Page 481 - 488 **DOI:** *http://doi.one/10.1732/IJLMH.25139*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 3 | Issue 6

2020

Consent Mechanism in India and GDPR in Light of the Concern of Personal Information Being Commodified

RADHIKA BELAPURKAR[1]

ABSTRACT

Privacy does not have a definite meaning; it keeps evolving with time. Privacy as a concept can be seen as freedom from society and as a part of human dignity . Privacy as a freedom from society would see the concept of privacy from an angle of being let alone and controlling in the way one would want to represent themselves in front of others. Dignity of a person attaches itself with various principles in relation to human behaviour which includes freedom to their any decisions without interference, individual autonomy and freely develop one's personality.

The technology has advanced to a greater extent and as a result of that boundaries of privacy have become blurred. Social media being a medium to express thoughts, share photos and videos, like, comment, get daily updates, etc. has become one of the means to obtain personal information. The privacy policies of social media inform the user about the collection of personal information and sharing them with the third party entities. This makes personal information as a valuable commodity which is sold to the third party entity to enhance their economic model. This leads to invasion of information privacy of the social media users.

Thus, this paper focuses on the legal framework in the European Union and India to understand the consent mechanism and the protection accorded to personal information under them. Further the paper explores the privacy concerns on social media and their consent model. The paper attempts to bring out the concept of commodification which affects the social media users in terms of their privacy.

Keywords: *Information privacy, social media, commodification, third-party entities, consent.*

[1] Author is an Assistant Professor at the School of Legal Studies, REVA University

 [ISSN 2581-5369]

I. INTRODUCTION

One Personal information encompasses the identity of a person as it reveals the nature of the personality of the person. The internet has made the world transparent wherein obtaining and accessing personal information has become easy. The need for a regulatory framework to be in place has become essential to address the privacy concerns faced by individuals. The framework should be structured so as to protect the interest of internet users and especially social media users to protect their privacy, which is now a constitutional right in India. This chapter will comparatively analyse the data protection laws of the European Union and India to understand the common grounds and the dissimilarities between the laws. The focus will remain on how the law addresses the concern of users' privacy by using twin parameters of: a) relying on user's consent to legitimise the collection of her private information, and b) specifying means of seeking such consent by the social media to collect user data. These broad parameters for the most part legalise the collection of user's private information. The last section of this chapter will look then introduce the practice of commodification and assert its legalisation based on the aforesaid parameters as the main privacy concern.

The data protection laws in most European countries who are the State Member of the European Union is based on the European Union's law called the General Data Protection Regulation (GDPR). The law contains the rules for the companies who access, collect, store and process a considerable amount of information. A large part of this information consists of the personal data of the residents of the European Union. The corporations who are getting access to such data are required to reveal what type of data they have and with whom the data is shared with[2]. The corporations who have a digital presence in the European Union have to comply with the law. Digital presence is defined as occupying the online space by having a website, presence on social media or engaging with an online advertisement[3]. The law clarifies the rules and responsibilities for the online services provided by the companies within the jurisdiction of the EU. The GDPR imposes penalties for non-compliance with the law.

In India, the amendment to the Information Technology Act, 2000 introduced provisions to ensure the safety and security of sensitive personal information. It made the entities mandatory to obtain consent before collecting the personal data. The amendment introduced

[2]Article 13, General Data Protection Rules, 2018. Also see Mira Burri and Rahel Schär, The Reform of the EU Data Protection Framework: Outlining Key Changes and Assessing Their Fitness for a Data-Driven Economy, 6 JIP 479, 485 (2016).

[3] https://www.pureperformancecomm.com/news/what-is-digital-presence/ (Last Accessed on 10th Feb 2019, 9:00pm)

 [ISSN 2581-5369]

Section 43A to the Act which notified the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 (hereinafter, "the rules"). These rules apply to the body corporates and the persons residing in India. These rules define what constitutes personal information, for instance, passwords, biometric information, sexual orientation, etc. The rules mandate if the body corporate is seeking sensitive personal information, then a privacy policy needs to be drafted and uploaded on their website. The purpose must be stated by the corporation who is seeking sensitive information and consent for the same needs to be given by the individual. The body corporate who is collecting the information should maintain a reasonable protection mechanism to preserve the confidentiality of sensitive information. The act prescribes the penalty of up to 3 years of imprisonment or fine in reference to the offenses prescribed under the Act with regard to sensitive personal information[4].

The common feature between both the regulations is seeking consent prior to the collection of information. The GDPR imposes various conditions with respect to consent prior to the collection of information. The consent should be free, given by the individuals, informed and unambiguous in the written statement[5]. The language of the consent should be clear and in plain language[6]. It should be clearly distinguishable from other matter of the document. The consent needs to specify that the individual has the right to withdraw his or her consent at any point in time. Further, the GDPR specifies that silence, pre-ticked boxes and inactivity does not amount to consent. If the data is being processed for multiple purposes, it should be specified as well as the consent should be taken for all of the purposes.

The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 states that before collecting sensitive personal data or information from the individual, consent needs to be obtained in writing by the means of letter or fax or email[7]. It also includes consent given by any mode of electronic communication. Prior to the collection of information, it is an obligation on the Body Corporate to inform the individual that they have an option of not disclosing sensitive personal data or any information as well as the right to withdraw the consent[8]. The rules are however not clear whether the body corporate has an obligation to delete the information

[4] Nicholas D. Wells, Poorvi Chothani and James M. Thurman, Information Services, Technology, and Data Protection, 44 Int'l Law. International Legal Developments Year in Review: 2009 355, (SPRING 2010).
[5] Article 7, General Data Protection Rules, 2018
[6] *Id*
[7] Rule 5(1), Information Technology (Reasonable Security Practices and Procedures and Personal Data or Information) Rules 2011.
[8] Rule 5(7), Information Technology (Reasonable Security Practices and Procedures and Personal Data or Information) Rules 2011.

 [ISSN 2581-5369]

upon the withdrawal of consent.

The legal framework of the GDPR and Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 impose strict conditions on the body corporates and data processors to obtain consent and in specific written consent from the data subjects or the individuals. The difference between both the regulation pertains to the guidelines laid down with respect to the mode in which consent should be obtained. GDPR is fairly detailed and very specific whereas the IT Rules, 2011 just states that consent should be obtained. IT Rules, 2011, leaves loopholes and ambiguity with respect to the procedure of obtaining consent which the social media entities take advantage of in framing their privacy policies. The language is not clear and simple for the user to understand as well as the consent forms are very lengthy, due to which the user usually skips reading the consent form. The user gives consent without having the knowledge of the implications of accepting these terms and conditions[9]. The consent forms are designed in such a way that they are within the legal boundaries specified by the rules.

Another important feature of both the regulation is the manner in which the information should be collected. Under the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, any sensitive personal information collected by the body corporate should be essential and for a lawful purpose in connection with the functioning of the body corporate[10]. The rules specify that the body corporate should take reasonable steps to ensure that the purpose of collecting such information is informed to the individual and information of the intended recipient of the information is provided along with the name and address of the agency which is collecting and retaining the information[11]. The rules further state that the information should be used only for the purpose for which it has been collected and retained for a period not longer than it is required to serve that purpose[12].

The laws under GDPR legalizes the collection of information based on the consent of the user. It lays down six principles to which the data collector should comply with while undertaking the process of collection of information. These principles specify that the

[9] Rahul Matthan, Beyond Consent – A New Paradigm for Data Protection, Takshashila Discussion Document, 2017-03.
[10] Rule 5(3), Information Technology (Reasonable Security Practices and Procedures and Personal Data or Information) Rules 2011.
[11] *Id*
[12] Rule 5(4), Information Technology (Reasonable Security Practices and Procedures and Personal Data or Information) Rules 2011.

 [ISSN 2581-5369]

information should be gathered legally and with transparency[13]. Further, the specified reasons should be given for the collection of information to the user. The collection and the use of the collected information should not go beyond the principles under the GDPR. The information which is collected should be retained for a limited period that has been informed to the information provider. The information which is retained should be secured. It is observed that the above principles indicate that under the permitted boundary of law, personal information can be collected.

In case of sharing of information to third parties, the IT Rules, 2011, specify that the apart from the information sought by government or under any applicable legal provisions, the body corporate has to obtain permission from the information provider, prior to the disclosure of such information to the third party, unless such disclosure has been agreed to in an agreement between the parties[14]. The GDPR has similar rules on sharing data with a third party. The consent of the data provider should be taken, there should be a legitimate interest for sharing such data which should be informed to the individual.

It can be noticed that sharing of data to the third party is permitted when there is a legitimate purpose within the legal boundaries and the same has been informed to the information providers. These social media websites place themselves well within these principles and the existing regulatory framework. The framework of their privacy policies lists down on how the information will be extracted, the purpose for retaining such information, sharing the information with third parties, etc. Once consent is given to these privacy policies by the user, these platforms are legally safeguarded. The social media platforms then involve sharing the data with the third party commercial entities which is collected by them.

II. INFORMATION PRIVACY CONCERNS ON SOCIAL MEDIA AND THE CONSENT MODEL OF THEIR PRIVACY POLICY

An abundance of people use the internet on daily basis and make it a mode of communication easier while keeping the concerns of privacy at stake[15]. Social media is available in the form of websites and mobile applications. This enables users to create and post content, interact with different users, thus involving in social networking. “In order to protect privacy over the internet, it is important to consider what information is private and what is not and the aspects

[13] Article 5, General Data Protection Rules, 2018
[14] Rule 6(1), Information Technology (Reasonable Security Practices and Procedures and Personal Data or Information) Rules 2011.
[15] Obar, J.A. and Wildman, S, *Social media definition and the governance challenge: An introduction to the special issue.* 39(9) Telecommunications Policy 745, (2015)

of privacy which the users are concerned about"[16]. While technology is growing, users are more open to sharing their personal information as well as being concerned about their right to privacy.

The language of these privacy policies is written carefully in order to avoid any legal complications. Various websites are not very secured and pose high risks to users. This risk includes cyberspace violations one of them being an invasion of privacy. Some of the privacy concerns include breach of information disclosure wherein the platform uses the information for their own monetary benefits, predicting the behaviour of the social media users by observing their activities on the platform and beyond the platform and cybercrimes such as phishing, harassment, virus attacks, etc.

The financial transaction of the users is recorded and is correlated with details such as location, gender, age, sexual orientation, political views, internet service provider, products which are being purchased, transaction details are major information which is being processed and shared. This correlated data then compiled and from which they create a profile of the user. This profile gives them an impression of the likes, dislikes, and preferences of the user, thus giving insights about the personality. The user may have no knowledge or access to this derived, correlated and analysed data. Upon going through the privacy policies of Twitter and Facebook, it can be noticed that the clauses provide that the data would be shared, but they remain silent on the fact that a new set of information can be derived from the collected data. However, the actual derived data is most often not made accessible. The raw data which is collected by these platforms undergo certain processing methods to make them into a valuable commodity.

There is a shared responsibility between the user of the social media as well as the platform. The user has to see what kind of information is being shared either in a manner or in substance. This information may include personal details like name, gender, photos, preferences, location, etc. This information may lead to social media platforms in identifying a person from its traits it has found from the information[17]. The advertisers on social media websites are the main cause of privacy invasions. While shared responsibility is being discussed, it is important for these platforms to reduce the activities of advertisers and hence, increasing the security of the platform.

[16] Nan Zhang, Chong Wang and Yan XU, *Privacy in Online Social Networks* (19th October 2018, 10:30 A.M.), http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.662.8584&rep=rep1&type=pdf,

[17] Mohammed-Issa Riad Mousa Jaradat and Anas Jebreen Atyeh, Do Personality Traits Play a Role in Social Media Addiction? Key Considerations for Successful Optimized Model to Avoid Social Networking Sites Addiction: A Developing Country Perspective, 17 IJCSNS International Journal of Computer Science and Network Security 129, 131 (2017)

 [ISSN 2581-5369]

Obtaining the consent of the user before using the user's profile for the purposes of marketing or advertising is very important and these platforms should note that[18]. There is a method of opt-out consent which is majorly used by the social media platform. This has not turned out to be a useful option as the number of advertisers keeps increasing. Instead of enjoying the social media platform, the user is fatigued by using the option of opting out every time a new advertisement appears. The social media entities as well as the advertising platforms have arrangements to share the data and based on the same target the audience for marketing the products.

III. THE COMMODIFICATION OF PERSONAL DATA

While signing up on these websites, the users provide their personal details. On the basis of the personal details provided by the user, a profile is created on the platform. When the individuals involve themselves in the voluntary disclosure of personal information, the information transforms from being privately owned to co-owned. This makes the information vulnerable to threats of being exploited, as described in the preceding paras. As aforesaid, based on the user profile and associated information, which is being shared, a database is built which records and stores these user's profiles and behaviour.

The individuals need to create a boundary to determine the categories of information into public and private. This will help in allowing the individuals in the careful disclosure of information as well as set an expectation on the co-ownership upon the disclosure[19]. Privacy concerns come into place when the individuals fear how could their personal information which is shared on social media could be used or exploited. Personal communication can be expropriated with the help of technology by deriving and processing data through data analytics.

With the popularity of social media on one side, there are negative trends that are growing on the other side. One of which is the commodification of personal information. The personal information of the users which is available on the social media platform in turned into a commodity by assigning an economic value[20]. The personal information of the people has become a tradeable product. The incentive of these networks upon selling the information in the form of commodities is attaining power and earning profits. It has become a booming source of income as marketing businesses use personal information without any reluctance.

[18] James Grimmelmann, Saving Facebook, 94 Iowa L. Rev. 1137, 1183 (2009)
[19] Anitha Chennamaneni and Aakash Taneja, Communication Privacy Management and Self-Disclosure on Social Media- A Case of Facebook (Last visited on Nov 02, 2018, 2:00 P.M), https://pdfs.semanticscholar.org/9ef3/0b61775be10b973ac4f31d9b85bc2b4d4a22.pdf
[20] Paul M. Schwartz, Property, Privacy, and Personal Data, 117 Harv. L. Rev.2056, 2069 (May, 2004).

It would be appropriate to define commodification as commercially utilising the users' personal information by social media and other similar entities that operate online platforms. It is essential that the nature of these online platforms be such that they require users to provide personal information in order to use the platforms. The privacy policies of the social media websites are designed in such a manner that they avoid the phrase selling the user data but instead use the phrase "sharing information with third parties"[21].

IV. CONCLUSION

Data has the unique feature of it being related to a person which adds the element of privacy. The right to privacy allows the individual to enjoy control over personal information as it contains the identity of the person[22]. It would be inappropriate for the individual if the personal information is revealed or used by a third party even though it is legal. The right to privacy over personal information is more valuable than the economic profits and property rights which the data processors are interested in. The consent mechanism in Indian context and in GDPR has vast difference. The Personal Data Protection Bill, 2019 is a step towards protection of personal data as it is influenced from the GDPR. It is necessary that with the advancement of technology, we are able to bring changes in law to cope up with that. The transparency which we think the internet provides in terms of interaction and communication, may not as transparent as it appears, especially with respect to protecting our privacy.

*****

[21] Chrisitian Fuchs, Social Media: A Critical Introduction 166 (2014).
[22] Julie E. Cohen, *Examined Life: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1375 (2000).

 [ISSN 2581-5369]