ISSN (O): 2584-2196

INTERNATIONAL JOURNAL OF LEGAL AFFAIRS AND EXPLORATION

Volume 2| Issue 5

2024

Protection of Personal Data of Consumers in the ambit of The Constitution of India Post Puttaswamy Judgement

Shikha Kamboj

Assistant Professor, Faculty of Law, University of Delhi, Delhi

ABSTRACT

Nothing comes for free; one has to pay the price for goods or services either directly or indirectly. In recent years we have seen a sudden boom in many online markets and social networking platforms owing to epidemic covid-19. The companies are on the spree of using or selling it for research and other purposes. The sharing of data knowingly and unknowingly by users or consumers is threat to privacy in many ways. Artificial Intelligence is grasping all what you say and what you do with your smart device and keep analysing the big data perceived tirelessly. May be the purpose of analysing the data is purely to make new business strategies and improve the services of companies towards the end users. It is a matter of great concern that this poking in lives of people affects the decisions directly or indirectly. Beyond doubt all apps and websites requires permissions and few apps comes as an inbuilt feature in these devices. Once you download the app certain permissions are sought by the service provider, while accepting the privacy policy how many of users are giving attention to the terms and conditions of the privacy agreement. These standard agreements are generally read in haste and very few understands them owing to multiple reasons. 'Ignorantia juris non excusat' one you entered into the contract you are bound by the terms and conditions you agreed knowingly or unknowingly. Thus, it is the duty of the companies to let know the consumers the privacy policy and repercussion of accepting and breach of the privacy policy.

In India post Puttaswamy judgement the "right to privacy has been declared a fundamental right and thus the remedy to ensure privacy has been declared an elemental or fundamental right. and thus, data protection has fallen in the ambit of constitution of India. The recent judgement by the honorable Supreme Court has made a pathway for Data protection laws in India related to consumers and users to protect their interest in full throttle. There is a need to address and research on present laws on data protection and E consumers to facilitate the newly proposed law related to data protection and to suggest required changes in consumer protection law and to synergise all laws related to data protection of E- consumers to meet the challenges of transactional environment.

Key Words: *Data, Artificial Intelligence, Data Privacy, Informatics, Personal Data, E-consumer, Fundamental Right.*

1. INTRODUCTION

Commerce is vital for the growth of economy of any nation. The rise in E-commerce has also arisen the worries for safe data sharing and privacy of data. The privacy concerns are very essential to be addressed and countered timely otherwise the customers may stop doing online transactions fearing of data theft and online frauds[1].

The data shared by the consumers is used for analytics and strategy building for new business opportunities and upgrading the quality of services and increasing the business transaction[2].Privacy is a core for any e-business. The relationship of consumer and service provider depends on high trust values. The values and ethics cannot be compromised for long. In era of competition this relationship is very fragile[3].Consumers are very much concern about the data theft and thus hesitate in sharing the information and they do not appreciate sharing of data and analysing of data by artificial intelligence[4].The rise in machine-based services using artificial intelligence has been a reason of debate from last many decades, and the need for reasonable policy[5].Access to data about the consumers for data processing and doing analysis is unfair. The US Federal Trade Commission intervened in 2008 to stop CompuCredit from engaging in unfair trade practises, on the basis of personal choices made by customers the organisation had made a data and reduces the credit limit for those who were visiting pawn shops and other short term credit giving institutes[6]. The storage of big data and then deeply analysing it to draw conclusions without the knowledge of customers or users is illegal under various provisions of law and even data shared with third parties[7] is not allowed.

[1]Budak C, Goel S, Rao J, Zervas G (2016) Understanding emerging threats to online advertising, ACM Conference on Economics and Computation pp: 561-578.
[2]Lee I (2016) User Privacy Concerns for E-Commerce. IGI Global:Encyclopedia of E-Commerce Development, Implementation, and Management pp: 1780-1787.
[3]Ackerman MS (2004) Privacy in pervasive environments: next generation labeling protocols. Personal and Ubiquitous Computing 8: 430-439.
[4]Ackerman MS, Davis TD (2003) Privacy and security issues in e-commerce. New economy handbook pp: 911-930.
[5] See, e.g., Ryan Calo, Artificial Intelligence Policy: A Primer and Roadmap, https://ssrn.com/abstract=3015350.
[6] Ryan Singel, Credit Card Firm Cut Limits After Massage Parlor Visits, Feds Allege, Wired, 20 June 2008.
[7] See generally, World Bank, New Forms of Data Processing Beyond Credit Reporting: Consumer and Privacy Aspects, 2018; and Responsible Finance Forum, Opportunities and Risks in Digital Financial Services: Protecting Consumer Data and Privacy, 2017.

Data privacy is a burning issue in a growing digital economy like India. Data is an asset of the individual thus sharing, using, selling and disposing it in any way is not allowed and attracts penalty, though in India we do not have any specific law for data protection since the Data Protection Bill, 2019 is even now pending. The new guidelines recently introduced for e commerce are to be read in light of Data protection laws.

Consumer informatics, e-consumers, data privacy, artificial intelligence, jurisprudential aspects of right to privacy, and Right to intrinsic privacy and the fundamental right as a cardinal right.

2. A BROAD PERSPECTIVE OF ARTIFICIAL INTELLIGENCE, DATA PRIVACY, INFORMATICS AND E- CONSUMERS

2.1 *Artificial Intelligence*

When we talk about artificial intelligence are we talking about future? As stated by the European commission, "Artificial intelligence (AI) is already a part of our lives—it is not a figment of science fiction. From using an online personal assistant to organise and maintain our working day, to travelling in a self-driven vehicle, to our mobiles giving options for songs or restaurants that we might like, AI is a reality."[8]According to the UK House of Lords' recent AI assessment, "AI is a tool which is already deeply embedded in our lives."[9]Artificial intelligence has captured the attention worldwide.

Definition of Artificial Intelligence:

"Technologies with the ability to perform tasks that would otherwise require human intelligence, such as visual, perception, speech recognition and language translation"[10]

In other words, Artificial Intelligence can be defined as- "a set of executable programmes, which is capable of learning through various commands embedded in a software", companies often use this technology to harvest data from different online platforms like- "Google Analytics, automation platforms, CRMs, etc."[11]

[8]Communication from the Commission, Artificial Intelligence for Europe, COM (2018) 237 final, <http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=51625>.
[9]House of Lords Select Committee in Artificial Intelligence, AI in the UK: Ready, Willing and Able? HL Paper 100 (2018), <https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/100.pdf>. (Last visited on 07/07/2021)
[10]Ibid
[11] https://estio.training/industry-insights/data-analysis/data-analysis-artificial-intelligence/2020/31/ last visit on 9/07/2021

Looking into the achievements of companies using AI, the companies are vying from each other to perform best in the market with the help of artificial intelligence.

Many organisations and companies showed interest in AI and jostled to fill there need. The current status is that more than 53% companies have upgraded themselves to the AI to cater the need of customers.

Alibaba the giant of e-commerce doing business more than the total business done by amazon and e-bay. Alibaba is using artificial intelligence to interact with customers. A natural human like voice interacts with customer and most of the customer care services are driven by machines. Alibaba is also contributing to make smart automated cities in China with the help of artificial intelligence[12]

Alphabet is working on fully automated automobile services. This parent company of google is working on voice calls through artificial intelligence and many more services without any human interventions.

Amazon is gaining popularity amongst consumers by catering the day to day needs and other products. The moment you log in to the website you get suggestions for your purchase and not only this you also get offers on the products you might be thinking to purchase all this is backend job of AI.

Facebook and Microsoft are also using artificial intelligence to cater the need of its users and to facilitate its customers in the best way they can. Deep face recognition in Facebook and automatic grammar check and other automated features in Microsoft software.

Therefore, at present artificial intelligence has penetrated in our day-to-day life and hardly anyone is left who might have remain untouched by the AI.

2.2 *Data Privacy*

Privacy embraces a broad range of belief. The concerns on loosing personal data are loss to "individuality, autonomy, integrity and dignity,"[13]that are part of a larger set of beliefs about personal and social freedom of space. Piercing in the privacy of an individual by analysing the data and knowing the preferences and developing of software which can hijack the future thought process too of an individual.

[12] Ibid
[13] Lee A Bygrave, Data Protection Law: Approaching Its Rationale, Logic and Limits 128-129

Data privacy is also important to keep the trust alive amongst the consumers and companies. The efforts to secure data gathered by the companies is viable and necessary steps to be initiated to have control on it. If the tripartite agreement is there and the data is shared to a third party, then it is mandate to understand the repercussions resulting due to breach of privacy policy.

2.3 *Information*

"Informatics"[14] Is the discipline of information; it is the analysis of the behaviour and composition of any set up that generates, reserves, processes, and ultimately reflects knowledge, processes, and ultimately shows information. The subject considers the interplay between information network and users and additionally the design of interfaces among both, for example the user interface **E-Consumers and The Paradigm in Consumer Behaviour**

Indian consumers are undergoing a shift in behavior driven by ease of use, privacy, trust and other technographic factors. A critical situation is changing the human behaviour towards different directions. The COVID-19 pandemic has shifted consumer behaviour to a large extent, and various steps were adopted to restrict the spread of disease, including absolute and later, partial lockdown. Buyers are the driving force of market competitiveness, economic integration and growth in retail. Consumers are altering their behaviour in consequence to economic uncertainty, yet what part of the change encountered during the calamity will last, poses a major question.

Many of the strata of population is still having the fear and risk for usage of digital or e-commerce platforms as per the study done by EY during pandemic. It is interesting to note that instead of having various benefits of the digital/ e-commerce platforms; low adoption is the reluctance among consumers because of the privacy and trust factors of the consumers.

It was observed that the role of experience was measured in the drivers of more familiar mobile shopping usages. The value of reassurance concerning financial and privacy concerns, as well as the enhancement of hedonic and emotional rewards.[15]

The outlook towards information and knowledge sharing includes mobile phone privacy dilemmas and confidence in the mobile platform and research provides contributions towards estimating

[14] https://www.techopedia.com/definition/30332/informatics
[15] GwarlanndeKerviler a,n, Nathalie T.M. Demoulin b, PietroZidda c (2016): Adoption ofin-storemobile payment: Are perceived risk and convenience theonly drivers?,Elsevier.

individuals' genuine information security procedures, validating the connection between behavioural intents and traversing through antecedents to TPB-derived constructs[16].

Jun lui's findings from 2018 shed light on aspects that can be targeted to improve people's protective activities in terms of limiting the quantity of digital information they share via their smartphone.[17]

3. PRIVACY POLICY

3.1 **Privacy Agreement**

Today we see the countries are moving ahead towards the digital economy, almost all countries of the world are in favour of digitalisation. The cross-border commerce is no more tiring and time consuming. The distance of thousands, lacs of miles can be covered in few seconds by using e-commerce. The digitalisation has accommodated almost all in one and the other way. The barriers in commerce are removed by switching the offline business mode to online business mode. Thus,it is not a matter of debate that why e-commerce is gaining popularity in India and overseas amongst all classes of society.

Now it is very important to mention here that once you log in to the websites or in apps you are asked to give access to various other things on your device, other than this you are asked to give general information and if you enter into the transactions then you also give your critical and sensitive information to complete the transaction. It is the obligation of the service provider to keep this data secured as per the rules framed. The privacy agreement is accepted from both the sides. This privacy agreement is very crucial and vital. The shared information builds a big data for the companies and this big data is asset of the individuals who shared it while interfacing with the service providers. The privacy policy has to be framed following the guidelines of the Information technology Act, 2000. In year 2011, the Ministry of Communication and Information Technology (MCIT), Government of India, notified "the IT (reasonable security practices and procedures and sensitive personal data or information) Rules 2011". These provisions have come as a saviour to the end users and the companies are bound to follow the rules framed for protecting personal data and they are also responsible for providing security to the big data received by the companies.

[16] France Belangera, Robert E. Crosslerb (2019), Dealing with Digital Traces: Understandingprotective behaviors on mobile devices, Elsevier.
[17] Jun Liu, Robert J. Kauffman, Dan Ma (2015), Competition, cooperation, and regulation: Understanding the evolution of the mobile payment technology ecosystem ElectronicCommerce Research and Applications.

3.2 **Visibility and Percipience Issues**

The terms and conditions of privacy policy should be clearly mentioned and should be written in the language to be easily understand by the end users. The only challenge is how much consumers/users are vigilant to check the terms and conditions. The consent to the privacy policy is to be given after understanding the policy conditions. The moment you click on accept, you accept the policy and later you cannot blame the companies. Lack of awareness is the key factor for the issues raised in later stage with regard to use of data.

3.3 **Breach of Privacy Agreement and Repercussion of Non-Observance of Unison**

What if the privacy policy is breached and what will be the consequences of such breach? In India section 43 A and 72 of IT Act, 2000 talks about the consequences of breach. After Puttaswamy judgement passed in 2017, right to privacy has become a fundamental right and the individual can seek protection under the ambit of constitution of India. We shall be discussing on this a little more in article under the head of right to securing privacy an elemental right under Part III of the Indian Constitution.

4. ROLE OF INTERMEDIARY AND CONTROL OVERDATA SHARED BY THE USERS

Along with the rapid development of e-consumerism, the role of intermediaries such as: Amazon, Flipkart, Zomato, Big-basket, etc. is getting sophisticated. These intermediaries are representing themselves as a platform that is only responsible for providing the product of sellers to e-consumers, but it is a well-known fact that they are using the e-consumers' data for their so called "behavioural analysis" and they claim that the consumer's data will be safe at their end.

Because of their technical supremacy, it is obvious to a non-technical user to believe the security mechanism of these intermediaries an as a result the data on the servers of these intermediaries are increasing enormously. According to "Politico"[18], "As the internet retailer expands into other parts of our lives, Amazon is building a data empire. Company's efforts to protect the user's data are insufficient, and there are some flaws in the company's security which is capable to expose customers' data to potential breaches, theft, and exploitation."[19]

[18] A global nonpartisan politics and policy news organization
[19] Vincent Manancourt, "Millions of people's data is at risk- Amazon insiders sound alarm over security", Politico, 24/02/2021, available at https://www.politico.eu/article/data-at-risk-amazon-security-threat/ accessed on 08/07/2021

Here, the most noticeable thing is that intermediaries' claims that they do not store their users' data, meanwhile in their privacy policies they have a list of information that is to be shared by their consumers while using their service. For example, Amazon's website plainly states what data they collect from their customers: "contacts stored in customer's mobile, device configuration settings, name, address, payment details, and so on, the list is pretty long."[20]

Do intermediaries sell their customer's data? or they do not sell, it is a debatable topic. Intermediaries initially decline that they transmit their customer's data to any third party, but gradually in their privacy policy clause, they accept that they may share its customer's data with their affiliates[21], some intermediaries accept that customer's data is an asset for them and they may transfer it to the third party if they have sold their business or service to the third party.[22]

After analysing the above facts, it can be stated that these intermediaries have a vital role in transmitting e-consumers' data from one end to another end.

Do Intermediaries Have Any Control Over Data Shared by User with Them

In e-consumer market it is obligatory to the consumers to share their data with the intermediaries, otherwise they will be deprived of using online services of those intermediaries or e-commerce platforms.

The main concern is, "How safe is a consumer's data on an intermediary's server?" There have been numerous instances where consumer data has been hacked, and the government of India has taken no action because there is no data protection law in presentwhich can address this type of failure.

Some examples of data breach in year 2021 in India are given below:

- According to Raj Shekhar Rajaharia, about hundred million user's data was leaked and was available at the dark web for sale.[23]

[20]https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ#GUID-8966E75F-9B92-4A2B-BFD5967D57513A40__SECTION_87C837F9CCD84769B4AE2BEB14AF4F01, accessed on 08/07/2021.

[21] Flipkart Privacy Policy, para 5- sharing of personal information, available at https://cloud.flipkart.com/privacy, accessed on 08/07/2021.

[22]Does Amazon share your personal information, available at https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ#GUID-8966E75F-9B92-4A2B-BFD5-967D57513A40__SECTION_3DF674DAB5B7439FB2A9B4465BC3E0AC, accessed on 08/07/2021.

[23]Reethu Ravi, "Five Biggest Data Breaches That Hit India in 2021", available at https://www.jumpstartmag.com/five-biggest-data-breaches-that-hit-india-in-2021/, accessed on 08/07/2021.

- More than 2.5 million consumer's data of a stockbroking firm Upstox was leaked including KYC details.[24]
- According to CERT-in, Facebook and Twitter user's data got stolen[25]

In 2019, it was exposed that the employees of Amazon were listening to Alexa recordings and transcribe to improve the features,[26] this incident took place just after the incident of automatic activation malfunction in Amazon's Alexa device. Thus, it can be concluded that intermediaries do not have complete control over consumer's data shared to them.

5. RIGHT TO PRIVACY AND THE CONSTITUTION OF INDIA

The Journey from No right to a legal right and then finally in 2017 it was called a fundamental right was not smooth. After a lengthy and perplexing deliberation by erudite supreme court judges while considering the Puttaswamy[27] writ case, the right to ensure privacy was declared a basic and essential right. The notion of privacy has progressed far beyond the right to be bygone, to the acceptance of privacy of information as a crucial fundamental right. The debate that follows will provide a bird's eye view of the situation.

Judicial Developments on the Right to Privacy in India

In Puttaswamy judgement, the Supreme Court of India repudiated its former judgments of "*M.P. Sharma v. Satish Chandra* (*M.P. Sharma*)"[28]and "Kharak Singh v. State of Uttar Pradesh"[29],in which it was noted by the court that "right to privacy in not a part of the fundamental rights under Article 21."It reaffirmed Kharak Singh's precedents, which acknowledged the right to ensuring privacy derived from the Article 21 of the Part III of the Constitution of India.[30] In M.P. Sharma, the Supreme Court considered if the legitimacy of a search and seizure of official papers before FIR would be an invasion of one's right over their privacy. A constitutional bench of eight judges stated in a majority finding that "the right to privacy was not a fundamental right under the Constitution." Thereafter, in Kharak Singh, the question was if the routine police inspection

[24] Ibid.
[25] ET Bureau," 8 biggest data leaks of 2019 that hit Indian users hard", The Economic Times, 17/12/2019, available at https://economictimes.indiatimes.com/industry/tech/8-biggest-data-leaks-of-2019-that-hit-indian-users-hard/what-causes-data-breach/slideshow/72839190.cms, accessed on 08/07/2021.
[26] Laura M, "Does Amazon Sell Your Personal Information?", available at https://joindeleteme.com/blog/does-amazon-sell-your-personal-information/, accessed on 08/07/2021.
[27]K.S. Puttaswamy v. union of India (2015) 8 SCC 735
[28] M.P. Sharma v. Satish Chandra, (1954) SCR 107
[29]Kharak Singh v. State of Uttar Pradesh, (1964) 1 SCR 332.
[30] Gobind v. State of Madhya Pradesh, (1975) 2 SCC 148; R. Rajagopal v. State of Tamil Nadu, (1994) 6 SCC 632; People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.

constituted a violation of fundamental rights enshrined within the Indian Constitution. A constitutional bench of six judges investigated the legality of the Uttar Pradesh police regulations, which legalised hidden picketing, domiciliary visits at odd hours and systematic surveillance. The court annulled late-hour routine visits from police as it was an encroachment of "ordered liberty" .[31]In addition, the Supreme Court ruled that,"Article 21 of the Constitution of India is the archive of residuary personal rights and it took into consideration the common law of right to privacy." Nevertheless, the court pointed out that the right to privacy is not promised under Part III. It should be emphasised, however, that Justice Subba Rao, a discordant judge, stated that,"even though the right to privacy was not explicitly acknowledged as a fundamental right, it was an integral ingredient of personal liberty under the scope of Article 21 and thus cardinal."

In consequence to the viewpoint of Justice Subba Rao, the nine-judges bench of the Apex Court in Puttaswamy, acknowledged "the Right to privacy" as an integral component of the fundamental rights under Article 21 of the Constitution of India and reversed the forenamed judgements to this degree.[32]

It was observed that the Indian Constitution must mature over time to address the issues that arise in a democracy guided by rule of law, and that the essence of the Indian Constitution shall not be fixed on the interpretations that existed at the time it was formed. The right to privacy was Established as per both the rights provided for under Article 21 and 19 of the Indian Constitution, which encompassed both physical and mental freedom. Also, it was observed that "privacy facilitates freedom and is intrinsic to the exercise of liberty"[33]and instances of the rights entrenched in Articles 25, 26, and 28(3) of the Constitution of India were offered to demonstrate the workings of the rights pertaining to privacy were required to enjoy all of the above mentioned.[34] The stance of the Apex court in *Kharak Singh* and *A.K. Gopalan v. State of Madras*[35], that segregated the liberties under the purview of Part III of the Constitution Of India into individual compartments, were equally disregarded. Alternatively, it was decided that both rights overlap and that restricting one freedom has an impact on the other, as was previously decided in the Maneka Gandhi v. Union of India[36]and *Cooper* judgments. Here we can conclude that the

[31]Kharak Singh v. State of Uttar Pradesh, (1964) 1 SCR 332. Also discussed: Per S.A. Bobde, J. at paragraph 6; Per Chelameswar, J. at paragraph 9; Per D.Y. Chandrachud, J. at paragraph 27.
[32]Per S.A. Bobde, J. at paragraph 6; Per Chelameswar, J. at paragraph 9; Per D.Y. Chandrachud, J. at paragraph 27.
[33]Per D.Y. Chandrachud, J. at paragraph 169.
[34]Per S.A. Bobde, J. at paragraph 32.
[35]A.K. Gopalan v. State of Madras, AIR 1950 SC 27
[36]Maneka Gandhi v. Union of India, (1978) 1 SCC 248

reasonable standards of articles 19 and article 14 should be considered if there is any provision which curtails the right under article 21 of the Indian Constitution.[37]

The highest court recognised that "the concept of the right to privacy, as seen from jurisprudence in India and abroad has evolved from the basic right to be let alone, to a range of negative and positive rights. Thus, it now includes 'the right to abort a foetus; rights as to procreation, contraception, general family relationships, child rearing, education, data protection, etc."[38]The Court acknowledged that "informational privacy' is an important part of the Right to Privacy that can be asserted against both state and non-state actors."[39]

The right in respect to information and privacy permits a person to keep personal information bar from getting shared with others.[40] The Court also acknowledged that the protection privileges pertaining to privacy is not in toto and there can co-exist just limitations. To curb the state's disposition is such cases, the Court established a test: the act must be authorized by virtue of law, it must be mandatory to achieve a lawful goal of the state, the scope of the state's intervention shall be "proportionate to the need for such interference," and there must exist procedural screening to intercept the infringement of rights.[41] It was explicitly acknowledged that "protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefitsas certain legitimate aims of the State."[42]

6. COMPARATIVE ANALYSIS OF LAW RELATED TO DATA PROTECTION IN INDIA, UNITED STATES AND EUROPEAN UNION

The law related to data protection in India has not developed so far in comparison to the law related to data protection of E.U. and USA. Though the Data Protection bill, 2018 is on the table but it has not been enacted till date. The proposed bill is drafted keeping in view the present requirement of Global and Transactional economy.

A Bird eye view on law related to data protection in European Union and United States:

The right to privacy is a fundamental right in the European Union that aims to protect an individual's dignity. The rights appertaining to privacy and the right to safeguard of personal data

[37]Rustom Cavasji Cooper v. Union of India, (1970) 1 SCC 248.
[38]Per D.Y. Chandrachud, J. at paragraph 164; per S.A. Bobde at Paragraph 7.
[39] Ibid.
[40]Per D.Y. Chandrachud, J. at paragraph 165
[41]Per S.K. Kaul, J., paragraph 71.
[42]Ibid.

are acknowledged accordingly in Article 8 and 7 (E.U. Charter). The Data Protection Directive Was the primary major EU legal mechanism on data and its protection.

The Directive of Data Protection, which was heavily influenced by the OECD Guidelines, aimed to provide a uniform high degree of data protection across the European Union by harmonising data protection legislation to guarantee that data flow was not hampered. Eventually, EU Member States have adopted the Data Protection Directive as national legislation. It left considerable space for interpretation because it was a non-binding instrument. The rapidly evolving data landscape prompted the European Union to revise its data protection legal environment. The General Data Protection Regulation of the European Union (GDPR) of 2016 is the result of this procedure (EU GDPR). The GDPR is widely regarded as the strictest data privacy regulations in the world, and because it is a regulation, it will take effect instantly, throughout the workings of EU member states, allowed significant amendments which it proposes, member states have been allowed two years to orient their legislations as EU regulations.

As compared to the status of privacy in E.U., the privacy protection in US is fundamentally a "liberty protection" i.e., safeguard of the private expanse from state. As a result, the "right to be let alone" has come to reflect a desire for as minimal government interference as possible in American culture. While the US Constitution does not explicitly provide a protection of privacy, it is mirrored in the Fourth Amendment in a restricted form which can be stated as – "the right against unreasonable searches and seizures". However, by piecing together the modest privacy safeguards expressed in the US Constitution's First, Fourth, Fifth, and Fourteenth Amendments, US courts have inclusively acknowledged a right associated with privacy. Aside from the differences in privacy, the approach by US courts to data protection and privacy differs from that of the EU in a number of ways. To begin with, unlike the EU, the United States lacks a far-reaching set of rights/principles for ensuring privacy that govern the usage, collection and divulgence of data. Rather, there is just a small amount of industry-specific regulation.

Secondly, the public and private sectors take different approaches to data protection. The government's activities and powers in relation to information of a private nature are fully expounded upon and handled by wide expansive statutes such as the "Privacy Act, 1974", which is constructed as per the FIPPS (concerning gathering of information by the federal government); "the Electronic Communications Privacy Act, 1986"; "the Right to Financial Privacy Act, 1978", etc. For In the private sector, which is excluded from these statutes, specific sector-based norms persist. These shall cover: "The Federal Trade Commission Act (FTC Act)", "The Financial Services Modernization Act (Gramm-Leach-Bliley Act or the GLB Act)", "The Health Insurance

Portability and Accountability Act (HIPAA)", and "the Children's Online Privacy Protection Act (COPPA)", etc. Furthermore, in US, each state has its own data privacy legislation. In terms of private sector regulation, notice and consent are at the heart of data protection practise in the United States. The Federal Trade Commission (FTC) is a two-party federal institution obligated with protection of consumers and the promotion of competition. It is also responsible for consumer privacy enforcement. It achieves so by taking legal action against corporations that violate customer privacy, such as failing to follow advertised privacy rules and disclosing personal information without permission.

The FTC has termed notice the "most fundamental principle" and concentrated its entire efforts in privacy matters on encouraging various websites to publish privacy rules and holding websites accountable when they don't follow them. Furthermore, U.S. laws and directives tend to emphasise "notice and consent". For example, Title V of the Gramm–Leach–Bliley Act, 1999 (the GLB Act) has only three essential limitations on fining of "personal information" and alternatively emphasizes on substantive mandates, essentially, the requirement for organizations to "clearly and conspicuously" bestow consumers with intimation relating to its practices of disclosure and a choice to opt out of such divulgence. Another instance is the HIPAA guidelines governing the privacy of personal health information.

In the United States, data protection rules place a strong focus on notice and consent. As a result, there are two noticeable trends in the US approach for data protection: the first one is - Stringent regulations for the fining of personal data by the government and associated notices and the second one is - Optional approaches for data processing in private sectors. This divide may mostly be attributed to an individualism mentality of the markets in US, contrary to the culture in EU which rights-centric.

7. JURISPRUDENTIAL ASPECTS OF RIGHT TO PRIVACY

"Tyranny would be banished from the earth, could it but once be sufficiently known"[43]. Jeremy Bentham has advocated the protection of privacy long back and made a pathway for endless discussions on the right to privacy.

Privacy is often, equivocal because of the various historical conjectures of privacy hypothesized by several jurists. In a book by John Locke named-"Two treaties on civil govt", he ingrained the idea of ---- by propounding the theory of Natural Rights, which as per him were absolute and

[43] (Bentham 1983b, p.386 [IX.20.A12])1

inalienable. As per Locke, institution of a government and formulation of laws was but a secondary undertaking between persons, the primary and principal being safeguard of life, property and liberty. According to him individuals abandon a segment of their natural rights while foregoing the "state of nature" and the reminiscent natural rights such as that of liberty, life and property are kept unflawed with them. Accordingly, therefore, in pursuance of his theory in his work he he inaugurates the idea of 'Tabula Rasa' which establishes that the mind of a person was a supreme state and individuals were liberal enough to dictate their own soul. Individuals also possessive of the freedom to define the constituents of their character.[44]

Also known as the leading proponent of empiricism due to the substantial ministrations which he lays down in his "Essay". Only an insignificant part of it is replicated here. The text here is from *The Philosophical Works of John Locke*, edited by J. A. St. John, London, G. Bell and Sons, 1913. In the present essay, Locke argues on the status of intrinsic laws of the mind, of concepts in an overview and the consortium of ideas [45]

Once the civilization draws a contrast in the "outer" and the "inner" persona, between the entity of soul and existence of body, between the material and non-material, between the sanctified and secular, between Caesar's realm and that of God, between State and Church, between innate rights which are inalienable and rights that are based on discretion of government, between private and public, between seclusion and society, it becomes impractical to curve the idea of privacy by any name it may be called- the concept of "private space in which man may become and remain himself."[46]

8. CONCLUSION AND SUGGESTIONS

India is an emerging digital economy. This ongoing epidemic has taught a very important lesson for the survival of business. In present times when all sectors are moving towards digitalisation, people are left with no choice other than learning and doing online transactions may be for commerce or may be for personal consumption. The users can be broadly classified into educated

[44]https://psycnet.apa.org/record/2006-10213-008 (last visited on 9/07/2021)
[45] Ibid at page 2
[46] Herbert Marcuse, One Dimensional Man, 10 (1964); Milton R. Konvitz, Privacy and The Law: A Philosophical Prelude, 31 Law and Contemporary Problems 273 (19)

and not educated, aware and less aware, not aware about the privacy policy and consequences of breach of privacy policy. Thus, creating awareness amongst masses is the need of the hour. Since Puttaswamy judgement a fundamental element of the rights ensured to ascertain protection to life and personal liberty has become the responsibility of the state to protect it.

Though we have legislations wherein data protection can be done but to stand tall in global market. we need a statute which binds and gives flexibility to the multi nationals too without harming data of consumers or users. And we need to have legislation for the welfare of e-consumers and data protection. The present IT Act is not sufficing and not able to cater the need in global market. We have to compete in global market with the global players. India should not lack behind due to paucity of law. Flexible laws which are globally acceptable with an essence of welfare of consumers. Judiciary brought right to privacy under the purview of constitution of India and opened the doors for data protection bill in 2017. Now we have to work on synergising the laws related to data protection and law related to consumers and e-commerce. Recently, E-commerce rules, 2020 has been notified and we all are waiting for new Data Protection law. Data protection bill is the aspiration to combat with the reservations of IT Act, 2000. It's never too late to start and ratify.