International Journal of Law, Policy and Social Review
www.lawjournals.net
Online ISSN: 2664-6838, Print ISSN: 2664-682X
Received: 07-05-2024, Accepted: 28-05-2024, Published: 22-06-2024
Volume 6, Issue 2, 2024, Page No. 146-150

Future perspective/Emerging trends in data privacy (DPDP Act, 2023)

Surendra Singh Chundawat[1], Laxmi Bhati[2]
[1] Assistant Professor, Department of Law, Janardan Rai Nagar Rajasthan Vidyapeeth (Deemed to be University) Udaipur, Rajasthan, India
[2] Research Scholar, Department of Law, Janardan Rai Nagar Rajasthan Vidyapeeth (Deemed to be University) Udaipur, Rajasthan, India

Abstract
In India, the law of data protection has been in contemplation for last about ten years and has gradually seen the changing shades of the societal demands of data protection. The vital concept of privacy introduced in the famous landmark judgment rendered by the Hon'ble Supreme Court in the case of Justice K.S. Puttaswamy (Retd) Vs. Union of India, gave an impetus to the data protection and privacy rights, making them akin to the Fundamental Rights. The concern of the country was the control of data, which was not there within the country and was seemingly lodged in the countries, like the United States.
The large-scale indications in the market and economy for the data management and data control as well as data protection became relevant, as the economy of the country grew beyond the national parameters. The integration of the data protection with the economy provided a mass scale requirement of interwoven protection in laws for the purpose.
The proposed law in the Parliament started taking shape in the year 2018, but when it was introduced as a Bill, it could not be finalized until August, 2023 when the first legislation was promulgated with the idea of protecting the personal data of individuals and also usage of data for the purposes of law. The balance between the privacy and requirement of the State is the key issue in the Indian Data Protection Act, and the concerns of both sides which are a private data right-holder versus the government data controller, have to be significantly dealt with to ensure a proper and effective data protection.

Keywords: Personal data, data control, data regulations, technology, artificial intelligence

Introduction
With the advent of civilization, fire and wheel gave strength to stabilize the homo sapien. Science and Technology helped the progress of human society. While such leaps and bounds of growth were going on, the modern society realized that a by- standing equipment in the shape of data became the most powerful tool of the day. The change in dimensions occurred due to the immense power that got attached to data control and data protection. Data generation not only multiplied the speed at which the societal changes take place, but also created a tool which could contribute towards stability and progress on one hand and destruction of the organized society on the other hand.
The law fraternity has an immense responsibility to study all facets of data generation, data control and data protection to make sure that the positivity attached to the most powerful tool of the day remains.

Advancements in Technology
The landscape of data privacy is inextricably linked to technological advancements. As we stand on the cusp of the Fourth Industrial Revolution, characterized by the integration of digital technologies into every aspect of society, the stakes for protecting personal data have never been higher. Innovations such as 5G connectivity, edge computing, and the Internet of Things (IoT) are reshaping how data is generated, processed, and utilized.
The proliferation of connected devices, from smart home appliances to wearable gadgets, has led to an exponential increase in data points. While these technological marvels enhance convenience and efficiency, they also raise concerns about the scope and granularity of personal information collected. The Act, while addressing conventional data sources, may struggle to encompass the entirety of data generated by these emerging technologies.

Rise of Artificial Intelligence and Machine Learning
Artificial Intelligence (AI) and Machine Learning (ML) are pivotal in the data-driven future, playing a central role in automating processes and extracting insights from vast datasets. However, the synergy between AI/ML and data privacy poses intricate challenges. AI algorithms often rely on large datasets to learn and make informed decisions, but the ethical use of such data becomes a paramount concern.
The Act, while being silent on the role of AI in data processing, might require further refinements to ensure that the principles of transparency, accountability, and fairness extend seamlessly into the realm of algorithmic decision-making. Striking a delicate balance between fostering innovation and safeguarding individual rights is an ongoing challenge in the face of evolving technological landscapes.

Impact of IoT on Personal Data
The IoT ecosystem, comprising interconnected devices sharing real-time data, epitomizes the interconnectedness of the modern world. From smart cities to industrial IoT applications, the vast network of sensors and devices collects and transmits an unprecedented volume of data. While this interconnectivity enhances efficiency and functionality, it amplifies the risks associated with data breaches and unauthorized access. The Act, with its emphasis on consent and purpose limitation, needs to adapt to the dynamic nature of IoT-generated data. As devices autonomously communicate and exchange information, ensuring that individuals retain control over their data in a seamless and meaningful manner becomes imperative.

Addressing the challenges posed by the IoT landscape is crucial for the Act to remain effective in safeguarding personal data in a hyper-connected world.

Impact on Individuals, Businesses, and the Economy
Empowering Individuals through Data Control
One of the primary objectives of the Act is to empower individuals with control over their personal data. By delineating the rights of individuals, including the right to access, correct, grievance redress, nominate, and erase their data, the legislation aims to rebalance the power dynamic between individuals and Data Fiduciaries.7 This empowerment has implications not only for personal privacy but also for the broader concept of digital autonomy.

Compliance Challenges for Businesses
The Act places substantial compliance responsibilities on businesses, requiring them to align their data practices with the stipulated regulations. This entails investing in robust data governance structures, implementing privacy-by-design principles, and establishing mechanisms for obtaining and managing consent effectively.
Small and medium-sized enterprises (SMEs), in particular, may face challenges in adapting to the stringent requirements of the Act. Compliance not only involves a financial commitment but also necessitates a cultural shift within organizations to prioritize data protection as a core business function. The economic impact on businesses, especially those operating on thin profit margins, raises questions about the feasibility of stringent data protection regulations.

Economic Ramifications of Stringent Data Regulations
While the Act aims to enhance data privacy, its stringent regulations may have unintended consequences for innovation and economic growth. Businesses, especially those reliant on data-driven models, may find it challenging to navigate the intricate web of compliance requirements without stifling creativity and competitiveness.
The economic landscape must strike a delicate balance, ensuring robust data protection without impeding the dynamism of industries that thrive on data-driven innovation. Policymakers need to continually reassess the economic impact of data protection regulations and calibrate them to foster innovation and sustainable economic growth.
The Data Protection has seen the new heights in the modern day digitization of the dimensions of daily life. The moment the significance of the Data Protection increased, the society had to deal with a direct conflict between the control of Data, Data Privacy and State intervention.
The development of Data Protection in India began with the series of precedent law, which started connecting the Data Protection as a constituent of Part III of the Constitution of India.
As the rights strengthened, Justice B.N. Srikrishna Committee proposed a Draft Bill to strengthen the individual rights, and giving privacy an element of importance. The Draft Bill could not meet the expectations of the thinkers and came under heavy criticism as it did not give the supremacy to the individual rights of privacy giving a controlled reign into the hands of the State.
The journey took a leap when the consolidation of such thoughts was made by the experts and the landmark judgment was rendered by the Hon'ble Apex Court in the case of *Justice KS Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 641*, whereby the societal concerns of the basics which constituted the privacy in a legal jurisprudence and the Indian conditions were looked into in a detailed manner. The concern of the State was obvious and the security concerns being an important element, would have completely overshadowed the right to privacy unless such thought process was evolved.
The cause of concern for the individual breach of privacy was not only commercial in nature, but also included the State surveillance as it was a reflection which overshadowed the concerns of an individual. The economic and the financial impact of the data for the business houses as well as for the State had its own role to play in the development of this law.
On one side, there was an individual citizen, who had recognized the precious rights which were emanating out of the data collection, and on the other side, were huge business forces which required data for enhancing the concept of data-based business. Though the State did not pay any heed to the right of a common citizen at the early times, but slowly the concept changed.
In *Justice KS Puttaswamy (Retd.) (supra)* where the Aadhar Card data was at stake, which included personal data of an individual, it triggered a concern among the citizens as to how such data, like retinal scans and fingerprints could lead to a huge issues for the private person in the long run, even leading to breach of his private aspects of life.
A common WhatsApp user, who ordinarily was given with a tag line of end-to-end encryption and particularly when, WhatsApp became a societal platform breaking across the user base from rural to urban, from commercial to daily usage, illegal to legal uses and societal binding uses was a game-changer. Owing to activation of social media to the immense seamless boundaries, the end to end encryption became an issue which impacted and affected the minds of the ordinary users. The WhatsApp introduction into the arena of data protection also gave an insight to the common man as to how far a privacy issue can be stirred, while dealing with the most powerful media, that was the social media. At one stage, WhatsApp itself created a huge anxiety of sharing the data with its sister concerns on count of commercial complexities, but at the same time, raising popular anxiety amongst the common men.
The growth of data protection vis-a-vis the importance of data for general use, were the two pressures that were being laid upon this concept and there was no easy solution to the same. The past could not give an answer as it did not cater for the privacy issues, but at the same time, in the current times, the gigantic concept of privacy and data protection became a cause of concern. The politico-economy status quo resulted into stagnation of the data protection laws at one stage, even when the societal pools for creating fresh laws, looking into the ramifications of the issue, was creating an internal tension in the society. The control of the data became the hallmark of power, whether it was by the political parties, or by the business houses. As the new aspects walked into the daily life of a common man, the significance of such regulations increased manifold.
The privacy which was only within the realms of a person's private domain which could include his home or bedroom, suddenly became a cause of societal discourse, as the privacy came in open on a social platform breaching the

private boundaries of an individual and causing a revolution in usage of technology, culture and society, requiring immediate legal solutions. The privacy which remained in the domain of an individual space, suddenly was breached by the beast force of technology and became a phenomena which was difficult to deal with. On one side, the private person was struggling to understand that as to how much control he still has over his data, which seemed like his property, and the answer of a common man would be that he demanded control over such property. The invasion was very difficult to sustain.

The information became the new formula for success and as it became more and more precious and volatile, the control over the information became a challenge to the society and the State. The technology boom provided an impetus giving a huge leap forward to the issue of data protection.

The issue of data protection was not only eminently walking into the lives of a common man as well as the State in our country, but also world over had an impact, which made it an international issue, where the lines between the advanced countries and the developing countries diminished as the right to privacy of a common man gained strength and the importance of such rights also took a sudden search.

The evolution of the law became strong in our country as event after event, it unlocked the involvement of the data being collected by the State, the business houses and the social media houses. The social media impact was so humongous that the Courts suddenly delved deep into the concept of connecting the right to privacy with right to life and giving it a protective layer of cover under Article 21 of the Constitution of India. The initial indulgence by the Indian Judiciary did not require the privacy to become a part of the Constitution as the privacy was only a concept without any threat and remained in the realms of the individual space. However, the push and pull between the power of the data kept on strengthening the privacy rights simultaneously.

In India, the phone tapping which became a huge issue by the Telecom operators and became a cause of concern for the Courts also, as the Telecom operators misused and abused the privacy causing serious negative impact on the public morale, and the morale constituting the individual privacy. The old movies used to show as to how the breach of privacy of the State had often lead to the powerful becoming weak and the State being impacted by the breach of such privacies which was a thought process in the imaginative minds of the film-makers. Gradually, with the States competing for more information about each other, and the State had become vulnerable through private information, it became a cause of larger concern and actually the States indulgence practices of breaching the privacy of the State Heads and particularly, the ones holding sensitive and high offices, giving rise to a general anxiety to the political structure for controlling the breach of privacy at one hand, and to create breach of privacy on the other hand.

The economic offences were another aspect which gained momentum on the shoulder of the technology whereby individual data was being misused and captured for the purpose of jeopardizing the concept of public safety. The sharing of the data by the people amongst each other became extremely sensitive due to the banking operations falling within the domain of the data control, the people abusing and misusing the data were found to cause severe dent in the credibility of the sensitive systems like that of banking system. The defence was another sector where the data control and the data breach conceptualized into an important element of warfare and secrecy.

Ultimately, the judgment rendered in the case of *Justice KS Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 641*, firmly enshrined the privacy as a Temple of an individual, the sanctity of which was required to be maintained at all costs. Suddenly, the twinkling right of privacy became a fundamental right, and also the significance of which was realized by the State as well as the private owners. The right to privacy also breached the national borders, and had an impact on the international frameworks, where it was required to have a common platform to meet the challenges which were arising out of the control and breach of the data. The popular social media platforms, like Facebook, Instagram and Twitter were running on a very high pitch for data control impacting the understanding of privacy for a common man.

The consolidation of the issue of privacy was considered by the Parliament for the purpose of a balance between the data protection, data consolidation and the data usage. On one hand, the messaging and communication services towered in the day to day life of a common man, and on the other hand, the race to control such data became an unlimited race. The access to data was an empowering impact and any kind of data erasure could also lead to a human emergency, and thus, the tool became a weapon and weapon became a concept.

The formulation of laws required a strong legal regime to balance the interests between the data protection and the data sharing, which were both essential and elementary concepts for development and growth of human society.

The Data Protection law was continuously being amended as the societal demands kept on fluctuating creating an awkward position for the State which in the fast developing process required to change its visionary aspects in smaller time durations. An absolute control of the data by the State was being resisted, whereas data sharing became a part of empowering, and thus, could not have been stopped.

The government slowly developed a thinking of having a limited control over the data so as to ensure the safety and security of a common man as well as the national issues, thus, making a breach into the complete spectrum of privacy, which was required to be dealt with in a sensitive manner. The executive control of the data for the purpose of surveillance became an idea which had to exist with the clear safeguards although a common citizen was not comfortable with such an idea.

The concept of a legitimate aim to control data for the purpose of larger sharing and widespread development could not have been avoided but certainly with safeguards which could restrict the abuse of the data in question.

The power of data was seeing the far-reaching consequences. The State interest and the private interest were no longer easy to balance and the stakeholders were equally worried to have their say in the process of development of law.

The powers and functions envisaged in the law raised the bar for the action of the State in privacy matters particularly, when sensitive personal data was involved. The concept of data kept on evolving. The State's might which sought control of data for providing a social security to a common man, became the first target of the societal fears and there was a decline in the fiduciary role of the State.

The development of law though try to create an equilibrium between the intervention to be permitted by the government for the purpose of control of data by giving them a wide role in the governmental
duties/governmental role in acting for such purpose.

The international development was also becoming a guiding force for such laws. Every aspect of human life including the day to day activities of eating, sleeping, drinking, purchasing, commodity consuming, activities governing individual habits and exercising became a value added data and collection of which became inevitable. The medical records became a landmine for the insurance companies and the exploratory medical community as they treaded on a path which directly breached the inner sanctum of an individual's privacy.

On one side, in the name of scientific research and implications, the data fiduciaries' role was getting enhanced, our country also saw a purge in the digital economy, which also included precious data. The data was required to see the smooth sailing for the purpose of growth in economy and the changing values of the financial aspects. The classification in various kinds of data diminished and despite serious deliberations in law, any perfect solution for balancing the equities between data protection and data usage was difficulty to demarcate.

The blurring of the lines between the personal data and non-personal data also created complications. The processing of data by an individual, any business house or the State became a source of conflict amongst the various stakeholders. However, to say that the law failed would not be fair to the law-makers who have tried to ride the tide of enhancement of the role of data in providing an appropriate relief and respective usage of the data science.

The Government also realized the need to align with the societal demands and thus, swallowed hard the dimensions of data protection which had the direct bearing upon the national security as well.

The role of the State in the phenomena of data control/data usage/data consumption put the personal data in an ambit which required sensitive handling. The State and the stakeholders including the businessmen were expanding the horizons of data, with the intention of breaching every single possibility of data collection and data consumption.

The time has arrived where the complete control of data with the State was not palpable with a common citizen and would amount to returning back to the strict State regimes which have been blurred with the democratic advancements made by the humanity, but at the same time, the concerns of the legislators raised by the involvement of national security, sovereignty and public order in the hands of the data holders, can be genuinely and bonafidely understood for the purpose of appreciating the value of a data.

The State though acting in a visionary mode could not plug all the holes which were there in the data science and thus, required serious contemplation to go on for the purpose of maintaining the equilibrium between the data protection and data consumption.

The data becoming a bigger force creating bigger responsibilities and with national interest as well as the individual interest expanding its boundaries for making a meaningful and an effective enhancement of the concept of data gained its own significance.

The State also contemplated the members appointed by the Central Government to deal with the checks and balances to be adopted as a mechanism for dealing with / handling with the data with good amount of transparency.

The State understood that with a discretion and categorization of sensitive personal data and notifying data fiduciaries, the directives to the Data Protection Authorities (DPA) on public policy and on the interest of national security and sovereignty were being highlighted upon.

The State organs had to become mature to such understanding, whereby interference of functional autonomy to deal with the data in question became a significant aspect.

The individual existence culminated into societal existence and such societal existence created a web of public and private dealings wherein the network in question had to work for the equilibrium to be drawn for consumption and protection of data.

The right to privacy which was always a flexible concept but with the stakes rising high and the communication and consumption of data became valuable, the risk factor to the data science being abused. The consequences of data becoming a victim of unlawful usage caused a furor in the society. The impact of the data consumption increased manifold and thus, the control of the data in the garb of creating a common societal web, for usage and consumption of such data without delving into the personal aspects of the data, was tried to be brought in, as a solution by the business houses.

The mapping of the data has suddenly become a process in vogue for the economists, politicians, architects, lawyers, teachers and every class of the society, as it gets impacted by spread of such data. On one side, there is an unquenched thirst of the data spreading into the society, whereby a person needs more information, knowledge and data for the purpose of operating smoothly, and on the other side, there is a direct challenge by the stakeholders, who wish to control the data for the purpose of privacy and personal skills enhancements.

The whole lot of grey-areas created a nature of crime, which became an industry in itself and the data theft as well as misuse and abuse of data became a whole concept which posed a serious challenge to the concept of rule of law and slowly the industry of data misuse and abuse became a whole time challenge to the law and order and became a serious cause of sufferings for a common citizen. The data theft and data abuse led to humongous losses to individuals, particularly the vulnerable class i.e. the old aged people, the lesser aware and lesser educated people and innocent citizens, who fell in the web of crime generated through data leakages/data consumption/data spread. This challenge now in the shape of data abuse is combined with the concept of Cyber crimes, resulting into a very challenging time for the State and the law & order machinery.

Thus, the concept of data protection has grown as a boon as well as a bane which our country as well as the world as a whole would require to stand up to and while permitting the humanity/common citizen to enjoy the optimum data privacy to the every possible extent, they have to also utilize the power of data for enhancing the safety, security and development of the humanity. Unless such power is utilized by the changing trends and by meeting the requirements of statutory changes and continuous development of jurisprudence, we shall not be able to utilize the potency of this huge tool of progress, which is also a part of our daily life.

Conclusion

If the law fraternity is able to synchronise the data and its protection, then it will not only serve humanity in its growth and developmental process, but also shall give peace to the common man. The satisfaction of dealing with data in an organized manner is bound to create a huge impact upon the societal growth and stability. The parameters of data shall have to be continuously worked upon in the larger interest of the society. The flexibility to deal with such situation which we as a society shall have to keep working on to ensure a balanced development and to continue to enjoy the power of data.

References

1. MP Sharma v, Satish Chandra. AIR 1954 SC 300
2. Kharak Singh v. State of *et al* U.P., AIR 1963 SC 1295, www.scconline.com
3. Wolf v. Colorado 1949 SCC OnLine US SC 102, www.scconline.com
4. 1975- Govind Singh v. State of M.P. 1975 AIR 1378, www.scconline.com
5. 1994- R. Rajagopal v. State of Tamil Nadu, 1995 AIR 264, www.scconline.com
6. K.S. Puttaswamy v. Union of India (2017) 10 SCC 1, www.scconline.com
7. 2018 – Sangamitra Acharya and Ors. v State (NCT of Delhi) and Ors., www.scconline.com
8. 2018 – Oommen Chandy v. State of Kerala &Raju Sebastian Vs Union of India, www.scconline.com