VOLUME 3 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

PRIVACY AND DATA PROTECTION IN INDIA

- Dr. Pradip Kumar Kashyap[1]

Abstract

Privacy is an idea that has been around since the beginning of human society. However, understanding Privacy may be challenging. There is no universally accepted definition of "Privacy" among scholars since the concept evolves with society. The debates about privacy and secrecy in the Constituent Assembly provide a window into its origins. Discussions in the Constituent Assembly reveal that the "Right to Privacy" was intentionally omitted from the Constitution. Who drove legislators to take this action? Post-independence, The Right to Privacy has evolved in India despite being unrecognized in the Constitution. It was initially recognized in the case of Kharak Singh. The "Indian Evidence Act," the "Information Technology Act," the "Indian Penal Code," "Criminal Law," the "Indian Telegraph Act," the "Indian Easement Act," and "Family Law" are all examples of laws that include provisions for Privacy. Different forms of Privacy, such as the right to be left alone or to maintain anonymity, have emerged throughout human history. Protecting this Right is crucial in the modern day because of the prevalence of digital media. The effect of social media on individuals' right to privacy in the Internet era has been the subject of some debate. In this article, I discuss the importance of data security and the several foundational regimes of data protection in India. All of the information comes from secondary sources.

Keywords: - Data, Privacy, Big Data, Rights, Protection

[1]Assistant Professor of Law, Teerthanker Mahaveer University, Moradabad

Introduction

The United Nations (UN) recognizes the right to privacy as a fundamental aspect of human rights. It takes much work to provide a succinct description of everything that falls under this protection. The idea of privacy may be seen from two different perspectives. Information or personal data, and the extent to which it is shared with other parties, is at the heart of this issue. Our understanding of privacy has been shaped by various factors, from the invention of reading and writing to the rise of bookkeeping, newspapers, and eventually the Internet as the dominant technology of the modern day. The widespread use of the Internet and the development of more efficient methods for storing and retrieving massive quantities of data have had far-reaching effects on how people see the concept of privacy in modern society. The current privacy debate focuses on the practices of third parties about the information they collect and store, including whether or not it is secured or preserved, who has access to it, and under what conditions they may do so.[2] The 'right to privacy' is a fundamental human right that is recognized in the Universal Declaration of Human Rights (UDHR), the International Covenant on Civil and Political Rights (ICCPR), the United Nations Convention on Migrant Workers, and the United Nations Convention on the Protection of the Child, as well as in many other international and regional treaties. Several international human rights agreements, conventions, and human rights courts3 explicitly include the right to privacy. In his first report, submitted to the UN on March 8, 2016, the UN Special Rapporteur mentioned the right to privacy. His study is predicated on two fundamental tenets: first, there must be access to privacy protections regardless of national boundaries, and second, there must also be access to remedies for breaches of privacy that occur across these borders. The Special Rapporteur has also established a ten-point action planto make implementing the Principles easier. The right to privacy is the bedrock upon which other rights and liberties, such as the freedoms of speech, association, and belief, are built. However, given that private information is frequently gathered and sold in the new economy, the right to privacy has emerged as an issue of critical importance in this era of big data. Researchers and analysts working with data are now attempting to recover privacy concerns and guarantee that any data obtained is kept safe. With big data analytics, 'communications monitoring' carried out by state

[2] Nandan Kamath, *Law Relating To Computers, Internet, And E-Commerce: A Guide To Cyber laws And The Information Technology Act, 2000* 121 (Kamal Law House, Calcutta,1st Ed. 2020)

and non-state actors, including commercial businesses, is rapidly becoming unavoidable and very aggressive. In today's world, the term "communications surveillance" refers to "the monitoring, intercepting, collecting, obtaining, analyzing, using, preserving, retaining, interfering with, accessing, or similar actions taken about information that includes, reflects, arises from, or is about a person's communications in the past, present, or future" (Necessary and Proportionate Coalition, 2014). Large data refers to not just the amount of data but also its velocity and the diversity of data items and sources. The term "big" refers to all of these aspects of big data. The government and commercial players gather, develop, and own these extensive databases they have generated. The majority of these enormous datasets are either picked by private technology businesses, managed by private stakeholders, or collected by the government for the government to be able to deliver welfare services. For instance, several government agencies in India, such as the Unique Identification Authority of India (UIDAI), the Census of India, the Stock Exchange, the Ministry of Rural Development for the Mahatma Gandhi National Rural Employment Guarantee (MGNREGA), and the Income Tax Department, all retain vast amounts of data. In addition, the Indian government maintains big data for additional initiatives, such as the Central Monitoring System, Human DNA Profiling, the Smart Cities Mission, and the Digital India program.[3] Big data analytics are being used to promote enterprises by various non-state players in addition to the government, such as online travel firms, online retail outlets, and telecom providers. There are some positive aspects of big data, and most big-data-oriented programs have a clearly laid out privacy policy. However, there needs to be a properly articulated access control mechanism and doubts over essential issues such as data ownership. This is because most projects involve public-private partnership, which involves private organizations collecting, processing, and retaining large amounts of data.[4]

Data security concerns in India

People often assert that data is the new oil. People's importance on data has skyrocketed in the past couple of decades, reaching new heights that were previously unimaginable thanks to the rapid rise of digitalization around the globe, including in India. The majority of cyber security

[3] Jason Asbury, Maria McClelland, Kris Torgerson, "India Vincent & Jennifer Boling, Law and Business Technology: Cyber Security & Data Privacy Update", 20 *Transactions: TENN. J. BUS. L*. 1065, 1067-71 (2019)
[4] Dhiraj R. Duraiswami, "Privacy and Data Protection in India", 6 *J.L. & CYBER WARFARE* 166, 169-172 (2017).

assaults that have occurred in India in recent years have intended to steal data as their primary target. There have been several occasions in which vital personal and sensitive data, such as medical records, financial records, and other types of data, have been compromised due to cyber-attacks. Recently, India needed stringent data protection laws to protect its citizens' sensitive and personal data adequately. As a result, numerous data breaches, such as hacking social media accounts, theft of credit and debit card details, and other privacy breaches went unreported. The lack of stringent data protection laws in India caused this. A surprising allegation was made in an investigation report that was published by The Tribune Newspaper in the year 2018, which claimed that the full Aadhar Database, which contains personally identifiable information of more than 1.3 billion Indians, could be accessed by paying a meager price of just 500 Indian Rupees. Think tanks and the international media have accurately termed the Aadhar data leak as the most significant data breach that has ever occurred anywhere in the world. In addition, according to a research released by a company specializing in digital security named Gem alto, India is responsible for more than 37 percent of all data breaches that occur worldwide, making it the second most vulnerable country behind the United States. The lack of a reliable data security framework in India has been brought to light by the multiple data breaches that have occurred in an economy that is becoming more data-driven. This research was undertaken to analyze the current and incoming data protection legislation in India while comparing it with the laws in advanced data protection regimes to identify the gaps in our data protection framework. The study was carried out to investigate the existing and upcoming data protection laws in India. The fact that India has such a large and diverse population is the most critical reason why the country should pay special attention to its data privacy legislation. Currently, India is by far the largest market in the digital economy. The country's number of Internet users now exceeds 500 million, which is increasing at a pace of over 8% per year. It may soon become a very urgent task to solve the challenges emerging out of voluminous transactions in the form of digital media, as the digital economy in India is heading towards an unprecedented boom11. The digital economy in India is going towards an unparalleled boom. Because of the influx of more advanced technologies and the aggressive posture taken by the government to promote digital transactions after demonetization, the use of data has become even more significant while simultaneously being more prone to misuse. In the recent past, India has also witnessed a fillip in the use of

digital space in the finance sector. The increasing popularity of online payment systems such as Google Pay, BHIM, Paytm, and many other start-ups that facilitate digital transactions is a testament to the fact that Indians have entered an age in which digital mediums have become an essential component of our lives.[5] As a result, there needs to be a robust and efficient system in place to provide adequate security to digital transactions. Because high-speed Internet access is becoming available in previously inaccessible areas of the nation, the risk to individuals' ability to maintain their informational privacy is more significant than it has ever been. Despite the fact that the digitalization of the economy has made it possible for a plethora of job opportunities in the fields of health, education, and governance, it is more important than ever before to have a robust law in place to ensure maximum protection to these personally sensitive data of the individuals. This is because the digitalization of the economy has made it possible to become more digital.[6]

Meaning Of Data Protection

It has been said that Data Protection is one of the most abstract ideas in the law and that it cannot be summed up in a single sentence to explain what it is adequately. According to the opinions of jurists, the phrase "data protection" is a catch-all terminology used to describe anything linked with the processing of personal data. This is because the word "data protection" is used to denote everything associated with the processing of personal data. The first legislation ever enacted to safeguard personal information was Sweden's Data Act, enacted over half a century ago, in 1973, and went into force the year after that. It is now against the law for any individual or business in Sweden to utilize information systems of any sort to handle personal data without first obtaining permission from the Swedish Data Protection Authority. In the late 1960s, the residents of the innovative Scandinavian country had been worried about the rising usage and storage of personal data; hence, the Data Act was designed to calm their anxieties and end such concerns.[7]

The term "data protection" refers to the procedures, protections, and legally enforceable laws that have been put into place to secure the personal information you provide and to guarantee that

[5] S Singh, "Privacy and Data Protection in India: A Critical Assessment", 53 *Journal of the Indian Law Institute*, 104-111(2012).
[6] Dhiraj R. Duraiswami, "Privacy and Data Protection in India", 166, *J.L. & Cyber Warfare*, 169-72 (2017).
[7]David Wallace & Mark Visger, "Responding to the Call for a Digital Geneva Convention: An Open Letter to Brad Smith and the Technology Community", 6 *J.L. & Cyber Warfare* 3, 12- 13 (2018).

you retain control over it. In a nutshell, you should choose whether or not you want to disclose certain information, who has access to it, for how long, and for what purpose; you should also be able to edit some aspects of this information and more. "Personal data" and "processing" are two tenets of data protection laws that establish the lion's share of the meaning of data protection laws as tenets of data protection laws. Because these two ideas play a crucial role in examining the fundamental logic behind data protection regulations, they need a significant amount of focus and attention. Because the meaning of the word "processing" is as broad as the whole legislation of data protection itself, it should be defined in a way that is generous to increase the scope of the protection bestowed by the law. A material action that has a direct influence on the data is referred to as processing, and this would go on to cover the gathering of data, its storage, its erasure, its utilization, and its distribution. Most sophisticated data protection regimes advocate for interpreting the word in the broadest sense feasible. It is necessary to acknowledge that the whole goal of having data protection legislation would be undermined if the meaning of the word "processing" could be interpreted in an overly broad manner. The second component of the Data Protection Laws is, unsurprisingly, the idea of "Personal Data." This phrase refers to anything that may be used to identify a person or any information that can be related to the individual identity of a person. It also refers to anything that can identify a group of people. In accordance with this same line of thinking, one must decide whether or not a category of data may be categorized as personal. Once these aspects of data protection laws have been clarified, one will be able to better understand the whole notion of data protection laws. A set of regulations that protect the dissemination, collection, use, erasure, storage, and destruction of all information that may be used to identify a person can be defined as "data protection laws." Considering this, one can frame the definition of data protection laws as "a set of rules that protect the dissemination, collection, using, erasure, storage, and destruction of all this information.[8]" When it comes to the processing of personal data, protection here refers to a reasonable degree of fairness that is in line with the standards that have been established. On the other hand, the rules governing data protection have advanced significantly from the days when they just required the honest handling of personal information. These days, they relate to a more jurisprudentially developed idea of informational self-determination and autonomy. Informational self-determination is the right of

[8] Umang Joshi, "Online Privacy and Data Protection in India: A Legal Perspective", 7 *NUALS L.J.* 95, 101-103 (2013).

an individual to select the circumstances under which their data may be revealed in the first place. This right is sometimes referred to as the right to privacy.[9] Consequently, the courts in the European Union have used the test of information that is "personally identifiable" to assess whether or not a category of data may be categorized as personal. Once these aspects of data protection laws have been clarified, one will better understand the whole notion of data protection laws. A set of regulations that protect the dissemination, collection, use, erasure, storage, and destruction of all information that may be used to identify a person can be defined as "data protection laws." Considering this, one can frame the definition of data protection laws as "a set of rules that protect the dissemination, collection, using, erasure, storage, and destruction of all this information." When it comes to the processing of personal data, protection in this context refers to a reasonable degree of fairness that is in line with the standards that have been established. On the other hand, the rules governing data protection have advanced significantly from the days when they just required the honest handling of personal information. These days, they relate to a more jurisprudentially developed idea of informational self-determination and autonomy. The right of an individual to select the conditions on which their data may be published in the first place is referred to as "informational self-determination," and it is a concept that is covered by the phrase "self-determination."

Right To Privacy And Its Relation To Data Protection

The normative truth that an unrestricted link exists between the right to privacy and data protection legislation is indisputable and cannot be denied under any circumstances. Even though these two abstract ideas are likely to be conceptually distinct, there is a real connection between the right to privacy and the right to data protection. The fact that the right to privacy has been acknowledged as a fundamental right is the precise basis for the claim that data protection regulations have gone a long way to be classified as one of those fundamental rights. Only after it had recognized the right to privacy as an inherent aspect of the right to life and liberty as provided by Article 21 of the Constitution of India did the Supreme Court of India instruct the Central government to devise a data protection law along the same lines. This happened after it had identified the right to privacy as an inherent part of the right to life and liberty. The

[9] D Bruschi, "Information privacy: Not just GDPR", *Philosophical Enquiry (Cepe) Proceedings*, (9 p).

conclusion that can be drawn from this is that the data protection legislationdoes have at its core the intention of safeguarding the people's inherent right to privacy. However, for the Data Protection law's purposes, there must be a clear and precise definition of the right to privacy.[10] This is particularly important in a nation like India, where the legal framework governing the right to privacy is just beginning to take shape. However, much like the Data Protection Law, the right to privacy is an abstract notion, and there is a great deal of uncertainty among the legislators of the various countries of the globe regarding providing a precise definition of the right to privacy. On the other hand, the right to privacy has to be defined in a way that is both tangible and logical if there is to be any hope of the data protection rules ever serving their intended purpose. Due to the limited number of legal precedents, it is necessary to depend on some of the well-established concepts connected to it. Additionally, and this is of the utmost importance, the data protection rules themselves should be comprehensive enough to state the meaning and extent of the right to privacy in the clearest of terms. The absence of a clear and concise definition of the right to privacy comes with its associated expenses and advantages. This may be an advantage since the lack of a description gives the judicial system much leeway to interpret it in the broadest possible way. This may be considered a benefit. Because the world of technology appears to be constantly reinventing itself, it may be in people's best interests, democratic frameworks, and the rule of law to maintain the right to privacy as open-ended as possible. This is because the world of technology is constantly evolving. There has been much discussion over the issue of what exactly constitutes the most precise and accurate definition of the right to personal privacy. The vast body of research that has been done on the topic of the connection between the right to privacy and data protection regulations has been written to establish the relationship between the right to informational self-determination and information control. One of the most widely accepted interpretations of the right to privacy in the context of the protection of personal information is as follows: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.[11]" The "right to self-determination" is an idea that has a great deal of weight in any democratic framework, and as a result, it has a great deal of sway over the

[10] Henry Pearce, "Systems Thinking, Big Data, and Data Protection Law", 18 *Eur. J.L. Reform* 478 (2016).
[11] Orla Lynskey, "Deconstructing Data Protection: The Added-Value of a Right to Data Protection in the EU Legal Order", 63 *INT'L & COMP. L.Q.* 569, 577-81 (2014).

people. This idea is the only reason for the popularity and acceptability of this method. However, there is a need to come to terms with the reality that no data protection regulation can, strictly speaking, provide total informational self-determination. On the other hand, a strong law may guarantee a controlled decision.

These aspects are taken into consideration by several data protection standards to guarantee that persons are provided with the highest level of practically practicable protection. The notion of having the right to be left alone is credited with being the seed that grew into other data protection principles, such as the principle of purpose restriction, the focuson fairness of processing, and the right to deletion, among others. Disclosing sensitive information is an additional method that may be used to integrate the right to privacy with data protection. Data that might reveal the identity of persons, such as their name, sexual preferences, residence address, and so on, are examples of the types of information considered sensitive materials. There is a great deal of disagreement amongst academics regarding the efficacy of this strategy due to the fact that it is highly probable that through the technological advancements in this era of big data, information that is not otherwise sensitive may be collected and processed in a way that would make them of a sensitive nature. As a result, there is a great deal of disagreement regarding the effectiveness of this strategy.[12]

This passage exemplifies the significance that the Supreme Court of India attaches to the individual's constitutionally protected right to privacy. This historic verdict will affect the future interpretation of the data protection legislation in India for many years to come, regardless of the outcome of the case. It is only permitted for the sensitive personal data to be transmitted outside of India for processing" The Bill makes this observation. Still, itsays this does not apply to "critical personal data." The interpretation of the right to privacy in its geographical, functional, and institutional forms has, for a very long time, been seen as an impediment to gender equality. As a result, the feminist school of jurisprudence has leveled a great deal of criticism in the direction of this interpretation. The feminist school of thought views the right to privacy in the home as a tool that should be used to celebrate the subjection of women in their households. This

[12] Silvia Lucia Cristea & Viorel Banulescu, "The Right to Personal Data Protection. The Right to Privacy. A Comparative Law Approach", 64 *Analele Stiintifice Ale Universitatii Alexandru Ioan Cuza Din Iasi Stiinte Juridice* 1, 03-05 (2018).

interpretation has been criticized on several occasions as a tool for immunizing the power imbalances within families by the exclusions of the constitutional system under the guise of privacy. These criticisms have been leveled against this interpretation as a weapon for immunizing family power imbalances. The spatial and functional conception of the right to privacy has been viewed as a weapon that may be used to "defend the exemption of marital rape from sexual assault laws and to discourage state interference with domestic violence or child abuse."[13]The new Personal Data Protection Bill also includes three crucial terms not previously contained in the Srikrishna draft version. These sections have caused significant alarm among privacy experts and technology businesses alike. These include portions that will enable the Centre to ask any "data fiduciary or data processor" to send up anonymized personal data or "other non-personal data" to allow for improved governance or targeting of citizen welfare services. For example, one of these sections is "data fiduciary or data processor." The Indian Data Protection Act of 2019,which is now being considered, looks, on the surface, to model itself after emerging global norms such as the right to be forgotten. Other criteria, like the need to keep sensitive data in systems that are physically situated inside the subcontinent, may restrict certain business operations and are seen as more contentious by some individuals. According to the proposed legislation, the central government can formulate a digital economy policy about data that does not include personal information. More specifically, it can require any data processor to "provide any personal data anonymized or other no personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government." The final version of the Bill makes a small but significant shift in India's position by stating that "sensitive personal data may be transferred outside India." At the same time, it emphasizes that such data should still be retained inside the nation. Nevertheless, the legislative aim of stringent data privacy legislation must be clarified. India stands to gain a significant amount from the practices of other countries that are recognized to have robust data protection regulations in place.[14] By avoiding common errors, India stands to gain the most from the experiences of these nations. Given that India, along with the rest of the world, is heading toward a more digitalized and globalized society, it becomes all the more vital to address the concerns of data protection

[13] Eva Fialova, "Data Portability and Informational Self-Determination", *8 MASARYK U. J.L. & TECH*. 45, 456-51 (2014).
[14] Edward J. Eberle, "The Right to Information Self-Determination", *UTAH L. REV*. 965, 969-971 (2001).

that may have transnational features linked to them. This is especially true given that India is a part of the globe. To make a compelling argument in favor of a Data Protection regime that is compatible with the entities located abroad, and in particular, in the developed world, the researcher might consider it beneficial to discuss the generally accepted principles of Data Protection, particularly in the EU, as well as the legislations that govern these jurisdictions. This would be done to establish a strong case for a Data Protection regime compatible with entities located abroad.[15]

Big Data And Its Relationship With Privacy

Big data is a new paradigm of data-driven choices. The amount of data produced by our regular usage of various networks, such as cellphones, TVs, social media networks, sensor-driven gadgets, and many more networks. Big data focuses on finding correlations rather than determining causes; it asks "what" questions rather than "why" questions. "big data" refers to a collection of several sorts of data, such as text, images, and videos. Articles from major news outlets, social media platforms, photos on Instagram, professional photography, satellite imagery, aerial imagery taken by Unmanned Aerial Vehicles (UAVs), and films sourced from television channels, YouTube, Vimeo, and other channels are examples of many sorts of data that may be obtained from various sources. This is not exclusive to the industrialized world; on the contrary, the developing world is also creating enormous volumes of big data. ICT innovations, together with user participation on platforms such as social media and microblogging sites, amongst others, offer unprecedented large data collection, storage, and analysis. The analysis of data gathered from social media platforms, websites, mobile GPS, and other sources, amongst others, might help solve a variety of socioeconomic issues (Morrison, 2016) and assist in developing efficient solutions and policies. As a result, big data is now regarded as an incredible resource that can provide one-of-a-kind possibilities for everyone. Along with large amounts of data, metadata1 can expose private details about the lives of individuals, such as their political leanings, religious beliefs, sexual orientation, and so on. Metadata may expose information such as when a certain website was viewed, the user's IP address, location, and other similar details. There have been situations in which governments

[15] Jakub Misek, "Consent to Personal Data Processing - The Panacea or the Dead End", 8 *MASARYK U. J.L. & TECH.* 69, 71-72 (2014)

have collected metadata. The business models of many internet firms rely on gathering metadata to enhance their services and infer user behavior to improve their goods even more. This allows the companies to provide more value for their customers.[16] Nevertheless, collecting, accessing, and using such data pose serious risks to basic freedoms and human rights. Big data and metadata both have the potential to pose a significant risk to people's rights to the privacy of their private and sensitive information and their ability to exercise control over how their information is used. Since the 1970s, business in the United States, in particular, has been eager to amass vast quantities of information about customers and run algorithms against that data. However, data mining and automated decision-making have witnessed tremendous development in the last twenty years. According to Privacy International's research, this kind of data analysis has spread to areas such as passenger profiling, anti-terrorist systems, border management (i.e., automated-targeting system), and money laundering (i.e., suspicious transaction reporting and analysis). All of these areas are related to the fight against terrorism. The capacity of new technologies to transport data across a network without necessitating human-to-human or human-to-computer contact is possibly another danger to privacy that is provided by the so-called 'Internet of Things (IoT). "Computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers" are all examples of what the Internet of Things (IoT) interrelates. The most important thing is that there is now an industry surrounding big data. This industry "sells solutions to governments and companies, while there are new opportunities for data collection." These new opportunities include mass communications surveillance, merging data sets, deploying new sensor technologies, and the emerging "Internet of Things." Governments are launching initiatives, such as bills, policies, regulations, and other sorts of legislation, to gather massive amounts of personal data3 and sensitive data, and they are also launching programs to provide various services to the inhabitants and residents of their respective nations. In recent years, political officials and corporate executives have begun to promote the use of big data as a solution to a wide variety of issues, including eliminating corruption, delivering government services and entitlements, the battle against illnesses, and many more. It has come to our attention that governments and corporate players are collecting, keeping, and analyzing vast amounts of data about individuals in the name of public service,

[16] Alina Savoiu & Catalin Capatina Basarabescu, "the Right to Privacy, 2013 Annals Constantin Brancusi"*U. Targu Jiu Juridical Sci. Series* 89, 92-98 (2013).

improved delivery of citizen-centric services, enhanced user experience, and providing safety and security for citizens. Concerns have grown, however, regarding the lack of transparency and accountability surrounding the design of algorithms that are used to process the data,[17] questionable security measures that are used in the storage and maintenance of large datasets, excessive reliance on big data as opposed to more traditional forms of analysis; and the creation of new digital divides. In the next part, we are going to talk about how various organizations and governments are collecting, storing, utilizing, transmitting, and reusing the data that has been obtained for a variety of different reasons, as well as how the right to privacy is being endangered and infringed upon in this era of Big Data. In conclusion, this article suggests a framework to be followed in India to secure individuals' personal and sensitive data on the Internet. This framework is based on the 'Ten Point Action Plan' presented by the UN special rapporteur for the right to privacy. In the last section, the article discusses a few different ways in which development may be made.

The Foundations Of Data Protection Regime In India

The B.N. Sri Krishna Committee was responsible for laying the groundwork that would eventually lead to the formation of a comprehensive framework for the data protection regime in India. Last year, the government of Narendra Modi created a committee that Justice would lead (Ret.) B.N Srikrishna. This group has been tasked with suggesting steps to address data protection and privacy concerns effectively. This committee has also considered establishing a regulator, which may be modeled after existing regulatory agencies such as the Securities and Exchange Board of India or the Reserve Bank of India. As a result of gaps in the existing laws, such as the lack of incorporation of the key data protection principles and the necessity of having a law that is both more comprehensive and centered on data protection principles, a committee was established to make recommendations regarding the structure of a brand new and comprehensive data protection legislation. Along with a draft of a data protection law, the report of the 10-person committee chaired by the Honorable Justice B N Sri Krishna, who served as a judge on India's Supreme Court in the past, was filed. The report included suggestions for a comprehensive data protection system in India. The rules of the GDPR were very closely

[17] David Bender, *Computer Law: A Guide to Cyber Law and Data Privacy Law*, 388-389 (Kamal Law House Culcutta, 1ST ED. 1978).

reflected by the suggestions, which also included provisions for incorporating the most important data protection principles into India's legal system. At the time of the draft law's publication, it was welcomed as the cornerstone of the basic concepts of India's impending data protection system. This praise came shortly after the draft bill was made public. To pave the way for an analysis of the proposed data protection legislation in India, it would be helpful to conduct a quick analysis of the important components and suggestions included in the report produced by the committee.[18] Along the same lines as the General Data Protection Regulation (GDPR), the fundamental features of the data protection system, such as the definition of data and processing, as well as personal and sensitive data, were outlined in the draft law. After that, it outlined the limited circumstances under which the state and private companies are permitted to handle people's personal information. In addition to advocating for strong data localization requirements, the law stipulated that at least one copy of any data intended to be moved internationally must be maintained in India. This requirement was intended to prevent data from being stolen or lost in transit. The proposed legislation also acknowledged the right to data portability, the right to be forgotten, the right to accessibility, and the right to rectification, in addition to advocating for a wide interpretation of the rights of the data principle. In addition to that, the significance of providing voluntary, informed consent was emphasized in the proposed law in a significant way. However, one of the most significant omissions from the original law was the lack of a provision for the right to erasure, and there was also no mention of the need to revise the existing monitoring system in the nation. Nevertheless, the vision of an independent data protection authority chosen by a committee that would include the Chief Justice of India was one of the most commendable components of the law. This was one of the most admirable aspects of the bill. Even so, while the Srikrishna committee suggested including the Chief Justice of India or her nominee as well as one expert of repute in the Selection Committee, the PDP Bill that was introduced in parliament provides for a committee that is entirely composed of members from the executive, i.e., secretaries from departments of the Central government, without a judicial member and an expert. This is in contrast to the recommendations made by the Srikrishna committee. The authority and discretion to remove any member of the DPA are vested in the Central government; however, neither the mechanism nor the process for such removal is

[18] Lee A. Bygrave, "Data Protection Pursuant to the Right to Privacy in Human Rights Treaties", 6 *Int'l J.L. & Info. Tech.*, 253-259 (1998).

expressly established.[19] This power and discretion are vested in the Central government. Additionally, the protection of the members' salaries has been weakened, and the central government will now dictate it. As envisioned under the draft law, the Data Protection of India would have various powers, including the ability to search for and seize evidence and impose severe fines. Much criticism was leveled at the report that the Committee produced. These objections ranged from the fact that the need to preserve the informational privacy of the people was relegated to a secondary position in favor of prioritizing the economic elements of personal data. It has received backlash from academics and campaigners for the right to information due to the poor construction of the report. The people who had been outspoken in their support of the Aadhar Act were the ones who made up the committee members. Some of these individuals even rejected the acknowledgment of the right to privacy as a basic right at different points in time. The report, even though it had mirrored many provisions along the lines of GDPR. It promised the dawn of a healthy and robust data protection regime in the country. Still, it failed to answer some of the pressing questions related to the safeguards against the intrusions of the state in the realm of the private affairs of the citizens. Specifically, the report failed to answer questions about the safeguards against the intrusions of the state in the realm of the citizens' medical records. The philosophical undertones of the study, which attempt to stress more the need for a thriving economy rather than protections against the violation of the basic right to privacy, are the source of the most substantial difference from the report. This deviation may be traced back to the overtones of the report. To a large degree, the study also misinterprets the landmark judgment in the case of K. S. Puttaswamy v. Union of India while neglecting the significance of the idea of proportionality, pushing the basic right over the backseat. The inability to acknowledge data ownership, the absence of rules addressing notification of the breach, and the non-mention of revisions in Aadhar are only some of the other factors on which the draft law came under heavy criticism. Since the days when data security was only considered relevant inside the confines of the information technology industries, India has made significant progress in this area.[20] As was said, the use of data has developed into an essential component of the Indian economy; thus, there is a need for a complete framework that can respond to the

[19] Brian Gorlick, "Human Rights and Refugees: Enhancing Protection through International Human Rights Law", 69 *Nordic J. Int'l L.* 117 (2000)

[20] Rosemary Jay, *Angus Hamilton, Data Protection Law and Practice* 445 (Kamal Law House Culcutta, 1995).

requirements of data security in India. In the next chapter, the researcher will go through some universally acknowledged data protection principles tobetter comprehend the normative facets of data protection law.[21]

Conclusion & Suggestion

Data storage and transport are now more convenient than ever in this age of globalization. There have been some excellent outcomes, but there have also been some dire ramifications, such as the well-publicized What Sapp data breach case. It is becoming less challenging to abuse data and invades people's privacy. There has yet to be an established body of law addressing this issue because of how recently it has arisen. While an effort was made to develop a comprehensive central level Law on the subject with the introduction of the Personal Data Protection Bill of 2019, such a law has yet to be enacted. Data privacy is crucial in all walks of life, especially in the business sector. Regarding protecting people's personal information online, India needs to catch up with other developed countries.

[21] Jordan J. Paust, "Can You Hear Me Now? Private Communications, National Security and the Human Rights Disconnect", 612, *Chicago Journal of International Law*, 625 (2015)