International Journal of Law
ISSN: 2455-2194; Impact Factor: RJIF 5.12
Received: 20-07-2020; Accepted: 05-08-2020; Published: 21-08-2020
www.lawjournals.org
Volume 6; Issue 4; 2020; Page No. 272-275

Personal Data And Privacy: In And Post Puttaswamy

Sameer Kumar Dwivedi[1*], Sanjay Prakash Srivastava[2]
[1] Research Scholar, School of Law & Governance, Central University of South Bihar, Gaya, Bihar, India
[2] Professor, School of Law & Governance, Central University of South Bihar, Gaya, Bihar, India

Abstract
The article discusses the importance of personal data and awareness of the citizens, invites a cross-disciplinary discussion on this issue. In *KS Puttaswamy v Union of India* (*Puttaswamy I*) Supreme Court ruled that a Constitutional Right to Privacy is part and parcel of the Constitution. This article is discussing privacy policy deliberation in India and examines liberty, autonomy, and dignity as they have articulated within the *Puttaswamy I*, the mechanism of data collection by the government as well as by private institutions and the mechanism of data protection policy, and practices. The article also, analyzes the current policy landscape in India, and submits the limitations of data-driven decision-making should be a fundamental consideration in privacy policy development, it must be up to date to tackle the problem of data theft, protect the misuse of power concerning data collection and processing.

Keywords: aadhar, privacy right, personal data, data protection, state surveillance, monitoring

1. Introduction
In any form of the State, citizen's right has been considered of paramount importance. When the police state was transformed in the welfare state, the intervention of the state authorities increased including the intervention of the state in the personal life of the citizen. But still, this cannot be left in the hands of the arbitrary state authorities to interfere as and when they wish to interfere. Thereby regulation of the above whims of the state is required; preferably the state should be guided by the constitutional mandates and also by the apex court. However, the current debate on data usage concerns that companies are collecting significant amounts of consumer data and using it inappropriately to gain detailed information about consumers while the consumer may not have access to these insights or the ability to derive value from them. A five-judge bench of the Supreme Court in *KS Puttaswamy v Union of India* [1] (*Aadhar Judgement*) weighed the Aadhar [2] scheme against the right to privacy and largely upheld the Constitutionality striking down certain provisions. *Puttaswamy I* [3] and *Aadhar Judgement* [4] changed the legal landscape in India in at least two distinct way, First, they explicitly while recognized the harm of surveillance, especially in the digital age. Second, while building upon an existing foundation, they crafted a tiered proportionality test applicable in a fundamental rights challenge.[5]

2. Data Technology Enabling Efficient Regulatory Compliances
These enormous data streams which are collected by these corporations and government can be utilized for the benefit of society using AI analyzing it, finding patterns, connections, and giving effective output. The emergence of a new concept in the system always shakes the proper functioning but does it mean entry should be banned or balance should be brought through controlled regulation? Cyber Laws are redundant and not on par with evolving technology. The prominent task is to align the security, laws and AI in one line to achieve desired growth and progress across the globe. Weighing this sweet and sour relationship of AI and Decision making will open the plethora of issues, Recently, Google partnered with NITI Aayog [6] to work on a range of initiatives including training and incubating Indian startups focused on AI. Through a series of events and speeches from earlier this year, Prime Minister Narendra Modi is seen to have been deliberately showcasing India as well as his government as technologically forward. According to a report, the prime minister wants NITI Aayog to adopt a comprehensive strategy for the commercialization of AI so that the national collective benefits from the technology [7]. The digital India [8] initiative of the government of India is a promising program and it is proving its usefulness by providing the basic

[1] KS Puttaswamy v Union of India (2019) 1SCC1
[2] Aadhar Act,2016 its full name is The Targeted Delivery of Financial and Other Subsidies, Benefits, and Services Act, 2016
[3] *Ibid1*
[4] *Ibid3*
[5] By Vrinda Bhandari and Karan Lahiri, The Surveillance State, Privacy and Criminal Investigation in India: Possible Futures in a Post-Puttaswamy World, available at http://ohrh.law.ox.ac.uk/publications/the-surveillance-state-privacy-and-criminal-investigation-in-india-possible-futures-in-a-post-puttaswamy-world/(last visited on July 10,2020)
[6] National Institution for Transforming India, is a policy think tank of the Government of India, established with the aim to achieve Sustainable Development Goals and to enhance cooperative federalism by fostering the involvement of State Governments of India in the economic policy-making process using a bottom-up approach.
[7] https://analyticsindiamag.com/has-ai-really-influenced-indian-lives-heres-the-real-picture/ (last visited on May 12,2020)
[8] Digital India is a campaign launched by the Government of India in order to ensure the Government's services are made available to citizens electronically by improved online infrastructure and by increasing Internet connectivity or making the country digitally empowered in the field of technology. http://digitalindia.gov.in/ (last visited on May 12,2020)

environment, infrastructure, and workforce to implement futuristic social welfare schemes and development programs of the government.

3. Privacy Capabilities and its Effects on Privacy Right

The old saying that cash is king is swiftly falling by the wayside. There can be no doubt that data is now king. The most successful businesses in the world must now deal with enormous amounts of data – and increasingly that data is gleaned from the actions of their customers. That data is gathered from an enormous number of sources [9]. Digital Footprint of the user and its effect on Data Privacy is one of the main focus of this research paper, to explore it the detailed study is needed but in India, there is no proper reporting about a privacy breach. Those have access to large datasets (because of the nature of their business models) it enables them to build a first-mover advantage when it comes to perfecting their algorithms and driving business value. Now Google-owned Android mobile phone operating system is a must and common, it offers limited opportunity to block advertising in the news section, websites, search section, and even in setting tab. And Google has no intention of giving up lucrative income streams that target consumers based on their online behavior. Large social media companies like Facebook and search engines are enjoying the same benefits and dominance of a large consumer base. AI needs massive amounts of data to be as effective as a human being in analyzing behavior – and those algorithms are getting better and better. It's that thorny issue of machine learning that is at the foundation of concerns when it comes to AI and privacy. A machine-learning algorithm may mine a user's sensitive personal data to supply human resources departments with information that the individual may not be comfortable to share with that department. Personal fitness devices are gathering data about your fitness which could be used for insurance purposes. All of this without human intervention Personal data is gathered from customer buying habits and their actions on the company's websites, blogs, social media accounts, and other sources. But it is also gathered from third parties [10]. Apart from basic user information and demographics, companies want to know about their shopping and personal habits, this does not necessarily and negatively impact the consumer.

4. *Quid Pro Quo* and Need of Fair Agreement Policy

Quid pro quo (something for something) is perfectly applicable with the digital service provider and a user of their services, it is well known that consumers sacrifice their anonymity when they use services of any social networking website for free. Think of Google and Facebook. There is a contract. It is not implied – it is part and parcel of the terms and conditions that consumers agree to when they use services and sites. So, consumers know that the information they supply and the behavior that they engage in will be used for (among other things) to target them with advertising. They also agree within those terms and conditions that these service *providers will be free to supply the information on their behavior to third parties* who use that to improve their sales through targeted advertising on those sites. The third-party sharing must be regulated properly as the GDPR [11] provides some restrictions and liability on data collector as well as the processor of the personal data. A mobile phone application can collect our name, contacts, relationship status, family details, photos, videos, emails, location data, IP addresses and many other kinds of data with or without the active consent of the user and it happens every moment because of this database and ability to process it our smartphone is smarter, much intelligent and much informed about us, it knows us more than we do about ourselves and by drawing together all collected data and building a coherent 'persona' from that data, without human intervention a machine learning algorithm can build an avatar of any single human being, including behavioral patterns, it is smarter than many people think about it. Collection of a large amount of data by business houses and other bodies is a serious issue and it is not acceptable to provide direct access of our sensitive personal data to anyone, whether by the government to non-governmental agencies and vice versa. The Supreme Court held that the right to privacy was an 'intrinsic part of the right to life and personal liberty under Article 21 and as a part of freedom guaranteed by Part III of the constitution [12].

5. Evaluation of Present Data Protection Mechanism of India

The access and use of biometric or other serious data of citizens without their proper and active consent is a serious issue of human rights as well as privacy rights. The privacy of personal data, inherent selection biases and resultant risk of profiling and discrimination, and non-transparent nature of their policy and safety measures and responsibility of proper care and attention on every step is serious debatable issues, permission for collection of biometric data and use of AI solutions are some of the issues requiring deliberation and proper recourse and serious attention of data experts, academia as well as of the legislature. Mitigating predicted privacy harms is a complex, multi-faceted problem that will be with us for many years to come. The discussion of privacy rights attracts many provisions of Human Rights, the I.T. Act [13] as well as the Constitution too, but we generally forget to discuss our contribution towards digital literacy and personal data behavior. After a long discussion in its *Aadhar Judgment* [14] the honorable Supreme Court has cleared many doubts about the use of AADHAR and declared it legal, the decision in respect of legality and guideline of its use is a great relief for the government as well as for citizen too. But the real issue before us is what attracts this kind of discussion, why the Supreme Court was engaged in this issue, and why some active intellectuals and citizens are demanding such relief from the apex court? In developing countries (also in India) privacy is a less-discussed and ignored point because people are less aware of its importance and in another hand, some people are compelling Supreme Court to declare AADHAR unconstitutional based on the violation of the privacy of

[9] https://www.cpomagazine.com/data-privacy/artificial-intelligence-and-the-privacy-challenge/(last visited on May 12,2020)

[10] https://www.cpomagazine.com/data-privacy/artificial-intelligence-and-the-privacy-challenge/ (last visited on May 22, 2020)

[11] The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area. It also addresses the export of personal data outside the EU and EEA areas.

[12] *Ibid. 3*

[13] The Information Technology Act 2000

[14] *Ibid. 3*

digital and biometric data, and some people are fully unaware or ignorant about the importance of personal data and Right to Be Informed [15], we are discussing Aadhar and biometric data collection and its safety but we are ignorant about our contribution to invite or donate our important data by clicking the acceptance button in any smart phone app. As social media and smartphones expand our digital footprint with amazing speed, this task is getting easier day by day, but in a developed country, Privacy protection and issues related to data protection are the most debatable issues. In real sense data is money; we are ignorant but not unaffected with it. Informational privacy is a facet of the right to privacy. The dangers to privacy in an age of information can originate not only from the state but from non-state actors as well. We commend to the Union Government the need to examine and put into place a robust regime for data protection. The creation of such a regime requires a careful and sensitive balance between individual interests and legitimate concerns of the state [16]. The EU General Data Protection Regulation [17] (GDPR) retains all the attention as it will regulate the world's biggest economic area. GDPR is the most important change in data privacy regulation in 20 years. But other approaches exist that might have an impact, from documenting model-building decisions to creating due process rights. The personal data Protection Bill of India is about to come, in absence of any dedicated law now privacy issues are being addressed by the Indian Telegraph Act 1885 and the Information Technology Act 2000.

The legal issues arising from the use of AI and data privacy in different spheres attract a serious discussion and the Central government has appointed Justice Sri Krishna Committee on data protection law to establish a data protection framework with legal backing. The committee has suggested 7-core principles of data protection and privacy are:

a. informed consent
b. technology agnosticism
c. data controller accountability
d. data minimization
e. holistic application
f. deterrent penalties
g. structured enforcement

are quite comprehensive and should provide a strong privacy protection regime. India's privacy protection regime will have to be continually updated to reflect an understanding of new risks and their impact.

The Global Initiative on Ethics of Autonomous and Intelligent Systems of the Institute of Electrical and Electronics Engineers (IEEE) has a chapter on 'Personal Data and Individual Access Control in Ethically Aligned Design'. The IEEE is suggesting some basic standards to cope with this issue and Indian enterprises and developers need to build this type of standards into AI design itself. In the technology realm, explainable algorithms are an area ripe for AI innovation, and some ongoing efforts on algorithmic transparency are summarized in the ICO Report [18]. An HBR (Harvard Business Review) study [19] found that people will accept potentially intrusive uses of their data, like predictions about their behaviors, in return for services like Google Now, and it's not only about value: trust is also important. On the other hand, a Pew Research study [20] shows that people's trust in the way corporations handle their data is eroding. As the Target pregnancy case shows, when customers lose trust, the result could be a public-relations disaster, trust of the customer is an important asset for the Corporations, and the losing trust means losing the customer, and the corporation should seize the opportunity to regain people's trust by handling their data with fairness.

6. Suggestions and Recommendations

India's unique challenges and aspirations, combined with the advancement and digitalization it requires large scale transformational interventions, primarily led by the government, and other governmental institutions. Our legal system, some Governmental bodies, and other non-governmental agencies are doing well by adopting necessary mechanism to protect the interest of the citizens they also provide suggestions and other necessary help to spread awareness in common people regarding the importance of personal data, their right and liability towards their right.

We can summaries the reasons why we are an easy target and how we can protect our privacy, are

a. Lack of enabling data ecosystems
b. The low intensity of AI research, Core research in fundamental technologies, Transforming core research into market applications
c. Inadequate availability of AI expertise, manpower, and skilling opportunities
d. High resource cost and low awareness for adopting AI in business processes
e. Unclear privacy, security, and ethical regulations e.g. the PDP [21] Bill, 2019 is pending before the Lok Sabha.
f. Unattractive Intellectual Property regime to incentivize research and adoption of AI

These challenges, while by no means exhaustive, if addressed in an expeditious and targeted manner through concerted collaborative efforts by relevant stakeholders, with the government playing a leading role, could lead to a fundamental change in the field of privacy protection. India can also take a leaf out of the UK's playbook, where a large amount of money is being invested to establish a new Centre for Data Ethics and Innovation [22] (CDEI), aimed at

[15] The General Data Protection Regulation (GDPR) gives individuals a right to be informed about the collection and use of their personal data, which leads to a variety of information obligations by the controller. https://gdpr-info.eu/issues/right-to-be-informed/ (last visited on May 02, 2020)

[16] *Ibid. 1*

[17] *Ibid. 13*

[18] https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf visited on ((last visited on May 22, 2020)

[19] Available at https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust (last visited on May 17, 2020)

[20] Americans and Cybersecurity, available at https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust ((last visited on May 02, 2020)

[21] The Personal Data Protection Bill, 2019 was introduced in Lok Sabha on December 11, 2019. The Bill seeks to provide for protection of personal data of individuals, and establishes a Data Protection Authority for the same. https://www.prsindia.org/billtrack/personal-data-protection-bill-2019 (last visited on May 01, 2020)

[22] The Centre for Data Ethics and Innovation (CDEI) is an advisory body set up by Government and led by an independent board of expert members to investigate and advise on how we maximize the benefits of data-enabled technologies, including artificial intelligence (AI).

enabling and ensuring ethical, safe, and innovative uses of data. This will include engaging with industry to explore the possibilities of establishing data trusts to facilitate easy and secure sharing of data.

7. Conclusion

It is noteworthy that on one hand, digitalization provides an opportunity to innovate across systems and processes but on the other hand, it raises major concerns within the legal framework that revolve around issues such as privacy, legal liability, enactment, and enforcement of regulatory laws, etc. The attention of governmental agencies and private players are doing well in this field and their effort will show a positive impact in this regard. The exact situation is that the privacy systems cannot be thought of as isolated mathematical problems, or as neutral in nature or as only beneficial because of their efficiency. Rather, the data protection technologies are complex, technical, and should not, be evaluated only based on efficiency and accuracy. Privacy has been termed as a fundamental right by the Supreme Court of India. The protection of this right with its multiple facets in a fast-changing technological environment will not just depend on State enforcement but also making citizens aware of their rights and how they can protect it. People often unknowingly give consent to sharing their data which they would not have ordinarily done had they known the purpose their data were being put to. There is an urgent need to spread awareness among individuals about the importance of consent, ethics, and privacy while dealing with technology. The collection, processing, and use of sensitive data should be protected. The agencies and person engaged in this proses ethical, legally, technically and philosophically responsible for any wrong with the stakeholder and requires proper care, attention, and imposes strict liability on the person or agency.

9. Acknowledgments

I, Sameer Kumar Dwivedi, author thanks ICSSR, New Delhi for financial support by awarding Short-term Contingency Grant.

10. References

1. Dr. Amita Verma. Cyber Crimes and Law (Central Law Publications), 2009.
2. Dr. RK Chaubey. An Introduction to Cyber Crime & Cyber Law (Kamal Law House Kolkata), 2008.
3. Dr. Farooq Ahmad: Cyber Law in India: Law on Internet, 2nd Edition (Pioneer Book Publication, Delhi), 2005.
4. Nandan Kamath. Law Relating to Computers Internet & Commerce, 2nd Edition (Universal Law Publications Co. Delhi), 2000.
5. R. Nagpal: What is Cyber Crime, 2003.
6. Ashish Pandey. Cyber-Crime - Deviation and Prevention (J.B.A. Publications), 2008.

https://www.gov.uk/government/groups/centre-for-data-ethics-and-innovation-cdei (last visited on June 12, 2020)