|LAW AUDIENCE JOURNAL|
|VOLUME 2|ISSUE 1|JAN 2020|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2018): 2.06|IMPACT FACTOR (2018): 2.527|

|LAW AUDIENCE JOURNAL®|

|VOLUME 2 & ISSUE 1|

|JAN 2020|

|ISSN (O): 2581-6705|

EDITED BY:

LAW AUDIENCE JOURNAL'S

EDITORIAL BOARD

|LAW AUDIENCE JOURNAL|
|VOLUME 2|ISSUE 1|JAN 2020|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2018): 2.06|IMPACT FACTOR (2018): 2.527|

Email: lawjournal@lawaudience.com, info@lawaudience.com,
Phone: +91-8351033361,
Website: www.lawaudience.com.
Facebook: www.facebook.com/lawaudience
Instagram: www.instagram.com/lawaudienceofficial
Contact Timings: 5:00 PM to 9:00 PM.

|LAW AUDIENCE JOURNAL|
|VOLUME 2|ISSUE 1|JAN 2020|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2018): 2.06|IMPACT FACTOR (2018): 2.527|

DISCLAIMER:

Law Audience Journal (ISSN (O): 2581-6705) and Its Editorial Board Members do not guarantee that the material published in it is 100 percent reliable. You can rely upon it at your own risk. But, however, the Journal and Its Editorial Board Members have taken the proper steps to provide the readers with relevant material. Proper footnotes & references have been given to avoid any copyright or plagiarism issue. Articles published in **Volume 2 & Issue1** are the original work of the authors.

Views or Opinions or Suggestions **(if any)**, expressed or published in the Journal are the personal point of views of the Author(s) or Contributor(s) and the Journal & Its Editorial Board Members are not liable for the same.

While every effort has been made to avoid any mistake or omission, this publication is published online on the condition and understanding that the publisher shall not be liable in any manner to any person by reason of any mistake or omission in this publication or for any action taken or omitted to be taken or advice rendered or accepted on the basis of this work.

All disputes subject to the exclusive jurisdiction of Courts, Tribunals and Forums at Himachal Pradesh only.

|LAW AUDIENCE JOURNAL|
|VOLUME 2|ISSUE 1|JAN 2020|ISSN (O): 2581-6705|
|INDEXED JOURNAL|IPI VALUE (2018): 2.06|IMPACT FACTOR (2018): 2.527|

"PERSONAL DATA PROTECTION LAWS: A NECESSITY FOR INDIA."

Authored By: Mr. Lokansh Alma, Hidayatullah National Law University, Co-Authored By: Ms. Brinda Singhania, Symbiosis Law College, Hyderabad
Email IDs: lokanshalma45@gmail.com, brindasinghania23@gmail.com,
Published At: www.lawaudience.com.

I. INTRODUCTION:

Changing generations involves changing trends which leads to changing ideas and technology. Gone are the days where people were not used to the virtual platforms. In the present information age with various upcoming projects and initiatives such as Digital India, Biometrical identification, more than 100 smart cities, online banking etc., invokes with itself an urgent need for having well framed legal procedures and regulations. Providing Constitutional safeguard and protection to personal data for security reasons is one of the biggest challenges, which requires outmost attention. Such regulation will promote the very principle of '***Right to Privacy***' of individual.

Data protection refers to policies and procedures seeking to minimise intrusion into the privacy of a private caused by collection and usage of their personal data. Different interpretations of the term 'liberty' can be drawn from the various definitions given by different jurists. John Stuart Mill in his essay, ***'On Liberty'*** (1859) stated that, one is amenable to society only when something of his concerns others. He is absolutely independent in matters merely concerning himself. The term privacy also connotes different meanings[1]. According to Tom Gaiety[2], 'right to privacy include intimacy and integrity of

[1] Journal of the Indian Law Institute Vol. 53, No. 4 (OCTOBER-DECEMBER 2011), pp. 663-677 (15 pages), published by: Indian Law Institute.
[2] Tom Gaiety, "Right to Privacy", 12 Harvard Civil Rights Civil Liberties Law Review 233.

personal identity'. Jude Cooley[3] defined it to be 'the right to be let alone without any kind of interference'. In the case, ***Peter Semayne v. Richard Gresham[4],*** Hon'ble Justice Coke has rightly pointed out that one's house is like a castle and fortress to oneself, he can defend against violence and injury for his repose.

Before the presentation of the Personal Data Protection Bill 2018 to the legislature of India, usage of personal data or information of citizens was regulated by the ***Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011,*** under Section 43A of the Information Technology Act, 2000[5]. This is a keystone development in the evolution of data protection law in India. Rule 2(1)(i) of Information Technology Rules, 2011, defines personal information as **"*any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a Body corporate, is capable of identifying such person*."** Personal data also includes password, medical records, biometric information, every kind of financial information and sexual identification[6].

With India moving towards digitization, a robust and efficient data protection law is the need of the hour. The Bill has been drafted with an intention to fill in the vacuum that existed in the current data protection regime, and to enhance individual rights by providing them full control over their personal data, while ensuring a high level of data protection.

One example of this is the biometric identification and verification system of Aadhaar that enables the government to ensure targeted delivery of State benefits, like LPG subsidies. The European Union has the General Data Protection Regulation, effective since May 25, 2018. It also addresses the transfer of personal data outside Europe and EEA (European RED LIGHT Area). The GDPR aims primarily to provide control to individuals over their personal data and to simplify the regulatory environment for international business by unifying the

[3] Thomas M Cooley, A Treatise on the Law of Torts (2nd ed. 1888).
[4] Peter Semayne v. Richard Gresham, 77 ER 194.
[5] http://meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf (Dec-13-2019, 2.45 PM).
[6] A Comparative analysis of Indian Privacy Law and the Asia- Pacific Economic Cooperation cross- border privacy rules, *David J. Kessler, Sue Ross and Elonnai Hickok*, National Law School of Indian Review, Vol. 26, No. 1 (2014), pp. 31- 61, Published by: *Student Advocate Committee.*

regulation within Europe. The GDPR in Europe gives 8 Rights to an individual securing his information and privacy. Switzerland is perhaps the simplest place to be for privacy. Article 13 of Swiss constitution guarantees citizens' their right to privacy and there are strict federal laws in situ to guard your data. The Federal Data Protection Act and the Data Protection Ordinance protect personal data and prohibit any processing of it unless authorized by the subjects or law. The current scenario of Data Protection Laws in India is at a very critical stage now; there is progressively explosion of cybercrimes on a global scale. India being the largest host of outsourced data processing in the world has high chances to become the epicentre of cybercrimes.

Digital Security in India is missing and the equivalent requires restoration with due legislative provisions along with suitable public and employee awareness. Indian organizations in the IT and Business Processing Outsourcing (BPO) sectors deal with and has a wide range of delicate and individual information of people all over the world, including their credit card details, money related data and even their medical history. There have been occasions of security breaks and information spillages in prominent Indian organizations.

The on-going episodes of information robberies in the Business Processing Outsourcing (BPO) business have raised worries about information security. While the Information Technology Act, 2000 (IT Act), contains arrangements with respect to digital and related IT laws in India and portrays the extent to which a party can access the information on a Personal Computer or Personal Computer framework, the arrangements of the IT Act don't really address the requirement for a stringent information assurance law that are being set up.

The prevalent framework does not illuminate as to when the provision of a privacy policy is applicable and when it is mandatory to provide notice for direct collection of information. After considering the landmark judgment given in ***Justice K.S Puttaswamy vs Union of India***[7]**,** which held that privacy is a constitutional right the MeitY formed a committee for making recommendations for a draft Bill on the protection of personal data. Thereafter there a much need of this bill in the framework of Indian information technology sector.

[7] Justice K.S Puttaswamy vs Union of India, W.P. (Civil) No. 494 of 2012.

II. EVOLUTION OF DATA PRIVACY CONCEPT IN INDIA:

Changing generations involves changing trends which leads to changing ideas and technology. This universal concept is very well pervasive in India. The roots of Right of Privacy can be traced down from the historical era of 800 to 950 CE. Hitopadesha[8], "beneficial Advice", deals with concepts which emphasises the need for protecting certain matters such as worship, sex and family from being disseminated to others. According to Upendra Baxi, national Jurist, 'privacy in ancient times was related to positive morality.[9] This evidence signifies that concept of privacy was very well established in ancient India. In the year 1986, many tech informants suggested the changes which would take place because of looming of information age. One of them mentioned that privacy, accuracy, property and accessibility will change drastically. No doubt the predictions so made were absolutely on track.[10]

II.I JUDICIAL PERSPECTIVE:

The Constitution of India does not envisage any rights relating to privacy. It is only through the Supreme Court's judgments that the very idea of privacy and data protection has been evolved in India. In the year 1954, the Supreme Court in the case of ***M.P. Sharma v. Satish Chandra***[11] and ***Kharak Singh v. State of Uttar Pradesh***[12]**,** held that Privacy is not a Fundamental right but violation of personal liberty cannot be entertained as it is covered under Article 21 of the Constitution of India, 1950. In the landmark case of ***Justice K.S. Puttaswamy v. Union of India***[13]**,** the issue raised was regarding the government's Aadhaar Scheme, according to which it was mandatory for those citizens who wants to avail various governmental benefits and schemes, that it violated the right of privacy of individuals. It was argued that Article 21 of the Constitution of India, 1950, includes liberty which can only be extended to limited rights of privacy. However, the court overruled the judgments passed in

[8] It is an Ancient Indian text consisting of fables just like Panchatantra. It was composed between 800 CE and 950 CE by Lord Narayana.
[9] https://www.lawteacher.net/free-law-essays/constitutional-law/evolution-of-the-right-to-privacy-constitutional-law-essay.php (Dec-22-2019, 12.40 PM).
[10] **Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems,** France Bélanger and Robert E. Crossler, Vol. 35, No. 4 (December 2011), pp. 1017-1041 (25 pages), Published by: Management Information Systems Research Center, University of Minnesota.
[11] M.P. Sharma v. Satish Chandra, AIR 1954 SCR 1077.
[12] Kharak Singh v. State of Uttar Pradesh, AIR 1964 (1) SCR 332.
[13] Justice K.S. Puttaswamy v. Union of India, W.P. (Civil) No. 494 of 2012.

the cases of ***M.P. Sharma v. Satish Chandra***[14] and ***Kharak Singh v. State of Uttar Pradesh***[15] and with one accord recognised that Article 21 of the Constitution of India, 1950 intrinsically guarantees Right to Privacy as a Fundamental Right. Right of Privacy has been defined by Indian Judiciary in many other cases, such as in ***Gobind v. State of Madhya Pradesh, R Rajagopal v State of Tamil Nadu, People's Union for Civil Liberties v Union of India and District Registrar and Collector, Hyderabad and another v. Canara Bank and another,*** the courts were of the view that right of privacy is a fundamental right envisaged in Indian Constitution. By this right of privacy was made an actionable claim.

The Supreme Court also made a distinction between mental privacy and physical privacy in the case of ***Selvi and Ors. v. State of Karnataka.***[16] The issue in this case was whether the provisions of Section 27 of the Indian Evidence Act, 1872[17] are in prohibition of Article 20(3) of The Constitution of India, 1950[18]. The court held that no individual can be forcibly subjected to any of the techniques such as the Narco analysis, polygraph examination and the Brain Electrical Aviation Profile (BEAP) as it violates Article 20(3) of the Constitution and causes unjustified intrusion into the mental privacy of an individual. The provisions of Section 27 of the India Evidence Act, 1872 are not in prohibition of Article 20(3) of the Constitution unless compulsion has been used in obtaining the information. However, having such a wide number of judicial decisions, still India finds the concept of data privacy and protection to be less focussed and up to the mark.

II.II LEGISLATURE PERSPECTIVE:

Several existing legislations in the country protect the right of privacy. With changing circumstances, these legislations have been moulded and amended continuously. There does not exist any common law for different sectors operating in the country, however, some sectors has its own legislations to regulate the privacy issues. Banking sector is governed by The Insurance Act, 1999, Section 29 of Credit Information Companies (Regulation) Act,

[14] Supra note 7.
[15] Supra note 8.
[16] Selvi and Ors. v. State of Karnataka, Criminal Appeal No. 1267 of 2004.
[17] Sec 27 of The Indian Evidence Act, 1872 states, "How much of the information received from accused may be proved.—Provided that, when any fact is deposed to as discovered in consequence of information received from a person accused of any offence, in the custody of a police officer, so much of such information, whether it amounts to a confession or not, as relates distinctly to the fact thereby discovered, may be proved."
[18] No person accused of any offence shall be compelled to be a witness against himself.

2005, Section 44 of Public Financial Institutions (Obligation as to Fidelity and Secrecy) Act, 1983, Payment and Settlement Systems Act, 2007, The Banking Regulation Act, 1949, Section 139A of the Income Tax Act, 1961, Foreign Contribution Regulation Act, 2010, RBI Guidelines, Fair Practice Code for Credit Card Operations, 2010, and Gopalkrishna Working Group report, 2011. These laws regulate the sharing of personal information with third parties without consent, stolen or lost banking cards, failure to provide adequate information to the person whose data is being used, and refusal to provide financial records of the clients, lacuna in security measures which leads to improper and illegal use of personal data of individuals.[19]

E-governance and Identity sector includes Section 2(c), 3(a), 10(3)(b), 10(5), 11(1), 12(1)(e), 13(1), 14 of The Passport Act, 1967, Section 146 of The Representation of Peoples Act, 1950, Section 205 of The Indian Penal Code, 1860, Section 11 of The Census Act, 1948, Section 14A of The Citizenship Act, 1955 and many other provisions of The Registration of Births and Deaths Act, 1969, The Collection of Statistics Act, 2008, The Unique Identification Bill, 2010 and The DNA Profiling Bill, 2007. Each of these legislation focuses on the privacy concerns related to identity including identity theft, impersonation, fraud and inaccurate or incomplete information in the database.

The Contract Act, 1872 and The Indian Consumer Act, 1986, provide protection to Consumers. Medical sector includes, Medical Council of India's Code of Ethics Regulations, 2002, Section 2.1 and 2.2(b) of The Epidemic Diseases Act, 1897, Section 13(1), 38 and 40 of Mental Health Act, 1987, The Persons with Disabilities Act, 1955, Pre-Natal Diagnostic Techniques Act, 1994, Regulation 4 and 5 of Medical Termination of Pregnancy Act, 1971 and Ethical Guidelines for Biomedical Research on Human Subjects, legislations and rules which aims to restrict the collection of information illegally and render protection to the privacy of patients.[20] The efforts of Legislature in India, coming up with all the above mentioned legislations and rules portray the need of having a complete protection mechanism for legal level protection of privacy of Individuals in India. The presence of different kinds of privacy protection provisions makes the situation chaotic, scattered, and inconsistent and

[19] https://cis-india.org/internet-governance/blog/privacy/privacy-banking (Dec-28-2019, 01.15 PM).
[20] https://cis-india.org/internet-governance/blog/privacy-in-healthcare-policy-guide (Dec-28-2019, 07.23PM).

ultimately results in failure. National privacy principles are required to be adhered by sectorial legislations for maintaining uniformity in proper redressal of the problem.

III. THE PERSONAL DATA PROTECTION BILL, 2019:

The right to privacy is a Fundamental right and it is necessary to provide protection to personal data of individuals, which would further upheld the essential facet of informational privacy. In this mushrooming era of digital economy, there is a necessity to create a collective culture that fosters a free and fair digital economy, respecting the individual's privacy and ensuring advancement, empowerment and innovation through digital governance. The Personal Data Protection Bill, 2019, protects the data from unauthorised and harmful processing, builds trust between people and entities processing personal data, ensures well organised and technical measures for data processing and establishes a Data Protection Authority of India for the said purposes. On December 11, 2019, the bill was introduced in the Lok Sabha by the Minister of Electronics and Information Technology (MeitY), Mr. Ravi Shankar Prasad.

III.I DRIFT FROM THE PROVISIONS OF 2018 BILL:

"The data protection bill will be like new shoe, tight in the beginning but comfortable eventually", quoted by Hon'ble Justice B.N. Krishnan. The Committee, chaired by Justice Srikrishna, was constituted by the Ministry of electronics & Information Technology to draft the Personal Data Protection Bill. The Bill has been generally supported the framework and principles of the General Data Protection Regulation (the "GDPR") recently notified within the European union also as the National Privacy Principles printed within the Justice A.P. Shah Committee Report[21]. The Bill is additionally supported the inspiration of the landmark judgement of the Apex Court: ***Justice K.S. Puttaswamy (Retd.) & Anr v Union of India & Ors.***[22] Whereby the Supreme Court of India upheld the right to privacy as a basic right underneath the Indian Constitution. The Bill has come in replacing of Section 43A of the information Technology, 2000 and therefore the information Technology (Reasonable Security Practices and Procedures and Sensitive Personal data or Information) Rules, 2011

[21] http://planningcommission.gov.in/reports/genrep/rep_privacy.pdf (Dec-27-2019, 10.49 PM).
[22] Justice K.S. Puttaswamy (Retd.) & Anr v Union of India & Ors, W.P. (Civil) No. 494 of 2012.

that was enacted underneath Section 43A of the IT Act. The Bill seeks to guard the autonomy of people with regard to their personal data, specify norms process by entities victimisation personal data, and started a regulative body to superintend processing activities. The Personal Data Protection Bill 2019 is the second draft version of the 2018 bill that aims to be a lot of focus on consent of individual. The bill may be a modified version of 2018 that brings forth many new provisions at intervals its range. However, the bottom of the bill remains an equivalent including some minute changes. Provision of localisation has been lewd which suggests that no copy of information needs to be kept in India before transferring it outside the Indian Territory. These points towards a compromise that government is aiming to hold the advantage of corporations and companies and maintain bigger consensus.

The bill brings out a better degree of safeguards than the previous bill. Government order is needed to exempt any agency of government from application of the Act within the interest of sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order or for preventing incitement to the commission of any cognoscible offence. Social media verification is created no obligatory that is an innocuous move, leaving no space for obligatory Aadhaar linkage. This voluntary user verification mechanism for users in India is somewhat similar to the blue tick present on the profiles of celebrities on social media like twitter.

III.II HIGHLIGHTS OF THE BILL:

The draft bill defines "Data" as means and 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 or artificial intelligence[23]. The bill judiciously divides data into two categories: (a) Personal Data and (b) Sensitive Personal Data. A ***"Personal Data"*** means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information[24]. ***"Personal Data breach"*** means any unauthorised or accidental disclosure, acquisition, sharing, use, and alteration, and destruction, loss of

[23] Section 3(11) of Personal Data Protection Bill, 2019.
[24] Section 3(28) of Personal Data Protection Bill, 2019.

access to, of personal data that compromises the confidentiality, integrity or availability of personal data to a data principal.[25] The Bill defines sensitive personal data to include personal data revealing or relating to password, financial data, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe or any other data categorised as sensitive personal data under Section 15[26] of the Act. Earlier Religion and Political Belief were not considered under the aspect of Sensitive Personal Data, but now under this bill it has been included under this head.[27] The Bill administers the handling of individual information by (I) both government and private elements consolidated in India, and (II) entities incorporated overseas. The bill also seems to have an extra territorial jurisdiction which implies that it covers both the public and private sectors within and outside the territory of India, processing any kind of personal data obtained from India.

Chapter V of the bill defines the rights of a Data Principal[28], which includes (I) right to obtain the information from the data fiduciary regarding the processing of data[29], (II) right to correction and erasure of inaccurate, incomplete, or out-of-date personal data[30], (III) right to data portability, which covers the right to receive data in a structured, commonly used and machine readable format and right to transfer personal data to any other data fiduciary in certain circumstances[31], (IV) right to be forgotten can be exercised by the data principal if it is no longer necessary or consent has been withdrawn.[32] The bill defines ***"Data fiduciary"*** as any person, including the State, a company, any juristic entity or any individual who alone or in conjunction with others determines the purpose and means of processing of personal data[33]. Section 4 to Section 11 of Chapter II of Personal Data Protection Bill, 2019, describes

[25] Section 3(29) of Personal Data Protection Bill, 2019.
[26] Section 15 of Personal Data Protection Bill, 2019, deals with the Categorisation of personal data as sensitive personal data, which includes the risk of significant harm that may be caused to the data principal by the processing of such category of data; expectation of confidentiality attached to such category of data; whether a significantly discernible class of data principals may suffer significant harm from processing of such category of personal data; and the adequacy of protection afforded by ordinary provisions applicable to personal data.
[27] Section 3(36) of Personal Data Protection Bill, 2019.
[28] Section 3(14) of Personal Data Protection Bill, 2019, defines data principal as the natural person to whom the personal data relates.
[29] Section 17 of Personal Data Protection Bill, 2019.
[30] Section 18 of Personal Data Protection Bill, 2019.
[31] Section 19 of Personal Data Protection Bill, 2019.
[32] Section 20 of Personal Data Protection Bill, 2019.
[33] Section 3(13) of Personal Data Protection Bill, 2019.

the obligations of Data Fiduciary. According to which person processing personal data must do it for specific, clear and lawful purpose; he must do it in a fair and reasonable manner and ensure the privacy of the data principal, sufficing all the limitations imposed by the Act. The data fiduciary shall also take necessary steps to ensure that the personal data processed is complete, accurate, not misleading and updated, having regard to the purpose for which it is processed.

Under the Justice B. N. SriKrishna Report, an exemption has been made depending on the standard of territoriality. The Report states that any entity situated in India processing individual information of remote nationals not present in India might be excluded from the application of the Bill by the Central Government. However, this exception has not been brought out in the Bill. And if no such exemption is provided under the rules, the scope and applicability of the Bill may become over-reaching than the General Data Protection Regulation. Central government and its agencies are exempted from the provisions of the bill if they act in the interest of security of the state, public order, sovereignty and integrity of India.[34] ***"Data processor"*** according to this bill means any person, including the State, a company, any juristic entity or any individual who processes personal data on behalf of a data fiduciary, but does not include an employee of the data fiduciary[35]. Data can be processed only with consent however; chapter III of the bill defines grounds for processing data even without obtaining consent. Chapter XIII of the bill deals with the Offences, which includes (I) any person re- identifying or processes any de- identified data without the consent of data fiduciary or data processor is liable for imprisonment not exceeding three years or with fine of two lakh rupees or both, (II) offences committed by company, (III) offences committed by state where the offence was committed without knowledge and diligence of such person.

III.III ADVANTAGES OFFERED BY THE PERSONAL DATA PROTECTION BILL, 2019:

The bill seeks to shield the autonomy of individuals with respect to their data, specify norms relating to information processing by various entities, the usage of non- public data, and set up a regulatory body to oversee information processing activities. The draft bill calls out the data protection obligations, with truthful and practical processing which is considered as the

[34] Chapter VIII of Personal Data Protection Bill, 2019.
[35] Section 3(15) of Personal Data Protection Bill, 2019.

core principle of the bill. The new privacy bill seems to be a multi- dimensional move, as it brings almost all the sectors whether it is banking, insurance, any corporate information or individual sexual orientation, to abide by the tenets of the data security and protection principles. Unlike past scenarios, where only bank and insurance laws had confidentiality clauses. The bill also intends to secure the economic sector of the country by strengthening the legal framework related to data privacy.

N.S. Nappinai, a Supreme Court lawyer and a cyber-law expert said, "The revised draft now circulated is actually much tighter than the 2018 version. With respect to the crisper language and draftsmanship, the 2019 draft scores". Indus law View also welcomes the bill and considers it to be a positive move towards building a strong data protection framework in India.

The bill sets out obligations for protecting data which includes:

- ***Data Mirroring:*** the data mirroring requirement for personal information has been eliminated and constrained to Sensitive Personal Data ('SPD'). Thus, a copy of information like religious, biometric, medical, monetary facts and the like will need to be saved in India. The ambiguous requirement of a 'serving' replica as underneath the 2018 Bill has been removed.
- ***Cross-Border Data Transfer:*** When transferring Sensitive Personal Data outside India, say if the business enterprise is a multinational group requiring such transfers or a place overseas cloud carrier provider is used, then two necessities ought to be fulfilled. First, the specific consent of the data principal is required and second, a cross-border information transfer measure should be in place, such as an adequacy decision or approved contract or intra-group scheme. The requirement for cross-border data transfers for personal information has been eliminated completely. While this is an advantageous step for agencies with one less compliance measure for data transfers.
- ***Redefined Consent Provisions:*** Under the Indian law, most processing will be consent-based. Exemptions are present, in the form of the reasonable purposes exemption, compliance with laws, the employment functions exemption, etc. The flexibility however, as under the GDPR, is lost. The 2019 Bill now re- emphasizes

the significance given to consent, by way of structurally positioning consent alongside with the simple standards of processing.

- ***Optional certification of privacy:*** The 2018 Bill had brought the idea of a 'data trust score', to be awarded primarily based on a company's data safety practices and which have to be disclosed in the privacy policy. This will serve as a public benchmark for privacy. The 2019 Bill now states that concern to regulations, data fiduciaries 'may' have their privateness via design policies certified.
- ***Specific provisions on Social Media Intermediaries:*** The 2019 Bill additionally consists of certain provisions on Social Media Intermediaries ('SMIs'), for which extraordinary requirements are to be prescribed for classification as an extensive data fiduciary. It also specifies that SMIs categorised as such need to mandatorily provide customers with the choice to confirm themselves, and such verification should be made demonstrable and visible. The jurisdictional clause under the bill is very comprehensive and broad in nature as it includes both intra and extra- territorial clause. This clause makes the provisions more effective as it protects individual and entities present across the world. The bill has enhanced the power of the Indian courts, which can now, on the application of such provisions, prevent the illegal misuse of personal data and protect the right of privacy of individuals.

III.IV DISADVANTAGES OFFERED BY THE PERSONAL DATA PROTECTION BILL, 2019:

The second draft bill though is a modification of the 2018 bill, but still turns out to be a mess. The Bill had been tabled in Parliament by the Electronics and IT Minister on December 11 and has now been referred to a joint committee for solving all the glitches. Udbhav Tiwari, Mozilla's public policy advisor, opined that the new bill has clear provisions of privacy when it comes to companies but it lacks to cover the true implication of "blanket surveillance" by the government. Vrinda Bhandari, a lawyer, made a direct comment on the very foundation of the bill, by stating that the bill is in contradiction with the spirit of Puttaswamy Committee. Privacy may kill innovation, as the strict laws will prevent new companies and corporations to look and work according to the previously stored data and experience. Risk of establishment will increase, which will drastically affect the developmental process within the country. Because of Lack of clarity several interpretations can be drawn from the bill which will enhance the current problems instead of solving it. As was opined by Akriti Gaur,

a senior fellow at Vidhi Centre for Legal Policy. And no doubt that this move will throw people and tech platforms into confusion. Kumar Deep Banarjee, the country manager of the Information Technology Industry (ITI) Council, said that, ***"the need of the hour is to have a regulation which is clyster clear and then based on such regulation only a definite law can be passed."*** The exemptions mentioned in the bill is very open ended and can lead to arbitrary practices by the State in the name of national security. It disappointingly gives extensive powers to the Government to dilute provisions of the bill for its agencies. ***"The exemptions granted in Section 35 of the bill completely drifts from the proposed law on privacy. It puts power in the hands of the central government and specifically makes it a party, judge and adjudicator of its own cause,"*** says Pavan Duggal, a cyber-law expert. Justice B.N. SriKrishna, who was behind the formation of the base of the bill, has raised certain concerns regarding its provisions. The committee chaired by him noted that dangers to privacy flow from state and non- state actors. Hence the exemptions laid down in the bill should be 'watertight', 'narrow' and must be used in 'limited circumstances'.

Recently, an Israeli company, which works for government businesses throughout the World, was found extracting information of some Indian journalists and rights activists using advanced technologies. Google too had alerted 12,000 users, which include 500 in India, involving "government-backed" phishing attempts towards them[36]. Therefore it may be drawn that the bill significantly deviates from the mechanism of checks and balances. The bill raises concerns regarding the constitution of the DPAI, authority rendered with power to make regulations. As all the members constituting the authority will be selected by a panel consisting of Government nominees and will only work in the interest of Government, who are themselves, are the major collectors and processors of data. The bill also overpowers the DPAI which lacks to provide the required transparency. Section 94 of the bill provides that the DPAI would by notifications make regulations, rules, safeguards for protection of privacy and restrictions on continuous or systematic collection of sensitive personal data, including even defining what is critical personal data. The power of defining what a critical personal data is on whims and caprice of the authority. This portrays the creation of a situation where misuse of personal data can be the ultimate result. The bill turns out to be neglecting towards

[36]https://www.thehindu.com/opinion/editorial/unfulfilled-promise-on-personal-data-protection-bill/article30323338.ece (Jan-01-2020, 07.10 PM).

its very objective of protecting personal data. The idea of privacy as was laid down in the Supreme Court judgment in ***Justice Puttaswamy v. Union of India*** is certainly missing in the current framework of the bill. From its very preamble it seeks to place the privacy interests of individuals on equal footing as those of corporations and the state. Here, by placing competing interests on an equal plane, two natural consequences visit the drafting choices within it. First, the principle of data protection to actualise the crucial right to privacy is no longer fulfilled as a principal intention but is conditioned from the very outset. Second, by putting competing goals which contradict each other, any balancing is clumsy, on account that no predominant goals are set. These effects in a muddy articulation that would finally ensure a weak data protection law.

Hence, on a broader read, the Data Protection Bill is now not a leaky oil barrel with massive exceptions, but it is a perfect one. It will refine, keep and then exchange the private information of Indians without their control; open for sale or open for appropriation to the interests of securitisation or revenue maximisation, with minimal degrees of protection.

IV. GENERAL DATA PROTECTION REGULATION, 2018:

GDPR stands for General Data Protection Regulation. It's the core of Europe's digital privacy legislation which had replaced the EU Directive 95/46/EC adopted by the European Parliament and Council on 24th Oct, 1995.[37] GDPR is a new set of rules designed to provide European Union citizens additional management over their personal information. It aims to change the regulatory settings for business so that each citizen and business within the European Economic Community can take pleasure in the digital economy. The provisions are consistent across all the 28 European Union member states, which mean that companies have to just meet one standard within the European Union. The GDPR replaces the European Union's Data Protection Directive, which went into effect in 1995. GDPR necessities apply to every member state of the European Union, planning to create a lot of consistent protection of client and private information across European Union nations.

[37] http://www.eugdpr.org/gdpr-faqs.html. (Dec-15-2019).

A number of the key privacy and information protection needs of the GDPR include:

- Requiring the consent of topics for information processing;
- Anonymizing accumulated information to guard privacy;
- Providing information breach notifications;
- Safely coping with the transfer of information throughout borders;
- Requiring certain agencies to appoint a data safety officer to oversee GDPR compliance.

The GDPR contains 11 chapters and 91 articles which have the greatest potential impact on security operations. Articles 17 and 18 of the GDPR provide data subjects more management over non-public information that is processed automatically. The end result is that information subjects may transfer their non-public information between carrier providers more effortlessly (also called the "right to portability"), and they may direct a controller to erase their non-public information under positive circumstances (also called the "right to erasure"). Articles 23 and 30 require companies to implement reasonable data protection measures to protect consumers' personal data and privacy against loss or exposure. Data breach notifications play a large position in the GDPR text. Article 31 specifies necessities for single information breaches: controllers should notify Supervising Authorities (SA)s of a personal record breach within seventy two hours of gaining knowledge of the breach and must provide precise important points of the breach such as the nature of it and the approximate number of data subjects affected. Article 32 requires statistics controllers to notify data subjects as shortly as viable of breaches when the breaches place their rights and freedoms at excessive risk. Article 35 requires that positive corporations appoint information protection officers. Specifically, any business enterprise that processes information revealing a subject's genetic data, health, racial or ethnic origin, spiritual beliefs, etc. need to designate a facts protection officer. Articles 36 and 37 outline the data protection officer position and its responsibilities in ensuring GDPR compliance as well as reporting to Supervisory Authorities and data subjects. The reforms are designed to replicate the world we're living in today, and brings legal guidelines and obligations - along with those around private data, privacy and consent - across Europe, up to pace for the internet-connected age. Fundamentally, nearly each and every aspect of our lives revolves around data. From social media companies, to banks, retailers, and governments nearly every provider we use includes

the collection and analysis of our private data. Your name, address, credit card number and many more are collected, analysed and, possibly most importantly, saved by the organisations. Lack of trust in how companies treat their personal information has led many consumers to take their own countermeasures.

According to the report of RSA Data Privacy & Security Report[38], for which RSA surveyed 7,500 consumers in France, Germany, Italy, the UK and the United States, 80% of the consumers said, 'lost banking and financial data is a top concern.' Lost security information (e.g., passwords) and identity information (e.g., passports or driving license) was cited as a concern by 76% of the respondents and 41% of the respondents said that they intentionally falsify data when signing up for services online. Security concerns, a wish to avoid unwanted marketing, or the risk of having their data resold were among their top concerns. Data breach happens inevitably. Information obtained are lost, stolen or otherwise flashed into the eyes of those people who were never intended to see it, which tends to use this information maliciously.

Under the provisions of GDPR, now not only do corporations have to make sure that private information is gathered legally and under strict conditions, but those who collect and manipulate it are obliged to defend it from misuse and exploitation, as properly as to recognize the rights of data principles or face penalties for not doing so. The GDPR additionally lets in Supervising Authorities to impose large fines than the Data Protection Directive; fines are decided based totally on the circumstances of the case and the SA may additionally pick whether to impose their corrective powers with or without fines. For corporations that fail to comply with established GDPR requirements, fines can also be up to 2% or 4% of the whole global annual turnover or €10m or €20m, whichever is greater[39]. One of the biggest scandals relating to violation of privacy rights is Facebook data privacy scandal. On March 16th, 2018, The New York Times and the Guardian reported that the political consulting and strategic communication firm Cambridge Analytica accessed

[38] https://www.rsa.com/content/dam/en/e-book/rsa-data-privacy-report.pdf (Dec-20- 2019, 03.16 PM).
[39]https://digitalguardian.com/blog/what-gdpr-general-data-protection-regulation-understanding-and-complying-gdpr-data-protection (Dec-28-2019, 10.55 PM).

personal data of about 87 million Facebook users[40]. This was possible only because of inadequate safeguards provided by the developers of Facebook against the company. Mark Zuckerberg, founder of Facebook explained that, ***"All the works undertaken by his team is done, meeting all the privacy commitments and privacy controls are well lined up with other financial controls guided by Sarbanes- Oxley legislation."***[41]

For such gross mistake Facebook was fined with $5 billion and the matter was settled. ***"The magnitude of the $5 billion civil penalty is unprecedented in global privacy enforcement, elaborating that such penalty is more than 200 times greater than the largest privacy penalty previously imposed in United States and 20 times greater than the largest fine imposed in Europe as per the General Data Protection Regulation",*** said FTC Chairman Joseph Simons.[42] Facebook has set certain new privacy obligations to ensure security, which includes conducting a full audit of any app with suspicious activity, restriction on developers' data access to prevent abuse and putting tool at the top of the news feed to revoke apps' permissions. The scandal has left Facebook with scares, which will probably take years and years to heal. Facebook shares are continuously dropping with the issue becoming messier every passing day. This is the direct result of the stringent laws prevailing in Europe relating to data privacy. The very evident of "location history" technology by Google has made the majority of works easier and handy. By this system it becomes easier for any person to track the location of another person or any place. But no technology comes up without any terms and conditions. In similar fashion this beautiful move is not free from its sharp prickles. This came into light when the BEUC[43] claimed that Google uses malafide practices to get users to enable the options of "Location History" and "Web and App Activity", without intimating anything happening like this to users. As per the stringent rules of GDPR, Google is liable to pay a fine of about $4 billion.[44] According to the acronym CNIL, French government agency, Google has breached certain provisions of GDPR which includes revealing its data collection

[40] https://thehackernews.com/2018/03/facebook-cambridge-analytica.html (Dec-23-2019, 10.49 PM).
[41] The Sarbanes- Oxley Act of 2002 or Public Company Accounting Reform and Investor Protection Act, is a federal law which was enacted by the 107th United States Congress to protect and control fraudulent financial practices taken by any Company.
[42]https://www.complianceweek.com/data-privacy/the-facebook-effect-price-of-privacy-violations-just-went-up/27462.article (Dec-20-19, 06.44 PM).
[43] The European Consumer Organisation (BEUC), https://www.beuc.eu/ (Dec-24-2019, 08.14PM).
[44]https://www.theverge.com/2018/11/27/18114111/google-location-tracking-gdpr-challenge-european-deceptive (Dec-24-2019, 08.23 PM).

policies easily available and also, lacking consent from users for ad personalization for YouTube, Google Maps etc. for this major violation of GDPR rules, Google was fined 50 million Euros by regulators.[45]

IV.I CHANGES BROUGHT BY GDPR IN EUROPEAN UNION:

The passing of GDPR has placed a stop to the non- stop struggle of organisations, by having an impression on data privacy and safety demand and by encouraging organisations to strengthen and enhance their cybersecurity measures, limiting the possibilities of any potential data breach. Cyber security breaches loom as an enormous threat to enterprises within the European Union, with 68 of huge companies within the Britain having encountered a cyber-attack, according to the Cyber Security Breaches Survey 2017[46].

Throughout the past year, attacks against corporations like Wonga[47] and Equifax[48] recommend that the implications of a data breach will be devastating to your brand equity, with client defection shooting through the roof and prices escalating for affected corporations. GDPR has brought with it a proof of loyalty or interest as a user that subscribes to associate degree organisation are one that has certified their activity with subscriptions.

Standardisation of data Protection: GDPR compliance is assessed by means that of information Protection Agencies from each nation, this makes it to have a standardisation without any demand to affect every country's separate data safety legislation[49].

With a possible fine of €20m or four-dimensional of global Annual Turnover as the price for non-compliance with the GDPR, the results of associate degree audit seems to be a daunting realisation of business closure. This way of creating groups to adjust to the principles is harsh and dominating.

[45]https://arstechnica.com/tech-policy/2019/01/google-fined-57m-after-france-finds-violations-of-new-eu-privacy-law/ (Dec-24-2019, 08.37 PM).
[46]https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf (Dec-28-2019, 10.41 PM).
[47]https://www.emarketer.com/Article/Wonga-Data-Breach-Puts-Customer-Loyalty-Risk/1015608 (Dec-28-2019, 10.42 PM).
[48]https://www.telegraph.co.uk/technology/2018/09/19/equifax-fined-500000-data-breach-15m-uk-customers/ (Dec-29-2019, 8:31 PM)
[49] https://www.timedatasecurity.com/blogs/the-positive-and-negative-implications-of-gdpr (Dec-19- 2019, 03.45 PM).

IV.II IMPACT OF GENERAL DATA PROTECTION REGULATION ON INDIA:

IV.II.I CHALLENGES BROUGHT BY GDRP IN INDIA:

a) After the implementation of the General Data Protection Regulation in European Union it not only impacted the European cyber sector but also laid challenges for other countries outside the European Union.

b) India's outsourcing industry, which is estimated to be worth over 150 billion USD, contributes almost 9.3% of the GDP[50]. The EU has been one of the substantial markets for the Indian outsourcing sector and India's highly vulnerable data protection laws make us less aggressive than different outsourcing markets in this space.

c) Another challenge faced is the largely inflexible, the GDPR reduces the extent to which groups can examine vulnerability and make choices when it comes to transferring data outside the European Union. Indian corporations would need to enforce enough safeguards, as required underneath the GDPR, in order to transfer private data outside the European Union, thereby additionally increasing compliance costs.

d) Article 3 (Territorial scope) of the GDPR makes it clear that the provisions will be ad rem regardless of whether or not or no longer the processing takes place in the EU. This means no enterprise for Indian businesses that do not comply with the GDPR or elevated compliance costs for those who do and the danger of massive penalties on failing to do so.

IV.II.II OPPORTUNITIES BROUGHT BY GDPR IN INDIA:

- Indian IT agencies serving the European Union market, are their second biggest after the US, would be needed to comply with the GDPR. However, on the contrary, seeing this as an additional burden in terms of compliance, Indian agencies should see it as an oversized industrial opportunity knocking at their doors. Over the years, India has become a technology hub equipped with deep experience and a proficient resource

[50] https://www.dsci.in/blogs/eu-gdpr-part-i/ (Dec-31-2019, 02.07 PM).

pool. The GDPR might be a chance for Indian firms to face out as leaders in providing privacy compliant services and solutions.

- The 'adequacy requirements' underneath the GDPR permits the European Commission to contemplate whether or not the legal framework well-known within the country to that the personal data is sought to be transferred affords adequate safety to data subjects in respect of privacy and protection of their information. In the abaft trends and also the Supreme Court finding, an information protection framework has been planned through the Srikrishna Committee. The Srikrishna Committee's planned draft information protection regulation has adopted concepts just like the right to access and correction, right to portability, right to be forgotten, however the extent of an individual's rights is confined in contrast with the European Union's law. The law conjointly mandates 'mirroring' of information, which needs a duplicate of an entity's personal data to be kept in a server or information centre in India.
- European Union's GDPR permits information controllers and processors to transfer information outside the European Union if they fulfil certain conditions. whereas GDPR prescribes a fine of up to EUR 20 million, or four-dimensional of the total international annual turnover just in case of an organization, for infringement of the law, the Srikrishna committee draft law prescribes each civil penalties and criminal offences. For the misuse of personal information, the draft law punishes non-compliant parties with a jail term of 3 years or a fine of Up to Rs. 2 lakh, or both.

V. CONCLUSION:

Data privacy is the connection between cumulative and promulgation of data technology. Every information has a standard confidentiality, which needs to be masked from the public. The simplest reason for the same is to prevent any kind of misuse and squander of the information of individuals. Now that the right to privacy has been recognised in the Constitution of India, it becomes essential for building a mechanism for a positive growth and build out. It is very difficult to prevent a data from spreading but if extreme steps are taken no further strenuous problems will follow and privacy laws can have it out most implication. India has been the house of various sectorial legislation like Information Technology Act, 2000 read with Information Technology (Reasonable Security Practice and

Procedure and Sensitive Personal Data or Information) Rules, 2011, Aadhaar Act, 2016, Indian Telegraph Act, 1885 and the Indian Wireless Telegraphy Act, 1933, The Citizenship Act, 1955, Medical Council of India's Code of Ethics Regulations, 2002, The Epidemic Diseases Act, 1897 etc. which, inter-alia, regulate data protection, storage of information and powers of Government to access personal data.

However, National privacy principles are required to be adhered by sectorial legislations for maintaining uniformity in proper redressal of the problem. The Supreme Court in this context has laid the foundation, by holding that the right to privacy is not merely a common law statutory right but an elevated fundamental right and that informational privacy is a facet of the 'Right to Privacy'. It is because of judicial activism that the right to privacy can come into the purview of Fundamental Rights.

The Bill has been broadly based on the report submitted by the Committee chaired by Justice SriKrishna and framework and principles of the GDPR, recently notified in the European Union as well as the National Privacy Principles outlined in the Justice A.P. Shah Committee Report.

The bill has a broader coverage which covers all the companies in and outside India that process data in connection with any activity within the territory in India. Companies are required to include a 'privacy by design' policy to specifically describe practices and all the technical advancements done to protect personal data to avoid harm to individuals. Though the bill marks the first step to protect individual's data in this era of technology.

However, this is not the end of the battle. While E.U. and many other developed nations has adopted stringent laws to curb data privacy and protection issues, Indian laws still remain unsatisfactory and unimplemented to the required level. Indian Judicial system should be that powerful and systematic so as to create a deterrent to all wrongful practices related to individual's privacy. To maintain its presence in simultaneously growing global technological areas, India needs to look forward to properly implement the legislated laws.

VI. RECOMMENDATION:

- The need of classification of Critical Personal Data which is still not been included under the Personal Data Protection Bill, 2019. Having this category will ensure that certain kinds of data and its processing will be handled by the government only and with proper authority to maintain the secrecy and confidentiality of the owner of the data.
- Citizens do not own their own data accordingly there are no provisions in the Personal Data Protection Bill, 2019 that indicate upon any kind of right or ownership given to the citizens for their data. The data is out de facto and the government and other institutions can encroach upon it whenever they want once after having the data from citizens.

  To this problem there should be either a regulation pattern for ownership of data by the citizens themselves or to the institutions handling these kinds of data so that when there is any misuse of data or tampering of data profiles, it would provide an easier measure to dispense the matters with appropriate judgments.
- The Personal Data Protection Bill, 2019 marks identified difference between the private and the Government body and creates certain exceptions towards government bodies and schemes which can process the personal data of the citizens on their need and will. The bill should give equal footing to the data fiduciary to process the data of the principal with compliance to the provisions of the bill. The bill covers the private cyber markets and industries but has not addressed solution to situation where the institution of the government is itself involved towards the handling of data. Taking the situation of phone tapping by the police officials.
- In this digital age and with India participating in the global market, it has become a surveillance state. Monitoring, Snooping and Surveillance which are becoming a silent threat not only in India but also worldwide should also be considered while handling its processing and transmission. There has been no analysis on the aspects of cyber-attacks and cyber encryptography for money laundering and other data breaches, which turn out to be essential while formulating a data policy which will run and govern the data processing in India. The bill must be laid down with respect

to the report given by Justice B.N. Srikrishna and Judgment given in the case of Justice K.S. Puttaswamy v. Union of India.

- There must be an awareness drive undertaken by the Government and civil societies to make common public know about the crux of the bill, the concept of consent which is necessary for processing an individual's personal data and the authority they can rely on for data protection and surveillance, when they click online.
- Data Protection Authority so constituted must consist of members from different fields of expertise, to create diversity and bring forth different aspects for resolving any data breach. The members of DPA must consist of members of Judiciary and experts from the tech field along with members of the Cabinet.
- After encoding regulations for such a multi-dimensional concept of data privacy and its protection, the main challenge which follows is the proper implementation and proper applicability of the same. This requires our judicial system to be efficient enough to cope up with the emerging digitization and crimes related to it. The functioning of the courts must be that systematic and transparent that it creates a deterrent to all other wrongful practices related to individual's privacy and upheld the sanctity of the Constitution of India by protecting the right of privacy of individuals. Establishment of Specialized Cyber Infringement courts can turn out to be the most efficient way to resolve India's judicial backlogs.