International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# Privacy and Data Protection in Cyberworld

**Mr. Vishesh Prakash Srivastava**

**Abstract:**
The rise of the digital age has transformed how personal data is collected, stored, and used, often without individuals' full knowledge or consent. With the increasing reliance on the internet, smart devices, and online platforms, concerns around data privacy and the protection of personal information have grown significantly. In India, the recognition of privacy as a fundamental right through the Puttaswamy judgment marked a turning point, but existing legal frameworks, including the Information Technology Act and the draft Personal Data Protection Bill, 2019, have faced criticism for lacking strong safeguards and accountability.This research aims to examine the evolution of the right to privacy in India, assess the effectiveness of current data protection laws, and explore how well they align with international standards, particularly in the context of emerging rights like the Right to Be Forgotten.
As our lives become increasingly digital, questions around privacy and data protection have never been more urgent. With personal information being shared, stored, and analyzed online every second, the need for robust laws to safeguard individual rights is clear. This dissertation explores how privacy has evolved as a legal concept in India, especially in the context of cyberspace. It examines the constitutional foundations of the right to privacy, how Indian courts have interpreted it, and the challenges posed by modern technologies like big data, surveillance systems, and smart devices.
Special attention is given to the 'Right to Be Forgotten' and the 'Right to Erasure', and how these rights are addressed in India's Personal Data Protection Bill, 2019. The study also compares India's data protection landscape with legal frameworks in the US, UK, and Australia, identifying key strengths and shortcomings.
While India has made strides in recognising privacy as a fundamental right, the current laws still give broad powers to the government and often fall short in terms of accountability and transparency. The dissertation concludes with recommendations for a more balanced, rights-based data protection regime that aligns with global standards and puts individuals' privacy at its core.

## CHAPTER-1
## Introduction

"Privacy is a special kind of freedom that can be understood as an effort to have at least some personal and spiritual freedom against all the stress of today's life". It aims to build a dishonorable wall, to distance oneself. whole world. The white man is a private person who still retains some of his thoughts and decisions and does not feel obliged to share all the consequences with others, even with people he loves and trusts.
In India, according to Article 21, the right to privacy is inseparable from the right to life and personal liberty It is preserved and preserved as part of the Consider the definition of the right to privacy: "solitude and privacy have become important to the individual; but modern commerce and production, by inflicting violence on him, cause him anxiety and suffering far beyond harming him. He must be protected from intrusion." - Our lives are increasingly filled with truly smart devices creating the "Internet of Things" .When we create smart buildings such as smart homes, shops, or offices, the perception of the environment

improves rapidly. Sensor networks and infrastructure are now enabling our wider environment, such as smart cities, to become a reality.

The content of the smart world should provide significant benefits. Our smart cities will be more accessible and safer places to live. Our home will understand and adjust to our needs Use resources to meet our needs. "Our devices will track our thoughts and behaviours to create and solve our current and future needs".

After the emergence of cyberspace, anyone can easily access information about anything or anyone

Anyone can send information to cyberspace and store it there, and the information will stay there forever. We use social media, conversations on Twitter, tweets and retweets, photos, and videos we upload and all the pages we like are stored as our "digital footprint". Globalization has made the world more open to Internet technology; e-business, e-government, e-education, e-court, etc. It made people's daily work easier. "We live in the age of big data, where algorithms monitor the activities of our digital selves". Collecting, using, storing, accessing, processing, and destroying this information leads to the solution of many legal problems, the most important of which is the right to privacy of online information

Current data protection laws in India include 2019. Draft Data Protection Bill, 2000, "Information Technology Act, 2000 and Information Technology (Security and Procedures and Personal Information or Data) Rules, 2011". Data Protection Bill, 2019 regulates data privacy, transfer, and processing, and determines the rules governing it. in India. However, it gives the state the authority to access information. Section 35 of the PDP Act empowers "the Central Government of India to exempt any government institution from the provisions of the Act in the context of national security and political and public policy". It gives more power to the central government and makes it clear that it is the party that decides and decides its affairs.

"Section 43A of the Information Technology Act provides that a corporate body (such as a company, a sole proprietorship, or any other association of persons engaged in business or employment)"

Personally controlled by or about equipment owned by it or any sensitive personal data or information contained in the computer services operated will be damaged by providing compensation to the affected persons.

"Rules 2011 protects an individual's data or information. Any person who collects, receives, owns, stores, processes, or otherwise processes data provided by or on behalf of the relevant organization shall be granted the right of confidentiality in respect of the handling or processing of personal data, including sensitive data, and that it is by the legal agreement that such data or data is the information can be viewed by the provider file".

In its simplest form, data privacy means giving users the power to decide how their data is collected, used, stored, and shared. This research topic is currently topical because the personal information of individuals in cyberspace is being breached online, often without their knowledge. If applicable, the Personal Data Protection Act, 2019 will regulate personal data in India. This proposal gives unlimited power to the central government, which raises concerns about state access to public information. The permanence and location of "digital footprints" is an interesting area of research. While many laws apply to the protection of data in cyberspace, the borderless nature of the Internet has territorial and practical consequences.

**Research question**

The emergence and proliferation of cyberspace as an indispensable part of human life has increased concerns about data protection and privacy in this area. The ubiquity and persistence of digital footprints

pose a serious threat to people's privacy. Are Indian laws adequate to protect personal privacy regarding cyberspace information?

**Scope**

1. Examine the level of privacy protection in cyberspace in India
2. Learn about various Indian laws regarding personal data protection.
3. "A detailed analysis of the adequacy of the provisions of the Data Protection Act 2019".
4. Compare legal frameworks in different countries to protect personal privacy regarding cyberspace information.
5. Understand the right and necessity of the right to be forgotten and the steps taken by Indian law to ensure its protection.

**Objectives**

The objectives of the research are

1. This study will trace the evolution of privacy laws in India, especially in relation to privacy.
2. This study will analyze the issues faced by data privacy in the digital age of smart devices.
3. "The study examines current data privacy in various areas and proposes international standards for data protection".
4. "The Data Protection Survey, 2019 is designed to highlight weaknesses and inefficiencies in its provisions and recommend changes necessary to protect data".
5. This project shows how easy (often unknown) it is to collect information and get permission to see the rules as of now.

**Hypothesis**

Personal privacy regarding personal information in cyberspace is not adequately protected by Indian law. The Data Protection Law allows the government to restrict data access according to law, which affects the public's right to privacy.

**Research Question**

1. What are the latest developments in the field of self-defense in India?
2. What is business and privacy in cyberspace?
3. What is the legal basis for protecting privacy rights in cyberspace?
4. How to protect personal data in cyberspace in the age of big data?
5. What are the important steps that India will take to ensure adequate protection of personal data?
6. Are there any significant differences "in the way personal data is protected under the Indian Data Protection Act and the GDPR?"
7. What laws does India have to protect personal information in cyberspace?

**Methodology**

Due to time limitations, the method of this study is theoretical. This study is an analysis of data protection law in various jurisdictions and can be done through theoretical research as it includes bridging and case analysis of various laws.

This research will be carried out by collecting data from primary and secondary sources. Primary sources include statutes, statutes, and cases, while other sources include books, journals, magazines, online resources, and other related resources.

The advent of Cyberspace and its expansion as an irreplaceable part of human life has raised a concern regarding" the protection of data and the privacy of people in that sphere". The universality and eternity of digital footprints are posing a great threat to the privacy of people. Are the laws in India adequate to protect "the privacy of individuals relating to their data in Cyberspace"?

## CHAPTER 2
## INDIAN ORIGIN AND DEVELOPMENT OF RIGHT TO PRIVACY

Today's concept of privacy is not just "black and white". At the same time, definitions and concerns about privacy have varied according to national culture and educational philosophy. Classic American definition, at the end of the last century expressed by Samuel Warren and Louis Brandeis, is "privacy is the right not to be disturbed." "However, it is an attempt to simplify the secret. The question of which aspects of personal life need to be protected may be, for example, privacy, behavior, confidential decisions, and private information."

Even the laws of the United States and Indian law does not clearly state that privacy is one of the fundamental rights and hence there is no attempt to define privacy. However, over time, courts in both countries have accepted, in many decisions, that" privacy is part of fundamental rights."

In India**, Kharak Singh v. the State of U.P**. decisions deny the right to privacy. However, over time, Indian courts, taking lessons from the decisions of "the American courts, began to interpret the Constitution" in a way that established the existence of the "right to privacy is a fundamental right", by defining the right to life insurance in Article 21. Supreme Court Justice Tan Ka Sing in **Puttaswamy v. UOI**, stated that the "right to privacy is a fundamental right to life and personal freedom"

## EVOLUTION OF THE CONCEPT OF THE RIGHT TO PRIVACY

According to Article 21, The person's right to privacy is jointly controlled and protected. their freedom. Its origins can be traced back to the idea that humans have certain natural or privileged qualities. Natural rights are inalienable because they are inextricably linked to human behavior. The human element in life is unthinkable without the existence of natural rights. Aristotle proposed that the public sphere be divided between the political sphere (which he called "polis") and the private sphere of human life (which he called "oikos"). This duality can lead to early recognition of the "latent space that represents public opinion."

By fundamental rights, life, liberty, and property are private, according to John Locke's Second Treatise of Government, published in 1690. Special funds are created to provide a limit to the government. Prevent outside interference. William Blackstone spoke of "natural liberty" in his Commentary on the Constitution of England in 1765. According to him, people are given absolute rights with immutable rights. "These rights include personal security, personal freedom, and property rights". "The right to security of person means the lawful and non-violent enjoyment of one's life, limb, body, health and reputation". According to Mill: - Part of the behavior for which a person is socially responsible is behavior that affects others. His freedom is clear as long as it concerns only himself. People have control over themselves, their bodies and their minds. James Madison, "the founder of the United States Constitution, decided to protect the right of citizens to be a part of the Constitution". The inalienable property of man. –"In the old sense, a man's land, goods or money are called his property. In the second sense, a man has property in the free exchange

of his thoughts and feelings". "He has an equal interest in the free exercise of his faculties and in the free choice of those who exercise them. Consequently, just as a person is said to have a right to property, he can also be said to have a property right". "When power ends, nothing will be given the respect it deserves". "No one's thoughts, people, talents or belongings are safe... The heart is the most sacred of possessions; "The heart is the purest of everything. Another property depends on some part of good law, the exercise of which is a natural right and not a right". "Keeping a house as his castle, paying public debts, and managing private debts with true faith, the husband who is holier than his castle cannot accept any law that violates the heart of his life or as a bond of relationship and the initial conditions imposed against debts are accepted by the public".

In the article in the book Privacy by Louis D. Brandeis and Samuel D. Warren "The right to freedom from interference" is synonymous with the right to privacy. The author states that with the progress of civilization, the effort and difficulty of life forced people to withdraw from the world, and at the same time, with the development of culture, the same people became less interested in public affairs. . sensitive, "so solitude and privacy become important to the individual"; but day-to-day trade and manufacturing inflict this upon him, subjecting him to more misery and stress than mere bodily injury could inflict. "The protection of personal writings and all other personal works is not only to prevent theft and misuse, but also to prevent publication of any kind"; The truth is not a method of private property, but the principle of the inviolability of the individual. Warren and Brandis interpreted existing law as solitary rock climbing left and right, such as deciding that thinking, thinking, and a thought should be communicated to others. The principle of this law is character immunity. Facts, thoughts, feelings, etc. the right not to interfere with attempts to prevent unwanted disclosure.

**RIGHT TO PRIVACY IN INTERNATIONAL LAW**

The power of human rights reaches its peak when there is an effort to unite it as a human right. With the establishment of the United Nations and the integration of human rights as an important issue into international law and policy, human rights began to receive greater attention at domestic and international conferences. International and regional agreements Privacy rights are recognized in many countries. "The importance of the right to privacy in this context is evident in almost all human rights discussions or debates". In modern human rights law, "the right to privacy is reflected in Article 12 of 1948 The Universal Declaration of Human Rights (UDHR) states": No right to privacy should be imposed on oneself, one's family, one's home or articles that are arbitrary and harmful to the honor and reputation. Everyone has the right to protection by law against harassment or assault. This article aims to create a legal framework that requires states to be responsible for physical and communication privacy in the international order. Additionally, the role is designed to encompass a wide range of human interactions and behaviors. These aspects of dignity include the right to dignity and family privacy. It is widely accepted that human rights have the aim of developing human character and protecting it from unjust interference. Therefore, confidentiality comes to the fore when trying to achieve the goals of human rights law. "Article 17 of the 1966 International Covenant on Civil and Political Rights (ICCPR) reaffirms that the right to privacy enshrined in the Universal Declaration of Human Rights is the right to enjoy the following legal protection:

1. "No one shall be subjected to arbitrary or unlawful interference with his or her private life, family, home or communication, nor shall his or her honor or reputation be unlawfully attacked".
2. "Everyone has the right to protect their rights against interference or attack. Article 14 of the International Convention for the Protection of the Rights of All Migrant Workers and Members of Their

Families uses similar terms in the context of immigrants and their families have the right to prevent interference with their family life and privacy". "Article 16 of the Convention on the Rights of the Child and Article 22 of the Convention on the Rights of Persons with Disabilities also aim to protect the privacy of children and persons with disabilities."
"On 30 June 2014, the United Nations High Commissioner for Human Rights' report on the right to privacy in the digital age said: The importance and associated privacy rights are widely recognized". The right to privacy and its importance is the enforcement of laws and practices.

**RIGHT TO PRIVACY IN INDIA**

"The Indian constitution does not specifically and clearly define the right to privacy. The right to privacy is not included as a fundamental right in the Constitution". "The right to privacy in the Constitution is understood from the expressions in Article 32 and the provisions of Article 33 of the Constitution". "Various issues regarding privacy policy and legal responses are discussed in detail in the following paragraphs."

**MP Sharma v. Satish Chandra**

In one of the most secret cases, "the search and seizure provisions of the Criminal Code are at issue. Rejecting the right to privacy, the Supreme Court, in its speech to the three-judge bench, ruled on the right to privacy if deemed necessary by the law procedure". The fundamental right to privacy is the same as the [U.S.] Fourth Amendment, and there's no reason why we should put it in a completely different law with some kind of heavy construction. The court ruled on the legality of the campaign, stating that the state had the authority to search and arrest for security reasons.

**Kharak Singh v. The state of Uttar Pradesh**

"A petition filed in the Supreme Court challenging the constitutional provisions of Article 22 (Rules 236 and 237) of the Uttar Pradesh The Police Law and many of its provisions give powers to the police because these provisions violate civil responsibilities under Articles 19(1)(d) and 21 of the Constitution. Court, J Frankfurt in Wolf v. Colorado security of personal privacy against police violation". It is the foundation of a free society. It is therefore implicit in the "idea of independent decision-making" and can therefore be used against states through appropriate procedures. Even knocking day and night is the beginning of a search without legal permission, relying solely on the police. "Recent historical statements that do not require punishment are incompatible with the concept of human rights in history. and legal documents of the English-speaking world". "We do not hesitate to say that any state that would prohibit such officers from intruding on privacy would violate the guarantees of the Fourteenth Amendment". The Court noted that: "It is clear that knocking on the door or waking the person will not interfere with or interfere with his movement" and therefore does not violate Section 19(1)(d).37 In our view, Section 236(a) Subsection (b) ) violates Section 21 and since there is no "law" to justify it, it should be entitled to protection. Justice Subba Rao, in his dissent, said that privacy by introducing "personal liberty" in Art. 21. SUBBA RAO, J.: "Furthermore, the right to liberty includes not only the right not to restrict one's movement but also the right not to violate law own life". "It is true that our Constitution does not clearly define the right to privacy as a fundamental right, but this right is an important part of personal freedom". All freedoms make family life sacred.

**Govind Vs. The State of Madhya Pradesh**

Govind v. M.P. The State Supreme Court provided more detailed information regarding privacy rights. In the Govind case, the Court considered the constitutionality of Articles 855 and 856 MP. Law enforcement enables the use of various surveillance systems. These provisions, Art. 21, Art. 21. The simple right to privacy is "made possible" by Art. 19(a), (d) and 21 were also approved by the Court. "However, the right to privacy is not absolute; Reasonable restrictions shall be determined in the public interest in accordance with Article 1. 19(5)." Therefore, MATHEW, J. observed in this case: "In every case, the right to privacy must go through a process of development in the particular case. Therefore, in India, even the right to personal liberty, the right to freedom of movement, and the right to freedom of expression constitutes a right to freedom of expression. Privacy can be made a derived law from these, a fundamental law. Yes, we do not believe that the law is absolute." MATHEW, J. also observed: "Documents relating to privacy and dignity deserve scrutiny and scrutiny and will be rejected only if the main conclusions of the discussion are shown to be more effective". If the court decides that this right is protected as a fundamental right to privacy, the law affecting this right must be satisfied in the national jurisdiction.

**Malak Singh v. The State of Punjab**

The Supreme Court considered the validity of certain checks under the Punjab Police Act. The judges recognized the need to balance the State's objectives of preventing terrorism, protecting public safety, and protecting freedoms under the law in articles 21 and 19(1)(d) and held that police custody should not interfere with personal freedom, dignity, or privacy. The court also pointed out that although preventing crime is in the public interest, monitoring for this purpose should not be considered "unlawful interference" in the lives of others. Observations should be limited to the realization of fundamental human rights. "Surveillance can be disruptive and seriously impact the public's privacy to the point of violating their rights," he said. Personal freedom is guaranteed by Article 21 of the Constitution, and freedom of movement is guaranteed by Article 19(1)(d). This is not allowed.

**R. Rajagopal v. Tamil Nadu State**

The Tamil Nadu case, popularly known as "Car Shank", has raised questions about the relationship between press freedom and the privacy rights of the country's citizens. The court drew attention to the following points in its decision. This is a "non-interference" rule. Citizens are concerned about themselves, their families, marriage, childbearing, parenthood, child-rearing, education, etc. has the right to protection. No one will publish the content of the above topic, whether true or not, praise or criticism, without my permission. If he does this, he will violate the privacy rights of both parties and the damage will need to be compensated. However, if the person is alone, his situation is different. Involve yourself in the conflict or invite others or cause the conflict. In other words, the above content will not be approved for publication as a public document (including court documents). Because once something is made public, the right to privacy is lost, it becomes a legal right of interpretation, and the news loses its currency. However, in the interests of justice, we believe there should be an exception to this rule: Women who are sexually assaulted should no longer accuse themselves of theft, robbery, embezzlement or similar crimes. Names and events published in newspapers/newspapers are slanderous. In the case of public officials, it is clear that the right to privacy, that is, their actions and behavior, affects only the effectiveness of their responsibilities, not how they will be paid during the trial. This is true regardless of whether the report is based on truth or falsehood, unless the officer proves that the report was made without knowledge of the facts. In this case,

it is sufficient for the defendant (the press or journalist) to prove that he did so after revealing the facts; Of course, if the advertisement is proven to be false and motivated by bad faith or personal vendetta, the defendant will have no defense and will be liable for damages. As noted in (1) and (2) above, it is clear that police officers enjoy the same protection as other citizens in matters unrelated to their duties. It is needless to repeat that the judiciary is protected by the power to punish contempt of court and the powers of the Parliament and the Legislative Assembly are protected by Articles 105 and 104 of the constitution. The Indian Constitution contains exceptions to this rule. (5) Sections 3 and 4 do not, however, mean that the Privacy Act 1923 or any similar provision or law will not be binding on the press or media. Authorities restrict or limit the ability of former officials to block the publication of news/information. This is part of the human right to freedom. Article 21 of the Constitution states that the state cannot exercise this right unless there is a public emergency or public security requires it. For this reason, we have no objection to the right to privacy being included within the scope of "right to life" and "right to personal freedom" in Article 1 of the Constitutional Bridge. Article 21 of the Constitution. Article 21 comes into play when the facts of a particular case give rise to special rights. The above rights will not be restricted except in accordance with the procedures established by law.

**People's Civil Liberties Union v. Union of India**

The Free Peoples Association (a non-profit organization) recently filed a lawsuit regarding the telephone case. According to Article 32 of the Constitution, there is public interest. The petitioners challenged the constitutionality of Section 5 of the Indian Telegraph Act, 1885, which allows the use of telegrams by the central or state governments in certain cases. A charge sheet has been filed with the Central Bureau of Investigation (CBI) regarding 'Call for intervention among politicians' (CBD). and other communications intended to influence the public interest in combating government violence and crime. The court was satisfied that the state had failed to enforce laws that prevented abuse of power. According to Articles 19(1)(a) and 21 of the Constitution, the power under Article 5(2) of the Indian Telegraph Act shall not apply in the interest of justice and equality. "Benefits" or "for public security" are "necessary conditions" for the application of Article 5(2) of the Law; the authorities cannot exercise the power by right, unless there is an emergency or the interests of public security require it. 49 The Court held that a state of emergency is a situation affecting public opinion and The term "public safety" refers to an event or situation where the public is at risk.

The court noted that if either of these two aspects are not met, phone tapping cannot be used by the central government, state government or competent authorities as necessary or in the interest of the nation and justice, even if they so desire.

**Hyderabad and Anr v. Canara Bank District Registrar and Collection Officer**

This was in view of the Maharashtra Control of Organized Crime Act, 1999 (MCOCA). 13-16 of the law. An objection was made to wiretapping in accordance with the articles. The court said, "Although interference in the conversation violates the right to privacy, this right can be limited according to the procedures prescribed by law." So the court needs to see what the process itself is. must be honest, fair and reasonable; It should not be arbitrary, capricious or oppressive. The Court held that these provisions constituted a "standard" established by law and Since Rule 16 provides for penalties for unauthorized users who obtain information, it has adequate procedures to prevent this from being unfair or arbitrary. by

interception of telegraph, electricity, or verbal communication. The court recognized the validity of illegal products:

1. it must be given due process; Cases recognized by Article 19 Cases examining fundamental rights that may apply in particular cases;
2. It will also be subjected to testing in accordance with Article 14.
3. The tender is deemed to have failed this test. More importantly, the court ruled that the concept of privacy applies to individuals rather than places. This statement means that it does not matter whether financial records are kept in pubs or banks. As long as financial information relates to an individual, the public's right to privacy protects it.

**Hinsa Virodhak Sangh vs Mirzapur Moti Kuresh Jamat & Ors**

The validity of the decision banning operations in slaughterhouses during Jain festivals has been questioned. The court said, "What you eat is private to the person and is part of the right to privacy in Article 21 of the Constitution."

**State of Maharashtra v. Bharat Shanti Lal Shah**

This is taken from the Maharashtra Control of Organized Crime Act, 1999 (MCOCA). 13-16 of the law. Articles. There are objections to wiretapping in these circumstances. The court said, "Even if interference with speech violates the right to privacy, this right can be limited in accordance with the procedures prescribed by law." said. Must be honest, fair and reasonable; It should not be arbitrary, capricious or oppressive. The court said these provisions were "standard" under the law and had procedures in place to prevent this from being unfair or unjust, as Article 16 provides penalties for unauthorized access to information. By interfering with telephone, electronic or verbal communications. Courts recognize the validity of illegal possessions.

**Judge Kuo Jiaxiang Puttaswamy v. Union of India**

The Supreme Court was considered an important authority in the decision of the nine-judge panel. However, some believe that this law is not correct, that the state is allowed to be limited to the conditions stipulated by the law in accordance with the types of legal purposes and to be allocated to the purposes sought by the state. To succeed. The court overturned M.P.'s decision. Sharma argued that the right to privacy was not protected by the Indian Constitution.

**Kharak Singh v. The State of Uttar Pradesh (UP)**

Writing for the majority, Chandrachud J. held that the right to privacy is protected by Article III of the Constitution. He argued that he was protected by the article. He said this was not separate from the other freedoms listed in Article 1. Chelameswar J., on the other hand, sees the right to privacy as three things: repose (protection from unnecessary transportation), residence (protection from surveillance) and decision-making (autonomy). personal life decisions). Nariman J. accepts Gary Bostwick's understanding of privacy as "rest, residence and discretion". He divided this idea into three categories: (1) influencing the government to obtain a person's body; (2) personal information affecting personal information for unlawful use; On the other hand, Kaur J.. It appears that private lawsuits can be brought against both state and non-state actors. For the state, it indicates the concern for monitoring and analysis, while for the non-state, it refers to the role of technology, especially the end-to-end collection and use of information. Digital

marketing. Kaul J. also discusses the impact of big data on human activities and the chilling impact it will have on freedom of speech and expression. That's why it decided to preserve some information about public and private actors.

**Bodily Privacy**

Indian jurisprudence provides immunity to medical records insofar as the right to privacy is concerned. However, this protection is qualified by the exception in the hands of courts, where non-disclosure may potentially endanger the lives of other beings.

In **'X' v. Hospital** 'Z'64, "the Supreme Court considered the scope of a blood donor's right to privacy in his medical records. The respondent hospital in this case had disclosed the fact that the blood donor had been diagnosed as an HIV patient without the consent of the blood donor. The lady who was to have married the blood donor had broken off their engagement as a result of the hospital's announcement, condemning the donor to societal ostracism. While medical records are meant to be private, the Supreme Court determined that doctors and hospitals could make exceptions in particular circumstances when the non-disclosure of medical information could risk the lives of other people, in this case, the wife's life. As a result, the purported intrusion was legalized based on another person's right to health."

In **Sharda v. Dharmpal,** the question for consideration was whether the Court could direct a person to undergo a medical examination in the course of matrimonial proceedings. The Supreme Court held that there is no absolute right to privacy. In this case, the conflicting rights were the right to seek divorce on grounds of unsoundness of mind of one party, which may require a medical examination, and the right to privacy of the other party. It was held that the Court could order a medical examination if the applicant has a strong prima facie case.

In **National Legal Services Authority v. Union of India** upheld the 'right to life' of the transgenders. It was held that "Gender identity, therefore, lies at the core of one's personal identity, gender expression, and presentation and, therefore, it will have to be protected under Article 19(1)(a) of the Constitution of India. A transgender's personality could be expressed by the transgender's behavior and presentation. The state cannot prohibit, restrict or interfere with a transgender's expression of such personality, which reflects that inherent personality. Often the State and its authorities either due to ignorance or otherwise fail to digest the innate character and identity of such persons. We, therefore, hold that values of privacy, self-identity, autonomy and personal integrity are fundamental rights guaranteed to members of the transgender community under Article 19(1)(a) of the Constitution of India and the State is bound to protect and recognize those rights."

In **Puttaswamy,** it is held that sexual orientation is an essential attribute of privacy. It is observed that, "Discrimination against an individual on the basis of sexual orientation is deeply offensive to the dignity and self-worth of the individual. Equality demands that the sexual orientation of each individual in society must be protected on an even platform. The right to privacy and the protection of sexual orientation lie at the core of the fundamental rights guaranteed by Articles 14, 15 and 21 of the Constitution."

**Women's Right**

The question of the rights of prostitutes arose in State of Maharashtra v. Madhukar Narayan Mardikar73 where a police officer was terminated from his job after engaging in deviant behavior with a woman. While the Maharashtra High Court decided that the woman's evidence could not be trusted, the Supreme

Court ruled in favor of a prostitute's right to privacy, stating that an invasion of private cannot be justified on the basis of a woman's easy virtues. Every individual has the right to privacy and anonymity.

The court was dealing with issues emanating from a departmental investigation into a police officer suspected of invading the lady in question's home and ravishing her while in uniform. While pronouncing the judgment preserving a prostitute's right to privacy, K. Jagannatha Shetty and A.M. Ahmadi JJ of the Supreme Court held: Even a woman of easy virtue is entitled to privacy and no one can invade her privacy as and when he likes. So also it is not open to any and every person to violate her as and when she wishes. She is entitled to protect her person if there is an attempt to violate it against her wish. She is equally entitled to the protection of law. Therefore, merely because she is a woman of easy virtue, her evidence cannot be thrown overboard. At most the officer called upon to evaluate her evidence would be required to administer caution unto himself before accepting her evidence.

In **Roe v. Wade**(1973), "the US Supreme Court established that a woman's right to an abortion was protected by the right to privacy implicit in the Fourteenth Amendment. In Suchita Srivastava v. Chandigarh Administration, 76 the question was regarding the abortion of a pregnant raped mentally retarded orphan woman. It was observed that, There is no doubt that a woman's right to make reproductive choices is also a dimension of 'personal liberty' as understood under Article 21 of the Constitution of India. It is important to recognize that reproductive choices can be exercised to procreate as well as to abstain from procreating. The crucial consideration is that a woman's right to privacy, dignity, and bodily integrity should be respected. This means that there should be no restriction whatsoever on the exercise of reproductive choices such as a woman's right to refuse participation in sexual activity or the insistence on the use of contraceptive methods".

Hence, the definition of privacy has been broadened to include a variety of specific examples of abuse of women's rights. In the era of contemporary law, the right to privacy has a substantial impact on women's rights.

## CHAPTER-3
## DATA PRIVACY
### Introduction

In the information age where we use digital tools for almost everything in our daily activities, we know little about the digital footprints we are forever creating. In his book Digital Man, Daniel J Solove explains how privacy is violated in the information age and how information can be stored forever. -An entrepreneur predicts that one day we will learn our likes, dislikes, interests and needs. We will categorize, analyze, categorize, every click of ours will be tracked. As we live more of our lives online, we build a solid record of consistency and depth. In fact, almost everything on the website is archived. One company even cleaned up all its Internet equipment and stored it in a large electronic warehouse.

Our online identity is reflected on our website and social media. We are used to things appearing and disappearing online, giving the impression that they are temporary. But when we delete or update information on the website, almost nothing is lost or forgotten. As our lives continue to digitalize in cyberspace, the amount of information stored will also increase.

### DATA AND BIG DATA

"Data is a record of observations behaviors, or patterns of characters that represent values. Readings, x-ray or scanner images, audio recordings, family charts, interview responses, hospital billing records, and

many other results from seeing, asking, hearing, measuring, recording, or scanning are just a few of the possibilities. 87 Almost all scientific information is now managed digitally, even if it must be written or translated from non-digital sources. Of course this will be very helpful in computer analysis. It is also possible to transfer materials from one place to another at near the speed of light and at low cost, which can be beneficial or problematic depending on how the materials are managed and used. The word "data" refers to information added to the translation to create meaning. Data and information are often used interchangeably."

"Section 2(11) of the Data Protection Act 2019 defines data as "data containing information, facts, ideas, opinions or instructions presented in a form suitable for communication, translated or processed by human or mechanical means;

Section 2 (28) Definition Personal information - means direct or indirect information about or relating to an identifiable person, including that person's characteristics, characteristics, behavior or characteristics, online or offline or a combination of such features with other information and incorporated therein for analytical purposes."

"Under Section 2(o) of the Information Technology Act, 2000 Information - in accordance with law means information, information, facts, ideas, or instructions prepared or prepared and intended to be implemented and implemented in a computer system or computer network. implemented and in some form (magnetic or optical fiber storage media computer printouts, punch cards, perforated tapes) or stored in computer memory."

Yvonne McDermott, in her article Conceptualizing Data Protection Rights in the Age of Big Data, states: "that this is a well-known concept (Ward and Barker, 2013), but there is a large amount of information about data protection rights. lesson. The characteristics of the dataset were analyzed: data volume, collection speed, data diversity, accuracy of the data (permission to link to other data clocks), and complementarity (Kitchin, 2013: 262). The International Business Machines Corporation's definition is: Big data is not about data, it is data. Philosophy is not just about language. Big data refers to the value that can be extracted from the data or the meaning contained in the data. The true meaning of the term Big Data is given by the fact that data is available faster, from more sources and in more formats than ever before. We should call this "big data" because big data is actually about the value (meaning) in the data, not the data itself."

"The Internet of Things (IoT) refers to sensors and systems that collect and store data built into everyday products such as refrigerators, cars, especially self-driving cars, methods, pacemakers, and watches. It also allows data to be sent to other products or systems, often over the Internet. All these collected data are brought together to create data called big data."

In a report to the White House, 96 The Internet of Things was defined as:

"A term used to describe the ability of devices to communicate via telephone and wireless using interconnected devices. These tools may include your thermometer, your car, or the medicine you swallow so your doctor can monitor your bowels. These connected devices use the Internet to transmit, collect and analyze information."

"The number and complexity of the site and structure is increasing. It includes public meetings, teleconferences, mobile communications, federal, state, and local records and data centers, data business documents that include proprietary data from a variety of business and public data, geospatial data, surveys, and traditional data, to name just a few. scanned into electronic form. As more and more network-enabled devices and sensors become available, the ability to collect information from sources such as

detectors and radio frequency identification (RFID) chips is expanding. Personal location information can be obtained using GPS devices, cell tower triangulation, wireless network mapping, and personal payments."

Huge amounts of data are created and collected every day. Millions of people interact using computers, cell phones, and other electronic devices. Online or mobile banking, social media, and other global processes now generate more than 2.5 quintillion bytes of big data every day.

Big data provides information about individuals that was simply impossible to know a generation ago when large amounts of data were collected and integrated. It quickly shows who the person talked to, what he said to him, where he went, where he went, who he worked for, where his relatives were, what he ate, what he bought. It shows interests, hobbies, finances, work and even criminal history. Complete profiles can be combined.

**DIGITAL AGE AND PRIVACY**

In the online community, individuals appear to be both academic and self-important at the same time. The quantified itself depends on large data collection mechanisms that enable people not only to be willing to learn the technologies of measurement and calculation but also to participate in the process of quantification as the representational system of technology that controls the functioning of the body. The curriculum is about personality, but it specifically refers to the way people perceive teaching, personality, thinking, and communication through technology, work and language work in the field of life.

Technology is making the world interconnected. Nowadays, technology has become an important part of our daily activities. Our shopping habits have now changed to online shopping We shop for groceries from nearby stores, we book flight, bus or hotel tickets online Instead of relying on travel agencies, we buy medicines, and e-books online, it can be with "service" or "cash" Now the Internet is used for communication, purchasing goods and services, business, etc. It is used for. Google answers every question we have within seconds. Internet usage has increased since the outbreak of the Covid19 virus in March 2020 and its nationwide shutdown to date. Over the years, traditional education, where children could go to school in person, has turned into e-school, where children can receive education online. This allows students to complete online courses using devices such as smartphones, laptops, or tablets. Meetings that require a speaker and participants are now moving online using apps like Zoom, Google Meet, and more. Governments around the world are starting to use digital tools to track and trace the coronavirus.

Although the Internet has many benefits, its impact on user privacy is often overlooked Every website we visit and every change we make is online, often without our knowledge. This website contains user-related information. But these information silos can seem inconvenient on their own. But collectively they share characteristics such as behaviour, diet, language, health, hobbies, sexual preferences, clothing, relationships and family, politics and religion.

Popular websites install cookies from users' browsers. Cookies can be used to register the browser with a unique identifier that allows the browser to quickly recognize the user and preserve information about their online activities. User profiles are created using data, specifically users' browsing history. Algorithms enable the creation of user profiles on the Internet. Reading user emails is usually done by automatically analyzing the content of the email. A person's interests can be calculated via email and the user can be presented with appropriate advertisements on Windows websites. Books people buy online often focus on ads in the same category. Even a ticket purchased in business or business class can reveal important

information about the employee and his business results. Online booking for a taxi ride to the mall makes the customer profile more attractive. A woman who bought pregnancy pills online will be accused of advertising baby products. Electronic surveillance of people's lives has become the norm.

US Supreme Court, **Whalen v. Roe** states:

"We are not aware of computerized databases or other threats to privacy affecting the large amounts of personal information collected in important government records.

Taxation, distribution of health and social security benefits, public healthcare, military administration, and the enforcement of the law as a whole to ensure the privacy of most of these. Because it is personal, disclosure may be embarrassing or damaging. -

Daniel Solove explains how privacy is compromised by the aggregation of "less valuable information" as colors combine to create "detailed pictures of ourselves and our character." 105 Solove calls this problem "collective," noting that businesses and governments often collect a lot of information, including our own. Drawing such a portrait cannot be considered a separate, special action.

He explained: "As lawyer Julie Cohen stated, the amount of information about a person is greater than the number of places he has been. I bought this phenomenon called Seurat's paintings many points side by side The data collected can create a picture of a person or create a digital book about us. Incorrect information can sometimes be a missing link, an important item in a person's digital history, or a key needed to unlock another store's personal information. As legal expert Stan Karas points out, the things we use tell us who we are.

In Chapter 108, Christian P. Monodidis describes certain characteristics of data that make privacy violations difficult to detect. - The challenge of personal information stems from the nature of information: it is non-competitive, invisible, and non-repetitive. These features make it possible to blindly observe damage to personal data. First, the data is negative because the positive can be used simultaneously; that is, one person's use of information does not reduce its access to others. Additionally, it is difficult to verify the personal information entered as it may not be visible. Information may be accessed, stored, and published without prior notice. The ability of data to travel at the speed of light increases the confidentiality of data entry, which means data collection will be the fastest form of theft. Therefore, the invisible and unchallenged consumption of data leads to serious privacy breaches without any consequences for the affected individuals. Additionally, the data is restructured: that is, the output data can be used as a tool to generate more output data, etc. For example, by developing applications called knowledge discovery and data mining techniques, data can be combined to "create the truth about an individual, specifically the likelihood that an individual will engage in certain behaviors." Creating new information violates the data privacy policy because it involves information that the individual does not have and could not otherwise know or disclose. Moreover, as our country becomes a more information-based "media nation"—information is defined as "the life force that supports political ownership and social and business decisions"—it becomes impossible to consider all the possibilities of data use and use. damage. This situation makes the job of the courts difficult, which should be effective and fix the invisible rather than causing harm.

The change made it easier to obtain images that were previously publicly available but difficult to obtain. New technology that expands understanding has already provided new insights through covert "observation." This surveillance allows personal data to be collected without consent or knowledge, thus creating a feeling of abuse. Changes in business models are increasingly focused on the idea of greater

customization of services and products, the process that requires the collection of large amounts of personal data to provide the necessary customization.

## POTENTIAL HARM

Moira Paterson and Maeve McDonagh discuss the implications of personal data collection.

Big personal data is a problem for privacy because it removes people's ability to control their data and therefore affects their freedom (i.e., to "live and organize their lives the way they want"). The concept of autonomy is central to liberal thought.

Christman defines personal freedom as "a generally understood concept that refers to the ability to be an individual, to live according to one's own reasons and motivations," rather than being the product of control or outside influence. "Except for the analysis of data collected and used with the consent of the person concerned, big data belonging to the person does not lead to data freedom in the processing of information; it also facilitates activities and transactions that control the person himself. It furthers decisions, leads to independence, is a tool of analysis and decision-making." It facilitates acquisition, increases transparency, and diminishes human dignity. An example of its use in political advertising.

Allegations about the use of analytics to influence the outcome of the Brexit referendum in the UK and the 2016 US presidential election are good examples of this. Cathy O Neil thinks that the practice of data analysis is common in politics. Political programs generate scores based on potential voters—their likelihood of voting for a party, their orientation on a particular issue, and their support for that issue. Politicians use asymmetric information to control votes or donations.

For example, in the United States, Walmart uses “sales, price, and financial data, as well as demographic and weather data, to adjust inventory and make forecasts Decisions based on large personal data are the same Individuals and groups may also be subjected to different conditions (for example, price discrimination based on different discount rates). This includes discrimination because it allows decision-makers to distinguish between individuals that could be used as a basis for differential treatment. Although this practice occurs in some industries, such as insurance, big data allows them to use more information that was not previously available. This raises an important question:

Is there a "difference" beyond existing protection against discrimination that cannot be ignored? Today, businesses need all the user data they can get their hands on, and efforts to find information are far from independent. The data collected goes beyond the customer's opinion of the products and includes customers' own characteristics, such as details of their lifestyle and even mental health data.

## DATA COLLECTION BY STATE

After the 9/11 terrorist attacks in the USA, the public called for national security measures to be taken. It can be seen as an important factor limiting the state's oversight of national security and international security.

Edward Snowden's revelations in 2013 made it clear that the NSA was monitoring its citizens' phones. Richard A Posner, in his article "**Privacy, Surveillance and the Law**", explains how government data surveillance can help protect national security. He said if people's records are digitized, compiled and searched electronically, it will reveal connections and interactions between people. 116 Intelligence officers will be able to access information that will be useful in analysis. Track terrorist groups' members, networks, and financial resources.

He observed: Stealth is the bad guy's best friend, and bad guys' stealth is enhanced by the same technological innovations that both enable data mining and enable the exfiltration of innocent people. A lot of personal information is obtained from the Internet: the Internet relies on its anonymity, and the secure encryption of digital data, together with the anonymity, makes Internet Nem a powerful tool for integration. The government must urgently use digitalization to protect the country's security.

Judge William O. Douglas, Osborne v. United States, says: There may be a time in the future when no person can decide whether his or her conversation will be recorded; when everyone will fear that his secret thoughts no longer belong to him but belong to the government; Confidential and intimate conversations are always open to willing, listening ears. At this point privacy and the freedom that comes with it will disappear. If a person's privacy can be violated at will, who can say that he or she is free? Who can say that he loves freedom of expression if his every word is recorded and measured or his every word is feared? If every conversation he makes is known and recorded, if his conversations with participants are hacked, who can say that he is enjoying the freedom of association? When this happens, our citizens will be afraid to speak outside the safest and most orthodox views; The freedoms provided by the Constitution will disappear.

Besides national security, there are other reasons for the state to collect and store information.

Information is collected for administrative purposes, including appropriate resource allocation, crime control and budget allocation. Identifying this information can ensure law enforcement and prevent others from stealing it. In case of health, it is inevitable to collect, store and analyze data to complete the work.

**DATAVEILLANCE**

In his book "**Digital People**" Daniel J. Solove discusses the concept of "data surveillance" and its consequences.120 According to legal expert Jerry Kang: Information on the Internet is stored in a detailed information file. source. is computer-processable, self-indexing, and permanent. Combined with the fact that cyberspace makes data collection and analysis exponentially cheaper than physical space, we get what Roger Clarke sees as the threat of “data surveillance.”

"Data analysis, as stated by technology expert Roger Clarke, is the use of personal data when investigating or monitoring the behaviour or communications of one or more individuals. According to political scientist Colin Bennet, the term "surveillance information" was coined on a large scale large used to describe the practice of observation that facilitates the collection and storage of large amounts of personal information. “Therefore, data analysis is a new form of observation; It is a method of observation done not through eyes or camera, but through collecting facts. and information. Kang believes surveillance is an attack on human dignity.

The opposition is interfering with free elections because it "leads to self-censorship". Likewise, Paul Schwartz argues that information gathering “can limit the ability to choose freely: The more you know about someone, the easier it is to coerce them into following.” The problem with the data, on this view, is this. They are a form of surveillance that limits personal freedom.

Jeremy Bentham's modern version of the "panopticon" - a panopticon consisting of cells arranged around a central wall that allows observation of prisoners without their knowledge, is called performing data analysis.

"Big Brother is watching you," George Orwell warned in "1984". Orwell wrote that television cameras and microphones are modern surveillance tools. But what Orwell did not know was that the digital computer was a better surveillance tool that could be used by the government and the private sector for

this purpose. Adam De Moore points out that video surveillance, GPS, biometrics, and data analysis can provide police officers with monitoring tools without burdening people.

In the **United States v. Jones,** Judge Sonia Sotomayor noted that the new method of surveillance does not require a physical search or access. It has been shown that "GPS tracking can generate accurate and detailed information about a public official, including family, political, employment, religious and sexual relationship details."

The trips presented in the profile will not raise suspicion and should be given some consideration: visits to the psychiatrist, plastic surgeon, abortion clinic, AIDS clinics, strip clubs, criminal defense lawyers, hotel hours, and union meetings. , mosques, synagogues or churches, gay bars and more... The government can save such information and my good information for the future. Information dating back many years… is classified as classified information and can avoid the same scrutiny that limits criminal law enforcement: "limited resources, no police, and no public violence"…. Attaching a global positioning system (GPS) device to a vehicle and using it to track the car's movements is unanimously considered Fourth Amendment research.

**DATA PRIVACY**

In the article "Privacy in the Digital Age" the author believes that "digital privacy for individuals is about the ability for individuals, companies to create an online identity and decide when, how and where to communicate it." Symbols of other selected fields. The freedom to establish one's identity online is central to the concept of privacy; In practice, it is the ability to create and edit digital images that influence one's interests.

Mark Burdon draws attention in his book "Digital Data Collection and Information Privacy Law". Regarding the Privacy Policy, the Information Privacy Law ensures the protection of many lives, starting from the moment the data is collected until the moment the data is collected. data is no longer destroyed or de-identified. Currently, data collection organizations need to complete a variety of tasks. Personal information is generally used only for a clearly defined purpose that the individual fully understands.

There is an interactive process designed to enable management by giving individuals the ability to verify the accuracy and value of personal documents. When personal data is collected and stored, it must be kept confidential. - When collecting personal data, the organization collecting the data must act in accordance with data integrity. Data ethics are the standards of practice that organizations that collect and use personal data must comply with to ensure the security of the data. These practices include notifying individuals of their personal information and knowing that their information is being collected, giving people choices about how their personal information will be used, and allowing individuals to review and object to information recorded about them. Notify them in a timely and cost-effective manner and take steps to ensure that the information collected about them is accurate.

Consider what rules might protect businesses' privacy regarding online information The FTC defends federal law against this issue The law requires commercial websites to use four ethical principles: Notice, Choice, Access, and Security, which were initially adopted by many government agencies. It was developed with the concern to consider the impact of the rapid growth of computerized data centers on the private sector. When applying for online content, the Notice requires commercial websites to disclose to their visitors not only how personal information is collected about them, but also how data will be collected, even if those sites do not collect information. Reasonable options include allowing online consumers to decide whether the information they provide to a website for a particular purpose can be

used by that website for other purposes. While access to policies allows customers to control and, if necessary, correct the information collected about them by certain websites, security means that websites must prevent the private information they collect from leaking into unauthorized hands.

**RIGHT TO BE FORGOTTEN**

The book "Erased" 131 begins with the story of Ms. Stacy Snyder. Woman. Stacey is a 25-year-old mother who has all the qualifications to become a teacher. School officials called him and told him that the certificate was denied due to his "disrespectful" behavior towards his teacher. The school's reasons for making this decision are surprising. He posted a photo of himself wearing a pirate hat and drinking from a plastic cup on the "MySpace" platform under the name "Drunk Pirate". Guilty person. After the incident, he tried to delete the photo. But the damage was done. The website remembers what Stacey wanted to erase, erase and forget.

Since the birth of the Internet, the current situation and information about people has changed a lot. Newspapers and official or government documents are no longer part of personal information. All pages or activities we like, favorite or share and our use of social media, Twitter micro-discussions, photos and videos that we or others tag in our uploads and all pages or events we like, favorite or share; It contributes to our digital footprint. When you consider information not produced by us, but created by public and private organizations that hold individuals' information in their databases, our Shadow digital image starts larger than the data we create. We indeed live in a big data environment where algorithms track the repetition of our digital identity. The reason for this is the system that allows some of the digital shadow to be removed.

**Google Spain Case**

Mr. González asked the Spanish Data Protection Authority to remove searches for the name on Google. The results were also reflected in the newspaper pages of a campaign to pay off the debt incurred years ago. Mr. Gonzalez believes that with the passage of time and the resolution of the relevant cases, all references to these cases become obsolete. While Spain's Data Protection Authority rejected the lawsuit against the publication, it also approved the complaint against Google. The document has been removed from the Google index and is prohibited from being accessed again. Google demanded that the decision be reversed. The Spanish court then referred several questions to the Court of Justice of the EU. The court ruled that Google had "perfected" personal information by allowing any internet user to obtain information about a person by searching for that person's name on the website. There is also information about many aspects of Mr. Gonzalez's personal life and cannot be linked or found without the use of a search engine. According to the court, search engines make information "everywhere", causing a violation of personal privacy. The "simple financial interest" of business owners does not appear to have a significant impact on individual rights. In this case, the court found that even information permitted by law may be contrary to the laws at that time. This will occur if the information is "insufficient, irrelevant or excessive... to the extent that it affects the purpose of the work." not kept up to date or… kept for longer than is necessary for the reason for which the information was collected or processed. "The Court ruled that the majority of the European Charter's right to privacy should give priority not only to the involvement of research employers but also to the interests of the public.

The right to be forgotten "Some data of a person has been erased so that third parties can no longer track it." It stands for "the right to no longer experience past life events, the right to remain silent." The right to

be forgotten allows a person to delete personal data, information, videos, or images from certain online documents so that they no longer appear in searches. The difference between the right to be forgotten and the right to privacy is that privacy means information that is not publicly disclosed means while the right to be forgotten refers to information that is not publicly disclosed. to remove previous information and prevent third parties from accessing this information.

Theoretically, the right to be forgotten solves the fundamental problem of the digital age: Since every photo, status update, and tweet is always stored in the cloud< It is difficult to delete your online history. However Europeans and Americans used different approaches to the problem. In Europe, principles of the right to be forgotten can be found in French law, which recognizes le droit I l'oubli (i.e. "the right to be forgotten"), the right of a criminal who has served his sentence. and was rehabilitated to combat publicity. The reality of conviction and imprisonment was restored to society. A historical example of misuse of archived data is described in "The Forgotten Virtue of the Digital Age."

In the 1920s and 1930s, the Dutch government established a civil registry to record its citizens' names, addresses, dates of birth, religion, and other personal information. The purpose of creating the list is to facilitate administration and policy development. However, when the Nazis occupied the Netherlands, they took over the registry office. It was misused to identify, locate and persecute Jews. The records made it easier for the Nazis to identify Jews, so the Netherlands suffered the most persecution. The author stated that citizens trust their governments and do not know what our future will bring, and warned that this could happen in every country.

**RIGHT OT BR FORGOTTEN IN INDIA**

The right to privacy includes the right to be forgotten. The right to be forgotten poses a legal challenge in India. Despite the importance of this law, the Indian Information Technology (IT) Act, 2000 (as amended in 2008) and the IT Rules, 2011 do not contain such provisions. The high court took up the dispute.

**Dharamraj Bhanushankar Dave Vs. Gujarat and other regions.**

The Gujarat High Court published the India Kanoon judgment, which is an "unpublished decision" and is presented in search results by Google. The complainant alleges that this conduct violates Article 21. The complainant alleges that Google and Indian Kanoon do not have the legal right to issue orders without notice, which would cause harm to him and his career. He added that as a result of the statement, the decision went viral, which was contrary to the court's classification. The court stated that "The decision to appeal is part of the proceedings and the decision was made by the court, so it is only published on the website does not include published, because the terms used for the Order are: The term "published" refers to legal journalists refers to the publications he published." The court confirmed that the removal decision had no legal basis and that the decision was made over the Internet. does not violate the petitioner's Article 21 rights.

**Sri Vaunathan v Registrar General**

The petitioner's father filed a petition in the Karnataka High Court seeking an order not to include his daughter's name in the decision because the name may be related to the previous incident and if anyone searches the name through an Internet service such as Google or Yahoo, this decision will be affected by the results. The petitioner's daughter fears that this will ruin both her marriage and her reputation and goodwill in society.

The court believes that "this is based on the 'right-wing' model in Western countries." It is generally "forgotten" in sensitive cases involving women and sensitive issues involving abuse or affecting dignity and reputation. from interested parties. " The court ordered the registrar to do everything to ensure that an internet search of public records does not return the dissatisfied girl's name in the file name of the petition or in the summary judgment Kerala High Court' 's Judgment in Civil Petition No. 9478 of 2016 The Kerala High Court declared the "right to be forgotten" in an order dated February 23, 2017. In the present case, the petitioner filed a writ petition in the Kerala High Court seeking protection of the right to privacy under Article 21 of the Constitution. The petitioners asked the court to protect their privacy and remove or remove all products displaying their names on Indian Kanoon, Yahoo, and Google. Due to the seriousness of the case and even after receiving notice, Indian Kanoon could not appear in court.

**Zulfiqar Ahman Khan v. Ms. Quintillion**

The petitioner approached the Delhi High Court seeking to quash the information published about her by the respondent in the wake of the #metoo campaign. Recognizing the plaintiffs' right to privacy, including the "right to be forgotten" and the "right to be left alone," the court ruled that the entire contents should be disclosed. The text of the article was first published on 12th October 2018 and Any quotation/or content of Article 31 and any modification thereof in any publication or digital/electronic platform will be prohibited during the pendency of this case.

**Subhranshu Rout v. Odisha**

The Odisha High Court rejected the bail application of the accused who attacked a woman and posted the video on the social network. The court did not allow. Respecting the right to be forgotten and imprisoned, "However, publishing objectionable photos and videos on social media platforms without the consent of women is a direct insult." Respecting the behavior of women, and more importantly, respecting their privacy. In such cases, the victim himself or the plaintiff may, if agreement is reached, request that appropriate measures be taken to protect the victim. He may violate the right to privacy by seeking appropriate action to eliminate these attacks by removing them from the website. Public platform regardless of ongoing violations.

**Karthick Theodore v. Madras High Court**

The name of an accused who was acquitted when the Madras High Court refused to say that the name had been removed from the trial court. The Court noted: "In fairness, this Court believes that our system of criminal justice has not reached a standard by which courts can operate by returning the name of a suspect based on a procedure written by rules or regulations. It will be necessary to wait for the adoption of the Data Protection Law and its rules, which can ensure an objective process when dealing with the protection of the names of the rightful persons being sued in a criminal case. If these standards are not complied with throughout the country, the Constitutional Court will be on the wrong horse and this will affect the current system.

**RIGHT TO BE ERASURE**

In most legal systems, the right to erasure is linked to the right to be forgotten or to be forgotten. Article 17 of the GDPR provides for the right to erasure, also known as the right to be forgotten. However, under the Data Protection Act 2019, the right to be forgotten and the right to erasure apply in many cases. Article

18 of the Privacy Law provides for the "right to correction and deletion", and Article 20 provides for the "right to be forgotten", which will be discussed in the next section.

## CONCLUSION

With the development of the digital age, we rely on the Internet and the services it provides. Although we have managed to use technology in many situations, we would not be wise if we did not know about the transition to an electronic lifestyle. 157 Most of the time we do not know that our information is being recorded. Personal information is an important part of human dignity and personal freedom. We have the right to know whether the information collected is used by government agencies or private organizations. Stable information is not necessary for a developing society. People enjoy the virtue of breaking and moving forward in life. Quote from Friedrich Nietzsche: "It is easy to live unconsciously." For a better future, some things need to be forgotten and some things need to be remembered. This law bans the digital sending of data to some extent forever.

In the age of innovation, a post or tweet may eventually become part of the web forever; On the other hand, information is needed to protect the public interest. Yes, privacy should be protected without jeopardizing people's peace, harmony, and security.

# CHAPTER-4
# DATA PROTECTION IN VARIOUS JURISDICTION

## INTRODUCTION

As digitalization grows exponentially everywhere, the need to protect data also increases.

The focus of governments around the world has shifted from controlling cyberspace to protecting civil rights. Although most developed countries such as India are still in the early stages of developing legislation, many developing countries such as the UK, Australia and the USA have set standards in this area. The US has constitutional and multi-governmental laws to protect privacy, the UK Data Protection Act 2018 has its roots in the EU GDPR, and Australia's privacy policy is based on the OECD Principles.

## DATA PROTECTION IN THE USA

United States data adopted an approach to protection. There is no significant information regarding the government's conservation policy. In contrast, federal law protects products in certain industries. These regulations apply only to certain activities, such as "health care, education, communications, financial services (and minors in written records)."

In other words, most privacy laws in the United States prohibit the processing of information based on the context in which the information is used (such as healthcare, banking, and education). In essence, private government in the United States is both substantive and operational, based on constitutional and federal legislation. and state law and often rely on private law or subsequent agreements enforced by federal or state law. 161 The Federal Trade Commission (FTC) is responsible for enforcing federal laws, but state attorneys general are also involved in protecting consumer privacy. 162 The Principles of Justice provide a procedural framework. WE. Department of Health, Education, and Welfare163, later incorporated into the US Privacy Act of 1974.

## THE FOURTH AMENDMENT

The Fourth Amendment to the US Constitution outlines the limits of privacy rights in the US. It protects

people from "unreasonable searches and seizures" by the government. Katz v. United States, The Supreme Court held that the government's denial of phone booths exceeded the defendant's expectation of privacy; this was perhaps made possible by protecting blocked people from Norms. Personal information under the Fourth Amendment, the reasonableness standard, and the privacy test. Therefore, in the United States, special requests are evaluated according to the standard of "two objective third parties," that is, "appropriately sensitive" persons.

The Supreme Court has also considered individuals' right to privacy on issues such as birth control, homosexuality, and abortion as a shadow of rights derived or influenced by the Constitution. These are also known as "unenumerated" privacy rights.

## SECTORAL LAWS

Most states have adopted privacy laws, either through statute or statute or through interpretation of state laws, to ensure privacy rights in the United States.

Privacy violations include access to privacy, public disclosure of private information, abuse, and misinformation. These restrictions protect four different human rights, all of which revolve around “the right to be alone,” as Samuel Warren and Louis Brandeis put it in an 1890 law review letter. Required provisions in both the United States constitution and the First Amendment restrict the right to privacy.

The most unique aspect of US privacy and data protection law is its function. or administrative district. US civil law/regulation is generally a guide. For example, different rules apply to the processing of information by government agencies and private companies. Also in various business affairs or management of various types of legal documents. Accordingly, regional laws are defined as necessary to protect the processing of different/various data, from consumer transactions to administrative regulations, and legal and medical records management. 180 In short, sectoral policies and regulations address threats to privacy and data protection as specific to certain types of business information or technologies.

## FEDERAL TRADE COMMISSION

The Federal Trade Commission (FTC) regulates the processing of personal information in the United States and plays an important role in protecting the privacy of the US public's used goods. It does this primarily through Section 5 of the Federal Trade Commission Act, which gives it the authority to freely regulate and enforce unfair and deceptive business practices. The FTC has the authority to issue injunctions and civil penalties against companies that violate consumer privacy rights and now “enforce privacy laws.”

While the FTC has been praised for influencing the behavior of large companies, it has also been heavily criticized for failing to pursue scandals that raise privacy concerns, such as the Facebook online survey.

The way. The FTC is the primary regulatory agency for federal privacy laws such as GLBA, 224 FCRA, 225, and COPPA. In recent years, it has played a key role in protecting consumer privacy, resolving disputes, and settling with companies accused of violating privacy laws.

There are many state laws as well as government laws. The most relevant here is the California Consumer Privacy Act (CCPA) California's implementation of the CCPA is a privacy law that critics have called "California's GDPR."

## CALIFORNIA CONSUMER PROTECTION ACT

The most significant bill to date in which the United States has recently achieved significant privacy. Bec-

ause California is so large and home to Silicon Valley, businesses across the United States and around the world are evaluating what this means for them.

CCPA is broad. The CCPA went into effect on January 1, 2020, and quickly became the most restrictive privacy or data protection law in the United States. The CCPA applies to fundraise organizations that do business in California, collect or decide to process personal information and fall into one of three main categories. Enforces nondisclosure obligations for businesses that collect personal information from California residents. It requires companies to provide California residents with the ability to access and delete their personal information, as well as the ability to opt out of having their information sold to third parties.

Prohibits companies from selling personal information of children under 16 without their express consent. The CCPA establishes a privacy action policy to address certain data breaches that result from a company's failure to follow and enforce policies and practices.

The California Attorney General has the authority to enforce the provisions of the CCPA and impose fines of up to $7,500 per violation.

**DATA PROTECTION IN UK**

In the UK, the main data protection law until 2016 was the Data Protection Act 1998230 (DPA 1998). DPA 1998 was prepared to implement the UK EU Data Protection Directive (DPD) 1995 law. 231 In 2016, the European Union's General Data Protection Regulation (GDPR) was announced, which abolished DPD. The UK Government transposed the General Data Protection Regulation (Regulation (EU) 2016/679) into UK domestic law after Brexit (renamed “UK GDPR”). To reflect its status as UK domestic law, the UK has made various changes to the GDPR (for example, changing the phrase "member states" to "United Kingdom").

The Data Protection, Privacy, and Electronic Communications (Amendment and Other Provisions) (EU Exit) Regulations 2019 apply to making these changes. Currently, all key obligations of controllers and processes in the UK GDPR and EU GDPR are essentially the same. Section 233 of the Data Protection Act 2018 ("DPA") continues to apply as national data protection legislation in addition to the UK's GDPR legislation. This refers to issues that previously allowed exceptions and exclusions under the EU GDPR (for example, citizens have an interest in the processing of certain data and certain content exemptions from GDPR conditions, such as data rights GDPR and This DPA 2018 The new data protection administration is like the government it replaces, although some changes have been introduced. DPA 2018 is divided into main areas: Employment Law, Legal Affairs, Intelligence Services, UK Data Protection, Data Protection Agency Operation (ICO), Operation and Additional Services and Final Terms.

The Privacy and Electronic Communications (EC Directive) Regulations 2003 (Replaced by the Privacy and Electronic Communications (EC Directive) (Amendment) (2011 Regulations) (PECR) regulates direct marketing, but The European Commission, which is also working on location and traffic data and the use of cookies and similar technologies, has introduced legislation on privacy and electronic communications (the Privacy Directive) to replace the Privacy Directive, as the Privacy Directive has not yet come into force, Although the UK Brexit There is also a question whether it will comply with the law after.

Main changes in e-Privacy rules:

1. It will make it more difficult to obtain consent to cookies.
2. Try to shift the burden of consent for the use of cookies to the web browser.

3. Making it difficult to obtain consent for direct marketing and requiring it to comply with GDPR standards; however existing exemptions will remain.

**The Data Protection Act 2018** governs the use of Personal Information by organizations, businesses, or governments. The Data Protection Act 2018 consists of four parts, which create four different "data protection regimes" in the UK:

1. The first part is built around the European GDPR, complementing it and translating it into UK domestic law.
2. Secondly, it goes beyond the scope of the EU GDPR and sometimes adapts it to apply differently to UK law.
3. Chapter 3 will create a new divide for authorities. 4. Chapter Four created new freedom for British intelligence.

The Data Protection Act 2018 also adopts the main definition of the EU GDPR239, for example:

- Personal data 240 means: information relating to identity or identity checks, checks the identity of a person. processing, writing, recording, storing, presenting, combining, etc. It means "an operation or operation performed on data".
- Information content A living person whose personal information is affected. Controller and Processor Meaning A natural or legal public authority, body or other body which, alone or jointly with others, decides on the purpose and means of the processing of personal data.

DPA has set some basic principles called "**Data Protection Principles**". They

1. The first principle of data protection is that the processing of personal data for all legal purposes must be lawful and fair.
2. The second principle states that the purpose of collecting information must be specific, legitimate, and clear.
3. Our data protection principle is that personal data processed for all administrative purposes must be adequate, relevant, and not overly relevant to the purposes for which they are processed.
4. The fourth principle provides for the deletion or correction of inaccurate personal data.
5. Article 5 of the data protection law stipulates that personal data processed for any legal purpose cannot be kept longer than the period necessary for the purpose for which they are processed.
6. The sixth data protection principle is that personal data processed for all administrative purposes should be processed using appropriate procedures or appropriate safeguards to ensure that personal information is secure. twenty-four

**RIGHT OF THE DATA SUBJECT**

The DPA gives to the Information Commissioner's Office (ICO) to comply with the UK's data protection law. The bill provides for ICO.

DPA 2018 to be administered by the ICO, and the ICO has enforcement power against organizations that comply with the data protection rules in the GDPR.

The ICO is independent and is responsible for

a) maintaining public records of regulators
b) promoting good practice by providing data protection advice and guidance and working with organizations through audits, consultations. Access and Data Protection Seminars

c) detecting complaints
d) Monitoring management to strengthen data practices.

- **Data Rights**

Data subjects have rules governing the processing of their personal data, similar to those in the EU GDPR. By default, the controller must publish action-related information in response to the request within one month, and if the request does not work, the controller can extend this period by another two months to connect.

- **Right of access**

The individual has the right to access and obtain a copy of his/her personal data, including data to consider how the controller will use this information.

- **Right to rectification**

The Labor has the right to correct or amend inaccurate or incomplete personal data as soon as possible.

- **Right to erasure ("Right to be forgotten")**

The individual has the right to have his personal data erased. Law is not absolute; used only in certain situations; It is used, for example, because the controller does not lawfully need additional information for the purpose for which it was collected or processed, or because the controller's actions to complete the strike or withdraw. right to leave.

- **The right to restrict processing**

In certain cases, the data subject has the right to restrict the processing of his or her data. These conditions include the accuracy of the application documents, illegal work, documentation that is not required other than official documentation of the study materials, or if the legality of the content of the study is questioned portability of information Act.

The educational information has the right to receive or transmit to another controller all personal information about him/her in a commonly used and machine-readable format; how the authority to act is legal, even on the basis of the work, or where the process is important for the performance of the contract.

- **Right to object**

If the legal basis for processing is the legitimate interests of the data controller or the public interest, an individual has the right to object to processing. Administrators must withhold work until they can demonstrate “good cause” for work that exceeds the requirements of the curriculum. In addition, the data subject has the right to object at any time to processing of personal data for direct marketing purposes.

Right not to be influenced by automated decision-making (including profiling) Automated decision-making (including profiling) that has a significant impact on data subjects Only "as long as necessary for entry or participation" in the completion of a contract , UK law or subject permit only allowed if open (see otherwise allowed to participate).

**POLICE AUTHORITIES**

ICO under DPA 2018 in the UK It has a number of regulatory powers, including monitoring and enforcement of the GDPR and DPA 2018. Such supervisory and regulatory powers include the power to issue:

- Notice 259: requiring regulators and processes to provide the ICO with necessary information requested from the Administrator for the purpose of measuring compliance GDPR or DPA 2018 .
- Assessment Notice 260: Requesting a controller or processor to authorize the ICO to carry out an assessment of the controller's or processor's compliance with the GDPR or DPA 2018

- Notice 261: Following an investigation, The ICO issues a notice intending to impose fines on controllers or processors for violations of the GDPR or DPA 2018. Such notification raises concerns that the ICO may be in breach of the GDPR or DPA 2018 and gives the controller or processor the right to represent. After careful consideration of such representatives the ICO will make the final decision on any regulatory action in a police report.
- Notification 262: This notification is published where the ICO ends. Failure of a controller or processor to comply with the GDPR or DPA 2018 sets out the consequences of non-compliance; This may include prohibiting the processing of all or part of personal data;
- Notice 263: If the ICO finds that a controller or processor has failed to comply with the GDPR or DPA 2018 or has failed to comply with an information notification, notification notice assessment, or police report, the ICO may: upon written notice, comply with the GDPR or DPA 2018 A fine will be required for non-compliance. Under the GDPR, these penalties can be up to €20 million or 4% of annual international turnover.

  Although the status of UK data protection law after Brexit remains unclear, EU GDPR is expected to remain law in the UK until the UK government advises Removing its content and legality in UK law Change the terms of the 2018 DPA as the GDPR comes into force ahead of the UK's planned exit from the EU.

## CHAPTER-5
## ANALYSIS OF THE DATA PROTECTION ACT, 2023
### INTRODUCTION

In 2017, work began on the latest version of India's data protection law. Despite repeated claims that India would implement the law soon, no progress has been made. Government of India, Supreme Court decision in KS Puttaswamy and Anr v. Union of India and Ors announced the formation of an expert panel to develop a data protection law in India to remove uncertainty regarding blocked data protection. Existence of privacy rights. The Ministry of Electronics and Information Technology (MeitY) has constituted a 10-member committee headed by retired Supreme Court Judge BN Srikrishna. This is not India's first attempt to create a data protection policy. Many challenges and similar costs have arisen in the last decade.

### DATA PROTECTION ACT, 2023

Justice AP Shah became the new chairman in 2012 making recommendations on the processing of data protection rights Justice Committee B.N Srikrishna presented a report - Liberty Only digital economy, protect privacy, empower Indians and Data Protection Act 2018. Although in the field his authority was recognized, he was criticized.

The Data Protection Act 2019 is the result of this restructuring, which makes major changes to various regulations and expands the power of the central government. The Data Protection Act 2019 establishes the legal framework for the collection and use of personal data. This law also refers to the establishment of data protection rights to establish regulations and maintain legal procedures. The justification of the bill includes the following statements: "To protect the privacy of individuals regarding their personal information, to ensure access and use of personal information, to create a relationship of trust between individuals and organizations that process personal data, and to protect personal data. The rights of individuals whose personal data are processed, in data processing. establishment of cooperation system and measures, development of social media standards, cross-border transfer,

Liability of organizations processing personal data, unauthorized protection and issues Actions and correction for the above purposes and related issues or problems India data protection established."
Personal information is defined as "personal information" in the law; means information about or relating to a natural person who can be identified, directly or indirectly, including any characteristics, characteristics, behavior
or other personal characteristics that person, whether online or offline or in any other document must have a combination of features and include the requirements in these documents for analysis and about personal data "processing" means:- processing or processing of personal data, collecting, collecting, organizing, creating, storing and other work, altering, altering, storing, using, enhancing or aggregating, indexing, transmitting, publishing or otherwise making available, limiting, suppressing or damage;

**APPLICABILITY**

The key features of the Personal Data Protection Act, 2019 are:

1. This Act implements for the collection, disclosure, and processing of disclosure of personal data in India.
2. A company incorporated by the Government of India/Indian Company/Citizen or incorporated under the laws of India.
3. By a controller or data processor who is not resident in the country or the Services if the work relates to any business in India or any physical activity for the supply of materials for education in India;

The law does not apply to the processing of anonymous information other than that described in section 91 (to provide) government services or evidence of production by the law

**OBLIGATIONS OF DATA FIDUCIARY**

Article 2. The PDP of the law imposes obligations regarding reliable documents318. It stipulates that personal data cannot be processed for purposes other than clear and legitimate purposes319 and requires that personal data processing procedures be fair and appropriate to ensure the speed and privacy of the data subject320. Article 6 of the Law states that "personal data is collected only when the processing of personal data is necessary". The bill also states that the data controller must provide information about the data collected and that the notification must include the purpose and nature of the data collected321. The Law also prohibits the storage of personal data beyond the period necessary for the purpose for which they are processed and obliges data controllers to comply with the provisions of the Law. The law stipulates that the consent in the documents must be and that to ensure that this consent is valid, it must be free, open, private, indefinite, and revocable.
This Law also has some exceptions to the general licensing rule. The Trustee will process information without consent in the following cases:

1. if the state needs to assist the person,
2. if a law requires it
3. Legal Proceedings
4. To respond to medical emergencies,
5. Process relevant,

Fraud prevention, mergers and acquisitions, debt collection, etc. Necessary for legitimate purposes such as. fiduciaries must implement steps to secure personal data and prevent misuse, unauthorized access, alteration, disclosure, or destruction of personal information, as well as certain security measures such as

de-identification and encryption. The trustee must report any breach of privacy by giving notice to the trustee. To see. They must carry out a relevant data analysis manage data, have their policies and personal data audited annually by an independent data auditor, and select their data protection office.

**ANALYSIS**

The Personal Protection Law (PDP) Bill 2019 has received mixed reactions, from positive to negative. The bill, which is hailed by some as progress in user rights and personal information, seems to be time-consuming, but on the other hand, it is taking time. 363

This use is a seemingly healthy framework for user privacy, but is ultimately eclipsed by the government's blanket immunity from access to user profiles. While the bill's language may seem important to users and their data, much of the final bill is about the Indian government's performance in how businesses handle user data.

**ISSUES WITH THE CONSENT-BASED MODEL**

By the preponderance of evidence, the notification and authorization mechanism in today's Internet is flawed. Licenses are often complex and confusing. So people don't read them; Even if they knew, they would not understand; and even if they did, no program could provide meaningful permission in a good way. The order of the 366 Consent form should be based on the importance of the guarantee: Recognize that users cannot allow value, but beyond that, they create an idea, it's somewhat paradoxical that a bigger deal could lead to better results.

While people believe businesses should control the data management environment more tightly, 71% are willing to give up privacy in exchange for the technology they want, according to IBM, and only 16% have left the company because of data management investigation.

If consumers do not take a view on protecting themselves online, what legal basis should determine consent qua consent, especially in the absence of clear evidence that it is effective? - a confusing question. Moreover, the agreement based on the agreement will now create more problems. According to one article, an approach to consent and notification modelled on the EU GDPR (like the Act) will increase the difficulty of effective consent. Users

According to the Srikrishna Committee, there is not a lack of information regarding the expression of consent under the current system, but too much. 370 If the existing agreement is too much in terms of data and authorization, the Certificate says that the "strong" agreement cannot make this problem good. The proposed process will therefore provide customers with more information without compromising personal data (The license agreement must contain additional explanations, rights and responsibilities, and new authorizations must be available for all new purposes).

Additionally, the harsh penalties for non-compliance with notifications and consents in the GDPR have been criticized as potentially exposing technology companies to more pressing risks, leading to strong rumours and further policy changes, leading to a consensus. According to the measure, fines will be imposed for violations. As a result, users and businesses will be harmed. Adding permissions will make users reluctant to accept the consent form. On the other hand, companies will find that users who believe they have been deceived do not trust them, even if the company complies with all laws. Information technology and civil rights expert Alessandro Acquits points out that over-reliance on authorization creates a range of costs that can undermine data protection objectives. He wrote: Social damage from “privacy conflict”: Consumers and businesses are unsure of the level of protection or the need for different types of

personal data when it comes to law and self-governance. This uncertainty itself is costly because it forces knowledge and information holders to invest capital in understanding the acceptability of the information provided. The second request may also be useful because it will preserve the file, making study materials and data processing ineffective or over-invested.

Therefore, notification and approval standards may be affected. It may not eliminate actual cyber damage, but it increases the threat to integrity. Users will become addicted to tracking and less careful in their online activities. Additionally, the user's cognitive load may also increase. Therefore, consent will become ineffective in terms of protecting personal data. If notification and agreement fail to achieve the goal of adopting a privacy protection system, the costs will outweigh the benefits for a country like India.

**POWERS OF CENTRAL GOVERNMENT**

The government is using the PDP bill as another opportunity to demonstrate the power of its parent: it has taken many steps to protect the concept of evidence in response to the constant information colonialism of foreign technology companies such as Facebook and Google. 376 Justice Srikrishna of the Commission agreed: "Information law protection if it is to be effective, must be implemented in law state. specific harm resulting from state processing of personal data, which is a strange fact. Bill proposed by the Intelligence Committee, Parliament According to Article 35 of the Personal Data Protection Law of 2019, a decision of the central government allowing state institutions to process personal information may allow them to be analysed without explicit protection. This decision allows the central government to exempt "any" government agency from "all or any" of the provisions of the Act relating to the processing of personal information. The government may take such action if it deems it "necessary or appropriate" in India's national interests, justice, security, public relations with foreign countries, and civil society. In addition, immunity may be granted to the government to prevent attacks that would violate India's freedom and integrity, security, and social welfare laws with foreign countries and citizens. Section 35 differs from the previous Justice Sri Krishna Committee on Personal Data, 2018, which exempted the processing of data of deaf people only "in the interest of national security". Although the Expert Group accepts that these exceptions are determined solely by law, the above changes should be considered as a deliberate weakening of the right to privacy.

Data Protection Act 35 simplified the government's duty to collect data to register citizens by refusing to ratify the Puttaswamy decision, which only allowed "essential and shared" information to be processed by the government. is under restrictions. In addition, the importance of regional information often allows the government to collect information about transactions made abroad before a bill is introduced.

The PDP Bill provides for the sharing of privately obtained and generated non-personal information by the government. Under Article 91(2) of the Act, governments may instruct data controllers or data processors to disclose anonymous personal data or other non-personal data to improve the efficiency of service in government or the production of legal documents. First of all, it is difficult to understand why personal data protection law is relevant to non-personal data. Second, the law is silent on how the government will use the information and how companies should share that information. Therefore, in these regulations, the central government has the authority to expropriate intellectual property rights, which may hurt the promotion of innovation in the long term.

According to Article 14 of the Personal Data Protection Law, the government may process personal information without consent for certain "reasonable reasons," including publicity. The law also gives the

government the authority to evaluate, through regulations, whether a notification duty is required for educational materials. Whistleblowers who expose lies or inconsistencies may be punished as a result.

**POWERS OF DATA PROTECTION AUTHORITY**

When compared to the latest version of the Personal Data Protection Bill, 2018, written by the expert panel led by Justice Sri Krishna, we find that this bill negates the power of the Data Protection Blocking Rules. 384 The main powers and responsibilities are now given to the central government. Consider the following situations: (i) The 2018 Act provides for the power to report other sensitive personal data. Under current law, the central government already has the authority to do this in cooperation with regional authorities. (ii) under the 2018 Act, the Company has the authority to verify the data file and report it to the trustees; However, according to the current law, the Head Office has the authority to notify members of the media in consultation with the Company. Comply with important trust documents.

**PUTTASWAMY CASE**

The PDP Bill in its current form appears to be lenient when it comes to user rights or data policies (as defined in the Bill). The first bill directly addresses user privacy issues; It appears to be similar to the European Union (EU) General Data Protection Regulation (GDPR) standard; allows and provides solutions to object to the transfer, interpretation, processing and processing of data resulting from such processing. The bill creates a Data Protection Act (DPA), which theoretically protects the rights of data subjects from tangible data, including commercial and government agencies. The right of disclosure allows DPA to share information about how its data is used. and how to use it.

However, the ideal creation of the DPA for the public good was undermined by the recommendations of the DPA itself; Unlike the previous version of the constitution, the Chief Justice includes a committee to appoint its members. Members of the DPA are not Representatives of the Court.

It is difficult to determine whether the DPA agency has public and consumer rights in its current form, and this confusion may not be intentional.

The 2018 Act exempts the processing of personal data if four conditions are met: first, it is authorized by law; secondly, it followed the procedures set out in the constitution enacted by Parliament; thirdly, it is necessary to achieve these goals; Fourth, its implementation is proportionate. These rules are based on the decision of the Supreme Court, Justice K.S. Puttaswamy v. Union of India (Privacy Act). In a controversial decision, Indians have a fundamental right to privacy guaranteed by the Constitution. The decision also emphasizes that all exceptions to applicable laws must be strictly implemented. However, the 2018 bill was criticized for essentially giving the government carte blanche.

In some cases, national security, defense, etc. It may require urgent action
and may violate people's privacy rights. This may be the reason why the Act empowers the Central Government to process personal data under Section 35 of the Act. As Justice Sri Krishna observed, in some cases when the interests of the state conflict with the interests of the individual, “national security exemptions should not be compromised to ensure that the information pillar protects the information.”

On the other hand, Law No. 2019 removes all these protections and replaces them with the provision that the central government must issue an order, state its reasons in writing and “follow such procedures, Security Agency and monitoring mechanisms.” The government is therefore transferring the main responsibility for monitoring and accountability from data protection law directly to the right to publish, which will not be debated in Parliament and will have virtually no judicial review. 389 The sweeping bill

gives the government the ability to conduct widespread surveillance that violates fundamental privacy rights. Therefore, the PDP Act does not comply with the criteria of the Puttaswamy judgment to detect violations of the right to privacy in various forms. The latest measures, unlike the GDPR and the 2018 iteration of the bill, propose creating a group of content "data trustees" called "social media intermediaries" to regulate business on social media.

## CHAPTER - 6
## CYBERLAW VS DATA PROTECTION ACT

Certainly! Here's a more elaborate breakdown of cyberlaw and data protection acts, highlighting their distinct purposes and how they work together.

**Cyberlaw: The Guardian of the Digital Frontier**

Imagine cyberlaw as a comprehensive rulebook for the online world. It establishes a legal framework for various aspects of our digital interactions, encompassing.

**Combating Cybercrime**: This is like having a digital police force. Cyberlaw defines and criminalizes online threats like hacking, identity theft, cyberstalking, and online fraud. It outlines procedures for investigating and prosecuting these crimes, deterring malicious actors, and fostering a safer online environment.

**Securing E-Transactions:** Just like securing your physical wallet, cyberlaw ensures the validity and enforceability of electronic transactions. It establishes mechanisms like digital signatures and secure payment gateways, facilitating trustworthy online commerce and financial activities.

**Protecting Intellectual Property**: In the digital realm, creativity needs protection too. Cyberlaw safeguards copyrights, trademarks, and patents, preventing unauthorized use of creative works and inventions online. This fosters innovation and protects the rights of creators in the digital age.

**Balancing Access and Control**: Striking a balance between free access to information and potential restrictions is crucial. Cyberlaw addresses issues related to online censorship and freedom of speech, aiming to create a space where information can flow freely while respecting legitimate limitations.

**Enhancing Online Security**: Data security is paramount in today's digital world. Cyberlaw sets guidelines for organizations to implement appropriate security measures, aiming to prevent cyberattacks and data breaches that could compromise personal information and disrupt online services.

**Data Protection Acts:** Empowering Individuals in the Digital Age

Data protection acts function with a laser focus – safeguarding personal information. They establish a set of rules dictating how organizations collect, store, use, and disclose our data. Here's how these acts empower individuals:

**Right to Consent:** Data protection acts put you in control. They grant you the right to decide whether your personal information can be collected by organizations in the first place. This prevents unwanted data collection and empowers you to choose how your information is used.

**Transparency:** Knowledge is power. These acts ensure you have the right to understand how your data is being used by organizations. This transparency allows you to make informed decisions about your data privacy.

**Security:** Your data deserves robust protection. Data protection acts mandate that organizations implement appropriate security measures to safeguard your personal information. This reduces the risk of data breaches and unauthorized access.

**Data Subject Rights:** Data protection acts go beyond simply informing you. They empower you with the right to access your personal data held by organizations. You can also request corrections to ensure its accuracy and, in some cases, even request its erasure.

## A SYMBIOTIC RELATIONSHIP

Cyberlaw serves as the broader legal framework for online activities, and data protection acts function as a key component within this framework. They work together synergistically:

- Cyberlaw establishes the overall well-being of the online ecosystem, ensuring a secure and functional environment for legitimate online activities.
- Data protection acts build upon this foundation by establishing specific requirements for handling personal information within the online space. This ensures a level of trust and privacy that's essential for a healthy digital society.

In essence, cyberlaw and data protection acts work hand-in-hand to create a secure and privacy-conscious digital space, where innovation can flourish alongside individual rights.

## CASELAWS

India's cyberlaw jurisprudence is a dynamic one, constantly evolving with new judgments. Here are some leading cases that have significantly impacted the legal understanding of cyberspace:

Shreya Singhal v. Union of India (2015): This landmark case challenged the unconstitutionality of Section 66A of the Information Technology Act, which provides penalties for sending malicious messages online. The Supreme Court's decision overturned this provision and highlighted the importance of freedom of expression online. The decision plays an important role in protecting online education in India.

**Shruti Shreya Dubey v. State of Madhya Pradesh (2020):** This case relates to the misuse of Section 67A of the Information Technology Act in connection with the publication or dissemination of obscene content online. The court's decision emphasizes the need for an appropriate investigation before taking action under this section. The decision is a reminder of the importance of due process in cybercrime cases.

**Reliance Industries Ltd. v. Union of India (2014):** This paper examines the concept of liability in the IT Act. Intermediaries are organizations that facilitate online communication, such as social media platforms or internet service providers. The court has created a framework for determining the extent to which intermediaries are liable for online content hosted on their platforms. This order provides much-needed clarity on the accountability of intermediaries in India's digital ecosystem.