International Journal of Law
ISSN: 2455-2194; Impact Factor: RJIF 5.12
Received: 12-05-2020; Accepted: 14-05-2020; Published: 18-06-2020
www.lawjournals.org
Volume 6; Issue 3; 2020; Page No. 269-279

A critical analysis on data protection and privacy issues in India

Rishabh Arora
B.com LLB (H), 5th year, Amity Law School, Amity University, Noida, Uttar Pradesh, India

Abstract
Data is something that surrounds everyone around & is generated virtually in everything we perform. We share the data deliberately & when we do something, the data is generated. For example, travelling or ordering a meal or using transportation. There is an uncertainty regarding the data when the data is of significant value & a number of companies are inclined to acquire such approach to the data. Data is the new currency in this newly advanced world. Regardless of all the information known, potentiality of the data is yet not known entirely. New forms of technology are emerging and new application are being developed, it results in enhancing the worth of such information. There are several questions regarding this: Whom does such data belong to? Who should have approach to such data? What must be the restrictions on manipulation of such data? Because of these questions, Jurists all over the world are still striving to understand these traditional notions of the law. Now that the situation is very critical, various governments are demanding & seeking approach to the data from the corporates & citizens. Meanwhile there are questions like about the bounds of privacy of an individual? Could the data be demanded for assisting such primary services, travel or interest of government? Would national security override the present concerns of privacy?
Disputation regarding this is on a new level now.
The Court of Last Resort in India reached the conclusion that 'right to privacy' considered as a fundamental right that is guaranteed by Part III of the Indian Constitution on 24th Aug,2017. A decision as such will be widespread, branching out any laws and regulations. The new laws would be tested on the parameters that are equivalent upon the laws which are making an unauthorised copy upon personal liberty and it has been tested under Article 21 of the Indian Constitution. After all this the right to privacy still possesses question in everyone's mind about its limits & contours.
India doesn't have any comprehensive legislation that deals in the protection of data & privacy. The policies & legislation which exist, essentially, are sectoral in its nature. These sectoral legislations are related provisions of such IT Act, 2000 & thus provided rules that regulates gathering process, usage of such private information & sensitive private information or date by the 'body corporate' within India.
The Government regulates the formulation for some depth legislation which helps govern data privacy & protection. Further efforts are required in that direction which was started by a group formed by experts on the privacy that is led by Justice A.P. Shah who is a preceding judge of the High Court of Delhi, that presented their comprehensive report on October 16, 2012. Then the government appointed one expert commission under the leadership of Justice Srikrishna who was a preceding judge of Last Resort in India, who review issues that concerns the data preservation in India & also regarding particular suggestions that are needful in the best interest of the Central Government on principles that are to be taken account for protection of data in India with a proposition draft a bill for data protection. The commission then submitted their report in mid-2018. Independently, the TRAI also proposed one deliberation paper on the privacy, ownership & security of data within the telecom sector. The report of our Household Finance Committee within RBI had prompted for the 'rights based' data protection framework which is against the idea of using consent to be considered as a first mechanism for protection of data to improve outcome of household financial.
There are some of the key legal provisions which focuses and governs privacy protection and personal data provisions
Key legislations are under as follows:
- Information Technology Act, 2000.
- Information Technology (Reasonable Practices & sensitive personal information & procedures) Rules, 2011.
- The rules & regulations that governs the following sectors:
- Telecommunications.
- Banking.
- Medical and Healthcare.
- Insurance.
- The Right to Information Act, 2005.
- General Data Protection Regulations-GDPR (EU).

Keywords: data protection, privacy issues, law, data protection regulatory bodies

Introduction
Data is something that surrounds us & is generated virtually in everything we do. We share the data deliberately & when we do something, the data is generated. For example, travelling or ordering a meal or using transportation. There is an uncertainty regarding the data when the data is of

significant value & a number of companies are inclined to acquire such approach to the data. Data is the new currency in this newly advanced world. Regardless of all the information known, potentiality of the data is yet not known entirely. New forms of technology are emerging and new application are being developed, it results in enhancing the worth of such information.

At present, India doesn't have any comprehensive legislation that deals in the protection of data & privacy. The policies & legislation which exist, essentially, are sectoral in its nature. These sectoral legislations are related provisions of such IT Act, 2000 & thus provided rules regulate gathering process, usage of such private information & sensitive private information or date by the 'body corporate' within India.

Jurists all over the world are still striving to understand these traditional notions of the law. Now that the situation is very critical, various governments are demanding & seeking approach to the data from the corporates & citizens. Meanwhile there are questions like about the bounds of privacy of an individual? Could the data be demanded for assisting such primary services, travel or interest of government? Would national security override the present concerns of privacy?

Data plays an essential part in today's world and its protection has become a huge workload as there are several loopholes and ways in which data can be breached and its security is at major risk. Data protection is essential and laws regarding it shall be constantly updated to protect the digital data of an individual or a company as a whole. There are several privacy issues within India which are addressed in case laws and new laws are being enacted, as we learn and grow so does the laws.

Chapter I: General Terms and Information

Concept of Data

The area 2(1)(o) of the Information Technology Act, 2000 characterizes "information" as "a portrayal of any data, information, ideas, directions or realities that are being readied or had been set up during any formalized way and which is intended to be prepared, is as of now being handled or has been handled during any figuring framework or organize and will be in any structure which incorporates PC printouts attractive or any sort of optical stockpiling media, punched cards, punched tapes or that is put away inside in the memory of the pc." Such electronic assent system that is given by Digital Locker Authority which characterizes 'information' as "any data that is held inside any electric structure by any open or private specialist co-op like a taxpayer driven organization office, a bank, and so on. This can incorporate both the records that are static or/and value-based. Notwithstanding, this idea of information isn't limited to such electronic data yet in addition reaches out to data that is put away in physical structure, for instance: on a bit of paper".

Privacy of Data

Throughout the most recent few years there has been some considerable increment in the measure of information that is produced with the utilization of different electronic gadgets and applications. These days, organizations acquire a generous incentive by breaking down the 'large information' and regularly decide their business techniques dependent on such examinations. While there is no contradiction to the effectiveness that is included, the consuming inquiry is that 'do an individual have any command over the way wherein such data relating to such an individual is gotten to and handled by others. Security is that the option to be disregarded or to be liberated from abuse or maltreatment of one's character. The privilege of protection is that the option to be liberated from ridiculous exposure, to gauge a lifetime of separation, and to quantify without unjustifiable impedance by the overall population in issues with which the overall population isn't really concerned.

The privilege of security isn't new. It has been one of the precedent-based law ideas and this is an attack of protection which gives a privilege to the person to guarantee tort-based harms. Where one of the first cases on the point is Semayne's Case, 1604. In this the route into a property by the Sheriff of London in order to perform a genuine writ. Sir Edward Coke, while perceiving a man's entitlement to protection broadly said that "the place of most are to him as his mansion and fortification where his barrier against a physical issue and the savagery for his rest". The idea of protection is additionally evolved in England inside the nineteenth century and has been entrenched in this day and age. If there should be an occurrence of Campbell v. MGN, the court arrived at the resolution that if "there is such interruption in any circumstance where an individual will sensibly anticipate that their security should be regarded then that interruption will be equipped for offering ascend to any obligation except if such interruption is regularly advocated".

Indian Jurisprudence on Right to Privacy

- Article 21 of the Indian Constitution watches: "No individual will be in hardship of his/her own freedom or life aside from with understanding to systems that are built up by the law". Be that as it may, the Indian Constitution prevents to explicitly perceive the 'right to security' as a major right yet.
- Regardless of whether such 'right to protection' is a major right or not was first reviewed by the Supreme Court inside the case: M. P. Sharma and Ors. v Satish Chandra, (District Magistrate), Delhi and Ors [1]. where such warrants were given for such hunt and seizure under the areas that are 94 & 96 (1) of the CRPC were put to challenge. The Supreme Court reached the conclusion that any intensity of search & seizure were not in repudiation of sacred arrangement. Further, the Supreme Court had ceased from giving any acknowledgment for the privilege to protection inside the crucial right that is ensured by the Indian Constitution by perception as under:

"An impact of such pursuit and seizure which is in any arrangement of statute and an abrogating capacity to the State for the insurance of Social Security which force is essentially managed by law. At the point when the constitution creators have seen that it is fit not to expose such guideline to any established impediments by acknowledgment of a key right to security, practically equivalent to the Fourth Amendment, we've no legitimization to import it, into a totally extraordinary central right, by some procedure of stressed development. nor is it genuine to accept that the sacred insurance under Article 20(3) would be vanquished by the legal arrangements for look."

- In such an instance of Kharak Singh v State of Uttar Pradesh and Ors [2]. The issue to be considered by the Supreme Court was if the reconnaissance by domiciliary visits near evening time against the blamed used to be a maltreatment to the right ensured under Article 21 of the Constitution of India, which brings the issue if Article 21 was complete within for right to protection. The Supreme Court reached the conclusion that if any such reconnaissance was truth be told, in contradiction of Article 21. Most of the judges additionally went to hold that Article 21 doesn't unreservedly or explicitly accommodate any protection arrangement along these lines right to security couldn't be understood inside any basic right. The Supreme Court watched:

"Having given such issues the best thought, we are obvious to the feeling, the opportunity that is ensured inside the Article 19(1)(d) doesn't encroach on any watch being kept over such developments of the suspect. Additionally, we don't consider that Article 21 has any importance to the setting as it was looked for to be proposed by learned Counsel for such a candidate. As it is now brought up that the privilege of protection isn't ensured directly under our Indian Constitution and accordingly any endeavour to find out such developments of a person which is just a way in which security attacks isn't some encroachment of a central right ensured by Part III of the Indian Constitution."

Be that as it may, the minority is of the supposition that by Justice Subba Rao perceived security as a significant aspect of our own freedom and accordingly Article 21 of the Indian Constitution by watching:

"In A.K. Gopalan case [3], which has been portrayed that freedom means identifying with or concerning such individual or body of an individual and covering up/her own freedom as in is the direct opposite of such physical limitation or compulsion.

The articulation has been wide enough to take in a correct that will be liberated from any limitations that are set on his developments. The articulation "pressure" in our advanced age can't be translated to a thin sense. In a general public which is unrefined, where there are no hindrances, just physical limitations which may diminish individual freedom, however as civilisation progresses the mental restrictions are more powerful than physical ones. The logical strategies that are utilized to condition to a man's brain which in genuine sense or physical restrictions as they incite the physical dread which channels one's activities through expectation and anticipated furrows. So the making of conditions which likewise essentially cause hindrances and dread edifices can be portrayed as physical restrictions. Further, the privilege to a person's freedom takes inside not just a correct which is to be liberated from any limitations put on his/her developments which is in addition liberated from any infringements on his/her private life. The facts confirm that the Indian Constitution doesn't explicitly pronounce any privilege to any security that is a crucial right however such said right to be a basic piece of our own freedom. Every nation which is popularity based bless residential life where it is relied upon to give him rest with physical satisfaction and genuine feeling of serenity and security.

The final hotel where such an individual's home where one lives among his/her family is his/her "palace"; it is his/her bulwark against any infringement on his/her own freedom. The expressions of that acclaimed Judge, J. Frankfurter in Wolf v. Colorado [4] called attention to the significance of the security of a person's protection against discretionary interruption of the police, could have no less be applied to an Indian home with respect to an American one. On the off chance that any physical restrictions on an individual's development would influence his/her own freedom or physical infringements on his/her private life will influence it to such a bigger degree. Which is undoubtedly nothing progressively pernicious to any man's physical joy or wellbeing in excess of a determined impedance inside his/her security. We will in this manner, characterize their privilege of individual freedom inside Article 21 which is a correct where an individual is to be liberated from any limitations or infringements with the rest of his personal effects, regardless of whether any of those limitations or infringements are straightforwardly forced or in a roundabout way realized by determined measures. It is comprehended to the point that any of the demonstrations of reconnaissance that are under Regulation 236 that encroaches the crucial right of such applicants under Article 21 of the Indian Constitution."

In this manner in such an instance of People's Union for Civil Liberties (PUCL) v Union of India [5] the Supreme Court plainly reached the conclusion that: -

"There is no faltering with holding the privilege to security as a section inside the privilege to "life' 'and "individual freedom" in Article 21 of the Indian Constitution. When the realities inside some random case that establish a privilege to protection, where Article 21 pulled in. The said right won't be reduced "aside from as per such technique built up by law".

As of late, the issue that was by and by raised under the watchful eye of the Hon'ble Supreme Court on account of one K. S. Puttaswamy (Retd.) v Union of India [6], Where the case 'Aadhaar Card Scheme' has been tested on the basis of the collection and aggregation of the section with the biometric details of the inhabitants of our nation which is to be used for different purposes and which is to penetrate the main right to protection enshrined in Article 21 of the Indian Constitution. In view of such unregulated quality from any previous point of law of reference to such a sacred status of the right to protection, the Supreme Court referred to the issue of an existing seat consisting of 9 (nine) judges.

It was contended as for the applications that the privilege to security is a central right that is co-end with the freedom and respect of an individual and that this privilege is found inside Articles 14, 19, 20, 21 & 25 of the Indian Constitution with different worldwide pledges. Despite what might be expected, the Union of India battled that the 'right to security' not being a basic right ensured under the Indian Constitution [7]. The essential guard given by the Union of India that (I) if the composers of our Constitution needed to incorporate such 'right to protection' as a major right, the equivalent will be explicitly included inside our Constitution; (ii) security is inalienably abstract and an obscure idea starting at now. The idea of security isn't anything but difficult to characterize. This dubious idea will not be raised to an essential right; (iii) The present laws as of now give enough assurance to a person against any such intrusion of security; and (iv) 'right to protection' being a genuine case had assent of customary law, any of such case will not be raised to a principal right. The Supreme Court by

arriving at a resolution articulated on August 24, 2017 [8] consistently that under: "The reference is discarded with the accompanying terms:

1. The choice in M.P. Sharma held “the privilege to security isn't ensured by the Indian Constitution presently remains over-ruled.
2. The choice in Kharak Singh that is to a degree which it holds the privilege to security not ensured by the Indian Constitution currently remains over-ruled.
3. The privilege to security that ensures which is a characteristic piece of our entitlement to life and individual freedom that is under Article 21 and which is a piece of the opportunities that is ensured by Part III of the Indian Constitution.
4. Choices ensuing to the Kharak Singh which have articulated our situation in the point gave over set out the present and right situation in law."

The Justice D.Y. Chandrachud, plainly held that

a. Life and individual freedom are an unavoidable right and that these rights are indivisible from any noble presence of human. Such pride of individual are balance b/w people & mission for such freedom are our fundamental mainstays of the Indian Constitution;
b. Security is unavoidably shielded right which develops fundamentally from Article 21 that incorporates individual freedom and assurance of life under the Indian Constitution. The component of protection may emerge in settings that are shifting from different aspects of opportunity and respect that are perceived and ensured by the basic rights contained in Part III of the Indian Constitution;
c. Security at the centre incorporates safeguarding of one's very own affections, the sacredness of a family life, multiplication, the home, sexual direction and marriage. Protection will likewise infer an option to be disregarded. Security shields the person's self-governance and furthermore perceives the capacity of the person to control essential parts of his/her life. Individual decisions that are administering a lifestyle are currently natural for protection. Security ensures the heterogeneity and furthermore perceives the majority and decent variety that are a piece of our way of life. While the genuine desire from the protection may shift from a sheltered zone to a progressively private zone and from private to accessible open fields, it is increasingly essential to comprehend that the security isn't lost or given up simply because the individual is in any open spot. Protection is appended to an individual since, it is a fundamental aspect of one's respect of being human;
d. Essentially, different rights that structure a piece of the major opportunities that are secured by Part III of the Indian Constitution, including the privilege to life and individual freedom given under Article 21, protection isn't simply considered as a flat out right. A law that can infringe upon one's security may need to withstand such touchstone of an admissible limitation on the key rights. In such a setting of Article 21, an attack of one's protection will be supported inside the extent of a law that specifies a strategy which is reasonable, just and sensible. The law will likewise be legitimate as per an infringement on one's life and individual freedom under Article 21. Such intrusion of life or individual freedom on an individual will be met with the three-overlap necessity of (I) legitimateness, that proposes presence of law; (ii) need, characterized inside terms of one's real estate point and (iii) proportionality, which will guarantee discerning nexus between one's items and any implies that are embraced to accomplish them;
e. Security has both positive and negative substances. Where such pessimistic substance prevents the state from submitting any interruption upon life & individual freedom of any resident. Its positive substance forces such commitment which is on the state to take all the fundamental estimates that can be utilized to ensure the security of the person."

Supreme Court dismissed the dispute introduced by the Union of India [9] and kept in mind that going through the given idea of right of security as respects the inception, the Supreme Court arrived at the resolution that the privilege to protection is an inborn and which is indistinguishable from the human component from individual and it's centre of human pride. Consequently, it was reasoned that protection exists in both positive and negative substances [10]. The pessimistic substance, which goes about as a ban to the State from submitting such an interruption on the individual freedom of the resident, their positive substance forces such a commitment on the state to take all the essential estimates that are expected to ensure the protection of the person [11]. Along these lines, the established assurance of one's security can offer ascent to two of the between related insurances, that are: against the world everywhere which is to be regarded by all including the State: the option to pick with what individual data that is accessible to the open space, that against the State: which are as fundamental attending of any equitable traits that are constrained to government and such constraint on intensity of the State [12].

Because of this, the given judgment on the privilege to protection has become 'more than the custom-based law right' and 'to a greater extent a powerful and hallowed' than any legal right. Along these lines, presently inside the setting of Article 21 of the Indian Constitution, an intrusion of such security will be supported based on 'a law' that specifies a strategy which is simply reasonable and sensible. It is to be noted since R.C. Cooper v UOI [13], that 'methodology set up by law' inside Article 21 has increased considerably with the fair treatment component also whereby even such substance of the law can be tested on being not as per the necessities of such legitimate law [14]. In this way, due to one side of protection being perceived as a principal directly with existing sectoral enactments, in the event that they are tested it might now need to breeze through the rigors of previously mentioned assessment. Same will not have been the position, if protection may have stayed negligible legal or custom-based law right.

As an outcome to this, presently the "Adhaar Card Scheme" that was claimed to be a penetration of crucial right to security, has now been tried by similar guidelines that are a law which attacks one's very own freedom under Article 21 is held at risk to be tried.

While examining the privilege to data with protection in this day and age, the Hon'ble D.Y. Chandrachud held that:

a. Informational protection, that is a feature of the privilege to security. The danger to one's protection during a time of data may start from the state as well as from some non-state on-screen characters also. We

recommend to the Union Government that the need to look at and to place into the spot a vigorous system that is required for information assurance. The formation of a system will require a progressively cautious and touchy harmony between an individual interest and the genuine worries of the state. The genuine focal point of the state will be on ensuring national security while it forestalls and examines wrongdoing with empowering the advancement and such appearance of information while forestalling the dissemination of one's social government assistance benefits. These are simply matters of arrangement that are to be considered by the Union government, while it designs a deliberately organized system for information security. Since the Union government had educated the Court it established a Committee that is led by Justice B.N. Srikrishna (previous Judge of the Court) and for the reason such issue will be managed suitably by the government which has due respect to what had been set out in the given judgment.

b. We are during a time that is educated, where the development and improvement of such innovation where more data is currently effectively accessible and open. The data blast had complex numerous points of interest yet in addition some simple impediments. The entrance to data, that an individual might not have any desire to give it needs the assurance of security.
c. The privilege to protection, which is asserted by the State and non-State on-screen characters. Acknowledgment and implementation of such cases qua non-state on-screen characters can require administrative mediation by the State."

Current Issues Surrounding Data Privacy

- Supreme Court constrains on the state to indulge with the basic rights enlisted in the constitution. Article 21 provides for the violation of privacy in the Indian constitution. The test of reasonableness concerned. The test of proportionality and reasonableness seeks to provide remedy in the case of infringement to right to privacy of the individual. with the form and the matter of the law lies under Article 14. It might take few years to jurisprudence in determination to what constitutes a fair state. The rationality of the Adhaar Scheme shall be examined on the basis of the evaluation.
- It is contended that India aims to protect the human rights in the case of the data security and is conflicted for the consent-based model. Under a consent-based model, where the person who is authorised as data controller has the access to information and can change and exchange data with the third party. However, many are unaware of the fact that the information can be shared at the time of the consent. At the other hand, the rights-based model that is aiming to protect the human rights, allows the users to have right to access their data despite ensuring to data controller that the rights are not misused by these users. This leads to high level of the control for the users over the personal data.
- It was held by the Supreme court that citizens can seek judicial redressal for the violation of any privacy rights. It was observed that this may affect the tech companies which are dealing with the privacy and security issues. Users may not only bear charges for the misconduct but may also invoke the fundamental privacy right.

Concerns and Difficulties

- What is the essence of the data being covered by the Indian legislature?

India does not have any multidisciplinary data preservation mechanism. The only act which deals with the privacy data or any protection of the knowledge is the Information Technology Act,2000 and therefore the Information Technology (Reasonable Security Practices & Procedures & Sensitive Personal information) Rules, 2011 were introduced for the protection of such data. The core objective of this act was to protect any personal data or any information which is confidential or is sensitive data that is: the information which involves password, pecuniary information as a bank account or credit card or debit card or any other payment instrument details, physical, physiological, mental health condition, sexual orientation of an individual, medical records or history, his/her biometric information.

However, such information that is freely available within the public domain is not considered in the ambit of 'sensitive personal data or information'. Further, such provisions only deal with the collection and dissemination of any information by a 'body corporate'.

In the addition to above stated, the respective sectoral regulators prescribe the data privacy measures that are required to be undertaken by: the telecommunications companies, the banking companies, the medical practitioners and the insurance companies to protect the privacy of data that is collected from its users and to avoid any unauthorised disclosures to any third parties

- Who can collect the personal data?

The Rules 5 of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011 orders that no body corporate or any person on behalf of it shall collect any sensitive personal data or information unless such information that is being collected for a lawful purpose which is connected to a activity or function of such 'body corporate' & such collection of info is to be considered necessary for such purpose only. While the info is collected such person who share's such information is required to be made aware towards the fact that his/her information is collected with the reason of collection of such information, the planned recipients of the info & the name with address of agency which is collecting such information & agency that will retain the info.

- To what degree will personal data be exchanged with third parties?

Personal data can be exchanged up to a degree where such data considered as sensitive private data is shared with the consent of such person or it is present as a contractual obligation. Or when such disclosure is with compliance as part of any legal obligation.

- What is the duration of storing such personal data?

Any corporate body or persons keeping confidential private data or information on behalf of such corporate body or persons shall not maintain the data for longer than is needed for those purposes for such information has been legally used or otherwise necessary by law until such time as it is in effect for such collection, and the information shall be used only for the reason for which it may be used. Therefore, the body, or another person on its behalf, collects such information, before collecting the information, it is appropriate to provide the information provider with an

choice not to supply the data or information that it seeks to collect. The provider of such information at any given time when making use of these services or otherwise has the option of withdrawing their prior consent.

- What are the responsibilities of employers with respect to the personal data obtained by their employees?

It is known that an employer collects information that is considered personal and sensitive from its employees within the normal course of the business, such information includes various types of data. Where such an employer retains and collects information on his computer. Such information collected by an employer must be detailed recorded with a security plan and policies that may include physical security that monitors and take measures that are necessary for the safety of such information. On the other side it was implemented that employers should use the international standards on Information technology that are IS/ISO/ICE, 27001 for security of management system and techniques.

Technology (Reasonable Security Practices and Procedures and Sensitive Personal information) Rules, 2011 was considered to be implemented where the employer who is considered to be a body corporate who collects any such data or receives any data or possess or store any sort of information of his or her employees which is required to have any policy for its privacy for handling or dealing with such information that is considered private. Then such an employer is requires to develop such policies that are available for the review of his or her employees and they shall also publish those at their website.

From the above mentioned statement it was considered as evident that such comprehensive statement that were regulating such collection of a person's data has been considered need for today's world. As there is no regulation that regulate such process of law that bounds the data that is not sensitive information or data

In such a case where WhatsApp was acquired by the Facebook and when it changed the privacy of the WhatsApp that integrates its data that will be used and shared with Facebook, it grabbed attention of a lot of users, whereas Facebook explained that such data will be collected to improve their advertisements and experiences. such users were asked to go through the updated terms and conditions and agree with the same to continue its use from 25th September, 2016. [15]**.** In view of a known development Karmanya Singh Sareen and others filed a writ petition against such change before the Hon'ble High Court of Delhi contending that taking away such protection of privacy to data of users of the app "WhatsApp" and sharing the data with Facebook was within the ambit of infringement of fundamental rights of the users that are guaranteed under Article 21 of the Indian Constitution.

The Delhi High Court while deciding upon the above stated case ordered, if any users opted to completely delete their WhatsApp account then WhatsApp should delete users data completely from their servers and refrain from sharing any of the users' data with Facebook and so far as the users who opt to remain in the app "WhatsApp" are concerned, the existing information/data/details of such users up to September 25, 2016 shall not be shared with "Facebook" or any one of their group companies.

Chapter-II: Cyber Laws in India

Information and Technology Act, 2000

Government provides legal framework for privacy and data protection through IT

(Information Technology) Act which are mentioned below:

The act lays down the provisions for the data protection by introducing privacy policies and sanctions which are violative of these privacy policies. The provisions of the IT law are listed below:

- **Section 43:** It states that any person who is engaged with the secure access to the computer system without the authorisation of the owner who is in charge of the systems, or extracts and downloads any information, or steals and destroys any information, or follows any person to slither and destroy any source code from the computer will be held liable for the damages. Person will be liable to pay the compensation for damages amounting to one crore rupees to the person who is affected.
- **Section 43A:** It lays down the legal person who is authorised to possess sensitive or personal information fails to comply with the security practices and policies negligently as mentioned in the provisions that causes damage and undue losses to such person. The person authorised will be held liable for the damages amounting not more than five crore rupees.
- **Section 66 C:** It deals with any person who is engaged theft and provides anyone with dishonest and fraudulent electronic signatures and passwords will be held liable with the imprisonment of three years and fine of one lakh rupees.
- **Section 66 E:** According to this section, any person who captures any image intentionally and publishes such image without the consent, violating the privacy of such person will be punishable for imprisonment up to three years or fine not exceeding two lakh rupees or both.
- **Section 72:** Person authorised to access and secure any information, book, register, document, or any electronic file discloses such data without anyone's consent will be punishable for imprisonment to two years or fine amounting maximum to one lakh rupees or both.
- **Section 72A:** Any person who involves a mediator in providing services under the legal contract and has access to personal information of another person having the intention of causing any loss or gain and reveals any private information or there exists any violation of the legal contract. Person will be liable for the prison term up to three years or chargeable with fine of five lakh rupees or both.

Information Technology (Reasonable Security Practices & Procedures & Sensitive Personal information) Rules, 2011

- **Rule 4:** This rule deals with the enterprises or any person who acts on behalf of the body corporates or enterprises who possesses any confidential information should have the privacy policy in dealing with such sensitive or personal data. The terms and conditions of the privacy policy should be published on the website of the enterprises. The conditions prescribed in the policy should be clear and fair and the utilization of such data should be well explained. Disclosure of any sensitive or personal data should be provided under rule 6. Security procedures are listed under rule 8.
- **Rule 5:** The collection of such information process by the person or the enterprises. The agreement has to be

obtained in writing in the way of letter or through fax or by email for any sensitive or confidential info. The body corporates shall not collect any sensitive information unless the purpose of collecting such information is for any legal purposes which is associated with the body corporate itself. There are certain steps to be followed for gathering such information that are: (a) the person concerned must have the knowledge of the facts of information provided. (b)Deliberate beneficiary of the information. (c)The name and address of the collecting agency and the agency that will deal with such information.

The enterprises could permit the providers to review any information which they find is inaccurate or is incorrect which needs to be amended. The enterprise cannot be held liable if provider is providing sensitive or any confidential information to the body corporates dealing on their behalf.
The provider has the option of withdrawing the consent provided to the body corporates once the purpose has been resolved. The withdrawal must be submitted in writing to the body corporate. The information should be kept fully secured.

- **Rule 6 -** This rule explains when the body corporate is disclosing information to the third party provides a prior permission from the provider for dealing with any sensitive data. The information provided is under a lawful contract.

It is compulsory to share the data with the Government agencies as described under the law to obtain such information which includes any sensitive or personal data for the verification purposes for the prevention from cyber incidents, prosecution and penalties for the offences. The Government for acquiring such information send a request to the body corporate in writing and the purpose for obtaining the information.
Notwithstanding anything that is contained in the rule, any sensitive personal data or any information that can be disclosed to a third party by an order under the law that is in force for the time being.
The third party acquiring the information cannot further disclose such personal data to anyone.

- **Rule 8** – While dealing with sensitive or personal data the body corporates needs to comply with certain measures with all reasonable security practices and procedures. The body corporates when implement all the security practices and have security programmes for the information documented and security policies which contains all the technical security control measures which are equivalent to the information of assets being protected within the business.

If there is any breach of the information security the body corporate or any person acting on their behalf shall demonstrate to agency as mandated by the law that they have implemented all the security measures as prescribed in the policies. 'Information Technology Requirements' is one standard on which it must be followed.
Associations or the entities formed where members are automated by the codes for the data protection shall get its codes approved and certified by the Central Government for effectual implementation.
The scrutiny of security procedures which are carried by auditor once in a year or the body corporates or person on their behalf who undertake noteworthy upgradation of its and process and the computer assets.

Chapter-III: Regulatory Bodies
Telecommunication Regulators
Indian Telegraph Act, 1885

- **Section 5:** The Government has the ground of the licensed telegraphs and to impede any of the messages on the account of public emergency or for the safety of the general public or for maintaining healthy relations with the foreign states or for the avoidance of any encouragement of any offence. An officer who is authorised by Central Government if satisfied should record the reasons in writing that any message to and from the person received by the telegraph who should not be detained or transmitted or can be disclosed to the government making such an order or to any politician as mentioned in the order. Any press message which is to be published in India of correspondents which is accepted by the Central Government or a Government cannot be detained unless the transmission is prohibited.
- **Section 24:** It states that if there arises any repercussion for attempting illegal learning any contents of the messages. Any person who commits such an offence which is unlawful to acquire any content of the message will be held liable with the prison term not exceeding one year and with a fine as described under section 23.
- **Section 25:** When the telegraphs are damaged intentionally, a person who performs such an act for obstructing such delivery or transmits any message or tries to involve to learn any contents of the message or removes, causes damages to any machinery or equipment, any wire or battery, or any other part which is utilized in the working of telegraph will be held liable with a fine or imprisonment of maximum three years or both.
- **Section 26:** Person who has the official duty of being telegraph officer connected to office which is recruited to the telegraphing office, who alters any kind of message that he had received wilfully for the transmission or otherwise which is in compliance with the Central Government or Government or any political leader to form the order who is authorized by the Central or Government intercepts, transmits any part of the message or in the execution of the official duty or with the compliance of competent court which discloses a message or party of any message, to the person who is not entitled to receive an equivalent, professes with any radiotelegraphic signal to a person who is not acquainted can be held liable with fine or imprisonment extending to three years or both.
- **Section 30:** When a person fraudulently retains any message which needs to be delivered to some other person or is to be acquired by the telegraph officer to deliver any message, deterioration of refuses to attempt to do so, will be punishable with fine or imprisonment for term extending to two years or both.

In PUCL v Union of India [16], petition had raised his voice against the validity of section 5(2) within Telegraph Act where in the opposed side it was suggested that such said means which are suitably read-down to incorporate

procedural guidelines for safety to rule out arbitrariness and to stop the aimless tapping of telephones. The Hon'ble Supreme Court while deciphering Section 5(2) within RTI Act had held that the section list down the conditions and scenarios which have the power to intercept any conversation or messages can be exercised. Although no deduction is made for the provisions of Section 7 (2) (b), there is no procedural support to ensure that it is a fair and equitable exercise of appropriate law. "The right to privacy is a fundamental component within the purview of the right to life under Article 21 of the Indian Constitution" as held by the Hon'ble Supreme Court. Moreover, the Hon'ble Supreme Court has also held that "the telephone tapping, unless it's within the restrictions of Article 19(2) of the Indian Constitution, may be a violation of the proper to privacy and therefore the laying down of procedural safeguards was necessary to guard the mentioned right of the people." The Hon'ble Supreme Court came to this strong conclusion that an order for tapping telephone under the ambits of section 5(2) of the RTI Act shall be issued by Home Secretary of Central or government who should maintain such proper records of intercepted communications and also disclose the materials being intercepted, moreover a review committee will conduct examination of these orders and shall set aside any orders that come in line with the mentioned provision. In addition to this the duration of the order shall not exceed six months.

Following that judgment, a new rule, called Rule 419A, to be inserted in the Indian Telegraph Rules of 1951, which elucidated the guidelines for the interception of a message in the ambits of section 5 of the Telegraph Act, should be issued only by the order passed by the Secretary of the Government of India. However, in the extraordinary and inevitable circumstances referred to above, a political leader who should at least be a Joint Secretary, a Government of India approved by the Union Home Secretary or a State Home Secretary, whatever the case may be, may also be named.

However, with the coming cases in areas that are remote wherein it is difficult to obtain prior guidelines for intercepting messages or. Wherein it is difficult to obtain any prior guideline for an interception of any message there the administration of specified interception of a message could be supervised with the beforehand authorization of the top or second most senior officer to the authorized security that is Law Agency belonging to Central Level & the officers allowed during their behalf should be at least be holding the rank of military officer of Police level next to state that is concerned authority needs to be notified of such interceptions on the directions of the approving authority within a period of three working days whereas the concerned competent authority could confirm the interceptions within seven (7) days. Given the confirmation from above mentioned competent authority is not received within the mentioned time period i.e. seven days then such interception shall cease to exist and will also result into the aforementioned message or class of messages not intercepting without any earlier approval of the Home Secretary of union or the Home Secretary of state, whatever the fact scenario brings. Moreover, the records relating to such guidelines for interception and received messages the competent authority which is relevant shall destroy it and the security which is authorised and the enforced agencies shall require functions of such agencies every six months. Furthermore, the service providers are required to destroy all and any mentioned records which relates to the directions for interception of message within the required time period of two months concerning the discontinue of the interception of any messages & extreme secrecy also needs to be maintained while doing the order.

Banking Regulators

State Bank of India Act, 1955

- **Section 44:** In this, a secrecy clause by which a bank and their team or members such as advisors, board members or employees etc who are in obligation to the state bank on secrecy in prescribed form by a statement. According to this, the depository finance institution will observe the usage and practice that is custom among their bankers. That it will not disclose any concerning information with any third party with exception of depository expressly declares to reveal such information. It shall be in accordance to the institution and their guidelines with case of sharing private information.

Banking Companies (Transfer & Acquisition of Undertakings) Act, 1980

- **Section 13:** According to this, every new bank should observe where it is compulsory by law, the usages and practices that are custom with bankers. it shall not reveal information concerning or the affairs of constituents except during which it is with accordance to law or usages and practices custom with bankers that are considered acceptable or necessary to correspond new bank to reveal any information provided. Further each and every director or any committee or member of an area Board or Adviser officer, Auditor or employee who are custodian to correspond new bank should consider before entering his/her duties, make a statement of secrecy within the form that is prescribed.

Credit Information Companies (Regulation) Act, 2005

- **Section 19**: A credit info company or specified users or info company shall take steps that are necessary to preserve security and accuracy of credit info while ensuring that such data related to credit info maintained is accurate, duly protected and complete against any kind of loss with any unauthorised access or revelation.
- **Section 20**: In this, each credit info company or specified users or credit institutions should take on privacy principles with reference to credit info and should take on the subsequent privacy principles with connection to sharing, processing and collection of information, recording, collecting data, preservation, usage and secrecy, of credit info, which are:

a. Propositions

a. which shall be applied to each and every banking concern institution for collecting data from their mendicants, clients and by each credit info corporation, where such collected data from such institutions or credit info businesses for protecting, notching, processing the info that concerns credit info be embellished and acquired from similar banking concern business or credit info company whatever the case be with allocation of data with such users.

b. which shall be embraced by each and every such user to process, protect and maintain the information received

or furnished in the concerned credit info.

c. which shall be adopted by company providing credit info to allow access to record that contains information credit of customers, borrowers and modification of documentation just in case.
b. The purpose of the credit info for which it will be used, disclosure and restriction on use.
c. The obligation of companies or specified users or credit institutions to check the accuracy of the credit information provided.
d. Credit info preservation for which the information is maintained by each credit institution, specified users and credit info company which includes the period for information to be maintained, the manner in which information is deleted and maintenance to such recorded credit info.
e. Credit info companies, specified users and credit institutions networking through e-mode.
f. Other procedures and principles which reserve bank may consider necessary relating to credit information and any appropriate regulations that are defined by the reserve bank.

- **Section 22:** Any unsanctioned access to credit info that is possessed or controlled of credit info company or specified user or any credit institute could be punished with fine up to INR One Lakh with deference of each felony and if he/she continues use of illicit access to the data then with further fine which may be up to INR Ten Thousand for given day that such access continues and unauthorised credit info should not have to be reserved into kindness for that reason.

Credit Information Companies Regulations, 2006:

- **Regulation 10:** Under the regulation, it specifies the addition to section: 20, Credit information Companies Act, where each credit knowledge company, specified user and credit organisation should acknowledge the subsequent privacy principles with correspondence to their functioning, these are:

a. Caring with respect to collection of credit knowledge which should be appropriately and precisely recorded, assembled and processed with protection in case of loss, unapproved approach, usage of such information, alteration or declaration.
b. Keep the credit knowledge provided by it up to date, precise and thorough.
c. Establishing and adopting policies related to declaration to an individual, upon appeal, his own credit knowledge and provided that the credentials are acceptable.
d. Retaining of such credit knowledge which is gathered, conserved and publicized by them for at least a duration of seven (7) years.
e. Establish guidelines & procedures that needs be acknowledged by CIC with consent of RBI with due respect to conservation and demolition of all credit knowledge.

- **Regulation 11:** The principle and procedures related to private data. Each and very credit Information company, organisation where particular user should acknowledge subsequent principles:

a. Private data should not be publicized, revealed or gathered other than for the motives that are related to the functions given within the Credit Information Company Act, or with relation to the position & functioning like an employer with respect to a person whoever has been in such an employment.
b. Ensuring prior to any data is gathered or it shall not be feasible as soon as data is gathered, such a person who is concerned be notified about such collection and data which is being conserved by the person should be preserved in case of any loss, or unauthorised approach, use, modify or any such reveal.
c. Retaining private data which is gathered, conserved and publicized by them for at least a duration of seven years;
d. Establish the procedures and guidelines to be acknowledged by them with consent of the RBI with respect to preserve and demolish private data.

The Public Financial Institutions (Obligation as To Fidelity and Secrecy) Act, 1983

- **Section 3**: The section concludes that any PFI should not approve as however given in any law related to for the time enforced reveal information related to or to the affairs of their constituents other than in given incidents during which they are in obedience to the law or usage and practice that are familiar within the bankers that are appropriate or necessary for public financial institution shall disclose that information.
- **Section 4:** The section concludes that each member or director of a committee, an officer or auditor or an employee of any PFI that the Public Financial Institutions Act applies then he/she should prior to entering on his/her duties construct a declaration of fidelity & confidentiality for the form that began within the Public Financial Institutions Act.

In District Registrar & Collector of Hyderabad v Canara Bank [17], Supreme court of India reached the conclusion & acknowledge that a person/s right to privacy should extend to his documents which are with his bank, those documents should remain confidential. The case clearly sustained the verdict of the high court that had considered section: 43, stamp act void that was changed in the state of Andhra Pradesh that empowered a collector in the state inspect any papers, records, or registers with his power and which is in custody of any officer appointed by the govt such as a public offer to secure their duty or prove which could lead to any revelation of any omission or fraud.

Medicine & Healthcare Regulators

Mental Health Act, 1987

- **Section 13:** According to this, any psychiatric nursing home or hospital require an inspection by an inspecting officer. Such an officer requires the entity to produce all records that are maintained with accordance to the Mental health act. Given that any records of a patient that are person which are inspected should be kept as confidential leaving the part where such officer is sure that any patient in such place is not getting real treatment and care that is of quality standards, then such officer can account the incident to the licensing power where the power can issue directions which it seems fit to such officer that is in charge the license of such place where such officer if bound to be in complete accordance to the given directions.
- **Section 38:** Any personal records that are kept by the hospital which is considered to be confidential by

opinion of the officer who is in charge of a patient, then such records will be kept confidential and any visitor of a patient shall be not entitled to inspect it.

Indian Medical Council (Professional Conduct, Etiquette & Ethics) Regulations, 2002

- **Regulation 7.14:** In this, a medical practitioner who is registered should not disclose any secrets of a patient which such practitioner had learnt during his or her profession except where it is by the order of a court where the circumstances consider such a patient as a risk to the community or the patient itself with any diseases. Then in case of such a disease that is communicable and concern the health of public should be notified to the competent authorities.

In Mr X v Hospital Z [18], Supreme Court reached a conclusion where the right to privacy towards a patient to maintain confidentiality by the doctor subjects to the health protection of others around such patient. It was concluded where any disclosure which the party was HIV+ concluded to not violate the right to privacy of the party on such ground where the female with whom the male was considered to be married shall be considered saved in time by disclosure from any risk of infection'.

Insurance Regulators

Insurance Regulatory & Development Authority of India (Sharing of Database for Distribution of Insurance Products) Regulations, 2017

Regulation 9: In the regulation, a company with a transfer that shall be approved by IRDAI which should also be registered by an insurer should not provide details of any of its customers without the consent which is in written or any details that provide any record of a business transaction that may be related to any firm/person or a company.

Insurance Regulatory & Development Authority of India (Maintenance of Insurance Records) Regulations, 2015

- **Regulation 3:** According to the given regulation every insurer should maintain records of an insurance policy and their data & any maintenance system that shall have such necessary features of security. The maintenance and manner of records should be according to the policy which is framed for insurers and also approved by board. To maintain such records in e-form, the policy should have:

a. Process & electronically maintain records,
b. Security & Privacy of their holder of policy with claim data,
c. Handle virus, issues which are vulnerable,
d. Hardware security and software,
e. Backup, recovery in case of disaster & continuity of business,
f. Data archive.

The policy shall also include detailed plan to review such implementation of the storage and maintenance of records that will be overseen by such risk management committee of the board of insurers. The records will be confined in data centres that are located and maintained only in India.

Insurance Regulatory & Development Authority of India (Outsourcing of Activities by Indian Insurers) Regulations, 2017

The regulations given to the board of directors of an insurance company to conduct the deploy policies where such assessment of a risk that are involved in deploying that include the confidential information of such data and standard of services which are rendered under deploying contracts is addressed [19]. Such agreements which are necessary to hold info & asset of such ownership rights, protection and safety of data to confidential information, termination of contract and information technology clause specifying orderly handing over of assets, data etc [20].

- **Regulation 12:** This regulates confidentiality and measures of security that needs to be managed by such insurers with deploying their services. Such insurer should satisfy themselves with deploying their service provider's policy for security, controls and such procedures shall be enabled by insurer for protecting his/her confidentiality and policyholders security information even when the termination of contract occurs. It should be the duty of an insurer who shall ensure where such data or the information provided be parted to any such deploying service provider under such agreements shall remain confidential towards it. The insurer should take in consider any contractual or legal duty on such part of service provider to disclose any circumstances and arrangement under the insurer's data for customers that to be disclosed. Where in event of such termination of such an agreement, insurer shall make sure that every data given to such provider is saved from any use.

Chapter IV: Right to Information Act, 2005

Right to Information Act came into force with the main objective to provide private citizens with the access to information which was controlled and regulated by the public authorities who provided with fair and clear information. However, the act also provided with certain exceptions regarding the disclosure of info.

- **Section 8(1)(j):** According to the section, there are certain confidential information which cannot be disclosed to public at large and does not have any relation to citizens or which might contain unjustified annexation of privacy of a person, except in the case where Central or SPI Officer or any other authority whatever the case be, if satisfied with the larger interest of public and accounts for disclosing any information. Any information which is already approved by the Parliament or State Legislature cannot be refused by an person.

There are several decisions made by the courts of India contradicting above given provisions.

- As in Supreme Court of India v Subhash Chandra Agarwal [21], the issue which arose whether the right to information should be declared & claimed with the relation to info about any declaration with all or any private assets of Judges. The High Court reached the conclusion that respondent "had right to information with respect of the knowledge related to making of declarations by the judges of the Supreme Court pursuant to the provided 1997 Resolution". Judges declared that it was not the first time that the assets

were introduced. However Subordinate judges needs to do so. The higher hierarchy judges have the higher degree of accountability. Since if subordinate judges are under the obligation to introduce the assets so are higher court judges. Any disclosure of information should comply with the provisions of section8(1)(j). This section also includes that personal information shall include tax return, medical record etc. that are not to be disclosed. The appeal was dismissed.

- Whereas, In such a case of Girish Ramchandra Deshpande v Central Information Commissioner and Ors, where question in front of the Supreme Court that matter which is pertaining to persons service career & such details about their liabilities & assets, immovable & movable property etc. shall be given or treated as private information which is given with section 8(1)(j) of the Right To Information Act. The Supreme Court reach the conclusion and reached the conclusion that "performance of an employee in any organization is a matter which is between the employer and the employee and any particulars called for by the petitioner which include any show-cause notice or orders of censure and/or punishment, that falls within the ambit of personal information. Such details disclosed within income tax returns shall be treated similarly". It shall be disclosed only when CPI Officer, State Public Information Officer or any appealing authority shall be satisfied given the larger public interest is justifiable declaration of that information [22].
- In Subhash Chandra Agarwal v The Registrar, Supreme Court of India and Ors, in this question arising before the high court was with regard to any disclose of information that includes medical facility details availed by a person. The high court reached the conclusion with the fact where the expenditure that was incurred by receiving medicinal cure of a judge for his stage in which it was well-appointed by CPI officer that is not with the case of the person filing appeal where the said expense is excessive. Reached to the judgement that any details of said medical facilities that were availed to be considered a type of private information and there is no need for disclosure on the ground of public interest [23].

Chapter-V: General Data Protection Regulations

In April 2016, European Parliament adopted the general data protection regulations. GDPR has replaced the EU Directive which was adopted by the European Parliament & Council on October 24, 1995.

The GDPR not only applies to organisations which are situated in EU but also applicable to organisation situated outside EU in such: (a) Processing the confidential data within the activities of business or businesses of any 'comptroller' or any 'central processor' in the EU, or (b) utilization of any personal data of EU data subjects, related to contribution of goods or services which comprises of free services or (c) Observing different types of conduct, if the conduct takes place within EU [24].

Though, a trivial website which is accessible with any kind of services within EU is not adequate to trigger any request of GDPR. Where elements as providing any amenity in languages or the currency which is utilised in the Member state provided that which is not availed in the third country, or bringing up users in other member states may also activate any supplication of the GDPR

Further, all the conditions for the consent had to be strengthened. The request for consent shall tend within an intelligible and simple accessible form, with the aim to process attached with consent: means that it shall be absolute. Consent shall be distinguishable & clear from any or all added matters. Provided within such intelligent & simple accessible form by using clear & simple language. They shall be easy as to take away consent because that what it is to offer it. Whenever assessed either consent shall be freely given there must be maximum account must be taken of even if the performance of any contract which includes the supply of a service, is conditional in consent for processing private data that does not necessarily given for performance of contract.

If there is any breach within the GDPR then entity may be get a fine that is more than 4% of their yearly turnover worldwide or €20 million. The GDPR implemented an approach. Any additional specified violation may attract fine which shall be in the upper of 22 of the yearly turnovers worldwide or €EUR 10 million [25].

References

1. SCR 1077, 1954.
2. 1 SCR 334, 1964.
3. SCR 88, 1950.
4. 238 US 25, 1949.
5. 1 SCC 301, 1997.
6. 8 SCC 735, 2015.
7. Supra note 10, at Para 359, 395,530,579, 626, 627, 650.
8. Justice K.S. Puttaswamy v UOI, SCC Online 996, 2017.
9. Ibid, para 53-65, 531-536, 718, 736.
10. Ibid, Para 304-307.
11. Ibid, Para 459
12. Ibid, Para 403.
13. 1 SCC 248, 1970.
14. Mohd. Arif v Registrar, Supreme Court of India: 9 SCC 714, 2014.
15. Karmanya Singh Sareen V Union of India, SCC Online Del 5334, 2016.
16. 1 SCC 301, 1997.
17. 1 SCC 496, 2005.
18. 8 SCC 296. Also see (2003) 1 SCC 500, 1998.
19. Regulation 7.
20. Regulation 11.
21. AIR 2010 Delhi 159.
22. 1 SCC 212, 2013.
23. (150) DRJ 628, 2015.
24. Article 3 of GDPR.
25. Article 7 of GDPR.