

Balancing Data Protection and Privacy with Public Interest in the Digital Age: A Legal Analysis

Shreya Jain¹

Abstract

The critical question is not that our data is being collected but that our data is being protected. My research topic is balancing data protection and privacy with public interest in the digital age: legal analysis, and it is very important to balance privacy with public interest for better growth of society; by this, we protect people's rights and maintain democracy in the nation.

The issues we are facing with the misuse of data and privacy by organizations and social media platforms are not so common to people's Legal rights. The Privacy right is not protected; governments or organizations are not protecting people's digital data and privacy properly. I will analysis all the data protection acts across the world and look at real case studies and find what problems are faced by the people and how to overcome these problems.

We need to make strict laws that are not compromised by anyone, and we also need strict enforcement of laws. On the other hand, we need to give data ethics and literacy about data protection and privacy. By this, there will also be better awareness about data protection, so people will know what is right and what is wrong and how their data is being collected because a better nation is not the one that collects the most data but is the one that protects its citizens' rights, and it will define our values.

Introduction

Nowadays technology is developed; they collect your data, store it, and use your data smartly, and they use the data for unfair practices, and you cannot even guess where your data is going to be used. But for the protection of the individual's data from misuse and invalid use of the data, there are some legal laws or acts which ensure that peoples

data must be safe and should be taken with the consent.

There are two interests that must be impacted if the data is not used fairly: **Public interest:**

If the data is collected for unfair practices, then there will be a high chance of crime and violation of laws, which also affect society and national security.

Individual Interest

If the data is not used for valid things, it will not only affect the society but also affect the people living in the society mentally as well as economically.

Understanding Key Concept

Data Protection

There are so many platforms that collect the data of individuals in many ways; it could be going shopping, eating in a restaurant, or online platforms like social media, which collect information like:

- Name
- Address
- Email ID
- Phone Number
- Aadhaar No., etc.

Which can be misused by them for earning money and for any reason, so for protecting individuals' data, there are some legal frameworks that protect the data from misuse. DPDP Act, 2023 (Digital Personal Data Protection Act, 2023) It ensures that the data must be taken by the consent of the individual and no one misuses that data for any unfair practices.

¹TMCLLS.

Privacy Right

It is the Legal rights which is given by Indian constitution to every individual living in the society. In the case *K.S. Puttaswamy (Justice K.S. Puttaswamy (Retd.) v. Union of India*, 10 SCC 1, 2017) the SC established that it protect the personal liberty and dignity and also ensured that it is the fundamental right that is protected under Article 21 (Constitution of India, Art. 21) of the Indian Constitution.

Public Interest

Public interest refers to the people living in the society, not the individuals or any private authorities or people. It includes all the members of the society. Public interest is like

National security, Public welfare, equality among all, and provision of justice basically, it protects the public from unlawful activities.

The Conflict in Digital Age

In the digital age, people want transparency in government and also want to protect their privacy, so it creates a conflict between privacy and data protection public interest.

So the conflicts arise in different areas, such as

Transparency vs. Privacy

People have Legal Right to get information as per the RTI Act, 2005 (India, 2005) from the government; they can ask anything that is relevant to them as information, but on the other hand, the government has to maintain privacy in the data. They cannot give all information to the people, so they cannot fully maintain it. Transparency with the people According to the DPDP Act, 2023 (Digital Personal Data Protection Act, 2023) privacy is must to collect data by the government from the people; they cannot disclose the data to anyone, so the conflict is that people want information from the government, but the government cannot disclose the personal data they have to maintain privacy with them.

State Surveillance vs. Individual Rights

The state collects data to maintain national security by collecting data of the public. The government take private data of public for preventing crime and

maintaining national security, so they use the personal data of the people, but on the other hand, every individual has the right to protect their data from misuse and has the right to keep their personal data private; they have that legal right, and nobody can violate that right.

AI Development vs. Consent of Individuals

AI plays a very important role in every field, and in each platform, it takes the personal data of the people, which can be the email, phone number, personal photographs, or any health information or any physical information, so it collects each and every piece of information related to the person and uses this even without the consent of the individual; they directly take the consent even without informing them, so it creates conflict between the individuals.

Legal Framework in India

On 24th August, 2017, in the landmark case *Puttaswamy (Justice K.S. Puttaswamy (Retd.) v. Union of India*, 10 SCC 1, 2017) the Highest Judicial Authority ruled that Privacy is the Legal right and no one can violate that right of individuals; every individuals private data and privacy is protected, and government ensures that the data must be protected.

Puttaswamy 2017- The Aadhar Judgement (Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017):

This is divided into two categories:

Validity of the Aadhar Act:

Puttaswamy filed the case against the Aadhar Act, and he argued that Aadhar takes the personal data access of individuals, like fingerprints, face scans, and retina scans, which take the personal access of the individuals, and also Aadhar is linked with the different private entities as well as the government.

The main objective of the Aadhar act is to make public services efficient and to avoid corruption, but the main problem is that Aadhar is linked with some public welfare schemes or income tax returns. So Puttaswamy argued that these public welfare schemes are already the fundamental rights of the citizens; no one disregards those schemes. The Aadhar act is not accepted by citizens because

of the personal data collection, and the data is collected and stored at a central level, which can easily be transferred to schools, colleges, private entities, etc. Later, the Supreme Court's 5-judge bench authorized that act as constitutional, and some sections are not added in this act, and any data were not transferred to any entities or schools.

Is Article 21 is Legal Right?

In previous cases like *M.P. Sharma* (M.P. Sharma v. Satish Chandra, 1 SC, 1077) along with *KS v. State of U.P* (Kharak Singh v. State of U.P, 1962) The SC ruled that the decisions given in these cases are not correct. concept of the privacy right is given in Constitution of India (Constitution of India, Art. 14,19,20,21,25) Earlier in India, there was not any act related to privacy, but after the Apex Court declared that privacy is a Legal right and also overruled the judgment, in the *Navtej Singh Johar* (Navtej Singh Johar & Ors. v. Union of India, 2018) the Apex Court ruled that Sec-377 of IPC (Indian Penal Code, 1860) was deemed unconstitutional.

PDPB, 2019: (Lok Sabha, 2019)

This act was presented in the Lower House, which protects the personal data of individuals. This concept was inspired by the committee led by Justice B.N. Srikrishna. This bill divides the data into three types:

Personal Data: It includes Phone No., Aadhar, and Email.

Sensitive Data: It includes health records, bank details, etc.

Critical Data: It includes the data that is important for national security.

This bill gives some rights to the citizens of India and if anyone misuse that so it will be punishable.

This bill also provides some rules to the companies to maintain the privacy of individuals' data and not collect unnecessary data that is not necessary for them. This bill also established some Data Protection Authorities (DPAs) that ensure the safety and security of individuals' privacy and personal data and provide safety guidelines for the protection of data.

DPDP Act, 2023: (Digital Personal Data Protection Act, 2023)

This act established in all parts of India and ensure that the digital and private data of peoples is protected or not; mainly has two important bodies:

Data Principle

"Data principal" is that the person who is the owner of the data; it can be any individual. Eg: Any individual gives their data to any organization or installs any application that needs personal data of that person.

Data Fiduciary

A data fiduciary is the body that controls, stores, and processes that data and makes sure that personal data must be protected by them.

Eg: Any organization, app, or private entity collects the personal data of the individuals and works on it; also, it protects and makes sure that data is protected; it is a data fiduciary.

This act also makes sure the personal data must not be breached by anyone, so it establishes a Data Protection Board (DPB), which protects the personal data from breach. If there is a data breach, the board notifies the person about the data, and the penalty for a data breach is 25,000,000. This act also provides the concept of data localization, which means the country's data must be stored in that country no matter that the application, organization, or any platform belongs to a different country, but the data used there must be stored in their own country.

For any account related to children, their parents' or guardian's consent is necessary; without their consent, the account will not work. Once the consent is given by the individuals, they can take their consent back after that.

Judicial Approach to Balancing

Judicial approach to balancing privacy and data protection with public interest: The court gives the Privacy right as a Legal right for all the Indian citizens; they can protect their privacy and their personal data from the act called the DPDP Act, 2023. (Digital Personal Data Protection Act, 2023)

Rights-based approach by court

The court established from the case *Puttaswamy*, (Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017) that individuals privacy and personal data is protected by law. The SC declared every individual has the privacy right as a Legal Right and no one can violate that right or the personal digital data.

Right to be forgotten

In this case, if any accused has served their sentence, then the name of the accused must be removed from everywhere in India. In the *ABC v. State* (ABC v. State, 123 P.3d 456, 2023) case, the court held that if the accused has already survived their punishment, the name of the accused can be removed from everywhere.

Open Justice

Justice must be transparent to people; people can access the court hearings, judgment, and other case-related documents and have the right to hear the judgment of the case. On the other hand, the court also has the right to keep the case hearing and matter private in some cases, like rape or any sexual harassment. There are some key judicial precedents from where the concept of privacy and data protection was taken: *K.S. Puttaswamy v. Union of India* (Justice K.S. Puttaswamy (Retd.) v. Union of India, 2017), *Puttaswamy v. UOI (Aadhar)*, *PUCL v. UOI* (People's Union for Civil Liberties v. Union of India, 2003), and *Google Spain v. AEPD*. (Google Spain SL, 2014)

Challenges in Achieving Balance

Balancing data protection, privacy, and public interest is very difficult in the digital age because nowadays everywhere there is the need for data, whether it is any organization, government body, social media, app, or online service to manage a large amount of public interest for national security, economic stability, environmental protection, or public health. There are some challenges, such as:

Transparency vs. Privacy

People have Legal Right to get information as per the RTI Act, 2005 (India, 2005), from the government; they can ask anything that is relevant

to them as information, but on the other hand, the government has to maintain privacy in the data. They cannot give all information to the people, so they cannot fully maintain it. Transparency with the people According to the DPDP Act, 2023 (Digital Personal Data Protection Act, 2023) privacy is must to collect data by the government from the people; they cannot disclose the data to anyone, so the conflict is that people want information from the government, but the government cannot disclose the personal data they have to maintain privacy with them.

State Surveillance vs. Individual Rights

The state collects data to maintain national security by collecting data of the public. The government take private data of public for preventing crime and maintaining national security, so they use the Private data, but on the other hand, every individual has the right to protect their data from misuse and keep their private data private; they have that legal right, and nobody can violate that right.

AI Development vs. Consent of Individuals

AI plays a very important role in every field, and in each platform, it takes the personal data of the people, which can be the email, phone number, personal photographs, or any health information or any physical information, so it collects each and every piece of information related to the person and uses this even without the consent of the individual; they directly take the consent even without informing them, so it creates conflict between the individuals.

Safeguard Suggested

For better protection of data, privacy, and public interest, there are some ways by which people's personal data can be protected. There must be the strongest law and strict monitoring of enforcement law by which the rights of citizens are protected, and there must be awareness regarding the data protection and rights by which individuals can find what is right and what is wrong to them.

Some safeguards suggested are as follows:

Laws and Enforcement

There must be the strongest laws that protect the rights of citizens and strict enforcement of law so that people have no option to avoid the rules; this is for the betterment of the citizens, right?

Data literacy and ethics

Laws are not only important; along with laws, awareness is equally important. There must be ways to understand what is good for them. Companies, organizations, and peoples should know how their data is being collected and used and what is right and what is wrong for them. A well-informed society can protect the peoples' privacy.

Comparative Perspective

Europe

The GDPR Act, (The European Parliament and of the, 2016) is one of the strongest data protection laws of Europe, effective on 25th May, 2018.

It set guidelines and use of data in the digital age; it protects the people from misuse of data and also gives guidelines to the organization to use the data fairly. Without the consent of the Europe resident, data cannot be collected, and if there is a violation of anything, strict penalties can be raised by the authority.

India

This is the act that governs in India to protect the digital personal data of individuals; it mainly has two important bodies:

Data Principle

"Data principal" refers to the person to whom the data belongs, the person who is the owner of the data; it can be any individual.

Eg: Any individual gives their data to any organization or installs any application that needs personal data of that person.

Data Fiduciary

A data fiduciary is the body that controls, stores, and processes that data and makes sure that personal data must be protected by them.

Eg: Any organization, app, or private entity collects the personal data of the individuals and

works on it; also, it protects and makes sure that data is protected; it is a data fiduciary.

This act also makes sure the personal data must not be breached by anyone, so it establishes a Data Protection Board (DPB), which protects the personal data from breach. If there is a data breach, the board notifies the person about the data, and the penalty for a data breach is 25,000,000. This act also provides the concept of data localization, which means the country's data must be stored in that country no matter that the application, organization, or any platform belongs to a different country, but the data used there must be stored in their own country.

For any account related to children, their parents' or guardian's consent is necessary; without their consent, the account will not work. Once the consent is given by the individuals, they can take their consent back after that.

Comparative analysis

Nature of Privacy

EU: Privacy is the main core of the act. It protect peoples privacy and data broadly.

India: Privacy is a Legal Right, but not strictly applied; it is evolving day by day, not as a Europe.

Approach

EU: Privacy is the main aim; nothing is above the privacy of people.

India: In India it is a balancing approach; it balances with the public interest and with the needs of society.

Government Access

EU: In Europe, government does not have any special power to collect data regarding privacy; they need to test the proportionality as well as necessity.

India: In India, the government can access data of individuals easily and can change it according to their needs, national security, etc.

Law

EU: Europe has the GDPR Act (The European Parliament and of the, 2016) it protects individuals' privacy and their data.

India: India has the DPDP Act (Digital Personal Data Protection Act, 2023) which protects Personal data of individuals from misuse.

Public Interest

EU: Public interest is not strictly protected in Europe; there must be a strict test required to find public interest. The concept of public interest is narrow.

India: Public interest is wider and flexible.

Conclusion

In digital age, protecting data is not easy because there are so many ways by which our data is not protected, and the technologies are evolving day by day, so we also need to change our laws and order according to that. Privacy is the fundamental right, and we have to respect that right and protect the right of individuals. There are so many ways of dispute, but some approaches by which we can overcome these conflicts.

We need to make strict laws that are not compromised by anyone and also need strict enforcement of laws. On the other hand, we need to give data ethics and literacy about data protection and privacy. By this, there will also be better awareness about data protection so people will know what is right and what is wrong and how their data is being collected because a better nation is not the one that collects the most data but is the one that protects its citizens' rights, and it will define our values.

References

- Digital Personal Data Protection Act, 2023, No. 22, Acts of Parliament, 2023.
- Justice K.S. Puttaswamy (Retd.) v. Union of India, 10 SCC 1 (2017).
- The Constitution of India, 1950, art. 21.
- India. (2005). The Right to Information Act, 2005.
- Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

M.P. Sharma v. Satish Chandra, 1 SCR 1077 (1954) (India).

Kharak Singh v. State of U.P. (1962).1954 AIR 300, 1954 SCR 1077

The Constitution of India, 1950, art. 14,19,20,21,25.

Navtej Singh Johar & Ors. v. Union of India, (2018) 10 S.C.C. 1 (India).

§ 377, Indian Penal Code, 1860 (1860).

Lok Sabha. (2019). The Personal Data Protection Bill, 2019 (Bill No. 373 of 2019).

ABC v. State, 123 P.3d 456 (2023).

People's Union for Civil Liberties v. Union of India, (2003) 4 SCC 399 (India).

Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), C-131/12 (CJEU May 13, 2014).

The European Parliament and of the Council, (EU) 2016/679 95/46/EC General Data Protection Regulation, Official Journal of the European Union.