xIlkogretim Online - Elementary Education Online,2021; Vol 20 (Issue 5): pp.1868-1876
http://ilkogretim-online.org
doi: 10.17051/ilkonline.2021.01.199

Right to Privacy with special reference to the Cyber world

AAYUSHI KUMARI, Student, B.A.LLB. (Hons); X Sem, Law College Dehradun, Uttaranchal University, Dehradun.
KULJIT SINGH, Assistant Professor, Law College Dehradun, Uttaranchal University, Dehradun.

"Right to be let alone; right of a person to be free from unwarranted publicity; and right to live without unwarranted interference by the public in matters with which the public is not necessarily concerned."

ABSTRACT- 'Right to Privacy' is a fundamental right, which had beenclarified finally by the landmark as well as historical judgment,*K .S. Puttaswamy and ors.* v.*Union of India,*which is implicit in'Right to Life' under Article 21 of COI.There should be Right to Privacy, subject to reasonable restriction and it should be safeguarded by the law. Cyber privacy is controversial issue, but our country do not have any stringent laws to deal with this controversial issue. Right to privacy with special reference to the cyber security is a debatable issue. As we are in era of Globalisation and Digitalisation, it is shocking and amazingly unbelievable that we don't still have any stringent laws regarding this issue. Right to Privacy under Art. 21 r/w Art. 19(1) (a)i.e.,Right to Freedom of Speech and Expressioncannot be invoked against the commission ofcyber-crime by an individual completely, but vigilant steps are also taken by the State as well as the Judiciary. As of now, there are the Information and Technology Act, 2000 amended in the year 2008 and the Personal Data Protection Bill,2019 in India, but these Acts do not cover the broad boundaries of the cyber-crimes infringing the Right to Privacy. This Article mainly focuses on the Right to Privacy with special reference to cyberworld and also discusses about the role of Judiciary in interpreting the word Right to Privacy with reference to the cyber security. Besides, it throws light on the role of State and Legislation regarding the aforesaid issue and also suggests some measures to cope up with this issue.

Keywords: **Right to Privacy, CyberCrime, Cyber Privacy, Freedom of Speech**

I. INTRODUCTION

"Privacy is not something that I'm merely entitled to, it's an absolute prerequisite."

The meaning of the "Right to Privacy" cannot be explained in a single ruling, its scope and ambit are extensive and subject to the interpretation by the court rendering to the case and subject matter. Privacy is something that should be maintained and no one has the right to intrude on the privacy of anyone just like life of the person. Right to Privacy is devoted to Right to Life and both should be treated the same. Hence, Privacy should be valued the same like as a life of a person, because somehow privacy defines the personality of a person, which is treasured and needs to be shielded by the State. Many psychologists and sociologists have proclaimed that Right to Privacy is equivalent to Right to Life, which is fundamental right enshrined under Art. 21 of the Constitution of India. The term "Privacy" has not defined anywhere, neither in the Constitution of India nor in any other laws. It's a matter of interpretation, to extract the meaning and nature of this term to address the real concern. Under tort law, Cooley tries to define the term. Under tort law, pecuniary damages are provided, in case, anyone infringes anyone's privacy, but there is need for some strict laws regarding "Right to Privacy".

What is the meaning of Privacy?

It is correct to say, "Privacy" is a fundamental right, enclosed in several International Human Rights Instruments. It is treated as human rights, which talks about the human dignity as well as the personality, which makes a democratic form of nation and also comprises Right to Freedom of Speech and Expression and such other rights.

Actions that confine the "Right to Privacy", such as, "surveillance" and "censorship", can only be reasonable, only if they are prescribed under laws and must be required to reach a legitimate aim.

A revolution in "Information Technology" have aided formerly an unimagined practices of accumulating, storing, and sharing personal data, the "Right to Privacy" has been evolved tocondense State onuses regarding protection of individual data. However, various International Instruments preserve data

protection principles, further, many domestic legislatures had incorporated such principles under the National Laws.

As per the report of Special Rapporteur in respect of advancement and security of the privilege with opportunity of assessment and articulation stress that the *right to protection is supposed as a fundamental necessity for the acknowledgment of the privilege to the opportunity of articulation. Undue interfering with individual's privacy can both, directly and indirectly, limit the free development and exchange of ideas."*

Historical Background of Right to Privacy

It is correct to state that, "Right to Privacy" is not a new concept. Basically, it has been derived from common law. In law of Tort, incursion of privacy can be claimed and can claim the damages against infringement of individual's privacy. *One of the first cases on this issue was Semayne's Case (1604).* The said case regarding the entry into a property by the Sheriff of London in order to execute a valid writ. *Sir Edward Coke talks about the person's "Right to Privacy" as "the house of everyone is to him as his castle and fortress, as well for his defence against injury and violence, as for his repose".*However, the meaning of the term "Right to Privacy" were introduced in England in 19th century and the same was accepted by all, the Court held that if "there is an intrusion in a situation, where a person can reasonably expect his privacy to be respected, that intrusion will be capable of giving rise to liability unless the intrusion can be justified".

Outlining the International Protection on Right to Privacy

It is pertinent to mention here that "Right to Privacy" had been recognized by almost all the neighbouring countries and further, this right had been guaranteed by a numerous legislative provision, such as, "the Privacy Act, 1974" in U.S.A. and in England, there were various statutes, which talks about the protection of "Privacy" and "Data protection" of individuals are enlisted below;

- *Universal Declaration of Human Rights* states that "no one shall be subjected to arbitrary intrusion with his privacy, family, home or correspondence nor will his honor and reputation be attacked. Everyone has the right to the protection of the law against such interference or attacks."
- *International Covenant on Civil and Political Rights*(to which, India is a party) states that "no one shall be subjected to arbitrary or unlawful interference with his privacy, family, home, and correspondence, nor to unlawful attacks on his honour and reputation".
- *European Convention on Human Rights* states that "everyone has the right to respect his personal and family life, his home and his correspondence; no intervention by the public authority shall be as if it is in accordance with law and a healthier or moral security is necessary for a democratic society in the interests of national security, public safety or the economic well-being of the country or to protect the rights and freedoms of others."

Right to Privacy: Recent Parameters

"Privacy makes the person individuality, and thus, freedom."However, "Right to Privacy" is measured as the most comprehensive and the most valuable right of a civilized person. Privacy is defined as a 'state' of being free from disruption or disturbances in one's personal life or affairs, respectively notwithstanding that "universal concepts and legal rights were related to privacy as two distinct subjects and should be treated differently. Although, everyone has their own expression on privacy, the fudamental idea on which the concept of privacy derives, has been around for centuries. Moreover, the courts concerned are still emerging the concept in relation to the Right to Privacy through their judicial verdicts.

Prior to 1975: Right to Privacy not Expressly Recognised

Earlier, it is known that "Right to Privacy" has not been derived as a Fundamental Right under the Constitution of India. Further, in 1954, the Supreme Court of India in the case of re *M. P. Sharma v. Satish Chandra*, rejected the averments that there is any existence of "Right to Privacy" under Article 20(3), due to the absence of any provision consistent with the Fourth Amendment of the US Constitution.

Subsequently, the scope of the Right of Privacy is first considered in*Kharak Singh v. The State of Uttar Pradesh & others***,** which was related to the existence of certain rules that allow the surveillance of suspects. This right to privacy is considered a right to live alone. In the context of surveillance, it has been held that surveillance, if intrusive and seriously encroached upon the privacy of citizens, can violate the freedom of movement, which is Art. 19 (1)(d) and are guaranteed by Art. 21ofthe Constitution of India. Although, the Supreme Court began to accept certain points of minority view, the right to privacy was still awaiting its place in Indian constitutional jurisprudence.

During the Period 1975-2000: Right to Privacy implicit in Art. 21 of the Indian Constitution

In the case of *Govind v. State of Madhya Pradesh*, *Justice Mathew admitted that the Right to Privacy as a freedom under Arts. 19 (1) (a), (d), and 21, but the Right to Privacy is not an absolute right*. "Fundamental rights expressly guaranteed to a citizen have peninsular territories and the right to privacy is a fundamental right.Surveillance, by which visits of occupants are not always an unreasonable invasion of an individual's privacy, caused by the character and antecedents of a person, who is subject to surveillance, and the objects and limits within which surveillance is established. The right to privacy rests only with person not the place. In this judgment, Justice Matthews took into account American jurisprudence noting that the right to privacy clearly exists within the Peninsular Areas of Fundamental Rights under Part III of the Constitution . In another case *Smt. Maneka Gandhi v. Union of India & Anr*, the Supreme Court held that 'Personal Liberty' under Art. 21 exhibits various rights and includes many rights under this Article and also it ensures the protection under Art. 19 of the Indian Constitution. The Triple Test for any law meddling with Personal Liberty is this way:

- It provides a procedure established by the law;
- The procedure must undergo the test of one or more of the fundamental rightsexhibitingunder Art. 19 of the Indian Constitution, which can be applicable in a given situation and
- It must endure test of Article 14. The law and procedure authorizing interference with Personal Liberty and Right of Privacy must be just, fair and reasonable and must not be arbitrary, fanciful or oppressive in the nature. In *P.U.C.L.* v. *Union of India*, the Supreme Court observed that the Right to Privacy is the most crucial part of the Fundamental Right to Life preserved under Art. 21 of the Constitution and this right should be vested against the State only. Justice P.N Bhagawati also observed that "*the Right to Life and Personal Liberty also includes the right to live with human dignity and all that goes along with it, namely, the bare necessities of life, such as, proper nutrition, clothing and shelter and facilities for reading, writing and expressing oneself in diverse forms, freely moving about and mixing with fellow human beings. The actions, which may damage individual's dignity will constitute the violation of his right to live and it would have to be in accordance with reasonable, fair and just procedure established by the law, which stands the test of other fundamental rights*."

Hence, one could observe from the above cases that the Supreme Court had acknowledged that the human dignity implies expressing oneself in diverse forms and acknowledges the worth of all individuals in the society.

Positionin 21stCentury: Rightto PRIVACY as a FUNDAMENTAL RIGHT with REASONABLE RESTRICTION

In the most recent judgement of the case *K.S. Puttaswamy (Retd.) and Ors.* v. *Union of India*

*and Ors,*the apex court decided that if the comments were delivered in *M.P. Sharma and Ors*. v. *Satish Chandra and Ors*.and *Kharak Singh*v.*State of U.P. and Ors*,literally and originally read as law, the Fundamental Right under the Constitution of India and freedom under Art. 21 of the Indian Constitution will be deprived of the tenacity and vitality of the right to freedom in particular. In case of institutional integrity and judicial discipline,judgment of a court is superior to institutional integrity and judicial discipline should not be scrutinized by the lower court, but the ratio prevails. The case should be investigated and referred to within the jurisdiction of the court.

The operative part of the judgment in *Puttaswamy Case* overruled the decisions of*M. P. Sharma and Kharak Singh* that Right to Privacy is not a Fundamental Right under the Indian Constitution. As in the abovementioned case, which is decided by a 9-judge bench held that 'Right to Privacy' shall be treated as Right to Life under Art. 21 and shall be considered as Fundamental Right. Admittedly, the Supreme Court in the *Puttaswamy* judgment explained that the Government's access to personal data for legitimate national security concerns is a reasonable restriction on Right to Privacy. However, the Apex Court also reiterated that such exceptions must be narrowly tailored and must meet the four-fold test prescribed in the decision. In the next section, we shall analyse as to whether the traceability requirement satisfies the four-pronged test. Justice Chandrachud and kaul laid down the four-fold test as follows:

- *Legitimate Aim Stage*: The court will examine whether right to privacy is infringed or not.
- *Rational Nexus Stage*: The court will examine the balanced between the infringement of the right and reasonable restriction.

- *Necessity Stage*: Court will ensure that there should be less restrictive or equally effective to meet the aim in terms of restrictions on the right.
- *Balancing stage*: The State should balance between the rights and restrictions.

In case of failing in adherence of four test, then it will amount to violation of Art. 21.

Threat to Privacy in the Cyber World

In the Modern era, we totally depend on the computer and we use it to share important data, to store our data and also share with the help of internet, this becomes an opportunity for the person, who involves in cyber hacking or involves in stealing secret information to make undue advantage by way of malicious spyware or by computer bugs or may be collected from the information saved in the cookies folder.As the majority of the population within the ambit of social media, who use to share their photos and information on social media platforms, such as, Instagram, Facebook, Twitter, LinkedIn etc., these data can be misused easily, which is a threat to privacy and cyber criminals can also leak information by attaching malware to emails that discloses personal information about the recipient to the sender. Children are at risk, because they are vulnerable to be manipulated.

It has been found that there are about 400 million netizens, it can be said that almost every individual user, who chat and upload their photos and give personal information on social media platforms. A computer is a weapon or a tool for cyber criminals to steal personal information, so that it can be misused and poses a threat to privacy.

So far, there have been many malfunctions within the corporate world, where a company hires a third party to its advantage to steal secret information and important files and data from other companies and to defeat the contests and to become best-selling company. Nowadays, data theft from internet has become a major issue of concern and most of the countries enact laws related to protection of personal privacy.

It is pertinent to mention here that the developed country U.S. enacted the Children Internet Protection Act, 2000, by the Federal Trade Commission in order to protect the rights and interests of children while using the internet.

Privacy Issues regarding Personal Data and Information in Cyber Space

Today, the meaning of information has gained varied meanings in terms of its production, collection, analysis, storage, and access using cyber tools and the internet. In the same way, the definition of personal data also has been redefined. For instance, the personal information of the user can be easily generated by tracking his movement on various Internet platforms like social media, online transactions, browsing history etc. This again advances the dilemma of what constitutes private and personal information. *In the present netizen's world, there are two different and extreme views, i.e., one school believes in the protection of privacy of an individual as the paramount virtue, as it is in the real world; but the other school believes that there is no privacy at all, when an individual enters into the web world*. *In other words, there is confusion as to what privacy is and what it is not, in a cyber-world*. It is quite true that the protection once secured to individuals with geographical barriers has now been removed by World Wide Web, the advent of which threatens one's own personal existence and privacy even within the four walls of his own room.

Data Protection in Cyber Space: Legal Frame Work in India

Due to the increasing need to protect cyber data, various countries have periodically enacted laws, such as, the Data Protection Act, 2018 (U.K.), the Electronic Communications Privacy Act, 1986 (U.S.A.), etc. The European Union has implemented the General Data Protection Regulation (GDPR), which came into force on May 25, 2018, replacing the Data Protection Directive, 1995. In India, there is no comprehensive legal framework that deals with privacy issues. The major cyber challenges are dealt with by the Information Technology Act, 2008 (IT Act), which was implemented with the major objective of facilitating e-commerce and hence privacy was not the primary concern.

The 2011 Rules issued under the IT Act provide for compensation from a body corporate on account of any negligence in implementing and maintaining the reasonable security practices and procedures while

dealing with sensitive personal data or information. These Rules also provide for various contingencies, such as, consent requirement, the lawfulness of purpose, subsequent withdrawal of consent, etc. There is still a danger with these Rules as it permits the wrongdoer to evade responsibility, by the payment of compensation to the person, who suffered an infringement of his Privacy Right. Further, *the proviso to Rule 3, which defines sensitive personal data, exemption from any information, that is freely available or accessible in the public domain or under the Right to Information Act, 2005 or any other law for the time being in force, out of the purview of sensitive personal data or information for the purposes of these rules*. As per Rule 7, "a body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under these Rules". This again creates suspicion as to the extent of privacy that can be availed by an individual. Is the 'level of data protection' envisaged by the Rules sufficient to ensure the privacy rights of an individual, particularly, when Rule 7 permits the transfer of sensitive personal data or information including any information? What are the criteria for determining the level of data protection?

The relevant provisions of the Indian Penal Code could also be utilized to deal with cybercrimes affecting privacy. The liability will be fixed on the basis of general principles of criminal law and the convict will be punished. When the prosecution fails to establish the commission of an offence, there is no scope for privacy protection under criminal law. *So, there is a vacuum in the legislative framework as far as the protection of privacy rights in cyber space is concerned.*

Pursuant to the *Puttaswamy* verdict, which called upon the government to create a data protection regime to protect the privacy of the individual in compliance with the international obligations, a new legislative measure viz., 'Data Protection Bill, 2019' was introduced in Lok Sabha on December 11, 2019 to provide for the protection of personal data of individuals, and establishing a Data Protection Authority, for the same. It recommends a powerful regime that balances individual interests and legitimate concerns of the State. As the judgment in *Puttaswamy* cautions, "Formulation of a regime for data protection is a complex exercise that needs to be undertaken by the State after a careful balancing of requirements of privacy coupled with other values, which the protection of data subseries together with the legitimate concerns of the State." For example, the SupremeCourt observes that the Government could protect the data to ensure resources to reach the intended beneficiaries. However, the bench restrains itself from providing further guidance on the issue.

Parliamentary Report on Cyber Security and Right to Privacy

The Parliamentary committee on Information Technology in its 52nd Report on Cyber Security and Right to Privacy said that a big increase in cyberspace activities and access to internet use in India including lack of user-end discipline, inadequate protection of computer systems, and also the possibility of anonymous use of ICT allowing users to impersonate and canopy their trends of crime has emboldened more number of users experimenting with ICT abuse for criminal activities. The Committee is of the opinion that this aspect features a significant impact in blunting the deterrence effect created by the legal framework within the provisions of the Information and Technology Act, 2000, and related laws.
The Committee has listed several offences within the purview of cyber-crimes and also the remedies available within the present legal framework. Cyber stalking or stealthily following an individual and tracking his internet chats is punishable under Secs. 43 and 66 of the IT Act, 2000 while video voyeurism and violation of privacy could be a crime under Sec. 66E of the IT Act with a punishment of three years with a fine. The Department of Electronics and Information Technology (DeiTY) submitted to the Committee that with reference to the information regarding privacy-related cases under Sec 72 A of the IT Act the number of cases registered has risen from 15 in 2010 to 46 in 2012 while the number of persons arrested was 22 in 2012.

The committee members were of the opinion that given the nature of cyberspace, which is borderless, balancing cyber security, cybercrime and the right to privacy is an extremely complex task. Members were also unhappy with the fact that the Government was yet to formulate a legal framework on secrecy. It urged the Department of Electronics and Information Technology (DeiTY) in coordination with the Department of Personnel and

The Personal Data Protection Bill, 2019

The Government of India with increase in the number of cases related to cybercrime, it becomes the area of concern to make effective law to deal with such issues in order to bring such laws.The Committee drafted the bill and it placed on the floor of Parliament in the year 2019, known as the Personal Data protection Bill, 2019 (PDP) and it is the first bill, which talks about the data protection and also talks about the repealing the Sec. 43A of the IT Act, 2000.
The PDPBill is not confined within territorial jurisdiction, it also applies to the person, who resides outside the territory of India in relation to business carried out in India. It applies to both online and manual records. The PDP Bill establishes Data Protection Authority in India. It ensures the protection of data principles, unfair use of personal data, and ensure strict adherence of the law.

The PDP Bill protects the personal data of the individual, which includes the basic information of the individual i.e. name, sex, sex life, bank details, religion, and social status, etc. The Organization, whichis processing the data, should have compliance of the law before data processing and consent is required from the person before data is being processed.

The organization are instructed to bring some change from time to time according to need of hour and the type of personal data and these are required to update according to the subject matter of the case. The appointment of data protection officer to address the matter and ensure justice to the complainants.

"The Supreme Court specified that all individual should have the right to manage the profitable use of his or her distinctiveness and that the right of person to solely use and economically abuse their individuality and his own information, to regulate the data that is accessibleon the internet and to broadcast their private information for certain tenacities , which derive from this right. This is for the first time, the Supreme Court has specifically documented the right of person on his private data."

II. CONCLUSION

From the above-mentioned discussion, it can be concluded that with the arrival of the technology, people are more liable to the digital world to urge easily plagued by the cyber threats and cybercrime. Nowadays, we've heard about the cybercrime, such as, cyber engineering and cyber bulling. Both legislature and Judiciary should work together and may have vigilant to ensure fundamental rights i.e., right to privacy, so persons can enjoy their liberty freely and therefore the action of the State regarding discharging function associated with interference with the privacy, should be subject to the writ jurisdiction. Whenever question arises within the Judiciary regarding right to privacy, it should be ensured that the privacy shouldn't be revealed and will be respected unless the guilt of an individual is proved. Collection of secret data and data during trial or investigation, the consent of the concerned person is permitted. During collection of private data, many questions such as, whether a strict data collection policy has been released and made known to an individual; whether information is collected by authorized agency; whether purpose of knowledge is sufficiently transmitted to the an individual; whether consent, which is the most important requirement, is obtained; whether any commercial interest is involved; whether the terms of the Master -Service Agreement was verified and adhered to the premise of a 'techno-legal audit', so privacy and data security is ensured; etc., shall be analysed to look into the appropriateness of collection of information and data. After collection, the information should be kept secret so that nobody can take undue advantage from the such information.
The appropriate measures should be taken to maintain the confidentiality of personal information and private data from the unlawful use of those who intentionally tries to conceal the non-public data and private information. The stringent action should also be taken against whom who tries to invade the privacy. With the consent of the a person, his data should be processed and then such processing would be lawful processing. The State should ensure the law to safeguard the privacy and data confidentiality. There should be a valid contract between the information security and dataholder, then it would only be effective cyber security.

In a nutshell, in all the cyber activities i.e., the data privacy, data protection and encryption can only be protected, if Judiciary, legislature, and the society should work hand in hand, then cyber security will only beprovided to every individual. The collection of personal information without consent of the concerned person should be treated as unfair, injustice and subject to the arbitrariness. The Right to Privacy should be treated as the Core Fundamental Right, should be respected, should never be infringed at any cost and

should be just fair and reasonable. Every individual should be vigilant about its privacy on the online domain and in case of infringement, speedy justice should be delivered. According to Brandeis, J., "*Our Government is the potent, the omnipresent teacher; for good or ill, it teaches the whole people by its example". Nowadays, it is expected for the interest of an individual that there should be enactment of Privacy Laws for legal protection of data and also there should be vigilant Judiciary and the active role of States to deal with the issues related to the cyber security, cyber space and online data protection*.

III. SUGGESTIONS

Now, it can be suggested that 'Cyber Privacy' means, "Yearning of every person,where no one can interrupt its personal life and seek its personal information." It is observed that 'Privacy' is something like joke in the current scenario, but it is not for netizens (users in cyberspace) who are cyber experts.
In the current scenario, software in the machine provides data protection and advanced technology and application are used to breach the privacy of the individuals. However, Cyber Jurisprudence should be watch dog of online data privacy. Now, it is high time to bring some strong enforceable legal provisions to deal with online data protection and the issues relating to online privacy. There are a few suggestions,which are enlisted below on the basis of the need of current online data protection and online privacy as follows:

- There should be cyber privacy to the every individual while sharing of any information on the online portal and should have awareness about online data safety and protection.
- It is high time to impartthe cyber ethics to the netizens. Cyber ethics means the field to review the commerce with ethical issues strengthened, altered or shaped by computer and network skill.
- Law policies must comprise inclusive acquiescence method, administration of inner privacy, employees' training, responsiveness, self-regulatory efforts, corporate edge with privacy alertness, seminars and online dispute resolution mechanism. *Every sector of society whether it is private, government or corporate, should fulfil ISO/ IEC: 27001: Data security management standards.*
- The Internet Service Providers must firmly verify the entity's assembly or 'handshake' with the provider, and must have to ensure that the user should have installed apps which will ensure data safety. The personal information on the online portal should not be accessible by the strangers without permission.

REFERENCES

1. Black's Law Dictionary.
2. Marlon Brando, American Motion Picture and Stage Actor, 1924 – 2004.
3. Art.12, the Universal Declaration of Human Rights; Art. 14 the United Nations Convention on Migrant Workers , Art.16 the UN Convention of the Protection of the Child, Art.17 the International Covenant on Civil and Political Rights, International Covenant on Civil and Political Rights; Art.10 the regional conventions including of the African Charter on the Rights and Welfare of the Child, Art. 11 of the American Convention on Human Rights, Art. 4 of the African Union Principles on Freedom of Expression, Art. 5 of the American Declaration of the Rights and Duties of Man, Art. 21 of the Arab Charter on Human Rights, and Art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; JohannesburgPrinciples on National Security, Free Expression and Access to Information, Camden Principles on Freedom of Expression and Equality.
4. Art. 29, the Universal Declaration of Human Rights; General Comment No. 27, Adopted by The Human Rights Committee under Art. 40, Paragraph 4, of the International Covenant on Civil and Political Rights, CCPR/C/21/Rev.1/Add.9, November 2, 1999; See also Martin Scheinin, "Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism," 2009, A/ HRC/17/34.
5. Human Rights Committee general comment No. 16 (1988) on the right to respect of privacy, family, home and correspondence, and protection of honour and reputation (Art. 17) See: A/HRC/WG.6/13/MAR/3, para. 37
6. See the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (No. 108), 1981; the Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data (1980); and the Guidelines for the regulation of computerized personal data files (General

Assembly resolution 45/95 and E/CN.4/1990/72) As of December 2013, 101 countries had enacted data protection legislation.

7. As of December 2013, 101 countries had enacted data protection legislation; See: David Banisar, National Comprehensive Data Protection/Privacy Laws and Bills 2014 Map (January 28, 2014), available at: SSRN:http://ssrn.com/abstract1951416 or http://dx.doi.org/10.2139/ssrn.1951416.
8. A/HRC/23/40.
9. Sir Edward Coke.
10. Campbell v. MGN, (2004) UKHL 22.
11. Art. 12, theUniversal Declaration of Human Right,1948.
12. Art. 17, the International Covenant of Civil and Political Right,1966.
13. Art. 8, the European Convention on Human Right,1953.
14. Robert S. Peck, The Right to be Left Alone, 15 *HUM. RTS.* 26, 27 (1987).
15. Olmstead v. United States, 277 U.S. 438,478 (1928).
16. Sharda v.Sharam Pal, AIR 2003 SC 3450.
17. District Registrar & Collector v. Canara Bank, 2005(1) SCC 496.
18. Griswold v. Connecticut, 381 U.S. 479, 483 (1965).
19. AIR 1954 SC 300.
20. Art. 20 of the Constitution of India.
21. AIR 1963 SC 1295
22. State of West Bengal v. Ashok Dey, AIR 1972 SC 1660.
23. AIR 1975SC 1378.
24. Bowers v. Hardwick, 478 U.S. 186 (1986).
25. Charles Henry Alexandrowicz-Alexander,"American Influence on Constitutional Interpretation in India", 5 *AM. J. COMP. L.* 98, 100 (1956).
26. AIR1978SC 597.
27. AIR1978 SC 597.
28. (1997)1 SCC 30.
29. In P.U.C.L. v. Union of India, (1997)1 SCC 30.
30. Francis Coralie Mullin v. The Administrator, Union Territory of Delhi & Others, (1981)2 SCR 516.
31. 2015 (8) SCALE 747.
32. AIR1954 SC 300.
33. AIR 1963 SC 1.
34. Indore Development Authority v. Shailendra (Dead) Through LRS. & Ors,, Civil Appeal No.20982 Of 2017.
35. State of Haryana v. M/s G.D.Goenka Tourism Corporation Limited, SLP No. 8453/2017.
36. Available at:https://www.livelaw.in/breaking-right-privacy-fundamental-right-sc/?infinitescroll=1 (Last visited on March 21,2021).
37. Jasmine Alex"Privacy in Cyberspace", available at :https://www.livelaw.in/columns/privacy-in-cyber-space-157769 (Last visited on March20,2021).
38. Ruth Granson tries to comprehend privacy: "the concept of privacy is a central one in most discussions of modern Western life, yet only recently have there been serious efforts to analyze just what is meant by privacy." Yet another scholar, Judith DeCew, examines the diversity of privacy conceptions: "The idea of privacy which is employed by various legal scholars, is not always the same. Privacy may refer to the separation of spheres of activity, limits on governmental authority, forbidden knowledge and experience, limited access, and ideas of group membership consequently privacy is commonly taken to incorporate different clusters of interest". See for a wide reading, Robert A. Reilly, Conceptual Foundations of Privacy: Looking Backward Before Stepping Forward, 6 *RICH. J.L. & TECH.* 6 (Fall 1999).
39. Schwartz M Paul, "Property, Privacy and Personal Data", 117:2055 *Harvard Law Review*2065. May 2004,
40. Amended in the years 1994,2001,2006 and 2008 with various Acts,availableat https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1285.
41. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules), were issued under section 87(2) read with Section 43-A , IT Act.
42. The Data Protection Bill, 2019 suggests the removal of such clauses by appropriate amendments in IT Act.
43. Emphasis supplied. The wordings of the Rule illustrate irresponsible legislative drafting.

44. The scope of Indian Penal Code is limited to an extent as pointed out by the High Court of Bombay in *Gagan Harsh Sharma & Anr* v. *Maharashtra & Anr.*[Writ Petition(Criminal) No. 4361 0f 2018] that when an offence is well covered under the provisions of IT Act, the IT Act should be applied as *lex specialis* excluding IPC.
45. As per Dr.D.Y.Chandrachud, J., in Puttaswamy case, (2017) 10 SCALE 1at para 179.
46. Availableat:http://www.legalserviceindia.com/legal/article-3763-a-study-of-indian-law-on-protection-of-right-to-privacy-in-the-cyber-world.html.
47. Justice K.S. Puttaswamy (Retd.) v. Union of India (Case NO- WP (C) 494/2012),277 US 438,48.
48. Available at: https://www.albany.edu/~goel/classes/spring2006/workshop/cyberethics.pdf (Last visited on March 21, 2021).
49. The ISO/IEC 27000 family of standards helps organizations keep information assets secure. Using this family of standards will help organization manage the security of assets such as financial information, intellectual property, employee details or information entrusted to you by third parties. ISO/IEC 27001 is the best-known standard in the family providing requirements for an information security management system (ISMS), https://www.iso.org/isoiec27001-information-security.html (Last visited on March. 21, 2021).
50. George R. Jr. Lucas, Privacy, "Anonymity and Cyber Security", 5 *Amsterdam L.F.* 107, 114 (2013).