Global Scientific JOURNALS

GSJ: Volume 9, Issue 5, May 2021, Online: ISSN 2320-9186

www.globalscientificjournal.com

RIGHT TO PRIVACY IN DIGITAL INDIA

Author: ABHISEKH RATH

Co-author: CHARVI

ABSTRACT

In today's world for most of our jobs we rely completely on technology. Our lives are deeply entangled with technology. The digital transformation which has taken place has made all of us go online. This is the time we understand how important privacy is on a digital platform. In this paper, we have explained how the Right to Privacy was made and fundamental right in India and have discussed the important judgements with regard to it. Further, this paper explains how the Data Protection Bill is a great step and how should the Data Protection Authority should function. We have then come to a conclusion that India's Constitution should have provisions for upholding the Right to Privacy on the digital platform.

INTRODUCTION

Privacy is interpreted as freedom from being watched or bringing public attention or individuals' capacity to isolate themselves and their data. Currently, the focus on the right to privacy is based on the modern digital era entities. Private spaces, moreover, securities that were earlier granted just by material separation, are no longer guarded. The digital network enters the most proximate areas and challenges those commonly believed understandings of the individual. It centers on modern means regarding handling social, economic, and political power and reducing sovereignty. Similarly to the public space, there should be a separation between the private and public space in the digital domain. We require a constitutional clarity and guarantee of the right to identity, individual liberty furthermore privacy in the digital era. The state's role regarding the right to privacy under this digital age is not just to abstain from its violation. It is fair to guarantee that such a right is not violated by private individuals. The court must especially guide the state to render this necessity.

The right to privacy is offered by article 21 of the Indian constitution states that "no person shall be deprived of his life or personal liberty except according to procedure established by law." The right to privacy was made a fundamental right guaranteed by part three of the Constitution of India, according to a ruling by the Supreme Court of India on 24th August 2017. That decision of the Supreme Court surely had very important consequences. According to that judgment, new regulations word to be tested based upon similar parameters in accordance with article 21 of the constitution under which the laws might violate personal freedom. Even though now the right to privacy is available, its extent and boundaries still are exceptional. There is no Comprehensive legislation for data protection and privacy in India. The general policies and law are sectoral. The Information Technology act, 2000, regulates the entire cycle of compilation, processing, and private information and sensitive private data by a corporate body in India.

In the case of MP Sharma versus Satish Chandra, a search and seizure warrant was granted and was brought into question in accordance to sections 94 in 96 of the Criminal Code of Procedure, Was the first instance when the Supreme Court of India Contemplated if the right to privacy is a basic right. The ruling given out by the Supreme Court of India stated that the search and seizure warrant was not contradictory to any of the constitutional provisions. The Supreme Court also denied acknowledging the right to privacy is a basic rate that India's constitution should guarantee.

Subsequently, in the case of Kharak Singh versus State of Uttar Pradesh, The Supreme Court considered if Examining a convict's place at night would be A degradation of the right provided under article 21 of India's constitution. This, in turn, raises the question if article 21 should also include the right to privacy. Furthermore, many judges believe that a confidentiality provision was not expressly mentioned under article 21 and hence right to privacy should not be interpreted as a fundamental right.

Afterward, in the case of Gobind v State of M.P. Police's power to housekeeping was challenged regarding being conflicting with the right to privacy stated under Article 21 in the Constitution of India. The Supreme Court directed that the statutes of the police did not comply with the postulate of private liberty, also recognized the right to privacy being a fundamental right assured by the Constitution of India, but recommended the development of the right to privacy under a case-by-case premise furthermore dismissed that for being an absolute right.

The same point was brought before the Supreme Court in the matter of K. S. Puttaswamy (Retd.) v Union of India; the Aadhaar Card Scheme was disputed because the accumulation furthermore compilation of population plus biometric data of citizens of India to be utilized for various purposes violated the basic right to privacy sanctified in Article 21 of the Constitution of India. Seeing this ambiguity encompassing the constitutional standing of the right to privacy from past judicial precedents, the Court regarded this subject to a constitutional panel that included nine judges.

A ruling was given out by the Supreme Court that the right to privacy is intrinsic to the human factor, and the essence of human dignity is inseparable. Therefore, privacy was believed to possess both useful but also harmful content. This adverse content performs as a restriction on the State by interfering with a person's life and personal autonomy; its helpful content forces the State to practice all needed steps to safeguard its privacy.

Hence, the constitutional assurance of privacy might lead to a couple of inter-related protection:

(i) Corresponding the society in general, to remain valued by each, including the State: the right to decide what private data is to be published.

(ii) As a significant concomitant regarding democratic implications, bounded government moreover limitation on State's power, against the State.

Consequently, compared to any statutory right, the right to privacy has grown stronger than simple common law, also reliable and true. Therefore, in the context of Article 21 of the Constitution, an intrusion of privacy must now be justified based on a law specifying a right, impartial and reasonable method.

Contentions raised by the ones asking for the right to privacy, nevertheless, remain worrying. For several, it appears as if the right is not corresponding much to the digital enterprises and only to the state. One understands premises similar to: the state is a monopoly unlike enterprises; enterprises rely on individual arrangements concerning data access, rendering data is willing, and so on.

A right can be called a substantive right alone when it operates in all conditions moreover for everyone. For example, a right to free expression toward a person regarding their exploitation holds no meaning without the actual security availability, ensuring that private authority cannot be practiced to prevent this right. Therefore, the state's role is to ensure that private parties cannot block rightful free expression and not simply abstain from controlling it.

Similarly, the State's role towards the right to privacy during this digital era is to refrain from its breach and ensure that private individuals cannot infringe that right.

In recent discussions concerning privacy, data being the primary social moreover financial resource in the digital age is the elephant in the room. Excluding the State from any substantial role concerning the community's data resources without restraining private enterprises will commence a future where companies grow as the key organizing actors for the community, dismissing the State to a remarkably mangled position.

In recent times, people have begun to rush to courts to enforce their privacy liberties fronting huge tech businesses, e-commerce policies, and retailing enterprises. Therefore, in the case of the recommended new data law, it is rather apparent that it's the State upon which people will approach the courts for enforcing their fundamental right to privacy.

In past times, constitutional courts were the domain for the adjudication of fundamental rights. Amidst the recommended Bill, a vital element of that statutory role, management of citizens' informational privacy, happens to be advised to be assigned to a Data Protection Authority (DPA). In the Puttaswamy case, the Supreme Court directed the government to pass legislation that would manage the informational privacy of non-state characters and the state bodies, including other people.

Maintaining stability between informational privacy and generating a solid digital market is a fairly challenging job, demanding a qualified, impartial body at the wheel. A core statutory job by the DPA; penalize governments moreover suspend their plans if they fail in protecting the personal data of an individual.

In the knowledge regarding the crucial adjudicatory function concerning the DPA to regulate private parties and the central government itself, there's a requirement to fix up a DPA autonomous of the central government that can impose the Personal Data Protection Bill in an impartial way. It cannot seem to be below the immediate command and direction of the Centre.

The Bill's present form provides a broad spectrum of powers to the central government that, it seems it is one central government's obligation only to secure the citizens' informational privacy rights. Such as, the DPA posts remain appointed by a panel including the central government administrators rather than a judicial or a parliamentary body or committee. That form of the Bill heads to the central government managing itself.

The design, as mentioned above, will further unfavourably influence the federal structure of the Constitution of India. For example, suppose a charge filed against the Chief Minister's Office for breach of data. In such a case, that will be determined through a panel delegated by the central government to see whether such an infringement was done or not. If it is found so, what the punishment or amount of fine/additional penalties would be.

Furthermore, the Bill allows the central government to determine whether an incident or occurrence in a secluded place in a state holds as a matter of 'public order' or not, asking exceptions of implementing the different protection provisions. That cannot offer fertile grounds concerning data administration through the Centre, leading to a huge federalism concern.

Hence, the DPA must be set not as a governing body designated by the central government though as a quasi-judicial self-governing body with legal representation. Furthermore, it should be restrained to only judicial oversight and monitoring and not the current Bill's administrative supervision.

Similarly, the state's rule regarding the right to privacy during this digital age is not only to abstain from its violation. The right to privacy in India is under severe threat. Because of the Central government's submissions in the matter which questions the constitutionality of biometric identification program in India, the right to privacy, fundamental rights been put into doubt. A comprehensive privacy statute is also absent in India. We second the constitutional right to privacy; furthermore, we consider that a comprehensive, people-friendly law implementation is crucially needed in India.

Understanding the constitutional right to privacy will continually develop as technology grows more pervasive and will be able to seize more personal data. Under these situations, it is essential to recognize the pros and cons of technology and only prescribe suitable policy and legal dilemmas. It is understood that enhanced technology appropriation creates an enormous value that can be accurately controlled under a privacy policy.

CONCLUSION

India has no specific provisions which defend privacy in regards to data infringement. Even though we have the right to privacy under article 21, it is inadequate and incompetent for data privacy safekeeping. The management of legal scrutiny in India serves as an incomplete non-transparent governing system that operates without investigation. There is a critical lack of cheques and balances, leading to telephone tapping arrangements being violated. Any

surveillance system news former judicial review and notification to the individual while the surveillance is terminated.

The Snowden disclosures have revealed the eerie Nature of undercover mass monitoring; every bit of data is drilled, plucked, and examined. The aforementioned is the real representation of a surveillance state that restricts transparency while keeping a watch on the citizens constantly. It is very concerning that the current policies of India's mass surveillance arrangements Are not operating under any explicit statutory authority. Mass surveillance, in principle, is contradictory to the fundamental rights under the constitution of India.