DATA PROTECTION IN INDIA

Disha Sivakumar, Symbiosis Law School, Hyderabad

In India, there existed no concept of *Right to Privacy*, in the case of *Kharak Singh v State of Uttar Pradesh*[1], wherein a six judge bench held that right to privacy is not a fundamental right and hence the surveillance of the petitioner due to his background by the police was held valid. In another case of *M P Sharma v Satish Chander*[2], an eight judge bench stated again that right to privacy was not a fundamental right, that India does not hold any right similar to the fourth amendment of the US constitution.

Later, the AADHAR Act came into existence, it was a central body collecting sensitive information of persons to issue them the identity of being an Indian citizen. In this process, the UIDAI(body administering and controlling AADHAR), collected biometric information, residential address, contact information and more. This information was stored in a single central server that did not have adequate safeguards in place. Retired Justice K S Puttaswamy filed a petition that the AADHAR Act was unconstitutional and one of the reasons was the violation of privacy and lack of adequate safeguards to the data collected, as any agency could access it. The Advocate General of India argued that right to privacy is not a fundamental right as held in previous cases. This was reversed by a landmark nine judge bench which over ruled the previous cases holding that *right to privacy* is a fundamental right under article 14, 19 and 21[3].

The AADHAR vault currently holds all sensitive information of the citizens relating to the AADHAR but only on a need to know basis, AADHAR is no longer mandatory for every process in the country. This is how the right to privacy emerged in India. This later translated to protecting to right to homosexual relationships[4] and prohibiting phone tapping of individuals[5] and others. Yet, this right to privacy as seen in the *Puttaswamy case*[6], applies to

[1] Kharak Singh v State of Uttar Pradesh, 1964 SCR (1) 332
[2] M P Sharma v Satish Chandra, (*1954) 1 SCR 1077*
[3] Justice (Retd.) K.S. Puttaswamy vs. Union of India, (2017) 10 SCC 1
[4] Navtej Singh v Union of India, AIR 2018 SC 4321
[5] Vinit Kumar v Union of India, 2019 ALLMR (Cri) 5227
[6] *Supra* note 3.

the sensitive information collected and stored for the AADHAR, yet this is under a broad umbrella. India does not have a right to data protection like the European Union. In India, there is no specific law for the protection of such information either.

Data protection includes storage of data, access, the purpose of collection of data and more. In India, there exists no specific act for data protection or protection of sensitive information, currently the Information Technology Act, 2000 is the primary Act governing this issue.

Information Technology Act

The IT Act, 2000 at its inception was not comprehensive in data protection or sensitive information protection, or even a definition of them. The Act soon had several amendments in this regard, beginning with the introduction of section 43A[7]. This section was introduced to make sure intermediaries protected and safeguarded *sensitive and personal information*[8] received by them with reasonable care and in case of default it shall be liable to pay adequate compensation to any injury caused as a result. Under this section, compensation would not be awarded unless the aggrieved party can prove that there has been legal injury as a result of the breach. In case of mere breach of sensitive or personal information, according to rule 8 of Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, *"the body corporate or a person on its behalf shall be required to demonstrate, as and when called upon to do so by the agency mandated under the law, that they have implemented security control measures as per their documented information security programme and information security policies."* The required security mandates and control have been mentioned under the same rules as notified by the Central Government.

In the case of *IDBI Bank v Sudhi S Dhupia*[9]*,* the petitioner through a mail had provided sensitive and personal data in the form of net banking details to an unauthorized email imitating IDBI bank. The court found that the bank had committed gross negligence in not installing adequate safeguards to prevent such a breach of data. The court stated that *"The respondent bank has failed to put in place a fool-proof internet banking system with adequate level of authentication and validation which would have prevented the type of unauthorised access.* The court also

[7] Ins. by s. 22, *ibid*. (w.e.f. 27-10-2009).
[8] Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011, G.S.R. 313(E)., Rule 3, It includes password, financial information such as credit/debit card details, sexual orientation, medical history and biometric information.
[9] IDBI v Sudhi S. Dhupia, 2019 SCC OnLine TDSAT 226

stated that "*The basic loophole in ensuring that a customer recognises an email as from the respondent bank was a glaring error on the respondent's part that would have prevented this severe incident".* This caused a wrongful loss to the aggrieved party, Rs.81, 700/- was withdrawn illegally from the bank of the petitioner. The court said the Adjudicating Officer made a reasonable judgment in awarding compensation for the present case amounting to Rs.1,00,000/-.

In another case, *Shri Umashankar Sivasubramanium v ICICI Bank*[10]*,* the facts of the same are also similar and the holding is the same, the point of difference lies in the quantum of compensation. In this present case, the court awarded a compensation of sum Rs. 12, 85,000/- . when the amount of money fraudulently withdrawn was Rs. 4, 95,000/-. The court in awarding compensation calculated 12% simple interest per annum which is the basic interest rate for banks on loans from the date of fraudulent withdrawal to date of passing judgment, which was 2 years and 7 months. This amounted to 1, 60, 648. The adjudication fees amounted to 27, 850 and travel expenses amounted to a lump sum of 6,00,000. Aggregating all the above-mentioned expenses and rounding to the nearest thousand the amount of compensation awarded was Rs. 12, 85,000/-.

From the above case laws, the determination of injury and the extent of compensation seems to depend on the extent of caution exercised by the aggrieved party and the security measures in place by the fiduciary. In both cases, the court only awarded compensation when the security measures evaded even the most sensible mind. It is not common for the courts to award compensation on such matters, as the security mechanisms employed and disclaimers with regard to fraud are always clearly emphasized, yet, under circumstances observed above the court is compelled[11]. The quantum of compensation on the other hand, is discretionary upon the judge. In both cases, which are recent, there seemed to be no set rationale on how the judge proceeded to calculate the sum to be awarded. Data protection may be compromised in a variety of situations, for health related information may be leaked from hospital servers, financial information as seen above or sexual orientation which has never been revealed; in such cases it is difficult to lay out the extent of injury or the compensation that is to awarded, as one may contain more emotional and mental injury than other or more financial injury, it is thus reasonable to be assessed on a case to case basis upon the discretion of the judge.

[10] Umashankar Sivasubramanian v. ICICI Bank, Civil Jurisdiction Petition No. 2462 of 2018

[11] *Supra* note 4.

Section 72A was introduced in the Act within the same amendment to yet again safeguard sensitive information received by intermediaries. The section is applicable when sensitive information is received and is misused against the terms of the contract with the intent of causing injury to the other party. This section carries a penalty up to five lakhs and imprisonment up to three years, or both. This section was introduced in pursuance of section 72 of the Act which was in existence during the inception of the Act. The section is provided for any person who through the powers conferred by the Act has access to any electronic record, books, sensitive information, data, computer resource or others publishes/transmits/sends the information without the consent of the other party will be liable with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. Both the sections, although having similar intentions, are applicable on different bodies. Section 75 states that the Act applies to crimes committed against India/Indian nationals by a person of any nationality from outside the country and against a foreign national/country from within India.

The IT Act, 2000 confers penalties and punishments under chapter IX and XI. It is clear from the reading of the Act that although data protection has been included in a meagre few sections through the 2008 amendment enforced in 2009, the major focus is on penalties and offenses committed in the course of misuse of Acts and not data protection specifically.

Amendments in IT Act, 2000

The Act[12] was brought into existence to facilitate the validity of online transactions, e-governance and to fight cybercrime (even then section 10A of the Act codifying that contracts formed online are not void but enforceable also came about through about through the 2009 amendment). The Act was formulated along the guidelines of the UNCITRAL Model Law on E-Commerce, 1996. This Act as seen above underwent major amendments in various provisions, with additions of various provisions as mentioned above in 2008, enforced in 2009 which include amendments in provisions relating to digital signature.

The 2017 amendment by the Finance Bill amended and omitted various provisions in Chapter X of the Act relating to the Appellate Tribunal. The amendment was due to the fact that the Tribunal for the longest time was not functional as the Chairperson has reached superannuation and the replacement was not made due to political turmoil at that time. The Finance Bill omitted

[12] Brought into effect October 17, 2000.

and amended sections from 49 to 54. The Telecom Disputes Settlement and Appellate Tribunal established under section 14 of the Telecom Regulatory Authority of India Act, 1997 had from the date of amendment, jurisdiction over the matters of the IT Act, 2000 and the Cyber Appellate Tribunal was only to exercise jurisdiction over matters and places stated by the Central Government. As jurisdiction over issues pertaining to IT Act predominantly lie with the The Telecom Disputes Settlement and Appellate Tribunal, suits in relation to data protection also lie under the jurisdiction to this tribunal.

Future of Data Protection in India

Growing technology and crimes with respect to data protection, especially in this digital age is proving that it is the need of the hour to introduce a Data Protection Act. In pursuance of this, various bills have been introduced in the parliament, but none of the bills have been passed.

1. Data Protection Bill, 2018

This bill mainly provided for three provisions. (i) Data localization[13] by intermediaries to make the process of access for law enforcement easier. (ii) It permitted the monitoring and processing of data in the name of state and national security, but this raised a lot of controversy that India would become a police state and surveillance state. India is a welfare state and such laws are a violation to privacy (iii) There were not proper regulatory authorities set up and the tenures of those appointed were very short, making it impractical to function

2. Data Protection Bill, 2019

Other than the provisions proposed in the 2018 bill, the 2019 bill included the rights of the data holders, offenses for sharing personal data without permission by fiduciary enhanced to 15 crores or 4 percent of turnover and failure to conduct and furnish data audit increased to 2 crores or 2% of turnover and the bill also included provisions related to transfer of sensitive information outside India. Yet, this bill was not passed. There was heavy backlash for the policing system and the heavy penalties for fiduciaries under this Act, stating that this will hamper growth of start-up industries.

[13] Data localisation was a provision in all drafts of the data protection bill except the 2022 draft. It effectively states that without the consent of the Data Principal sensitive or personal information cannot be transferred outside and must be stored within India.

3. Data Protection Bill, 2021

The fourth iteration of the bill was proposed by the Justice Srikrishna Committee, it proposed localization of data, a single data protection authority and minimum restriction on fiduciary on collection of data. Under the recommendations, the fiduciary's responsibility of collection restraint was absent. The data classification of sensitive information such as health, photos, genetic information to other data such as preferences, education qualification, etc was absent; sensitive information is awarded a higher degree of protection. The 2019 draft has not proposed this classification and allows fiduciary to collect data without knowing the details of the purpose for collection. It also provided for deemed consent in certain areas, reduced information to be provided to the Data Principal and more. Fundamentally, the 2019 draft was also received with heavy backlash and was withdrawn.

4. Data Personal Protection Bill, 2022

The new bill which is yet to be presented in the parliament has proposed higher penalties on offenses for stricter compliance, jurisdiction to extend beyond the scope of the Indian territory and the right to be forgotten. The applicability of the new bill is on *digital personal data.* According to the bill it is defined as *"any data about an individual who is identifiable by or in relation to such data"*[14] This is the scope of application that has been adopted by both the European Union and Singapore.

The new draft adopting the 2018 draft has amended it by adding that although data will be collected by the fiduciaries, it will also be accessible from the localized storage destination by the Data Principal and the principal has the right to withdraw consent at any point in time from the fiduciary in processing data. The draft has also proposed that all data fiduciaries are required to appoint a data protection officer to represent the fiduciaries. The new draft has also proposed that a separate and independent organization the Bureau of Indian Standards (BIS) to be the new standard for setting data privacy in India.

The Bill has also proposed that no fiduciary can process data relating to children that may cause harm to the child. It has also provided that advertising cannot be targeted towards children.

A major change in the new draft as opposed to the previous iterations is cross-border transfer of data. The previous drafts had always emphasized on data localisation, this bill states that

[14] The Digital Data Protection Bill, 2022

data may be transferred to organizations in other countries that have been notified by the Central Government.

The new draft has proposed a comprehensive legislation of data privacy in India. The acceptance of the draft during public opinion and both houses of parliament will translate the bill into Act, if provided.

Data Protection in Other Countries

India is in desperate need of a uniform data protection law to be at par with other countries who have more stringent legislations on the same. Although, US does not have a separate law on this, its data protection legislations have heavily safeguarded data privacy. Other countries such as the UK, France and Australia have unified legislations on this front.

It is worthy to note that the 2022 draft has been formulated after perusing the laws of the EU, Australia, United States and Singapore. In the 2022 draft it has proposed that in case of any breach of data it will be notified to the Data Principal without delay, although the Central Government has stated that rules to the Act will follow for effective functioning of the law a timeline and process of escalation is necessary. In the EU and Singaporean data protection laws, it has outlined a specific process for intimation to the Data Principal regarding the data breach. In the EU, according to Article 34 the controller[15] must intimate the European Data Protection Supervisor[16] within 72 hours. In Singapore, the data breach is to be notified by the organization to the Commission[17] within 3 calendar days[18] and also the data principal. The Acts also provide under what circumstances or severity of breach it will pass from the controller/ supervisor the next authority and finally the data principal. In India, it has been mentioned by

[15] According to Article 3 of the Regulation (EU) 2018/1725 Of The European Parliament And Of The Council of 23 October 2018 on The Protection Of Natural Persons With Regard to The Processing Of Personal Data By The Union Institutions, Bodies, Offices And Agencies And On The Free Movement Of Such Data, And Repealing Regulation (EC) NO 45/2001 And Decision No 1247/2002/EC "controller" is means the Union institution or body or the directorate-general or any other organisational entity which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by a specific Union act, the controller or the specific criteria for its nomination can be provided for by Union law;
"controllers" other than Union institutions and bodies' means controllers within the meaning of point (7) of Article 4 of Regulation (EU) 2016/679 and controllers within the meaning of point (8) of Article 3 of Directive (EU) 2016/680;

[16] The European Data Protection Supervisor is an independent supervisory authority responsible for monitoring the processing of personal data by the Union institutions and bodies. However, it does not apply to the processing of personal data in the course of an activity of Union institutions and bodies which fall outside the scope of Union law.

[17] The Info-communications Media Development Authority is designated as the Personal Data Protection Commission.

[18] Personal Data Protection Act, 2012, §26D,

the Central Government that rules will follow the Act if it is passed. In case it does become an Act, the period of notifying the breach, the process of escalation and the remedy provided should be outlined in the Act.

As the Indian draft has derived many provisions from the Singapore and EU the provisions with relation to consent are almost identical. The only differences come from the EU, it has provided that the Data Principal the limit the data provided for research and under Article 23[19] has the right to object to the extent of data provided for research, such a provision is absent in both Singaporean and Indian laws. In both Singapore and India, the use of personal data for research only in conditions wherein it is mandatory, does not have any right to be objected by the Data Principal if already provided to the fiduciary as both these countries value public interest more than individual interest. Countries in the west more often than not value individual interest above all. This difference, whether harmful to Data Principals will only be known in due time.

A positive aspect of the new draft is the restriction on processing data related to children and the draft also states that a Data Fiduciary cannot undertake to provide any targeted advertisements towards children. This is a step forward in our law. The EU has implemented an age limit from when a child's information can be processed but has not provision in relation to targeted advertisements towards children. Under Article 8, the provision states that if the child is at least 13 years of age then his/her information can be processed, whereas Singapore has no provisions relating to restriction on data processing or advertising towards children. UK, under section 9 of its Data Protection Act, 2018, has amended the age limit from 16 to 13 years. India needs to provide for an age limit as well as the age limit from when the information of children can be processed, as the standard 18 years is too old with regards to this issue.

A major addition in the new draft is the transfer of data outside India, the previous drafts has expressly provided for data localization. The IT Rules, 2011 provide that transfer of data outside India can be allowed for two reasons, one being to enforce a contract and the second if the Data Principal consents. The new draft has introduced a host of reasons which may affect the transfer of data. It does not within this provision require the consent of the Data Principal. This provision is identical in the law of Singapore and the EU, yet should attempt to upkeep the 2011 rules in this regard and inculcate that this transfer will only be affected after its intimation to the Data Principal and provide the Data Principal the right to object to the same.

[19] Article 23, *Supra* note 10.

The EU as already mentioned provides this right with regards to research, which is one of the plethora of reasons provided for transfer of information outside India in the new draft.

Last but not least, one of the most important additions that must be made to the new draft is protection against *phishing.* As already seen through the case laws above, India has one of the most notable problems of phishing and this must be addressed. This issue is not addressed in the IT Act, 2000 either. This provision has not been given in the laws of EU or Singapore either. Yet, it is imperative to inculcate into our laws. Currently, the issue of phishing is being dealt with by IPC. The sections prohibit Theft[20], Criminal Breach of Trust[21], Cheating[22], Mischief[23] and Fabrication[24]. There are no provisions otherwise to deal with protection of data in this scam, although there must be criminal penalties for this crime, it must be codified within the data protection law of the country as well. The law must introduce measures and efforts to educate people on this scam as well. The government should implement a provision for representative in Substantive Data Fiduciaries to appoint a data represent to specifically deal with the grievances relating to crimes regarding phishing and provide a timeline for its resolution. Although, a Data Protection Officer is appointed to deal with the grievances under provisions of the draft, phishing is a pressing issue and it must be resolved on an expedited timeline especially in organizations such as financial institutions wherein money is involved. Hence, a special officer on this account must be appointed.

In conclusion, the new draft for data protection in the country is very comprehensive and requires rules to be formulated to effectively implement it if passed as an Act. There are few additions that are required to made in the draft and the above-mentioned suggestions are few of the major recommendations. Data protection in other countries has become a codified law in or before 2018 as already seen, and India is still in the phase of getting a draft approved. A country with a population such as India's must at the very latest codify and implement a law on data protection, and the new draft is on the right track.

[20] Indian Penal Code, 1860 §378, 379.
[21] *Id* at 16. § 405, 406.
[22] *Id* at 16. § 415-419.
[23] *Id* at 16. § 425-426.
[24] *Id* at 16. § 463-477.