International Journal of Advance and Applied Research (IJAAR)
Peer Reviewed Bi-Monthly
ISSN – 2347-7075
Impact Factor –7.328
Vol.9 Issue. 3 Jan-Feb-2022

INDIVIDUAL PARTICIPATION PRINCIPLE AND RIGHT TO BE FORGOTTEN UNDER DATA PROTECTION LAW: A CRITICAL APPROACH

Dr. Suresh G. Santani
G.J. Advani Law College, Bandra, Mumbai, University of Mumbai
E-mail -sureshsantani@rediffmail.com

Abstract:

Today's world is digital world where the security and protection is the complex but the utmost needed aspect. In the context under the data protection laws the rights of users should be effectively ensured as well as implemented in true sense. To achieve this legal object, the principle of individual participation and right to be forgotten play crucial role. This simply means transparency while processing of personal data and where data should be capable of being influenced by the data subject. The data protection law should allow the users to practically participate in and persuade / effect the mode and way in which one's data can be used by the data controllers and other stakeholders. No doubt the users need to give consent for using one's data but mere consent is not effective mode of ensuring total protection. Self-participation and direct self-right to delete once own data would serve means to have privacy with self-control. No doubt we have few relevant laws and policies in this context but smooth, effective and updated legal system which not only ensures the rights but also the effectual execution of the same is the foundation key of present era of digitalisation and globalisation. No doubt the internet era and digital world are full of complications but it can never the ground to let the laymen be victim of misuse of tools by the delinquents having culpable mind. The adoption of new rights such as right to participation and right to be forgotten is a mean to achieve this object. However, it needs an active and positive role and involvement of all the concerned stakeholders i.e. law makers, service providers, controllers, users, consumers and other government agencies involved in the functioning of digital system.

Rationale of the study: As the world is being rapidly globalised and digitalised the basic rights of the centralised phenomena i.e. users or sharer of data on internet should also be updated and reformed time to time.

Objective of the study: To know the nature, importance and need of crucial rights i.e. right to participate and right to be forgotten.

Hypothesis: In India we do not have adequate legal provisions ensuring the right to participate and right to be forgotten.

Methodology: Doctrine method has been adopted to do the complete justice with the topic and to have the basic complete theoretical knowledge of the subject.

Full Paper:

Today's world is digital world where the security and protection is the complex but the utmost needed aspect. In the context under the data protection laws the rights of users should be effectively ensured as well as implemented in true sense. To achieve this legal object, the principle of individual participation and right to be forgotten play crucial role. This simply means transparency while processing of personal data and where data should be capable of being influenced by the data subject. The data protection law should allow the users to practically participate in and persuade / effect the mode and way in which one's data can be used by the data controllers and other stakeholders. No doubt the users need to give consent for using one's data but mere consent is not effective mode of ensuring total protection. Self-participation and direct self-right to delete once own data would serve means to have privacy with self control.

Origin of Principle of Participation*:*

This concept is recognised under FIPPS (Code of Fair Information Practices based on Fair Information Practices Principles)[1]. It emphasise that -

1. Users should be able to decide what personal data should be in record and that who should be allowed to use shared personal data i.e. including controllers of online platform, service providers and relevant stakeholders.
2. One should be able to change or make corrections/amendments in shared record of information about oneself.

[1] Paul M. Schwartz, Privacy and Democracy in the Cyber Space', 52 Vanderbilt Law Review 1609 (1999).

3. Individual should have right to allow or deny the use of one's information collected for one reasons as to be used for some other purpose with or without consent.

In 1980 the Organisation for Economic Cooperation and Development Privacy Guidelines (OECD Guidelines)[2] also supported the importance of participation of individuals in the context of data sharing digitally. These guidelines focussed on three rights i.e.

1. The right to ask for verification of self processed data.
2. The right to access once personal data. Including the basic rights such as right -

1. To know about the purpose of processing the data
2. To know the period for which the data would be stored
3. To know about the mode of processing the data.
4. To file grievances in case of misuse of personal data without consent or otherwise. Etc.

3. The right to confront the correctness of one's personal data.

Hence, saying that principle of individual participation is the base of rest of rights in the context of digital data would not be wrong. With above background the data protection laws should ensure this right.

Possible Challenges:

However, there are certain challenges to ensure this right. These are like:

Expensive Execution: The practical implementation of this right is too expensive for data controllers. While replying the request from the side of data users/individuals fee may be imposed as per existing data protection law. It may be a burden on the only users.

[2] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data' (2013), available at:

http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.ht m

(last accessed 31 October 2017).

Technological Challenges: Managing a large quantity of data in a systemic mode is itself a challenge for any data controller or service provider. The data is needed to be maintained in various formats and also in mixed variations. Even the inter connectivity amongst data is also a fact that must be managed effectively.

Restricted Rights: Users are generally not able to guess the impact of use, collections of data and misuse of data in current digital world. This also due to low level of understanding about legal provisions and their legal impacts and also low awareness about enforcing mechanism of data protection laws and provision. These facts certainly result into restrictive exercise of rights by users.

Other rights centralised to Right to Participation:

The importance and scope of right to participation is very huge. In addition to right to verification, right to access and right to confront, it also creates few other basic rights such as:

The right to raise objections as to processing: Even where the data has been processed by complying with the legal requirements the same may be objected if it is inconsistent with the recognised rights and interests of user or individuals as against the data controller. Usually such objections can be taken on the reasonable grounds like -

1. Data has been processed ultra viresly i.e. beyond the authorised limits.
2. Data has been process against public interest at large.

Right in case of direct marketing: A communication which is directly connected with specified individuals that is used for marketing is known as direct marketing. Here users may not be aware of or not consented to such direct communication because the marketers may assemble the personal data from various online sources without any prior message.

Right in respect of an automated processing: Automated decisions are those decisions where there is no role of any human intervention. Such decisions may be defective or unfair because of not any uniformed or not any standard mechanism of sampling process. It would certainly affect the transparency of data processing denying the basic rights of users.

Right to prohibit/stop Processing: This right is required to be exercised immediately as provisional remedy is situations like :

1. When the correctness of data is in the dispute.
2. Where the processing is unlawful.
3. Unauthorised use of collected data for the purpose other than the consented one.

Right to Portability of Data: With this right the user can easily shift, carry or spread once personal data from one platform to another digitally. This would ensure protection against being locked into a particular service. It further requires two important aspects i.e.

1. The individual / user should be entitled to obtain the personal data provided by the individual to the controller in a universally used machine readable format.
2. The individual / user should be entitled to convey personal data from one system/controller to another.

Possible Challenges:

1. Expensive operation and execution of such rights.
2. Vague scope and functioning of rights.
3. Inappropriateness for Indian system.
4. Overlie with other segment / definite regulations.
5. Computerized assessment process

Right to be forgotten:

This right entitles the individual users to request the controller or organisations to delete any data about him existing in the digital world / system. This right shows a substantial development in the accessibility and openness of information connected with the digital world. Once the data is uploaded or released on the internet there is every possibility that the users wants to withdraw or remove the same from the internet. One may letter on wishes to keep it secret again or not to continue the open accessibility of once personal data. No doubt it is usually said that once data is made available on the internet it cannot be truly forgotten or removed. The problem is that once the personal

data is available on internet the basic object / aim of uploading the same is lost because the data would be openly available for anybody for any purpose at any time. It may results into humiliation and loss of name of the users / individuals. For example in Google Spain Case[3], previous data relating to an attachment and garnishment action against a Spanish individual was all the time the first link whenever anybody do search on internet of this individual's name. This definitely caused defamation of such user.

The Apex Court of India in the case of Sri. Vasunathan[4] acknowledged the right to be forgotten. The court recognised this right to protect the users in crucial and critical matters involving the women image and status or offences against women or other vulnerable groups like rape, modesty of child defamation cases etc. Even in Justice K.S. Puttaswamy case[5] our Apex Court observed that the effect of sharing data on internet era is perpetual. Any attempt even from an expert to delete permanently such digital data from the internet world cannot be assured. Human beings are not inactive and are flexible ever are constantly growing. One should be entitled to re-invent oneself and change past actions. It simply means to ensure the right to protect self-data and personal data shared on the internet. This right is a part of right to privacy and right to life under Article 21 of the Indian Constitution.

Possible Challenges:

Balance with the fundamental freedom of speech: Prima facially right to be forgotten implies three different categories of rights that seems to be inconsistent with the freedom of speech and expression[6].

These rights are : When the data is shared in internet world then the individual/user sharing the data should possess the right also to delete the same from the internet.

---

[3] Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, Case C131/12, (2014), European Court of Justice.

[4] Sri Vasunathan v. The Registrar General, 2017 SCC OnLine Kar 424.

[5] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCALE 1

[6] *Jeffrey Rosen, The Right to be Forgotten' 64 Stanford Law Review 90 (February 2012).*

Re-sharing of data: When the data is shared in internet world and same has been copied by some other and if same has been re-shared on internet by such person i.e. re-shared in once own name and concerned field. They who would have the right to delete that data? Unfavourable Reviews: After sharing the personal day if anyone has posted some comment on once data or if the data has been posted on the internet for me by someone else without my consent and knowledge. Would the right to delete would be there?

Third Parties Liability: The liability of third party e.g. controller or search engines or other service providers is a complex issue to be considered while deciding the scope and implementation of right to be forgotten. But transparency requires the accountability of all the concerned stakeholders.

Relevant Laws in India:

At present we have various laws in India that contain express provisions that deal with the handing out / processing of personal data. Data may be personal data or and sensitive personal data. But now there is a need to re-examine and re-frame or made changes in existing laws in the context of new era of data protection fields. Such laws are dealing with deferent aspect such as:

Financial segment: It includes laws like Banking Regulation Act, 1949, Credit Information Companies (Regulation) Act, 2005, Credit Information Companies Regulation, 2006, The Insolvency and Bankruptcy Code, 2016, Payment and Settlement Systems Act, 2007 and Reserve Bank of India Act, 1934 etc.

Health segment: It covers legislations like The Indian Medical Council (Professional Conduct, Etiquette and Ethics) Regulations, 2002, Pre-Conception and Pre-Natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994 and The Mental Health Act, 1987 etc.

Information Technology and Telecommunications segment*:* It includes laws such as The Indian Telegraph Act, 1885, The Telecom Regulatory Authority of India Act, 1997 and Information Technology Act, 2000 including it's Rules and Regulation etc.

Other Miscellaneous Laws*:* In addition to above referred laws few other laws are also directly or indirectly connected with the data sharing process. Such laws

are like The Aadhaar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016 including Regulations, Census Act, 1948, Collection of Statistics Act, 2008, Consumer Protection Act, The Act of 1986, Right of Children to Free and Compulsory Education Act, 2009 and Right to Information Act, 2005 etc.

Foreign Provisions:

Sufficient legal protection can be easily traced in other countries that ensure safety of individuals who shares data on the internet world.

European Union:

The General Data Protection Regulation, 2016 at European Union ensures the right to obtain information relating to -

1. Complete details and status of the data controller and service provider.
2. The use of processing information, storage time period, methods and process of automatic decisions.
3. The legality of processing information method and platform.
4. The nature and scope of other legal rights of user sharing the information.
5. The right to access once personal information including the right to authenticate once shared private information… etc.

United Kingdom:

The Data Protection Act (DPA), 1988 was enacted at United Kingdom to ensure and safeguard basic rights of the data sharer. It contains rights such as right to access self information, right to be aware about when and to what extend shared information would be processed and for what purpose it would be used. Even it has recognized right to know the reasoning i.e. the basis of decisions in case of automatic decisions. In case of erroneous personal details or personal data represented in wrong manner the data sharer should be entitled to take recourse of the courts to seek remedies like making required corrections in the data, delete the data for a period or permanently and to get substantial compensation in case of injury sustained due to mistake of service providers or controller or other involved agencies.

Canada:

The Personal Information Protection and Electronic Documents Act (PIPEDA), 2000 has provisions regarding the individual's right to access. Through these provisions the information sharer can request to know about the existence, purpose of disclosure of once personal information. And if the data is tempered or manipulated same can be challenged to get legal remedy.

The similar legal protection is available in Australia[7] and South Africa[8] for safeguarding the basic rights of individual sharing the data on the internet.

Recommendation*:*

1. Personal Data Protection Bill, 2019 should be adopted at the earliest.
2. Periodical public awareness programmes at the large level should be a mandatory provision that to be complied with the service providers and controllers.
3. Periodical assessment of legality of data processing mechanism is a need of time and the report of the same must be made published in the public.
4. The educational institutions should also paly positive and active role in making public awareness events.

Conclusion:

Smooth, effective and updated legal system which not only ensures the rights but also the effectual execution of the same is the foundation key of present era of digitalisation and globalisation. No doubt the internet era and digital world are full of complications but it can never the ground to let the laymen be victim of misuse of tools by the delinquents having culpable mind. The adoption of new rights such as right to participation and right to be forgotten is a mean to achieve this object. However, it needs an active and positive role and involvement of all the concerned stakeholders i.e. law makers, service providers, controllers, users, consumers and other government agencies involved in the functioning of digital system.

[7] The Privacy Act, 1988 and the Freedom of Information Act, 1982

[8] Protection of Personal Information Act (POPI Act) – POPIA, 2013

References:

1. Report of the Joint Committee on the Personal Data Protection Bill, 2019
2. White Paper Of The Committee Of Experts On A Data Protection Framework For India: https://meity.gov.in
3. Online Platforms and digital advertising: Market Study final report 2020 by CMA Competition and Martket Authority.
4. Subhranshu Rout Gugul vs State Of Odisha decided on 23 November, 2020
5. Monitoring and Restricting Digital marketing Of unhealthy products to children And adolescents Report based on the expert meeting on monitoring of digital marketing of unhealthy products to children and adolescents. WHO European Office for the Prevention and Control of Noncommunicable Diseases (NCD Office) Moscow, Russian Federation June 2018.