DIGITAL PERSONAL DATA PROTECTION AND THE RIGHT TO PRIVACY

Anudeep Kaur* *Ph.D. Scholar, School of Law, Sharda University, Noida

Dr. Bhumika Sharma** **Assistant Professor(Law), School of Law, Sharda University, Noida

Abstract

The protection of personal data and information, particularly the right to privacy, is already facing significant disruptions in the realm of digital technology. Information that can be used to identify or contact a specific individual is known as personal data. Personal data is processed by businesses and government agencies for the delivery of services and facilities. Processing personal data makes it possible to understand people's preferences, which is helpful for developing directions and personalizing experiences. Individuals may suffer harm from it including financial loss, reputational damage, and profiling. Privacy and data protection are intertwined. The key principles on privacy and data protection are listed in the Information Technology (Amendment) Act, 2008. To secure materials of stored personal information and data protection, India does not have a distinct and comprehensive personal data protection law. The 2019 Personal Data Protection Bill is still being debated and has not become legislation.

Key words-

Digital technology, Personal data, Data protection, Data breach and Right to Privacy.

Introduction

Privacy is one of the most affected things in the world of digital technology. Dispute between the privacy and new technology have happened throughout the record. Concern over the growth of the mass media, such as newspapers, in the nineteenth century led to legal protection against abuse of the public's right to know specific facts and unauthorized use of names. Radio communications were restricted by rules against wiretapping from the 20th century, and they did not always keep up with the technological advancement of modern digital services. Data infringement seems to be new rule. They accommodate not only email accounts and passwords, but also other personal details. The data infringement reveals personal information of an individual, group or an organization that can be misused in many other different methods. Naming theft is one of the methods in which person is stealing anyone's personal information for monetary gain[1]. Digital Personal Data Protection should be prime concern for marketing and commerce, nevertheless the size of business and its geological locality. Data cluster is now an analytical ingredient for all type of commerce operations. In 21st century of cyber world with the continued growth of digital economy, data are a judgmental commercial boon. In spite of performance and seriousness of data safety still it is hard to

[1] J du Toit, "Protection Private Data Using Digital Rights Management"17(3) JOIW 64-77 (2018)

encourage the market to safeguard data on their own. In digital world, major drawback is that transactions do not know how to develop their intelligence on safety to line up with directions in computer and technology[2]. Personal data is controlled and prepared on a different scale. Countless unique details are being gathered by all kinds of public and private entities, frequently without the subjects' knowledge or consent. Personal data is information that is collected about an individual without that person's knowledge, and its usage has sparked concerns about the rights of individuals to privacy and protection.

The study of the right to privacy and the discussion of digital personal data protection may lead to improved digital personal data protection techniques. In the United States, General Data Protection considered one of the significant sections of legislation which got effected in 2018. GDPR lays out inflexible laws for personal data to be accessed safely without its misuse without the consent of individual or organization. It has also given the access their personal data so that anyone can correct their details and erased the data which is no more valid and required[3]. In the 1970s, data protection laws became enforceable. Germany passed the first privacy law in the world, and after that, other European countries followed suit, making data protection a priority for international organizations[4]. The Organization for Economic Co-operation and Development (OECD) has endorsed the UN's Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data. Though these guidelines were not mandatory infect these are in advisory form. They were helpful in placing the matters in front of national and international legislators. According to OECD guidelines, it describes personal data as information of individual which identifies the individual? Data Controller is a party who decides that which data to be collected and stored by which party. Trans border flows of personal data means where controller decides the national border of data[5]. Data Privacy Law especially regulates all or most phases in the filtering of specific kinds of data. All type of data doesn't fall under same scope. Regularly, data privacy law is focused mainly at protecting specific interests and right of individuals in their part as data fields- that is, when data about them is treated by others. Recently, it suggested that "personal data" itself is an energetic abstraction. With the growth of computers, more and more particulars can come down under the property of personal data and be concern to personal data safeguard regulations. The foundation on which the judgment is recognizable should be built still a point of dispute. The examination is whether the data theme must be recognizable to the regulator to establish personal data or whether it is important that some third party or regulator is able to link the data in examination to a genuine person. It is still unsettled, whether an Internet Protocol (IP) address is personal data but it has observed IP addresses as data concern to an identifiable person.

According to Data Privacy Law, personal data should be gathered through lawful process. It should be gathered for legal purpose and safeguarded from unofficial

[2]Kiersten E. Todt, "Data Privacy and Protection" 4(2) TCDR 39-46 (2019)

[3]European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council on General Data Protection Regulation" (2016) , available at: https:/eur-lex.europa.eu/eli/reg/2016/679/oj. (accessed on 3-4-2023)

[4]Andrews Wiebe and Nils Dietrich, Open Data Protection, 15 (Universitatsverlag Gottingen, 2017)

[5]OECD Library, "OECD Guidelines on the Protection of Privacy and Trans border Flows of Personal Data", (2002), available at: https://doi.org/10.1787/9789264196391-en. (accessed on 3-4-2023)

ventures to delete or make any kind of changes in it[6]. The most important tool for protecting human rights is the convention for the Protection of Human Rights and Fundamental Freedoms which says in its Article 8 about right to respect individual's private life[7]. According to the court's ruling in the case of Justice K.S. Puttaswamy and others v. Union of India and others, Article 21 of the Indian Constitution, which addresses the right to life and personal liberty, recognizes the right to privacy as a basic right. It plays a significant role in data protection and privacy violations by state or non-state organizations. In order to defend citizens' right to privacy in the digital era, the Supreme Court also ordered the government to enact a comprehensive data protection law. The government appointed a Committee of Experts on the order of Justice B.N. Sri Krishna to investigate various data protection-related concerns and recommend a draft Bill[8]. In September 2019, the Ministry of Electronics and Information Technology established an expert group to offer suggestions on the governance framework for non-personal data. Shri Kris Gopalakrishnan, a partner of Infosys, is its chairman. Even if it isn't specifically stated in the Constitution, Article 21 protects the human right to privacy as a fundamental freedom[9]. The EU General Protection data Regulation (GDPR) is a complete data protection law that controls the transforming of personal data of individuals in the European Union (EU). It was adopted in April 2016 by European government and affected on 25.05.2018. Actually, GDPR was earlier known as EU Data Protection Directive and all over EU member states accepted it as a legal framework for data protection[10]. Today's trouble about big data consider both the considerable rise in the amount of data being controlled and correlated changes, both genuine and future, in how they are used. Digital conversion of society raises concerns about privacy. Collection of personal data could be threat of life-logging. Information system are degraded in three main sections, hardware, software and communications with the motives to recognize and apply information security industry standards as instrument of protection and prevention at three measures : " Physical, private and institutional. The intention of computer security involves safeguarding of information and property from stealing, misconduct or circumstances beyond one's control, while permitting the information and property to carry on obtainable and productive to its intentional users. People are anxious about privacy; they are nervous that the digital systems they use on regular basis may bring undesirable consequences into their lives. In society, generally people are aware of that they can be stalked through their cells and their emails can be interrupted. Such worries are lawful: how the amalgamation of information and

[6]Lee A. Bygrave, Data Privacy Law An International Perspective 5 (Oxford University Press, 1stedn., 2014) available at: https://fdslive.oup.com/www.oup.com/academic/pdf/13/9780199675555_chapter1.pdf (accessed on 3-4-2023)

[7]Supra Note 4

[8]Justice K.S Puttaswamy and Anr. Vs. Union of India AIR 2017 SC 4161.

[9]Puneet Pathak and Ashwin Ghosh, "Right Based Approach To Data Protection: An Analysis Of Personal Data Protection Bill, 2019"AIL Journal 190 (2022)

[10]European Union, "Regulation (EU) 2016/679 of the European Parliament and of the Council on General Data Protection Regulation" (2016) , available at: https:/eur-lex.europa.eu/eli/reg/2016/679/oj (accessed on 3-4-2023).

communication technologies will soon permits uninterrupted surveillance of personal activities[11].

Big Data, Privacy Data and Data Protection

Big data means any pleased data and circumstantial data means which created or accessible automatically. Big data partition is frequently acknowledged as data refining with size and speed. Big data is spacious datasets gathered from various derivations so that it can be examined and investigate at high speed through technological sources. Privacy is a well-established right based on an individual's sensible assumptions, viably gained from the classical Rome. It is accepted as a basic civil right in numerous intercontinental acceptances. Their main interests are in personal space, not allowed interference of other person in their personal territory. To control their information held by others without their consent and knowledge. Looking for liberty from any kind of interference in their transmissions and monitoring privacy. Data Protection is proportionately almost new theory, mentioning to an individual's right to manage the cluster and use of data through which they can be recognized i.e. Personal data[12].

History and Impact of digital world and technology on personal data protection

Life without computer, internet, laptop and mobile phones is unintelligible. But in spite of profundity of their insight into our daily lives, the presence of these devices is very much sensational. The expansion of the internet and technical devices had a tremulous impact on our information in 1990s. The continuous growth of social networking along with the computerization of trading has an intense impression on the ways in which public talk and go about their commerce. In 1939, first computer was discovered and information system was developed in 1960s. In 1980s culture of personal computer came and 1990s internet was developed. These developments had given birth to collection of data in the form of information which was available easily on one click. Now in 2020, it is hard to imagine the world without technology and digital communication sources. We can collect anyone's information easily through internet without making knowing other person and without his consent. We can communicate with our friends by looking at the face book link. These websites allowing us to communicate with our friends and family members even if we are staying far from them. Now the question is how much control individual should have over their personal information and from others within society. Protection of information also known as access to information. Why it is necessary to defend privacy and promote information freedom? Every scientists, politicians and economists got occupied in searching the answer for the complex relation between access and privacy. An individuals and group of individuals both can protest for right to privacy which means they have right to keep their information private. With the remarkable streak of technology, especially communication devices regarding gathering and storing of information needs access on it. So that no one can misuse it[13].

---

[11]Sagir Ahmed Khan, "Digital evolution impact of information technology and information system on privacy of data management in digital domain an analytical approach" (2019) (Unpublished PhD thesis, OPJS University) available at: http://hdl.handle.net/10603/250793. (accessed on 3-4-2023)

[12]Brian A. Ho, "Personal Data Protection in the context of Big Data Technology", (2019) available at: https://www.academia.edu/42191657/Personal_Data_Protection_and_Big_Data_Technology?email_work_card=view-paper. (accessed on 3-4-2023).

[13]Lora Stefanick, Controlling knowledge, 3-4 (AU Press, Edminton, 2011) available at: sharda.refread.com/#/result Overview/45291521. (accessed on 3-4-2023).

India Legal framework for Personal Data Protection

Data Protection law-makers issues a legal framework for system creators and data keepers conscious to protect privacy rights in a progressively electronic to digital world. Appearing digital technology attending a new chance for personal data stores and gathers more information though law-makers are usually not renovated regularly adequate answer to the problems appearing from new technology. According to the European Commission (2012), personal data is any information that can be used to identify a customer based on his or her name, location, or other physical or social characteristics[14]. In current data protection codification and forthcoming regulation, ambivalence exists regarding the defense afforded by user rights and restriction placed on the depository and examination of personal data. The facilities offered in forthcoming legislation which rules the gathered and stored personal data which justifies expectant survey; because DP law makers donate outstandingly to the legal and social framework in which future expansion and formation occur. According to Article 12 of the 1948 Universal Declaration of Human Rights (UDHR), no one shall be the target of arbitrary intrusion into his or her private or public affairs, or of an assault on their honor or reputation. Everyone is entitled to legal protection from any type of intrusion into their private lives. Additionally, the UDHR has ratified the 1976 International Covenant on Civil and Political Rights (ICCPR). The UDHR and ICCPR are unquestionably binding on India. India has ratified both of the agreements[15].

Constitution of India

According to Article 21, no one may be deprived of their life or personal liberty unless doing so in accordance with a legal process. A citizen has a right to defend his or her own privacy as well as the privacy of his or her family and education, among other things. Without his permission, no information on the aforementioned proceedings may be published, whether it is positive or negative[16]. *Govind v.State of Madhya Pradesh*[17] Regarding the right to privacy, a significant decision called "Govind v. State of Madhya Pradesh" has been decided. Other names for the case include "Kharak Singh case" and "MP Sharma case." It consists of two distinct cases that the Indian Supreme Court jointly heard and determined. The Indian Supreme Court in this case considered the parameters and application of the Constitution's right to privacy. According to the Supreme Court's ruling, the Indian Constitution does not explicitly specify a right to privacy. Additionally, it was decided that police surveillance and home visits were not always a violation of someone's right to privacy as long as they were legal and supported by solid justification. Despite the fact that this ruling did not expressly recognize the right to privacy as a fundamental freedom in India, it served as a prelude to subsequent cases, such as the aforementioned Justice K.S. Puttaswamy v. Union of India, which led

[14]Brent Mittelstadt, " Personal Data Protection", (2013) available at: academia.edu/3749876/Personal-Data-Protection. (accessed on 3-4-2023)

[15]Aashit Shah and Nilesh Zacharias, "Right to Privacy and Data Protection", Nishith Desai Associates (2001)

[16]P.M Bakshi, Commentary on the Indian Constitution of India, 255 (Universal Law Publishing Co. Enlarged edn., 2014)

[17]AIR 1975 SC 1378: (1975)2 SCC 148: 1975 Cr Lj1111.

to the establishment of the right to privacy as a fundamental freedom under Article 21 of the Indian Constitution.

Rani Jethmalani v. Union of India[18] Individuals' right to privacy would be violated if the specifics of their bank accounts were disclosed without first establishing sufficient evidence to hold them responsible for wrongdoing[19]. *People's Union of Civil Liberties ... v. Union of India And Anr. on 18 December, 1996*[20] With the advancement of technology, the freedom to listen in on anyone's phone conversation is also a privacy issue. The right to privacy of its citizens must be protected against abuse by the current government, even though it is democratic to work for covert operations as a part of an intelligence group.

The Information Technology (Amendment) Act, 2008 The Information Technology Act and "data protection" have their own implications in reference to one another. The protection of cyber relationship matters is expressly mentioned in the Act 47's objectives. It offers defense against a few breaches involving information from computer systems. The aforementioned Act48 has provisions to stop the unauthorized use of computers, computer systems, and the data stored on them. There have been a number of provisions added that deal with "data protection." Data protection is clearly addressed in the new sections 72A and 43A of the Act[21]. The ITA was approved to furnish complete commanding surroundings for e-purchasing. In relationship with the right to privacy on the cyberspace, it is relevant to inspect Section 69 and Section 72 and Section 75 of the act. Sec 72 is only exhibit solution in the act attached with privacy and breach of its secretiveness. Sec 72 says that the person who so have right to ingress the data in form of information, he or she should not use that data for dishonest benefit without disclosing and its consent of the third party or without revealing to the concerned person. A responsibility of faith lies between the 'data collector' and 'data subject'. According to some critiques this act is not digital protection personal data legislation per se. It is not giving any specific section which can explain about any privacy principles. This act is actually effective for cyber offences, digital signatures and key infrastructure etc. Right now, there is no actual legislation for data protection and privacy issues. India has still insufficient legislation for data protection and privacy[22].

Personal Data Protection Bill, 2019

India's proposed Personal Data Protection Bill, 2019, aims to balance the collection of people' personal data by organizations, including the government. On December 11, 2019, the bill was introduced in the Lok Sabha, the lower chamber of the Indian parliament, where it is now being debated. The foremost intention of the bill is to supply individuals with significant control over their personal data, set up a data protection official to supervise and impose data protection regulations, and apply penalties for violations of the law. The legislation mandates that organizations obtain consent from

[18](2011) 8 SCC1

[19]Supra note 16

[20]AIR 1997 SC 568, JT 1997 available at:https://indiankanoon.org/doc/31276692/(accessed on 21.03.23)

[21]Jayanta Ghosh and Uday Shankar, "Privacy and Data Protection Laws in India: A Right- Based Analysis" BLR 72 (2016)

[22]Legal Advice, Breach of Privacy and confidentiality under information Technology Act,2000, available at: legalserviceindia.co/article/1288-Breach-of-confidentiality-html#: ~:text.(accessed on 21.03.23)

people before collecting, using, or disclosing their personal information. A small number of personal data types must only be gathered in India, according to the bill. Only a few exceptions ought to be allowed. The measure grants people the ability to alter their personal data anytime a legitimate need arises. A data protection officer must be appointed by a designated entity in order for the bill to be approved. The bill can force important sanctions on institutions for infringement of the law, including fines and detentions. The bill is anticipated to have a significant influence on the way personal data is processed and protected in India. Once passed, it will replace the current Information Technology Rules, 2011[23].

International Expansion

The EU legislature on data protection. It had taken some time for the EU to accept the irrevocable directives on data protection. The EU devices that were finally acquired have nevertheless been the almost enterprising, extensive and compound in the field. The Union now recognizes the right to data protection as being the fundamental law. Article 8 of the European charter says, "Everyone has the right to the shielding of personal data". Article 7 says, "The right to esteem for private life with hold to the refining of personal data."The EU's preparing and assumption of a directions on the protection of personal data took over five years. The Data Protection Directive institute for the first-time irrevocable regulations on data protection with which the Member countries of the EU must obey. Data protection directives put in only to those particulars which certified as personal data. The most critical inquiry in the assessment of observation with the personal data framework is whether applicable data licensed as personal data and whether data preservation regulations are relevant to the operating of the material data. The directions are relevant in every case of mechanical extracting of personal data. Mechanical extracting means the examination of data by using data extracting methods[24].

European Union's GDPR

The European Union (EU) unveiled the General Data Protection Regulation (GDPR) in May 2018. Therefore, its history may be traced back to the EU's pioneering data protection rules and guidelines. The Data Protection Directive, which agreed to a legal framework for protecting individuals' personal data, was ratified by the EU in 1995. The Directive recommended EU member states to execute national data protection laws that observed with its principles. However, there were important differences in the applications and administrations of these laws covering the EU, which guide to a deficiency of stability and intelligibility for commerce and individuals. The EU starts a procedure of improving its data protection laws. In order to reinstate the Data Protection Directive, the European Commission proposed a new data protection regulation in 2012. The suggested law was sketched to build up individuals' rights strongly, clarifying observance for commerce, and supply an additional compatible framework for data protection covering the EU. The GDPR was previously acquired by the EU in April 2016

[23]Personal Data Protection Bill, 2019, No. 373 of 2019, India, available at: https://prsindia.org/billtrack/the-personal-data-protection-bill-2019(accessed on 21.03.2023)

[24]Supra note. 4, Pp 20-22

and approached into result on May 25, 2018. The rules supplying a complete framework for safeguarding individuals' personal data, as well as regulations on how data should be possessed, pre-owned, and shared, as well as individuals' rights to attack and command their personal data. The GDPR has been authoritative in making data protection laws and rules throughout the society. Its theory has been embraced in other countries and zone, such as Brazil's General Data Protection Law and California's Consumer Privacy Act. The GDPR has also had a important influence on commerce that utilize in the EU or summons personal data of EU inhabitants, as they must obey with the fines and penalties[25].

United Nations

The UN convention on the protection of children and The United Nations (UN) have recognized the need of safeguarding personal information in the digital era and have called on certain businesses to support and uphold privacy rights. The UN has contributed to raising awareness about the value of protecting personal data and advocating for strong legislative frameworks to safeguard individuals' right to privacy. The significant actions done are: Universal Declaration of Human Rights (UDHR) was adopted in 1948. A provision for the preservation of privacy rights is included in the 1950 Convention for the preservation of Human Rights and Fundamental Freedoms. Guidelines about Digitalized Personal Data Files, which outlined guidelines for the gathering, utilization, and declaration of personal data, were acquired by the UN in 1980. In many nations, the recommendations have been considered authoritative in establishing data protection laws and policies. The Resolution on the Right to Privacy in the Digital Age was approved by the UN General Assembly in 2013[26]. *Digital privacy and human rights*: Digital automation does not survive in a hover. They can be a strong device for promoting human development and donate very much to the advancement and safeguarding of human rights. Nevertheless, data-thorough machinery, such as artificial intelligence execution, subscribe to create digital surroundings in which both States and commerce ventures are progressively talented to trail, analyse, consequences and even influence people's conduct to an unmatched standard. These computer progresses hold very important chance for human nobility, liberty and privacy and the movement of human rights in common, if registered without essential protection[27].

United States

The Privacy Act of 1974 safeguards the accounts grasped by US Government organizations and need them to try fundamental honest particulars implementation. Like the Indian Constitution, there is no direct right to privacy in the US Constitution. Nevertheless, US Courts have explained the right to privacy to be comprised in the US Constitution. The US has no complete privacy protection law for the private sector. A significant read taken in the US with regard to the defense of privacy on the Internet was

[25]European Commission (2018). General Data Protection Regulation (GDPR). available at: https (accessed on 23-03-23)

[26]Supra note 15, Pp -5

[27]United Nations. (n.d.)About digital privacy and human rights. available at:https://www.ohchr.org/en/privacy-in-the- digital-age. (accessed on 24.03.23)

the staging of Children's Online Privacy Protection Act. Accordingly, the principles, business internet sites and online resources to manage children under 13 or that consciously gather personal details from them must notify parents of their personal data application and acquired changeable parental agreement before gathering, sharing or disclosing personal data of children[28].

Internet privacy is one of the concerns among online users that are growing the fastest, according to Trust Arc. According to research, 45% of consumers are more concerned about their internet privacy than they were a year ago, and 68% of users are anxious about not knowing how their personal information is acquired online. Internet usage is growing quickly in upper-middle-income countries, virtually at a pace of 6% yearly, and up to 2% in low-income countries, according to Web Index. According to Pew Research, persons in lower socioeconomic brackets use many devices, while those in higher socioeconomic brackets use computers, tablets, smart phones, and high-speed broadband .With a score of 90.1, Norway exhibits the highest level of commitment to online privacy. Australia receives a score of 89.1, placing it in second position. Denmark comes in third with a score of 87.4, Sweden comes in fourth with a result of 85.2, and Finland comes in fifth with a score of 83.6 for internet privacy. China gained the fewest points with a result of 13. Second-place Uzbekistan received a score of 15.0. With a score of 68.6, the US sits in 18th position. As a result, Norway scored the highest overall in terms of Internet privacy, with 90.1 points. Despite having the greatest usage rate and the best internet speed. What does Norway do to achieve the top ratings for protecting digitally stored personal information is now the question? Norway has taken few steps to safeguard the internet privacy. Norway has among of the world's few strict laws governing internet privacy. Some of their laws provide protection for the privacy of their citizens. Norway also doesn't allow foreign organizations to "spy" on its citizens' data[29].

Conclusion and Suggestions

Digital personal data protection and the right to privacy are critical affair in today's electronic era. People have a right to regulate how their personal data is collected, used, and disclosed as well as a right to know what information about them is being gathered and how it will be used. Organizations must take precautions to secure and protect personal data from unauthorized access, use, and disclosure. The use of technology is expanding daily, so stronger data is needed to maintain this growing phenomena protective regime for preserving personal freedom. A general approach to data protection might be provided by the institutional status of data protection. The components of data protection, including data collection, processing, storage, security, and access, should function together as a legal framework to give it particular status as a right. The correct fundamental approach to data protection and privacy must become universally understood[30]. The protection of personal data, or informational privacy, is just as significant as the right to privacy. There is currently no law that offers an acceptable foundation for Indian citizens' data privacy. Following the Puttuswamy

[28]Supra note 15, Pp 6-7

[29]Best VPN.org, Internet Privacy Index (2023), available at: https://bestvpn.org/privacy-index/(Last updated on January 9th, 2023)

[30]Supra Note 22,Pp- 72

according to the Supreme Court's ruling, the right to privacy includes the privacy of one's information. Based on the recommendations of the Justice B.N. Sri Krishna committee, the Indian government drafted the Personal Data Protection Bill in response to the Supreme Court's directive. The Personal Data Protection Bill may establish a thorough framework for protecting personal data while enabling the Indian economy to gain from improvements in data processing. The Bill does contain several provisions, nevertheless, that may weaken an individual's right to privacy[31]. The GDPR rules and obligations may supply important directions for U.S. legislatures as they observe whether the U.S. should adopt similar legislation. But the particularity of the EU development and conditions should be endured in mind, as should the problems the EU labels as it enforces the directives[32]. Internet appeals needed private details from their customers for many causes. The applications required to give details and contribute resources customized for the user. Internet users don't know that their data is used in a safe and firm way or not. Many data breaks in data place used by other internet sites have appeared that personal data is in danger[33]. While taking care of international trade, India is badly in the need of strict rules regarding protection of digital personal data as many countries are interested to trade but because of unsafe data protection and issues of data privacy are stopping international traders to trade in India. Inadequate Privacy regulations is hurdle in the growth of commerce business of India. Another obstacle to promoting a secure environment for transmission in the online world is the concern of privacy. To accept the precise standards related to the offline and online handling of personal data, a special legislative framework is needed. Internet users must be made aware of the need of consent-based information exchange, and no data should be gathered without it. The future of India's trade depends on a stable balance between individual autonomy and secure business and transaction practices[34].

[31] Supra Note 9, Pp-199

[32] Peter H. Chase, "Perspective on the General Data Protection Regulation of the European Union" GMFOTUS 12-13(2019) available at: http://www.jstor.com/stable/resrep21227

[33] Supra note 1, Pp 75

[34] Supra note15, Pp 10