Page 3159 - 3171 **DOI:** *https://doij.org/10.10000/IJLMH.11714*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 4 | Issue 3

2021

The Data Protection Regime: A Critical Analysis of Global Scenario with Special Emphasis on India

SAKSHAM MAHAJAN[1] AND MANAS AGRAWAL[2]

ABSTRACT

Today, in this era of rapidly changing technology, everything from monetary transactions to private data has been and is yet getting digitally transformed. If one has to send his credentials, one tap and the person on the other end will receive it. The same goes for several other day to day activities. However, it is the ever-increasing want of the bureaucrats of various nations who are trying to hamper the growth of this digitalized mechanism. Be it is for the purpose of national security or for its own selfish and shallow reasons, the governments are leaving no stone unturned to gather the information of its citizens.

Recent trends make the desperate attempts of government to seek as much personal data of its people as possible clearly visible. Linking of the Aadhar cards, latest proposed amendment to acts are all illustrations of such hustle. In the paper, the authors seek to put forth an analysis of the different models of three countries, namely The United States of America, The Republic of China and the Europe, as to how they gather information of their citizens and put forward their national policies. Then, the current situation of India has also been studied and critiqued minutely on the basis of the recommendations of Justice Verma Committee along with the study of the proposed amendment regarding the Bills Act. Later, a different view has been put forward by authors by studying the different side of the issue of data gathering as how much the nation's data is secured with the Government of India and as if the Government is ready to securely keep and protect the humongous amount of digital data from any sort of cyber-attacks.

Keywords: *Data protection, Data privacy.*

I. INTRODUCTION

The recent past has undoubtedly witnessed a sudden shift, growth as well as transformation in the technological field. This transformation of technology has indeed led to the birth of

[1] Author is a student at Amity Law School, Noida, India.
[2] Author is a student at Amity Law School, Noida, India.

 [ISSN 2581-5369]

extremely complex and sophisticated problems as never seen before some of which are data theft, cyber-attacks and foreign surveillance. Looking forward to the technological advancements and the ever-increasing enormous amount of data being collected and processed on a daily basis across the globe, the grave need for a dedicated law over the subject was realized. The developed and more technologically advanced nations enacted independent legislations dealing with the matter of data protection so as to protect personal and sensitive data of the state from being compromised.

As far as the term "***data***" is concerned, as yet it lacks a clear and precise legal definition however several countries across the globe have attempted to define what comprises personal or sensitive or sensitive personal data through definition clause of their exclusive legislations dealing with the data protection regime. The ***General Data Protection Regulation, 2018*** of Europe more commonly referred to as (GDPR) vide ***Article 4.1*** and ***Data Protection Act, 2018 of UK*** modelled on GDPR serve as best examples of such comprehensive definitions defining personal data.

However, as far as India is concerned, it still seems to be at a primitive stage in this regard and lacks any separate exclusive legislation dealing with data protection. In India, ***The Information Technology Act, 2000*** along with rules made thereunder which is "***Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011***" introduced under ***Section 43A*** of the Act vide notification no. ***G.S.R. 313(E)*** of 13 April 2011) make up the legislative base for data protection.

Looking forward to the rapidly changing times as well as the immediate need that was being increasingly felt due to lack of any exclusive legislation over the subject, in an attempt to join the league of western nations, India also Introduced the ***Draft Data Protection Bill, 2018*** and subsequently ***The Data Protection Bill, 2019*** was introduced as recently as 11th December 2019 by Ravi Shankar Prasad, Minister of Electronics and information technology. The bill provides for establishing Data protection authority so as to ensure protection of personal data of individuals.

Generally, personal data includes private information and data about a person such as health and medical records, sexual orientation, financial information, passwords and other such information. Currently in India, ***Rule 3 of*** "***Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011***" define Sensitive Personal Data and includes all aforementioned information within its ambit amongst

several others.[3] ***The Data Protection Bill, 2019*** is amongst a few legislations which defines the term "data". ***S. 2(11) of the Bill*** provides that "*data*" includes a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by humans or by automated means.[4]

Besides defining the term data, the bill also provides comprehensive definitions for several other terms such as biometric data, genetic data, financial data, health data, personal data and sensitive personal data and also defines harm and person.

Deliberation over the topic of Data Protection raises a question in our minds that what is the need to protect data. The answer to this question though simple requires a radical insight in several aspects of law such as Privacy, Human Rights and morality. Hence, the legal regime over data protection aims at setting up of practices, policies, procedures, and penalties in case of any breach so as to prevent and prohibit undue intrusion into one's privacy caused by collection, storage and/or dissemination of personal data.

The Indian constitution does not manifestly grant the Fundamental right to privacy. However, the recent judicial opinion is somewhat different. The Indian courts have read right to Privacy as natural, inalienable and integral part of other existing Fundamental Rights which are *Right to Freedom of Speech and Expression under Article 19 (1)(a), Freedom of Movement under Article 19 (1)(d) and Right to life & Personal Liberty under Article 21* of the Indian Constitution. However, the fundamental rights are subject to reasonable restrictions especially in case of freedoms provided under Article 19, *Article 19 (2) to Article 19(6) provide for reasonable restrictions* that may be imposed by the state under certain circumstances.

Recently, the Landmark Judgement of the case ***Justice K S Puttaswamy (Retd.) & Anr. vs. Union of India and Ors.***[5], which overruled – ***MP Sharma v Satish Chandra, District Magistrate, Delhi (8 Judges Bench)***[6] as well as ***Kharak Singh v State of Uttar Pradesh (6 Judges Bench)***[7] and rather upheld the decision ***Gobind v State of Madhya Pradesh***[8] & ***R Rajagopal v State of Tamil Nadu***.[9] *These subsequent decisions which affirmed the existence of a constitutionally protected right of privacy, were rendered by Benches of a strength smaller than those in M P Sharma and Kharak Singh. In Puttaswamy Case,* the constitution bench of

[3] *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*. Rule 3.
[4] *Data Protection Bill, 2019*.Section. 2(11).
[5] [2017] AIR 10 SCC 1.
[6] [1954] SCR 1077.
[7] [1964] 1 SCR 332.
[8] [1975] 2 SCC 148
[9] [1994] 6 SCC 632.

 [ISSN 2581-5369]

the Hon'ble Supreme Court finally cleared this cloud of ambiguity and has held Right to Privacy as a fundamental right, subject to certain reasonable restrictions.

Hence looking forward to the history and present scenario, there's an immediate need to discuss and deliberate over the Data Protection Regime of India and compare it with those of other well-developed nations in connection with the Fundamental Right to Privacy. Also, there is a need to look over to the situations prevailing in different countries and steps taken therein to tackle the modern data protection problems. The researchers have attempted the same in fore coming sections of this paper.

II. GLOBAL ANALYSIS OF DATA PROTECTION REGIME

In this section, the authors have made an attempt to advance the comparison between three types of models of data protection. These three models are pioneered and followed by the most advanced countries of the globe. First, is that of the United States, Second of the European Union and lastly, of the People's Republic of China.

The United States of America follow a *laissez faire* system of data protection and does not have an overarching data protection framework. The US lacks Federal legislation for data protection. Along with this, there are several state levels laws in this regard. Due to the dominance of the state level laws, the state attorney general plays a key role in the enforcement. Also, at the Federal level, there is the presence of Federal Trade Commission which has an authority to ensure that there is compliance with data protection laws. Along with this, the bigger problem that persists is that the states have different laws with less unanimity. This can be analysed by the fact that all States of the US have adopted data protection notification laws of some sort, however there are differences in the definition of the term '*personal data*' and as to what circumstances lead to breach of such data.

The American courts have however, collectively recognized the right to privacy protections being reflected in different constitutional amendments. The Fourth Amendment prohibits '*unreasonable searches and seizures*' by the government. '*Reasonableness*' of search can be premised on the putting forward of a valid judicial warrant. Reasonableness can also be established if one of the exceptions to the warrant exists, as established by the courts and along with that if the government meets any additional reasonableness test applied by the courts in particular circumstances. However, the scope of Fourth amendment is pretty limited in the context of data protection[10]. This is because the scope of the amendment is cut short by the

[10] Bowden C and Bigo D, 'The US Surveillance programmes and their impact on EU citizens' fundamental rights' (2013)

words '*where the individual has legitimate expectation of privacy*'[11]. In the 1970's, the Supreme Court in different cases held that individuals have no "*legitimate expectation of privacy*" in information which they are voluntarily turning to third parties, including telephone records[12] and banking records[13] and therefore most of the government data processing falls outside the purview of the Fourth amendment. The Federal Courts of Appeal has observed that this is an issue in which 'Supreme Court's jurisprudence is in turmoil'.

Also, there has been a made *a fourteenth amendment* in the American Constitution. Though this amendment was not related to the data protection but did protect the privacy rights of a pregnant woman. As per the change, several State and Federal Abortion Laws were declared void. The state has no right to interfere with the rights of a pregnant woman when she opts for abortion, however, certain conditions were indeed proposed[14].

There is also a Federal Act present which regulates the collection, use and disclosure of all types of personal information, by all types of federal agencies, including the law enforcement agencies called the ***Privacy Act of 1974***. This Act seeks to ensure transparency in personal data processing of individuals by alerting them about the presence of a personal records system by publishing a notice in the Federal Register.

There are several states of America which are actively developing and amending their data privacy legislation, and detailing their similarities and scaling out the differences in their approaches, illuminating the complexities in privacy protection. ***The California Consumer Privacy*** Act is an initiative against the tech giants who have been collecting the data of users and selling them over for long period of time. The Act incorporates the core principles of data protection and data privacy of the European Union's, The GDPR Law. This Act will come in force from 1st January, 2020. The next Act is by the State of Massachusetts called the ***Standards for The Protection of Personal Information*** of Residents of the Commonwealth. This legislation is very important for the protection of Massachusetts residents against any sort of data theft or identity fraud. Any organizations which licenses, stores or maintains about personal information about the residents are required to follow a comprehensive information security program. The next law is the ***Minnesota Government Data Practices Act of 1979***. This Act safeguards the rights of residents of State of Minnesota to access government data and controls collection and storage and use and dissemination of private data.

[11] Katz v United States (1967) 347
[12] Smith v Maryland (1979) 442 US
[13] United States v Miller (1976) 425 US
[14] Roe v Wade (1973) 410 US

 [ISSN 2581-5369]

Next is the model of the European Union. The EU has been at the forefront of global protection norms. Recently it has enacted in 2018, the ***EU General Data Protection Regulation (GDPR) Law***, replacing the ***Data Protection Directive of 1995***. This model has inspired the California Consumer Privacy Act.

According to the law, the focus will be on the users that they fully know, understand and consent to the data collected about them. The users will not be forced to consent before signing in on any online platform. According to the European Union Commission, "*Personal data is information that relates to an identified or identifiable individual. If you cannot directly identify an individual from that information, then you need to consider whether the individual is still identifiable. You should take into account the information you are processing together with all the means reasonably likely to be used by either you or any other person to identify that individual*". The law provides that unless there is a detailed consent given by the data subject for one or more purposes, the data cannot be processed till there is atleast one legal basis to do so. For this purpose, ***Article 6 of the GDPR*** has enlisted different provisions for data collection.

The rights of the subject are very carefully taken care of by attaching different rights. These rights include information and access of subject's data, rectification and erasure of data and right to object and automated decisions. **Article 25** makes sure that data protection measures are designed and incorporated in business procedures for products and services. Different measures are employed by the data controller in this regard. Pseudonymization of personal data of subjects is one such method. The law is one of the best pieces of legislation in the world relating to the data privacy and protection. However, there are some limitations present. One such limitation is its wording. The wording of law is weakening it as the data of the subjects can be collected by the outside entities and processed outside of the EU. Thus, resulting in '*escaping of the data'* to foreign lands.

Another latest model being established is that of People's Republic of China. The PRC lacked a comprehensive legislation protecting the privacy and data protection laws. However, in 2018, the PRC **Cyber-security Law** came into force and became the first piece of legislation to address the cyber-security and data protection concerns by the name of the Information Security Technology – Personal Information Security Specification. From the law passed by the PRC, a different approach has been observed. PRC has made clear its intention that it intends to link data protection with the cyber security, which is in contrast with its counterparts. Many at times it was found that the data of its citizens was leaked and being sold illegally. **Article 64** provides for the stringent actions to be taken against culprits responsible for privacy breaches and cyber-attacks, including warnings, ratifications, confiscation of illegal earnings,

 [ISSN 2581-5369]

and fines; in severe cases, the punishments may cover suspension of related business, winding up for rectification, shutdown of their website, and revocation of their business license.

III. DATA PROTECTION REGIME IN INDIA

The past few decades have witnessed enormous developments as well as transformations and transitions in the field of technology. However, the Indian legislative attitude suggests that Indian legislature has been slow to respond and mould its legislative environment in accordance to the fast-moving technology and the rapidly changing times moving times. The Indian Legislative scenario has been pretty much different from that of European Union which adopted the Data Protection Directive as early as 1995. EU recently introduced General Data Protection Directive popularly known as GDPR which assumed force since 25th May, 2018.

Unfortunately, India still as of yet lacks an exclusive legislation over Data Protection and it is pertinent to note that the Information Technology Act as originally passed did not contain any provisions relating to protection or procedure to be undertaken so as to protect an individual's Sensitive personal data. It was only in 2006, when India realized the immediate need to protect data, as digitalization was taking place and the amount of data being collected stored and processed was more than ever before. This finally led the introduction of **Information Technology (Amendment) Act, 2008** the provisions of which came into force in 27 October, 2009. This Amendment introduced several new sections related to privacy, cybercrimes, monitoring, surveillance and data protection. In context of data protection, **S. 43A and 72A** were inserted and it was the first step towards data protection regime in India. Subsequently, the Central Government in exercise of Powers Conferred under **S.87(2)(ob) read with S.43 A** of the IT Act, 2000 introduced ***Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011*** (hereinafter referred to as the "2011 Rules").

S.43A provides for the liability of a corporate body when it possesses or deals with sensitive personal data of Information and is negligent while delating with such data and consequently causes wrongful gain or wrongful loss to any person. S. 72A provides for punishment in case of breach of lawful contract.

The 2011 Rules were notified vide notification **G.S.R. 313(E) in April 2011**, the Rules apply only to corporate bodies and persons located in India. **Rule 3** defines "***Sensitive Personal Information***" **(SPD)** and includes within its ambit information such as passwords, sexual orientation, biometric and financial information etc. It if further made clear that the information

in Public domain falls out of the Scope of SPD.[15] **Rule 5 to Rule 8** deal with the ***procedures and practices to be adopted by the Corporate bodies*** while dealing with the SPD. These include drafting a privacy policy and making it easily accessible to information provider, seeking permission to disclose such information to any 3rd party, duties of the corporate body and lastly the international standards and reasonable security practices and procedures to be adopted by the body corporate.[16]

Interestingly, data protection regime also experienced a shift with to Right to Privacy being lifted up to the pedestal of Fundamental Right. The Position was very uncertain and doubtful till the Nine Judge Bench passed the judgment of **K.S Puttaswamy v. Union of India[17]** in 2017. This Judgement made the position clear and held Right to Privacy to be a Fundamental Right under Article 21 of the Indian Constitution. The Apex Court of India has read right to Privacy as natural, inalienable and integral part of other existing Fundamental Rights which are *Right to Freedom of Speech and Expression under Article 19(1)(a), Freedom of Movement under Article 19(1)(d) and Right to life & Personal Liberty under Article 21* of the Indian Constitution. However, the fundamental rights are subject to reasonable restrictions especially in case of freedoms provided under Article 19, *Article 19(2) to Article 19(6) provide for reasonable restrictions* that may be imposed by the state under certain circumstances.

Before the Puttaswamy Judgement the position was uncertain as the in the first two cases relating to Right to Privacy, first **MP Sharma v. Satish Chandra, District Magistrate, Delhi**[18] rendered by a Bench of eight judges and the second, **Kharak Singh v. State of Uttar Pradesh**[19] rendered by a Bench of six judges observed that the Indian Constitution does not specifically protect the Right to Privacy.

However, the Supreme Court also took note of several decisions of this Court in which the right to privacy has been held to be a constitutionally protected Fundamental Right. Those decisions include**: Gobind v. State of Madhya Pradesh[20]**; **R Rajagopal v. State of Tamil Nadu[21]**; and **People's Union for Civil Liberties v. Union of India[22]**. *These subsequent decisions which affirmed the existence of a constitutionally protected right of privacy, were*

[15] *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*. Rule 3.
[16] *Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011*.
[17] (2017) 10 SCC 1.
[18] (1954) SCR 1077.
[19] (1964) 1 SCR 332.
[20] (1975) 2 SCC 148.
[21] (1994) 6 SCC 632.
[22] (1997) 1 SCC 301.

 [ISSN 2581-5369]

rendered by Benches of a strength smaller than those in MP Sharma and Kharak Singh. Faced with this predicament and having due regard to the far-reaching questions of importance involving interpretation of the Constitution the matter was Referred to a larger bench of Nine Judges so as to finally adjudicate and make the position clear in respect of Right to Privacy. Hence, the Supreme Court finally cleared out the dense cloud of ambiguity in **K.S Puttaswamy v. Union of India (2017)**[23] and unambiguously **held Right to Privacy to be a Fundamental Right under Article 21 of the Indian Constitution.**

With the passing of this judgement the B.N. Srikrishna committee was setup upon the report & recommendation of which Draft Data Protection Bill was introduced in 2018. On 11th December 2019, the Data Protection Bill,2019 was introduced in the parliament which had certain major deviations from the recommendations of the committee and was an amended and altered version of 2018 draft. The bill has not yet seen the light of the day, once it is passed it will be an exclusive law over data protection. It will be interesting to see how Indian legislature will meet the needs of the day, along international standards set by EU and US as well as how it will overcome modern challenges.

IV. DATA PROTECTION: ANOTHER ASPECT

The data protection should be assessed from a different angle, that is, the preparation of government to protect the digitally gathered data from any potential cyber-aggressions.

Government of any country has a very grave responsibility of ensuring that the data gathered by it is in safe hands. By safe hands it is meant that the data should be protected against all sorts of cyber-attacks, cyber vulnerabilities as well as against any negligent handling. Any data which has been obtained by digital means is for sure prone to such aforementioned problems. However, it has been observed and analysed that the Government of India is still not prepared to counter such insurgencies and protect the public's data. By this, a very important point needs to be covered that the cyber threats mentioned above are different from the cyber vulnerabilities. A cyber vulnerability is not any type of virus or malware but some deficiency in the operating systems of electronic machines like computers. For instance, an alert has been generated by the Ministry of Home Affairs that a bug has been found in the Android Operating System by the name of "Strandhogg". This bug is not any sort of malware still can attack the personal data of its user and give hackers the autonomy to exploit the users' data.

Now coming on to the cyber vulnerability, recently a major malware-attack on one of India's

[23] (2017) 10 SCC 1.

Nuclear power plant was seen. This attack took place on the "**Kudankulum Nuclear Power Plant**" situated in Tamil Nadu. This power plant was established in accordance to *joint-partnership* of *India* and *Russia*. The magnitude of this attack cannot be over seen. The catastrophe which can be caused by exploiting the data of any nuclear power plant of any country needs no explanation. The reason why this issue needs an early hearing is because if the government is not able to protect its own confidential data of research and experiments, then how it seeks to assure the citizens of the country that their data will be secured with it and no exploitation of it will take place. This type of issue raises questions over the national security of India.

The information regarding the cyber-attack on the power plant was with the Government of India weeks before the actual press release was made. However, the Government tried to hide this fact that installation facility of such power plant was hit by such attack. The famous *cyber security analyst* of India, **Mr. Pukhraj Singh** gave a statement that cyber-attack has resulted in the "*domain-controlled level access at Kudankulum Nuclear Power Plant*". Accordingly, it was also claimed that "extremely mission-critical targets were hit" and the government was notified "way back". After that, the pressure of media rose, resulting in the official release. The virus which hit the systems of the power plant was "*D Track*" virus. This type of malicious software is used by **North Korean** backed hackers' group "*Lazarus*".

These hackers have notorious history of using this type of virus in other countries too, for instance, against South Korea in the recent past. Hereinafter, the more shocking discovery which was made was that the computer containing the critical data was of an administrative level computer. These types of computers do not have any connection with the outside world as they are not connected via the world-wide-web. So, to target these computers, there needs to be an insider who has to inject such malicious software manually through hard disc or pen-drive or through any other means. So, a conclusion is drawn that a scientist belonging to the facility has tried to sell out the information of the power plant to an outsider. Though the technology containing systems were not infected, still the files containing the functioning of the power plant were compromised.

Yet no official release has been made confirming that who actually did this cyber-attack and what kind of official confidential data was taken. It is often said that the Government of India has still no measures to fight a cyber war and protect its digitally secured data. **Mr. Sudhir Kumar**, *former Director General of the Defence Research and Development Organization*, specifically has warned in the past regarding this '*fifth dimensional warfare'* and India's vulnerability against it. Unlike other countries like China or the United States, India has no

 [ISSN 2581-5369]

special means to combat these types of breaches. If an internal attack can be conducted from within the power plant, then any other brutal attack can be launched against systems which are connected with the outside internet services crippling our banks and other institutions.

This critical analysis of assessing the other aspect connected with data protection, that is, cyber-attack on digitally stored data with the government, is inserted only with the aim of providing a self-introspection, as to whether our facilities are well equipped to safeguard the digitally collected, secured and confidential data of its own people against any sort of cyber aggression or will be at the mercy of cyber aggressors. If the government was not able to safeguard its own data, how the public can trust as if it would be able to safeguard their information too. It is the need of the hour to first strengthen our own technologies and facilities before taking the responsibility of gathering the private data.

Another instance is seen in the time of Coronavirus pandemic. The Government of India in one of many initiatives launched the 'Arogya Setu' mobile Application. Through this application, the main aim is to assist people in assessing whether they are showing any symptoms of COVID-19 or are they being vulnerable to it or any associated risk. The noble intentions of the Government cannot be suspected to be tainted, but the issue which popped up was with respect to the way user data is collected and how it violates user privacy. This app was launched by the Ministry of Electronics and Information Technology under the Central Government. The app uses cutting edge Bluetooth technology, artificial intelligence mechanism and algorithms for collection of data. However, the issues came with the transparency of the working of application. There was not much information provided with respect to the usage of collected data and time limit till when it will be stored. This is because the app's privacy policy specifies only the data available on the app and does not specify how long the Government of India will retain 'sever-side data'. Further, the proportionality aspect of this app is also an issue as if the proportionality test ,as given in the Puttaswamy Judgment, is applied then to which extent the privacy of an individual be compromised for greater public good. The foremost concern was that the application was not an open-based application which meant that not everyone can access the data collected in this app. Further, it was a criminal offence for anyone who via reverse-engineering crack its code. Next issue being that the Government of India can share data collected with anyone for medical or other administrative intervention[24].

So to address these issues The GOI on 11th May, 2020 released guidelines to clear confusions. The Government provided that the data shall be made 'de-identified' which means it will get

[24] Privacy Policy, Arogya Setu Application, Clause 2(a)

 [ISSN 2581-5369]

stripped off from any collected personal information of the users. Further, with whom data might be shared was broadly told and the data shall be kept for 180 days. Yet the vagueness prevails, as this cannot be done by an Executive Order as now legislation to protect the data privacy of the citizens prevail in the country, though one such Bill is pending in the Parliament and only needs the President's approval. And more precisely to be said, the Government is again going with the "Adhar Way". Now, it was expected that specific third parties name might be told with whom the data might get shared but again no clarification was given as the Government can do so with whom it seemed necessary. Further, the process of 'de-identification' can be reversed to get know of whose personal information is stored with the government database. Recently, to re-address the issues, the Government made the android version of the app 'Open Sourced', through which software developers can easily check and improve the functioning of application. To show the app's robustness, the Government launched a bug-bounty programme to find any vulnerability or flaws in the Aarogya Setu App. However, the concerns were not fully again addressed. The Source Code released by the Government was of the previous version of the application which 1.1.3 and not for the version 1.2. Also, the 'server side code' was not made public of the app. This is one such instance which despite falling under the protection of unprecedented emergency circumstances raises concerns over continual arbitrary use of powers by the central government conferred upon it under the it act allied rules along with its effect on the privacy concerns of the common public.

The holistic view of the current data privacy regime in India alongside the conduct of the government has somewhere sent out a message that it reserves with it unfettered powers to manipulate data privacy laws as per its whims and will. However the future though under a cloud of haze as of yet provides a faint ray of hope with data privacy bill still pending to receive assent of the president.

V. CONCLUSION

India has seen a seismic shift of its stand on the issues of right to privacy. The passing of the Puttaswamy judgement has elevated the status of privacy to that of the Fundamental Right of Right to Life as enshrined under Article 21 of the Indian Constitution.

Though, India does not have an umbrella legislation which will take of all the issues of privacy, data breaches and prevention from cyber-attacks, it must observe the measures being adopted by different countries. Each model of data and privacy protection of countries mentioned has its pros and cons as to cater the needs of their specific regions. As seen in the USA, there is presence of both federal and state legislations; in the EU there was an overhaul of its existing

 [ISSN 2581-5369]

law to cater the needs of its citizens and in China, a whole new different approach is followed.

Unfortunately, India as of now has no such robust legislation to protect its citizens from any sort of privacy breaches. Though, the Government of India has proposed for the passing of a new legislation called the Data Protection Bill, it has been varied from the recommendations as provided by the Justice Srikrishna Committee. The new bill has given unchecked power to the Government. It has also provided for setting up of Regulatory Authority, yet this also seems to have been flawed. The recommendation has provided for the members to be independent from the Government, but the same is not incorporated in the bill. The want of Government to intervene so much into the lives of people in the name of any arbitrary reason has been a sign of worry. Along with this, it was also assessed that the government is still in its primitive stage when it comes to protecting its own confidential data from cyber aggressors. If the government is not able to guard its own top-secret information, not much can be expected from it with regards to its citizens' private data.

Therefore, it is submitted that India first needs to introspect the need of the hour by clearing the clouds of its own self-governed beliefs. A well planned and comprehensive legislation needs to be enacted, in which at the enforcement front, an autonomous panel can function without any pressure. The recommendations forwarded by the Justice Srikrishna Committee should be seriously taken into consideration without any tampering. After that, a strong 'Anti Cyber-Attack' force is required to be established to protect the nations', including citizens' and Government's, digitally stored data. Then only, the government should embark on its journey of data collection.

*****

 [ISSN 2581-5369]