



DATA PRIVACY: AN IMPERATIVE NEED

By *Zakia Khan and Raza Abbas*
From *Aligarh Muslim University*

ABSTRACT

Privacy is the core of personal liberty. **J.S.Mill** in his essay “**On Liberty**” gave expression to the need to preserve a zone within which the liberty of citizen would be free from the authority of the state. The main purpose of this paper is to identify the sanctity of privacy in relation with our data which is being given to the government and the protection of that data. In this paper we will be dealing with various Articles of constitution like 19, 21, as well as with informational technology act 2000 and Sensitive Information Rules, 2011. There are various laws and legislation which are yet to be introduced and various initiative taken by the government for setting up of committee to draft a bill on data protection law which will be a dream come true and a much awaited bill in today’s scenario. New challenges which have emerged in terms of constitutional understanding of where liberty places oneself in the context of social order like the present Aadhaar scheme in relation with the data privacy of individual. In the present **Justice Ks puttaswamy case** debates on privacy which has been analysed in context of global information based society. In an age where information technology governs every aspect of our lives the privacy of data is a quiet difficult task but yet a need of hour. Individual as citizen and consumers need to have the means to exercise their right to privacy and protect themselves and their information from

abuse. This new emergence of privacy has built a foundation for new jurisprudence of civil rights the legacy of Puttaswamy case could become what it promises to be the foundation for a transformative civil rights jurisprudence or it could become only a rhetorical lodestar a beautiful and ineffectual angel beating in the void its luminous wings in vain.

INTRODUCTION:-

“Privacy is a special kind of independent, which can be understood as an attempt to secure autonomy in at least a few personal and spiritual concern, if necessary in defiance of all the pressure of modern society. It is an attempt that is to safe to do more than maintain the posture of self-respecting independence towards other men, its seeks to erects an unbreakable wall of dignity and reserve against the entire world”.

Clinton Rossiter, “**The free man in the free society**”, the essential of **freedom.**

The expression ‘**data**’ is very wide in ambit and scope it covers not only the personal aspect of individual but also commercial aspect. The preamble of the constitution of India has also kept the *LIBERTY of thought, expression, belief, faith and worship*, in **Justice KS Puttaswamy** case, the court discovered a gem that the Right to privacy is an inalienable part of Art 21 Right to Life and Personal Liberty. Therefore every action of government that affect the citizens must be examined through the lens of Right To privacy. The latter is protected in the form of privacy rights whereas the former is



protected as proprietary right. The privacy rights are protected under art 21 of Indian constitution similarly proprietary rights are protected under various statutes like the IT act 2000¹. Thus a citizen has data protection right under the Indian laws. The latter is violated when the personal information regarding individuals is compromised whereas the former is infringed when they are disclosed or misused without authority.

The term privacy is the recognition of individual's right to be let alone and to have his own personal space. Privacy primarily concerns the individual. The right to privacy also mean that the one's control over the collection and disclosure of personal information and these personal information could be anything like habits, education record, and personal interest and in recent years there has been a fear of large amount of information of person in computer file which can be easily hacked. An individual could be easily harmed by the existence of this personal data which can be easily transferred at high speed. This growth in the use of personal data has many benefits but it could also lead to many problems. Further the convergence of technologies has spawned a different set of issue concerning privacy rights and data protection. Innovative technologies make this data easily accessible. There is an inherent conflict between right to privacy and data protection it should be reconcile. But the data of individuals and organization should

¹Praveen Dalal, "Data protection law in India: The TRIPS Prospective", 11 *journal of Intellectual property right* 125(2006).

be protected in such a manner that their privacy rights are not compromised².

Concept of Privacy:-

The term privacy and right can't be easily conceptualized. It has been taken different ways in different situations. **TOM GAIETY** opined that "right to privacy is bound to include body's inviolability integrity and intimacy of personal identity including marital privacy"³. **Jude Cooley** explained the law of privacy and has asserted that privacy is synonymous to 'the right to be let alone'⁴. **Edward Shills** has also explained privacy as 'zero relationship between two or more persons in the sense that there is no interaction or communication between them, if they so choose'⁵. In modern society privacy has been recognized both in the eyes of law and in common parlance. But it varies in different legal systems as they emphasize different aspects.

The Indian Constitution provides a right to freedom of speech and expression,⁶ which implies that a person is free to express his will about certain things⁷. A person has the freedom of life and personal liberty, which

² Shiv Shankar Singh, "Privacy & data protection in India critical assessment", 53(4) *journal of Indian law institute* 663 (2011).

³Tom gaiety, "right to privacy" 12 *Harvard civil right civil liberties law review* 233

⁴Thomas M Cooley, A treatise on the law of torts 29(2nd edition 1888)

⁵ Edward shills "privacy: its constitution and vicissitudes". 31 *Law and contemporary problem* 281(1966).

⁶ Constitution of India , art 19(1) 2

⁷Id., Art. 19(2).



can be taken only by procedure established by law⁸. These provisions improvably provide right to privacy to individuals and/or groups of persons. The privacy of a person is further secured from unreasonable arrests⁹ the person is entitled to express his wishes regarding professing and propagating any religion.¹⁰ The privacy of property is also secured unless the law so authorises i.e. a person cannot be deprived of his property unlawfully.¹¹ The personal liberty mentioned in article 21 is of the widest amplitude and it covers a variety of rights which go to constitute the personal liberty Article 21 as such protects the right to privacy and promotes the dignity of the individual

Judicial Response of Privacy:-

The judiciary has recognized right to privacy as a necessary ingredient of the right to life and personal liberty

There were also many instance where right to privacy was highlighted as an important right under the Constitution through judicial activism like -:

Kharak Singh v. The State of U.P. (1962)¹². In this case before the Supreme Court, a minority opinion recognised the right to privacy as a fundamental right. The minority judges located the right to privacy under both the right to personal liberty as well as freedom of movement.

Govind v. State of M.P¹³. The Supreme Court confirmed that the right to privacy is a fundamental right. It derived the right to privacy from both the right to life and personal liberty as well as freedom of speech and movement However, the right to privacy is subject to “compelling state interest”

R. Rajagopal v. Union of India (1994)¹⁴ -It was determined by the Supreme Court that the right to privacy is a part of the right to personal liberty guaranteed under the constitution. It recognized that the right to privacy can be both a tort (actionable claim) as well as a fundamental right. A citizen has a right to safeguard the privacy of his or her own family, marriage, procreation, motherhood, child-bearing and education among other matters and nobody can publish anything regarding the same unless (i) he or she consents or voluntarily thrusts himself into controversy, (ii) the publication is made using material which is in public records (except for cases of rape, kidnapping and abduction), or (iii) he or she is a public servant and the matter relates to his/her discharge of official duties.

KS Puttaswamy v. Union of India¹⁵- The Court ruled that “right to privacy is an intrinsic part of Right to Life and Personal Liberty under Article 21 and entire Part III of the Constitution”.

These are the above mentioned cases on the concept of privacy and now this right

⁸Id., Art. 21.

⁹Id., Art. 22.

¹⁰Id., Art. 25.

¹¹Id., Art. 300A.

¹²AIR 1963 SC 1295

¹³ AIR 1975 SC 1378

¹⁴ AIR 1995 SC 264

¹⁵ AIR 2014 6 SCC 433



of privacy has been made as a fundamental right in the apex judgement of Justice KS puttaswamy case

Informational Privacy:-

Our's is an age of information. Information is knowledge the old adage that '**knowledge is power**' has stark implication for the position of the individual where data is ubiquitous an all-encompassing presence .Technology has made life fundamentally interconnected .Internet has become all pervasive as individual spend more and more time online each day of their lives . Every transaction of an individual user that he use to visit leave an electronic track generally without his knowledge .These electronic track contain powerful means of information which provides knowledge of all sort of person that the user is and his interest . **For example** – the book that an individual purchases online provide footprint for targeted advertisement of same genre. Lives of people are open to electronic scrutiny. To put it mildly, privacy concerns are seriously an issue in an age of information.

This age of information has resulted in complex issues of informational privacy. Invasion of data privacy are difficult to detect because they can be invisible¹⁶ . Information collection can be swiftest theft of all .It is also an age of big data or data sets. The data sets are capable of being searched they have linkages with other data sets and the data gets leaked. The balance between data regulation and individual

¹⁶ CHRISTINA p. monodies, “ moving from Nixon to Nasa: privacy second strand- right to information privacy”,15(1) *Yala journal of law and technology*153 (2012)

privacy raises complex issues requiring delicate balance to be draw between them.

As it was held in the case of JUSTICE KS PUTTASWAMY that:-

“The sphere of privacy stretches at one end to those intimate matters to which a reasonable expectation of privacy may attach. It expresses a right to be left alone. A broader connotation which has emerged in academic literature of a comparatively recent origin is related to the protection of one’s identity. Data protection relates closely with the latter sphere. Data such as medical information would be a category to which a reasonable expectation of privacy attaches. Apart from safeguarding privacy, data protection regimes seek to protect the autonomy of the individual.”

One of the chief concerns which the formulation of a data protection regime has to take into account is that while the web is a source of lawful activity-both personal and commercial, concerns of national security intervene since the seamless structure of the web can be exploited by terrorists to wreak havoc and destruction on civilised societies. Cyber-attacks can threaten financial systems .**Richard A Posner**, in an illuminating article, has observed:

“Privacy is the terrorist’s best friend, and the terrorist’s privacy has been enhanced by the same technological developments that have both made data mining feasible and elicited vast quantities of personal information from innocents: the internet, with its anonymity, and the secure encryption of digitized data which, when combined with that anonymity, make the internet a powerful tool of conspiracy. The government has a compelling need to



exploit digitization in defence of national security...¹⁷

Posner notes that while “people value their informational privacy”, yet “they surrender it at the drop of a hat” by readily sharing personal data in the course of simple daily transactions. Hence Privacy has been held to be an intrinsic element of the right to life and personal liberty under Article 21 and as a constitutional value which is embodied in the fundamental freedoms embedded in Part III of the Constitution. The protection of the information from being leaked is a need of the hour. as today's scenario is a time where a person can be easily traced by a GPS can be a boon or ban it depends on us how do we handle it and the informational privacy of the person's data has got a new dimension after this case of JUSTICE KS PUTTASWAMY which has restored the citizen rights in the form of right to privacy in part III of the constitution of India.

Data Privacy and Aadhaar scheme:-

“Right To Privacy” has multiple facets and therefore the same has to go through a process of case to case development as and when any citizen raises his grievances complaining of infringement of his alleged right in accordance with law .It is pertinent to note that in the judgement of Justice KS puttaswamy case the Supreme court did not decide upon the constitutionality of Aadhaar Scheme and instead examined the Right To

Privacy in the abstract in around 545 pages of dicta the court placed the individual right at the heart of right to .The main question which needs to be determine is that as to **What should be the extent of data privacy in Aadhaar case?**

This answer can be determine in the case of **Govind V State of Maharashtra**¹⁸ **The SC recognized decisional autonomy, full development of personality, special privacy, in addition to informational privacy as an important element of Right To Privacy.**

The present Aadhaaract possess serious threat to informational privacy and endangering the liberty and dignity of individual Right To Privacy of all the citizen is being put at stake in the name of state interest, which must be set aside. **The state is the means and the individual is end.** Informational traces are also area which is the subject matter of huge debate in various jurisdiction falling within the realm of Right to Privacy, such data is as personal as that of the choices of appearance and apparels.

Over the last one year, there have been multiple instance of Aadhaar data leaking online through government websites or its mobile app. 210 government websites made the Aadhaar details of people with Aadhaar public on the internet. It takes, sometimes, a negative event to bring important issues on the debating table. The 4 January 2018 report¹⁹ alleging data breach of Aadhaar brings the larger issue of data protection,

¹⁸(1975) 2 SCC 148

¹⁹Rachnakhaira, the tribute, 4 January 2018,available at

<http://www.tributeindia.com/news/nation/523361.html>,

(last modified on 5 January 2018)

¹⁷ Richard a posner, “privacy, surveillance and law” , 75 *The university of Chicago law review*

251(2008)



privacy and their protection back in public discourse. The Right To Informational Self-Determination Had Become A Crucial Facet Of The Right To Personal Autonomy, And Was Protected Under Articles 14, 19, And 21 Of The Constitution. The Principle Of Informational Self-Determination Was Specifically Comprised Because Data Was Required To Be Handed Over To Private Parties And Compelling The Handing Over Of Personal Data To Private Parties With Such Minimal Safeguards Over Their Functioning Amounted To “A Complete Destruction Of Personal Autonomy And A Debasement Of The Right To Informational Self-Determination.”²⁰

point that is highlighted by the CSI report²¹. *“Information and data leak have been occurring in India for a long time, and the leak around Aadhaar are not the first data leak. But with the scale and design of Aadhaar, any information being leaked is dangerous and its impact not entirely reversible.”* for example, “A biometric identifier such as a fingerprint can be effective and highly accurate, way to establish the identity of an individual but it can also facilitate a much higher degree of tracking and profiling then would be appropriate for many transaction, the problem which arises when Biometric identifiers are compromised are severe, what

²⁰ Rethink Aadhaar, available at: <http://www.rethinkaadhaar.com> (visited on march 7,2018)

²¹The centre for internet & society India, available at: <http://www.cis-india.org/internet-governance/news/times-of-india-aadhaar-number-leaked-claims-cis-report> (last visited on march 7 , 2018)

will happen at the point that your biometric identifiers ‘No longer Identifies you.’ The machine which can identify you if suddenly doesn’t accept your detail what will happen? Here we are lacking behind for this we need a proper laws and regulation to regulate it. Here we are not against the Aadhaar scheme but against the lack of infrastructural resources to carry out this scheme and in today’s era where all of the information of person is just a click away this scheme without any protection of data with the legislation could be very dangerous for individuals.

Privacy and Data Protection:-

Data protection is legal safeguard to prevent misuse of information of individual person on a medium including computers. It is adoption of administrative, technical, or physical deterrents to safeguard personal data. Privacy is closely connected to data protection. Maintaining of data bases is not as difficult as maintaining its integrity, so in this era there is a growing concern of data protection. Privacy and data protection require that information about individuals should not be automatically made available to other individuals and organizations. Each person must be able to exercise a substantial degree of control over that data and its use. An individual’s data like his name address, telephone-numbers, profession, family, choices, etc. are often available at various places like schools, colleges, banks, directories, surveys and on various web sites²². Passing of such information to

²²Shiv Shankar Singh, “Privacy & data protection in India critical Assesment” 53(4) *journal of India law institute* 671(2011)



interested parties can lead to intrusion in privacy like incessant marketing calls. The main principles on privacy and data protection enumerated under the Information Technology Act, 2000 and Sensitive Information Rules, 2011 is defining it.

Individual as citizen and consumers need to have the means to exercise their right to privacy and protect themselves and their information from abuse. This is particularly the case when it comes to our privacy and protect themselves and their information from abuse. Data protection is about safeguarding our fundamental right to privacy, which is enshrined in international and regional laws and conventions. India being a welfare state must work for the welfare of individual. Individual's liberty should be kept at par and collection of data for impractical project without drawing the extent of privacy should be waived off. The protection of data and privacy has become a celebrated concept now days after the landmark judgement of Justice KS Puttaswamy Case. Earlier also certain legislation were there related to data privacy. But after this judgement this concept has been widened in its widest amplitude.

Data Protection and Current Legislation in India:-

With the advancement of technology in India the ratio of crime rate have also increased. In the present era most of the crime are being done by the professional through easiest way like computer and electronic gadgets. Just by the single click the criminal are able to get the whole of information, the lust of information is acting as a catalyst in the growth of cybercrimes. It is a very big headache for business houses,

financial institution and the governmental bodies so as to give adequate protection to huge data bases. In the absence of any particular stringent Law relating to data protection the miscreants are gaining expertise in their work day by day. Though this word simplified our lifestyle but it left certain anomalies in procurement of its objective which resulted in involuntary disclosure of data.²³

For example –

1. On every login to the e-mail account in cyber cafes, the electronic trail of software remain left there unsecured.
2. Through hacking the hackers can whimsically alter anyone's account
3. Source code theft is the most preferred act of miscreants

These are some of the examples that how easily we are providing room to the miscreants to enhance and simplify their acts and it is not safe is to avail the services of digital world.

The right to privacy is an important concept originated in law of torts under which a new cause of action for damages resulting from unlawful invasion of privacy was recognised. And in India this concept is now widely accepted in the form of constitutional regime under art 21 of constitution which states as ***"No Person Shall Be Deprived of His Life or Personal Liberty except according To Procedure Established by Law."*** There are following provision relating to data protection in India:-

In the year 2000, effort has been made by our legislature to embrace privacy issues relating to computer system under the

²³ Data protection law in India, available at : <http://www.legal service India .com> (last visited on march 7,2018)



purview of [IT Act, 2000](#). This Act contains certain provisions which provide protection of stored data. In the year 2006, our legislature has also introduced a bill known as 'The Personal Data Protection Bill' so as to provide protection to the personal information of the person. **According to section 2(1) (o) of the Information Technology Act, "Data means a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalised manner, and is intended to be processed or is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer"**. The IT Act doesn't provide for any definition of personal data and, the definition of "data" would be more relevant in the field of cyber-crime. The idea behind the aforesaid section is that the person who has secured access to any such information shall not take unfair advantage of it by disclosing it to the third party without obtaining the consent of the concerned party. UNDER INFORMATION TECHNOLOGY ACT, 2000 sec 43, 65, 66, 70 and 72 deals with data protection laws.

Sensitive Information Rules, 2011

Section 43A of the Information Technology Act, 2000 read with the Information Technology (reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("*Sensitive Information Rules*") requires every business in India, which collects, receives, possesses, stores, transmits, processes or can associate

pretty much any other verb with 'personal information' directly under a contractual obligation with the provider of information²⁴, to have a privacy policy. Such privacy policy must provide the following²⁵:

1. Clear and easily accessible statements of its practices and policies;
2. Type of personal and sensitive personal data or information collected by it;
3. Purpose of collection and usage of such information;
4. Disclosure of information including sensitive personal data or information collected;
5. Reasonable security practices and procedures adopted by it.

The essential elements of a privacy policy as per the extant data protection laws of India are as follows:

1. **Consent:** The most crucial component of a privacy policy is 'consent'. In this regard the Supreme Court has in Puttaswamy case made the following observations:

"It was rightly expressed on behalf of the Petitioners that the technology has made it possible to enter a citizen's house without knocking at his/her door and this is equally possible both by the State and non-State actors. It is an individual's choice as to who enters his house, how he lives and in what relationship. The privacy of the home must protect the family, marriage, procreation and sexual orientation which are all important aspects of dignity. If the

²⁴ Information Technology(Reasonable Security practises data or Information) Rules, 2011 (Act 21 of 2000) sec.43A

²⁵ Sensitive Information Rules ,rule.4



individual permits someone to enter the house it does not mean that others can enter the house. The only check and balance is that it should not harm the other individual or affect his or her rights. This applies both to the physical form and to technology."

2. **Choice:** The other vital component is choice²⁶. It is not enough that users have been shown to have accepted the privacy policy through a click-wrap mode; they should have the ability to opt-in and/or opt-out of the information sharing requirements of the business. The present laws allow the data controller to withhold the provision of the goods of services for which the information is sought, if the provider of information does not provide or later chooses to withdraw his consent.²⁷

3. **Purpose of information collected**²⁸. The privacy policy needs to clearly specify the purpose of collection of the information. Only that personal information should be collected from data subjects as is necessary for the purposes identified for such collection, regarding which notice has been provided and consent of the individual taken²⁹. An omnibus purpose which ambiguously refers to future commercial usage may not be favourably viewed by Indian courts, especially if the other elements of the privacy policy have not been met³⁰. If there is a change of purpose, this must be notified to the individual. The information collected for a specified purpose

cannot be retained for longer than it is required of the purposes³¹

4. **Disclosure of information.** The type of information collected must also be clearly informed to the information provider. Technological advancement is not equivalent to technological literacy. It is not audacious to assume that many of the internet users are still unaware of the perils of data divulge. Therefore, it is vital that the information provider be informed about the nature of his personal information that is being collected. The data controller must also permit the providers of information, as and when requested by them, to review the information they had provided³².

5. **Security practises**³³ - the Sensitive Information Rule mandate every data controller to have comprehensively documented information security programme and Information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of the business. This document is often confused by the business with their privacy policy which is not the case.

India does not have specific data protection legislation, other than the IT Act, which may give the authorities sweeping power to monitor and collect traffic data, and possibly other data. These are some of the prevalent means in today's scenario by which we can safeguard our data but these laws are not specific in their nature. They can't be imposed directly hence there is a need of

²⁶ Id. rule 5 (7)

²⁷ Ibid.

²⁸ Id. rule 5(5)

²⁹ Id. rule 5(3)

³⁰ Id. rule 5(3)

³¹ Id. rule 5(4)

³² Id. rule 5(6)

³³ Id. rule 8



proper legislation in India as there is a growing concern of cyber-crime and leakages of personal and intimate matter of one's life which can be used by anyone for their own benefit. Hence a need for proper data protection in relation with privacy is needed and after the judgement *of justice KS puttaswamy* case the wings of data privacy seems to be flying up in the sky because this judgement gave a new scope to protect the data privacy of individual by which the sanctity of data privacy can be maintained in today's scenario.

Conclusion:-

"Digitalization has changed society. While data is becoming the 'new oil', data protection is becoming the new 'pollution control.' The issue of data protection is important both intrinsically and instrumentally. Intrinsically, a regime for data protection is synonymous with protection of informational privacy. As the Supreme Court observed in Puttaswamy, "Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state."

Privacy is a basic human right and computer system contain large amount of data that can be sensitive. However one can access any information related to anyone from anywhere at any time but this pose a new threat to private and confidential

information. Globalization has given acceptance to technology in the whole world. As per growing requirement different countries have introduced different legal framework like DPA (Data Protection Act) 1998 UK, ECPA (Electronic Communications Privacy Act of 1986) USA etc. from time to time. In the USA some special privacy laws exist for protecting student education records, children's online privacy, individual's medical records and private financial information. In both countries self-regulatory efforts are facilitating to define improved privacy surroundings. But India being a developing country does not possess any separate law or data protection however the court on several occasion have interpreted data protection within the ambit of Art 19 and 21 of constitution of India . However the Ministry of Electronic and Information Technology has appointed an expert group headed by former SC judge BN Sri Krishna to draft a data protection bill

The terms of reference of the Committee are:

- a) To study various issues relating to data protection in India;
- b) To make specific suggestions for consideration of the Central Government on principles to be considered for data protection in India and suggest a draft data protection bill³⁴.

Data privacy and protection by their very nature need to be dynamic constantly expanding and improving to deal with new impediments and hindrances. One such

³⁴Justice k s puttaswamy v. union of India [(2015) 10 SCC 92]



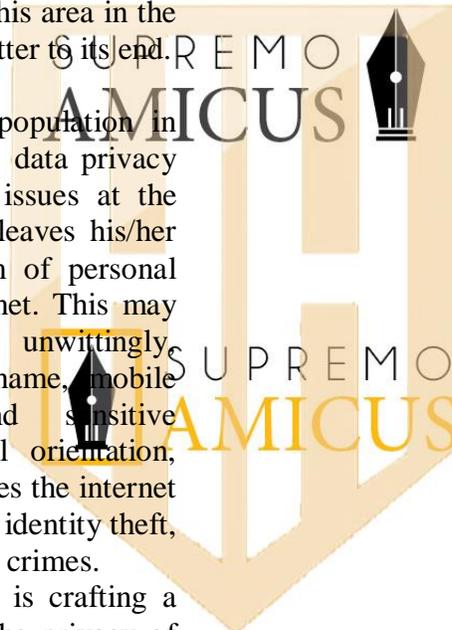
encouraging step towards data protection is the most apex judgement of Supreme Court of Justice KS Puttaswamy case. There is an unparalleled thrust to upgrade the data privacy and data protection standards in India as the country is heading towards being a prominent part of global economy with increase in foreign investment in India. With new beginning it is the need of the hour for the government to come up with a robust regime For data protection that would deliver a careful and sensitive balance between individual interest and legitimate concerns of the state. It would be interesting to follow the development in this area in the near future and observe the matter to its end.

Considering that the digital population in India has grown substantially, data privacy and data protection are key issues at the moment. Every internet user leaves his/her digital footprints in the form of personal data when browsing the internet. This may range from, knowingly or unwittingly, providing their IP address, name, mobile number to personal and sensitive information like their sexual orientation, medical records, etc. This leaves the internet users vulnerable to crimes like identity theft, breach of privacy and financial crimes.

The pervasive question today is crafting a privacy policy that balances the privacy of the internet user with the burgeoning requirements of the businesses. Terms of use and privacy policy should be treated as an art form, rather than long form, i.e., craft the document carefully customizing it to the needs of the business and the general principles of law.

Drafting a data protection law for India is a complex exercise.

But as the scriptures say “From each debate, there arises knowledge of the Ultimate Principle”³⁵. Hence this committee will bring a robust regime for data protection law in India. As privacy is now intrinsic part for individual which will be rightly protected



³⁵Government of India, Report: White paper of committee of expert on data protection(ministry of election and information, 2017)