IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

RAYAT BAHRA UNIVERSITY, KHARAR, MOHALI ANALYTICAL EXPERIMENTATION ON OBSTACLE TO THE RIGHT TO PRIVACY IN THE DIGITAL AGE

By

Ms. Swapanpreet Kaur

Assistant Professor

ABSTRACT

The necessity for data privacy regulations and the civic right to privacy of every person, regardless of sexual inclination, essentially set off the privacy debate in the twenty-first century. A crucial aspect of life and liberty, privacy is a natural component of the fundamental rights guaranteed by the Constitution. It is present in every person equally, regardless of class, social standing, gender, or orientation. It is important for the growth of a person's personality, integrity, and dignity. The right to privacy is not absolute, thus every invasion must be justified by law and must be founded on necessity, legality, and proportionality in order to protect this prized right. In this article, the writers trace the history of privacy through a number of judicial rulings, establishing privacy as a fundamental right protected by Article 21 of the Indian Constitution. The majority of the essay is devoted to the legal analysis of how this right came to be recognised as a fundamental right. Additionally, given that the period in which we live is one of information, not all of the information we possess must be disclosed and some information must be protected, privacy plays a crucial part in this situation. In the 21st century's technologically advanced period, the idea of protecting such privacy in the form of information is of the utmost importance.

Keywords: Jurisprudence, Privacy, Fundamental Right, Article 21, Indian Constitution.

INTRODUCTION

India is well-known for having the largest democracy in the world, one of the fastest-growing economies, and a young population that will benefit from demographic trends in the next decades. One of the most important Drivers of social effect in India is the cell phone. It is increasingly being used by Indians to get inspirational services. A near-perfect confluence of supply factors, including falling bandwidth prices, low mobile device prices, the quick rollout of 4G, and aggressive mobile technology navigation, and demand factors, including rapidly rising affluence, quick adoption of mobile technology across demography, and mobile technology catering to a large population who had limited opportunities to connect with one another efficiently and effectively, is driving the unprecedented pace and scale of digital adoption. Rapid digital adoption is nourishing a "mobile-first" ecosystem, with mobile as the primary device.

From a cultural standpoint, India has long been used to nuclear or extended families, while urbanisation has had an impact on the average family size, which is still around 5.5. The famed Indian "thrifty gene" has been attributed to a vast population that lives at subsistence or

sustenance levels. Indians are known for being exceedingly value conscious. With all the information, prices, and connections at your fingertips, a cheap mobile device with cheap or unlimited data leverages the frugal heritage mindset while enabling social interaction and feeling very intimate. Indians spend a lot more time than the average person using their phones since they live in huge joint families and create their own virtual spaces. For many Indians, a mobile phone serves as more than simply a means of communication; it also serves as their only window to the outside world.

Mobile devices are now exposed to a variety of security risks and dangerous threats. Modern mobile applications are widely available and fairly simple to set up on practically all mobile operating systems. It was an information scam. Businesses have tricked consumers into believing that they are connecting with friends, navigating their way around town, or discovering the ideal jumper. Companies are amassing a multi-billion-dollar war chest of information to use against one other as they tout the merits of each new digital tool and rave about the newest apps to one another. The adage "You are the product" applies here.

PRIVACY IN THE DIGITAL WORLD

India has started a significant transformation towards becoming a data economy over the last few years. People all around India are creating enormous amounts of data every day thanks to the growth of digital services. India is one of the nation’s producing the most data in the world, producing 150 Exabytes of data annually.

We are surrounded by data, which is produced in almost everything. Data is valuable when it is shared, creating a significant amount of efficiency. One sort of data is that which we may deliberately disclose, and the other type of data is that which is generated practically every time we carry out an action, such as travelling, placing an order for food, or using transportation. There is no denying the great value of this data, and a number of businesses are willing to pay for access to it. Data has become the new money in this era of almost universal access to the internet. The fact that the data's full potential is unknown makes it much more intriguing. Newer applications that increase the value of the data appear as technology develops. The biggest taxi company in the world, Uber, does not own any cars; the biggest media company in the world, Facebook, does not produce any content; the most valuable store in the world, Alibaba, does not have any inventory; and the biggest hotel firm in the world, Airbnb, does not own any real estate. Nowadays, even something as basic as calling a cab requires the use of a smartphone app that gathers and uses a variety of data kinds, including the user's financial information, real-time location, details about prior trips, etc.

Data is the new currency, and internet access is practically free. Even more intriguing is the fact that the data's entire potential is unknown. Newer applications are developed as technology advances, increasing the value of the data. The biggest taxi firm in the world, Uber, does not own any cars, Facebook, the most popular media company in the world, does not produce any content, Alibaba, the most valuable retailer, does not have any inventory, and Airbnb, the biggest hotel chain in the world, does not own any real estate. Even something as basic as calling a cab requires the use of a mobile application today, which gathers and uses a variety of data kinds, including the user's financial information, real-time location, details about prior travels, etc. Data is significantly changing how people conduct business, communicate, and make decisions.

Information can now be compressed, saved, modified, discovered, and interpreted like never before, making it easier to turn it into knowledge that is useful. The prevalence of long-term information storage and the ease of data collecting, together with the low cost of keeping and processing information, have made it possible to compile substantial user profiles by gathering ever-more-intricate data about a person. Based on past online conduct, this information can subsequently be utilised to develop customised user profiles, which has the advantage of speeding up transaction processing.

The problem caused by this proliferation has less to do with big data and more to do with behavioural data. Digitally recorded information includes more specific information on our purchases, thoughts, time spent, and who we interact with. Inferring our personal features that were previously concealed from view using this information is becoming more and more common. It is utilised to create our in-depth online personas, which are then used for targeted messaging, suggestions, and customisation. These representations frequently depend on data that are muddled together in ways that are impossible to predict and data that are not always knowingly disclosed. These portrayals may also conflict with our personal and public views of who we are.

Consideration should be given to a number of issues, including who owns the data, who has access to it, and what restrictions are in place about its use. Law is making up for any technological shortcomings. Multiple governments requesting and wanting access to data from their citizens and corporations further complicates the situation.

What are the boundaries of privacy? Data sharing for the sake of essential services, travel, or even government benefits? National security takes precedence over all privacy concerns.

In India, Right to Privacy has been acknowledged as one of the fundamental rights by virtue of Article 21. In the case of K. S Puttuswamy v. Union of India it was held that "The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution".

The main shortcoming in the current jurisprudence, according to the court's analysis, was the absence of a "doctrinal formulation" that could be used to determine whether Privacy is constitutionally protected. The court referenced a lengthy line of reasoning when reaching its decision. As a result, the jurisprudence on privacy shifted from being regarded as a right that protected other goals to being considered an end in and of itself. The judgement not only ruled that privacy is a basic right but also that informational privacy is a subset of the right to privacy.

Mobile devices are gathering and processing a growing amount of user-related data. They are becoming the standard for how we store our personal data. The simplicity of gathering massive amounts of data has increased dramatically since the development of numerous sensors, such the GPS, camera, and fingerprint scanner. Due to the fact that mobile applications are frequently untrusted software running on a trusted platform, this poses serious dangers to data privacy and protection. The ability to access, transport, and store data in mobile applications often occurs without the user's knowledge. Even with such mitigations in place, it might be challenging to determine what a programme truly performs with the rights it is given. Many applications have recently come under fire for being overly privileged.

SIGNIFICANCE OF THE RESEARCH

The end user's trust and confidence have been eroded as a result of the quick commercial usage of personal data. The misuse of sensitive and important personal data is a source of growing anxiety and worry. Regarding what "they" know about them, there is a broad feeling of anxiety among the populace. The conflict between "us" V. "they" has left consumers and citizens with a lack of trust.

Data collection procedures are frequently secretive and obscured by confusing privacy forms, which results in procedures that users have little control over. Unfortunate realities include incomplete statistics on data flows and, worst still, more obvious effects. People have the right to anticipate that businesses would gather, utilise, and disclose data in ways that are consistent with the context in which customers supply it. By focusing on respect for the individual rather than formalities like privacy notices, consent boxes, and structured data, this research will contribute to the current need to do so. The context, who is gathering the information, who is analysing it, who is disseminating it and to whom, the type of information being collected, and the relationships between the different parties are all important considerations in this study's assessment of privacy interests.

In India, legal and regulatory compliance has largely dictated the dominant narrative on data privacy and the ethical use of data. By concentrating on the ethical and societal implications of data, new tactics for achieving long-term commercial success can be developed. Big Data doesn't have to just be about a struggle between commercial opportunity and social acceptability; it can also be about innovation-fueled growth and profitability. Understanding where India is today as a country is essential to influencing the narrative of data privacy in the country's future. Individuals are often not aware and explicitly informed about the ways their personal, transaction, and behavioural data could be used. In most cases, personal data is used to build detailed online profiles and deliver value back to the user. However, these profiles, in some cases, could lead to unfair discrimination or marginalization, as they are incomplete or inaccurate. Several private enterprises currently do not track data privacy and security practices followed by their vendors. There is a high incidence of data

breaches and incidents in India. In 2021 India experienced the third highest number of data breaches across the world.

Businesses are at a great risk of having their data breached by insiders, such as employees or unauthorised third parties. Early-stage businesses frequently struggle to obtain the bandwidth and money necessary to keep up adequate security measures. Mobile applications do not offer users the Right to be Forgotten and do not have a standardised or easily accessible method for periodically deleting data. A double-edged sword, the ongoing collecting and use of personal data poses serious threats to both individuals and businesses.

In particular, it may result in the invasion of a person's privacy, monetary losses in the event of a breach, and discrimination, marginalisation, or exclusion of people or groups. Incidents involving data security can raise the cost of litigation, regulatory fines, compliance costs, and fraud claims, among other things. They may result in the loss of consumer confidence and reputation. Key players in the privacy ecosystem, including businesses, policymakers, consumers, and civil society, must establish guidelines and standards for gathering, handling, and using personal data in light of these rising concerns. Data breaches, hacking attacks, identity thefts, lost credit/debit cards, false news crises, and a number of other data-related incidents have reignited a global discussion on personal privacy and data ethics norms.

India does not have a comprehensive legislation which deals with Data Protection and Privacy. There is a requirement to formulate robust data management policies, standards and best practices with accurate data, appropriate data access, strong data security, and privacy and ownership rights. Deploying advanced digital infrastructure for connecting and when mass data is collected, it is impossible to distinguish between personal data and non-personal data, as various kind of data deal with various level of security. To avert contradiction, confusion and mismanagement, a single administration and regulatory body is necessitated.

Privacy is a fundamental right only in some jurisdictions, but protected by all societies across the spectrum. Moreover, there is still an ongoing debate on the implementation of data protection regimes. Ranging from one regime for all to a sector specific be spoke approach to complete exemption of some or a combination, jurisdictions are yet to converge on the basic principles of implementation. The research will help to review the law and compare it with other countries how they have been tackling the issue of Data Privacy. Data Privacy in order to harness the benefits of the digital economy and mitigate the harms consequent to it, formulating a data protection law is the need of the hour for India and this research will be way towards it.

REGARDING INDIAN CULTURE PRIVACY

We need to go back to the cultural dynamics and societal structure of families and societies to understand attitude of people towards in India.

Culture:

India has never viewed communication or information as being "private" due to cultural traditions. In India, where practically every aspect of one's life is visible to, connected to, and dependent on a family, a group, a village, or a society, there is also little awareness of private existence. The idea of privacy has always been challenging to understand in a world where individual decisions are meaningless and family members share a room. This is the reason why "Privacy" and "Security" are frequently associated with luxuries and the wealthy, respectively. Furthermore, there is a lack of awareness of what is personal and what is private, leading to a variety of personal and private discussions at local meetings around the nation. Indian Panchayat and Kangaroo courts frequently debate a family's private concern in a public setting, with community members contributing their opinions. In India, cultural practises are so pervasive that they trump individual freedom of choice and ownership.

In contrast to the US, which is an individualist society with a greater IDV and a lower PDI, Hofstede claims that India is a collectivist society with a lower Individualism Index (IDV) and a higher Power Distance Index (PDI).

According to research by Hofstede, people in collectivist cultures are more likely to have faith in and trust in other people than people in individualist ones.

Caste and Creed:

Caste and creed are deeply ingrained in Indian culture, making it difficult for laws prohibiting discrimination based on caste and creed to be very effective. Although caste and creed are individual identities, there are few opportunities or options in India for keeping them secret. In Indian villages and cities, communities have historically been split based on traditional occupations. These professions are directly related to a person's caste and religion. So these identities are usually public knowledge in smaller towns and villages where occupations have not diversified as much as in urban locations. The segregation is common knowledge, and rarely do people frown upon in.

Meddling Nature:

Indians have a habit of asking too many questions and interfering in other's life more than they need to. Ironically, they don't even consider seeking personal and private information of an individual or a family as interference or breach of Privacy.

Marriages in India:

Arranged weddings are still more or less the norm in India, despite the fact that it seems strange to many people throughout the world, especially in the West. Even in the most cosmopolitan and metropolitan of cities, where a person's marriage is not a personal decision but a decision arrived at after discussions and approvals from the immediate family, the extended family, and frequently even the community and the village, marriages in India are between two families, rather than two individuals, and it is still one of the most common routes to marriage. This interference in personal space is not enough, community members do not only decide who a person should marry but also want to know how much is being spent on a wedding, when will the couple have kids or why is a couple not having kids. And this intrusion into one's personal life starts from a very young age.

Privacy in Indian Homes:

Indian youngsters are not taught to close their bedroom doors even when they go to bed as a way of protecting their privacy. Even closing your door as an adult in many homes in rural and urban India unless you are changing clothes is seen as a secretive behaviour and not a matter of privacy. In addition, it is frequently the parents, the adults in the family, or the community, who choose what is appropriate to wear, what is appropriate to eat, who is appropriate to speak with, and what is appropriate for everyone to share. In India, encroachment on one's personal space is rarely regarded as an invasion or embarrassing. Personal space is not valued at all, whether it is when people are crammed into a bus or when strangers share a bunk on a train without raising an eyebrow.

Indian Languages:

Privacy is not a word in the majority of Indian languages. Indian words for seclusion or humiliation are the closest the language gets to privacy. This might be as a result of the society-based communal structures that are more common in India than in the West, where living is more focused on the individual.

Diversity:

India is an extremely diverse country where its diversity lies not just in its geographical landscape, topography and state boundaries but also in its culture, traditions, food habits, attire, language, dialects, script, behaviour, religion and caste. As the proverb goes, "Every two miles the water changes, every four miles the speech".

Socio-Economic Strata:

Additionally, socioeconomic considerations contribute to disparities in the importance and use of privacy. Higher socioeconomic strata were reported to be more worried about privacy rights in surveys done in Bangkok in 1996, whereas lower socioeconomic groups were found to be unaware about surveillance techniques. The perception of privacy has grown as more people from different socioeconomic backgrounds get access to the internet. In a 2001 research of Thai internet users, it was discovered that although 70% of users were aware of their online privacy rights, only 50% were aware of what to do in the event of data abuse.

Oral Communication as means of Knowledge:

Culturally India has been a country where much of its knowledge has been transferred from one generation to another orally. In such as community, where little is documented on paper or in audio-visual formats, there is little meaning of Privacy or at best it needs serious deliberations. This lack of documentation of oral and ancient information applies to traditional knowledge about health, medicine, architecture, culture, craft, art, folk tales, folk music, language and more. There is no hard drive that stores this oral communication knowledge of India. In such a scenario where most conversations and flow of knowledge between large populations of India takes place through oral communication the idea of information protection or privacy of data has little resonance.

Dissemination of personal, private and public information, all takes place through oral communication. Our cultural society is at a crossroads, crediting to the digital revolution. Given the cultural dynamics and societal structure of interdependence, coupled with the close-knit community structures, the lack of Privacy in India's physical society is entering its digital society as well.

Disregard to cultural difference:

The same threats to personal privacy are presented by information and communications technology, virtually completely disregarding culture differences. Asians react with the same fury as Westerners when their personal private is violated. As a result, current events have sparked changes in legislation and attitudes. and forced them to march around a nearby neighbourhood as their names and addresses were made public, wearing attire provided by the government.

Shift to interdependence on trust:

Privacy in Information and Communications technologies present the same challenges to Personal Privacy in India People often believe they have nothing to hide when asked if they would want to maintain privacy, even the privacy of the data on their mobile phones. Indians need to understand that privacy is not about what you want to hide but what others need not see. As the country moves increasingly towards the digital medium almost paradoxically there is also interdependence on trust.

Privacy Calculus:

The dimensions of privacy and definitions vary across disciplines but at their core most acknowledge the role of the individual in controlling access to their own information as central. The theft or misuse of personal information is the basis of discussions of online privacy given the value that this data has when collected, mined, categorized and shared. A literature on information privacy and its diminishment resulting from information and communications technologies exists that analyses how people make decisions about revealing their personal data. An individual's concept of privacy is changeable depending on the benefit they expect in return for revealing their information.

Interdependent Privacy:

Not only personal, but also interdependent, is privacy. People are socially intertwined and create bonds with one another through information sharing. As a result, anyone who has information about a user, including businesses and other customers, may jeopardise privacy by disclosing personal data that the user may not have voluntarily provided. Therefore, privacy is a multifaceted concept. Consumers who keep and collect information on others, such as their family or co-workers, pose an increasing threat to these individuals' privacy as technology progresses to enable passive information sharing through an expanding range of devices. It is anticipated that the extent and complexity of this danger will rise globally. It has an impact on policy makers who have not yet given privacy violations brought on by the use of data by private individuals its full attention. It also has an impact on marketers who are frequently in charge of data gathering. Even the best-in-class European Union General Data Protection Regulation (EU GDPR) currently has a regulatory gap when it comes to the problem of interdependent privacy. One of our most basic needs is a sense of belonging.

Connection to and interaction with people are essential for one's health and happiness. Communication serves as the medium for social connection. Despite the fact that people also share personal information with one

another, the idea of privacy as a mutually exclusive occurrence arises from the fact that people know things about one another. Due to the interdependence of privacy, anyone possessing information about a person may damage that person's privacy without that person even realising it. This suggests that there could be a much larger number of actors who violate privacy than those who work to do so. Even the most private information is simple to lose control of once it has been shared. Peer privacy protection seems to function according to implicit standards regarding what, why, and with whom information is shared within particular connections in an analogue world where everyone knows everything about everyone else. People instinctively agree to respect each other's privacy and limit the amount of information they provide. These negotiations are mostly missing thanks to new information and communication technology. With new technologies the scope for interdependent privacy infringements is significantly larger. In online settings where people use devices to automatically and effortlessly collect and disclose information digitally, peer- privacy protection frequently fails. Although consumers are wary about others sharing their information online, and may even suffer from the social costs of having their trust in others broken, they nonetheless regularly click accept to requests for data about others, effectively infringing others' privacy.

To illustrate, when people sign into a website with their social media account, they are potentially sharing the data of people in their network. When an app uses Facebook authorization, it can ask for up to 40 different permissions, ranging from access to photos to timeline posts to friends' lists. As a result, Facebook can track what consumers have done on over 8.4 million websites with the Facebook like button.

Types of Privacy:

Spatial rings of privacy with diminish expectations of privacy for the individual the more distant the ring gets.

Physical Privacy Space:

Right to Physical Privacy Space concern an individual most. In terms of spatial depiction this is the space that surrounds him most closely. The right to physical privacy ranges from protection against the denial of life and personal liberty, the right of an individual to do what he wants, see what he wants, say what he wishes, eat and drink what he likes, read what he reds, have a consensual adult relationship with whom soever he pleases etc. without State encroachments or denials by way earliest laws pertaining to the sanctity of the home, freedom from unjust imprisonment or arbitrary detention without the "due process of law" or , as in the case of India "only if the law be just, fair and reasonable". It also includes "personal privacy" namely protection from peeping toms and fro defamatory publications.

Family Privacy:

In reality, it is a larger portion of a person's physical privacy. The spatial rings still represent a significant area of concern to the individual and have a significant place in privacy law, while not being as intensively loaded with privacy expression as the physical privacy rings. The family would typically consist of immediate family members, close friends, and relations.

Commercial Privacy:

It encompasses a large array of laws that are all designed to protect the privacy, confidentiality, and security of trade secrets, patents, copy rights, trademarks, and other sensitive corporate information. Commercial privacy does not affect a person's life as intimately as family privacy, sensitive data privacy, and physical privacy do. Additionally, business privacy issues are almost never treated as fundamental rights issues and are typically handled under commercial or mercantile regulations

Communication Privacy:

It encompasses the enormous range of communication that is not covered by the first three spatial rings of privacy. WhatsApp, Instagram, faster internet, cell phones, and messaging apps have made the globe into an ocean of nonstop talk, and people are frequently more invested in seemingly arm's-length contact than they would be in face-to-face interactions. When communications tend to invade the person's physical or emotional character, his sensitive data, his family, or his business, it is almost meant to preserve the individual. The enormous volume of data that floats outside the inner four spatial rings is good news for corporate giants and

LEAs. The state would search for anomalies, codes, or subliminal material within the data to create marketing tactics and sales techniques as opposed to the latter, who would use this data to do so.

THE EVOLUTION OF PRIVACY PRINCIPLES:

An advisory committee was established in the Department of Health, Education, and Welfare (HEW) in the 1970s to address concerns about data processing that was becoming more and more computerised.

The Fair Information Practises Principles (FIPPS) are the foundation upon which the HEW Committee advised the US Congress to create a code of fair information practises.

The FIPPS are a set of guidelines that outline how to handle, manage, and keep data in order to uphold fairness, privacy, and security in a constantly evolving international technology environment. FIPPS are now acknowledged as the cornerstone of contemporary data protection regulations everywhere.

In the 1980s, FIPPS was replaced by the Organisation for Economic Cooperation and Development (OECD) Privacy Guidelines. The OECD Guidelines, which are regarded as the first globally accepted articulation of fundamental information privacy principles, have had a significant impact on data protection systems all over the world. Numerous data protection frameworks, including the 2004 Asia-Pacific Economic Cooperation Framework (APEC Framework), the European Directive 95/46/EC on the processing of personal data and the free movement of such data (Data Protection Directive), and data protection laws, including Australia's Privacy Act, 1988 (Privacy Act), New Zealand's Privacy Act, 1993, and Japan's Protection of Personal Information Act, 2003, were all influenced by the OECD Guidelines.

Traditional privacy principles have come under a lot of scrutiny recently, but it has been argued that they may not be well-suited to address the problems caused by the dramatically increased volume and use of personal data, technological advancements, and international data flows. As a result of these worries, an expert group was formed to review and modernise the OECD Guidelines. (The 2013 revisions to the OECD Recommendations).

OECD 2013 Guidelines keep the core privacy principles such as collection limitation, data quality and purpose specification etc. Intact several new elements to strengthen data safeguards have been introduced. These include privacy management programs to enhance accountability of the data controller, data security breach notification which oblige data controllers to inform individuals authorities of a security breach and establishment and maintenance of privacy enforcement authorities. The 2013 OECD Guidelines are criticised as being fundamentally incompatible with modern technologies and Big Data analytics which have revolutionized how data is collected and processed.

JUDICIAL EVOLUTION OF THE RIGHT TO PRIVACY IN INDIA:

Article 21 of the Constitution of India provides that “No person shall be deprived of his life or personal liberty except according to procedure established by law”. However, the Constitution of India does not specifically recognize ‘right to privacy’ as a fundamental right. Whether the ‘right to privacy’ is a fundamental right was first considered by the Hon’ble Supreme Court in the case of *M. P. Sharma and Others v. Satish Chandra*, District Magistrate, Delhi and Others., wherein the warrant issued for search and seizure under Sections 94 and 96 (1) of the Code of Criminal Procedure was challenged.

The Hon’ble Supreme Court had held that the power of search and seizure was not in contravention of any constitutional provision. The Hon’ble Supreme Court refrained from giving recognition to right to privacy as a fundamental right guaranteed by the Constitution of India by observing that:

“A power of search and seizure is in any system of jurisprudence an overriding power of the State for the protection of social security and that power is necessarily regulated by law. When the constitution makers have thought fit not to subject such regulation to constitutional limitations by recognition of a fundamental right to privacy, analogous to the Fourth Amendment, we have no justification to import it, into a totally different fundamental right, by some process of strained construction. Nor is it legitimate to assume that the constitutional protection under Article 20(3) would be defeated by the statutory provisions for searches”.

The scope of this right first came up for consideration in *Kharak Singh v. State of Uttar Pradesh* case which was concerned with the validity of certain regulations that permitted the surveillance of suspects. In the context of Article 19(1) (d), the right to privacy was again considered by the Supreme Court in 1975. The Supreme Court while deciding the case of Govind v. State of Madhya Pradesh135 laid down that "a number of fundamental rights of citizens can be described as contributing to the right to privacy." However, the Supreme Court also stated that the right to privacy would have to go through a process of case-by-case development. The Supreme Court in the case of *R. Rajagopal v. State of Tamil Nadu*, for the first time directly linked the right to privacy to Article 21 of the Constitution and laid down thus:

"The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a 'right to be let alone'. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing, and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned".

Justice Subba Rao did say that privacy is a important facet of personal Liberty and thus Article 21 of the Constitution of India by observing as under: "In *A.K. Gopalan case*, it is described to mean liberty relating to or concerning the person or body of the individual and personal liberty in this sense is the antithesis of physical restraint or coercion. The expression is wide enough to take in a right to be free from restrictions placed on his movements.

"The expression "coercion" in the modern age cannot be construed in a narrow sense. In an uncivilized society where there are no inhibitions, only physical restraints may detract from personal liberty, but as civilization advances the psychological restraints are more effective than physical ones. The scientific methods used to condition a man's mind are in real sense physical restraints, for they engender physical fear channeling one's actions through anticipated and expected grooves. So also the creation of conditions which necessarily engender inhibitions and fear complexes can be described as physical restraints. Further, the right to personal liberty takes in not only a right to be free from restrictions placed on his movements, but also free from encroachments on his private life. It is true our Constitution does not expressly declare a right to privacy as a fundamental right, but the said right is an essential ingredient of personal liberty. Every democratic country sanctifies domestic life; it is expected to give him rest, physical happiness, peace of mind and security. In the last resort, a person's house, where he lives with his family, is his "castle"; it is his rampart against encroachment on his personal liberty. The pregnant words of that famous Judge, Frankfurter J., in Wolf v. Colorado pointing out the importance of the security of one's privacy against arbitrary intrusion by the police, could have no less application to an Indian home as to an American one. If physical restraints on a person's movements affect his personal liberty, physical encroachments on his private life would affect it in a larger degree. Indeed, nothing is more deleterious to a man's physical happiness and health than a calculated interference with his privacy. We would, therefore, define the right of personal liberty in Article 21 as a right of an individual to be free from restrictions or encroachments on his person, whether those restrictions or encroachments are directly imposed or indirectly brought about by calculated measures. It so understood, all the acts of surveillance under Regulation infringe the fundamental right of the petitioner under Article 21 of the Constitution."

The case of *Gobind v. State of M.P.* the right of the police to make domiciliary surveillance was challenged to be inconsistent with the right to privacy embodied under Article 21 of the Constitution of India. The Hon'ble Supreme Court held that the police regulations were not in compliance with the essence of personal freedom and also accepted the right to privacy as a fundamental right guaranteed by the Constitution of India but favoured evolution of the right to privacy on case-to-case basis and negated it to be absolute in nature. The Hon'ble Supreme Court observed as under:

"The right to privacy in any event will necessarily have to go through a process of case-by-case development. Therefore, even assuming that the right to personal liberty, the right to move freely throughout the territory of India and the freedom of speech create an independent right of privacy as an emanation from them which one can characterize as a fundamental right, we do not think that the right is absolute."

The Supreme Court in the case of R. Rajagopal v. State of Tamil Nadu, for the first time directly linked the right to privacy to Article 21 of the Constitution and laid down thus: "The right to privacy is implicit in the right to life and liberty guaranteed to the citizens of this country by Article 21. It is a 'right to be let alone'. A citizen has a right to safeguard the privacy of his own, his family, marriage, procreation, motherhood, child bearing, and education among other matters. None can publish anything concerning the above matters without his consent whether truthful or otherwise and whether laudatory or critical. If he does so, he would be violating the right to privacy of the person concerned17 …"

Subsequently in the case of *People's Union for Civil Liberties (PUCL) v. Union* of India the Hon'ble Supreme Court clearly held that "right to privacy is a part of the right to "life" and "personal liberty" enshrined under Article 21 of the Constitution. Once the facts in a given case constitute a right to privacy, Article 21 is attracted. The said right cannot be curtailed "except according to procedure established by law".143 The issue was once again raised before the Hon'ble Supreme Court in the case of *K. S. Puttaswamy (Retd.) v. Union of India*, in which case the 'Aadhaar Card Scheme' was challenged on the ground that collecting and compiling the demographic and biometric data of the residents of the country to be used for various purposes is in breach of the fundamental right to privacy embodied in Article 21 of the Constitution of India. Given the ambiguity from prior judicial precedents on the constitutional status of right to privacy, the Hon'ble Supreme Court referred the matter to a constitutional bench consisting of 9 (nine) judges.

It was argued on behalf of the Petitioners that the right to privacy is very much a fundamental right which is co terminus with the liberty and dignity of the individual and this right is found in Articles 14, 19, 20, 21 and 25 of the Constitution of India read with several international covenants. On the contrary, Union of India contended that 'right to privacy' is not a fundamental right guaranteed under the Constitution. The primary defence of the Union of India was that:

(i) if the framers of the Constitution wanted to include the 'right to privacy' as a fundamental right, the same would have been specifically included within the Constitution;

(ii) privacy is inherently a subjective and vague concept. The concept of privacy is difficult to define. Such vague concept cannot be elevated to a fundamental right;

(iii) The present laws already confer sufficient protection to individuals against invasion of privacy; and

(iv) 'right to privacy' is a legitimate claim having sanction of common law, each such claim cannot be elevated to fundamental right. The Hon'ble Supreme Court by its decision pronounced on August 24, 2017 unanimously held as under: -

The reference is disposed of in the following terms:

i.The decision in M P Sharma which holds that the right to privacy is not protected by the Constitution stands over-ruled;

ii. The decision in Kharak Singh to the extent that it holds that the right to privacy is not protected by the Constitution stands over-ruled;

iii. The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution.

iv. Decisions subsequent to Kharak Singh which have enunciated the position in (iii) above lay down the correct position in law."

Hon'ble Mr. Justice D.Y. Chandrachud, clearly held that: -

A. Life and personal liberty are inalienable rights. These are rights which are inseparable froma dignified human existence. The dignity of the individual, equality between human beings and the quest for liberty are the foundational pillars of the Indian Constitution; …

B. Privacy is a constitutionally protected right which emerges primarily from the guarantee of life and personal liberty in Article 21 of the Constitution. Elements of privacy also arise in varying contexts from the other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III; …

C. Privacy includes at its core the preservation of personal intimacies, the sanctity of family life, marriage, procreation, the home and sexual orientation. Privacy also connotes a right to be left alone. Privacy safeguards individual autonomy and recognises the ability of the individual to control vital aspects of his or her life. Personal choices governing a way of life are intrinsic to privacy. Privacy protects heterogeneity and recognises the plurality and diversity of our culture. While the legitimate expectation of privacy may vary from the intimate zone to the private zone and from the private to the public arenas, it is important to underscore that privacy is not lost or surrendered merely because the individual is in a public place.

D. Like other rights which form part of the fundamental freedoms protected by Part III, including the right to life and personal liberty under Article 21, privacy is not an absolute right. A law which encroaches upon privacy will have to withstand the touchstone of permissible restrictions on fundamental rights. In the context of Article 21 an invasion of privacy must be justified on the basis of a law which stipulates a procedure which is fair, just and reasonable. The law must also be valid with reference to the encroachment on life and personal liberty under Article 21. An invasion of life or personal liberty must meet the three-fold requirement of :

(i) legality, which postulates the existence of law;

(ii) need, defined in terms of a legitimate state aim; and

(iii) proportionality which ensures a rational nexus between the objects and the means adopted to achieve them; and

E. Privacy has both positive and negative content. The negative content restrains the state from committing an intrusion upon the life and personal liberty of a citizen. Its positive content imposes an obligation on the state to take all necessary measures to protect the privacy of the individual."

The Hon'ble Supreme Court rejected the arguments of the Union of India, and while analysing the nature of right of privacy as regards its origin, the Hon'ble Supreme Court held that the right to privacy is intrinsic to and inseparable from human element in human being and core of human dignity. Thus, it was held that privacy has both positive and negative content. The negative content acts as an embargo on the State from committing an intrusion upon the life and personal liberty of a citizen and its positive content imposes an obligation on the state to take all necessary measures to protect the privacy of the individual. Therefore, the constitutional protection of privacy may give rise to two inter-related protections i.e.

(i) against world at large, to be respected by all including State: right to choose that what personal information is to be released into the public space

(ii) against the State: as necessary concomitant of democratic values, limited government and limitation on power of State. The issue of data protection is important both intrinsically and instrumentally. Intrinsically, a regime for data protection is synonymous with protection of informational privacy. As the Supreme Court observed in Puttaswamy, "Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state."

In *R.C. Cooper v. UOI*, 'procedure established by law' in Article 21 has gained substantive due process element as well whereby even the contents of the law can be challenged being not in accordance with requirements of a valid law. Therefore, because of right of privacy being recognised as fundamental right, existing sectoral legislations, if challenged, may now have to pass the rigors of aforesaid test. Same would not have been the position, if privacy would have remained mere statutory or common law right.

The "Adhaar Card Scheme" which was alleged to be in breach of fundamental right to privacy, will now be tested by the same standards by which a law which invades personal liberty under Article 21 is liable to be tested. The Hon'ble Mr. Justice D.Y. Chandrachud concluded as under:

"Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the

need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state. The legitimate aims of the state would include for instance protecting national security, preventing and investigating crime, encouraging innovation and the spread of knowledge, and preventing the dissipation of social welfare benefits. These are matters of policy to be considered by the Union government while designing a carefully structured regime for the protection of the data. Since the Union government has informed the Court that it has constituted a Committee chaired by Hon'ble Shri Justice B.N. Srikrishna, former Judge of this Court, for that purpose, the matter shall be dealt with appropriately by the Union government having due regard to what has been set out in this judgment. We are in an information age. With the growth and development of technology, more information is now easily available. The information explosion has manifold advantages but also some disadvantages. The access to information, which an individual may not want to give, needs the protection of privacy. The right to privacy is claimed qua the State and non-State actors. Recognition and enforcement of claims qua non-state actors may require legislative intervention by the State".

WhatsApp Inc. after being acquired by Facebook Inc. changed its privacy policy, and the users were put to notice that WhatsApp account information of users would be shared with "Facebook" to improve "Facebook" ads and products experiences and the users' were asked to agree to the revised terms for continued use of WhatsApp on or before September 25, 2016. In view this development Karmanya Singh Sareen and another filed a writ petition before the Hon'ble High Court of Delhi contending that taking away the protection to privacy of data of users of WhatsApp and sharing the same with Facebook was in infringement of fundamental rights of the users guaranteed under Article 21 of the Constitution. The Hon'ble Delhi High Court while deciding upon the case ordered that if the users opt to completely delete the WhatsApp account, WhatsApp shall delete users' data completely from its servers and refrain from sharing users' data with Facebook, and so far as the users who opt to remain in WhatsApp are concerned, the existing information/data/details of such users up to September 25, 2016 shall not be shared with "Facebook" or any one of its group companies. The court also directed the Government to consider whether it is feasible to bring messaging apps like WhatsApp under some statutory regulatory framework. This decision has however, been challenged before the Hon'ble Supreme Court of India through a special leave petition. The matter is sub-judice and is presently pending for decision. The verdict of the Hon'ble Supreme Court and the policy formulated by the Government will, however, have a far-reaching impact on the manner in which personal data is handled in India, especially by non-state actors.

CONCLUSION:

Privacy rights are essential elements of life and personal freedom rights under Article 21. Privacy rights are not absolute rights. They are subject to rational limitations for the protection of crimes, disadvantaged, or morality, or the protection of other human rights. If there is a contradiction between the two derived rights. If one looks at the later judgments of the Apex Court one can observe the desirability of the court to treat the basic rights as water-tight compartments. This was felt foremost within the case of *A.K Gopalan v. the State of Madras* (1950) and also the relaxation of this stringent stand may well be felt within the decision of *Maneka Gandhi v. Union of India* (1978). The right to life was considered to not be the embodiment of mere animal existence, but the guarantee of a full and meaningful life.

Being a part of society often overrides the very fact that we are individuals first. Each individual needs their private space for whichever activity (assuming here that it shall be legal). The state accordingly gives each person the right to enjoy those private moments. Clinton Rossiter has said that privacy could be special reasonable independence that may be understood as a trial to secure autonomy in a minimum of some personal and spiritual concerns. This autonomy is the most special thing that the person can enjoy. They're truly free humans there. This is often not a right against the state, but against the planet.

REFERENCE

ARTICLES

• Digital India: Technology to transform a connected nation, Mc KINSEY GLOBAL INSTITUTE, available at

https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20india%20technology%20to%20transform%20a%20connected%20nation/mgi-digital-india-report-april-2019.

• Eliciting meta consent for future secondary research use of health data using a smart phone application - a proof of concept study in the Danish population Thomas Ploug1* and Søren Holm2,3,4Ploug and Holm BMC Medical Ethics (2017)

• Electronic Informed Consent in Mobile Applications Research John T. Wilbanks The Journal of Law, Medicine & Ethics, 48 S1 (2020): 147-153.

• The impact of mobile and rapid digital adoption on how India consumes, WORLD ECONOMIC FORUM, available at https://www.weforum.org/agenda/2019/01/how-mobile-is-disruptingconsumption-in-india/

• There's No Such Thing As A Free Lunch in the Digital Economy, 2018

• Wendy C.Y. Li ,Makoto Nirei, Kazu fum Yamana, Value of Data:

BOOKS

• Right to Privacy in India; Concepts and Evolution by Gaurav Goyal and Ravindera Kumar. • Why Privacy Matters by Neil Richards.

• Privacy In India in Age of Big Data By Buddadeb Halder.

• A Ultimate Cookie Handbook For Privacy Professional June 2020, One Trust Privacy, Security And Third -Party Risk

REPORTS

• A Guide to Data Protection in Mobile applications, Wipo, World Intellectual Property Organization,2021

• United Nations Conference on Trade and Development Unctad Digital Economy Report 2021

• Federal Reserve Bank Of New York Staff Reports, Monetizing Privacy, 2021

• Report To The President Big Data And Privacy: A Technological Perspective, Executive Office of the President President's Council of Advisors on Science and Technology May 2014 • Privacy and Data Protection by Design – from policy to engineering

• December 2014 European Union Agency for Network and Information Security

• The OECD Privacy Framework OECD 2013

• European Treaty Series - No. 181

• Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows

• ETS 181 – Automatic Processing of Personal Data (Protocol), 8.XI.2001

• Privacy by Design The 7 Foundational Principles

• Implementation and Mapping of Fair Information Practices

• Ann Cavoukian, Ph.D. Information & Privacy Commissioner, Ontario, Canada

LIST OF STATUTES

• PDP Bill- Personal Data Protection Bill, 2019

• Data Protection Bill 2021 (DP Bill)