VOLUME 6 | ISSUE 1

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

DIGITAL RIGHTS IN INDIA: PRESERVING CONSTITUTIONAL INTEGRITY

- Dheeraj Kumar*

Abstract

The evolution of human beings can be answered within the realms of changingeras, based on the advancement of tools and themechanical mindset. It is the notion of progress that has brought humans to survive on this planet throughthe evolution of time. The most rampant technological growth can be previewed in the Millennium Era and upon the advancement of the internet and fibre optics. The 21st Century saw a wide demand for computer-based technology, which in the coming decades not only transformed the way and outlook of human working and assessment, but also enslaved the human brain into a fast modern digital era. The ways of communicationhave evolved into a specific sphere of networking with the use of electronic media and a flourishing market of smart electronic devices with wireless technologies. The rights which are fundamental to the inherent existence of humans on earth are now not to be severed only towards preserving of body or mind of a person, but also towards the acts of personal privacy in public and private arenas of one's life. The trans-boundary sharing of Data and the expanding use of internet technology have brought an obligation upon the states to prevent, protect and legislate upon the extensive data pooling in this digital economy. This review article shall focus on the several constraints faced by the government and citizens in the development of a new thought of digital rights and its incompatibility with the inherent advancement of new threats to national security and the use of surveillance monitoring techniques.

Keywords: *Human Rights, Privacy, Digital Rights, National Security, Digital Era*

INTRODUCTION

The idea of personal privacy is not relatively new to India. The Ancient Administrative system of governance, which is based on Vedic literature and Upanishads, mandated certain

*Ph.D. Research Scholar, Department of Law,Central University of Haryana, Jant Pali, Mahendergarh, Haryana.
For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

https://www.ijalr.in/

acts to be done in seclusion from the outside world, like 'meditation', thus enumerating the concept of autonomy of privacy. Politico-legal texts like 'Arthashastra' also demonstrate reverence for the individual's privacy in a welfare society.[1]

As Dr. Leon A. Pastalan defined, "Within the definitional frame of reference, there are four delimitable modes of privacy - *solitude, intimacy, anonymity* and *reserve*. Privacy for our purposes may be defined as the right of the individual to decide what information about himself should be communicated to others and under what conditions".[2]

The Constitution of India is an ever-evolving document, adaptive to the changing conditions of the world around it, which is an unarguable reality that cannot be refuted. In addition to several other basic rights, it acknowledges the privacy rights to be inherent in the many rights that fall within the purview of *Article 21*. It states that *"no individual shall be deprived of his life and personal liberty except according to the method prescribed by law,"* which means that no one has the authority to take away a right to lead a dignified life, except those who have been given the power to do so as per the law of the nation. Since the right to privacy is connected to an individual's life and liberty, Article 21 guarantees protection for this fundamental human right.[3]

For the first time in 1994, the Apex Court of India accepted the *legal presence* of any 'person's privacy in a society' and 'the right to be left alone' undisturbed in the famous *Auto Shankar* case. In this case, the SC made it clear that the right to privacy of an individual is a part of the Right to freedom of speech and expression under Article 19(1)(a), which is granted to any individual, being a 'convict' and even the press.[4]Further, SC in *State of Maharashtra* v. *Madhukar Narain*[5], decided that a lady has the same access to right to privacy as a woman to protect her against the allegations put against her as any other person, and that no one has the right to breach her privacy.

[1]Anjali Kumari, "Need of Privacy Law in India" 4(3) *International Journal of Law Management & Humanities* 1956 (2021).
[2] Leon A. Pastalan, "Privacy as a Behavioural Concept", 45(2) *Social Science* 93, 95 (1970).
[3]Sonam Rawat, "Revisiting Right to Privacy in Indian context", 4(4) *International Journal of Law Management & Humanities* 4036 (2021).
[4]Vijay P Dalmia, "Data Protection Laws In India - Everything You Must Know - Data Protection - India" *Mondaq.com*, (2017), *available at*: https://www.mondaq.com/india/data-protection/655034/data-protection-laws-in-india--everything-you-must-know (last visited June 10, 2022).
[5] AIR 1991 SC 207.

In the famous '*Phone Tapping*' case of *People's Union for Civil Liberties* v. *Union of India*[6], said that the government should not use this power to *conduct surveillance*activities, unless there is a public interest, an emergency or a danger to the public. It also said that Article 21 of the Constitution protects citizens' rights to life and liberty, including their right to privacy.[7]These arguments are founded on the Constitution of India's provision of reasonable limits to freedom of expression, which may be found in the document.[8]It was noted by the Supreme Court in *R.M. Malkani* v. *State of Maharashtra*[9] that the court would not accept measures for the protection of citizens being jeopardized by allowing the police to continue illegally or irregularly[10]. The government is not permitted to place prior restraints on the dissemination of defamatory information about its officials; if it were to do so, it would be in contravention of Articles 21 as well as 19(1)(a) of the Constitution.[11]

However, in the year 2017, the '*right to privacy*' was finally acknowledged as a basic human right. The landmark decision by the Supreme Court in the case of *Justice K. S. Puttaswamy (Retd.) and Another* v. *Union of India*[12], established that the privacy right is inherent under Articles 14, 19 and 21 of the Constitution of India.[13]It was argued that the state and non-state organizations may both be held liable for violating people's privacy when it comes to protecting the personal information of citizens.[14]This decision was hailed as a constitutional victory, which inter alia, accepted a new "*right to informational privacy*".

PROTECTION OF DIGITAL RIGHTS TO PRIVACY

The idea of data protection is the most important aspect that is coextensively associated with the Right to Privacy.[15] Since, in the modern day, a person is more likely to be found on the internet, on social media and in *cyberspace* than portraying his physical presence or rather

[6] AIR 1997 SC 568.
[7]Nivedita Baraily, "An Analysis of Data Protection and Privacy Laws in India" *International Journal of Law Management & Humanities*, 2021, *available at*: https://www.ijlmh.com/an-analysis-of-data-protection-and-privacy-laws-in-india/ (last visited June 10, 2022).
[8]Abraham, "Data Privacy: Finding the Right Balance Between Data Personalisation and Consumer Privacy" 5(1) *IJLMH* 1541 (2022).
[9] 1973 SCC (1) 471.
[10]B. Madhana, "A Study on Law Relating to Data Protection in India" 4(3) *IJLMH* 6186 (2021).
[11]*Ibid.*
[12] (2017) 10 SCC 1
[13]"A study on Right to Privacy in light of K.S. Puttaswamy v Union of India," *International Journal of Law Management & Humanities, available at*: https://www.ijlmh.com/paper/a-study-on-right-to-privacy-in-light-of-k-s-puttaswamy-v-union-of-india/ (last visited June 10, 2022).
[14]*Ibid.*
[15]Shiv Shankar Singh, "Privacy and Data Protection in India: A Critical Assessment," 53 *Journal of the Indian Law Institute* 663–77 (2011).

existence in public, thus making the relevance of data protection more significant and necessary. The digital rights can be classified based on the legislation and Digital Rights Charters of various countries. It can be said that, in drafting any legislation or general guidelines by any country, the following rights should be enunciated:

1. Right to Universal and Equal Access
2. Right to Freedom of expression, information and communication
3. Right to Privacy and Data Protection
4. Right to Anonymity
5. Right to be Forgotten
6. Right to Protection of Minors
7. Right to Preserve Intellectual Property

We can see how technology can invade your privacy and produce errors in your life. According to researchers, the advancement of legislation on data privacy from the 2030s will be solely based on interactions and protections from *Artificial Intelligence* (AI) technology, which can bring new obstacles and obstructions in the way of the Right to Privacy and Data Protection in India, as well as the rest of the world.[16]

Talking about the storing of information while communicating through social media, a "*Digital Footprint*"is created withevery moment. It is the precise reproduction of the accounted activities of any person on the servers that may be retrieved from a backup by law enforcement investigations.[17]In the past 5 years, we have seen the Investigating Authorities of India, have been investigating many citizens andIndian celebrities on charges of drugs or anti-national tweets and even against the offence of creating enmity between religious groups. This is done after retrieving their old deleted communication texts, images or video files dating back upto a decade. Nonetheless, as it is done to protect and prevent the furtherance of a crime, as may be in all other situations, save for the voluntary agreement, such an act can amount to a contravention of the privacy right of a person.[18]

There are still not sufficient privacy and data protection laws in place, which has been a source of worry. This worry has been voiced in particular by international businesses that are

[16]Atul Singh, "Data Protection: India in the Information Age," 59 *Journal of the Indian Law Institute* 78–101 (2017).
[17]*Ibid.*
[18] Parminder Jeet Singh, "*Privacy in the Digital Era*", The Hindu, Aug. 8, 2017, 12:03 AM, *available at:* https://www.thehindu.com/opinion/op-ed/privacy-in-the-digital-age/article19446279.ece (last visited on June 16, 2022).

doing operations in India and are transferring sensitive data into the country. It is needed that all of the stakeholders align their policies with the standards of data protection and promote the adoption of the principles of privacy by design for the data protection regime to be effectively implemented. This is a necessity for effective implementation. Consequently, by enacting trustworthy data privacy legislation, India has the potential to become much more than a simple provider of services to the multinational enterprises of the globe. In other words, it's trying to turn India into a business hub.

LAWS RELATING TO PROTECTION OF DIGITAL PRIVACY

The Information Technology Act of 2000 was the first National legislation of India that protected the '*Internet Privacy*' of the web users.Many provisions were added to reduce online crimes and induce safeguards upon online privacy, such as prohibition and penalizing Child Pornography[19], Hacking and online fraud/Scams[20] and defining standards of data protection for corporate bodies. Although there were certain gaps which diluted the online privacy of users such as "the ITAct, 2000 did not addressed questions and circumstances like the evidentiary status of social media content in India, merging and sharing of data across databases, whether individuals can transmit images of their own private areas across the internet, if users have the right to be notified of the presence of cookies and do-not track options, the use of electronic personal identifiers across data bases and if individuals have the right to request service providers to take down and delete their personal content".[21]

Since the Puttaswamy ruling in 2017, it ruled the effective need fordata protection legislation. The *European Union*(EU) passed a regulation known as the "*General Data Protection Regulation* (GDPR)" in 2018, which imposed various restrictions on companies regarding the use and management of individuals' personal data. On the heels of multiple high-profile data breaches by Indian commercial organizations, a committee under the guidance of Justice *B.N. Srikrishna*was formed in 2018 to address this loophole in the country's statutory legislations on data privacy and protection. Later, "The Personal Data Protection Bill, 2019" (PDP), which is a spin-off version of this report, was tabledin the Lok Sabha in December 2019. The GDPR served as inspiration for the proposed PDP Bill, which was intended to bring about a

[19] Sec. 67, I.T. Act, 2000.
[20] Sec. 43, 66 and 66F, I.T. Act, 2000.
[21] *Refer to* "Internet Privacy in India", The Centre for Internet & Society (2013), *available at:* https://cis-india.org/telecom/knowledge-repository-on-internet-access/internet-privacy-in-india#fr10 (last visited on June 16, 2022).

thorough reform of the present data protection framework inIndia, which wasthen controlled by the IT Act, 2000 and the other relevant rules of 2011.[22]

The bill provides a mandate for how information pertaining to persons must be handled and stored,and it also outlines the rights of individuals in relation to the information they provide about themselves. In order for this legislation to be enforced, it is intended that an autonomous organization, the *Data Protection Authority* (DPA), would be established in India.[23]However, in May 2021, a fourth extension was granted to the Committee to submit its report for deliberation in the Parliament.

On 25thFebruary 2021, the *Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021*,were released by the Ministry of Electronics and Information Technology. The 2021 rules replaced the *Information Technology (Intermediaries Guidelines) Rules of 2011*, with an aim "to provide ordinary users of digital platforms to seek redressal for their grievances and command accountability when their rights are infringedand distinguishbetween '*social media intermediaries'* and '*significant social media intermediaries'* based on user numbers and place. A much heavier burden on significant social media intermediaries in respect of personal data protection. For instance, all social media intermediaries are now required to have a grievance redressal mechanism for users, conduct due diligence if they wish to seek refuge under safe harbour provisions and ensure the safety and dignity of users (especially women) online. However, significant social media intermediaries must institute additional due diligence mechanisms. These include the appointment of a '*Chief Compliance Officer*' (CCO), who must be resident in India and will be responsible for ensuring compliance with the law and a nodal contact person, who must also be resident in India and available 24/7 for coordination with law enforcement agencies. Significant social media intermediaries must also publish a '*Monthly Compliance Report*' (MCR), which will include details of any complaints they have received and actions they have taken to address said complaints".[24]

[22]Devika Sharma, "Personal Data Protection Bill, 2019 –Examined through the Prism of Fundamental Right to Privacy – A Critical Study", *SCC Blog*, (2020), *available at*: https://www.scconline.com/blog/post/2020/05/22/personal-data-protection-bill-2019-examined-through-the-prism-of-fundamental-right-to-privacy-a-critical-study/ (last visited June 11, 2022).

[23]Dr G. Mallikarjun and B. Md Irfan, "Right To Privacy In India: The Technical And Legal Framework," 6 *Journal of Positive School Psychology* 5785–90 (2022).

[24] Aditi Subramaniyam & Sanju Das, "The Privacy Data Protection and Cyber Security Law Review: India", The Law Reviews (Nov. 5, 2021), available at: https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/india (last visited on June 16, 2022).

NATIONAL SECURITY & DATA TRANSPERANCY

The 23rd Session of the Human Rights Commission was held in April 2013, where the members discussed the relevance of privacy & freedom of speech and the use of state surveillance mechanisms for reforming national security. This defined the meaning and importance of National Security &the misuse of law in the name of it, stating that: "*Innovations in technology have increased the possibilities for communication and protections of free expression and opinion, enabling anonymity, rapid information-sharing and cross-cultural dialogues. Technological changes have concurrently increased opportunities for State surveillance and interventions into individuals' private communications. The concept of national integrity or security is usually defined very broadly and is vulnerable to misuse as a means to target certain kinds of actors and propagate unnecessary secrecy around law enforcement measures, thus hurting transparency and accountability*.[25]

Article 12 of the *Universal Declaration of Human Rights* (UDHR), along with other International Conventions,guarantees the protection of the right to privacy of human beings, as an important human right. The need for uniform legislation must be reformed to better protect and preserve basic rights in the *age of digitalization*. Rights to digital media and technology are intertwined with freedom of speech and privacy because they grant people the liberties that accompany these technologies, including the freedom to use the internet, mobile phones, and other electronic devices.Digital technologies are influencing the exercise, protection, and violation of fundamental rights such as freedom of expression and access to information, as well as the recognition of new rights. The law is therefore adjusting to this new era through the establishment of digital rights and digital citizenship, permitting and regulating secure and transparent access to online information.[26]

Protection rules have a propensity to direct databases in both the law of India and the law of the United Kingdom (UK). There is a similar "assent rationale" in Indian and British legislation, which shows that the rule of law of certainty produced in the UK is a source of

[25]*Refer to* "A/HRC/23/40" of General Assembly (2013), *available at:* https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf.

[26] "Digital rights, essential in the Internet age", Iberdrola (2020), *available at:* https://www.iberdrola.com/innovation/what-are-digital-rights#:~:text=Digital%20rights%2C%20closely%20linked%20to,rights%20for%20the%20Internet%20age. (last visited on June 17, 2022).

inspiration. This model demands that individual data needs to be obtained for particular reasons/purposes from a man merely after his assent\sand data so gathered ought not to be employed for any causes other than those to which the man consented. The divulgence of individual data to another for a specified cause under legislation of certainty is like agreeing to use by that other of data thus disclosed for such reason.[27]

In November 2021, *P.P. Chaudhary*, the Head of the *Joint Parliamentary Committee* (JPC) formed for reviewing the proposed Data Protection Law, said that "procedures built into the bill provide for a framework even more detailed than the Constitution. We have removed the provisions of public order and morality from the clause. But one must understand that national security cannot be compromised instead of individual privacy. When the central government is satisfied that it is necessary and expedient, it may grant exemptions, say to the army or to Intelligence Agencies, but under only the conditions provided for."[28] The JPC in its report suggested that this new data protection legislation shall grant more authority to the state and lesser obligation on government agencies in case of any disruption of rights or public order. Although the opposition termed this legislation as an act that shall grant "*unbridled power*" in the hands of the centre.[29]

CONCLUSION & SUGGESTIONS

Data is the new oil for the 21st century, with technology growing at a rapid pace, andthe use of AI in every modern technology raises some issues relating to breach of data privacy relating to it. Such technologies use some amount of data or information; thus, the choice of making information selectively disclosable becomes pertinent. Right to privacy or right to be forgotten is one such privilege that enables that choice. The extension of the right to privacy is data protection. Data protection is a mechanism to protect the privilege of privacy that has been guaranteed to every person in India by virtue of the decision in the Puttaswamy case.

The ultimate law of the nation in India is the Constitution. The Constitution of India is an ever-evolving document, adaptive to the changing conditions of the world around it. This is an unarguable reality that cannot be refuted. In India, there is no specific legislation that relates to privacy or data protection in a comprehensive manner. The existing framework is

[27] Meenakshi Bains, "Right to Privacy in Digital Era", 6(1) *Amity Law Review* 63,66 (2015).
[28] Deeksha Bhardwaj, *National Security comes before Privacy, says Data Protection Panel Chief*, Hindustan Times, Nov. 25, 2021, 11:37AM, available at: https://www.hindustantimes.com/india-news/national-security-comes-before-privacy-says-data-protection-panel-chief-101637863651248.html (last visited on June 13, 2022).
[29] *Ibid*.

through combination of various pre-existing legislations, such as the *Information Technology Act, 2000*. However, the amendment to the Act in 2008 didn't effectively deal with the issue of data protection as a whole, but in bits and pieces. The *Data Protection Rules of 2011* and *The Personal Data Protection Bill, 2019*, which is based upon the *European Union's General Data Protection Regulation, 2018,*are a step in a positive direction. However, there are various concerns, such as blanket exceptions to state actors, that haven't been addressed while drafting the *Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021*.

The Lack of Digital Literacy in India has resultedin many cyber frauds and scams at the national and global levels. The use of the internet has been most widely encouraged by the anti-national elements to wage attacks and riots in the name of religion. To curb this menace and protect the sovereignty of the state, we need to establish an effective oversight mechanism to monitor such activities is much needed. Furthermore, judicial oversight alone is not enough; rather, all three branches of government should be engaged. Independent and adequately resourced parliamentary committees, review boards, data protection commissioners, independent advocates, and ombudspersons all have the potential to provide oversight of both state and business conduct.Professional standards and codes of conduct for those who are tasked with monitoring data surveillance need to be developed. Such standards could be developed at a regional or potentially international level through consultations with stakeholders. Reporting requirements, applicable to both businesses and states, are also an integral part of maintaining transparency and allowing oversight.