The Asian Thinker
A Quarterly Bilingual Peer-Reviewed Journal for Social Sciences and Humanities
Year-8 Volume: II, April-June, 2026 Issue-30 ISSN: 2582-1296 (Online)
Website: www.theasianthinker.com **Email**: asianthinkerjournal@gmail.com

4. Digital Privacy in India: Assessing Its Necessity and the Influence of the Brussels Effect on the Indian Digital Economy

Dr. Kaushiki Roy
Asst. Professor at IIMT College of Law, Greater Noida
Email: kaushikiroy290@gmail.com

Abstract
Digital privacy has become a critical issue in India's rapidly growing digital economy, where personal data is increasingly collected and monetized by large technology companies. This article examines the importance of protecting digital privacy as a fundamental right and analyzes the development of privacy law in India, particularly after the landmark Justice K.S. Puttaswamy judgment. It also explores the influence of the European Union's General Data Protection Regulation (GDPR) and the "Brussels Effect" on India's regulatory framework. The study concludes that while global privacy standards provide useful guidance, India should develop an indigenous regulatory model that balances privacy protection, innovation, free speech, and digital sovereignty.
Keywords: Digital Privacy; Data Protection; GDPR; Brussels Effect; Digital Economy; Right to Privacy; DPDP Act 2023; India.

Introduction

The digital economy relies heavily on the collection, processing, and exchange of user data. Technology companies use personal information to improve services, generate revenue, and support targeted advertising. However, this extensive use of data raises concerns about privacy, consent, and individual rights. In India, where millions depend on digital platforms, protecting digital privacy has become essential for ensuring a fair and secure online environment. The recognition of privacy as a fundamental right has further strengthened the need for effective data protection laws.

Why Digital Privacy?

Today, we are living in the world of the internet. we all are connected to our friends and family in the digital space, where tech companies have made a virtual environment which works parallel to the physical world1. Platforms emerged as the creators of metaverse where a person sitting in one corner of the world can easily interact with a person sitting in another corner. The life of people is not limited to real world now they have become the citizens i.e., Netizens of this world. This world has its own economy which heavily depends upon the different players who made contribution in it. The economy is known as the Digital Economy where the flow of information is an important part of it. The players who control this economy are the tech companies including the social media platforms with whom we interact daily from checking the feeds to uploading the images and sharing the content with each other. These tech players are known as giants of this economy because they have the capacity as well as power to control the flow of information to a very extent. They are 5 big giants (GFAAM) Google, Facebook, Amazon, Apple, and Microsoft.

The information or Data which we as a user generate in the form of content uploaded in social media services, making the profile in job hunting websites, browsing the internet

The Asian Thinker
A Quarterly Bilingual Peer-Reviewed Journal for Social Sciences and Humanities
Year-8 Volume: II, April-June, 2026 Issue-30 ISSN: 2582-1296 (Online)
Website: www.theasianthinker.com **Email**: asianthinkerjournal@gmail.com

through search engines and ordering the goods or services from the online marketplace becomes the currency of this economy. These 5 giants have made revenue model upon the Information or Data of the users where they monetize this data to sustain and prosper in this economy. Since their service is free so most of the users use it without any subscription in the exchange of data, sometimes including the personal data too. Data is like new oil for them, they can utilize it for making their service better (more user friendly and centric), they can further sell this data to third party advertisers for targeted advertisement, and they can do the commercial surveillance with help of vast amount of stored data in the big data storage houses. These giant players are in a dominant position in this economy where the problem with the data-revenue based model is that it's against the human rights of people in a way it violates the right to privacy and human dignity because most of time there is no consent is given by the user to utilize his/her data for the monetization purposes. The reach of this online world is not limited to one territory or jurisdiction and the users of different parts of the world are affected by the abuse of dominant position of the tech players.

Indian people are also the users of these global services, and this model also made a chilling effect upon the fundamental right to privacy enshrined under Article 21 of the Indian Constitution. The supreme court of India recognizes this right as the inalienable right which is violated by the tech giants without bearing any consequences of their acts. Thus, to protect the digital privacy is essential for making the digital economy fairer and more innovative, where the people can exercise the right to freedom of speech and expression while their right to privacy is safeguarded. There is a need to balance between the interest of users at one hand with the interest of tech players, we cannot altogether deny the access to platforms of the national market because their survival is also necessary for making the democracy healthy and information society more participated where the diverse views of people are recognized and the knowledge is shared freely between the people.

Privacy Law in India:

Indian Constitution does not expressly recognize the right to privacy anywhere. The development of law regarding the right to privacy starts from the case of MP Sharma v. Satish Chandra, District Magistrate Delhi (1954) where the Supreme Court of India first time dealt with the notion of the fundamental right to privacy. In that case the court rejected the plea of the accused that his right to privacy is violated by the search and seizure warrant. The Court held that the Indian constitution does not expressly grant a such a right unlike the US constitution under its fourth amendment. The supreme court refused to imply the right to privacy under the Article 21 (right to life and personal liberty). The next case regarding the development of privacy law is Kharak Singh v. State of Uttar Pradesh (1962) where again the Supreme Court dealt with affirmation of the right to privacy as a fundamental right, in that case the Court reaffirmed the MP Sharma case and held that the Indian Constitution does not expressly guarantee a right to privacy and such right cannot be read under the Part III (fundamental rights), upon the plea of personal liberty under Article 21, the court interpreted it narrowly and held that personal liberty

The Asian Thinker
A Quarterly Bilingual Peer-Reviewed Journal for Social Sciences and Humanities
Year-8 Volume: II, April-June, 2026 Issue-30 ISSN: 2582-1296 (Online)
Website: www.theasianthinker.com **Email**: asianthinkerjournal@gmail.com

means only those rights expressly recognized elsewhere in the constitution but it does not include a general right to privacy.

These two case laws shut the door for the right to privacy in the Indian constitution as a fundamental right even though it is expressly recognized under Article 12 of the UDHR, 1988. The situation does not change in India until the year 2017 where the supreme court of India in its landmark judgment of Justice K.S Puttaswamy (Retd.) & Anr v. Union of India & Ors (2017), where the court held the right to privacy is implicitly included in the article 21 (right to life and personal liberty) of the Indian constitution. Dr. DY Chandrachud J. speaking for majority held that "right to privacy is protected as an intrinsic part of the right to life and personal liberty under article 21 and as a part of the freedoms guaranteed by the Part III". He elaborated the concept of privacy which included bodily privacy, decisional autonomy (free choices in personal matters) and informational privacy.

At para 328 of his judgment, he mentions that "Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the State but from non-State actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection".

The judgment of Justice K.S Puttaswamy became the law of the land regarding the right to privacy. The Parliament of India two times tried two times to enact the law regarding the privacy including the digital privacy. The first time the parliament passed the bill, "the personal data protection bill, 2019". which was withdrawn in 2022.

The second time parliament enacted a fresh law, "Digital Personal Data Protection Act, 2023" (DPDP act) which is passed and in force, but the law is implemented in phases not fully. Thus, till now there is no active comprehensive legislation in India which governs the digital aspect of privacy. The only remedy to citizens has to reach the higher courts under Article 32 or 226 for enforcement of right to privacy. The limitation of legal proceedings in the form of expensive and delayed justice provides the upper hand for these global tech companies to continuously affect the rights of people without any responsibility of their acts.

European Union (EU)'s Golden standard in Digital Privacy:

The European Union through their Parliament and Council of EU adopted several digital laws to safeguard the EU's citizens right to Privacy, Human Dignity and Right to Control of Personal Data. The primary law in the EU which governs this aspect is the General Data Protection Regulation, 2016 (GDPR). Under Article 5, six fundamental principles are given:

1. Principle of Lawfulness- The data of the users shall be processed for lawful purposes.
2. Limitation Principle – Once the purpose is fulfilled then data cannot be processed further, each time the consent is required from the user.
3. Minimization Principle- the use of data shall be limited to what is necessary for purpose and use beyond the purpose is prohibited.
4. Accuracy Principle- Data of the users shall be accurate or up-to-date. If the data is inaccurate that should be erased or updated.

The Asian Thinker
A Quarterly Bilingual Peer-Reviewed Journal for Social Sciences and Humanities
Year-8 Volume: II, April-June, 2026 Issue-30 ISSN: 2582-1296 (Online)
Website: www.theasianthinker.com **Email**: asianthinkerjournal@gmail.com

5. Storage Principle- data should not be stored for perpetual time without the express consent from the user.

6. Confidentiality Principle – appropriate measures shall be taken for security purposes in case of breach of data to third parties.

In the GDPR, there are a number of rights are recognized for the protection of privacy of data subjects like:

(a) Right to access- the users have the right to access their own personal data without excessive delay or expense.

(b) Right to Rectification- the right to control the integrity of data.

(c) Right to Data portability- users have the right to transmit the data from one service provider to another without hindrance.

(d) Right to erasure (right to be forgotten)- right to erase the data which is no longer relevant.

The enforcement of these rights is also provided in the GDPR itself where the penalty in the form of monetary fines can be imposed upon the defaulting players of the digital economy.

EU's GDPR divided the definition of 'Data' into four categories i.e.

(i) Personal Data,
(ii) Sensitive Personal Data,
(iii) Anonymous Data and
(iv) Pseudonymous Data.

Personal Data means any information relating to an identified or identifiable natural person. In other words, any information about the natural person including his/her name, address, profession etc. the users of tech companies including social media platforms provide this information for creating the account or availing the service. Sensitive Personal Data means any information which is intensely private to the natural person, revelation of it can cause harm to that person in the form of bias, discrimination and abuse. It includes information relating to political opinions, health and sex life, religious, caste, race, other beliefs and criminal records etc.

These two kinds of data are strongly protected under the GDPR, special liabilities imposed upon the tech companies to safeguard these two kinds of data against the abusive processing of them.

The most interesting factor of GDPR is that it does not leave the enforcement of it to member states' government bodies, there is a Data Protection Authority (DPA) of each Member states in their national jurisdiction for enforcement of GDPR's mechanism and the authority is an independent body which acts freely without commercial or government pressure. Apart from DPA, there is a European Data Protection Board (EDPB) which work in collaboration of DPA of each member state for ensuring the compliance of GDPR.

The next law which also safeguards the interest of EU's citizens is the E-Privacy Regulation (EPR) which has set the EU's model of Digital Privacy one step further from GDPR, Although the EPR has not come into force but its provision on the enforcement of right to data portability and consent requirement is very challenging for the tech

companies. Under the EPR there is an obligation upon the tech companies including social media platforms to allow the user to migrate his/her data from one platform to another even though the new platform may be the rival of the earlier one. No formalities can be imposed against the user for availment of the right to portability and it should not be unnecessarily delayed.

Through these digital laws EU caught the big tech companies into its net where certain restrictions are made against them like: to curb the evil of tracking or the activities of commercial surveillance EU digital laws make cookie consent essential, now it is mandatory upon the tech companies to take express consent from the users and make the users aware of the cookie purpose clearly.

Second, to curb the evil of online behavior targeting advertisement (ads shown to person of interest deliberately), it's now mandatory upon the tech companies to maintain the identity of user anonymous and the sharing of personal data of users to third party advertisers without the user's express consent is prohibited.

Third, to curb the evil of machine learning of user's data (AI algorithms system made upon the machine learning) and profiling, it is now mandatory upon the tech companies that only limited purposeful machine learning is allowed (machine learning necessary to better availment of service) and full express consent must be taken from the users, the machine learning should be fair, encrypted, anonymous and free from any discrimination or bias. The latest EPR made profiling of user prohibited with or without consent.

Impact of EU digital laws:

The access of EU's single market by the global tech companies is subject to compliance with EU's digital laws. If any tech companies fail to comply with them, they can be fined, as per EU's GDPR DPA can impose the fine upon the companies who are in default up to 4 per cent of annual worldwide turnover or 20 million euro. The companies feel fear of breach of provisions because of this they incorporated EU's regulatory model into their compliance policy not just for Europe but the whole world. They are heavily dependent upon EU's market thus they changed their way of doing business as per Europe's demand and their service is one for the entire world and mostly on internet, so they changed their way of business entirely for all countries wherever their users are based.

This kind of global change in the tech companies' policy creates effect upon several jurisdictions like India where the EU's regulatory model is exported in the Indian digital economy without India's consent. For EU it's like shaping the global digital economy through their regulatory power but for other countries it is like encroachment in their digital sovereignty. This effect is known as "Brussels effect" coined term given by writer Anu Bradford in her book Digital Empires.

Sometimes Indian legislature itself heavily influenced from the EU's model as it can be seen when the Indian Parliament made privacy bill known as "the personal data protection bill, 2019 which was influenced from the EU's GDPR, this Brussels effect known as de jure while the effect created by the tech companies' policy known as De facto.

India does not require both because being the sovereign nation as highlighted in the preamble of the Indian Constitution, India should fulfill its need by its own laws, and the

The Asian Thinker
A Quarterly Bilingual Peer-Reviewed Journal for Social Sciences and Humanities
Year-8 Volume: II, April-June, 2026 Issue-30 ISSN: 2582-1296 (Online)
Website: www.theasianthinker.com **Email**: asianthinkerjournal@gmail.com

regulation should be indigenous which should take care of the different interest of Indian people.

The need arises for Indian Regulatory Model:

Tech companies including social media platforms are in a dominant position because they are the provider of service to users and they have the full control of platforms, they are gatekeepers who have the power to decide what content is shown on their platforms, who is allowed on the platform, what is good speech or what is bad, like this they take many decisions upon the daily users activity from uploading the content to writing comments on a post. This decision-making power is necessary for them because digital laws of EU made it an obligation upon the tech companies to provide their services while safeguarding the citizens right to speech, Privacy and right against harmful effect of their platforms. They have made the policy of content moderation to implement the EU's demands. Their content moderation policy is not limited to Europe, but they have made a single policy for the entire globe which heavily influenced from the EU's regulatory model. As above we call this as de facto Brussels Effect. Content moderation policy includes Terms & conditions of service and community guidelines. These policies are applied globally without taking into account the local culture of other states like India for example Facebook Community guidelines ban the nudity in their platforms which reflect the views of European and American society where generally nude images are considered inappropriate content, but it does not consider India's Tribal Cultural Heritage and the Ajanta Sculptures.

Thus, for safeguarding the Indian people's rights India has a need to set its own indigenous model. India has required to regulate these Tech companies which are continuously making chilling effect upon the Indian citizens right to speech and expression by taking the decisions on content moderation policies and right to privacy by monetizing the data of Indian users without their effective consent. Indian model should be different from the EU and advocate the Free and global Internet but while making sufficient safeguards for harmful effect of it. India's Privacy act "Digital Personal Data Protection Act, 2023 (DPDP act) could be one step in Indian Regulatory model but the provision of Data localization (storage of Indian users' data locally in Indian data centers) makes the model shifted toward the splinternet (fragmentation of global internet) ideology of the Chinese Model. India being a democratic country should base its model upon the ideals of Democracy and free speech while at the same time sufficient protection is provided to Indians for their Digital Privacy and other harmful effects of today's internet.

Conclusion

Digital privacy is essential for protecting citizens' rights in the modern digital economy. Although India has made significant progress by recognizing privacy as a fundamental right and enacting the DPDP Act, further regulatory development is necessary. The influence of the EU's GDPR demonstrates the global importance of privacy protection, but India should establish an independent and balanced regulatory model that safeguards privacy while promoting innovation, free speech, and digital growth.

References

1. Bradford, A. (2012). The Brussels effect. Northwestern University Law Review, 107(1), 1–67.
2. Bradford, A. (2023). Digital empires: The global battle to regulate technology. Oxford University Press.
3. Cohen, J. (2019). Between truth and power: The legal constructions of informational capitalism. Oxford University Press.
4. European Union. (2016). General Data Protection Regulation (GDPR). European Parliament and Council.
5. Justice K. S. Puttaswamy (Retd.) & Anr v. Union of India & Ors, (2017) 10 SCC 1.
6. Kharak Singh v. State of Uttar Pradesh, AIR 1963 SC 1295.
7. MP Sharma v. Satish Chandra, District Magistrate Delhi, AIR 1954 SC 300.