e-ISSN 2582-4570

EMERGING TECHNOLOGIES AND LAWS TO UPLIFT RIGHT TO PRIVACY

Dr. Narender Kumar Bishnoi[*] *Arvind Singh Kushwaha*[**]

Abstract

The issue of privacy is one of the rising legal concerns which requires an extra layer of protection of laws to encounter the ongoing technological changes which is affecting the individual's information including data. The misuse of technology in the administering of information presents crucial concerns most about the right to privacy. Recent application of Pegasus spyware raised the concern bar further as to how much protection can be granted as part of fundamental right. There is an extreme demand of practical regulations in the management of these challenges which must be formulated expeditiously corresponding to the set principles of freedom, liberty and human rights. The author in this paper have followed the foundations of privacy, through different international and national legal frame work along with areas recognising protection as privacy under Article 21 of the Indian Constitution. The paper essentially centres around the law of technological advancement of this right as a Fundamental right. The idea of security of such protection as data is the greatest possible level of requirement in this instinctively progressing time of today's world.

I. INTRODUCTION

The aspect of human rights remains one of the utmost concerns at every historical instance of time. These anthropological rights are of inherent nature which are available to every human being, irrespective of their race, sex, caste, religion, nationality, culture, dialectal etc. From time to time, these rights had been widened to include eachrelated viewpoint. The horizon of these rights is extended to inclusion of the right to human dignity, life, liberty, right to work, education, freedom from slavery and torture, freedom of opinion and expression, and countless additional civil liberties.[1]Human rights are universal, inalienable, interrelated, interdependent and indivisible in nature[2] which are intended to accomplish economic, social

[*] Assistant Professor of Law, Campus Law Centre, University of Delhi
[**] Ph.D. (Law) Scholar, University of Delhi

[1]UN Global Issues | Human Rights. Available at: https://www.un.org/en/global-issues/human-rights(last visited on Dec 09, 2021).

[2]UN Human Rights Office of the High Commissioner | Human Rights Indicators – A Guide to Measurement and Implementation. Available at: https://www.ohchr.org/documents/publications/human_rights_indicators_en.pdf(last visited on Dec 09, 2021).

and cultural rights.[3]Every person is entitled to these rights without any form of prejudice. Several occurrences can be indeed brought herein throughout the history to show the concern.

One of such fragments of human rights is the Right to privacy which brought utterly a challenging view by inclusion of it as a fundamental right. The privacy is linked with information secrecy, bodily discretion, communication space and territorial seclusionof any person. Yet, the right to privacy likewise other rights requires compatibility to legal and institutional standards related to ethics, law and human rights.The continuous rise of threats to privacy at many events such as at globalization, convergence and transmission of data over internet showed the necessity of identifying it as a basic right which must be accessible to all, and this issue is now at larger focus than at any point of time.[4]The importance of recognition of such rights are specially required contemplating the use of identity and private information in cyberworld. The present efforts might not be longer suitable to guard privacy principle, in chunk because "*big data enables new, non-obvious, unexpectedly powerful uses of data*".[5]

The rights related to privacy are not isolate in nature rather it had links with other social and economic factors, as these rights ensure: -

a. Protection against unauthorized spying
b. Protection against giving out and misuse of personal data and information
c. Protection against freedom of speech and expression
d. Protection against rights related to reputations
e. Boundaries over social media and internet-based platforms

[3] Human Rights Committee general comment No. 31 (2004) on the nature of the general legal obligation imposed on States parties to the Covenant and Committee on Economic, Social and Cultural Rights general comment No. 3 (1990) on the nature of States parties' obligations (art. 2, para.1). Available at: https://digitallibrary.un.org/record/533996?ln=en (last visited on Dec 09, 2021).

[4]Simon Davies "*Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity*", in Agre and Rotenberg (ed) "*Technology and Privacy: the new landscape*", MIT Press, 1997 p.143.

[5]Executive Office of the President of the United States, "*Big Data: Seizing Opportunities, Preserving Values*", May 2014 available at: www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf, p. 54 (last visited on Dec 09, 2021).

II. INTERNATIONAL FRAMEWORK

The 1948 UDHR[6] through Article 12 documented the modern privacy laws benchmark at international level by covering territorial, honour, and reputation privacy primarily. After its inclusion in UDHR, outlines of such right were also found in numerous later international frameworks. The ICCPR 1967[7] convention set out the privacy right under Article 17[8] by giving importance to principle of data collection whereby the collection of such data shall ensure no abuse of sensitive data. This trend was further continued by UN Convention on migrant workers (Article 14)[9] and UN Convention on Protection of the Child (Article 16)[10] which adopted similar set of words. The American Convent on Human Rights under Article 11[11]also sets the privacy rights in the same manner as UDHR. The General Comment No. 16 by Human Rights Committee (1988)[12] focused upon regulation of privacy rights by law. This general comment incorporated the collection, holding and assembling of personal and private information available on computers, servers, and other devices. It was also recommended that the states shall safeguard the personal information of individual to extent that it doesn't ends up in the hands of wrong user or unauthorised person and such safeguard shall be ensured through legal modes. Furthermore, every concerned individual shall be able to control his/her personal data.

[6]UN General Assembly, *Universal Declaration of Human Rights*, 10 December 1948, 217 A (III). Available at: https://www.un.org/en/about-us/universal-declaration-of-human-rights (last visited on Dec 09, 2021).

[7]UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171. Available at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx (last visited on Dec 09, 2021).

[8] Article 17. 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*.

[9]Article 14. No migrant worker or member of his or her family shall be subjected to *arbitrary or unlawful interference* with *his or her privacy*, family, home, correspondence or other communications, or to unlawful attacks on his or her *honour and reputation*. Each migrant worker and member of his or her family shall have the right to the protection of the law *against such interference or attacks*.

[10]Article 16. 1. 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*. 2. The child has the right to the protection of the law *against such interference or attacks*.

[11]Article 11. Right To Privacy. 1. Everyone has the right to have his *honor respected* and his *dignityrecognized*. 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*. 3. Everyone has the right to the protection of the law *against such interference or attacks*.

[12]General Comment No. 16 by Human Rights Committee. Available at: http://ccprcentre.org/page/view/general_comments/27798 (last visited on Dec 09, 2021).

The issue of privacy in digital age was elaborated by UN OHCHR through resolution 68\167 adopted by General Assembly.[13] The submitted report by Human Rights Council in 69th session (2014)gave perspective of the privacy rights in circumstance of internal and international observation and interference of communication and personal digital data on high level. The report also stated that the even non-state assemblies are progressing towardhigh tech surveillance proficiencies which continuously threatens the individual liberty and privacy. OECD Council (1980, updated later in 2013) under chairmanship of Justice MD Kirby also recommended fortification of privacy and trans-border surge of personal data.[14]The recommendations also included list of principles to be maintained as basic principles of national application. Moreover, there is required international cooperation for observances of principles set forth.

On regional level, both the European Commission of Human Rights and the European Court of Human Rights are exclusively enthusiastic in enforcement of right to privacy and had constantly worked toward the expansion of the idea. In the case of *X v. Iceland*[15], the ECHR stated that the private life doesn't end to individual only instead it extends to "*the right to establish and develop relationships with other human beings, especially in the emotional field for the development and fulfilment of one's own personality*." The execution of General Data Protection Regulation (2018) delivered significant safeguard of data protection and privacy in the European Union regional zone. Additionally, the enforcement of Federal Data Protection Act, 1977 among European countries provides further protection to data. At present, Germany continues as one of the strictest countries to have laws related to privacy.

III. RIGHT TO PRIVACY IN INDIAN LEGAL FRAMEWORK

Neither the constitution of India nor any other Indian laws specifically mention the right to privacy though protections were given to individuals to respect the individual liberty under Article 21 and other laws. Likewise other rights associated with Article 21, this right was also extracted out of the bare words of Article 21 as intrinsic part. However, this right is also

[13]UN General Assembly | Resolution No. 68/167. The Right to Privacy in Digital Age. Available at: https://undocs.org/A/RES/68/167 (last visited on Dec 09, 2021).
[14]OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Available at: https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (last visited on Dec 09, 2021).
[15]5 Eur Commin HR 86.87 (1976)

subject to few restrictions under the head 'procedure established by law'. The journey of recognition of this right can be observed through respective case laws:

1. *M.P. Sharmav. Satish Chandra*[16]: In 1950s, right to Privacy was claimed by the petitioner based on the Fourth American Constitutional Amendment against the principle of Self-incrimination under Article 20(3). However, the Hon'ble Supreme Court denied the protection under Article 20 as it might defeat the statutory provisions for searches and there is no legitimate obligation to follow the American constitution.
2. *Kharak Singh* v. *State of Uttar Pradesh*[17]*:* In the presentcase, though the Court relied on the United States judgment based on right to privacy, this judgment took a different approach by referring Article 21. The Hon'ble Supreme Court observed that the Indian Constitution doesn't guarantee right to privacy and an attempt to ascertain the movements of an individual by authorized agency is not an infringement of fundamental rights which are provided under the Part III of the Constitution.
3. *Gobind* v. *State of Madhya Pradesh*[18]*:* It was observed by Hon'ble Supreme Court that the issue related to privacy is an emanation of personal liberty, but it can be absolute in nature and a broad connotation of privacy will advancesignificant issues about the modesty of judicial dependence on a right which is not explicitly guaranteed under the Constitution.
4. *Justice K.S. Puttuswamy* v. *Union of India*[19]*:* It was decided by nine-judge bench of the Apex Court whereby it was held that right to privacy is sheltered as fundamental rights underneath Article 21 of the Indian Constitution. This landmark judgement introduced ramifications throughout both State and non-State actors and this judgement resulted into passing of a comprehensive laws and policies on privacy.

To keep pace with the ongoing developments, laws are required to be developed accordingly. This rule of interpretation is timeless and applies to almost every new emerging law which provide protection to the concerned individuals. The issue of privacy is not left untouched by this principle. Throughout time we came across to develop it as part of fundamental right, yet there is continuous need to protect this right considering ongoing changes in day-to-day world. When this issue was firstly raised in *MP Sharma*(1954) case, issue of privacy was concerned with self-incrimination principle. In the subsequent case of *Kharak Singh*(1964), it

[16] 1954 SCR 1077.
[17] 1964 SCR (1) 332.
[18] 1975 SCR (3) 946.
[19] (2017) 10 SCC 1: AIR 2017 SC 4161.

was associated with Article 21 as part of individual liberty. In the case of *Gobind Singh* (1975), the Supreme Court took a narrower approach by recognizing the right to privacy, yet they didn't declare it as fundamental right. However, the landmark case of *Puttuswamy* (2017), also commonly referred as Aadhar Judgement, expressly referred privacy right as a part of important rights under the Constitution. In furtherance to it, the case judgment also bound the state and non-state actors.

Apart from the Constitution, this trend can also be observed in other Indian laws. The Information Technology Act, 2000[20] along with the Indian Penal Code, 1860[21] and the Code of Criminal Procedure, 1973[22] protected the privacy of an individual from others by prescribing punishment. The IT Act of 2000 was significant introduction of new provisions against cybercrimes committed in cyberspace. The trend can be seen by introduction of these enactments in three different years covering almost a gap of 140 years, yet these laws are pioneering in nature which are being enjoyed till now. Additionally, time to time amendments in the provisions of these enactments keeps them updated to challenge new issues. For eg. The IT Amendment of 2008 and later introduction of Intermediaries guidelines and Interception in 2008, 2011, 2018 and 2021. However, these laws were primarily dealing with the relations between two individuals or one individual with an agency, but it doesn't cover the relations between an individual and government. The latter matter was covered under the constitution after the Aadhar Judgement. The introduction of privacy right as fundamental right laid an extra layer of protection against the government.

As there was shift of identity on the internet and other media platforms over period, the laws were required to keep pace with the technology. The communication surveillance is primarily covered under the Telegraph Act, 1855[23] (with respect to interception of calls) and Information Technology, 2000 (with respect to interception of electronic data). The telegraph Act even though of 1855 contains the basic required principles and mechanism required to protect interest of "public safety". The surveillance over telephone calls played an important role to eliminate the conspiracy affecting public interest at initial stage. This scenario was not covered under traditional laws and the communication over telephones showed a loophole. However, within a short span of time, the law covered the gap and became even stronger. Rule 419A was introduced in the Telegraph Rules, 2007 which enhanced the procedural

[20] Act No. 21 of 2000.
[21] Act No. 45 of 1860.
[22] Act No. 2 of 1974.
[23] Act No. 13 of 1885.

safeguards and laid down guidelines for interceptions. A similar legislative intent is represented under Section 69 of the IT Act[24] whereby it provides for interference, monitoring and decryption of digital data and information in public interest including sovereignty, integrity, defence and security of India, State and friendly nations, public order etc. This trending aspect can also be observed not only in criminal laws but also in civil laws whereby law recognized the communication and transmission of data over such connections. For e.g. Recipient rule, performance of online agreements, purchase and selling via shopping websites etc.

The issue of Data Protection is a new character of the privacy right in the virtual-world or cyberworld. Such data includes not only identity of individual but also his all details and data used by him. An individual makes his digital identity whenever he/she logs in on the internet-based platform using technology. The details entered by user are a matter of private right and breach of it is like injury to the victim. Though this part has been legally recognized in several countries, this issue is not yet covered by any data protection specific Indian laws. Since the enactment of European Union GDPR in 2018, concern was raised over the data protection. In Indian legal context, we had the case of *Puttuswamy* (2017)[25], which further pushed the question of safety of individual's data. With reference to this matter, the *Personal Data Protection Bill, 2019* was proposed in Lok Sabha on Dec 11, 2019. Few Highlights of the Bill are:

1. Divided data into 3 categories – personal, sensitive and critical data.

[24]Section 69. Power to issue directions for interception or monitoring or decryption of any information through any computer resource. -
(1) Where the Central Government or a State Government or any of its officers specially authorised by the Central Government or the State Government, as the case may be, in this behalf may, if satisfied that it is necessary or expedient to do in the interest of the sovereignty or integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above or for investigation of any offence, it may, subject to the provisions of sub-section (2), for reasons to be recorded in writing, by order, direct any agency of the appropriate Government to intercept, monitor or decrypt or cause to be intercepted or monitored or decrypted any information generated, transmitted, received or stored in any computer resource.
(2) The procedure and safeguards subject to which such interception or monitoring or decryption may be carried out, shall be such as may be prescribed.
(3) The subscriber or intermediary or any person in-charge of the computer resource shall, when called upon by any agency referred to in sub-section (1), extend all facilities and technical assistance to-
(a) provide access to or secure access to the computer resource generating, transmitting, receiving or storing such information; or
(b) intercept, monitor, or decrypt the information, as the case may be; or
(c) provide information stored in computer resource.
(4) The subscriber or intermediary or any person who fails to assist the agency referred to in sub-section (3) shall be punished with imprisonment for a term which may extend to seven years and shall also be liable to fine.
[25](2017) 10 SCC 1: AIR 2017 SC 4161.

2. Emphasis more on protection of personal data than protection of non-personal data.
3. To cover the gap as the present IT Act 2000 applies only to companies and not to the Government.
4. Regulates Individual's personal data and processing, collection and storage of personal information in form of data.
5. Use of *consent* by data principal for processing, collection and storage of his/her data.
6. Provided obligations for data fiduciaries for purpose, collection and storage limitations.
7. Made the offence punishable with fine and for grievance purposes, set up of Data Protection Authority comprising of field experts.
8. Power to exempt of any of agencies by the Government.

The bill will repeal Section 43A of the IT Act[26] which provides for compensation against failure of protection of data. The bill purposely intends to cover the ambit of personal data protection; however, the effectiveness of this bill is yet to be determined as it hasn't been implemented yet. Prior to this bill, there were two other related bills also which were introduced in the Houses earlier but not enacted yet i.e., Personal (Protection) Bill, 2013 and Data (Privacy and Protection) Bill, 2017. Thus, enactment of this bill remains one of the major concerns.

Recently on Dec 16, 2021, the Joint Parliament Committee on Personal Data Protection Bill, 2019 under the chairmanship of Shri P.P. Chaudhary presented recommendations on the bill introduced.[27]Few of the highlights of the recommendations were:

1. The Bill introduced will substantially cover the issue of privacy as fundamental right which emerged from the *Puttuswamy* judgment and also as under the recommendations of *Justice BN Sri Krishna* Committee (also known as *Data Protection Committee*)[28].

[26] Section 43A. Compensation for failure to protect data. Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

[27]Press Release (dt. 16 Dec 2021). Joint Committee on the Personal Data Protection Bill, 2019. Available at: http://164.100.47.193/lsscommittee/Joint%20Committee%20on%20the%20Personal%20Data%20Protection%20Bill,%202019/pr_files/Press%20Release%20on%20the%20presentation%20Report.pdf(last visited on Dec 17, 2021).

[28]A free and Fair Digital Economy. Report by Justice BN Srikrishna. Available at: https://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report.pdf (last visited on Dec 17, 2021).

2. The Bill shall cover both personal as well as non-personal data which shall be upheld by the Data Protection Authority (DPA).
3. The Bill shall be implemented in phase wise manner within a period of 24 months. This will benefit the legislative interest to overcome issues within time.
4. There shall be specific principles to guide and handle the data breach going on. Furthermore, the Committee enlisted 4 principles in order to maintain the right to privacy.
5. For sharing the personal data and sensitive personal data, there shall be a requirement of prior consent.
6. The Social media platforms shall be treated as publishers and such platforms shall be regulated under the bill.
7. There shall be alternative financial system in India as Ripple in USA and INSTEX in European Union etc. which will protect privacy as well as digital economy.
8. For faster procedure, the committee recommended that there shall be issuance of notice of breach within 72 hours of becoming aware of it.
9. The Data Protection Officer plays a vital role; thus, they shall be holding a key position in the management of company who must have adequate technological knowledge.
10. There shall be a system of single window for dealing with the subjects of complaints, penalties, compensation etc.

The incorporation of these recommendations will considerably improve the present condition as well as the intensifying issues of data breach. The committee also focused upon establishment of quite a few authorities assigned with different roles to cover the technical, legal, practical, management and academic aspect of the breaches. The inclusion of experts from earlier mentioned background which will keep the authorities efficient in order to deal with foreseeable events. Within the recommendations, the commission also focused upon the issue of liability by counting every person liable. Furthermore, the committee also asked the government to localize the technology in order to have a better hold of the offences taking places through data leaks.

In Mid Sept 2021, the issue of surveillance was uncovered further by the detection of use of Pegasus Project by the Government of India. This issue was raised before 3-judges bench of

the hon'ble Supreme Court through the case of *Manohar Lal Sharma v. Union of India*[29].It was argued by the petitioner that the Pegasus spyware was being misused by targeting journalists, ministers and opposition party members for their personal gain and not for public interest which is against the recently professed fundamental right to privacy. The Government had not denied the usage of the spyware but on July 22, 2021, IT Minister stated that Pegasus reports had '*no factual basis*', sufficient checks and balances are placed, and the power of surveillance is permitted under the Telegraph Act and IT Act. In the recent order dt. Oct 27, 2021, the Supreme Court noted that there are three key imperatives lying with the snoop allegations i.e.,"right to privacy of citizens, freedom of press and limits of national security as an alibi." The Hon'ble court also rejected the contentions linked with national security. Mentioning about the right to privacy, the hon'ble court stated that

> "*Privacy is not the singular concern of journalists or social activists…. In a democratic country governed by the rule of law, indiscriminate spying on individuals cannot be allowed except with sufficient statutory safeguards, by following the procedure established by law under the Constitution*."[30]

On the other hand, Pegasus running Israeli organization, NSO Group had acknowledged the involvement with Indian Government. However, the Israeli government had classified this spyware as cyber-arms and only national governments had access to purchase the spyware after the authorisation of the Israeli government. In response to the facts, the Supreme Court ordered an independent probe into the dispute by a 3-member committee. The case hasnot been decided yet.

IV. RIGHT TO BE FORGOTTEN

Right to be Forgotten is another dimension of Rights connected to privacy whereby it professesthe idea of removal of personal information over public platforms.Right to be forgotten arises from right to privacy under Article 21 and partially from Article 14. This right is more explicit aboutsafety of online data available in public domain, and it mentions that it should be limited to search engines only whereas the right to privacy has a much wider explanation of protecting all personal and sensitive information of individuals.This right

[29] Writ Petition (Crl) no. 314/2021.
[30] Ibid. Order Dt. Oct 27, 2021, Para 32 and Para 36.

gained importance from the case of *Google* v. *AEPD and Mario Costeja González*[31] whereby it was codified later into GDPR in addition to the right to erasure.

It was noted by the Apex Court, in the *Puttuswamy's* case[32], that right to be forgotten cannot exist in sphere of the justice administration predominantly in the context of judgments delivered by the Courts. However, an exception is provided for protection of identity of victims in sexual offences which cannot be disclosed without permission of the court.[33] This issue was also reflected in a recent 2021 case of *Jorawer Singh Mundy* v. *Union of India*[34], whereby the appellant moved to court for removal of his name from judgments after his acquittal in a 2013NDPS case as it affected his professional life. In such scenario, it may be notice that the names cannot be removed completely from the judgments. In another recent case of July 2021, *Ashutosh Kaushik* v. *Union of India*[35], the petitioner moved to the Hon'ble High Court of Delhi for deletion of his videos, photos and related articles on the internet quoting his '*right to be forgotten*'. After consideration of the facts, the Court vide order dt. 22 July 2021 delivered notice seeking instructions to get rid of all the posts, videos and articles related to him across the internet.

In an ongoing case of *Jaideep Mirchandani & Anr.* v. *Union of India & Ors*.[36], the Respondent has enlightened that the right associated with privacy also comprises of right to be forgotten. Furthermore, this part is covered in the Personal Data Protection Bill, 2019 which is yet to be enforced. The Centre contended that the IT Act, 2000 also cover this ambit whereby there shall be blocking and removal of such unlawful information and data from an intermediary. Similar to *Jorawar Singh case*[37], the main issue revolves around the removal of concerned decision and new articles published earlier from the internet.

The right to be forgotten existence depend upon balance among conflicting rights of personal information and right to free expression. In the present digital age, data is a treasured resource that should be regulated as per law and without a proper legislation, there are some varying and irregular adjudications from the courts, which resulted into ambiguity to form an appropriate position.

[31]Court of Justice of EU, C-131/12 (decided on May 13, 2014)
[32](2017) 10 SCC 1: AIR 2017 SC 4161.
[33]*Nipun Saxena* v. *Union of India*, (2019) 2 SCC 703.
[34] Writ Petition (Civil) 3918/2021.
[35] Writ Petition (Civil) 6970/2021.
[36]Writ Petition (Civil) 12620/2021.
[37]Supra Note 34.

V. FINAL REMARKS

The debate of privacy protection profoundly taps off in the physical as well as new digital world with the requirement for information security laws and social equality of security of each person, irrespective of any discrimination. Privacy is a significant element to life, liberty and freedom and an innate part of the essential human rights sacred in the Constitution. It exists likewise amongst all peopleindependent of class, caste, sex etc. In any case, the reality the security is certainly not a flat out right, yet an attack should be founded on lawfulness, need and proportionality for defending this appreciated right and such an intrusion should be legitimized by law.

The term 'privacy' had a broad meaning which covers almost each aspect of day-to-day activities performed by an individual. Few of the international conventions explicitly mentioned the right to privacy but they are mentioned in narrower manner. It is left for the states to cover the gap whereby a responsibility arises against the states to include it under the basic and traditional laws. In Indian context, this vision was not incorporated by the constituent assembly while forming the constitution, nevertheless, with the development we came across to encompass it as part of fundamental right under Article 21. It is yet to be integrated with other rules, laws and policies as conceptualized by the Supreme Court in Aadhar case judgment. Additionally considering the way that the period we live in is the time of data and few out of every odd data we have is needed to be given and certain limitations and protection are needed to such information and data and thus the right to privacy becomes considerable. The idea of protection of privacyof data is the greatest possible level of requirement in this instinctively progressing time of the 21st century.

Like other rights, the rights to privacy comes with few limitations and restrictions as it cannot be absolute in nature. If it is made absolute, the concept of anonymity will overshadow the human right related to privacy and will open floodgate for the number of lawsuits which might defeat the ultimate purpose of protection of data. On the other hand, whenever the data or information is collected, it is very problematic task to keep it anonymous. This problem becomes more larger when it is done with large data sets which calls for more advanced technological efforts to re-identify ostensibly '*anonymous'*information.