Internel, New Delhi :
- I.K. International Ltd., 2002.
- Ghandi, P.R., The Human Rights Committee and the Right ofindividual Communication: Law and Practice, 1998.
- M.P. Jain, "The Constitution of India", VIIIth Edition, 2012.
- Dr. J.N. Pandey, "Constitutional Law of India", 52nd EDN edition (2015)
- P.M. Bakshi, " Commentary on the Constitution of India: An Exhaustive Article Wise Commentary on the Constitution of India Based on Plethora of Case Law", 2014.
- I.N. Pandey, "Constitutional Law of India", 2016.
- Anderson David A., The Failure of American Privacy Law, in Protecting Privacy, 139
- lan Hosein and Simon Daviesd, "Liberty on the Line" in Liberating Cyberspace, London: Pluto Press, 1998.
- James, Skone, Copinger and Shone James on Copyright, 13th ed., Sweet & Maxwell, 1991.
- Merrills, J.C. and Robertson A.H., Human Rights in Europe: A Study of the European Convention on Human Rights, 2001,
- Miller Arthur R., The Assault on Privacy -Computer Data Banks and Dossiers, 2nd ed., Ann
- Arbor: The University ofMichigan Press, 1971.
- Naikar Lohit D., -77ie Law Relating to Human Rights, Bangalore: Pulani and Pulani, 2004.
- Nirmal, Chairanjivi J. Human Rights in India, Historical, Social and Political Perspective, New Delhi: Oxford University Press, 2002.
- Ovey Clare & White, Robin C.., and Jacobs: European Convention on Human Rights, 2002.

 [ISSN 2581-5369]

- Radin Margaret Jane et al, -Privacy Online in Internet Commerce: The Emerging Legal 108 Framework, New York: Foundation Pres, 2002.

(B) Article /journals

- Alpa, Guido The Protection ofPrivacy in Italian Lav: Case Law in a Codified Legal System
- Tul. Euro. Civ. LF 1,2 (1997).
- Amelung Tilman Ulrich, Damage Awards For The Infringement Of Privacy - The German
- Approach, 14 Tul, Euro. Civ. LF 15, 19 (1999). • Beaney Wiliam M., -The Right to Privacy and American Lawl, 31 Law & Contemp. Probs. 253, 255 (1966)
- Bergmann Susanne, Publicity Rights in the U.S. and in Germany: A comparative Analysis, 19 Loy. L.A. Ent. L.J. 479, 480 (1999).
- Bryniczka Peter M, Irvine v. Talksport Ltd.: Snatching victoryfrom the jaws ofdefeat—English law nowoffers betterprotection ofcelebrities ' rights, 11 Sports Law. J. 171, 193 (2004).

(C) Website

- Vishalaxmi Singh, AN ANALYSIS OF PERSONAL DATA PROTECTION WITH SPECIAL EMPHASIS ON CURRENT AMENDMENTS AND PRIVACY BILL, International Journal of Law and Legal Jurisprudence Studies :ISSN:2348-8212:Volume 4 Issue1.http://ijlljs.in/wpcontent/uploads/2017/02/AN_ANALYSIS_OF_PERSONAL_DATA_PROTECTION_WITH_SPECIAL_EMPHASIS_ON_CURRENT_AMENDMENT S_AND_PRIVACY_BILL.pdf
- Warren & Brandeis, The Right to Privacy, HARVARD LAW REVIEW, Vol. IV,December15,1890.https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html
- SANGH PRIY GAOUTAM, THE RIGHT TO PRIVACY IN EMERGING DIGITAL ERA: INDIAN LEGAL SCENARIO, http://www.dbrau.org.in/attachment/SANGHPRIYGOUTAM.pdf
- CHANGMAI DAISY, THE RIGHT TO PRIVACY, GAUHATI UNIVERSITY, https://shodhganga.inflibnet.ac.in/handle/10603/301829

 [ISSN 2581-5369]

- AMALIA BERGGREN, SURVEILLANCE IN NINETYEIGHTY-FOUR, THE DISMANTLING OF PRIVACY IN OCEANIA, http://kau.diva-portal.org/smash/get/diva2:920358/FULLTEXT02.pdf
- Jayanta Bourah & Bandita Das, Right to Privacy and Data Protection under Indian Legal Regime, SSRN, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827766
- Universal Declaration on Human Rights, http://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf
- India UPR Stakeholder Report Right to Privacy.

*****

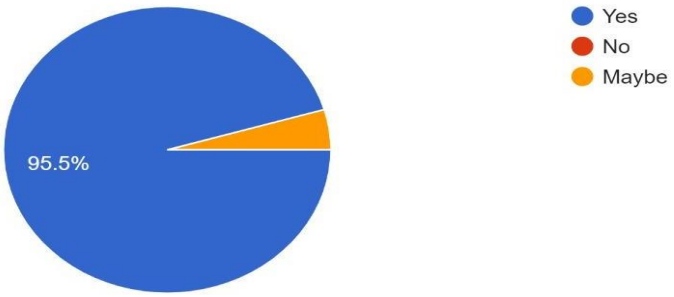
 [ISSN 2581-5369]

XIII. APPENDIX

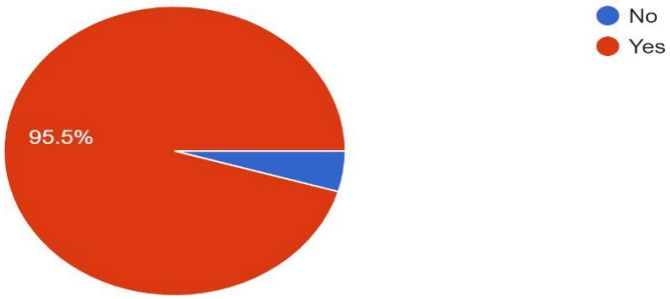
A student survey was created by the author to know the current scenario of people for Right to Privacy. https://forms.gle/Mpa6eWECWWCTTA2v7

Results of the survey are as follows:

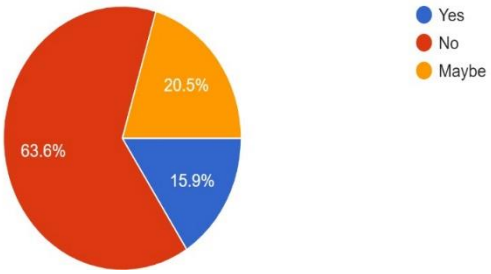
Do you understand what is Right to Privacy?
44 responses



Do you think Indian Privacy Laws needs stricter reforms?
44 responses

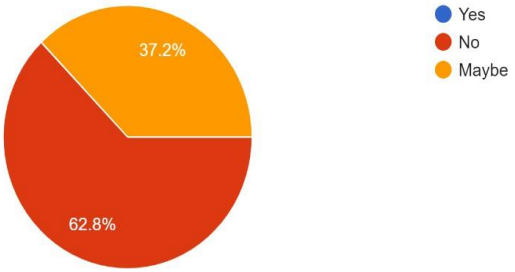


Do you feel safe while using your mobile phone with the risk that your Data may get leaked or get misused?
44 responses



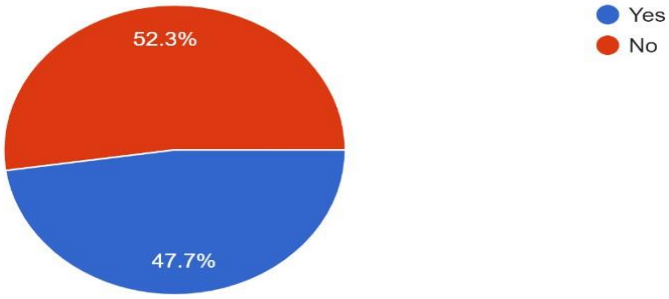
Is your Personal Information safe with Government or any Private Individual (including social media platforms)?

43 responses



Do you know about Right to be Forgotten and Right to be let Alone?

44 responses



*****