VOLUME 1 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

EVOLVING JURISPRUDENCE OF DATA PRIVACY: AN INDIA CONTEXT

- Adv. Vanya Diwan[1]

ABSTRACT

As in the 20th century control over oil resources became the power-wielding barometer, the 21st century has found its oil. It is none other than "data", which in simple terms a collection of facts that have the potential to become meaningful information. The Industrial Revolution 4.0 (IR 4.0) is rightly so the 'information age'. With the advancement of technology, interplay of Big Data Analytics, Artificial Intelligence and Machine Learning, data became an integral part of human existence. Identification of patterns and the correlations are crucial for human choices, and more so for the budding business ecosystem around it. The epithet set by the global tech companies like Google, Facebook and Uber is being emulated by small start- up ventures and has proved to be a guiding light for the Governments across the world. Both public and private sectors are employing these data analytics tools, collecting data at an unprecedented scale and using it for multifarious purposes. Data Privacy and Data Protection have occupied a center stage to the ethical use of data analytics by the big tech firms and government entities.

INTRODUCTION

With the transition from a classical economy to a digital economy, the data processing has already become ubiquitous. Data is valuable *per se*, but when it is collected, shared and stored, efficiency increases manifold. The reality of the digital ecosystem today, every transaction entails to a data transaction in some or the other form. Those involved in the collection, organization, and processing of personal data, whether directly or indirectly have transformed the traditional business models for the long haul.

A number of benefits are associated with collecting and processing personal data. Data mining and analysis allows detection of trends and accurate targeting. The knowledge from these

[1] Practicing Advocate, enrolled with the Bar Council of Delhi.

pooled datasets can be put to use to almost every facet of life. Employing such analytics enables organizations and governments to gain remarkable insights into areas such as health, food security, intelligent transport systems, energy efficiency and urban planning.[2] For instance, in the healthcare sector, employing trend analysis helps health care providers make better diagnostic predictions and treatment suggestions, banks can use Big Data Analytics to improve fraud detection.

However, data breach and misuse of data is a cause of concern. Data protection principles are designed to protect the personal information by restricting how information should be collected, used, shared, processed and disclosed. It has developed as a legal right in many jurisdictions because automated processing of huge and pooled datasets. In order to understand the issues surrounding data privacy, it is important to examine "how" and more importantly, "who" can use this personal information. The need for data protection thus arises out of the need to prevent data breach, and hinges on the question of who should be permitted to use personal information.

PRIVACY JURISPRUDENCE

Article 21 of the Constitution of India guarantees right to life and personal liberty.[3] Over the years, the Supreme Court has widened its ambit through its various judgements, it included within its purview right to live with dignity. Right to privacy is read to be a part and parcel of Right to life and personal liberty, it is held to be at the core of Right to live with Dignity.

The apex court in ***Kharak Singh v. State of Uttar Pradesh***[4], police regulations mandated to put habitual offenders under surveillance which included domiciliary visits at night. The court held that while Article 19(1)(d) deals with a particular species or attributes of that freedom, "personal liberty" in Article 21 takes in and comprise the residue, thereby, the restricting movement of an individual does not invade one's privacy. Adding to that the "right to privacy is not a guaranteed right under our Constitution." However, the minority judgement by Subba Rao J differed on this. In ***Gobind v. State of M.P.***[5], the court contemplated right to privacy is included within the ambit of right to personal liberty. The apex court held that even a woman of easy virtue is entitled to privacy.[6] The court expanded the scope of right to privacy that it includes right to be let alone and a citizen has the right to maintain privacy of his own, family,

[2] European Commission, 'European Data Protection Reform and Big Data: Factsheet', 2016, https://ec.europa.eu/info/law/law-topic/data-protection_en.
[3] INDIA CONST. art. 21.
[4] (1964) SCR (1) 332.
[5] (1975) 2 SCC 148: AIR 1975 SC 1378
[6] *State of Maharashtra v. Madhukar Narayan Mardikar*, (1991) 1 SCC 57.

marriage, procreation, child bearing and education among other things.[7] It expands to telephone-tapping, which amounts to violation of right to privacy unless it is permitted under procedure established by law.[8] It also extends to protecting the confidential health information but it isn't an absolute right, a HIV positive person does not have the right to privacy against the doctor not to disclose his status.[9] In addition, the court has held that involuntary subjection of a person to tests such as narco-analysis, polygraph examination and the BEAP violates the right to privacy.[10]

Privacy has been recognized to be an important facet to enjoy the Right to live with dignity.

DATA PRIVACY JURISPRUDENCE

The Data Protection rules formulated under **Section 43A Information Technology Act, 2000 (IT Act)** referred to as **The Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011 (SPDI Rules),** to a limited extent adopted the **Organization for Economic Co-operation (OECD) Standard Guidelines, 1980.** It restricts to collection limitation, use limitation, purpose specification and limited individual participation. The rules are applicable only over the corporate entities, incorporated inside or outside India, leaving the government entities outside its ambit. **The Aadhar (Targeted Delivery of Financial and other Subsidies, Benefits and Services) Act, 2016** referred to popularly as the Aadhar Act, brought this ambiguity to the fore. The Aadhar Act enables the government to collect and store personal data of its citizens including their biometrics, to issue a unique identification 12-digit identification number by the **Unique Identification Authority of India (UIDAI)**. The novel purpose being to provide targeted services to its citizens, especially targeted subsidies. The UIDAI is obligated to ensure security and confidentiality of the identity information and prohibits sharing of such information with third-party entities. However, it has been observed that the data protection principles are flouted by the authority and it has come under public criticism. The mandate of the act was to grant discretion to the citizens, however, its usage became mandatory and got looked upon as a coercive State act. With such a humongous data set of the nation citizens' being stored and accessed by the government surrounds a potential database breach scare and makes it susceptible to cyber attack. The sharing of such information with third-party entities is another grey area.

[7] *R. Rajagopal v. State of T.N.*, (1994) 6 SCC 632.
[8] People's Union for Civil Liberties v. Union of India, (1997) 1 SCC 301.
[9] *'X' v. Hospital 'Z'*, (1998) 8 SCC 296.
[10] *Selvi v. State of Karnataka*, (2010) 7 SCC 263,370: AIR 2010 SC 1974.

The debate surrounding whether 'privacy' forms an intrinsic part of Right to life and personal liberty was finally settled by a nine-judge bench of the Supreme Court in the landmark judgement: ***Justice K.S. Puttaswamy (Retd.) v. Union of India & Ors***.[11] It recognized privacy as an inalienable fundamental right. The court also recognized 'informational privacy' as:

> "*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.*"

It puts the onus on the government and other private entities to come up with reasonable justification in case of its derogation. It adds to the literature of the data privacy jurisprudence with the 'element of necessity', the State must while exercising its discretion needs to fulfil a legitimate aim for state action. The court also enlisted certain legitimate cocerns of the state as: protecting national security, preventing dissipation of social welfare benefits, preventing and investigating crimes and encouraging innovation.

KEY CONCEPTS OF DATA PROTECTION

Personal data:

The word 'information' is defined in the Information Technology Act, 2000 (IT Act, 2000):

Section 2(1)(v):

> *"information" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro films or computer generated micro fiche;*

Not all information about an individual comes within the ambit of 'personal data'. It only encompasses that information which 'identifies' an individual. The question of 'identifiability' is central to data privacy.

Personal Sensitive Data:

Section 43 A of the IT Act mandates the body corporate possessing, dealing or handling any sensitive personal information should not allow it cause any wrongful loss or wrongful gain to any person. The act does not *per se* define the personal sensitive data; it puts the onus on the Central Government in consultation with professional bodies or associations to define it. As per that view, it includes within its ambit Genetic information, Health information, caste

[11] (2017) 10 SCALE 1.

information, racial origin, sexual orientation, ethnic origin and religious beliefs.

Data Processing:

Personal data and Personal Sensitive Data collected, stored and used, whether manually or automated amounts to data processing. It also includes any other ancillary activity associated with these three operations. Given the extent by which automated data can be processed and put to illicit use is the core area of data privacy.

Data Collectors and Data Processors:

Control over data is central to data privacy, the entities that collect data and are required to comply with the data protection norms is termed as a 'Data Collector', this could include the person voluntarily providing information to the entity or the entity storing the information without prior consent. Data Processors are involved with the processing of data and works under the data controller. [12]

There are certain 'key principles' to be borne in mind while drafting Data Protection legislations:

1. **Technology agnosticism**: The law must be accommodating to take into account the changing technologies and compliance standards.
2. **Holistic application**: The private sector and government entities must comply with obligations, though differential in scope.
3. **Informed consent**: Consent must be fully-informed and meaningful.
4. **Data minimization**: Data collected should be minimal, 'personal data' should not be unnecessarily stored.
5. **Controller accountability**: Data processing by the Data collectors or third-party entities shall be held accountable.
6. **Structured enforcement**: Data Protection Framework must be enforced by a statutorily empowered authority.
7. **Deterrent Penalties**: In case of data breach, adequate deterrence must exist and enforced by the empowered statutory authority.[13]

The data protection legislation should encompass both **natural and juristic persons**, while in

[12] 'OECD Guidelines Concerning the Protection of Privacy and Trans border Flows of Personal Data', 2013, https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part1.

[13] Justice B.N. Srikrishna, White Paper of the Committee of Experts on a Data Protection Framework for India, 2017, https://www.meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf.

most jurisdictions it is still applicable on the natural persons, companies especially the big technology giants are the beneficial owner and user of data in this day and age. It is important for the data protection legislations to acknowledge the same.

DATA PROTECTION LAWS: POSITION IN INDIA VERSUS OTHER JURISDICTIONS

The **Organization for Economic Co-operation(OECD) first- generation Standard Guidelines, 1980**, are considered as a harbinger of 'data' privacy' which has been emulated by over 120 countries.

Relying on the above guidelines, two popular and distinct models evolved in the data protection regime:

1. EU model, and
2. US model

The two models function on different aspects of privacy, while the former places reliance on '**individual privacy**', the latter on '**information privacy**'. In the EU-model, right to privacy is recognized as a fundamental inalienable right, whereas in the US-model emphasis is on unrestrained innovation, thereby disregarding the rights of the vulnerable section of the society.

The **EU General Data Protection Regulation of 2016** (EU GDPR)[14], is considered the most comprehensive and stringent data protection laws in the world. It is made applicable on all private and government entities processing data with the sole exceptions being national security, defence etc. It follows a rights-based approach revolving around the individual privacy, it prohibits collection of sensitive personal data subject to certain restrictions. The unique feature being individual participation rights are guaranteed within the legislation itself, which empowers the individual to control the use of data post collection. It empowers an independent supervising authority and equips it impose penalties.

The EU model is adopted in various jurisdictions, the famous being the co-hybrid models of Australia and Canada (PIPEDA, 2000).

The usage, storage and transfer of personal data in India was governed by **Information Technology (IT) Rules, 2011** under the IT Act, 2000. To streamline the personal data law based on global best practices, **The Personal Data Protection Bill, 2019** was introduced in the Parliament. It governs the data processing by the following entities:

[14] EU GDPR, GENERAL DATA PROTECTION REGULATION, 2016, https://gdpr-info.eu/.

a) the government,
b) companies incorporated in India and,
c) foreign companies dealing with personal data of individuals residing in India. [15]

It emulates the rights-based approach of the EU GDPR, putting 'individual privacy' at the core of the debate. The individuals are regarded as the Data Principal and have been given certain rights which includes processing of data, usage, storage, the right to be forgotten i.e. erasure of data, disclosure of data and sharing of data with third-party entities. 'Informed consent' is central to such individual participation rights.

However, the central government can exempt any of its agencies from the provisions of the Act on the following grounds:

1. in interest of security of state, public order, sovereignty and integrity of India and friendly relations with foreign states, and
2. or preventing incitement to commission of any cognizable offence (i.e. arrest without warrant) relating to the above matters.16

The bill has widened the scope for data fiduciaries to include within its ambit the social media intermediaries, because of the sheer volume of data processed by them. It too seeks to put certain obligations on them. The bill mandates the processing of data for specific, clear and lawful purpose. It also seeks to empower a statutory authority, **Data Protection Authority** with the power to take stringent action against data fiduciaries and non-state entities in case of breach or misuse of data.

DATA PRIVACY AND NATIONAL SECURITY: A CONUNDRUM

Data privacy and National Security have often been found to be at loggerheads with each other. The content generated every day runs into terabytes of data, the over dependency of an individual on the Internet increases the chances of transgressions by non-state actors. Cyber terrorism or cyber warfare is a cause of global concern. It goes beyond the traditional warfare, wherein the attack can be masterminded beyond the territorial confines of a country, making it extremely difficult to deal with the faceless attacker and to fix jurisdiction in such a scenario. The investigation of 26/11 Mumbai attacks unearthed horrors. The evidence showed the use of technologies like Google Earth by the terrorists, the Cyber telecommunication to establish a

[15] Ministry of Law and Justice, The Data Protection Bill, 2019, https://prsindia.org/billtrack/the-personal-data-protection-bill-2019.
[16] *Id.*

secure link and social media to track the defence forces. To deal with such unfortunate scenario in future, an amendment to the IT Act was introduced in 2008, and **Section 66 F** was inserted which specifies the '**Punishment for Cyber Terrorism'**. In addition, the aftermath of the attack also saw establishing of National Investigation Agency (NIA) and revamping National Intelligence Grid (NATGRID), to ensure better co-ordination amongst various intelligence gathering agencies. The electronic jihad popularized by the Islamic State (ISIS) operated under the cyber lens, using electronic media to recruit and brainwash the young and vulnerable. The network systems have been subjected to various malware, spyware and Denial of Service (DOS) attacks, making it all the more important to strengthen the IT capabilities and Cyber Security of the nation.

Apart from a threat by the non-state actors, a new area of Cyber hegemony has emerged. Cyber deterrence capabilities, both offensive and defensive, as possessed by countries with advanced IT-infrastructure like United States of America, China, European countries and Israel who seek to establish their data hegemony in the changing power dynamics is a cause of grave concern. Even certain rogue nations like North Korea are advancing their offensive IT capabilities to further their interests.

There is a compelling need to secure cross-border flow of data, decentralize storage of data and provide for a level-playing field to all countries.

DATA LOCALISATION AND EXTRA-TERRITORIALITY SCOPE

Data Localization is a novel idea, which requires the companies to store and process data within the confines of national boundaries to give the Government appropriate jurisdiction especially, in case of cyber threats and data breaches. It is in a way to uphold sovereignty and protect the interests of its citizens. The principle of territoriality comes into picture, a state can only exercise its jurisdictional powers within its territorial bounds. But, the borders seem futile when it comes to cyber related offences. Jurisdictional claims against foreign companies and persons is a matter of concern. It is imperative to bring within its ambit the extra-territorial jurisdiction.

Data localization is crucial for developing countries like India to assert their sovereignty, protect their citizens from misuse of data by business giants and other non-state actors, and prevent surveillance by foreign entities. Another pertinent facet to the need for data localization is to ensure easy access of data to law enforcement agencies like Central Bureau of Investigation (CBI), Enforcement Directorate (ED) and cyber cell, and in the public interest. It

will act as a deterrent in the fight against cross-border terrorism. This apart from having a National Security angle to it, will also improve upon the scaling up of India's Analytical capabilities.

The data localization mandate and best practices might vary across countries, it is imperative to strike a balance between the National Security aspect vis-a-vis the logistical costs associated with it and the storage limitation. To ensure compliance by business giants like Facebook, Google, WhatsApp etc. it is imperative to upgrade the IT infrastructure to tackle the evolving data privacy landscape.

ACCOUNTABILITY

To effectively translate data protection framework into reality, it is imperative to acknowledge the core issue of 'Accountability'. Control over data by Data Collectors, Data Processors, third-party entities whether foreign or India, private or public is accountable to the end-user. Data Protection Framework must protect individuals and their sensitive personal data from being misused. Owing to the complex data mining algorithms applied on the personal data, 'informed consent' by an individual is crucial. This is found central to the EU GDPR, and must be emulated by the Indian law. This includes two important facets: the data controller must adopt appropriate data protection principles and it should be in a position to demonstrate the same in the time of need. The government should be made accountable to set an example for other data fiduciaries, and avoid indulging into mass-surveillance to get beneficial results.

The recent controversial Privacy Policy update by the instant over-the-top messaging app WhatsApp brought it at loggerheads with the Indian Government. The reach and popularity of the App in the Indian subcontinent gives it an enviable position with respect to other over-the-top instant messaging applications like Signal and Telegram. It is pertinent for the big giants to comply with the IT and Data Protection Laws of the home country. In another instance, social media giant Twitter was asked to comply with the new **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**. The position prior to these rules for 'intermediaries' was limited confining there function to providing access to a communication system over which information was made available by third parties is transmitted or temporarily stored or hosted.[17] The intermediaries acted merely as facilitators but the new rules passes the onus on the part of intermediaries to employ due-diligence and an oversight mechanism. In addition, it stipulates on the part of intermediaries to block content for

[17] Information Technology Act, 2000, s. 79.

public access if the Authorized Officer deems fit.[18]

Accountability has to be ensured by the Data collectors and Processors within the reasonable Data Protection Framework. Data Protection Authority (DPA) and Regulators must be empowered and well-equipped to deal with such a tussle in future.

CONCLUSION

Data has become an integral part of our lives, it is an asset on which empires are built. With the huge data generated online every day, it is crucial to ensure data privacy and data protection of the individuals. Data Protection Laws need to be strengthened and the Adjudicating Authorities be empowered to deal with data breach. The compliance of such laws by social media giants, data fiduciaries, private and public entities is necessary to create a safe ecosystem. Susceptibility to cyberattack and emerging concerns surrounding cyber security should be borne in mind and an amicable balance must be struck without compromising the individual privacy.

SUGGESTIONS

In the age of Big Data Analytics being employed in literally in every facet of our lives, it is crucial for the businesses and data collectors to ensure high level of privacy and secure access. Here are a few suggestions to strengthen the privacy ecosystem:

- With cybersecurity threats and online espionage being a real threat, it is crucial to ensure to protect individuals and empower the Data Protecting Authorities to identify the data leakage source.
- Digital safeguards for different stakeholders and employing best practices to keep the 'personal sensitive data' safe.
- 'Informed consent' to be an integral part of data storage and usage. Employing better online tools to educate end-users.
- Refrain from collecting and storing unnecessary personal information.
- Prior-authorization by the Government in case of cross-border cyber threats and national security.
- Empower Regulatory authorities like CBI, ED etc. to ensure data protection compliance.
- Deployment of Privacy Enhancing Technologies for better protection of user data like passwords, biometric and financial information.[19]
- Strengthen Cyber Cell and proper training to qualified personnel to deal with cyber threats.

[18] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, s.16.
[19] 2 Buddhadeb Halder, Privacy in India in the Age of Big Data, 37-41 (Distribution Empowerment Foundation).

REFERENCES

https://gdpr-info.eu/

https://innovate.mygov.in/wpcontent/uploads/2017/11/Final_Draft_White_Paper_on_Data_Protection_in_India.pdf

https://prsindia.org/billtrack/the-personal-data-protection-bill-2019