Chapter Four

Right to Privacy and IT Act, 2000: An Interface

Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011
4.5.3.5 Information Technology (Intermediaries Guidelines) Rules, 2011
4.5.4 Credit Information Company (Regulation) Act, 2005
4.5.5 Privacy Bills
4.5.5.1 Right to Privacy Bill 2011
4.5.5.2 Privacy Bill 2014
4.5.5.3 Personal Data (Protection) Bill, 2013
4.5.5.4 J. Shrikrishna Committee Report
4.5.5.5 The Personal Data Protection Bill, 2018
4.5.5.6 The Personal Data Protection Bill, 2019
4.5.5.7 Digital Information Security in Healthcare Act ,2019 (DISHA)
4.6 Interface between Right to Privacy and Information Technology Act, 2000
4.6.1 Use of Information Technology
4.6.2 Need for Data Protection
4.6.3 Aadhaar and Privacy Issues
4.6.4 Information Technology Law and Right to Privacy: An Interface

4.1 Introduction

Privacy has many aspects. One of these aspects is protection of the information relating to an individual which is known as 'data privacy' or 'information privacy'. The core of this privacy is that an individual can claim legitimately that information about him shall not be available to other individuals or organisations. Not only this, but he shall exercise the control over the data possessed by others and use of such data. He expects that he shall have significant control over handling of the data by others. So individuals felt it necessary to have certain framework to protect their interests. This protection must be such to maintain the balance between privacy and other competing interests. Threat to security of information has increased many folds as communication and information technology is used widely in day to day life, because of its interoperability.

Technologically advanced countries like United States of America, United Kingdom and European Union were started to face the consequences of the invasion on the rights of their citizens. European Union was first to respond to such threats and tried to enact the legislation. European Union considered right to privacy as human right first and accordingly provided it under convention ECHR, which the member countries were expected to protect under their respective legislations. Afterwards it enacted strong data protection legislations which provide the guiding light for other countries. United States of America responded it with sector specific legislations protecting rights in that particular sector. United Kingdom did not recognise right to privacy but provided protection under Law of Tort initially and afterwards drafted Data Protection Laws being the member of European Union. Countries all over the world followed by enacting laws and provide legal framework for protection of right to privacy and data protection.

It will be appropriate to note the international development for enactment of laws regarding privacy and data protection. India is also slowly following the footsteps of such laws and statutes enacted on the principles recognised by other countries. The researcher has tried to compare the provisions and enactments

made by other countries with provisions made by India for protection of privacy and data protection.

4.2. European Union: Legislative Measures

European Union was and is sensitive about the right of person regarding his personal life, his home and family. This right to privacy was and is recognised as 'human right' in European Union, which means it is born with an individual and cannot be taken away. The researcher attempts to trace this development of privacy principles in European Union in following discussion. It can be observed that physical privacy and that right to privacy regarding the aspect of 'privacy to correspondence or information' are different in Europe and later is termed and recognised as 'data protection' in European Union.

As right to personal life, family and correspondence is recognised in Universal Declaration of Human Rights (UDHR)[1] by United Nations in 1948, member countries of European Union resolved to enforce the rights contained in UDHR and passed a resolution to that effect in 1950 which is known as European Convention of Human Rights.(ECHR)

4.2.1 European Convention of Human Rights

In 1950 European Convention of Human Rights (ECHR)[2] was enacted by Council of Europe with an intention to provide for protection of human rights in Europe. In this convention, Article 8 provided the Right to Privacy- "Everyone has right to respect for his private and family life, his home and correspondence. This right can be restricted by public authorities in accordance with law and which are necessary in democratic society".[3] This article protects the privacy rights of the persons staying in European Union. European Court of Human Right was established by the provision under the convention. If any person feels that his or her rights are violated by any state party, can reach to the Court.

[1] www.un.org/en/universal-declaration-human-right (Last visited on May 23, 2017)
[2] https://www.coe.int/en/wb/human-rights-convention. (Last visited on May 23, 2017)
[3] European Convention of Human Right, Art. 8,

These principles were followed by the member countries of European Union by inculcating the provision in their law. The cases for privacy protection were decided referring the right to privacy provided under Art 8 ECHR.

As business transactions were increased among the nations of European Union and outside it also, the transfer of data to such other countries was also increased. With the emergence of Information technology in the 1960, it was observed that this data was processed using information technology with automatic data processing. In this situations, it has become essential to protect privacy and to frame the principles governing the collection, use, and processing of data. A growing need developed for more detailed rules to safeguard the individuals for protection of their personal data. Researcher is trying to trace the development of the right to privacy to data protection in European Union in following paragraphs.

By the mid-1970, the Committee of Ministers of the Council of Europe (CoE)[4] adopted various resolutions on the protection of personal data, referring to Article 8 of the ECHR. OECD[5] suggested privacy principles to be followed by the data controllers while collecting and processing the data in 1981. Council of Europe cannot make the laws. But can issue guidelines and convention. Accordingly it had proposed convention 108 in 1981 which was adopted and ratified by member countries. With the passage of time as processing of personal data was done with advanced technology by transferring it to outside European Union, the immediate need was felt to protect the rights of citizens of European Union. For this purpose Directive 95/46/EC in 1995 and General Data Protection Regulation (GDPR) in 2018 was issued.

But to start with, to harmonise national legislations for privacy protection and simultaneously to prohibit to interrupt flow of data within the countries, the

[4] Founded in 1949, have 47 member Countries. Distinct from European Union, which has 27 member countries. Country belonging CoE, can only become the member of EU. Law enforcing body of CoE is European Court of Human Rights.

[5] It was originally Organisation for European Economic Co-Operation (OEEC) in 1948. But reformed in 1961 as OECD for stimulating economic progress and world trade. It is intergovernmental economic organisation, having 37 member countries. Now its membership is extended to outside European Union.

guidelines were developed by Organisation for Economic Co-Operation and Development (OECD) in 1980.

4.2.2 Privacy Principles

These Organisation for Economic Co-operation and Development (OECD) guidelines on Protection of Privacy and Trans-border flow of Personal Data were accepted in 1980[6]. They are followed by the member countries of European Union. These *Privacy Principles* have become the basis of the legislations for protection of privacy including informational privacy in various countries in the world. Some other principles are also developed using these principles, but these principles provide the base for legislations.

These principles are applicable to personal data processing in any manner, in any context in private or public sector. According to them, collection, storage, processing, or dissemination is permitted if privacy and liberty of human is protected. They apply to automatic processing of personal data.

The Guidelines consist of 8 basic principles[7]

1. Collection Limitation Principle- Collection of personal data should be limited, obtained lawfully and fairly and with consent of the person[8].

2. Data Quality Principle-It should be relevant and necessary for purposes. Also it should be accurate, complete and kept updated[9].

3. Purpose Specification Principle-The purposes for which personal data are collected should be specified at the time of data collection and the subsequent use limited to the fulfilment of those purposes or compatible with such purposes[10].

4. Use Limitation Principle-Personal data should not be disclosed, made available or otherwise used for purposes other than those specified except a) with the consent of the data subject; or b) by the authority of law[11].

[6] https://oecd.org/internet/economy/oecdguidelines. (Last visited on May 23, 2017)
[7] OECD guidelines https://www.oecd.org/document_(Last visited on May 23, 2017)
[8] Organisation for Economic Co-operation and Development Principle 1
[9] Organisation for Economic Co-operation and Development Principle 2
[10] Organisation for Economic Co-operation and Development Principle 3
[11] Organisation for Economic Co-operation and Development Principle 4

5. Security Safeguards Principle-Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.[12]

6. Openness Principle-There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.[13]

7. Individual Participation Principle-An individual should have the right to obtain confirmation that data controller has data relating to him; also has a right to be informed about such fact within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; to be given reasons if a request made is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended[14].

8. Accountability Principle- A data controller should be accountable for complying with measures which give effect to the principles stated above.[15]

These principles were the first attempt to crystalize the method to observe privacy of information. Duty was cast on the person who collects of data to observe the privacy by collection limitation as he was obligated to collect data which is appropriate in quantity and not more than that. In purpose limitation, the data should be collected which is required to serve the purpose of collection, which means the data which is required to serve the purpose incidental to the main purpose can also be allowed. For openness principle, the right of the individual is recognised that he can ask the data collector about the use of data, its security and the identity of data controller.

[12] Organisation for Economic Co-operation and Development Principle 5
[13] Organisation for Economic Co-operation and Development Principle 6
[14] Organisation for Economic Co-operation and Development Principle 7
[15] Organisation for Economic Co-operation and Development Principle 8,

As this was the initial attempt to protect the rights of individual, they were providing the limited protection. Guidelines regarding time for storage of data and cross-border transfer of such data were not given. These principles were only the guidelines for the any data collector-controller, who deals with the collection and processing of data in very basic way.

But due to the inadequacies regarding the guidelines processing in and outside the countries and cross-border transfer of data in the era of information technological advancement, the Council of Europe adopted a first international treaty to address the rights of the individual to protection of their personal data.

4.2.3 'Convention 108'.[16]

In 1981, a convention for the protection of the individuals with regard to the automatic processing of personal data known as Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data-was framed (Convention 108). Convention 108 is legally binding instrument in the data protection field. Convention 108 applies to all data processing entities, both the private and public sector which carry out the data processing. It protects the individual with regard to processing of personal data contributing to human rights and fundamental freedoms and particularly right to privacy.[17] The nationality of the person is immaterial for protection of personal data.[18] In this convention, the definitions regarding 'personal data' 'processor' etc. are provided[19].

The privacy principles laid down in the convention concern, in particular, fair and lawful collection and automatic processing of data, stored for specified legitimate purposes and not for use for ends incompatible with these purposes nor kept for longer than is necessary[20]. They also concern the quality of the data,

[16] https://rm.coe.int/16808ade9d. Available at https://www.coe.int/en/web/conventionns/full-list/conventions/treaty/108. (Last visited on May 23, 2017)
[17] Convention 108 Art. 1
[18] Convention 108 Art. 1
[19] Convention, 108 Art. 2
[20] Convention 108 Art.5

in particular that they must be adequate, relevant and not excessive (proportionately) as well as accurate.[21]

It prohibits, in the absence of proper legal safeguards, the processing of 'sensitive' data, such as person's race, politics, health, religion, sexual orientation or criminal record.[22] The Convention also provides for the individual's right to know that information is stored on him.[23] These rights can be restricted only if there are overriding interest like security of state etc.[24] Although the convention provides for free flow of personal data between State Parties to the Convention, it also imposes some restrictions on those flows to states where legal regulation does not provide equivalent protection.[25] Supervisory authority is created for compliance of the convention.[26]

This convention is a binding document for the European Union countries. The states party have to enact legal framework for implementing the rights provided under this convention. The member states of European Union inculcated the rights and obligations provided in this convention in their respective legal structure and provided the protection for the right to privacy to the persons. The provisions of this convention was followed by member countries.

After the increased use of internet after 1995 and because of technological advancement in the area of personal data processing, the character and volume of processing of data is changed. Increase in internet transactions also contributed to this. In this situations, guidelines and provisions of convention 108 were inadequate to protect the prevent misuse or abuse of data. The need was felt to provide protection for personal data through advanced technological processing by entities. This led to the issuance of new directive by Council of Europe for data protection named as Directive 95/46/EC.

[21] Convention, 108 Art. 5
[22] Convention 108 Art. 6
[23] Convention 108 Art. 9
[24] Convention 108 Art. 11
[25] Convention 108 Art. 14
[26] Convention 108 Art. 15

4.2.4 European Union Directive 95/46/EC

This directive is of European parliament and European Council on protection of individual regarding processing of personal data and free movement of such data. It regulates processing of personal data within European Union. This directive is important part of European Union privacy and human rights.

The Directive 95/46/EC[27] was inculcating the principles provided in European Union's OECD principles. In the Directive, **personal data** is defined as "any information relating to identified or identifiable natural person."[28] The **Identifiable person** is "who can be identified directly, indirectly or in particular by reference to the identification number or to one or more factors specific to his physical, psychological, economic, cultural or social identity."[29] It is very broad definition. Processing means "any operation or set of operations performed on personal data, automatically or not for collection, storage, adaptation or alteration, retrieval, disclosure by transmission, dissemination or otherwise making available, for erasure or destruction."[30]

Processing is allowed only on consent, transparency, for legislative purpose and proportionality[31]. If sensitive personal data is processed, more strict restrictions are provided. An objection may be taken by data subject at any time for processing of personal data. Every member state may set up supervisory authority for monitoring data protection level[32]. If personal data is transferred to third countries outside EU, it was allowed only if that country provides adequate level of protection.[33]

Even though this directive was issued, certain areas in which the online activity is conducted through information technology was out of the reach of the protection given under it. It is pertinent to note that EU Directive 95/46/EC was not providing protection against the threats of new technologies like social

[27] https://eur-lex.europa.eu/legal-content/en/TXT (Last visited on May 30 2017)
[28] Directive 95/46/EC Art. 2 (a)
[29] Directive 95/46/EC Art. 2(a)
[30] Directive 95/46/EC Art. 2(b)
[31] Directive 95/46 Art. 7
[32] Directive 95/46, Art. 28,
[33] Directive 95/46, Art. 25,

networking, mobiles and cloud computing. These services are provided by internet service providers. But protection is not provided under the Directive.

Another area is the online gaming. Online gaming activity by the persons irrespective of their age has increased. People use information technology for entertainment. The Internet Service Providers and the Online Game Providers were not covered under the Directive. Computer games are designed specifically for the computer and technology lovers especially the children. Privacy and security of these users is also important while they use information technology. Council of Europe has issued the guidelines about their activities.

4.2.5 Human Rights Guidelines for the Internet Service Providers and Online Games Providers[34] in 2010.

Council of Europe, in co-operation with European Online game designers and publishers and with internet service providers has created two sets of guidelines. The object was to make the internet use safe and right to privacy of the users shall be protected.[35]

The guidelines for internet service providers:

A) To encourage providers to inform i) users about potential risk on internet about illegal content or information causing harm, or chances of exposure to harmful behaviour of other users, ii) security risks for data integrity and confidentiality, iii) privacy risks as collection, recording or processing of data.[36] B) Inform about filtering software that may block or restrict access to certain content. C) They should ensure that additional services like chat, e-mails are safe as possible. D) They should establish appropriate procedures and technology to protect privacy of users and secrecy of content. E) Except under certain situation, they should not collect or store information about users.[37]

Guidelines for Game designers and publishers:

[34] https://www.coe.int/en/web/portal/guidelines-for-providers (Last visited on May 23, 2017)
[35] https://www.coe.int/en/web/portal/guidelines-for-providers (Last visited on May 23, 2017)
[36] https://www.coe.int/en/web/portal/guidelines-for-providers (Last visited on May 23, 2017)
[37] https://www.coe.int/en/web/portal/guidelines-for-providers (Last visited on May 23, 2017)

1. They should pay attention that violence, racist content or content advocating criminal behaviour shall not be portrayed especially when such game is targeted to children.[38]

2. They should apply independent labelling and rating system to inform gamers, parents and carers bout the content of the game.[39]

3. Where game is marketed, they should provide information to gamers, parents and carers about the risks in user guides in the language of such region[40].

4. They should develop more in-game parental control tools. And facilities should be created for reporting illegal or harmful information[41]

5. They should develop automatic removal of content generated by users after certain period to avoid prejudice to their dignity, privacy and security.[42]

6. They should clearly inform gamers about presence of advertisements[43].

These guidelines are applicable in European Union.

In computer games level of violence and obscenity is on high to make the game more interesting. Such material is not fit for the children. Sometimes the content is objectionable in very subtle way. It is very difficult to control this content as there is no standard available to compare it. The test of reasonable man may be applied here. But again the standard of violence regarding war games and in other games may be different. The standard may fluctuate depending upon the region also. So it is difficult to regulate and control these activities altogether. But these provisions provide certain guidelines for further regulations.

Due to these developments in technology and as there was substantial increase in cross border flow of personal data because of increasing economic activities, the generation of data is also increased. It was observed that due to technological innovations, more protection is required against the automated processing of personal data and for protection of privacy of personal data. Moreover the protection provided by member countries by following Directive 95/46/EC was not same in each country. The provisions for protection were conflicting.

[38] https://www.coe.int/en/web/portal/guidelines-for-providers (Last visited on May 23, 2017)
[39] https://www.coe.int/en/web/portal/guidelines-for-providers(Last visited on May 23, 2017)
[40] https://www.coe.int/en/web/portal/guidelines-for-providers(Last visited on May 23, 2017)
[41] https://www.coe.int/en/web/portal/guidelines-for-providers (Last visited on May 23, 2017)
[42] https://www.coe.int/en/web/portal/guidelines-for-providers(Last visited on May 23, 2017)
[43] https://www.coe.int/en/web/portal/guidelines-for-providers(Last visited on May 23, 2017)

All these factors contributed for issuing the new regulation in 2016 by European Union. It is known as General Data Protection Regulation. It replaces the European Union Directive 95/46/EC.

4.2.6 European Union–General Data Protection Regulation (GDPR)

European Commission attempted to unify the data protection laws across European Union through General Data Protection Regulation (GDPR) 2016/679[44]. It is enforced in 2018 after ratification by member countries. Objectives of GDPR are to provide protection relating to processing of personal data of natural person and free flow of such personal data, and also it protects the fundamental rights of natural person specifically their personal data.[45]

GDPR applies to the processing of personal data by data processor not only situated in European Union but outside European Union also. It is applicable irrespective of the nationality of the person. It is applicable not only to private entities but also to government or entities controlled by government. It provides protection to data processing by social networking sites and by cloud computing.

It defines the terms in detail to provide maximum protection to the individuals. Personal information includes any information relating to an individual whether it relates to his private, professional or public life[46].

It is applicable to all companies processing the personal data of data subjects residing in European Union, regardless of company's location[47]. No exclusion of Government bodies or related organisation.[48] Processing shall be done in fair manner, according to purpose for which data is collection, legally and accurately and after obtaining consent.[49] Even the processing is in European Union or not, it is applicable[50]. It is also applicable to controllers and processors not established in European Union but where activities relate to offering of goods or services to European Union citizens (irrespective of whether payment is

[44] https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng?eliuri=eli:reg:2016:679:oj (Last visited on May 23, 2017)
[45] General Data Protection Regulation Art. 1
[46] General Data Protection Regulation Art. 4(1)
[47] General Data Protection Regulation Art. 3(1)
[48] General Data Protection Regulation Art. 4 (7), (8)
[49] General Data Protection Regulation Art. 5 (1)
[50] General Data Protection Regulation Art. 3(1)

required or not) [51] and monitoring of behaviour that takes place within European Union.[52] Non- European Union business processing the data of European Union citizens will also have to appoint a representative in European Union. Informed consent must be obtained before collection and processing[53]. For giving consent, the requirement of age is 16 years. The person who has not completed 16 years is considered as child.[54] (In UK age of giving consent is 13 Years) If the information is relating to personal data of a child, consent of the parents is must.[55]

This shows the extra-territorial applicability of the Regulation. Internet has no physical borders and therefore it is difficult to control and regulate invasion on or breach of the data privacy. GDPR has tried to provide protection even when processing activities are conducted outside the physical border of European Union.

Processing of data is held lawful when it is processed with the informed consent, for contractual obligation, for legal obligation of data controller, vital interest of data subject, if the task is in public interest and legitimate interest of data controller.[56] The data subject has right to access information, verify the purpose for which it is collected and processed[57].

They have right to be forgotten i.e. to rectify[58] and erase the data[59]. This is a novel concept which is protected under General Data Protection Regulation. The question of scope of the erasure of personal data had cropped up in two cases before the Court of Justice of European Union (CJEU) in Google v. Spain[60] and Google v. CNIL[61] (both in 2010). The researcher has discussed them in the Chapter 5: Judicial decisions. Because of these two cases the scope of right to

[51] General Data Protection Regulation Art. 3(2)
[52]General Data Protection Regulation Recital 24
[53] General Data Protection Regulation Art. 6
[54] General Data Protection Regulation Art. 8(1)
[55] General Data Protection Regulation Art. 8(1)
[56] General Data Protection Regulation Art. 5 (1
[57] General Data Protection Regulation Art. 12
[58] General Data Protection Regulation Art. 16
[59] General Data Protection Regulation Art. 17
[60] Google v. Spain (2010) C-131/12,
[61] Google v. CNIL, C-507/17, EUR-Lex CELEX NO 62017CJ0507

erasure or right to be forgotten is widened with some limitations. The Controller, who has made the data public, shall inform the other controllers who are processing the data to erase any link to, or copies or replications of such data[62]. This provision is not provided under Directive 95/46/EC. Under GDPR, the right cannot be exercised if data processing is necessary under legal obligation, for exercising freedom of expression and information, and for public interest as public health, and other exemptions[63]. No officer is provided to decide the erasure. Only Data Controller has to decide.

Data subject has right to transfer the data to another controller[64] which means right to data portability is available. Data controller is obligated to transfer the data in a structured and machine readable format.[65]

For protection of data while processing the data controller and data processor shall apply pseudo-anonymisation and data minimisation.[66] They have to apply privacy protection through privacy by design and privacy by default[67]. For transferring the data cross border for process, it is permissible only such country is providing adequate level of data protection, through standard contractual clauses, by complying with approved certification mechanism[68]. Data Protection supervisory authority is created.[69] Data breaches are to be reported to such authority.[70]

For transferring the data to the country outside European Union, the country shall provide adequate level of data protection. For this adequacy level the decision given by the Commission is final.

For personal data regarding health information, General Data Protection Regulation provides for three types of data. They are data concerning health

[62] General Data Protection Regulation Recital 66,
[63] General Data Protection Regulation Art. 17,
[64] General Data Protection Regulation Art. 20,
[65] General Data Protection Regulation Art. 20,
[66] General Data Protection Regulation Art. 25,
[67] General Data Protection Regulation Art. 25,
[68] General Data Protection Regulation Art. 45,
[69] General Data Protection Regulation Art. 51,
[70] General Data Protection Regulation Art. 71,

data[71], genetic data[72] and biometric data.[73] They are classified as 'sensitive personal data'.[74] Under GDPR, special protection like explicit consent shall be given for processing of such data by the Data controller and processor of such data.[75]

The technological advancement reached at another peak as processing of personal data was started to be done with combination of more than one technological methods of processing. It was observed by the data processors that by employing such method the result is more benefiting for their business purpose or is benefiting to achieve some other incidental purpose apart from which the data was collected. This process is known as 'Big Data Processing.' Big Data means, in general, data (personal) in very large quantity. This type of processing benefits to assess and understand personality choices, trends of consumers, changes in society etc. This assessment is valuable for the businesses to expand their activities through advertisements targeting the concerned group of individuals. But this may harm the decisional privacy of the individual and may result in the loss of other rights also. European Commission has issued guidelines for processing of Big Data in 2017 to protect the rights to privacy and fundamental freedom of persons.

4.2.7 Guidelines for processing of Personal Data in world of Big Data

In 2017, these guidelines were issued by European Commission. This was done with the objective "to prevent the potential negative impact of the use of Big Data on human dignity, human rights and fundamental independence and collective freedoms, in particular with regard to personal data protection. Some traditional principles of data processing may be challenging in this type of technology."[76] These guidelines suggest specific application of principles of convention 108 to make them more effective.[77]

[71] General Data Protection Regulation Art. 4(15),
[72] General Data Protection Regulation Art. 4(13),
[73] General Data Protection Regulation Art. 4(14)
[74] General Data Protection Regulation Art. 9
[75] General Data Protection Regulation Art. 9
[76] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 23, 2017)
[77] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 23, 2017)

The guidelines include certain definitions to apply them effectively. There are many definitions and differ depending upon specific discipline. But in relating to data protection 'Big Data' is defined by "main issue does not only concern the volume, velocity and variety of processed data, but about the analysis of data using software to extract new and predictive knowledge of decision making purposes regarding individual and group for the purposes of these guidelines. This definition of Big Data therefore encompasses both Big Data and Big Data analytics." [78]

Big Data is explained in foot note that 'Extremely large data sets that may be analysed computationally to extract inferences about data patterns, trends and conditions".[79]Big Data Analytics defined according to European Union Agency for Network and Information Security as "Big Data analytics refer to the whole data management lifecycle of collecting, organising and analysing data to discover pattern, to infer situations or states to predict and to understand behaviour"[80](ENISA 2015) Supervisory Authority and Sensitive Data defined as per the definitions under Convention 108.

Part IV provides for the principles and guidelines for processing. 1.1) where information is used for predicting purposes in decision making process, the likely impact of intended Big Data processing and its broader ethical and social implications to safeguard human rights and fundamental freedoms shall be taken in to consideration. 1.2) Processing shall not be in conflict with ethical values commonly accepted in relevant community and should not prejudice social interest, values and norms. 1.3) Assessment of impact shall highlight a high impact of use of Big Data on ethical values, 1.4) Data processor or data controller shall establish ad hoc committee to identify specific ethical values or the help shall be taken from the existing committee.

[78] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 23, 2017)
[79] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 23, 2017)
[80] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 23, 2017)

2. Preventive policies and risk assessment shall be done[81]. 3. Purpose limitation and transparency shall be followed and maintained[82]. 4. For risk assessment and preventive policies, the processors shall adopt adequate by-design solutions[83]. 5. Consent shall be obtained by providing comprehensive information about outcome of assessment process as use of Big Data is complex. [84]Here the informed consent is provided specifically explaining the outcome and its impact on the individual shall be done.

6.1) Data protection principles are to be followed as long as data enables the identification or re-identification of individual. Process of anonymisation which is followed in data protection shall be followed[85]. 6.2) Risk of re-identification shall be assessed by Controller[86]. 6.3) To prevent re-identification, technological measures may be combined with legal or contractual obligations[87].

To prevent breach of right to privacy by mechanical and static decisions after processing of Big Data, the human intervention is provided. 7.1) Use of Big Data should preserve the autonomy of human intervention in decision making process.[88] 7.2) Decisions shall not to be based on merely de-contextualised information or data processing results.[89] 7.3) Where decisions are based on Big Data might affect individual rights significantly or produce legal effects, a human decision maker, if requested by such individual, should provide him the reasoning underlying the processing.[90]

7.4) On basis of reasonable arguments, human decision maker should be allowed the freedom not to rely on result of recommendations provided using

[81] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 23, 2017)
[82] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0(Last visited on May 23, 2017)
[83] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 23, 2017)
[84] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 23, 2017)
[85] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 24, 2017)
[86] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 24, 2017)
[87] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 24, 2017)
[88] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 24, 2017)
[89] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 24, 2017)
[90] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 24, 2017)

Big Data[91]. The intervention of human decision maker is allowed where the rights of the individual is affected because of processing of Big Data.

This is important as the mechanical decisions are not arrived at by considering the situation of the individual and decision may affect the rights and fundamental freedoms. Human intervener can make the decision in appropriate conditions. It is important to note that the European Commission provided for human intervention in cases where the rights of the persons or fundamental freedoms are invaded or encroached. This lessens the threat of mechanically given decisions same for all persons.

Under 7.5) the responsibility to prove that discrimination is not done is cast on controller and processor of Big Data. It is provided that "if there are indications from which it can be presumed that there has been direct or indirect discrimination based on Big Data analysis, controller and processor should demonstrate the absence of discrimination.[92]

In these guidelines protection for analysis of Open Data is provided. Open Data is defined as "Publically available information that can be freely used, modified, shared and reused by any purpose according to conditions of open licenses."[93] This is novel concept providing protection for the data not collected directly from the persons but available publically. It recognises that the analysis of such Big Data available in public domain may also result into loss of privacy of the person. In this era of computerisation this publically available data is in significant quantity.

Under 8 guidelines regarding Open Data are given. 8.1) It is provided that "public and private entities should carefully consider their Open Data policies concerning personal data since open data might be used to extract inferences about individual and groups"[94]. 8.2) "Assessment process shall take into

[91] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 24, 2017)
[92] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 24, 2017)
[93] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 24, 2017)
[94] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 24, 2017)

account the effects of merging and mining different data belonging to different Open Data sets"[95].

For Open Data sets, the precautionary provisions are made as results of merging or mining of data may result into loss of rights. In computer technology merging or mining of data is done using advanced techniques like Machine Learning and Data Mining. They are used to assess the decision making patterns from the large data sets like Big Data. Here Commission has touched the issue but it is not fully developed. Also in Open Data, not only the personal data in public domain but non-personal data which is available in public domain is also included. By using advanced processing technics, personally identifiable information can be sorted out from non-personal data. But the guidelines are silent about this non-personal data protection.

The radical development in information and communication technology is observed after development of Artificial Intelligence.(AI) Artificial Intelligence is the technique which uses the computer to perform tasks as humans do in those particular tasks. They copy the cognitive functions of human minds as learning and problem solving. Machine becomes increasingly capable for tasks considering the requirement of 'intelligence'. AI uses methods based on statistics, probabilities and economics. The information provided is disseminated and processed by machine learning and data processing and computer takes the decision as human works in that particular situation. But these uses pose threat to privacy of the individual. As computer takes the decisions as human takes in the particular situation, more and more tasks will be performed using Artificial Intelligence. It is used in smart cities, smart homes. European Union has issued guidelines for the Artificial Intelligence for data protection in 2019 under the Convention 108.

4.2.8 Guidelines on Artificial Intelligence and Data Protection:[96]

[95] https://rm.coe.int/t/-pd-2017-1-bigdtaguidelines-en/16806f06d0 (Last visited on May 24, 2017)
[96] https://www.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8 (Last visited on May 2, 2019)

The definition of Artificial Intelligence is provided as "A set of sciences, theories and technique whose purpose is to reproduce by a machine the cognitive abilities of a human being, Current developments aim, for instance, to be able to entrust a machine with complex tasks previously delegated to a human".[97] These guidelines are in three categories, one general category, second guidelines for developers, manufacturers and service providers, and third for policy makers and legislators. The guidelines in general category include that i)all AI application used in decision making shall maintain human rights, particularly right to protection of personal data, fundamental freedoms. ii) development in processing of personal data by AI applications shall be based on privacy principles including risk management and data security. Iii) Focus in innovation of AI shall be on avoiding and mitigating potential risks of processing of personal data. iv) risk assessment shall be done according to the principles set in Guidelines for Big Data and shall include functioning of democracies and social and ethical values along with privacy principles. v) meaningful control of data subject over data processing shall be allowed.

Guidelines for developers and manufacturers and service providers include value oriented approach shall be adopted in designing products in consistent with Convention 108, assessment of possibility of average consequences on human rights and fundamental freedoms, adopt precautionary measures for mitigating risks, human right by-design approach shall be adopted, set up and consult independent committee for ethically and socially oriented designed AI applications, adopt algorithm which promote accountability etc.

For policy makers and legislators the guidelines are public procurement procedures shall be imposed on AI developers, Supervisory authorities shall be given adequate funds to control and administer, human intervention in decision making with AI shall be preserved, appropriate mechanisms to be established to ensure independence of consulting committees.

[97] https://www.coe.int/en/web/huan-rights-rule-of-law/artificial-intelligence/glossary (Last visited on May 2, 2019)

These guidelines are provided for the countries in European Union. It was explained in the guidelines on Big Data that the guidelines are issued to modernise the Convention 108 i.e. to keep pace with the technological advancement, which is continuous process. Still we do not observe the adverse effects of AI applications and their role in data processing. But with the passing of time, the effects will be observed. When the legal framework is prepared for protection, these guidelines will provide the sound base.

Technologically advanced countries like United States of America and United Kingdom have substantial business transactions with European countries. Due to globalisation, business transactions have increased its pace and quantity. Data protection is important to protect the business interests and legal rights of the persons. These countries also have framed privacy and data protection legislations. The researcher tries to trace the development of right to privacy and data protection in these countries.

4.3 United States of America: Legislative Measures

In the early history of America, the privacy was associated with 'gossip' and 'eavesdropping'. But these gossipmongers and eavesdroppers could be punished in very few cases. The Constitution of United States of America has not recognised the right to privacy in it. Bill of Rights provides certain rights and freedoms which can provide protection for this right. The Right to Privacy is recognised first time in the article 'Right to Privacy' by Warren and Brandies[98] and then upheld by courts in America while providing protection by interpreting the rights and freedoms provided. It was interpreted by the court that Right to Privacy is covered under the different constitutional amendments. Partly because of these decisions of court and partly it was necessary to mitigate the adverse effects of technological advancements, the government initiated to enact different legislations protecting privacy and personal information or data.

[98] Warren and Brandeis, "Right to Privacy", Harvard Law Review, Vol. IV, no.5, 1890

It can be observed that the privacy protection was first provided under constitutional rights and then by legislations. USA does not have one overall privacy and data protection legislation but it has sector specific legislation providing protection to stakeholders in that particular sector, e.g. stakeholders in health data are covered under HIPAA. The development of these laws is discussed in following paragraphs by the researcher.

4.3.1 Constitutional Provisions

This the fundamental law of US federal system. This right is not specifically protected by the provision in Constitution. Even when the Bill of Rights were enacted, this right was not included. But right to privacy can be searched under First, Third, Fourth, Fifth and Fourteenth Amendment of the Constitution of United States. First amendment protects the right to peaceful assembly and liberty to associate in private.[99] Under Third amendment without consent of owner of the home, government is prohibited of quartering the soldiers[100]. Fourth amendment gives protection against the warrantless and unreasonable searches of any area in which a person maintains reasonable expectation of privacy by the government.[101] Right of criminal suspects to keep secret any incriminating evidence that might help the government to obtain a conviction against him is protected by Fifth Amendment[102]. Under Fourteenth amendment, citizens cannot be denied by the State its citizens certain fundamental rights which are essential to the concepts of equality or liberty, including right to autonomy, dignity and self-determination[103]. These Amendments protects the right to privacy in various cases. It can be seen the development of the concept from right to physical privacy to right to data protection from the decisions of the courts.

Courts in different cases granted the protection against the invasion. For that purpose Court has interpreted the Amendments to Constitution. Starting from protection for physical privacy in Rochester Folding Box (1902) use of the name

[99] First Amendment, www.whitehouse.gov (Last visited on May 24, 2017)
[100] Third Amendment, www.whitehouse.gov (Last visited on May 24, 2017)
[101] Fourth Amendment, www.whitehouse.gov (Last visited on May 24, 2017)
[102] Fifth Amendment, www.whitehouse.gov (Last visited on May 24, 2017)
[103] Fourteenth Amendment,www.whitehouse.gov (Last visited on May 24, 2017)

of plaintiff without permission, Pavesich (1905) where name of the plaintiff was wrongly used without his permission by company, New Comb Hotel ((1921) intrusion in the room the plaintiff was protected. Regarding communication privacy in Olmsted (1928) where issue of wiretapping of the telephone was involved, and Katz (1976) for evidence collected by tapping of the telephone privacy was protected-under Fourth amendment. Regarding decision about one's family life in Ulman (1961) and, Griswold (1965) and Roe (1973) decision regarding married life and parenting, court has protected the decisional privacy under freedom of expression in First Amendment. In Jones (2012), Court held that Global Positioning System used by Police to track the movements of suspect is 'search' and covered under the protection of Fourth Amendment. In Supnick (2000) where data accessed by Amazon's Alexa when used by Amezon was challenged and court held that Right to privacy is protected under Electronic Communication Privacy Act, 1986 (ECPA). So it can be observed that the protection is provided earlier for physical privacy was extended to invasion on informational privacy.

4.3.2 Other legislations

Apart from the Constitutional provisions, some legislations are there for protection of privacy of the individual. With evolution of new challenges because of advent in technology, it was observed that the Right to Privacy is encroached and violated in various situations. This threat to the right was protected by enacting the sector specific privacy legislations. United States does not have omnibus provision for protection of privacy but sector specific legislations are protecting the rights of the stakeholders regarding that particular field. Eg. HIPAA for Health data. It can be found from these legislations that from the beginning the protection is provided regarding information of the person and not for physical privacy and with the development of technology, the legal protection was provided by enacting the laws. Some of the major legislations are in this regard are as follows:

- Fair Credit Reporting Act, 1970
- Family Educational Rights and Privacy Act, 1974

- Privacy Act, 1974
- Right to Financial Privacy Act, 1978
- The Cable Communication Policy Act, 1984
- Electronic Communication Privacy Act, 1986
- Computer Matching and Privacy Protection Act, 1988
- Video Privacy Protection Act, 1998
- The Health Insurance Portability and Accountability Act of 1996
- The Children's Online Privacy Protection Act, 1998 (COPPA)
- E-Government Act, 2002
- Federal Information Security Management Act, 2002
- Driver's Data Privacy Act, 2015

4.3.2.1 Fair Credit Reporting Act 1970[104]- This federal Act was passed to control the misuse of the personal information in the field of financial data privacy. Loan and financial credit is given on the basis of credit report of the credit reporting Agency. Many credit agencies started misusing the information of the person. To eradicate the complaints against such agencies, Congress enacted this Act.

It was passed with an objective to have fairness, accuracy and privacy of personal information contained in credit reporting agencies[105]. This credit report is necessary for the credit agencies to decide the eligibility of the consumer. The Act regulates the collection, dissemination and use of consumer information. Consumers have right to access every 12 months the information they have submitted to the agency and also have rights to verify, to dispute the information, to remove outdated or negative information (after 7 years in general, 10 years in cases of bankruptcy)[106].

This legislation protects the personal information held by credit reporting agencies which is crucial for obtaining the loan and financial assistance. In the

[104] Fair Credit Reporting Act, 1970. Available at www.govinfor.gov/content/pkg (Last visited on May 24, 2017)
[105] Fair Credit Reporting Act, 1970, Title 15 S. 1681(a)
[106], Fair Credit Reporting Act, 1970,S.1681g (c),(B)

Act, the duty is cast on the agency to collect information in lawful and fair way. It gives right to consumer to verify the information held by agency as it is important to remove or erase false or irrelevant information with the agency to give fair chance to the person to enhance his credit eligibility.

The information with the educational institution can also be compromised when such data is access for commercial purpose like targeting the advertisement regarding children or adolescents. To prevent this the information collected by educational institution is protected by Family Educational Rights and Privacy Act, in 1974.

4.3.2.2 Family Educational Rights and Privacy Act, 1974[107] was enacted to protect the stakeholders in educational sector who are registered with any educational institutions about their information with them.

Under this Act, educational institutions shall maintain the privacy of parents and students and shall not release the personally identifiable information about student in the educational record to outsiders.[108] Parents can access the record and inspect the record to ascertain the educational record of the student[109]. They have right to ask the educational entities to rectify the information if it is incorrect[110]. The law applies to all schools that receive funds under an applicable program of U.S. Department of Education. Students when completes 18 years, these rights are transferred to them[111].

The objective is served when the school or educational institution receive funds by U.S. Department of Education. But if the school is not receiving funds, the protection may not be available to stakeholders. Information collected and held by non-governmental entities are protected by the Acts. But the information collected and held by government agencies can also be compromised which may

[107] Family Educational Rights and Privacy Act, 1974. https://www.2ed.gov/policy (Last visited on May 24, 2017)
[108] Family Educational Rights and Privacy Act, 1974 CFR 34 CFR, S.99.2, along with 20 U.S.C. s.1232g
[109] Family Educational Rights and Privacy Act, 1974 CFR, S. 99.4along with 20.U.S.C.s.1232g34.
[110] Family Educational Rights and Privacy Act, 1974 34 CFR S. 99.4
[111] Family Educational Rights and Privacy Act, 1974 CFR 34 S.99.5

result in to privacy breach of the individual. To protect against such danger the Privacy Act is enacted.

4.3.2.3 Privacy Act, 1974

In 1974, **Privacy Act 1974**[112] was enacted. It was amended in 2006. This Act provides protection of the personal information held with the federal agencies i.e. by the government.

The Privacy Act does apply to the records of every 'individual' but it applies only to the records held by an 'agency'.[113] A United States Federal Law which gives guidelines for fair use about collection, maintenance, use and dissemination of that information which is maintained by federal agencies in their records. [114]Agency shall not disclose information of a person without obtaining written consent of him.[115] If the disclosure is pursuant to one of the twelve statutory exceptions consent is dispensed with[116]. Individuals have right to seek access and amendment of their records.[117] Each United States Government Agency shall have an administrative and physical security system to prevent the unauthorized release of personal records.

Fair credit Reporting act governs the data collected by credit reporting agencies. But government can access any information about the financial position of the person while deciding his creditworthiness. It was important to regulate the power of government to access the information about financial status of the person. Government has enacted the Right to Financial Privacy Act.

4.3.2.4 Right to Financial Privacy Act, 1978[118]This Act limits the power of federal government to access the information regarding the citizen's financial records. The government has to follow certain procedure to access the information. This Act establishes specific procedures that federal government

[112] The privacy Act, 1974. www.justice.gov/opcl (Last visited on May 28, 2017)
[113]The Privacy Act, 1974, 5 U.S.C. s.552a (1)
[114] The Privacy Act, 1974, 5 U.S.C.s. 552a(e)
[115] The Privacy Act, 1974, 5 U.S.C.s. 552a(b)
[116] The Privacy act, 1974, 5 U.S.C.s. 552a (b)(1)
[117] The Privacy Act, 1974, 5 U.S.C.s. 552a (d) (1)(2)
[118] www.epic.org (Last visited on May 28, 2017)

authorities must follow in order to claim information from financial institution about customer's financial records[119]. Duties are cast on financial institutions prior to release of information requested by federal authorities[120]. It is amended several times permitting greater access without customer's notice to collect customer's information requested for criminal law enforcement purposes and for certain intelligence activities.

Another development was the use of technology in the field of cable television. They are run by state governments, federal government and by local authorities. Subscriber's personal data is collected with them when a person subscribe for the services. For protection of this data became important which resulted in to Cable Communication policy Act.

4.3.2.5 The Cable Communication Policy Act, 1984[121].

This Act applies to Cable Television Industry. It establishes uniform national policy for regulation of cable television communication by federal, state and local authorities. This Act was enacted with the object to protect subscribers against the unreasonable charging of fees, cable connection with unreasonable conditions also. Under this Act, cable companies must provide a written notice of privacy practices to each subscriber at the time of entering into a service contract an at least once a year thereafter.[122] In the privacy notice, it is to be specified the uses of personally identifiable information after the collection of it.[123] Privacy principles provided by OECD are included in this Act. Disclosure of personal information without consent is permitted in certain situations as on consent or pursuant to a court order[124]. The cable service customer must be given access to the persona information collected about him or her, "at reasonable times and at a convenient place"[125]. The subscriber must be provided with a reasonable opportunity to have any errors in that information corrected.[126] The cable service provider must destroy personal information when it is no longer

[119] Right to Financial Privacy Act,1978, 12 U.S.C. S.3402 along with S. 3403,
[120] Right to Financial Privacy Act, 1978, 12 U.S.C. S. 3011
[121] www.govtrack.us/congrss/bills/98/s66/text. (Last visited on May 28, 2017)
[122] Cable Communications Privacy Act, 1984, 47 U.S.C. s. 631(a) (1)
[123] Cable Communications Privacy Act, 1984, 47 U.S.C. s. 631(a) (1)
[124] Cable Communications Privacy Act, 1984, 47 U.S.C. s. 631(a) (2)
[125] Cable Communications Privacy Act, 1984, 47 U.S.C. s. 631(a) (2),(d)
[126] Cable Communications Privacy Act, 1984, 47 U.S.C. s. 631(a) (2),(d)

needed for the purposes for which it was collected and there are no pending requests for access[127].

It protects the subscribers to the cable services providers against the release of the personal information. But the objective of the Act was not fulfilled as cable operators dominated the committee for enactment of this Act and many provisions were against the interests of the subscribers.

After innovations in the field of information technology during this period, the use of internet was increased. Communication was done through internet by sending e-mails. The government felt need to protect the interests of the users of internet and enacted Electronic Communication Privacy Act.

4.3.2.6 Electronic Communication Privacy Act[128] 1986.

Electronic Communications Privacy Act (ECPA) updated Federal Wire Tap Act 1968. It was amended after the advent of electronic communication and increase in use of internet. It protects wire, oral and electronic communications while those communications being made are in transit and then they are stored on computers.[129] The Act applies to e-mails, telephone conversation and data stored electronically. It prohibits intentional, actual or attempted interception, use, disclosure or "procurement of any other person to intercept or endeavour to intercept any wire, oral or electronic communication[130]. It also prohibits use of illegally obtained communication as evidence.[131] Title II of ECPA 1986 include Stored Communication Privacy Act which protects privacy of contents of files stored by service providers and of records held about the subscriber by service providers.[132] This Act extends the protection from the telephone communication to the computer messages in emails and other information.

The identification of the citizen is done for various purposes by the government. For this purpose, the information stored in various computer systems of different

[127] Cable Communications Privacy Act, 1984, 47 U.S.C. s. 631(a) (e)
[128] www.it.ojp.gov/privacyliberty/authorities/statutes/1285 (Last visited on June 2, 2017)
[129] Electronic Communication Privacy Act, 1986, 18 U.S.C. S.2511
[130] 18.U.S.C. S2515
[131] 18 U.S.C. S2515
[132] 18 U.S.C. Ss. 2701-12

government departments are accessed and matched. In this process, the privacy of the individual is threatened and his interests may be jeopardised because of this matching. To protect the rights of citizen, government has enacted legislation for computer matching.

4.3.2.7 Computer Matching and Privacy Protection Act, 1988

The Computer Matching and Privacy Protection Act, 1988[133] has amended Privacy Act, 1974, by adding certain provisions of protection for the subject of privacy Act records whose records are used in automated matching programs. It applies to systems of records a defined by the Act: collections of records about U.S citizen or legal, permanent resident alien.[134] In records he is connected to an identifier of an individual and retrieved by an identifier[135]. It requires an agency to conclude an agreement with partner matching agency describing the records that will be matched and procedures to be followed before, during and after the matching.[136] Agencies are prohibited to reducing, terminating or suspending financial assistance to the individual before verifying the accuracy of computerised data in the matching program. The affected individual shall be given notice of 30 days before doing the same.

Even though the protection is provided, it is very difficult for a common citizen to receive protection from the government's access of his information. It is providing only procedural safeguards but protection against use of personally identifiable data for other purposes and decision making through automated means are not provided under this fully.

An individual watches the program, or entertaining films or materials on various devices. Video tapes are one of them. Person hires these tapes from the video parlours. The record of the video tapes shows information regarding the taste, psychological inclination etc. of the individual. This information shall be protected to preserve his right to privacy. To provide the protection, Video Privacy Protection Act was enacted.

---

[133] https://uscode.house.gov/ (Last visited on June 2, 2017_
[134] Computer Matching and Privacy Protection Act, 1988, S. 552a(2)
[135] Computer Matching and Privacy Protection Act, 1988, S. 552a(5),
[136] Computer Matching and Privacy Protection Act, 1988, S.552a (a)(o),

4.3.2.8 Video Privacy Protection Act, 1998[137]-

This Act protects privacy of consumer who has purchased or rented videos. Personally identifiable information (PII) includes information which identifies a person having requested or obtained specific video material or services from video service provider.[138] Such information cannot be disclosed without consent by customer in writing regarding the Personally Identifiable Information (PII).[139] It regulates videotape service providers which is defined as "any person engaged in business in or affecting interstate or foreign commerce, of rental, sale, or delivery of pre-recorded video cassatte tapes or similar audio visual materials or any person or entity to who a disclosure is made".[140]

This Act protects the personal choice of the person, his freedom to choose for himself as what to observe in his leisure time. Protection is provided for both, rented and hired video tapes or cassettes.

4.3.2.9 The Health Insurance Portability and Accountability Act of 1996[141]

A very important and crucial area where the privacy is needed is health sector. The information regarding health data is sensitive personal information. Compromise of this data may harms the individual vey severely. The government has enacted the law to protect the privacy of health data.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted to protect the privacy of the information regarding the patients. The office of Civil Rights enforces the **HIPAA Privacy rules,** which protects the privacy of individually identifiable health information and sets national standards for the security of electronic protected health information[142]; the HIPAA breach Notification Rule, which requires covered entities[143] and business associates[144] to provide notification following a breach of unsecured protected health information;[145] and the confidentiality provisions of the Patient

[137] https://epic.org/privacy/vppa/ (Last visited on June 2, 2017)
[138] Video Privacy Act, 1998 S. 2710 (a) (3)
[139] Video Privacy Act, 1998. S.2710 (b)(2) (B)
[140] Video Privacy Act, 1998. S.2710 (a)(4)
[141] Public law 104-191, https://www.hhs.gov/ocr/privacy (Last visited on June 2, 2017)
[142] Health Insurance Portability and Accountability Act, 45 CFR S. 160.103
[143] Health Insurance Portability and Accountability Act, 45 CFR S. 160.103
[144] Health Insurance Portability and Accountability Act, 45 CFR S.160.103
[145] Health Insurance Portability and Accountability Act, 45 CFR S.164.410

Safety Rules, which provide that protected information may be used for treatment, or healthcare operations. [146]

The provisions of this Act and the Rules under it are applicable to the 'covered entities' means the health professionals and their associates which are covered described under the Act. It is not for the health care professionals who are not 'covered entities'. Intra and inter-hospital transfer of health data is not specifically protected and provided for sufficiently.

4.3.2.10 The Children's Online Privacy Protection Act, 1998 [147]

Children are in the vulnerable group of persons. Protection of children is very crucial and sensitive issue as they are using information technology more than elders. Privacy invasion on children may result not only to physical harm but psychological harm also.

The Children's Online Privacy Protection Act, 1998 (COPPA) Act was enacted to protect the children below 13 years of age while using the internet[148]. The Act provides that it is unlawful to collect the information from a child including name, residential address, telephone numbers and social security number without following the provisions of Act[149]. The express consent of the parent must be obtained by website owner before they collect, use or circulate any sensitive personal information about the children[150].

Though the objective of this Act is laudable but where children creates fake identity by providing wrong information, the objective to protect fails. There is no system to verify the true age of the child.

Today government provides services to its citizens through information technology. For this, personal information is collected by the government. The privacy, security and confidentiality of the persons are at stake if the information

[146],Health Insurance Portability and Accountability Act, 45 CFR S. 164.506
[147] https://www.fts.gov/ogc/coppa1htm (Last visited on June 2, 2017)
[148] Objective-15 U.S.C. 6501
[149]Children's Online Privacy Protection Act, 1998, S.312.3
[150] Children's Online Privacy Protection Act, 1998, S.312.5,

gathered with the government is compromised. To provide security and protection, E-Government Act is enacted.

4.3.2.11 E-Government Act, 2002.[151]

Computer and internet is rapidly changing interactions and relationship among citizens, private business and government.[152] E-government is important element in management of government. It is implemented as part of management framework which addresses finance, procurement, human capital and other challenges to improve the performance of government. The purposes are – i) to provide effective leadership of federal government efforts to development and promote electronic government services and processes by establishing an administrator of new Office of Electronic Government within Office of Management and Budget,[153] ii) promote use of internet and other information technology to provide increase opportunities for citizen participating in government[154], iii) to promote interagency collaboration for service to citizen[155], iv) improve ability of government to achieve agency missions and program performance.,[156] v) to promote better informed decision making by policy makers,[157] vi) to promote access to high quality government information and services across the multiple channels[158].

It establishes a framework of measures that require using internet based information technology to improve citizen access to government information and services and for other purposes. It provides that Agency collecting the information shall conduct Privacy Impact Assessment before collecting the information from citizens.[159] Also privacy notice shall be given before collection specifying the purpose, type of information collected, intended use of the information etc.

[151] https://www.justice.gov.us/opcl/e-governemnt-act-2002 (Last visited on June5, 2017)
[152] E-Government Act, 2002, S.2 (1)
[153], E-Government Act, 2002, S.2 (b) (1)
[154], E-Government Act, 2002, S.2 (b) (2)
[155] E-Government Act, 2002, S.2 (b) (3),
[156] E-Government Act, 2002 S.2 (b)(4)
[157] E-Government Act, 2002 S.2 (b) (7)
[158] E-Government Act, 2002 S.2(b) (8)
[159] E-Government Act, 2002. S.208 (b) (B)

4.3.2.12 Federal Information Security Management Act, 2002

Information in the federal system has to be protected. The government enacted the **Computer Security Act, 1987**[160]**-** It was federal law. It was intended to improve the security and privacy of sensitive information in federal computer systems to establish minimally acceptable security practices or such systems. But this Act was repealed and enacted in to Federal Information Security Act, 2002 as Title III of E-Government Act, 2002.

It is included as Title III of E-government Act, 2002. This Act assign responsibility to federal agencies, National Institute of Standards and Technology and Office of Management and Budget to strengthen information security system. It requires that such agencies provide and implement policies and procedures to cost effectively reduce information technology security risks to an acceptable level.

With the development of technology, the security devices are used in the vehicles also. Such devices are used to record the information before the crash of the vehicle. Such device is generally installed in aeroplanes but in modern technologically developed cars also it is installed. Such data needed to be protected to prevent misuse. Driver's data privacy act serve the purpose.

4.3.2.13 Driver's Data Privacy Act, 2015[161]

It protects consumer's personal information recorded in device fitted in vehicle. It provides for data recorded and stored within an on-board known as Event Data Recorder (EDR). Any data retained by Event Data Recorder is a property of owner of car or lessee of motor vehicle. [162] The EDR is a device that records the vehicle's dynamic time-series data during the time period just prior to crash or during crash. It is used for retrieval of data after crash. It includes read and write memory considering the speed of the vehicle, sudden stoppage, low oil pressure etc.

[160] https://epic.org/crypto/csa/csa.html (Last visited on June 5, 2017)
[161] www.epic.org/privacy/drivers (Last visited on June 5, 2017)
[162] Driver's Data Privacy Act, 2015, S.2 (a)

Such data shall not be accessed by a person than owner or lessee except, i) court's order or judicial or administrative authority, ii) owner or lessee provides written, electronic or recorded audio consent to retrieval of data, iii) pursuant to investigation or inspection authorised and personally identifiable information of owner or lessee is not disclosed in connection with retrieved data, iv) for purpose of determining the need for or facilitating emergency medical response in motor vehicle crash, v) for traffic safety research and personally identifiable information of owner or lessee is not disclosed. [163]

'Privacy' from the beginning of the civilization was valued dearly. It was covered under constitutional protection. In absence of any legislation for privacy of the stakeholders, it is difficult for any nation to protect the legal rights of the citizens and interests of the state. Use of technological devices in modern era results in 'invasion and intrusion on seclusion'[164]. Due to emergence of information and communication technology, the threat to the privacy of personal information had increased as monetary value of information is increasing day by day. America, the country with highest connectivity and convergence has become susceptible to the threats and encroachments.

It had responded in appropriate manner with enacting Acts as and when required. It can be seen from the enacted legislation in USA that privacy protection has developed and informational privacy has become important aspect of privacy and data protection legislation. America has developed the legal framework for data protection as and when the need arises due to technological innovations. The speciality of US legal framework is that there is separate laws for privacy breaches, national security, online obscenity, data protection in various fields like health data and driver's data etc.

[163] Driver's Data Privacy Act, 2015, S.2 (b)
[164] Lloyd Ian J and Simpson, M.J "Computer Crime" in Chris Reed (Ed), Computer Law(3rd Edition, Universal Law Publishing) 92

4.4 United Kingdom: Legislative Measures

In colonial England, the privacy was associated with the activities of gossip mongers. Religious beliefs maintained the surveillance over the behaviour of the fellow citizens. British constitution is in unwritten form. In Briton there are no specific provisions for right to privacy under the constitution as a fundamental right. In the beginning, the right to privacy was protected up to certain extent under Law of Torts, provisions of defamation and of trespass to property or person.

But Law of defamation does not provide any protection where the facts are true. In such cases if a person does not want the facts to be disclosed to public, how much damage he suffers or how much agony he suffers because of the disclosure, he does not have any remedy. He had to argue on the basis of breach of confidence if the relationship is of formal nature.

British government appointed committee to verify whether right to privacy is required. But the committee opined that it is not required in England. Being a member of European Union, Briton was bound by the Convention and Directives issued by the European Union. Because of this, it had enacted Data Protection Acts. So, in England privacy was and is associated with the protection of personal information or data. Where data is not involved, privacy is protected by law of trespass to person and breach of confidence.

The situation was slightly changed when England has enacted Human Rights Act, under which the protection to the privacy of person, his family and personal life is provided. The researcher discussed the development of right to privacy and data protection in UK in the following paragraphs.

4.4.1. Legislative efforts

In England many people were in favour of acceptance of the law of privacy. Three bills were presented in parliament during 1960s to create such right. In 1961, Lord Mancroft presented the private members bill, it was withdrawn due to lack of support from the government. In 1967, Mr. Alexander Lyon presented the bill, it was rejected for being too limited and in 1969, Mr. Brian Walden

presented the bill, it was rejected for encroaching too far in freedom of expression. Lord Denning spoke in support of Lord Mancroft's Bill of privacy in House of Lords.[165] These reports are set out in Younger Report.[166]. It was felt that it is difficult to enact legislation providing same standard of protection for private and public sectors effectively. Threat to data contained in computers is more than the threat to paper documents.

In 1969, Lord Windlesham introduced private member Bill dealing specifically with computerised personal records. Although it was unsuccessful, private member's bill presented in 1970, led to government concern and resulted in appointment of Committee under **Sir Kenneth Younger.**

4.4.2 Younger Committee:[167]

The object for forming the committee was "To consider whether legislation is needed to give further protection to individual citizen and to commercial and industrial interests against intrusions in to privacy by private persons and organisation or by companies and to make recommendation."[168] The investigations were explicitly limited to private sector. The committee's request to deal in the public sector including the intelligence system and defence of the country was refuted by Home secretary.

The committee found very difficult to define 'privacy' and felt that it is illusive. It was felt that if the legal force is applied for enforcing privacy, it will cover the area too wide and result into encroaching other freedoms. The committee examined the intrusion on privacy by media, but it was of the opinion that the existing laws are sufficient for controlling the intrusion. Three remedies were suggested by the Committee, one- new tort of unlawful surveillance should be considered as criminal offence, secondly- disclosure or other use of information which is unlawfully acquired shall be protected by tortuous action, third- it was suggested that encroachment shall be covered under breach of confidence.

[165] H.L Debates, Vo. 229 Col.638.
[166] Appendix F.PP 273-278
[167] https://onlinelibrary.wiley.com/doi/pdf/10.1111 (Last visited on June 5, 2019)
[168] Lord Byers on presenting committee report. https://api.parliament.uk/historic-hansard/lords/1973/jun/06 (Last visited on June 5, 2019)

The committee thought that in many cases legal action is too harsh and administrative control is also undesirable. Therefore it had suggested the measures like self-discipline. So for control over the media i.e. press, press council shall have appoint control committee. The Committee has suggested increase in the membership of the control committee of laymen i.e. person from outside the press, for control over the press. Moreover, the Press Council shall create Code of Ethics for the guidance of 'working journalists'. Complaints received and adjudicated by the Complaints Review Board, should be published.

On surveillance devices- Wide variety of surveillance material and bugging devices was shown to the committee and bugging work was also demonstrated to it. It was difficult for the Committee how to define 'unlawful surveillance'. The committee concluded that surreptitious use of devices without the knowledge of victim is the unlawful surveillance.
So, the emphasis is on use and not on the device. This offence is applicable to photography, including infra-red or two- way mirrors and all other tricks. On the issue of private detectives, it was suggested that they should be given licenses.

The committee had observed the working of computers and provided confirmation of existence of level of concern about computers. It stated, "We cannot on the evidence before us conclude that the computer as used in private sector is at present a threat to privacy, but we recognised that there is a possibility of such a threat becoming a reality in future"[169] and it has suggested appointment of standing commission for examination of the use of computers particularly for the handling of the personal information. The committee's report was published in 1972 and it found no necessity for general right of privacy.

It is evident from the Younger Committee's report that the committee was not of the opinion that right to privacy shall be separately enacted. The committee found difficult to define 'privacy' It was of the opinion that instead of separate

[169] https://api.parliament.uk/historic-hansard/lords/1973/jun/06 (Last visited on June 5, 2019)

legislation, self-regulation by the invading entities will serve the purpose. At that time the invasion by the press was the issue. The Committee had held that existing laws are sufficient to control the invasion and stressed that press council itself shall regulate by making rules and laws about intrusion in the privacy of the person. But self-regulation does not work when the news hungry reporters try to get sensational news. Regarding computers also the committee failed to grasp the impact of information technology on the privacy of the person.

4.4.3 Post Younger Committee

Three years after **Younger Committee**'s report that a Government white paper was issued on "Computer and Privacy" together with a supplement "Computer: Safeguard for Privacy". These papers responded Younger Committee's Report finding relative to private sector and provided evidence that study of confidentiality in state computer. Views expressed by **Younger Committee** were supported by **McGregor Commission** in 1977.[170]These reports were followed by two bills presented within 1988-89 parliament sessions but again both were failed.[171] In 1990, **Calcutt Committee** again rejected creation of tort of Privacy in favour of press self- regulation through Press Complaint Commission.[172]

A final statement of **Calcutt Committee** expressing government's view was presented in 1995. Once again self-regulation was preferred and intention to introduced tort of privacy was not expressed.[173] However, subsequent review in 1993 of Calcutt Committee was critical of this approach and recommended a statutory system for complaints and new tort of invasion of privacy.[174] The government came to the conclusion that there is no need for protection of privacy specifically as it is sufficiently protected under provisions of other laws.

[170] (Third) Royal Commission on the Press (Cmnd. 6810, July 1977)
[171] Bill on Protection of Privacy and Right to Reply-introduced by John Brown M P and Tony Worthington MP.
[172] Committee on Privacy and related matters. Report Committee on privacy and related matters- Chairman: David Calcutt.(Cm 1102, June 1990)
[173] Privacy and Media intrusion (Cm 2918, July 1995)
[174] Department of National Heritage, D. Calcutt, Review of Press Self-Regulation(London:HMSO, Cm 2135, 1993)

Briton has enacted Human Rights Act, 1998,[175] which inculcated most of the rights vested by Articles of European Commission of Human Rights (ECHR)[176]. These rights have provided substantial relief in the cases of violation or breach of privacy of individuals e.g. Art. 8 provides for respect for your private and family life[177]. So when it is difficult to enforce Right to Privacy under any other legislation, provisions of Human Rights Act were useful. This Act came into force in 2000. Data protection and privacy both are the different issues under British legal system. So, Briton has enacted Data Protection Acts separately.

4.4.4 Data Protection Acts

Being a member of European Union, Britain is bound by council of Europe's 1953 European Convention on Human Rights and Fundamental Freedom[178]. In this Convention, Article 8 provides for Right to privacy. The convention allows individual petitions against governments to European Commission on Human Right, if all possible domestic remedies have been exhausted. Since 1966, Britain has accepted right of individual petition under the convention and compulsory jurisdiction of European Court of Human Rights.

The white paper "Computer and Privacy" proposed legislation to cover both public and private sector information systems. The creation of Data Protection Authority was also proposed, to supervise the legislation and ensure that appropriate safeguards for individual privacy were implemented. To provide detailed structure of Data Protection authority, the Government appointed a Data protection Committee under the chairmanship of Sir Norman Lindop.[179] It presented the report in 1978. It was suggested that the Data Protection Authority shall be given responsibility for ensuring compliance with those privacy principles. The codes of practice for various sectors shall be drafted by this Authority. Overall, the report has suggested that handling of personal

[175] www.lgislation.gov.uk (Last visited on June 5, 2019)
[176] www.echr.coe.int/Documents (Last visited on June 5, 2019)
[177] www.echr.coe.int/Documents (Last visited on June 5, 2019)
[178] www.echr.coe.int/Documents (Last visited on June 5, 2017)
[179] Statistics and Report of Data Protection Committee, Available on www.jstor.org/stable/2982483? (Last visited on June 15, 2019)

information shall be regulated by different method. But nothing concrete was done by the Government.

In 1982 England being a member of European Union, there was an obligation under the 1981 convention by European Union. The Government enacted Data Protection Act 1984. In terms of the scope the Act, it was limited to data defined as 'Information recorded in a form in which it can be processed by equipment operating automatically in response to instructions given for that purpose'[180]. After this, in 1995, there was directive by European Commission being Directive 95/46/EC regarding data protection.

Need was felt to enact, amend or modify the data protection legislation because of technological development and innovations. Briton had repealed the Data Protection Act, 1984 and has enacted Data Protection Act, 1998. It was based on the principles of Directive for protection of personal data and processing of it on the basis of the principles of this directive.

4.4.4.1 Data Protection Act 1998[181]

With adoption of European Council Directive 95/46/EC, the government had an obligation to inculcate it in to national law by October 1998. The government chose to enact new legislation and repeal to Data Protection Act 1984. Data Protection Act, 1998 has 75 sections and 16 Schedules. Sections are divided in Part I to VI. The Schedules provide for the protection and processing procedures and different authorities and their powers.

Under the Data Protection Law, the protection offered to an individual data subject is on the basis of 'personal data' defined as-data which relate to a living individual who can be identified--a) from those data or, b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of the opinion

[180] Data Protection Act, 1984. S. 1(2).
[181] www.legislation.gov.uk (Last visited on June 25, 2019)

about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.[182]

The Sensitive personal data includes a) the racial or ethnic origin of the data subject, b) his political opinions, c) his religious beliefs or other beliefs of a similar nature, d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act1992), e) his physical or mental health or condition, f) his sexual life, g) the commission or alleged commission by him of any offence, or h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.[183]

For processing of the personal data, such data is to be processed fairly and lawfully after fulfilment of the conditions specified in schedules 2 i.e. with consent of data subject, for fulfilment of the contract, for compliance of legal obligation, if in the interest of data subject etc. [184] and sensitive personal data shall be processed after fulfilling the conditions in schedule i.e. with explicit consent of data subject, for performing right or obligation which is imposed by law on data controller etc.[185]

Personal data shall be obtained of specified lawful purposes and shall be not be further process incompatible with that purposes.[186] Such data shall be relevant, adequate and not excessive to the purpose.[187] It shall be accurate[188]. After the process such data shall not be kept for the longer period.[189] It should be processed according to the rights of the data subjects.[190] Personal data shall not be transferred to a country or territory outside European Economic Area unless that country or territory ensures an adequate level of protection for the rights

[182] Data Protection Act, 1998, Basic interpretations, S. 1(v),
[183] Data Protection Act, 1998, S.2
[184] Data Protection Act, 1998, Schedule 2
[185] Data Protection Act, 1998,Schedule 3, DPA, 1998
[186] Data Protection Act, 1998, Part I, Principle 1, Sch. 2
[187] Data Protection Act, 1998, Part I, Principle 3, Sch. 2
[188] Data Protection Act, 1998, Part I, Principle 4, Sch. 2
[189] Data Protection Act, 1998, Part I, Principle 5, Sch. 2
[190] Data Protection Act, 1998, Part I, Principle 6, Sch. 2

and freedoms of the data subjects in relation to the processing of personal data.[191]

The rights of the data subjects are provided in Part III as right of access to personal data[192], right to prevent processing if cause distress[193], right to prevent processing if for purpose of direct marketing[194]and right in relations to automated data processing[195]. Consent of the data subject should be freely given, specific and informed. Where the data controller does not have the consent of the data subject, the processing of personal data must be 'necessary' for one of the specified purposes, either detailed in Schedules themselves e.g. 'performance of the contract to which the data subject is a party' or 'exercise of any functions conferred on any person by or under any enactment' or in related secondary legislation.[196]

The Data Protection Act, 1998 was totally based on the Directive 95/46/EC. But in 2016, Briton has left European Union by referendum and ceased to be a member of European Union. But as the General Data Protection Regulation was scheduled to be directly applicable in all the member states beforehand i.e. from 25/05/2018, U.K. government decided to legislate to implement derogation, exemptions and adaptations in GDPR into national law during pre-withdrawal period.[197]

4.4.4.2 Data Protection Act, 2018

After General Data Protection Regulation (GDPR) by EU in 2018, though Briton has opted out of European Union, it has adopted the data protection laws as Data Protection Act, 2018. It has received Royal assent on 23rd May, 2018. It applies GDPR standards in data processing of personal data. Objectives are, protection of natural persons with regard to processing of personal data by competent authority for purpose of prevention, investigation, detection, or

[191] Data Protection Act, 1998, Part II, Schedule 2, DPA
[192] Data Protection Act, 1998, S, 7,
[193] Data Protection Act, 1998, S.10
[194]Data Protection Act, 1998, S.11
[195] Data Protection Act, 1998, S. 12
[196] Data Protection Act, 1998, Schedule 2.
[197] Data Protection Bill (HL) 2017-19 at https://services.parliament/uk/bills/2017-19/dataprotection.html (Last visited on July, 3 2019)

prosecution of criminal offences or execution of criminal penalties and on free movement of such data.

Britain has enacted the Data Protection Act, 2018 following the principles and standards provided by GDPR by modifying certain provisions. Provision are divided in six parts and there are twenty schedules in the Act. Most processing of data is subject to GDPR. Data Protection Act has provisions as provided in GDPR, applied GDPR and provisions of Law Enforcement Directive. Applied GDPR is where UK has varied GDPR. Law in applied GDPR should be read as in GDPR but qualified by modified terms and meanings under Data Protection Act, 2018. It applies to Part 2 chapter 2 and 3 mainly and some provisions relating to applied GDPR in Schedule 6 of Data Protection Act, 2018. Data Protection Act, 2018 has different principles, requirements and exemptions that are under GDPR according to requirements of UK.

Provisions for processing the personal data are enacted and these provisions are also applicable to intelligence service processing, Immigration services processing. The definitions are same as provided under GDPR for different terms. Personal data is information relating to any [198]identified or identifiable living individual, living person identifiable means any person identified directly or indirectly with any identifier. Identifier means names, location data etc.[199]

Provisions for collection, processing, storage, usage of personal data are same as provided under GDPR. But there is a difference in the age for giving consent. Under GDPR the age for giving consent is 16 years, while under Data Protection Act, 2018 age for giving consent is 13 years if the personal data is processed by Information Society Service.[200] It was controversial but the explanatory note to the bill stated that this was in line with the minimum age set by Facebook, WhatsApp and Instagram[201].

[198] General Data Protection Regulation, S.3(2)
[199] General Data Protection Regulation, S.3 (3)
[200] General Data Protection Regulation, S.9 (a), Chap.2, part 2, also www.ico.org.uk/media/guide (Last visited on September 9, 2019)
[201] Public Bill Committee 30 October, 2017cc 1264-70, House of Lords, Data Protection Bill, Second Reading, 10/10/2017 vol. 785, Column 134 mentioned in UK: GDPR Adaptations by Dr. Karen Mc Cullagh. At https://blogdroiteuropeen.files.wordpress.com/2019/02 (Last visited on September 9, 2019)

It can be argued that whether the child is mature enough to give consent. But the provision was made in Data Protection act, 2018. It was suggested that Age Appropriate Design code of Practice shall be developed. But today it is not done.

Transfer of personal data or not transfer to third countries is decided by Secretary of State who specify the necessary conditions.[202] Under GDPR, transfer to third countries is allowed if adequacy decision given by the European Commission. This provision is inculcated in the DPA, 2018 for granting the permission by Secretary of State.[203]

Processing of personal data by competent authority for law enforcement purposes and implements are provided Law Enforcement Directive (EU Data Protection Directive 2016/680). The processing relating to personal data by automated means is covered.[204] The secretary of state appoints the 'competent authority'. But intelligence service authorities are not competent authorities in this[205]. Law enforcement purpose means prevention, investigation, detection or prosecution of criminal offences or execution of criminal penalties including safeguarding against and prevention of threats to public security.[206]

Novel provisions regarding Intelligence services processing are provided. These provisions are different from GDPR as they are not provided under it. Personal data is processed by intelligence services by automated means or otherwise is included in this part.[207] Intelligence services means- security service, secret intelligence service and Government Communications Headquarters[208]. Processing the data is according to the principles same as above.[209]

Data subject has rights to have information about name and address of controller, legal basis or purpose of processing, about the categories of data

[202] Data Protection Act, 2018, Part 2, Chap.2, S. 18(1),
[203] Data Protection Act, 2018, Part 2, Chap.2, S. 18(2)
[204] Data Protection Act, 2018, Part 3, chap.1
[205] Data Protection Act, 2018, Part 3, chap.1, S.30
[206] Data Protection Act, 2018, Part 3, chap.1, S.31
[207] Data Protection Act, 2018,Part 4, Chap. 1 S. 82 (1)
[208] Data Protection Act, 2018,Part 4, Chap. 1 S. 82 (2)
[209] Data Protection Act, 2018,Part 4, Chap. 2, S. 86 to 91

processed etc. Data controller shall provide him the information about how to file complaint against controller with commissioner. Data subject also has right to access information about purpose of processing of categories of data concerned[210], the recipients' period for which this data is preserved. He also has right not to be subject to automated decision making,[211] right to intervene in automated decision making,[212] right to object to processing of data by notice [213]and right to rectification and erasure of data[214] by giving notice to controller.

Processing of information is allowed when it is necessary for the performance of task carried out in public interest or in exercise of the controller's official authority, or in administration of justice[215], or in exercise of functions of either house of Parliament[216], or in case of functions conferred on any person by enactment of rule of law[217], or in exercise of functions of Crown, minister of Crown or government department[218] or activity that supports or promotes democratic engagement[219].

4.4.5 Emerging Challenges: Data Misuse

Cambridge Analytica data security scam is a case on data misuse. This issue of misuse of data by Facebook and compromise of right to privacy had arisen in this case. The case is discussed in brief:

It is a London based company, in the field of election consultancy, providing services regarding election campaign to the political personnel. The whole story started in 2010 when Facebook launched 'Open Graph' platform which can be used by third party developers to reach out Facebook users and their personal information. Under this, the outsider app developer can also access the personal information of Facebook friends of such users. A Cambridge academic Kogen had developed an app called "thisisyourdigitallife" in 2013 which was uploaded

[210] Data Protection Act, 2018,Part 4, Chap. 3 S. 93
[211]Data Protection Act, 2018,Part 4, Chap. 3 S 94
[212] Data Protection Act, 2018,Part 4, Chap. 3 S. 96
[213] Data Protection Act, 2018,Part 4, Chap. 3 S. 97
[214] Data Protection Act, 2018,Part 4, Chap. 3 S. 99
[215] Data Protection Act, 2018,S.8(a), Part2, Chp.2
[216] Data Protection Act, 2018,S.8(b), Part2, Chp.2
[217] Data Protection Act, 2018,S.8(c), Part2, Chp.2
[218] Data Protection Act, 2018,S.8(d), Part2, Chp.2
[219] Data Protection Act, 2018,S.8(e), Part2, Chp.2

on this Open Graph. The app prompted the users to answer the questions for their psychological profile. It was reported that more than 3 million people availed the services for their psycho profiles. While using this app, user has to give permission to use his personal information. But using this information the app can access the personal information of users' Facebook friends also. Cambridge Analytica contracted with Kogen for data and obtained it.

In 2014, Facebook changed the rules for accessing the information by such apps. It had provided that the apps can access the personal information of user only and not Facebook friends without re-permission from user. But the rule was not retroactive, so Kogen did not delete the information which he had gathered in earlier profiles. That information was stored with him.

In 2015, it was reported in Newspaper, that Ted Cruz, a Presidential candidate in America is taking help from Cambridge Analytica, Facebook responded that after learning this they had banned Kogen's app and legally pressurised them to delete the data. Both Kogen and Cambridge Analytica certified it but did not delete it.

In election campaign of 2016 in America, both the candidates for presidential election took the help of Cambridge Analytica. In 2018, it was reported that more than 87 million people's personal information was accessed and political campaign was designed according to their psychological responses through processing of such data. It was disclosed afterwards by an employee of Cambridge Analytica that by doing this, the results of election was swayed.

This data privacy scam shows that data predators can access the data with legal method and then they process the data using innovative advanced methods of processing and use the data for the purposes other than for which it is collected. The purpose limitation principle is included in the Data Protection Acts but these data predators circumvent it by innovative use of technology. This also shows that even if 'consent' is mandatory condition to collect and use the data, but after giving consent a person loses the control over his own personal information that how it should be used. These breaches pose serious threats not only to privacy

but becoming a 'commodity' for the data predators and he may loses other rights, liberty and freedom also.

In recent years the use of social media sites is increased. The users have to provide their personal information for use of such sites. It is mandated that social media sites shall have the privacy policies under which the service provider is obligated to protect the personal data gathered with him. Even though the data protection is provided under these policies, still there are instances of misuse of the personal data.

Privacy was not recognised as right in UK. For the protection of the right to privacy, Briton has followed the path set by European Union by enacting Data Protection Act for protection of privacy of personal data. Data Protection Acts, 1984 and Data Protection Act, 1998 both were enacted as the directives of the European Union. But in Data Protection Act, 2018, some provisions are differently provided.

The technologically advanced countries like USA, UK and countries in European Union have enacted legislations for protection of privacy and personal data. While these countries trying to regulate and control the possible and probable encroachment on privacy of a person by electronic media and trying to protect individuals by strong laws, there was no awareness regarding the basic requirement regarding protection of privacy of the information or data. As business transactions were conducted and completed using computer and information technology in India after 1990, the legal framework for protection of the information related to business was not considered. In this situation, privacy of personal information or data was very distant thought at that time. It will be apt to know the privacy and data protection legislations in India.

4.5 India: Legislative Measures

Being a collectivist society, there was no right to privacy available in Indian society. Ancient scriptures like Arthshastra and Manusmriti provide the right to enjoy one's property without interference from others. The right in limited way was associated with the property. During the British period, i.e the pre independence era, as in other judicial systems, the right was associated with

enjoyment of property, may it be house or land. Courts in British era, in Nuth Mull (1855)[220] or Gokal Prasad (1888)[221] tried to protect the right to privacy observing that it cannot be proved that right to privacy exist in that part of territory due to mutiny as records were destroyed. But it was observed by the judges in Gokal Prasad (1888) various earlier cases like Goor Das (1867)[222].

After independence, people are preoccupied with the idea of earning the basic necessities like food, clothes and shelter. Instead of privacy, to get next meal on time was the important worry and job on hand for majority of people. The growth of urbanisation, rise in population; various shortages including shortage of living space caused a contraction in the living. Moreover, because of the radical change in economic, social, political scenario, the need for right to privacy was being realised.

4.5.1 Right to Privacy and Constitution of India

Constitution of India does not provide for the right to privacy as fundamental right. In the Constituent Assembly, an amendment on the lines of Fourth Amendment of the United States. But the members did not agree, that, this right as necessary element to achieve personal liberty and these rights were strongly opposed from the beginning. B. N. Rau himself had opposed this inclusion of right to privacy in Constitution, as he felt that, it may seriously affect the powers of investigation of the police. Also, it was felt that this right will create hardships for administering the vast country like India.

In Constitution of India, right to life and liberty is protected under Art. 21. Right to privacy was protected by the courts through the judicial creativity holding that this right is covered under Art. 21. In many cases, the Supreme Court, touched the various aspects of right to privacy and upheld this right under the fundamental right governed under Article 21 i.e. Right to Life and several other

[220] Nuth Mull v/s Zuka-Oolah Beg Sr.D.A.N.W.P.R.1855,
[221] Gokal Prasad v.Radho ILR Allahabad (10), 358 (1888),
[222] Goor Das v. Manohar Das N.W.P.H.C. Rep. 1867, 269 cited in Gokal Prasad (1888) at www.indiakanoon.org/doc/103879 (Last visited on September 3, 2018)

provisions of the Constitution read with the Directive Principles of the State Policy.

4.5.2 E -Governance and Protection of Privacy

The effect of technology on the Right to privacy is so intrusive in every aspect of human life that the demand for protection of different aspects is always made. One such aspect is informational privacy. After 1990, government started adopting e-governance in which delivery of services are done through information technology tools. Information technology and internet was introduced in India in 1990s. Due to globalisation, trade and business transactions with global firms started increasing through internet. Moreover, technology is reinvented into cheaper and cost-effective options by the technologists. Nature of business transactions was also changing due to increase in e-commerce, outsourcing of business, accepting e-governance etc. While transacting with business corporations of foreign countries, it was felt essential to have legal framework for protection of privacy of business data or information. Countries outside India have such protection in their respective legislative systems.

To control and regulate the invasion and intrusion of privacy on internet, the Government has to enact two types of legislations. One protecting the privacy of transactions on internet and cyberspace, including the physical privacy of stakeholder and secondly, protecting the privacy of personal information or data, i.e. controlling and regulating the misuse of Big Data.

For protection of privacy in cyberspace including physical privacy, the Government has enacted The Information Technology Act, 2000. It was amended in 2008 widening the scope of its applicability in the circumstances which are threatening the privacy. Various Rules like Certifying Authorities Rules, 2000, Security Procedures Rules, 2004 are also made. For the implementation procedure like Procedure and Safeguards for Interception, Monitoring and Decryption Rules, 2009 and explaining the responsibilities under the Act e.g. Intermediaries guidelines, 2011 are enacted. For protection of the privacy rights of the person, Rules regarding Reasonable Security Practices

and Procedures and Sensitive Personal Data or Information are enacted in 2011 under this Act.

For protection of credit information, the Credit Information Company (Regulation) Act, 2005 is enacted. For protection of personal data, the Government has drafted Privacy Bills in 2011, 2014 and Data Protection Bills in 2013, 2018 and 2019. But these bills are not finalised and passed by the Parliament.

To decide authenticity of benefit receiver, the government had issued Unique Identification scheme and provided identity cards. For issuance of the card personal information including biometric information was collected. Separate legislation is enacted for this as Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016. This was challenged in K.S. Puttaswamy[223] (2012), on the ground that it is violative of right to privacy.

The researcher has discussed the legislative provisions for protection of privacy in Indian legal system in the following paragraphs.

4.5.3 Legislative Provisions

In advent of information technology and internet and specifically the exposure to global market, it had become essential to provide some protection to the commercial activities in India. With this specific intention, Information Technology Act, 2000 was enacted. The object of this Act is to facilitate e-commerce mainly. The main provisions related to transactions by electronic data interchange and other means of communications are provided in the Act. The government has enacted various Rules governing the protection of privacy and empowering the government under the Act. These provisions are discussed in the following paragraphs.

4.5.3.1 Information Technology Act, 2000

[223] J.K..S. Puttaswamy and Anr. v. Union of India & Ors. W.P. 494 of 2012

The Information Technology Act, 2000 was enacted with the objective of providing legal framework for facilitating e-commerce, e-governance and protecting privacy of individuals. After enactment of the Act, information and communication technology through internet has engulfed almost all human activities at alarming speed. Almost all transactions of businesses and also the governments were done through internet. Due to its omnipotent and omnipresent nature, security, confidentiality and privacy was threatened. There were only two options, either to enact new legislation covering the protection of transactions done through information and communication technology via internet or amend or modify the existing legal provisions under Act. Indian Government has chosen the second option of amending the IT Act, 2000. The government selected to amend and enact some more provisions in the existing Act instead of enacting new legislation for data protection. This Act was amended in 2008 and its scope is widened. It covers many new activities including provisions for data protection and crimes.

4.5.3.1.1 Salient Features of the IT Act, 2000

This Act is omnibus provision for protection of transactions done through computer and internet. Some salient features of this Act are:

1. It provides for extra-territorial jurisdiction, so difficulties in deciding jurisdiction can be avoided.
2. Facilitation of e-governance activities- recognition, authentication and security of e-records is provided.
3. Recognition and security of electronic contracts.
4. Provisions of encryption and electronic signatures.
5. Data protection and reasonable security practices.
6. Intermediaries are responsible in certain situations.

It can be seen that the provisions are mainly covering and applicable to electronic transactions conducted by and in relation to government, body corporates, private persons, and intermediaries which have direct impact on protection and preservation of data and information. Apart from this the control mechanism on the transactions by these categories is also provided. Some acts

or omissions are termed as offences and crimes and penalties are provided for in the Act.

4.5.3.1.2 IT Act, 2000: Analysis

In the coming paragraphs, various provisions in Information Technology Act, 2000 which have direct impact on privacy and protection of data or information are discussed. But in the beginning, definitions of the terms which are essential for governing the privacy and data protection are to be discussed.

4.5.3.1.2.1: Definitions

For conducting electronic transactions, computer, computer network and computer resource and computer system is essential. Definition of each is provided extensively in definition section.

1. S. 2 (1) (i) provides in very time term-Computer is any electro-magnetic, optical, or any high-speed data processing device or system which performs logical, arithmetical and memory functions. Also, these functions must be performed by manipulations of electronic, magnetic or optical impulses. Definition of computer is extensive as it includes any input, output, processing, storage, computer, software or communication facilities. Any or all of them must be connected or related to the computer in a computer system or computer network.

   It has tried to cover futuristic development in technology. But today many transactions are done through non-computer device or on smart mobiles. This definition is silent about smart devices.

2. In definition of Computer network, interconnection of one or more computers, computer systems or communication device is included. This inter connection can be not only through satellite, microwave, terrestrial line, wire, but wireless or other communication media also. This interconnection done through two or more inter-connected computers or two or more inter-connected devices even though the inter-connection is not maintained continuously is provided for. The ambit of definition is vast. It incorporates all prevailing and future networks which may be perceived.

This wireless connection means wi-fi is included. But it is to be noted that 'other communication media' is not defined in the Act. This definition is important as it is extensive and include any media that help, connect other communication media.

3. S. 2 (1) (k) provides for definition of computer resource which includes 'data' as resource along with computer system, computer network, computer data base or software. It means all things provided in computer network; computer system is also covered under computer resource.

Moreover, computer data base and software are also included in computer resource which makes the definition exhaustive.

4. Computer system is defined as device or collection of devices. This collection includes input and output support devices. But it excludes devices which are not capable of working in conjunction with external files and calculators which are not programmable. The devices are included shall be capable of working in conjunction of external files which contain computer programs, electronic instructions, input data and output data, that performs logic, arithmetic, data storage, retrieval, communication control and other functions.

Computer includes any one high speed data processing device, but computer system includes any one or collection of devices which also includes input and output support.

5. Data is separately defined under the Act under S. 2 (1) (0) of the Act. It includes many things. i) information, representation of information, fact, concept, knowledge or instruction.

ii) This representation of information which may be already prepared or may going to be prepared in formalized manner is also included.

iii) If this prepared representation in formalised manner is already processed or going to be processed or is in the action of processing it is known as data.

iv) The processing must have been done in computer system or computer network otherwise it is not data.

v) Computer printouts, magnetic, or optical storage media, punch cards or paunch tapes are the recognised forms of data in the Act.

vi)The representation prepared of the information in a formalized manner which is stored in internal memory of computer is also termed as 'Data'.

6. Definition of data uses many new terms which are explained in the Act separately. Information is data. Then information includes data, text images, sound, codes, computer programmes, software and database or microfilm or computer-generated microfiche.[224] In this definition every type of representation using text, images etc. which is prepared or going to be prepared in computer system is covered.

7. Information is to be stored in electronic form if it is to be stored in the internal memory of the computer. Electronic Form means any information generated, sent, received or stores in media, magnetic, optical, computer memory, microfilm, computer generated micro fiche or similar device.[225]

8. Electronic record is created when computer and internet is used for dealing with information. Therefore, electronic record includes 'data' and 'information' which are defined earlier in the Act. It is provided under s. 2 (1)(t) and includes data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer-generated micro fiche.[226]

4.5.3.1.2.2 IT Act and Invasion of Privacy and Personal Data

When the information is collected, stored, used and processed by the Government, body corporates, private persons and intermediaries for various purposes, there is a possibility of invasion of privacy and personal data. The provisions for privacy and protection of information or data under Information Technology Act, 2000 relating to (1) Government (2) Body corporates and natural person (3) For intermediaries and (4) Other activities are discussed in following paragraphs.

Government provides services by accepting electronic mode which is known as e-governance. Privacy protection regarding government action can be subdivided in two parts:

[224] Information Technology Act, 2000 S. 2 (1)(v)
[225] Information Technology Act, 2000 S. 2(1) (r)
[226] Information Technology Act, 2000. S. 2(1)(t)

A]. E-governance

B] Powers for interception and monitoring data, etc.

A] Government actions-E-governance

1. The Act provides legality to electronic records. Due to this, all information which is in electronic form, electronic records, data bases, electronic documents become legal documents which are admissible in court of law as per S. 65B of Indian Evidence Act, 1872, which was inserted by amending Indian Evidence Act, 1872. It has to satisfy two conditions that any information or data prepared and made available in electronic form and that it can be possible to access and use for subsequent use. If they are satisfied, it is legal. Because of this provision, E-mail is also become legal.

Under S. 65B (4) Indian Evidence Act, a certificate to the authenticity of evidence is to be presented which is sometimes difficult for a common person.

2. Digital signature and Electronic signature: Electronic records can be replicated easily at low cost. It is difficult to prove whether the record is tampered with. So, the provision is made that any person can authenticate the electronic record by putting his digital signature/electronic signature. Digital signature is created using asymmetric crypto system. S. 3. Government of India prescribes the electronic signature or electronic authentication technique and procedure for affixing the signature in Schedule II. The technique is considered reliable if the conditions prescribed in the section is satisfied. -S.3 A. Government's Ministry of Corporate Affairs, Department of Revenue and Ministry or Finance accept electronic record.

By using digital/electronic signature information and data is made safe and authentic. If the document is digitally signed, it need not be signed again using ink. It is to be noted that today for authentication only digital signature is used. No other kind of electronic signature is provided by Government of India.

3) Digital signature is done by creating key pair. Public key and private key. Both are generated by Certifying Authority. He issues Digital Signature Certificate after this. Public key is in the possession of the Authority and private

key is with the subscriber. In certificate, the public key shall match with private key. The subscriber shall take care of his private key. If it is compromised, he shall inform the Authority.

Adv. Pavan Duggal raised certain practical questions about the protection by digital signature through key pairs. "Many subscribers do not have technical knowledge that how and when the private key is compromised. But he is held liable for the loss. Moreover, what if this private key is lost? Not only that what happens to those documents which are digitally signed? The IT Act is silent."[227]

4) For availing services, an application is to be made or form is to be filled. If any form, application or any other document is to be filed with any authority, office, body or instrumentality of government, it is allowed if it is filed in electronic form. Also, if issue of grant of any sanction, permit, licence or approval by particular manner, is done in electronic form by government then it is valid. If any receipt or payment of money is required to be done, it is valid if such receipt or payment of money is done by means of electronic form prescribed by Government.

Accordingly, government has issued Bhim App as e-payment gateway along with other payment Apps.

5. Delivery of services to public through electronic means are done through service providers. Government is obligated to appoint service provider to set up, maintain, and upgrade computerised service and such other services on which is specified by government for such delivery. Service providers may be all kinds of entities.

Services of private service providers-including mobile service providers can be used by government as per the provision. These service providers help to make efficient delivery of services to people. They have to follow the data protection provisions in law.

[227] Pavan, Duggal "Data Protection Law in India", (2016) Universal Law Publication.

6.Retention of electronic record or document is directly connected with the protection of data or information. Documents and records in physical forms are retained for subsequent reference generally. Where the law provides for the specific period of retention of documents or records in physical form and if such documents are preserved in electronic form, it satisfies the fulfilment of the provision as per IT Act.

But where law is silent about period for retention of documents in physical form, this provision does not apply. The document or information generated through electronic media generate lot of information automatically. So where the law provides for retention of records or information in electronic form this provision does not apply. Back up of the electronic information comes under the purview of this provision.

Secondly, it has to satisfy three conditions that i) such document, record or information shall remain accessible for subsequent reference, and ii) it must be in retained in the same form in which it is generated and iii) retained electronic record must contain the details for identification of origin, destination, date and time of dispatch or receipt of it.
This is important for the protection of information retained in physical form. But there are certain difficulties relating to filing of the forms, creation of electronic record, storage and accessing the information for reference and privacy of information contained in it.

When today's technology is developed and changed in more advanced devices for storing and accessing information, the information stored and retained in the old and less advanced devices, it is difficult to access the information. Eg. Earlier the information was stored on Compact Discs and now it is stored on pen drives. Now CD players are rarely in use.

- Moreover, as time passes, chances are high that the information stored may not be accessible because of corrupted CDs or Pen Drives or other devices on which the information is stored. Whether such record is considered as valid record?

- In recruiting procedure while filling the posts with government, applications are invited through electronic media which include personal information of candidates. Also before appointment candidate is chosen on the basis of clearance of his medical examination which is preferably done in hospital run by Government. All this data is gathered with the government. Such information may be misused, abused or criminally accessed by data predators. The information of the candidates who are not selected is also held by the government. There are no rules and regulations for the protection of such personal information with the government in this Act.
- Even though government mandate that a person required to file any document or form or application electronically, any person cannot insist the government department or ministry to accept any document in electronic form. It is not the right of the person. Now this is the negation of the provisions allowing the filing of the application, or form in electronic form under the Act.

7) Protection of privacy of information has many ways. One of them is encryption. Information Technology Act, 2000 provides for security of electronic medium and for promotion of e-governance and e-commerce an encryption modes and methods. Encryption is process where information is transformed using algorithm in such a way that nobody can read it except the person who possess the special knowledge. To make the encrypted information readable again the process of decryption is done. Department of Tele-communication, Ministry of Communication and Information Technology, Government of India specified 40 bit encryption.

But there is a discrepancy in legal provision and practice. Banks and other financial institutions are using 128 bit or 256 bit encryption. Social media site WhatsApp has end-to-end encryption of 256 bit. It was challenged before Supreme Court by filing PIL in 2016 on two grounds that this encryption is against the regulation by Government and that it prevents the compliance of S. 69 of IT Act i.e. power of central government for interception in certain cases. If the order is passed to decrypt the information, the company has to decrypt it. But it is cannot be complied due to high encryption bit. Ironically, WhatsApp

itself does not have decryption key to this high encryption. Supreme Court dismissed the plea with a direction to file the action in appropriate forum.

But the crucial issue of high encryption than prescribed limit by government of India was not decided. Neither the government has taken any action for it. In this situation it is possible that it can be misused against sovereignty, integrity and security of India.

With the initiation of the national programs like Unique Identification number, provision of services through ICT platforms and increased collection of citizen information by the Government, concerns have emerged on their impact on Privacy of persons. This information ranges from health, taxes, education, financial status, employment, disability, crime records etc.

But there are no rules and regulations for government departments for collecting, accessing and use of the information collected by departments. United States of America has enacted E-Government Act, 2002 to develop and promote the e-Government services but also prescribe the procedure to follow for the collection, storage, use of the information. Computer Matching and Privacy Protection Act, 1988 also limits the power of government by prescribing certain procedure to use the information by matching the information with other agency of government for taking decision about him.

India does not have such e-Government Act, or any Act to restrict or limit the powers of government. Lack of control system over the government regarding the access, use and dissemination of information may result into authoritarian government.

B] Government's power of interception, monitoring or decryption

The government has power to intercept, monitor or decrypt any communication between two persons in the situations mentioned under S. 69 of IT Act, 2000. The interception, monitoring or decryption is done for any information which is generated, transmitted, received or stored in any computer resource. The power to intercept is restricted by providing certain preconditions which are to be satisfied (a) interest of sovereignty and integrity of India, b) the security of state,

c) friendly relation with foreign state, d) public order, e) preventing incitement to the commission of any cognisable offence. The circumstances are equivalent to circumstances mentioned in Art. 19(2) of Constitution of India. The section is similar to S. 5(2) of the Telegraph Act, 1885. It also provides that any subscriber or intermediary or any person who is in charge of computer resource is bound to follow the direction for helping to intercept, monitor or decryption.

For interception, monitoring and decryption the central government has enacted the rules under S. 69 of the Information Technology Act, 2000. These rules empower the government for interception. Its objective is to get directions for interception, monitoring and decryption.

2] Body corporates or legal entity and individual

The second important part of the provisions are relating to body corporates under Information Technology Act, 2000. The interaction is done with body corporate and with another individual also. These interactions with body corporates result it gathering or collection of personal information with them. This collection generates more data which may be processed by these body corporates. This processing may harm the informational, decisional or physical privacy of an individual. The Information Technology Act, 2000 provides for protection of the personal information collected and processed by body corporates.

The main objective for legislation pertaining to electronic media is for the provision of adequate protection to privacy, confidentiality and security of person and personal information or data on electronic media. The law which provides the reasonable security practices and procedures which need to be adopted by body corporates, or any legal entity that is dealing, handling, processing of data and information in electronic form. This protection is available against two types of actions,

i) By unauthorised actions of an individual, there is a damage to the information in the computer, computer system or computer network and

ii) If there is failure to protect personal data by any body corporate.

These provisions for protection are discussed below:

a) Compensation for Damage to computer, computer system and computer network:

The redress against the first action is provided under S. 43 of IT Act, 2000. It deals with the penalty and compensation in situations when any person, without any authority, handles the operations of computer which may result in damage to computer, computer system and computer network. It is important to note that protection is given for the information or data held or stored in such computer, computer system and computer network including removable storage medium. The actions covered under this provision are access, downloads, copies or extraction of data, introduction of contaminant or computer virus, damaging of data, causes disruption of computer, help any other person to access, destroys, delete or alters any information which diminishes its utility or value after that, steal, conceal, destroy any computer source code with intention to cause damage.[228]

S.43 provides for the damages by way of compensation in ten separate and distinct conditions. Access or damage to computer may be physical or by internet. Both are included. Any type of 'information' and 'data', which is defined under the Act are included. The damage may be caused even if the action is done without intention. Under the Act, damages by way of compensation are provided for each action. The damages are provided to compensate the person who has suffered the loss because of unauthorised action of other. It is a civil liability.

Some important points about this provision are:

1. Actions shall be without permission from the owner or person in charge of the computer. The action must be such that if permission is not given or sought, action is illegal.
2. These actions for damage shall be such which destroy the utility or value of data or information stored in it. It includes tampering or manipulating.

[228] Information Technology Act, 2000. S. 43

3. This damage shall result into disruption of normal function of computer.
4. The protection is given to damage by stealing or concealing to computer source codes-i.e. computer commands and design. In layman's language it is known as list of instructions on which computer works.
5. In contaminant, any instruction or information or program t
6. That damage the normal working of computer and computer viruses, worm, Trojan horse, denial of service (DoS) attack is also included.
7. The person who assist to make the unauthorised access easy is also liable. Any act or omission relating to such unauthorised access, both are included.

   The Act provides for the action which diminishes the value of the information. Now it is not clear how value of information can be proved. Information itself is invaluable. There are no standards or parameters for measuring diminishing value of information in the Act. 'Concealing' of source code is also not defined in the Act.

a) Compensation for failure to protect data:

   After share of India has increased in the Business Processing Outsourcing industry, the processing the data of outside country was on progressive path. Due to which various challenges regarding privacy and security of information have emerged. Therefore, the need for protection of data or information has increased. Information Technology Act, 2000 have responded with the provision in the Act under S. 43A.

   Today any organisation or entity which is handling any activity becomes the data collectors-repository- after some time. Different types of information or data-personal and sensitive personal data are gathered or collected in computer systems of such entities. S. 43 A imposes corporate liability for protection of data.

   The section applies to any body corporate which is dealing, possessing or handling any sensitive personal data or information in its computer resource, if negligent in implementing and maintaining reasonable security practices and

procedures which cause wrongful loss or wrongful gain to any person, is liable to pay damages by way of compensation to the affected person[229].

Under this section a body corporate which is negligent in implementing and maintaining reasonable security practices and procedure which are designed to protect the security challenges mentioned in the explanation is liable. It is not all-inclusive engulfing privacy provision. Damage to sensitive personal information due to negligence is one of the many ways for compromise of the data. It may be observed that protection of privacy of information or data against other threats is not provided in this section.

It is pertinent to note that the negligent action of the body corporate must cause the wrongful gain or wrongful loss to any person. The terms 'wrongful loss' or 'wrongful gain' are not defined in this Act. Definitions of both the terms are provided in Indian Penal Code and are to be interpreted as the same.

In the explanation to this section, three terms are explained. i) Any association or group engaged in commercial professional activities such as firm, sole proprietorship, and company is specified as 'body corporate'. This is broad definition. But government departments cannot be specified in body corporate as they are not engaged in commercial activities. So, provision is silent about government responsibility in dealing with data even though it is delivering services in e-governance.

ii) 'Reasonable security practices and procedures' means any security practices and procedures designed to protect the information from unauthorised access, damage, use, modification, disclosure or impairment provided in agreement between the parties or in absence of them 'as prescribed by Central Government after consulting professional bodies'.

In the system where awareness to the protection of personal information is minimal, it is very possible that any type of security procedures and practices

[229] Information Technology Act, 2000. S.43 A

may be availed by parties. How and who will decide whether they are reasonable. It is also possible that the standard provided by other countries is different from the security practice accepted by Indian party. If they do not agree on some standard rules in agreement, ultimately the responsibility is placed on central government to decide them, and government had prescribed the one in Privacy Rules, 2011(discussed below) and not in the Act.

iii) 'Sensitive personal data or information' is the same which is prescribed by Central Government. But Central government had not provided any definition or parameters to decide the 'sensitive personal information in the Act. (They are in Privacy Rules, 2011, discussed below)

After the implementation of the amended Act, it was observed that the difficulties regarding protection of privacy of personal information and protection of the same were not eased or solved. The Central Government has enacted security rules known as Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules in 2011.

C] Responsibility of an Intermediary: A definition of 'Intermediary' provides "a person, with respect to any particular electronic records, means who on behalf of another person receives, stores or transmits that record or provides any service with respect to the record and includes telecom service providers, network service providers, internet service providers, webhosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes".[230]

Under S. 79 of IT act, 2000, various kinds of service providers are covered within the ambit of definition of the term. Any service provider of any nature, even direct or indirect, which is provided on a computer or using computer network is covered. While using the electronic system, apart from connecting to internet, number of services are provided by various service providers and also

[230] Information Technology Act, 2000, S.2 (1) (w),

by content service providers. By receiving these services, individual can use the communication devices very effectively. Social media sites are also included as service provider which facilitate access and communication.

Under the Act, intermediaries are exempted from liability for third party data or information, data or communication link made available or hosted by them except in certain situations explained under S. 79 (2) & (3) of the Act. The term third party information has been defined in Explanation to the section. It provides - any information dealt with by an intermediary in his capacity as an intermediary[231]. An 'information' and 'data' is defined in the IT Act.

Under S. 79 (2) it is obligatory for the intermediary to ensure that its function is limited to providing access to electronic systems and communication system for making the information available which is transmitted by third party. The liability of intermediary is nil if he has no control over third party transmitted data. He is not liable if he does not have any participation in initiating the transmission, or selecting the receiver of the transmission, or he has not selected or modify the information. It is expected that the intermediary must observe due diligence while discharging his duties.

Only liability is placed on intermediary under the Act that if the intermediary assisted or abated or conspire in commission of illegal act, he is liable under S. 79 (3). He should also notify the commission of illegal act as and when he comes to know about it. He should expeditiously remove such matter from the link. Under this provision the period specified by central government is within 36 hours of complaint made by an aggrieved person.

One of the significant parameter of S. 79 is that the intermediary has to mandatorily observe due diligence while discharging his duties. But 'Diligence' is nowhere defined in the Act but it describes a general duty to exercise care in any transaction which may be subjective.

[231] Information Technology Act, 2000, Explanation S.79.

S 79 excludes intermediaries from liabilities such as those which only provide access to a communication system and do not initiate transmission or select a receiver or alter information being transmitted. This is particularly beneficial broadband service providers or blog hosting companies and social networking sites. They escape liability for objectionable third-party content uploaded as they do not in their internal function control or monitor third party content. So, it cannot be assumed that they had actual knowledge or intention of such objectionable content unless actual notice of objectionable content is served on the intermediary by the affected party.

D] **Other:** Information technology is beneficial to individual in countless way. But it has given an opportunity to predators for commission of crime. Because of these growing instances of crimes, law has criminalised many actions as cyber-crimes.

1) The S. 66 criminalise the act which is done under S. 43 with dishonest or fraudulent intention, and provides that the person is punishable with imprisonment or fine as prescribed. Under S. 43, act has civil liability but same act, if committed with 'dishonest or fraudulent intention', it attracts liability under this section. Earlier it prohibited 'hacking' but now it is enlarged in scope providing any act under S.43. Dishonest or fraudulent intention is defined under Indian Penal code. It is to be noted that in this provision not only actus resus but mens rea or destructive intent is included.

2) Sending offensive messages through communication devices is covered under S.66A, which is declared unconstitutional be Supreme Court as it obstructs the fundamental right to freedom of speech and expression under Art. 19 (1) (a). Now there is no protection available against harassment by sending offensive messages through communication under Information Technology Act, 2000.

3) Crime for identity theft is covered under S. 66C. Use of electronic signature, password or any other unique identification feature of another with fraudulent or dishonest intention is punishable. Forgery of electronic signature may be used

to harm the data privacy of person or tampering with password, which is also compromise the data or information privacy.

4) Electronic voyeurism which is associated with physical privacy is provided in S. 66E. It prohibit the publishing or transmitting electronically the captured image of private parts of any person without the consent of him. The capturing, publishing or transmitting the images of private parts shall be punishable where the person has reasonable expectation of privacy.

5) The provision for protection against cyber terrorism is provided under S. 66F. It includes introducing or causing to introduce any computer contaminant, which affect the data or information quality and therefore damage information privacy relating to sovereignty, integrity and security of India. Introducing contaminant is also imposes civil liability under S. 43 and criminal liability under S. 43A to harm the individual. But under this section if the contaminant is introduced to harm the national security he is punishable.

6) Publishing obscene material is punishable. Putting information which is lascivious or of prurient nature using electronic media is punishable. What is 'lascivious' or of" prurient' is not defined. The standard is provided as 'which have tendency to deprave and corrupt those, whose minds are open to such immoral offences.' But it is very subjective term. The government has power to block the website which publishes such material online under S. 69A

7) Under S. 72, the person who is authorised to have information under the provisions of this Act and Rules and Regulations under it, due to access to any electronic record, have the information, he is bound to keep the information secret. He shall not disclose it without the consent of the person.

While using information technology, an intermediary has an important part to play as he facilitates the user to access internet. In this process, the intermediary not only facilitate to access but publish and store the published information with him. In a way he handles the personal information or data. The Information

Technology Act, 2000 provides for the protection of information facilitated by intermediary.

Issue of controlling or regulating the third-party content posted on social networking sites comes up again and again. But due to magnitude of content posted or information uploaded on such sites, it is very difficult to control them from technical and administrative point of view. But to regulate the conduct of intermediaries of all types, the Central government has enacted the guidelines for intermediaries.

4.5.3.2 Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009.

Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 were passed to provide control. It provides the procedure to conduct interception. But privacy of the persons is thought of as it is provided that such interception requires prior approval from the competent authority i.e. Secretary in Ministry of Home Affairs, in case of Central Government and Secretary in charge of Home department in case of State Government. In the cases of emergency different procedure is to be followed. The purpose for interception must be the same which is specified in S. 69(1) of Information Technology Act, 2000, i.e. for protection of sovereignty and integrity of India. It is mandatory to record reasons for Interception. Interception is permitted for the period of 60 days and on renewal not to exceed 180 days.

Intercepted communications shall be kept confidential not only by intermediaries but their employees. Rule 25 prohibits its disclosure except to the officer of authorised agency who can use such information only for specified uses pursuant to direction of competent authority[232]. Rule 23 prescribes that unless the intercepted information is required by law, it should be destroyed after six months.

[232] IT (Procedure and Safeguard interception, Monitoring and Decryption of Information) Rules, 2009, Rule, 25

The power of interception is regulated with the provision that competent authority shall first verify whether there are alternative means to acquire the information. If it is observed that such alternative mean or method is not available then and then only the direction for interception, monitoring or decryption is issued. Government's power to intercept or monitor or decrypt without finding other means to get information is checked and regulated by this and interests of individuals are protected.

After interception, monitoring and decryption, the data is collected and used by the government. There are two actions, one is interception, monitoring and decryption of information and other is monitoring and collection of traffic data or information. For collection of traffic data, interception is essential. For these two actions different legislations are enacted.

4.5.3.3 Information Technology (Procedure and Safeguard for Monitoring and Collecting Traffic Data or Information) Rules, 2009

What is 'Traffic Data'? It is defined in explanation ii) of S. 69B IT Act, 2000. It is defined in simple language as, "any data identifying or purporting to identify any person, computer system, or computer network or location to or from which the communication is or may be transmitted and includes communication's origin, destination, route, time, date, size, duration or type of underlying service or any other information." From the definition itself it is clear that by monitoring or collecting data, the personal information of any individual, his whereabouts can be gathered. Monitoring and collection of traffic data of the communication continuously requires interception of the computer, computer system or computer network. So, for monitoring and collecting the traffic data, rules regarding interception, monitoring and decryption can also be applied.

This monitoring is for the purpose of identifying any person, computer system and computer network or for identifying the location of communication. By collecting traffic data by interception, identity of person, location and origin of communication, its destination, route by which it reaches, date, time and duration of communication, size of communication i.e. KB or MB etc. can be known.

Objective of the monitoring and collection is for enhancing cyber security. It is done for forecasting eminent cyber incidents, identifying and determination of viruses or computer contaminant, tracking cyber security breaches and computer resource breaching cyber security, identifying the person who has breached or conducting forensic investigation.[233]

Prior permission of Secretary, Dept. of Information Technology is mandatory to conduct monitoring or collection of traffic data for cyber security reasons, inter alia, forecasting of imminent cyber incidents, tracking of persons and computer resource breaching cyber security. To eradicate the chances of arbitrary decisions for monitoring and collection of traffic data, it is mandated that these decisions are ought to be reasoned decisions and shall be reviewed by Review committee within seven working days.

Intermediaries are responsible for themselves and behaviour of their employees for unauthorised monitoring and maintenance of secrecy of information collected. To prevent the misuse of such information the check is provided. Except when it is still required for law enforcement purposes, the collected information shall be destroyed after nine months of collection. Rules prohibits monitoring and collection of traffic data without authorisation[234] Disclosure of such information is not allowed unless it is required for forecasting imminent threats of cyber security, general analysis of web traffic and cyber incidents or for investigation or in judicial proceedings.

4.5.3.4 Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.

To facilitate the implementation of the provisions for protection of privacy of sensitive personal information or data in IT Act, 2000, the Central Government in 2011 has enacted Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (hereafter Privacy Rules, 2011). If these rules are observed, the privacy

[233] IT(Procedure and safeguard for monitoring and collecting Traffic Data or Information)Rules, 2009 Rule 3 (2)
[234] IT(Procedure and safeguard for monitoring and collecting Traffic Data or Information)Rules, 2009 Rule 9,

principles in Directive 95/46/EC by European Union are mirrored in them. Purpose limitation principle of the Directive is reflected in Rule 5(2). Data quality principle is followed in Rule 5 (6), Data security principle is provided in Rule 5 (8), Special protection for the sensitive personal data is being enforced in Rule 3, the Transparency principle is provided under Rule 5(9). Data transfer rule is guarded under Rule 7. These rules are discussed in following paragraphs.

1)But to begin with as the privacy protection is applicable to Sensitive Personal Data, the parameters provided to know the term are to be discussed. It includes personal information related to important things as password- including his user name, secret question relating to password is also included as it is information related to personal information. His financial details, credit or debit card includes payment instructions regarding any financial transaction about bank account is also included. His physical, psychological or mental condition of person is provided. His sexual inclination that if he belongs to LGBTQ community is protected. Information relating to his medical records is provided. It can be felt that it is repeated as information relating to physical and mental status is already provided but medical reports include much more than information relating to physical or mental records. Information relating to biometric data like his iris scan, retina, thumb or finger impressions are included. But information relating to genetic information is not included and the Privacy Rules, 2011 are silent about it.

If any information in detail regarding above parameters is provided to any body corporate to receive service from them is also included. Also all information satisfying the parameters provided in the Rule, which is given to the body corporate for processing, storing and handling under any lawful contract or otherwise, would qualify as sensitive personal information according to the Privacy Rules, 2011. But information available or accessible in public domain or furnished for fulfilment of Right to Information, 2005 and under any other law in force is out of the purview of ‘sensitive personal information’. In this regard, it can be said that information available on social media like Facebook or Google is in public domain and it is not ‘sensitive’ personal information.

2) Under Rule 4, it is mandatory for body corporate to have privacy policy for handling or dealing in personal information including sensitive personal information. The body corporate is obligated to inform every person who submits his personal information under lawful contract to it for processing. This privacy policy shall be published on the website of this body corporate explaining the purpose and usage of personal data and security practices and procedures adopted by it. By this provision, transparency in collection and handling of information is ensured.

3) Fair collection principle is provided in Rule 5. Consent is mandatory for collection. Without obtaining written consent before collection, sensitive personal information shall not be collected. Collection of sensitive personal information shall be done for the lawful purpose and collection which is 'necessary'.

The consent may be called 'simple consent' after informing the purported use of collected information. But it cannot be termed as 'informed consent' in which the probable security glitches are informed. All possibilities are to be explained to the person who is submitting his sensitive personal information. The Rules are not providing about 'Informed consent'.

4) Data quality principle is followed as body corporate is obligated to give access and review of the sensitive personal information to the provider of information on their request and has to correct or amend if found inaccurate.

5) Data security is provided as body corporate is obligated to keep the information secure by following security procedures and practices provided under the Rule 8.

6) Rule against disclosure provides that disclosure of sensitive personal information can be disclosed only on receiving consent, except if it is disclosed under contract or to fulfil the order of the court.

7) Transparency is provided as body corporate is obligated to appoint to redress the grievances of their providers, a Grievance Officer and publish the name and contact details of him on the website.

8) Transfer of data to outside country for processing is allowed if such country is providing the same level of data protection and that only for the fulfilment of contract. This provision is equivalent to the protection given by EU for transfer of data to outside country. To decide the equivalency of protection of such transferee country, the decision is given by European Commission. But in India, the standard is agreed by the parties at the time of contract.

9) These rules require the body corporate to adopt and implement reasonable security practices and standards including comprehensive information security policy which contain "managerial, technical, operational, and physical security control measures that are commensurate with the information assets being protected with nature of business."[235] It is clearly provided that in case of security breach of information, the burden and onus of proof is on the body corporate.

If no security standard is agreed by the parties, the Central Government has provided the international standard for protection IS/ISO/IEC 27001 which is to be implemented by body corporate. Before enactment of these rules, it was a practice of the parties to mutually adopt security rules prescribing standard under the law of other countries in their agreement. After the enactment of these rules, if parties decide in agreement to follow standard prescribed under any law of the country outside India, it is permitted.

4.5.3.5 Information Technology (Intermediaries Guidelines) Rules, 2011.

These rules provide standard of diligence to be observed by intermediary while discharging his duties. Rule 3 (1) of these Rules provides publication of rules and regulations, privacy policy and user agreement for access or usage of his computer resource by intermediary.[236]' Various kinds of data, content is barred, and under R. 3 (2) intermediary has to inform its users that they should not host, display, upload, modify, publish, transmit, update or share any such information

[235] Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Rule 8(1)
[236] Information Technology (Intermediary Guidelines) Rules, 2011, Rule 3(1)

that is grossly harmful, harassing, blasphemous, defamatory, obscene, pornographic, paedophilic, libellous, invasive of another's privacy, hateful, or racially, ethnically objectionable, disparaging, relating, or encouraging money laundering or gambling, or otherwise unlawful in any manner whatever.

It is difficult to decide the proper meaning of the terms provided in Rule 3 (2) (b) of Intermediary Guide line) Rules, 2011. Application of these terms may curtail the freedom of speech and expression. Any comment or expression of thought may be covered by "grossly offensive or menacing" because of ambiguity in explaining the term. Also terms like 'breaching other's privacy, 'hateful', 'harmful', 'harassing' 'blasphemous' are not objectively defined and capable of subjective interpretation.

Under Rule 3(2) the intermediary shall inform the user that the formation which "(c) harm the minors, (d)which infringes patent or copyright etc, (e) violates any law, (f) deceive or misleads the addressee about the origin of such messages or communicate any information which is grossly offensive or menacing in nature,(g) impersonate any person, (h) information containing virus or computer code which designed to interrupt, destroy, or limit functionality of computer, (i) threats unity, integrity, defence, security or sovereignty of India, friendly relations with foreign states, or public order or causes incitement to the commission of any cognisable offence or prevents investigation of any offence or is insulting any other nation shall not be posted by user of the computer resource through intermediary"[237].

It specifically provides that intermediary shall not be part of the various illegal activities relating to the aforesaid banned content or information. The intermediary is obligated not to host or publish knowingly any information provided under Rule 3 (2)[238]. Proviso to Rule 3 (3) exempt from the ambit of hosting or publishing of information by an intermediary, which information is automatically stored within the computer resource as an intrinsic feature of such computer resource or there is no human editorial control from ambit of

[237] IT (Intermediary Guidelines) Rules, 2011, Rule 3(2)
[238] IT (Intermediary Guidelines) Rules, 2011, Rule 3(3)

information, such content is excluded even it is hosted or published by intermediary.[239] By this provision, the social media sites, which are also intermediaries are excluded from liability.

The provisions of these guidelines are lacking in certain areas:

1)Cloud computing is widely used by organisations. Cloud computing means delivery of different services through internet tools and applications like data storage, servers, data bases and networking and software[240]. This means that the users which includes corporations, companies, non-profit organisations, and government, do not need to set up infrastructure themselves. The cloud computing service companies, it may be government or third parties, set up infrastructure and provide services by accessing internet to the users. The data of the users is stored or processed by the cloud service providers.

But when the data is transferred to cloud for storage or processing, the privacy, security and confidentiality of the data or information may be compromised. But this vulnerability is not thought of by the information Technology Act, 2000. S.79 of IT Act, 2000. It provides for the responsibility of internet service providers and does not provide for responsibility of the cloud service providers specifically. Today they are providing services to organisations and facilitate the commercial or non-commercial transactions.

It is to be noted that in power to intercept, monitor and decryption, the power is generally can be used for single communication also. But for monitoring and collection of traffic data, interception, monitoring is to be done for more than one communication.

Though this power is essential for protection of country against any threat by using surveillance, it harms the privacy and security of individual. It is well explained by Daniel J. Solove [241] Accessing the information by interception and monitoring, results into collection by surveillance and interrogation. After

[239] IT (Intermediary Guidelines) Rules, 2011, Proviso to Rule 3 (3)

[240] https://aws.amazon.com/what-is-cloud-computing/? (Last visited on March 28, 2020)

[241] Daniel, Solove J, "A Taxonomy of Privacy", 154 U. PA L.REV. 477, 482-483 (2006)
(He approached 'privacy' by 'harms' resulted because of its b reach. In his taxonomy, he categorised as a) information collection, b) information processing, c) information dissemination, d) invasion.

collection, such information is processed to get useful information for the probable cause or its secondary use. This processed information is disseminated which may result into breach of confidentiality, disclosure, exposure, increased accessibility, appropriation and distortion of information. All these result into invasion of privacy. India has long judicial history for grievance against unwanted state intrusion and Indian Supreme Court invoked tort of privacy under Art. 21, Right to life and liberty of Constitution of India to protect the privacy.

The internet has defied the long- standing infrastructure of the print industry and cable world. The internet is always in struggle with the legal principles. The openness and unboundness of internet are tried to be regulated by law. Because of fast advancing technology, law relating to internet becomes redundant very fast. It gives opportunity to agile minds of criminals. Information Technology Act, 2000 provides for the protection for personal privacy by using communication technology with intention to harm an individual. These acts may harm the privacy of information regarding him.

In the age of internet, the personal information relating to financial status is considered as sensitive personal data. This information is governed by the rules enacted in Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011. In the rules the information relating to bank accounts is protected, but when the person wants to seek loan from the financial institutions, his credit record matters for it. His creditworthiness is checked by the institutions. To maintain privacy and security of this sensitive personal information government has enacted a legislation.

4.5.4 Credit Information Company (Regulation) Act, 2005

The legislation is to protect the financial institutions. The objectives are to make efficient credit decisions, to discourage habitual defaulters, to reduce selection of defaulting customers with freely available information, past and current history, for better judgement of customer risk and probability of default etc.

These companies are governed by the rules framed by Reserve Bank of India in this regard. They are to be registered with Reserve Bank of India. Members of these Credit Information Companies are credit institutions which include banks, credit information companies and other specified users. The Credit Information Company shall gather information about the consumer in the format specified by RBI. The credit information includes amounts and nature of loans or advances, nature of security taken, guarantee furnishing, credit worthiness etc.

In case information relating to the credit history of a card holder is to be provided to a Credit Information Company, the card issuer ought to clearly bring this fact before the customer. Under this Act, every Credit Information Company which are in possession or control of credit information shall take steps as prescribed to ensure that data relating to credit information maintained by them is accurate, complete, duly protected against any loss or unauthorised access or use or unauthorised disclosure.[242] It shall adopt privacy principles in relation to collection, processing, recording, preservation, secrecy, sharing and usage of credit information under this Act.[243] By enacting this law the government tried to protect the credit information report of an individual secure.

4.5.5 Privacy Bills

After the EU Directive in 1995, the law relating to data privacy was much stronger in countries outside India. But in India, lone privacy legislation in the form of Information Technology Act, 2000 and Rules enacted under it was trying to provide protection.

The Information Technology Act, 2000 was a lone act covering protection for e-commerce transactions, facilitating e-governance and providing privacy of person. The main function of legislation pertaining to electronic communication that is protection of personal information or data is not provided substantially. As threats on privacy, confidentiality and security of personal information or data are increased and resulted in loss to concerned individuals, the demand for

[242] Credit Information Company (Regulation) act, 2005, S. 19,
[243] Credit Information Company (Regulation) act, 2005, S. 20

privacy and data protection law gained force. The demand for enactment of such legislation was increasing, the Government had drafted two bills which were proposing the Right to Privacy and data protection. But they were not finalised and enacted in law. The unsuccessful and aborted legislative attempts in this regard are discussed hereunder.

4.5.5.1 Right to Privacy Bill- 2011[244]

It was the first attempt from the government to prepare any legislation for protection of privacy of persons when the draft of the Privacy Bill 2011 was made. Even though it is termed as Right to Privacy Bill, its main focus was on protection of privacy of information or data. The overview of the Act is discussed in following paragraphs.

Applicability

These provisions are applicable to data controller who has a place of business in India, but if he does not have such place, he has to nominate a person as representative. A statutory right to privacy was created by this proposed bill. Applicability of provisions of this bill was limited only to citizens of India and predominance of this law was provided in the Bill. But many laws were exempted from the applicability of this Act. e.g. Right to Information Act, 2005 or Prevention of Corruption Act etc. It included provisions about protection of personal data as it was provided in privacy principles under European Union regarding the issues like collection with consent, processing, maintaining quality of data etc. of personal data. Processing shall be done by following all privacy principles like fairness and relating to the purpose for which it is collected.

For protection of health data privacy, provisions relating to sensitive personal data mention various parameters. Inclusion of genetic data and results of narco/ polygraph test data was made which was very bold step. But definition did not provide for religious, political belief in it. Retention of personal data shall be done till the purpose for which it is collected is not served except in certain

[244] https://cis-india-org/internet-governance/draft-bill-on-right-to-privacy (Last visited on September 9, 2019)

circumstances like for research purpose it can be retained longer. Sharing (disclosure) of personal data can be done after obtaining consent of data subject.

For Security of sensitive personal data, it was provided that appropriate security measures shall be adopted by the data controller. Notification of breach of security shall be given by data controller to data subject and Authority.

Rights of Data Subjects

Rights of the data subjects were provided and protected in the following way. He shall be provided access to his personal data on his request. Data subject can seek updation of personal data if there is any inaccuracy or change in it. It had provided for mandatory processing of data under certain circumstances like if data subject is bound to do it under any law. Same principles for protection of data subjects are provided as EU Directive but inadequate as right to erasure of the data was not provided.

Trans Border Flow of Personal Data

Trans-border flow of personal data is only permitted if recipient follow the law and code of conduct similar to this law, and if consent is provided or for performance of contract by data subject. Data controller was obligated for complying protection and security of data transferred outside India. It is same as provided under European Union data protection principle. But whether the country is following same code of conduct or not, the guidelines to that effect or deciding authority was not provided. In European Union the European Council decides the equivalency of protection.

Surveillance means covert[245] surveillance, using individual or device and use of CCTV or other image capturing devices. For the first time, rules limiting the powers for surveillance with some enabling provisions were provided for protection of personal data. It is not permitted unless authorised by law and only in national or public interest. All the rules regarding the storage, retention, processing etc of personal data are applicable to data obtained by surveillance.

[245] 'without knowledge of person' www.tremark.co.uk (Last visited on September 9, 2019)

Powers of Government

The government's power of interception includes telephone tapping. Provisions were made against interception for ensuring information privacy. The modification was with respect to several procedural safeguards which were put into place to avoid unauthorised and unnecessary tap orders.

But whether this provision was qualifying and specifying the necessary rules for protection of privacy against the power vested in to government under s. 69 of Information Technology Act, 2000 was not specified. Because government is empowered for interception under this section. And provision in this Bill bars the government to intercept except authorised by law. Also, it provides some additional rules if such interception is regarding communication regarding to religious, medical, journalistic or privileged communication. A provision is made that intercepted communication may not be used as evidence in court.

Privacy Safeguards

The Privacy Bill, 2011 also prescribed various safeguards for the other forms of privacy. Some exceptions are provided for breach of privacy like for journalistic purpose, processing data for personal or household purposes, installation of surveillance equipment for the security of private premises, disclosure of information via the Right to Information Act 2005, and any other activity exempted under the Act. The novel provision regarding direct marketing was there. Nobody shall use personal data for direct marketing unless the person is registered with National Data Registry. A person has choice to opt out of such data marketing after making request.

Exemptions from restrictions on processing were provided including new grounds that if it is to be done for assessment of tax and other duty. This ground is different than EU data protection directive. Purpose may be for tightening the tax net.

Regulatory Framework

A regulatory mechanism was created by providing the Data Protection Authority of India, and Cyber Appellate Tribunal. Also a new regulatory authority is created by providing National Data Controller Registry. Purpose for its establishment is to facilitate the data controllers to make entries and create national digital data base. These authorities were going to supervise the collection and storage of personal data by private parties. Disputes under the Bill will be referred to the Cyber Appellate Tribunal which has been set up under the Information Technology Act, 2000. These disputes are primarily in the nature of claims by individuals against private data controllers[246].

Remedies

Different remedies were provided under the bill as a) Compensation-Any person who suffers damage can claim for compensation any damage caused to him by any data controller. [247]b) Civil Remedies- The individual, whose right to privacy has been adversely affected, may bring a civil action against such persons have caused such violation. This is addition to any criminal proceedings existing against such person (violator). c) Offences- where Court may take cognizance of offence under this Bill, solely on the compliant made by the Authority.

This Bill had many shortcomings but it was the first attempt in India to provide protection to personal data. The provisions mirrored the provisions of European Union Directive for major part, but some new provisions were also provided like surveillance and interception. After the attempt to make the law failed, the demand for privacy legislation was increasing as adverse repercussions of advancing technology was felt by the stake holders. The government had appointed Group of Expert Committee in the chairmanship of Justice A. P. Shah to identify key privacy issues and to facilitate to enact the Privacy Bill on the backdrop of international privacy laws, and privacy issues in the era of technological advancement. The Committee had submitted the draft of suggestions and accordingly the draft Bill was drafted.

[246] Right to Privacy Bill, 2011 S.50
[247] Right to Privacy Bill, 2011 S. 51-56 , S.58-61

4.5.5.2 Right to Privacy Bill, 2014

Another bill was drafted by Department of Personal and Training, Government of India, in 2014. But this Bill was not presented in the Parliament. Before presentation it was leaked. Government accepted that it is drafting the bill. The provisions contained in the leaked Bill was compared with Privacy Bill, 2011 and published on website of an organisation Centre for Internet and Society.[248]

Applicability

The 2014 Bill extends the right to Privacy to all residents of India and not only citizens which were protected under 2011 Bill. The 2014 Bill furthermore recognizes the Right to Privacy as a part of Article 21 of the Indian Constitution.

Many new terms were included in this Bill which were not provided in earlier Bill, 2011, e.g. personal identifier, control, telecommunication system etc. Telecommunication system included any system used for transmission or reception of any communication by wire, radio, visual or other electromagnetic means. Parameters in these definitions were drafted after considering the technological development while using communication devises. Most of the definitions were retained in the Bill but some were redefined by broadening their scope.

Many terms were more inclusive of other parameters for the act. E.g. sensitive personal data includes criminal convictions. Directed surveillance, intrusive surveillance and covert human surveillance all are included in the term 'Covert Surveillance'. In 2011 Bill only covert surveillance was provided. Exceptions for Right to Privacy were same as reasonable restrictions under Art. 19 (2) of constitution of India, which were also provided in earlier Bill of 2011.

Rules for processing sensitive personal data by following health information privacy, are same as with authorisation and as they were under 2011 Bill. But exemption from authorisation under certain circumstances under which

[248] https://cis-india-org/internet-governance/blog/leaked-privacy-bill-2014 (Last visited on September 9, 2019)

authorization is not required for sensitive personal data are provided. Authority may add additional safeguard.

Data Privacy Principle

2014 Bill followed collection of data privacy principle. It had covered that for collection of personal data, purpose for which the data is collected shall be declared by notice. If the purpose for which the data is collected is changed, notice is required. Without the consent of data subject the information of data subject shall not be disclosed except in certain situations. Interception of the communication is allowed with some safeguards. In the power of interception, e-mail of the employee was not protected and therefore no privacy principles like notice, consent etc. are applicable.

Cross -Border transfer of Personal Data

Equivalency or higher standard of data protection is required for cross border transfer of personal data. But law enforcement and intelligence agencies are exempted from this. They can transfer personal data for reasons of national security, or sovereignty, integrity. This exception was not provided in the Bill of 2011.

Mandatory processing of personal data is allowed if data subject must disclose such data under provisions of law. Under this Bill National Data Controller Registry is removed. Instead of it privacy officers shall be appointed by data controllers for supervising the security of personal data. An Authority has power to exempt or waive from applicability of some provisions.

Bill provides the installation and use of video recording equipment in public places. It allows the use of CCTV but prevents the use of recording equipment and CCTVs for the purpose of identifying an individual, monitoring his personal particulars, or revealing personal, or otherwise adversely affecting his right to privacy. It requires that the use of recording equipment must be in accordance with procedures, for a legitimate purpose, and proportionate to the objective for which the equipment was installed.

Data Protection Authority

In the Bill, Data Protection Authority was created. Power to waive the applicability of the Act with broadened power to receive, investigate complaints about alleged violations of privacy and issue appropriate orders or directions was given. But intelligence agencies cannot be restricted if they use this power in national interest. This power is instead vested with a court of competent jurisdiction.

Redressal Mechanism

For dispute redressal, Privacy officer appointed by data controller or the industry level Ombudsman obligated to address the disputes. If individuals are not satisfied with the decision of the Ombudsman, complaint to the Authority is made. If an individual is aggrieved with the decision of the Authority, or by a privacy officer or ombudsman through the Alternative Dispute Resolution mechanism, or by the adjudicating officer of the Authority, they may approach the Appellate Tribunal. Any order from the Appellate Tribunal can be appealed at a high court.

Bill provides for self- regulation mechanism where industry associations will develop privacy standards and adhere to them. For this purpose, an industry ombudsman should be appointed. The standards must be in conformity with the National Privacy Principles and the provisions of the Privacy Bill. If an industry association has not developed privacy standards, the Authority may frame regulations for a specific sector.

Offences and Penalties

It had provided for offences and penalties. Offences include unauthorized interception of communications, disclosure of intercepted communications, undertaking unauthorized Covert Surveillance, and unauthorized use of disclosure of communication data. It is punishable with imprisonment and fine.

It provides a list of penalties like penalty for obtaining personal data on false pretext, for violation of conditions of license pertaining to maintenance of secrecy and confidentiality by telecommunications service providers, for

disclosure of other personal information, for contravention of directions of the Authority, for data theft, for unauthorised collection, processing, and disclosure of personal data, for unauthorized use of personal data for direction marketing.

Status of the Bill

This Bill was not put before the Parliament and discussed. In both these privacy bills, the informational privacy was provided for. The provisions covering the personal data or information were given importance.

After the enactment of the Bill in 2014, no attempt was made by Indian government for enactment of legislation for protection of privacy and personal data. The society working in the field of internet and information technology has suggested the draft for a bill for protection of personal data in 2013.

4.5.5.3 The Personal Data (Protection) Bill-2013[249]

With increasing use of information and communication technology in day to day life, the personal data breach and invasion on the personal information had increased. The data breach was not only by intermediaries or commercial organisations, but by the government also. To eradicate the misuse of personal data collected by the data collectors, the draft was proposed for the Personal Data (Protection) Bill by Centre for Internet and Society.

Applicability

The applicability of the Bill was for the data which related to natural person directly or directly to identity him. The definition of sensitive personal data include new criteria of biometric data, DNA data which was not provided earlier with detailed definitions. Data collection privacy principles with purpose specification were provided like with consent, purpose, fairness, lawfulness, security practices etc. The data subject has right to withdrew his consent and his data is be destroyed by the controller. These provisions match with the EU Directive.

[249] Available at https://www.cis-india-org/ (Last visited on October 11, 2019)

Collection without consent is permitted if it is for medical assistance to data subject, for establishing identity of subject and collection is authorised by law, for prevention to national security, for prosecution, investigation of cognisable offence. Again these provisions are also following the EU Directive.

The Bill has suggested storage limitation principle as such collected data cannot be stored in excess of the period necessary to store the data for processing.

Trans-border transfer of data was provided if different manner than EU Directive. It had provided for taking strong measures for protection and not the country having equally strong data protection legislation. The responsibility was on the Data Controller for the data breach. Data Controller shall notify the data subject regarding breach of data in his possession.

Disclosure of the personal data is prohibited except on consent of data subject and he should be informed about time, purpose, security practices, privacy policies, procedures regarding such disclosure. In national interest such disclosure is permitted without consent.

Special proviso is made for the intelligence organisations. The procedure is prescribed to be followed before processing of information. Special provisions were made for intelligence agencies. But they are not made liable for breach. It is pertinent to note that intelligence agencies are not generally specified under EU Directive or the earlier Bills. Data Protection Authority is created under this Act. Offences under this are cognisable and non-bailable.

It can be observed from the provisions of the above bill, many key terms for protection of personal information or data are not included. Use of surveillance devices and data generated by them were not provided for. But in overall it had provided some guideline.

4.5.5.4 Shrikrishna Committee[250]

[250] "A Free and Fair Digital Economy" Report of the Committee of Experts under the chairmanship of J. B. N.

When European Union has enacted General Data Protection Regulation, there was a demand in India to enact legislation for protection of personal data or information. Government of India established a committee under the Chairmanship of J. B. N. Shrikrishna to suggest such framework. The Commission verified various issues and also took into consideration the legislations all over the world for protection of personal data. The framework was suggested for the Indians.

After Supreme Court has recognised the Right to Privacy a fundamental right to give this right a meaning the personal data is to be made secure. The committee recognised this need because of the progress in technology by use of Artificial Intelligence and other scientific inventions on security of personal data, it is essential to enact legislation for protection of personal data of Indians. It has also recognised that the definition of 'sensitive personal data' has become narrow because of these inventions. Though Artificial Intelligence, processing of Big Data by machine learning and data mining has advantages for the better delivery of services to citizens, but it poses danger to data privacy and security as opined by the Committee. It had referred the incident of Cambridge Analytica.

The Committee opined that the legislation must protect the public good as well as fair digital economy. It believed that the relationship between the data principal and data fiduciary shall be of trust. Person must be the principal-who takes the decision for himself-. The Committee followed the ratio provided in Puttaswamy's judgment which held that individual's privacy is essential for liberty and dignity of him. The Right to Privacy includes the person's right to protect his identity which can be achieved by protecting the information about him. The Committee held that the right to privacy is based on right to autonomy and self-determination regarding personal information.[251]. This can be restricted

Shrikrishna, at https://meity.gov.in/writereaddata/data/files/Data_Protection_Committee_Report_comp.pdf (Last visited on October 11, 2019)

[251] "A Free and Fair Digital Economy" Report of the Committee of Experts under the chairmanship of J. B. N. Shrikrishna, at https://meity.gov.in/writereaddata/data/files/Data_Protection_Committee_Report_comp.pdf p. 16. (Last visited on October 11, 2019)

in well-defined circumstances by the state for the protection of state's interests. Whether such restriction is valid or not can be interpreted by the courts. To achieve these motives and also to ensure free and fair digital economy the Committee has provided various suggestions in the chapters.

The report was prepared with consultation to the experts in various fields. Public consultation were also done and then the framework was finalised. The Commission has carved the fourth way i.e. different from United States, European Union and China inculcating the principles essential for Indian nationals for protection of their rights with a motive to achieve maximum common good.

The suggestions made by the Committee are as follows:

a. The law will be applicable where the data is used, shared, disclosed, collected or otherwise processed in India. It will be applicable to public and private entities both.
b. If it is used, shared, disclosed, collected or otherwise processed by companies incorporated in India it is applicable. But Central Government is empowered to exempt the companies from this.
c. This law will not have respective effect. The Data Protection Authority shall be created. Central Government shall established the appellate tribunal.
d. Penalties are provided. Penalties may be imposed as per fixed upper limit or percentage of worldwide turnover of the preceding financial year whichever is higher.
e. The state can process the data without obtaining consent on the grounds of national security, public welfare, law and order and emergency situations.
f. Cross-border transfer of data other than critical personal data is permitted. This transfer is to be done on model contractual clauses providing for liability of transferor in cases of violation or harm caused to data principal.
g. Critical personal data shall be processed in India and stored in India only.

4.5.5.5 Personal Data Protection Bill, 2018

There was a quantum leap in technology which resulted increase in e-commerce and escalation of social media. The earlier legislation, The Information

Technology Act, 2000 was amended in 2008 and there was no other law for protection of e-transactions for a long time. Also there was thrust towards digital economy after demonetisation in 2016. Many attempt were made to enact privacy bills and personal data protection bills but those efforts were not fruitful. People from all strata of the society persistently demanding the protection of personal data generated through electronic media. The need was felt for strong legislation covering data sovereignty, data retention along with responsibility of government, corporations and individuals while handling third party data. The fear was also expressed about security of personal data which is gathered by government under Aadhaar. Supreme Court of India has recognised Right to Privacy as a fundamental right in the leading case of Justice K. S. Puttaswamy in 2017. Also the regulations by European Union on Data Protection in 2018 (GDPR) has contributed in guiding the enactment of data privacy legislations all over the world.

All these factors contributed for a government to decide to enact a legislation. Government of India established the committee under the chairmanship of J. B. N. Srikrishna and formulated the draft for protection of personal data in 2018. This is known of Personal Data Protection Bill, 2018.

The **Personal Data Protection Bill, 2018-** Provisions for protection of personal data are covered in fifteen chapters containing 112 sections. The provisions which mainly protect the privacy of personal data or information are provided extensively. As these provisions are applicable to personal data processing by body corporate or an individual, it is important to know the provisions. Definitions are provided in very detailed manner.

Object

It has provided the protection on same line of GDPR. Its object which is mentioned in the Bill provides mainly protecting data as it is essential for information privacy which is fundamental right. It also aimed to foster a free and fair digital economy which respects informational privacy. It aims to protect it because it gives empowerment, progress and innovation. Its aim is to protect

autonomy of individual with their personal data and also to specify situations in which the flow and usage of personal data is appropriate. It wanted to create relationship of trust between person and entity processing the personal data. The Bill also specify rights of individual whose personal data is processed and also to create framework for it.

Applicability

The provisions of the Bill were made applicable in relation to processing in India, both by government and private body corporates which are incorporated in India. They are also applicable to body corporates incorporated outside India, but deals with the personal data of data principals in India. But here central government is empowered to exempt any Indian entity dealing with data principals outside India only.

Different types of data like personal data, financial data, biometric data, genetic data, health data etc. are defined under this Bill. Personal data is data of natural identifiable person, Data is defined differently from the definition provided under Information Technology Act, 2000. Under IT act, 2000, information shall be in 'formalised manner', but here the qualifying criteria is 'suitable for communication'. Both are differently provided. Here it includes the information by automated means also under the Bill.

The person whose data is processed is known as data principal and not as data subject as described under GDPR. Data fiduciary is instead of 'data controller' as under GDPR, and includes any person including state, company, any juristic entity or any individual decides to process the personal data. Data processor includes any person or individual who processes personal data on behalf of data fiduciary. It includes state if it processes data.

Grounds for Processing

The bill provides for the conditions for processing the data. The privacy principles are to be followed while processing i. e. with free, informed, clear, specific and capable to be withdrawn, consent of data principal. It should be processed in fair and reasonable way. Processing is allowed without obtaining

consent if it is done for functions of state, compliance with law or courts order, prompt action or purposes related to employment, or inappropriate in respect of the professional relations with data fiduciary or involve disproportionate efforts for processing or any other reasonable purpose specified by Authority e.g. prevention or detection of any unlawful activity including fraud, whistle blowing, mergers and acquisitions, network and information security, credit scoring, recovery of debt, processing for publicly available personal data or purpose specified by the authorities[252].

Processing is to be done in fair and reasonable way. But there are absence of guidelines for what is 'fair and reasonable' way. This is important as data fiduciary has to be able to show to Data Protection Authority that data had been processed in a fair and reasonable way. If no standard is provided, it is difficult to prove. Shrikrishna Committee has recommended that law and regulatory authority should be allowed to evolve principles of fair and reasonable processing, as these standards may vary with technological advancement.[253]

Sensitive personal data

It has provided for the wider definition of personal data and included password, and financial data of the person also. It provides health data, official identifier, information about sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation or any other category which is specified by Authority[254]. It is much wider definition.

In sensitive personal data, 'transgender status' is also provided. It is defined as 'condition of data principal whose sense of gender does not match with the gender assigned to that data principal at birth, whether or not they have undergone sex reassignment surgery, hormone therapy, laser therapy, or any

[252] The Personal Data Protection Bill, 2018, S.17 (2)
[253] "A Free and Fair Digital Economy" Report of the Committee of Experts under the chairmanship of J. B. N. Shrikrishna, at https://meity.gov.in/writereaddata/data/files/Data_Protection_Committee_Report_comp.pdf (Last visited on October 11, 2019)
[254] The Personal Data Protection Bill, 2018 S. 3 (35)

other similar medical procedure.[255] The information about a person belonging to LGBTQ community is protected.

In sensitive personal data intersex Status is covered. Conditions of data principal who is i) combination of male and female, ii) neither wholly male nor wholly female, iii) neither male nor female.[256] New definition in covered. It is different than transgender state of individual. Transgender is born with normal body parts but he feels that he is locked in wrong body, while intersex is defect in body regarding to his gender. For Intersex person, doctor or parents feel that there is something unusual about his body.

Processing of sensitive personal data

Processing can be done by obtaining explicit consent apart from the other criteria of the consent. But in this Bill, the explicit consent is defined as consent under s. 18 and no parameters are provided. Exceptions for the processing are provided that if it is done for functions of state, compliance of law or order of any court or tribunal, for any prompt action eg. Medical emergency or for the purpose as specified by Authority with additional safeguards, it is permitted.

Disclosure or compromise of personal information or data result in to harm to any individual. The 'harm' explained in this Bill is not limited to bodily or mental injury, but loss to his identity, loss in respect of property, reputation, employment etc. also covered. If the disclosure result into the discriminatory treatment or blackmail or extortion, or humiliation, it is covered. If his freedom of movements or speech is jeopardised because of disclosure, it is harm. On the wider scale, it protects the individual's privacy.

Obligations of the data fiduciary

It provides that processing must be fair and reasonable, and data quality should be maintained. It also provides for purpose limitation ie. Data shall be collected for the specified purpose. Storage and retention of data is permitted for the

[255] The Personal Data Protection Bill, 2018 S. 3(41)
[256] The Personal Data Protection Bill, 2018 S. 3 (23)

specified and necessary period. But if he has to comply with any obligation of law it can be retained for longer period. The data fiduciary shall give notice for the details about the purpose of collection and processing, period of storage, information about data fiduciary, rights of the data principal for withdrawal of the consent and how to file complaints to authorities, if data is transferred to cross-border for processing, the intimation about the fact etc.[257]

He shall maintain accountability and transparency. He shall practice those methods and technology which anticipate, identify and avoid harm to data principal. Data fiduciary shall notify the personal data breach to Authority if such breach is likely to cause harm to data principal, about nature of personal data, its possible consequences and measures being taken by data fiduciary.

Period of retention is 'necessary period', the specific period is not provided. Here the Data fiduciary is obligated to report to Authority only if data breach is likely to harm the data principal, so discretion is vested in data fiduciary. This discretion may be exercised in a wrong way. Instances of breaches of personal data when reported to an Authority, separate audit to such transaction is ordered by Data Protection Authority. Result of this audit is shown in score and such score is made public. This publication affect the trustworthiness of the data fiduciary. So, fiduciaries may have tendency not to report data breaches as far as possible. More incidents of data breaches may also affect the stock prices of the company in negative way.

Data Protection Impact Assessment

The Bill introduces concept of Data Protection Impact Assessment. Data protection Impact Assessment shall be done if data is processed with using new technology or on large scale profiling is done which carries a risk of significant harm to data principal[258]. Data fiduciary shall maintain accurate and updated records with periodic review of the activities. Data audits are to be carried out annually.

[257] The Personal Data Protection Bill, 2018, S. 8
[258] The Personal Data Protection Bill, S. 33

Data protection Impact Assessment is provided but the method is not provided. It is very difficult to anticipate the effects of data processing as with the advancement of technology, new techniques are used to process data. It may be possible that the harm which was not anticipated at the time of assessment, may emerged after the processing.

Provisions relating to children

The provision says that 'child' is person below 18 years but in GDPR the age requirement is 16years. Processing of the data of child consent of the parent is required. The requirement of consent is applicable in all the transactions pertaining to children and not only where the consent is required.

Rights of data principal

He has right of confirmation and access and brief summary of the processing of his personal data[259], right to correction for the inaccurate or misleading or incomplete data. He also has a right of updating of personal data.[260]. He has a right to transfer his data to another data fiduciary.

Right to be forgotten

This bill provides for right to be forgotten in different way than GDPR. It provides data principal has right to restrict or prevent continuing disclosure of personal data by data fiduciary related to data principal where such disclosure has served the purpose or no longer necessary, if consent is withdrawn, made contrary to provisions of this Act, or any other law.

It provides that if Adjudicating Officer determines its applicability, after considering the conditions in sub-section (3) and such right can only be exercised if data principal's rights and interests are overriding the right to freedom of speech and expression and right to information of any citizen.[261]

[259] The Personal Data Protection Bill, 2018, S.24,
[260] The Personal Data Protection Bill, 2018, S.25
[261] The Personal Data Protection Bill, 2018, S.27(2)

Here authority to decide as to erase the personal data is vested with the Adjudicating Officer and only if data principal's interests are overriding the right to freedom and speech and right to information of others, then he decide to erase the data. But under GDPR, the right cannot be exercised if data processing is necessary under legal obligation, for exercising freedom of expression and information, and for public interest as public health, and other exemptions[262]. No officer is provided to decide the erasure. Only Data Controller has to decide. Under GDPR, the controller, who has made the data public, shall inform the other controllers who are processing the data to erase any link to, or copies or replications of such data[263]. This provision is not included in this Bill.

Data principal shall have right to raise grievance to data fiduciary about his rights regarding processing of his personal data only showing that it had caused him a harm. Otherwise no complaint can be raised. This provision is negation of the rights of data principal. If harm is not caused, complaint cannot be made.

Significant data fiduciary is appointed by an Authority on the basis of volume of personal data processed, sensitivity of the data processed, and turnover of the data fiduciary, risk of harm from the processing done by him, use of new technologies and any other factor causing harm.[264] This is the new category of data fiduciary created under the Bill.

Storage of data in cross-border transfer

One serving copy of the personal data is to be stored in data centre located in Indian Territory. Data which is notified by Central Government as critical personal data, cannot be processed outside India. [265]

The provision for 'serving copy' of personal data is provided. Data may be available live and on server or as back up. But serving copy definition is not

[262] General Data Protection Regulation, Art. 17,
[263] General Data Protection Regulation, Recital 66
[264] The Personal Data Protection Bill, 2018, S. 38
[265] The Personal Data Protection Bill, 2018, S.40

provided in the Bill. In the same was central government has not notified any data as 'critical data'. So ambiguity lies in the definition of the provision.

Cross-border transfer of data

Personal data other than sensitive personal data can be transferred outside India under contract between the parties and if Central Government with consultation of Authority permits to transfer to other country, or Authority permits to transfer due to necessity.[266] Transfer may be permitted if data protection regime in such country is adequate under the laws and enforced properly by such country. The condition is prescribed that authority can order the transfer if there is necessity, the parameters for 'necessity' are not defined or no guidelines provided.

Exemptions from processing

Rules and regulations in this Bill are not applicable if processing of personal data is done for certain reasons like for national security, or prevention, detection, investigation and prosecution of contravention of law,[267] or if needed for enforcing the legal right or claim seeking any relief, defending any change, legal proceeding,[268] research, archiving, or statistical purpose,[269] or personal domestic purposes,[270] g) journalistic purpose,[271] and h) manual processing by small entities.[272]

The only rules applicable to such processing are that the processing shall be done in fair and reasonable manner and with proper security safeguard. As other rules for processing are not applicable, means such data can be processed without obtaining consent and data principal do not have any right regarding processing of data. These provisions may harm the privacy of persons. Without obtaining consent if the data is processed for research or for archiving, it can be somewhat justified. But for journalistic purposes, the freedom of press may overweigh the right to privacy of an individual.

[266] The Personal Data Protection Bill, 2018, S. 41 (1)
[267] The Personal Data Protection Bill, 2018, S.43,
[268] The Personal Data Protection Bill, 2018, S.44
[269]The Personal Data Protection Bill, 2018, S.45
[270] The Personal Data Protection Bill, 2018, S.46
[271] The Personal Data Protection Bill, 2018, S.47
[272] The Personal Data Protection Bill, 2018, S.48,

Control mechanism

Data Protection Authority is created by issuing notification by Central Government in S. 60 of the Bill. Powers are vested in Data Protection authority to exercise the functions.

Functions are a) maintaining, enforcing, application of provisions of this Act, b) specifying reasonable purposes for which personal data may be processed, b) specifying residuary categories of sensitive data, c) taking prompt and appropriate action in response to data security breach, d) specifying circumstances where Data Protection Impact Assessment may be required to be undertaken in accordance with Act, e) examination of data audit reports submitted, f) monitoring cross-border transfer of personal data. [273] Bill provides for the Appellate Tribunal. It is created by central government notification consisting chairperson and members as notified by Central Government.[274] Appeal against order or decision of Authority or adjudicating officer may be made to Tribunal. An appeal against its order can be made to Supreme Court. Authority can issue orders, directions, conduct inquiry, and also have to power of search and seizure.

Penalties

Penalties are provided under S.69 to 78 in of the Bill for various contraventions of law by data fiduciary. Penalty is provided very high as deterrent. If Data fiduciary contravenes the provisions relating to complying obligations, then he is punishable with penalty up to Rs. 5 crores or 2% of its total worldwide turnover of preceding financing year whichever is higher.[275]

If data fiduciary contravenes the provisions relating to processing of personal data, and processing of sensitive personal data or transfers personal data outside India in violation of provisions then he is liable to penalty up to Rs.15 crores or 4% of its total worldwide turnover of preceding financial year.[276]

[273] The Personal Data Protection Bill, 2018, S.60
[274] The Personal Data Protection Bill, 2018, S. 79
[275] The Personal Data Protection Bill, 2018, S. 69 (1)
[276] The Personal Data Protection Bill, 2018, S. 69 (2)

Penalty for failure to comply directions or orders issued by Authority, Rs. 20,000/- each day subject to maximum Rs. 2 crores for data fiduciary and for data processor Rs. 5,000/- each day subject to maximum Rs. 50 Lakh.[277] Where no separate penalty is provided, for contravention of such provision, person is liable to penalty maximum Rs. 1 crore for significant data fiduciary and Maximum Rs.25 lakhs for others. Penalty is imposed after inquiry by adjudicating officer.[278]

Compensation

Data principal who suffered harm as result of violation by data fiduciary or data processor shall have right to seek compensation by filing a complaint before adjudicating officer[279].

Offences

It provides for offences under s. 90 to 96. Any person who alone, knowingly, intentionally, or recklessly obtains personal data or discloses personal data or transfer personal data to another person or sells or offer to sell personal data to another person, which result in significant harm to data principal, is punishable. 'Recklessly' is not defined but it means doing anything without taking due care. For obtaining, transferring or selling sensitive personal data, any person who alone, knowingly, intentionally, or recklessly obtains personal data or discloses personal data or transfer personal data to another person or sells or offer to sell personal data to another person, which result in significant harm to data principal, is punishable. Person doing re-identification and processing of de-identified personal data without consent of data fiduciary or data processor he is punishable. Punishment is by imprisonment or fine or both. Offences are cognisable and non-bailable.[280]

[277] The Personal Data Protection Bill, 2018, S.72
[278] The Personal Data Protection Bill, 2018, S.73
[279] The Personal Data Protection Bill, 2018, S. 75
[280] The Personal Data Protection Bill, 2018, S. 93,

This bill was covering many points as they are provided under GDPR. But some provisions were not clearly defined. Data was divided in three categories.1. Personal Data, 2.sensitive personal data and 3.critical personal data. But definition of critical personal data was nowhere provided in the Bill. It was to be defined by the authorities. Data fiduciaries shall take periodic review that data shall not be stored for longer period i.e beyond the period which is necessary for purpose of processing. But what is the proper period is not provided in the Bill.

As it is provided in GDPR, Bill also provides for the liability of Government or other agency related to government as it is included in definition of 'data fiduciary'[281]. No exemption is granted to government. Extraterritorial jurisdiction is granted as provided under GDPR. It is applicable to data fiduciary or processor not located within the territory of India if such processing is in connection with business carried out in India, or there is systematic activity or offering of goods and services to data principals within the territory of India, or in connection with any activity involving profiling of data principals within the territory of India. The provisions will not be retrospectively effective.

After receiving the comments and opinions on The Personal Data Protection Bill, 2018, the government has presented a draft personal data protection legislation naming 'The Personal Data Protection Bill, 2019' in Lok Sabha in December 2019.

4.5.5.6 The Personal Data Protection Bill, 2019

This bill retains most of the provisions which were provided in The Personal Data Protection Bill, 2018. Objective of both the Bills is same i.e. to provide for protection of informational privacy as it is a facet of Fundamental right to Privacy. But some definitions and provisions are amended e.g. regarding exempting government's liability are differently provided. The Bill contains 14 chapters and one Schedule. Amended provisions are discussed in following paragraphs as most of the provisions are retained in the earlier Bill of 2018. This

[281] The Personal Data Protection Bill, 2018, S.3 (13)

Bill provides for the general protection for the personal data including sensitive personal data. Personal data is classified in 'sensitive personal data' which includes health data-relating to physical, physiological and mental health. For protection of health data specific provisions are needed as their characteristics are different from the other personal data.

Jurisdiction: These provisions are applicable to processing done by government, private entities incorporated in India, and foreign companies dealing and handling personal data of individuals in India.

Most of the definitions are kept as they were in Bill, 2018. Some terms are redefined by expanding their scope and some are deleted. Definition of Aadhaar number which was provided under earlier bill is deleted in this Bill.

Definition of 'Data Auditor' is provided as this is a new authority created which has to audit the policies and conduct of processing of personal data by Significant Data fiduciary under S. 29.

The provision for 'explicit consent' is deleted from the definition clause but it is provided under the provisions of sensitive personal data. In earlier Bill, it was defined as it is provided under s. 18. In this Bill, explicit consent means 'clear, informed, separately for each act of processing, about the harm which is likely to cause.' This is more accurate than provided in GDPR.

The terms 'intersex status' and 'transgender status' are defined in explanation to the definition of 'sensitive personal data'[282] and not separately as in earlier Bill.

Definition of 'Personal Data' is modified and now it is provided also the data of the person 'online or offline or combination of such features with other information, and inference drawn from such data for purpose of profiling'.[283]

[282] The Personal Data Protection Bill, 2019, S.2(36),
[283] The Personal Data Protection Bill, 2019, S.2(28)

Here the purpose 'profiling' is included for which the personal attributes are used by combining some other attributes. Profiling is done to predict the capabilities of person in a certain sphere which harm the privacy of individual.

Processing without consent[284]

Processing is to be done with the consent, but on some grounds processing of personal data without consent is permitted. It is permitted for performance of functions of state, under any law in India, for compliance with any order of court or tribunal., in response of medical emergency, if such processing is necessary for recruitment or termination of employment by data fiduciary, or verification of attendance, or for the assessment of performance of data principal who is an employee of the data fiduciary. Processing of personal data without consent is permissible where it is necessary for the reasonable purposes specified in regulations. These reasonable purposes are prevention or detection of unlawful activity, credit scoring recovery of debt, the operation of search engines among other grounds.[285]

Only two conditions are required to be followed when data is processed without consent that it should be processed in fair and reasonable manner and applying security safeguard to the processing.

Consent is not required for processing the data for the functions of the state which may include provision of services or benefits to data principal from the state. This purpose is ambiguous. Shrikrishna Committee Report provides that validity of consent given by individual while availing state services for benefits is questionable. Such benefits shall be given without consent for processing. Moreover, only those government bodies which are performing functions directly related to provisions of welfare benefits or regularity functions should be allowed the processing of data without consent. But in reality, processing without consent for all services of public functions by state is too wide.[286]

[284] The Personal Data Protection Bill, 2019, S.12,
[285] The Personal Data Protection Bill, 2019, S.14 (2) (a) to (e)
[286] "A Free and Fair Digital Economy" Report of the Committee of Experts under the chairmanship of J. B. N. Shrikrishna, at https://meity.gov.in/writereaddata/data/files/Data_Protection_Committee_Report_comp.pdf (Last visited on October 11, 2019)

Moreover private sector companies exercising same function has to obtain consent but Public Sector Company does not need. Eg. Public sector banks or telecom companies.

Sensitive personal data

From the definition of 'sensitive personal data', personal data related to 'password' is deleted. Apart from the parameters provided in definition like financial status, health data, official identifier, sex life, sexual orientation, biometric data, genetic data, transgender status, intersex status, caste or tribe, religious or political belief or affiliation, or any other category, categories of personal data are notified as 'sensitive personal data' by Central Government after consulting the Authority, on the basis of risk of significant harm caused by processing, or expectation of confidentiality attached to such data.[287] This provision is providing for the additional criteria for sensitive personal data. Bill enlarges the applicability by providing this. GDPR provides for the additional provisions for the data relating to criminal convictions and offences which are excluded from the sensitive personal data under this Bill.

Provisions relating to children[288]

Same as in earlier Bill, 2018. It provides for personal data and sensitive personal data of children. Person who is below 18 years of age is considered as child under the Bill. Personal data of children shall be processed in a way which is in best interest of them. It is responsibility of data fiduciary to verify the age of child and obtain consent. Consent is essential for the processing of the children's data. Age of child is 16years under GDPR.

A Guardian fiduciary[289]: A new entity is created. The data fiduciary who operates commercial website or online services directed at children or process large volumes of personal data of children is classified as 'Guardian Data Fiduciary' by the Authority. Such guardian data fiduciary is barred from profiling, tracking or behaviouraly monitoring of or targeted advertising

[287] The Personal Data Protection Bill, 2019, S.15,
[288] The Personal Data Protection Bill, 2019, S.16 (1),
[289] The Personal Data Protection Bill, 2019, S.16 (4)

directed at children and also barred to process the personal data in a way which may cause significant harm to child. The data fiduciary who offers counselling or child protection services to child, has to follow some restrictions specified by Authority. Additional protection is provided to children as they are using social media.

Rights of data principal

The data principal has right to receive confirmation, to receive summery, right of access the identities of data fiduciaries who had shared his personal data with other data fiduciaries[290], right to correction of inaccurate data, completion of incomplete data, updating of out-of- date data, and erasure of personal data which is no longer necessary. The data principal has right to data portability. The data principal has right to receive personal data in structured, commonly used and machine readable format where the processing has carried out through automated means. [291]

Right to be forgotten is provided in different form than that is provided under GDPR. Here the data principal has right to restrict or prevent the continuing disclosure of his personal data by data fiduciary where such disclosure has served its purpose, or no longer necessary, or where consent is provided, such consent is withdrawn, or made contrary to provisions of any law in force.[292]

The data exercising any right regarding enforcement of his rights, data principal shall make a complaint in writing directly, or through **consent manager,** to data fiduciary except in case of right to be forgotten[293].

The **consent manager**[294]

It is the new entity introduced in this bill who deals with the consent of data principal, if data principal chooses to give or withdraw through consent manager, to the data fiduciary and he should be registered with data fiduciary.

[290] The Personal Data Protection Bill, 2019, S.17(3)
[291] The Personal Data Protection Bill, 2019, S.19
[292] The Personal Data Protection Bill, 2019, S.20
[293] The Personal Data Protection Bill, 2019, S.21
[294] The Personal Data Protection Bill, 2019, S.23 (5)

The consent given or withdrawn through consent manager is deemed to be given or withdrawn by data principal himself[295]. He should maintain transparency.

Security and Transparency provisions

It provides for the provisions regarding transparency and accountability of data fiduciary. For the security of the personal data, the policy of privacy by design is provided. It is specified that data fiduciary shall prepare privacy by design policy containing the managerial, organisational, business practices and technical systems designed to anticipate, identify and avoid harm to data principal[296]. Technological standards for processing should match the certified standards. While processing the personal data, legitimate interests of businesses shall be achieved. In this process, privacy interests shall not be compromised, and privacy shall be protected throughout processing at all stages.

Processing without consent

Processing is generally with the consent, but processing is permitted without consent in the Bill in certain circumstances. They are complying with court's order, for state's interests, for medical emergency, to provide assistance or service in disaster. It is also permitted for reasonable purposes specified by notification for any public interest.

GDPR also provides exceptions for law enforcement data access and for taxation purposes. These 'reasonable purposes' include whistleblowing, mergers and acquisitions, network and information security, credit scoring, recovery of debt, processing of publically available data and operation of search engine. These exemptions from consent requirement may be susceptible to be misused by the government. Such authority may be used for surveillance.

Duties of data fiduciary and data processor

The data fiduciary shall maintain transparency in collection and in processing of personal data, make available the information relating to collection and

[295] The Personal Data Protection Bill, 2019, S.23 (4)
[296] The Personal Data Protection Bill, 2019, S.22 (1)(a), (b)

processing of personal data, rights of data principal, regarding cross-border transfer. The data fiduciary and data processor shall implement the necessary safeguards for the risks associated with the processing of personal data[297]. The breach of personal data shall be reported to Authority within specified period. Significant data fiduciary is appointed by an Authority on fulfilling certain conditions.

In the earlier bill, the Authority was empowered to classify the significant data fiduciary out of data fiduciaries on the basis of certain factors. But social media intermediary as data fiduciary was not included in the bill. But in this Bill of 2019, Central Government, in consultation with the Authority, is empowered to notify the social media intermediary as significant data fiduciary. Any social media intermediary having users above particular number (the threshold) as notified by Central government and whose action have significant impact on electoral democracy, security of state, public order, or sovereignty and integrity of India shall be notified as significant data fiduciary.[298] The Central Government is empowered to notify different thresholds for different classes of social media data fiduciary. [299] 'Social Media Intermediary' means "Social media intermediary is an intermediary who primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify, or access information using its services". [300]

But from the definition of 'social media intermediary' the search engines, online encyclopaedias, e-mail services or online storage services, intermediaries which provide access to internet or enable commercial or business oriented transactions are excluded.[301]

In this Bill the provisions regarding '**data protection impact assessment'** are included which is mandatorily be conducted if the data fiduciary intends to undertake any processing involving new technologies or large scale profiling or use of sensitive personal data such as genetic or biometric data or any other

[297] The Personal Data Protection Bill, 2019
[298] The Personal Data Protection Bill, 2019, S.26 (4)
[299] The Personal Data Protection Bill, 2019, Proviso to S. 26(4),
[300] The Personal Data Protection Bill, 2019, Explanation to S.26 (4),
[301] The Personal Data Protection Bill, 2019, Explanation to S.26 (4),

processing which carries a risk of significant harm to data principals.[302] This provision regarding data protection impact assessment is retained in this Bill.

The Authority may specify the circumstances, or class of data fiduciary or processing operation where such data protection assessment shall be mandatory and also specify instances where data auditor shall be engaged by data fiduciary to undertake data protection assessment.[303] The Assessment shall contain detailed description of processing, assessment of potential harm and measures for managing, minimising or removing such risk.[304] The data protection officer is to be appointed[305].

There are provisions for duties of significant data fiduciary. He shall maintain accurate and up-to-date records of important operations in collection, transfers and erasure of personal data to demonstrate the compliance and he shall take periodic review of security safeguards, data protection impact assessment etc.[306] It is mandated that data protection officer shall be appointed. Data fiduciary shall have maintain the procedure and effective mechanisms to redress the grievances of data principals efficiently and speedy way.

Cross-border Transfers and storage of data

It provides for restrictions on transfer of personal data outside India. It provides that explicit consent is essential for transferring the sensitive personal data outside India on contract or intra-group scheme approved by Authority.

A remarkable deviation from the provisions in earlier Bill that now only certain types of data, and not all types of data, have to be stored in India. Critical data and sensitive personal information or data must be stored in India. Copy of sensitive personal data can be stored outside India if certain conditions are met. Earlier it was not permitted in the Bill, 2018. For such storage the other country

[302] The Personal Data Protection Bill, 2019, S. 27 (1)
[303] The Personal Data Protection Bill, 2019, S.27 (2),
[304] The Personal Data Protection Bill, 2019, S.27(3)
[305] The Personal Data Protection Bill, 2019, S.27(4)
[306] The Personal Data Protection Bill, 2019 ,S.28

must satisfy the adequacy principle i.e. adequate level of protection under the law. But Critical personal data must be processed and stored in India.

Any critical personal data may be transferred outside India where such transfer is to a person or entity engaged in provision of health services or emergency services where such transfer is necessary for prompt action or to country where Central Government has permitted[307].

Storage of data at local places is introduced by Reserve Bank of India, which has mandated that the payment data using digital means shall be stored in India[308].The Bill followed the practice and provides for such important data to be stored in India.

Exemptions

It provides in S. 35 for power of Central Government to exempt any agency of Government in respect of the processing of the personal data from application of the Act. Processing of personal data includes sharing by or sharing with such agency of Government by any data fiduciary, data processor or data principal. Where Central Government is satisfied that it is 'necessary or expedient' in the interest of sovereignty and integrity of India, security of state, friendly relations with foreign states, public order or preventing the cognisable offence relating to sovereignty and integrity of India, security of state, friendly relations with foreign states, public order, it exempts government agencies specifically regarding processing of personal data.

It is feared that the provision in above section, may be misused or abused by the government. The term 'necessary and expedient' gives power to state to form subjective opinion about the threat. Earlier in S. 42 of the Bill, 2018, the words used were 'necessary and proportionate' which are replaced by 'necessary and expedient'. The test of 'proportionality' is repealed. In the decision of Puttaswamy (2012), Supreme Court held that the law should be just, reasonable

[307] The Personal Data Protection Bill, 2019, S.34 (2)
[308] 'Storage of Payment data', RBI/2017-18/153 at www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0 (Last visited on October 11, 2019)

and proportionate, to take away right to privacy. In this provision that condition is removed. The term 'necessary and expedient' does not balance the interests of individual and state properly.

Under S.91, the government has power to frame any policy for digital economy including taking measures for growth, security, integrity, prevention of misuse as long as it does not use personal data which directly identify person. Government can direct any data fiduciary to hand over any anonymised data or non-personal data for better delivery of services or for evidence-based formulation of policies.

This power to instruct the data fiduciary to hand over non-personal data is not very clear. Non-personal data is explained as which is not personal. No other parameter is provided. Moreover, any non-personal data can become personal data with advanced technics of data processing. So there is a possibility of threat to right to privacy from the government itself.

The provisions of Bill shall not apply where personal data is processed in the interests of prevention, detection, investigation, and prosecution of an offence or any contravention of any law or disclosure is necessary for enforcing any legal right or claim, or processing is necessary for exercise of any judicial function by court, for personal or domestic or journalistic purposes research, archiving or statistical purposes etc.[309]

Exemption may be granted by the Central Government to any data processor from processing the personal data of the data principals residing outside the country on the contract with any person outside India. Exemption may be granted on certain conditions to small entities which do not process data with automated means.

AI, ML and Data Protection

[309] The Personal Data Protection Bill, 2019, S.36 and 38

In this Bill, a new concept is provided for encouragement of innovation in Artificial Intelligence, machine learning or any other emerging technology in public interest. The Authority shall create a '**Sandbox'** for the purpose specified above.[310] The definition of 'Sandbox' is not provided in the Bill. But the condition that any data fiduciary whose privacy by design policy is certified by Authority shall be eligible to apply for inclusion in 'Sandbox', further such inclusion shall be for the period of twelve months and may be renewed for not more than twice, subject to total period of thirty- six months.[311]

Data Protection Authority

Data Protection Authority is provided. Central government is empowered to establish by issuing notification.[312] Authority has general power of superintendence and directions.[313] The Authority issues directions, instructions and conduct inquiry if complaints are received by appointing inquiry officer. It can warn, suspend or discontinue the business activity. It may appoint inquiry officer to conduct inquiry and on receipt of the report may initiate an appropriate action.

Functions of Data Protection Authority are mainly to protect interests of data principles, prevent misuse of data, ensure compliance of the provisions, shall monitor and enforce the application of the provisions, take prompt and appropriate action in response to personal data breach, maintain database on its website containing names of significant data fiduciaries along with rating as trust scores, shall monitor cross-border transfer of personal data, specify the codes of practice by issuing regulations.

There is a possibility for controlling the data processing by the government. The Authority can decide which data to process and which should not be processed as per the government's instructions which may have serious consequences of violating the privacy of people.

[310] The Personal Data Protection Bill, 2019, S.40 (1)
[311] The Personal Data Protection Bill, 2019, S.40 (4)
[312] The Personal Data Protection Bill, 2019, S.41,
[313] The Personal Data Protection Bill, 2019, S.45

Offences

It provides different offences. Any person knowingly or intentionally re-identifies personal data which was de-identified by data fiduciary or data processor, or re-identifies and processes such personal data without consent of such data fiduciary, shall be punishable with imprisonment for term not exceeding three years of with a fine which may extend to two lakh rupees or both. [314]The offence under this Act shall be cognizable and non-bailable, and civil court has no jurisdiction for the offences under this Act.[315]

Penalties and compensation

For breach of privacy of personal information, the penalty is provided. The salient feature of these provisions is that where the breach is done by company as data fiduciary or data processor, the penalty includes certain percentage of their turnover worldwide.

Penalties for failure to comply different provisions in the Bill, significant data fiduciary is severely punished than simple data fiduciary. Where any person fails to comply with the provisions of this Act, for which no separate penalty is prescribed, then such person shall be liable to penalty which may extend to a maximum of Rs. one crore in cases of significant data fiduciary and Rs. 25 lakh in other cases.[316] Adjudicating officer may be appointed to decide penalties and compensation.

Compensation

If data processor has acted contrary to instructions of data fiduciary or acted in violation of this Act, which may have harmed the data principal, data principal may ask for compensation from him. Data processor is liable only where he has acted outside or contrary to instruction of data fiduciary, or data processor has acted in negligent manner or he had not incorporated adequate security safeguards.[317] Compensation may be awarded depending upon the factors.

[314] The Personal Data Protection Bill, 2019, S.82(1)
[315] The Personal Data Protection Bill, 2019, S.83(1), (2)
[316] The Personal Data Protection Bill, 2019, S.61
[317] The Personal Data Protection Bill, 2019, Explanation to (1) S.64

Redressal Mechanism

Central Government by notification establish an Appellate Tribunal. The person aggrieved by the order of Adjudicating officer may apply to Tribunal. An appeal shall lie against the order of Tribunal, not being an interlocutory order, to Supreme Court of India on any substantial question of law within ninety days from the receipt of order appealed.[318]

Current Status

The Personal Data Protection Bill, 2019 was presented in Parliament and sent to joint select committee. After this it will be enacted as Act. Therefore, as of today, India does not have any specific legislation for protection of data.

Issues

The health data including biometric and genetic data is generated while using medical facilities and receiving medical treatment for different ailments. Various pathological reports and X-rays, MRI, and Scan reports are also used while treating the patients. The transfer of sensitive health data is done intra and inter hospitals in the same territory as well as outside India. The diagnostic centres are also dealing and handling the health data. Pharmaceutical organisations are keen to obtain such data for research and development of medicines. There is a possibility that patient's data will be obtained and used unauthorised, by which patient's privacy is violated and security is endangered.

In Personal Data Protection Bill, 2019 the provisions relating to collection, storage, use, dissemination and transfer of health data are covered generally. But the health data is sensitive information which is protected under S.3 of Privacy Rules, 2011. These transactions shall be given very strong and specific protection relating to collection, storage, use, transfer and dissemination of sensitive health data.

To eradicate the possibility of unauthorised access, collection, use and storage, Ministry of Health and Family Welfare has enacted the provisions for protection

[318] The Personal Data Protection Bill, 2019, S.75

of privacy of persons regarding health data. This draft is put for public comment on the website. As Personal Data Protection Bill, 2019 is drafted for protection of personal data, this draft is handed over to Ministry of Electronics and Telecommunication for inclusion in the Personal Data Protection Bill, 2019. It is done with the objective that there shall not be two legislations for the protection of personal data. But it is important that provisions which are drafted under this Act shall be taken into consideration. The provisions for protection of health data contained in the Act are discussed in following paragraphs.

4.5.5.7 Digital Information Security of Healthcare Act (DISHA)

Ministry of Health and Family Welfare enacted the provisions for protection of privacy, confidentiality and integrity of such medical data under Digital Information Security in Healthcare Act, herein after (DISHA)[319] in 2018 and it was kept for public comment.

Objectives

Act aims at establishing National and State eHealth Authority and Health Exchanges, to provide standardised the process related to collection, storing, transmission and use of digital health data and to ensure reliability, to regulate the process. It also aims to maintain data privacy and confidentiality and security of digital health data and other matters related and incidental to. The provisions are contained in seven chapters. To protect the digital health data, terms are defined in widest possible limits.

Definition of the terms relating to health data security and protection are provided extensively. It provides that, 'unless the context otherwise requires', which means if more criteria is needed for protection it can be used and permitted, but if no parameters are in existence, the parameters provided in the definitions given in Act will govern the term.

[319]Available at www.nhp.gov.in/NHPfiles/R_4179_1521627488625_O.pdf (Last visited on October 29, 2019)

There are two processes for keeping confidentiality of data. Anonymisation means deletion of all personally identifiable information from person's digital health data.[320]

'De-identification' means the process of removing, obscuring, redacting or delinking all personally identifiable information from an individual's digital health data in a manner that eliminates the risk of unintended disclosure of the identity of the owner and such that, if necessary, the data may be linked to the owner again.[321]

The health data can be processed by obtaining consent. The term 'consent' is all inclusive of possible ways in which it is to be given. 'Consent' means expressed, informed consent, whether in written or electronic form, given by the owner after understanding the nature, purpose and consequences of the collection, use, storage or disclosure of the digital health data, provided that consent shall include proxy consent on behalf of the owner, subject to the circumstances envisaged under this Act[322].

The protection is given to digital health data. 'Digital Health Data' means an electronic record of health- related information about an individual. It includes not only the information concerning the physical or mental health of the individual but other information concerning any health service provided to the individual. The information collected while providing health services are also included or information concerning the donation of body part or bodily substance by the individual. It also includes digital health information derived from the testing body part or bodily substance. Which means it includes the test reports containing health of the individual by diagnostic centres. If an individual access services of clinical establishment, the information submitted to the establishment is protected.

[320] Digital Information Security of Health care Act, S.3(1) (a)
[321] Digital Information Security of Health care Act, S.3(1)(d)
[322] Digital Information Security of Health care Act, S.3(1) (c)

'Entity' includes any of the following, not being a clinical establishment:(i) An individual;(ii)A company;(iii)A department of the Central or State Government;(iv)A firm;(v) An association of persons or a body of individuals, whether incorporated or not, in India or outside India; or (vi) Any corporation established by or under any Central, State or a Government company (vii) Any body corporate incorporated by or under the laws of a country outside India;(viii) A co-operative society (ix)A local authority;(x) Every artificial juridical person, not falling within any of the preceding sub-clauses.[323] It is applicable to Indian and foreign entity.

Definition of clinical establishment is given extensively covering every type of entity giving medical/health care established as an independent entity or part of any other entity. It also includes clinic run by one doctor. The services provided relating to deformity, injury or abnormality etc. by the institutions, these institutions are known as clinical establishment. Diagnostic laboratories and pathological laboratories are included. The establishment owned by Government, trust, corporation, local authority or single doctor are governed by the provisions. The diagnostic laboratory is established and governed under any clinical establishment under the provided parameters, the provisions apply.

'Personally Identifiable Information' means any information that can be used to uniquely identify, contact or locate an individual, or can be used with other sources to uniquely identify a person, and includes the information stated in Schedule I. [324] This definition does not provide for specific parameters for personal identifier, and is too wide. But information mentioned in the schedule I does not include 'genetic data or information' which is covered by Personal Data Protection Bill, 2019. In respect of health information inclusion of genetic data is essential.

'Sensitive health-related information' means information, that if lost, compromised, or disclosed, could result in substantial harm, embarrassment,

[323]Digital Information Security of Health care Act S.3(1)(f)
[324] Digital Information Security of Health care Act S.3(1) (k)

inconvenience, violence, discrimination or unfairness to an individual, including but not limited to, one's physical or mental health condition, sexual orientation, use of narcotic or psychotropic substances, consumption of alcohol, sexual practices, Human Immunodeficiency Virus status, Sexually Transmitted Infections treatment, and abortion. [325] Very exhaustive definition. These parameters can be used to get personally identifiable information and these parameters qualify the personally identifiable information in health data.

National Electronic Health Authority of India (NeHA)

(1)The Central Government shall establish for the purposes of this Act, a National Electronic Health Authority of India, by Notification in the Official Gazette, which may be referred to as NeHA in its abbreviated form.[326]

Composition

National Electronic Health Authority of India shall consist of the following members, to be appointed by the Central Government by Notification, namely:(a)A full time Chairperson;(b)A member -secretary; equivalent to the rank of Joint Secretary to the Government of India(c)Four full-time members to be appointed by the Central Government one from health informatics, public health, law; and, public policy, each (d)Four ex-officio members, not less than the rank of Joint Secretary to the Government of India to be appointed by the Central Government each one from Ministry of Electronics and Information Technology, Ministry of Panchayati Raj/ Ministry of Women & Child Development; Directorate General of Health Services; and Ministry of Law and Justice.

Representation from sectors crucial for protection of sensitive digital health nformation is given by the government at national level. For the state level, the members essential for protection of sensitive digital health information is provided.

State Electronic Health Authorities

[325] Digital Information Security of Health care Act, S.3(1)(o)
[326] Digital Information Security of Health care Act, S.4

Every State Government shall, by notification in the Official Gazette, establish a State Electronic Health Authority, which may be referred to as SeHA in its abbreviated form[327].

Composition

Composition of State Electronic Health Authorities (1) State Electronic Health Authority shall consists (a)A full time Chairperson;(b)Secretary in-charge of State Health Department or equivalent as member-secretary; (c)Three full-time members to be appointed by the State Government:(i)One from health informatics;(ii)One from public health; and(iii)One from law. Three ex-officio members are to be appointed[328].

Health Information Exchange

It shall be established by Central Government by issuing notification and it should conduct and carry out their affairs strictly as per norms, standards or protocols specified by National Electronic Health Authority. It shall have Chief Health Information Executive.[329]

Functions of NeHA

Powers and functions of National Electronic Health Authority and State Electronic Health Authority by issuing notification in Official Gazette respectively[330]. The objective to establish them is to ensure confidentiality and privacy of digital health data. Function of the authority include i. to formulate standards, operational guidelines and protocol for generation, collection, storage and transmission of digital health data available to clinical establishment and health information exchange. ii. To ensure data protection and prevention of breach or theft of digital health data. [331]It has a power of inspection, investigation and issuance of directions.[332]

[327] Digital Information Security of Health care Act,S.7
[328] Digital Information Security of Health care Act, S.8
[329] Digital Information Security of Health care Act, S.19
[330] Digital Information Security of Health care Act, S.22(1)
[331] Digital Information Security of Health care Act, S.22 (1) (a), (b)
[332] Digital Information Security of Health care Act, S.23

Rights of the Owner of digital health data:

Under this Act, Ownership of digital health data is of the individual whose health data has been converted into digital form. He has right to privacy, confidentiality and security of his health data. He has right to give or refuse consent for generation and collection of digital health data, ii. to withdraw the consent given. He has right to give or refuse or withdraw consent for storage and transmission and also has right to prevent transmission. He has a right to access or disclosure of digital health data. He also has right to know clinical establishment entities which may have or access to digital health data and about the recipient of such data. Right of rectification of the digital health data is also available to him. [333]

Prior explicit consent of data owners shall be taken prior to transmission of or use of data in identifiable form. Transmission shall be in encrypted form. Health Information Exchange shall retain the copy of this. They shall not be refused health services if they refuse to consent to generation, collection, storage or transmission or disclosure of data. Data owners have right to know for which purpose data is used. This protection is important as the clinical establishment or entity giving health care may exploit the patient. They may compel the person to give consent in lieu of the health services which may affect the legal rights of the person.

Purposes of the collection of data

Purpose of the collection of health data are to advance delivery of patient centred medical care, improve co-ordination of care and information among hospitals, medical professionals, or secure and authorised exchange of digital health data, to improve public health activities, facilitate health and clinical research among other.[334] Personal health data shall not be collected for converting it in digital health data.

Access of the health data

[333] Digital Information Security of Health care Act, S.28
[334] Digital Information Security of Health care Act, S.29

Stored, transmitted digital health data can be accessed by clinical establishment only on need to know basis. It can be accessed by specific person for specific and lawful purpose. Government departments may access data in de-identified/anonymised form by following procedure from Health Information Exchange. If it is necessary for investigation of offence, with the order of the court can be accessed. It can be accessed by relatives and legal heirs of the owner in case of emergency or death.

Storage of Data

The relationship of Clinical establishments or Health Information Exchange to a person whose data is stored is of trust. The hold such data as custodian. Digital health data shall be stored by clinical establishments or Health Information Exchange as per the provisions. Clinical establishment or Health Information Exchange shall hold data on behalf of National Electronic Health Authority and shall use it without compromising privacy and confidentiality of such data. For transmission, provisions of this Act must be followed.

For protection of privacy, confidentiality and security of digital health data clinical establishment, Health Information Exchange, State Electronic Health Authority and National Electronic Health Authority are duty bound.

Offences and penalties

Breach is said to occur when any person generates, collects, stores, transmits or discloses digital health information, or any person damages, destroys, deletes, affects injuriously by any means or tapers with digital health data.

Serious breach or breach in aggravated form occurs when any person i. intentionally, dishonestly, fraudulently or negligently, ii. Breach relating to information which is not anonymised or de-identified, iii. Person fails to secure health data, iv. Person uses digital health data for commercial purpose or commercial gain, v. any entity, clinical establishment or Health Information Exchange commits the breach repeatedly.[335]

[335] Digital Information Security of Health care Act, S.38

Penalties- a person who is guilty of committing the offence of obtaining fraudulently or dishonestly digital health information of a person shall liable to imprisonment and fine or both. Whoever dishonestly or without authorisation acquires or accesses any digital health data shall be liable to imprisonment which may extend to 5 years or fine not less than 5 lakhs rupees or both.[336]

Penalty for not providing information, filing return or failure to observe rules and directions shall liable to imprisonment which may extend to 3 years to 5 years or fine not less than 5 lakhs.[337]

Owner of data has a right to obtain compensation for serious breach[338]. No court has cognisance of any offence punishable under this Act.[339] There is a provision for offences by companies. The person who is in control of the administration or looking after the business at the time of breach is liable to be punished. [340]

State Adjudicating Authority and National Adjudicating Authority.

Data owner is to report data breach by clinical establishment or any entity to State Electronic Health Authority. Any person aggrieved by the order or direction or penalty imposed by State Electronic Authority may prefer an appeal to State Adjudicatory Authority.[341] Appeal may be preferred to Central Adjudicatory Authority If breach of digital health data is by health information exchange, State Electronic Health Authority or Central Electronic Health Authority, by owner.[342]

Central Government appoints National Adjudicatory Authority by issuing notification in official gazette. State Government appoints State Adjudicatory Authority by issuing notification in official gazette. Inquiry before it is judicial

[336] Digital Information Security of Health care Act, S.43
[337] Digital Information Security of Health care Act, S.40
[338] Digital Information Security of Health care Act, S.39
[339] Digital Information Security of Health care Act, S.43
[340] Digital Information Security of Health care Act, S.44
[341] Digital Information Security of Health care Act, S.46
[342] Digital Information Security of Health care Act S.46

inquiry. The decision of Central adjudicatory authority can be challenged in high court[343].

With respect to digital medical record, provisions of this Act have predominance.

The draft of this Act was submitted to Ministry of Electronics and Information Technology for their inputs but as the Ministry was drafting the Data Protection legislation, the draft is subsumed in the upcoming data protection legislation to avoid duplicity, as per the press release from the Ministry of Health and Family Welfare.[344]

4.6 An Interface between Right to Privacy and Information Technology Act, 2000

Use of the Communication technology has reached to maximum for connecting with the world. It is developed from verbal communication to letter writing to telephone conversation to communication using computer. Invasion on these media has also developed from eves dropping to unauthorised opening of letter to tapping of the telephone to hacking of the computer. By gaining information through these invasions, the personal information is collected and disclosed to society. This information was published for personal gain or for harassment in newspaper or on electronic media. These invasions threaten the personal image, peace of mind and personal space of the individual. It is a right of the individual that his personal space shall not be invaded is breached by this. This personal space is termed as 'Right to Privacy".[345]

4.6.1 Use of Information Technology

Information technology is used from small shop to big business houses for doing business. Common people use it for many purposes like purchase, sell, travel booking, entertainment, or only for chatting on social media. Government is using this technology for better governance. For receiving services or social benefits provided by government, personal information is submitted to the

[343] Digital Information Security of Health care Act S.51
[344] https://pib.gov.in/Pressreleaseshare.aspx?PRID=1578929
[345] Warren and Brandeis, "Right to Privacy" Harvard Law Review, Vol. IV, no.5, 1890

government. This personal information is also known as 'data'. Any entity, however small it may be soon become the repository of data or information relating to individuals who have dealt with it. Communication technology and Internet have covered the whole world in their tentacles.

Information Technology is developing with great speed. Every person expects that his personal information shall not be accessed, misused or abused. When information stored in the electronic device i.e. computer, is accessed and used without the permission of a person, his informational privacy is violated. Data mining is used to create facts by combining and processing two or more facts about the individual. Data mining means "the process of discovering interesting and useful patterns and relationship in large volume of data."[346] With the use of data mining and Artificial intelligence-"machines mimic cognitive functions that human associates with the human mind like learning"[347], physical, or behavioural information is gathered. It is processed by applying one or more parameters and it is possible to gather information about not only the person but information about people around him.

4.6.2 Need for Data Protection

To gain some advantage, the information about the person is gathered. It has become the age of 'dataveillance'.[348] 'Dataveillance' is a practice of monitoring digital data relating to personal details or online activities.[349] Cambridge Analytica was the example. It had harvested the personal data of millions of users of social media without their consent and processed it for political advertising. By doing so, the paradigm for voting in favour or against the particular political party was predicted and accordingly the political canvassing was designed. The outcome was unexpected. This has shown that how person become vulnerable and lose his decision- making power which may result in losing his legal rights.

[346] Christopher Clifton, "Data Mining", www.britannica.com (Last visited on December 11, 2019)
[347] Russell and Norvig, "Artificial Intelligence: A Modern Approach", (3rd edi.).Upper Saddle River, New Jersey, Prentice Hall., p.2
[348] Clarke Roger A., "Information Technology and Dataveillance", Communication of the ACM, Vol. 31, Issue 5, May (1988) Pp 498-512. Doi: 10.1145/42411.42413.
[349] Oxford Dictionary.

The data breaches and its consequences are reaching on the threshold of India also. It was reported that banks in India have to change the security codes of as many as 3.2 million debit cards because of financial data breach. As reported by SISA- a payment security specialist, that the breach is said to have originated in malware introduced in systems of Hitachi payment services. Through this the information is stolen and funds were cleaned.[350] Most affected banks were SBI, HDFC, ICICI, YES and AXIX.

It was reported in 2019, "that on an average, 35,636 records are compromised in data breach in India. Data breaches cost organisations in India is about 12.8 crore within the period July 2018 to April 2019", [351] according to report of IBM. The findings are part of 2019 Cost of Data Breach Report, conducted by the Ponemon Institute, and sponsored by IBM Security. The report said major causes of data breach in India comprised malicious or criminal attacks (51%).

4.6.3 Aadhaar and Privacy Issues

Government of India has introduced unique identity number to its citizens. For which Aadhar card was issued. For registering under Aadhar, person has to give his personal information including biometric information like fingerprint, print of iris etc. There is a possibility that information collected may be misused by government. In 2017, Supreme Court of India has recognised that Right to privacy as a fundamental Right but also held that it is not absolute. When and where the state interest is involved, it has to give way to state interest.

This Aadhaar card data was also compromised in 2018. World Economic Forum's Global Risk Report, 2019, mentioned that the government ID data base, Aadhaar reportedly suffered multiple breaches. Those breaches potentially compromised records of 1.1billion registered users. It had mentioned that in January, 2018 the criminals were selling access to data base of Aadhaar at the rate of Rs. 500/- per 10 minutes. In March, a leak at state owned utility company allowed any one to download names and ID numbers.[352] Data on the State of

[350] www.m.economictimes.com published on 20/10/2016. (Last visited on December 11, 2019).
[351] www.thehindu.com published on 23/07/2019. (Last visited on December 11, 2019).
[352] https://www.wefoum.org/reports/the-global-risks-report 2019. (Last visited on December 11, 2019).

Jharkhand website, which was maintaining attendance record of the workers, was accessed and data with Aadhaar numbers of those workers was leaked. The legal systems find it difficult to imagine of all the possible uses of information and also difficult to imagine consequences.

4.6.4 Information Technology Law and Right to Privacy: An Interface

India has information Technology Act which provides protection for personal data or information in limited sense. Basically, it provides the legal framework for protection of such data or personal information and provides for privacy for information related to business transactions. Privacy Rules are made in 2011 under this Act. But these regulations are not covering privacy encroachments which are the outcome of the processing of personal data by new and advanced technology. The process of enacting law takes time, within which the technology advances by leaps and bounds.

Protection of privacy of personal information is crucial for maintaining the person's liberty and freedom. It becomes possible when the rules, regulations and legislations are enacted against the violation by any entity including government.

The concept of right to privacy has undergone a sea change with the advent of technology. In the preceding chapters, the researcher has discussed the development of the concept of Privacy at length. Also, in the above discussion, the researcher has discussed and analysed the Information Technology Act, 2000 with the Rules and guidelines. Also, the various legislative attempts at data protection have been discussed. After studying and analysing the above legislations, it has been observed that there is an interface between Right to Privacy and Information Technology Act. Also, it has emerged from the above discussion that the enactment of Information Technology Act, 2000 was not sufficient to cover the right to privacy issues arising over of data protection.

The law has to maintain balance between rights of people and interests of the State. A study of the laws in European Union show that it has tried to control violation of informational privacy by providing guidelines and regulations for

personal data protection. Member countries of European Union have adopted these regulations. Many other countries like UK and USA have also enacted the legislations for privacy of personal data or information.

India has also attempted to enact a legislation for Data Protection. The protection of Data, the right to manage and control the data, choice and control over data, disclosure of information, power to intercept / encrypt the data, security of information, are a few privacy issues which remain unaddressed by the Information Technology Act and press an urgent need for a separate legislation for protection of informational Privacy in this digital age.