LEGALFOXES LAW TIMES

PERSONAL DATA PROTECTION AND PRIVACY – A COMPARATIVE ANALYSIS

R. SARANI[1]

ABSTRACT:

Data is vital and is considered to be a treasure. In today's technological world, data is present everywhere and in everything. India is becoming digital, and without technology, it is not possible for humans to survive. We understand the importance of data and its protection, but India does not have specific legislation for data protection and privacy, so the mainline of this dissertation is to state the importance of data, the right to privacy concept with the landmark rulings starting from the Kharak Singh case to Puttaswamy judgment (AADHAR CARD case), then the Indian laws related to personal data protection – IT Act, IT Rules with the advantages and flaws of the Personal data protection Bill 2019, Srikrishna committee report.

In 2019, over 3.13 lakh cybersecurity incidents were reported, and Edutech start-up Unacademy disclosed a data breach that compromised the accounts of 22 million users, and they were put up for sale on the dark web. Recently India has banned 118 Chinese apps as Indian user's data is being stolen and used by the Chinese Government.

The Article would like to address the problem of data protection and privacy. Everyone is aware of the importance of data, and it is central to all consumers and all economic transactions. Today society has gone online, and everything is involved with technology; there are risks of misuse of personal data, and most crimes are taking place related to this. To protect data, we would require strong laws for protection, but unfortunately, India does not have specific legislation related to data protection. The Article ends by suggesting changes to the Personal Data Protection Bill 2019.

[1]R.SARANI, LLM CCL – CHRIST UNIVERSITY DEEMED TO BE UNIVERSITY

INTRODUCTION:

The terms privacy and right to privacy can't be easily conceptualized. It has been taken in different ways in different situations. Tom Gaiety said 'right to privacy is bound to include body' inviolability and integrity and intimacy of personal identity including marital privacy[2]. Edward Shilshas also explained privacy is 'zero relationship between two or more persons in the sense that there is no interaction or communication between them, if they so choose'[3]. Privacy is a neutral relationship between persons or groups or between groups and persons. Privacy is a value, a cultural state or condition directed towards individual on collective self-realization varying from society to society.

PUTTASWAMY CASE:

Firstly, the right to privacy was discussed in the M.P. Sharma and Ors vs Satish Chandra[4] case where the Hon'ble Supreme court discussed about search and seizure and held that it is not in contravention of any constitutional provision and did not give recognition to right to privacy as a fundamental right.

Then in the case of Kharak Singh vs State of Uttar Pradesh and Ors[5], the surveillance by domiciliary visits at night was in contravention of Article 21 and they also further held that Article 21[6] does not expressly provide for privacy provision.

Other cases related to privacy are the Govind vs State of Madhya Pradesh[7], R. Rajagopal and Anr vs State of TamilNadu[8], People's Union for civil liberties vs Union of India[9]. Then came the landmark case of K.S. Puttaswamy (Retd.) vs Union of India[10] famously known as AADHAR CARD CASE where it was challenged that collecting and compiling the demographic and

[2] Gaiety Gom. Right to Privacy, 12 Harvard Civil Rights Civil Liberties Law Review, P.233
[3]Shils Edward, Privacy. Its Constitution and Vicissitudes, 31 Law & Contempt Problems, 1966, p.281.
[4]1954 AIR 300, 1954 SCR 1077
[5]1963 AIR 1295, 1964 SCR (1) 332
[6]Protection of life and personal liberty - No person shall be deprived of his life or personal liberty except according to procedure established by law
[7]1975 AIR 1378, 1975 SCR(3) 946
[8]1995 AIR 264, 1994 SCC(6) 632
[9]AIR 1997 SC 568
[10](2017) 10 SCC 1

biometric data of the citizens in in breach or violation of Article 21 of the Indian Constitution. As the ambiguity in reference to the constitutional status of right to privacy – this case was referred to a constitutional bench of 9 nine judges.

The petitioners pointed that right to privacy is a fundamental right which is co-terminus with the liberty and dignity of the individual under Articles 14[11],19[12],21,25[13] of Indian constitution. On the opposite side, the Union of India – respondents stated that the right to privacy is nowhere mentioned in the Indian Constitution as a fundamental right.

The Hon'ble Supreme Court on August 24, 2017 held that the decisions of M.P. Sharma and Kharak Singh case stands overruled. In addition to it the bench held that "The right to privacy is protected as an intrinsic part of the right to life and personal liberty under Article 21 and as a part of the freedoms guaranteed by Part III of the Constitution[14]". So therefore, from this case the right to privacy was made as a fundamental right covered under Article 21.

ISSUES IN THE CURRENT INDIAN LAW RELATING TO DATA PRIVACY

The Information Technology Act 2000[15] was notified on October 17, 2000 and is a law dealing with the cybercrime and electronic commerce in India. This act does not deal with the concept of data protection and privacy. It does not contain a word relating to the same, there is only 2 provisions – SECTIONS 43A[16] and 72A[17].

It lacked for strong provisions relating to protection and the procedure to be followed to ensure the safety and security of sensitive personal information of an individual. The above stated 2 provisions are also grossly inadequate and due to the movement towards DIGITAL INDIA – we

[11]Equality before law - The State shall not deny to any person equality before the law or the equal protection of the laws within the territory of India Prohibition of discrimination on grounds of religion, race, caste, sex or place of birth

[12]Protection of certain rights regarding freedom of speech etc

[13]Freedom of conscience and free profession, practice and propagation of religion

[14] FUNDAMENTAL RIGHTS

[15]Enacted and assented on 9 June 2000

[16] Compensation for failure to protect data

[17]Punishment for disclosure of information in breach of lawful contract

are in need of a separate comprehensive legislation related to personal data protection and privacy.

The Information Technology Act, 2000 deals with the issue of data protection and privacy in a piecemeal fashion. There is no an actual legal framework in the form of Data Protection Authority, data quality and proportionality, data transparency etc. which properly addresses and covers data protection issues in accordance with the principles of the EU Directive, OECD Guidelines or Safe Harbour Principles

PERSONAL DATA PROTECTION BILL and its ISSUES:

After the Puttaswamy judgement in the year 2017, the Supreme court decided to create the Personal Data Protection Act as right to privacy was made a fundamental right and no specific, comprehensive legislation for data protection is present. A Committee under the chairmanship of Retired Supreme Court Judge B.N. Srikrishna was set up by the government for the framing of Personal Data protection Bill[18]. This bill is based mostly upon the frameworks that already protects privacy in other countries – it is based upon GDPR and Asia Pacific Economic cooperation (APEC) privacy framework. This PDP Bill 2019 provides the legal framework for the collection and use of personal information, creates set of rights and responsibilities for the personal data processing, vests substantive standard setting powers with the central government. A separate Data Protection Authority is proposed to be created for making regulations and enforcing the legal framework. The scope of this bill is wide and is applicable to all enterprises across India, technology companies, ecommerce platforms, real estate firms, brokers, hotels and restaurants.

One important feature to be noted is CONSENT, the personal data can be processed on the basis of free, informed and specific consent with provisions that allow such consent to be withdrawn. If any data is processed without obtaining the consent, then such an act is in violation and results in penalties. The sensitive personal data is made as a separate category and can be processed with explicit consent.

[18]Tabled in the Indian Parliament by the Ministry of Electronics and Information Technology on 11 December 2019

The Data Principal – user is given adequate information about the kinds of data that will be collected and for what purpose it is collected. A notice related to the rights and obligations of the users and data collectors has to be given. The bill exempts certain kinds of data collection and processing from specific requirements.

The bill provides exemptions[19] from the requirements of notice and consent in certain situations: when performing state functions authorized by law, delivering medical or health services during emergencies or epidemics, and providing services during disasters or the "breakdown of public order." It also contains exemptions from the requirements for "purposes related to employment."

DRAWBACKS OF THE PERSONAL DATA PROTECTION BILL 2019

The Personal Data Protection Bill did not address the privacy related harms in the data economy of India correctly. It only proposes a preventive framework that is oversupplying government intervention and is strengthening the state. In this bill there is no framework for protecting personal data with precise understanding of the role of privacy in society and for the harms emanating from such privacy violation.

This bill strengthens the state's role in the data economy, dilutes the property rights in data and surveillance power of the state is increased without adequate checks and balances. Other reasons is that there is significant reliance upon the consent based mechanisms but this is not effective, this bill could lead to significant compliance costs for private businesses. The next reason is the design of the DATA PROTECTION AUTHORITY as they have been given wide powers to regulate but they have not been given adequate checks and balances so that they will act in a reasonable manner. The chairman of the committee Justice B.N. SRIKRISHNA[20] has itself conveyed in a press meet that when the Personal data protection bill comes into existence, it is going to make India – an ORWELLIAN STATE[21] meaning the state has control over its user information. He himself conveyed this as the safeguards stated for the protection of personal data and privacy is removed by the central government and it has also got the power to exempt any of its agency from the provisions of the Act.

[19]PERSONAL DATA PROTECTION BILL 2019, CHAPTER VIII – Sections 35 to 40
[20]Indian Jurist and a retired judge of the Supreme Court of India
[21]Described in the "Nineteen Eighty four: A Novel by English Novelist George Orwell

COMPARATIVE ANALYSIS OF

- EUROPEAN UNION

The European Charter of Fundamental Rights[22] in the Article 7[23], 8[24] recognizes the right to privacy and the right to protection of personal data. The first principal[25] of the charter is the data protection directive which is inspired from the OECD Guidelines[26], it sought to achieve uniform high level of data protection by harmonizing the data protection legislations so that the free flow of data is not impeded.

When the data landscape is rapidly changing the EU updated its regulatory environment on the protection of data, so the EU General data protection regulation of 2016 (EU-GDPR) came into picture. This is seen as one of the stringent data protection laws in the world. Our Indian Personal data protection bill 2019 that was drafted after the Puttaswamy case is based upon the EU GDPR. It follows a right based approach towards the concept of data protection and the centre position is given to the individual. This EU GDPR applies to both the Government as well as the private entities, the exemptions given are the national security, defense, public security etc.

The collection of sensitive personal data such as the ethnic origin, sex life, religion, health data is prohibited but that is also subjected to certain exceptions. The collection, processing of data is lawful and fair if the entity or organization that is collecting the personal data complies with the extensive range of principles such as purpose specification, data minimization, security safeguards and data quality.

- USA

The format of United States for protection of data and its privacy is different when compared with other countries like India, Japan, Europe and United Kingdom.They do not have a single comprehensive national law for the protection of personal data. Like India they do not have a express provision for right to privacy but in the fourth Amendment the right is expressed in a

[22]2000 O.J.(C364) 18 Dec 2000
[23]Respect for private and family life
[24]Right to Privacy
[25]Human Dignity
[26]Organisation for economic cooperation and development - OECD

limited form. US has limited sector specific regulation and the approach for protection level are different for the public and private sector. They have the concept of different data has different value and utility so depending upon the value and utility the protection levels differ.

The US has grouped the data into several classes and a different degree of protection is awarded to the classes of data according to the importance and utility. The Privacy Act 1974[27] provides for establishing standards for when it is reasonable, ethical and justifiable for government agencies to compare data in different data bases.

The Electronic Communications Privacy Act[28] is enacted for the purpose of restricting the interception of electronic communications and provides for prohibition for the access of personal data without the user consent. For the children welfare and protection, they have enacted separate legislation – Children's online privacy protection Act[29] and for the protection of finance they have the Financial Privacy Act 1978[30]. In the Private sector acts such as Federal Trade Commission Act[31], Health Insurance Portability and Accountability Act, Financial services modernization acts are enacted.

- UNITED KINGDOM

UK has the Data Protection Act (DPA) 1984and it repealed by 1998 Data protection Act[32]. This Act aims to provide protection and privacy of the personal data of the individual in UK – data includes name, date of birth, address, contact numbers, emails address and fax numbers. The persons and other organizations storing the personal data must register their names with the information commissioner to protect and oversee the Act. The Act does not give absolute power to collect the data but rather limits or restricts the data collection. The data may be collected and can be processed only for lawful purposes. It shall be relevant, adequate and must not be in excessive of the purpose of purposes for which they are processed.

[27]Enacted by the 93rd United States Congress and effective on December 31, 1974
[28]Enacted by the 99th United States Congress and effective on October 21, 1986
[29]15 U.S.C. SS 6501-6506
[30] 12 U.S.C. ch. 35 S 3401
[31] 15 U.S.C. SS 41 - 58
[32]1998 c.29

Currently we have the Data Protection Act 2018[33] which is the implementation of UK of the General Data Protection Regulation (GDPR). This act regulates the personal data processing, protects the rights of the data subject, rules relating to data protection authority is enabled and the fines and punishment for breach of the rules by the authorities or organizations are detailed in order for safe regulation and protection of personal data of citizens.

CONCLUSION AND SUGGESTIONS:

The researcher at the end of the paper would like to conclude that awareness regarding the importance of data protection has to be spread among people. The landmark judgement of Puttaswamy case was given in the year 2017 and measures regarding the draft of Personal Data protection bill was initiated in the year 2017 itself but we are now in the year 2020 (3 years gone) but the bill is still not enacted and is decided to be tabled in the budget session of 2021 year. India is moving towards Digital India approach but unfortunately, we do not have a separate comprehensive legislation on data privacy and protection. The Personal data protection bill 2019 is based upon the European union general data protection regime (EU-GDPR) but the costs and benefits of applying those laws is not assessed – an evaluation for the application of European union laws to India has to be made and in the researcher's opinion- I am of the view that the approach of US laws for data protection is comparatively better when compared with the UK and Europe as they group data on the basis of their value and utility and then protect data based on the importance of the same. Now that the Personal data protection Bill 2019 is drafted it is impossible to change it but certain changes to the bill can be made inorder as stated above to make it more efficient.

[33] 2018 c.12