Name- Upasana Borah

Student of N.E.F LAW COLLEGE AFFILIATED TO GAUHATI UNIVERSITY ,ASSAM, GUWAHATI

Course- B.B.A LL.B (Hons)

8th Semester/4th Year (2016-2021)

THEME- DATA PROTECTION LAWS

DATA PROTECTION LAWS

ABSTRACT

Data protection is one of the most common process of safeguarding data to prevent it from getting corrupt .The key principle of Data Protection is to protect and safeguard the data and make it available under the circumstances. It is to be applied to all forms of data either personal or corporate which deals with both integrity and protection of data. Protecting the privacy of the people in the modern era is essential to an effective democratic government. However, an increase in the awareness and recognition for data protection across the world is still not enough, as we suffer from a lack of legal infrastructure to protect the Right to Privacy which is regarded as a Fundamental Right under Article 21 of The Indian Constitution.

KEYWORDS- INFORMATION TECHNOLOGY, PRIVACY, DEMOCRATIC, LEGAL FRAMEWORK, CONTRACT, ELECTRONIC, DATA.

HISTORY OF DATA PROTECTION

In today's digital world almost everyone has a valid e-mail address. Many people have e-mail accounts on free web-based e-mail platforms. Similarly Facebook is used as a platform to manifest our thoughts by means of words and various forms of media. Technology has raced past us rapidly in the last few decades. Hence it is a timeworn concept. People are growing their advent and awareness toward the protection and preservation of their data. That is the reason why different nations have devised and adopted varied means to protect data of every individual. Data has been sought to be protected from the beginning of human civilization. Over the period of time different kings and kingdoms tried to protect data by enshrining them in various forms of tangible mediums including stone. In fact, the focus of data protection is protecting the rights of individuals with respect to their data. The invention of internet and the global explosion of growth in data have necessitated different nations to come up with their own distinct national legislations to deal with data protection. Not only this, even international organizations have been working on various principles pertaining to data protection.

CONCEPT OF DATA PROTECTION

Internet is one of the most significant innovations in the human history after the advent of fire. No single event has impacted the growth of humanity as much as the internet. While the advent of internet has on the one hand made history and on the other hand ushered in the new data economy. The concept of data protection has emerged across the world. India has not endorsed any particular international approach in the context of data protection. Data protection has not been a priority as far as national legislation is concerned with. India distinctly lacks a dedicated legislation on data protection. However many countries like United Kingdom, European Union have passed influential legislation on pertaining to data protection.

DEFINITION OF DATA PROTECTION

Data Protection has been defined in different manner and styles by different sources and legal entities. According to Collinsdictionary.com, data protection means, "safeguards for individuals relating to personal data stored on computer".

Dataprotection.eu has defined the term data protection as, "a type of privacy protection manifesting in special legal regulation. Data Protection right ensures a person the right of disposal over all data in connection with his personality".

In simple words, data protection can also be defined as protection or safeguarding of data from getting hacked or destroyed or manipulated in any way.

Data becomes extremely significant in our lives. It cannot be denied that we are continuously producing more and more electronic data.

Further Wikipedia defines Information Privacy/Data Protection as, "the relationship between the collection and dissemination of data, technology, the public expectation of privacy and also the legal and political issues surrounding them".

DATA PROTECTION LAW IN INDIA

India has a dedicated mother legislation dealing with data and information in an electronic form i.e. Information Technology Act (I.T), 2000. In India, Cyber Law being the Information

Technology Act, 2000 has various provisions which have a direct impact upon the protection and preservation of data and information. Initially the I.T Act was enacted with the aim to facilitate electronic commerce or e-commerce but as time passed by new innovations were adopted which replaced older technology, which thereby compelled the lawmakers to amend the I.T ACT, 2000.

OBJECTS OF I.T ACT, 2000

The main object of this act is to provide legal recognition to the transactions carried out by the means of electronic data interchange and other means of electronic communication, commonly referred as [i]electronic methods of communication and storage of information to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code 1860 , Indian Evidence Act 1872, the Banker's Book Evidence Act 1891, and the Reserve Bank of India Act 1934 and for matters connected therewith or incidental thereto. Towards that end, the Act stipulates numerous provisions. It aims to provide for a legal framework so that legal sanctity is accorded to all electronic records and other activities carried out of electronic means.

According to SECTION 2 of I.T 2000 has legally defined some important and technical terms under the different terms under the definition clauses; some important terms which are frequently used –

SEC 2(1) (i) defines COMPUTER- "as any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or [ii]optical impulses and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network".

SEC 2(1) (j) defines COMPUTER NETWORK – "means the inter-connection of one or more computers or computer systems or communication device through:

I. The use of satellite, microwave, terrestrial line, wire, wireless or other communication media; and
II. Terminals or a complex consisting of two or more inter-connected computers or communication devices whether or not the inter-connection is continuously maintained"

SEC 2(1) (k) defines COMPUTER RESOURCE as-"means computer, communication device, computer system, computer network, data, computer database or software. The term

'resource' indicates something that is ready for use or available as needed wealth, assets and means to an end. Computer resource can be defined under SEC 2(1) (j) of I.T Act, 2000 to mean the following-

1. A Computer
2. Computer System
3. Computer Network
4. Data
5. Computer database or
6. Software.

SEC 2(1) (k) defines Computer Resource to mean a computer network which is defined under SEC 2(1) (j) as the interconnection of one or more computer through-

1. The use of satellite, microwave, terrestrial line or other communication media ; and
2. Terminals or a complex consisting of two or more interconnected is continuously maintained.

SEC 2(1) (l) defines Computer system as – "a device or collection of devices, including input and output support devices and excluding calculators which are not programmable and [iii] capable of being used in conjunction with external files which contain computer programmes, electronic instructions, input data and output data, that performs logic, arithmetic, data storage and retrieval communication control and other functions".

SEC 2(1) (o) defines Data as- "a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been processed or have been processed in a computer system or [iv] computer network and may be in any form (including computer printouts magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer system".

SEC 2(1)(r) defines Electronic form as-"any information or any means of information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device".

SEC 2(1) (t) defines Electronic record as-"a means of data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche".

Further SEC 2(1) (v) defines Information as-"to include data, text, images, sounds, codes, computer programmes, software and database".

ELECTRONIC RECORDS AND AUTHENTICATION

SEC 4 of I.T ACT, 2000 provides legal recognition to all records, documentations and information in an electronic form. Before I.T Act came into force there was universally no recognition of electronic form. This was because of the absence of any specific enactment of act to deal with it.

SEC 4 of INFORMATION TECHNOLOGY DEALS WITH LEGAL RECOGNITION OF ELECTRONIC RECORDS-

[v]"Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law such requirement shall be deemed to have been satisfied if such information or matter is-

(a) Rendered or made available in an electronic form ; and
(b) Accessible so as to be usable for the subsequent reference".

By a single stroke, Sec 4 has achieved what no other law had achieved earlier. It has made all electronic information, electronic records, electronic documents, databases as legal electronic records which can be duly proved and produced in Court of Law.

Another important question comes up for consideration is whether a contract can come into existence without affixation of Digital/Electronic signatures?

Hence contracts are governed by Indian Contract Act, 1872. It is pertinent to note that Information Technology Act, 2000 has not amended the Indian Contract Act, 1872. The definition of "CONTRACT" is been defined in SEC 2(h) of Indian Contract Act, 1872 as- " An agreement enforceable by law is a contract" and SEC 2(e) defines AGREEMENT as-"Every promise or every set of promises, forming the consideration for each other, is termed as agreement".

The definitions of Indian Contract Act, 1872 have not clarified the modes of agreements, but after the enactment of I.T ACT, 2000, an agreement includes electronic agreements too. Electronic agreements/Contracts concluded by using the electronic means will be valid agreements/contracts.

Under Indian Contract Law, a Contract can be both - written or oral. Oral contracts can be duly proved under law. In the context of the electronic medium, it is possible for two persons sitting at different places to enter into a valid agreement, merely exchanging e-mails/sms which have been digitally signed in.

SEC 3 OF INFORMATION TECHNOLOGY DEALS WITH AUTHENTICATION OF ELECTRONIC RECORDS-

[vi](1) Subject to the provisions of this section any subscriber may authenticate an electronic record by affixing his digital signature.

(2) The authentication of the electronic record shall be effected by the use of asymmetric crypto system and hash function which envelop and transform the initial electronic record into another electronic record.

(3) Any person by the use of a public key of the subscriber can verify the electronic record.

(4) The private key and the public key are unique to the subscriber and constitute a functioning key pair.

SEC 3A of INFORMATION TECHNOLOGY 2000 DEALS WITH ELECTRONIC SIGNATURE-

[vii](1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2) a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which—

(a) is considered reliable; and

(b) may be specified in the Second Schedule.

(2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if—

(a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person;

(b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person;

(c) any alteration to the electronic signature made after affixing such signature is detectable;

(d) any alteration to the information made after its authentication by electronic signature is detectable; and

(e) it fulfils such other conditions which may be prescribed.

SEC 4 of INFORMATION TECHNOLOGY DEALS WITH LEGAL RECOGNITION OF ELECTRONIC RECORDS—

[viii]"Where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied if such information or matter is–

(a) rendered or made available in an electronic form; and

(b) accessible so as to be usable for a subsequent reference".

SEC 5 of INFORMATION TECHNOLOGY DEALS WITH LEGAL RECOGNITION OF ELECTRONIC SIGNATURES-

[ix]"Where any law provides that information or any other matter shall be authenticated by affixing the signature or any document shall be signed or bear the signature of any person, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been satisfied, if such information or matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government".

SEC 5 provides for legal recognition of electronic signatures. Under the existing law, signatures of persons are used as a means of authenticating any information or matter . Therefore, signatures assumes immense significance in the eyes of law.

The lawmakers inserted new provisions in the I.T ACT, 2000 by the way of its I.T (AMENDMENT) ACT, 2008 with the aim to validate e-contract/electronic contracts.

SEC 10A of INFORMATION TECHNOLOGY 2000 DEALS WITH VALIDITY OF CONTRACTS FORMED THROUGH ELECTRONIC MEANS—

[x] "Where in a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic records, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose".

However the term "CONTRACT" has been defined under SEC 2(h) of the INDIAN CONTRACT ACT 1872 which states that an agreement enforceable by law is a contract. Further SEC 10 of INDIAN CONTRACT ACT, 1872 provides essential conditions of a valid contract which are as follows-

1. All agreements are contracts if they are made by the free consent of parties competent to contract, for a lawful consideration and with a lawful object, and are not hereby expressly declared to be void.
2. All agreements are contracts if they are made by the free consent of parties competent to contract, for a lawful consideration and with a lawful object, and are not hereby expressly declared to be void.
3. "Nothing herein contained shall affect any law in force in India, and not hereby expressly repealed, by which any contract is required to be made in writing or in the presence of witnesses, or any law relating to the registration of documents.

Thus for the purpose of valid contracts, an agreement must satisfy the above criteria to called it as a valid one. It provides legality to all kinds of e-contracts/electronic contracts.

SEC 14 OF INFORMATION TECHNOLOGY DEALS WITH SECURE ELECTRONIC RECORDS-

[xi]"Where any security procedure has been applied to an electronic record at a specific point of time, then such record shall he deemed to be a secure electronic record from such point of time to the time of verification."

SEC 15 OF INFORMATION TECHNOLOGY DEALS WITH SECURE ELECTRONIC SIGNATURES-

[xii]"An electronic signature shall be deemed to be a secure electronic signature if—

A. the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and

B. the signature creation data was stored and affixed in such exclusive manner as may be prescribed".

DATA PROTECTION

One of the most effective data protection legal regime is to ensure that adequate protections and security mechanisms are accorded to electronic data so that it becomes more and more difficult for data predators to unauthorized access and target the said data. The Indian Law has come up with the concept of reasonable security practices and procedures which needed to be adopted not just by intermediary but as a legal entity that is dealing, handling and processing the data along with information in electronic form.

COMPENSATION FOR FAILURE TO PROTECT DATA-India pioneered the BPO i.e. BUSINESS PROCESS OUTSOURCING industry, providing a fertile framework for processing of outside information within India. As time passed by India has seen the emergence of various legal challenges pertaining to preservation and protection of sensitive personal data and information.

SEC 43 of INFORMATION TECHNOLOGY ACT DEALS WITH PENALTY AND COMPENSATION FOR DAMAGE TO COMPUTER, COMPUTER SYSTEM, ETC.

[xiii]"If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network, or computer resource —

1. accesses or secures access to such computer, computer system or computer network;
2. downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
3. introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
4. damages or causes to be damaged any computer, computer system or computer network, data, computer data base or any other programmes residing in such computer, computer system or computer network;
5. disrupts or causes disruption of any computer, computer system or computer network;
6. denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (g) provides any assistance to any

person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder;

7. charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation to the person so affected.
8. destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
9. steel, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage";

Explanation.

For the purposes of this section:

1. "computer contaminant" means any set of computer instructions that are designed —
   - to modify, destroy, record, transmit data or programme residing within a computer, computer system or computer network; or
   - by any means to usurp the normal operation of the computer, computer system, or computer network;
2. "computer data base" means a representation of information, knowledge, facts, concepts or instructions in text, image, audio, video that are being prepared or have been prepared in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
3. "computer virus" means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;
4. "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.
5. "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

SEC 43A of INFORMATION TECHNOLOGY ACT DEALS WITH COMPENSATION FOR FAILURE TO PROTECT DATA-

[xiv]"Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected"

The first thing to note about this section that SEC 43A of I.T ACT, 2000 is that it is applicable to that body corporate which is possessing, dealing or handling any sensitive personal data or information . SEC 43A provides the body corporate to mean the following-

1. Any Company,
2. A Firm;
3. Sole proprietorship;
4. Other association of individual engaged in commercial or professional activities.

For the purpose of appreciating this portion of Sec 43A it also means the following-

a. Security practices and procedures designed to protect sensitive personal data or information from authorised access;
b. Security practices and procedures designed to protect sensitive personal data or information from getting damage;
c. Security practices and procedures designed to protect sensitive personal data or information from unauthorised use;
d. Security practices and procedures designed to protect sensitive personal data or information from unauthorised modification;
e. Security practices and procedures designed to protect sensitive personal data or information from authorised disclosure;
f. Security practices and procedures designed to protect sensitive personal data or information from unauthorised impairment.

SENSITIVE PERSONAL DATA OR INFORMATION

Sensitive personal data or information of a person means such personal information which consists of information relating to-

1. Password
2. Financial information such as Bank Account or Credit card details
3. Physical, physiological and mental health conditions
4. Sexual orientation
5. Medical Records & History
6. Biometric Information

While SEC 43A of the I.T ACT, 2000 provides for the civil exposure to pay for the damages by the way of compensation, it also needs to be noted that in case the reasonable security practices and procedures are specified in a contract being a lawful agreement and in case of breach of lawful agreement or contract then SEC 72A of INFORMATION TECHNOLOGY, 2000 would also have applicability.

The another part of SEC 43A of the INFORMATION TECHNOLOGY ACT , 2000 is it also deals with the negligence of the body corporate in implementing and maintaining reasonable security practices and procedures causing wrongful loss or wrongful gain to another person. It is pertinent to note that the term "wrongful loss" or "wrongful gain" is not defined under I.T ACT, 2000 but it has widely defined in INDIAN PENAL CODE, 1860.

SEC 72A of INFORMATION TECHNOLOGY, 2000 reads as-

[xv]"Punishment for disclosure of information in breach of lawful contract.–Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both".

Technologies have now made it possible for people to communicate, exchange our thoughts in process of email or other social media. Consequently, the increase usage of electronic devices has now changed the way people perceive, think, govern as well as do commerce.

Today electronic ecosystem and digital devices are increasingly being used not only for accessing internet, sending emails but also for educational and entertainment purposes too.

SEC 79 OF INFORMATION TECHNOLOGY, 2000 reads as-

[xvi]"(1) Notwithstanding anything contained in any law for the time being in force but subject to the provisions of sub-sections (2) and (3), an intermediary shall not be liable for any third party information, data, or communication link made available or hasted by him.

(2) The provisions of sub-section (1) shall apply if—

(a) the function of the intermediary is limited to providing access to a communication system over which information made available by third parties is transmitted or temporarily stored or hasted; or

(b) the intermediary does not—

(i) initiate the transmission,

(ii) select the receiver of the transmission, and

(iii) select or modify the information contained in the transmission;

(c) the intermediary observes due diligence while discharging his duties under this Act and also observes such other guidelines as the Central Government may prescribe in this behalf.

(3) The provisions of sub-section (1) shall not apply if—

(a) the intermediary has conspired or abetted or aided or induced, whether by threats or promise or authorise in the commission of the unlawful act;

(b) upon receiving actual knowledge, or on being notified by the appropriate Government or its agency that any information, data or communication link residing in or connected to a computer resource controlled by the intermediary is being used to commit the unlawful act, the intermediary fails to expeditiously remove or disable access to that material on that resource without vitiating the evidence in any manner.

Explanation.—For the purposes of this section, the expression "third party information" means any information dealt with by an intermediary in his capacity as an intermediary."

SEC 79 is a code in its own self. This is so because this is the only relevant section which provided complete detailed provisions pertaining to the liability of intermediaries and other

service providers for third party data or information, which fall within the parameters of the applicability of the I.T ACT, 2000.

[xvii]AMENDMENTS AS INTRODUCED BY THE IT AMENDMENT ACT, 2008

Section 10A was inserted in the IT Act which deals with the validity of contracts formed through electronic means which lays down that contracts formed through electronic means "shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose".

The following important sections have been substituted and inserted by the IT Amendment Act, 2008:

1. Section 43A – Compensation for failure to protect data.

2. Section 66 – Computer Related Offences

3. Section 66A – Punishment for sending offensive messages through communication service, etc. (This provision had been struck down by the Hon'ble Supreme Court as unconstitutional on 24th March 2015 in Shreya Singhal vs. Union of India)

4. Section 66B – Punishment for dishonestly receiving stolen computer resource or communication device.

5. Section 66C – Punishment for identity theft.

6. Section 66D – Punishment for cheating by personation by using computer resource.

7. Section 66E – Punishment for violation for privacy.

8. Section 66F – Punishment for cyber terrorism.

9. Section 67 – Punishment for publishing or transmitting obscene material in electronic form.

10. Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.

11. Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.

12. Section 67C – Preservation and Retention of information by intermediaries.

13. Section 69 – Powers to issue directions for interception or monitoring or decryption of any information through any computer resource.

14. Section 69A – Power to issue directions for blocking for public access of any information through any computer resource.

15. Section 69B – Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security.

16. Section 72A – Punishment for disclosure of information in breach of lawful contract.

17. Section 79 – Exemption from liability of intermediary in certain cases.

18. Section 84A –Modes or methods for encryption.

19. Section 84B –Punishment for abetment of offences.

20. Section 84C –Punishment for attempt to commit offences.

LIABILITY FOR BREACH OF E-DATA CIVIL OR CRIMINAL

SEC 43 of the Information Technology, 2000 is an extremely important provision under the I.T ACT, 2000 as it deals with penalty and compensation for damage to computer, computer system, data or computer database information resident in such computer or computer system. The law of tort in the country is not well developed even after more than 60 years of independence and not much progress has been made in this discipline of law. One of the primary objects of any data protection legal regime is to ensure that electronic data should not be able to accessed or used in an unauthorised manner.

INDIAN PENAL CODE

The Indian Penal code doesn't specifically address breaches of knowledge privacy. Under the Indian legal code, liability for such breaches must be inferred from related

crimes. Section 403 of the IPC, 1860 imposes criminal penalty for dishonest misappropriation or conversion of "movable property" for one's own use.

INTELLECTUAL PROPERTY LAWS

The Indian Copyright Act prescribes mandatory punishment for piracy of copyrighted matter commensurate with the gravity of the offence. Section 63B of the Indian Copyright Act provides that a person who knowingly makes use on a computer of an infringing copy of computer virus shall be punishable for a minimum period of six months and a maximum of three years in prison.

CONCLUSION

The lack of a comprehensive legislation for privacy and data protection has been a matter of concern. Even though the data protection laws don't seem to be specifically laid down in any statute so far, the Indian industry have begun the method of sensitising the government and therefore the masses regarding the importance of privacy.

[i] http://digitalindialaw.com/act-2000/
[ii] http://ipindia.nic.in/writereaddata/portal/images/pdf/revised_guidelines_for_examination_of_computer-related_inventions_cri_.pdf
[iii] http://ipindia.nic.in/writereaddata/portal/images/pdf/revised_guidelines_for_examination_of_computer-related_inventions_cri_.pdf
[iv] https://indiankanoon.org/doc/1752240/
[v] https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf
[vi] https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf
[vii] https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf
[viii] https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf
[ix] https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf
[x] https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf
[xi] https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf
[xii] https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf
[xiii] https://cis-india.org/internet-governance/resources/section-43-it-act.txt
[xiv] https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf
[xv] https://indiacode.nic.in/bitstream/123456789/1999/3/A2000-21.pdf
[xvi] https://cis-india.org/internet-governance/resources/section-79-information-technology-act
[xvii] https://www.mondaq.com/india/Privacy/655034/Data-Protection-Laws-In-India--Everything-You-Must-Know