The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2024

Editor-in-Chief – Prof. (Dr.) Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

Cyber Law- An Introduction to Various Act and Rules Pertaining to Cyber Law

Abstract: The swift advancement of technology has resulted in a multifaceted network of legal concerns pertaining to the internet. Cyberlaw is the umbrella term for a variety of laws, rules, and policies aimed at resolving these issues and controlling actions in the digital sphere. The goals, provisions, and ramifications of numerous laws and regulations that are relevant to cyber law are thoroughly examined in this research article. It seeks to improve knowledge of the laws regulating cyberspace and how they affect people, companies, and society at large through a thorough analysis.

Introduction: The arrival of the digital era has completely changed how we engage with information, communicate, and do business. But despite all of its advantages, the digital world has also resulted in a number of difficult legal issues. Cyberlaw is the collection of legal rules and guidelines that control online behaviour and transactions. It is often referred to as Internet law or digital law. It covers a broad range of topics, including as cybercrimes, online commerce, data privacy, cybersecurity, and intellectual property rights.

This study examines the major laws and regulations that establish the framework for cyber law. It gives a summary of their goals, reach, and importance in controlling conduct and guaranteeing responsibility in cyberspace. This study seeks to clarify these legal systems by closely researching them and the evolving nature of cyber law and its implication to various stakeholders.

Cyber law on India [Law on Internet]:

1. Authentication of Electronic Records and Electronic Governance:

Generally, law does not favour any particular mode of execution of commercial transactions save in exceptional situations where it is expressly provided that a commercial transaction be in writing and signed by the parties so as to be enforceable. This document is the record of the parties' agreement and the signature is the stamp of a person's identity, and the marks his intention to commit himself legally. The commercial community has found these two requirements convenient to create legal relationship and forms now a well established mode of executing business transactions.

Authentication of Electronic Records: Every user of the internet whether he is an originator or addressee is always concerned about the security, confidentially and integrity of the electronic record and its authenticity is the concern of the addressee. Any person is interested in executing commercial relationship over internet will always be particular about: 1. Who sent this message? 2. When was it sent? 3. To whom was it sent? 4. Was it received? 5. When was it received? 6. Did it arrive in the same form in which it was sent? 7. Has it remained confidential?

Data security is the protection of data against accidental or intentional destruction, disclosure or modification. Computer security refers to the technological safeguards and managerial procedures, which can be applied to computer hardware, programmes, and data to assure that organization assets and individual privacy are protected.

Confidentially is a concept that applies to data. It is the status accord to data, which has been agreed upon between the persons or person and organization furnishing the data and the organization receiving it, and which describes the degree of protection to be provided.

Digital Signature: A digital signature can be defined as a short unit of data that bears a mathematical relationship to the data in the document's context and provides assurance to the recipient that the data is authentic. It also means authentication of any electronic record by a subscriber by applying asymmetric cryptosystem and hash function, which envelop and transform the initial record into another electronic record. The electronic record means data, record or data generated, image or sound stored, received or sent in an electronic form. The electronic form with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory or similar device. The word "data" and "record" in the definition of "electronic record" has to be interpreted liberally. Otherwise, the definition will be unnecessarily restrictive in scope, as it does not mention, for example, text, graphics, video or multimedia services. However, one may argue that the definition of the electronic form widens the scope of the definition of the "electronic record" by including the words "information". These two definitions have to be read conjunctively and the words "any information" used in the definition have to be construed with reference to the content provided in the definition of "electronic records".

Electronic Governance: Legal Recognition of Electronic Records:

The two main legal impediments of e-commerce and governance were the requirements of recording an information on tangible medium and handwritten signature. The existing legal regime, throughout the globe, did not originally provide express provision for the electronic communication, as these communications could not be foreseen.

To overcome these legal barriers and to facilitate e-commerce and e-governance, section 4 of the IT Act provides that where any law requires that an 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.

The legal requirements that any information be in writing or in the type written or printed form shall be met if that information is in electronic form, satisfying the criteria set out in section 4. The IT Act makes it clear that section 4 will apply notwithstanding anything contained contrary in any other law. This provision will have overriding effect over other laws as the IT Act is a special legislation dealing with electronic transactions. All other legislations including special legislation, like consumer protection Act, 1986, will become general legislation for the purpose of the electronic communications.

However, the above rules does not apply to:

(a) Will
(b) A negotiable instrument except in case electronic cheque;
(c) Trusts and power of attorney (except constructive and resulting trusts);
(d) Contracts for the disposition of "immovable property", or any interest in such property;
(e) Document of title;
(f) Any other document notified by the Central government.

2. Electronic Commerce: Contracts by electronic interchange:

Electronic data interchange means the electronic transfer from computer to computer of information using an agreed standard to structure the information. It is also defined as the electronic interchange of machine processable structure data which has been formatted according to agreed standards and which can be transmitted directly between different computer systems with the aid of telecommunication interface with or without human intervention.

Before the advent of the internet, business communities used to execute their contracts by electronic data interchange. It facilitates direct electronic exchange of business information between computers in a computer processable format and is generally used by the parties having continuing business relationship. These parties, before establishing any contractual relationship, generally exchange an agreement called as "trading partner agreement" in which the details about the warranties, disclaimers, liabilities and the relevant rules that will be applicable in case of dispute, are mentioned. In pursuance to trading partner agreement parties transmit through EDI, purchase orders, acceptances and invoices.

Cyber contracts: Internet enjoys the luxury of a wide variety of communication methods. Since technology is continuously changing, new methods of

communication are evolving which make their categorization difficult. The communication methods, presently possible, are e-mail, listserv, newsgroup, real time communication and world wide web(www). At present the commonly used methods of communication of business information via the Internet, are e-mail and commercial websites. The other methods make disclosure of information possible to the public, which make them infeasible for executing bipartite contracts.

Legal Validity of Electronic Contracts: one of the objectives of the original IT Act spelt in the statement of objects and reasons is to legalize e-commerce. This objective is reiterated in the objective of the IT (Amendment) Act,2008 also. Surprisingly, there was no expression provision in the original IT Act validating contracts executed electronically. This lapse in the model Law which forms the basis of the IT Act as claimed in its statement of objects and reasons.

The IT (Amendment) Act now provides that where in a contract formation, the communication of proposal, the acceptance of proposal, the revocation of proposal and acceptance, as the case may be, expressed in the electronic form or by means of an electronic record, such contract shall not to be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose.

3. **Personal Data Protection Bill, 2019, Act:** The PDPB regulates the processing of "personal data" which is basically any data that can identify an individual. The Bill applies to any private/public body or corporation incorporated in India. It also applies to any overseas corporation dealing with personal data of Indian entities. Data, as per the Bill, should be processed in a 'fair and reasonable' manner. The bill also includes "sensitive personal data" which requires a more severe level of supervision and regulation. Sensitive personal data includes financial data, biometric data, data about caste, religion and political beliefs etc. The Bill grants an individual certain rights during data processing. Data fiduciaries/processors are under certain obligations to maintain definite standards for data protection. However, exemptions are provided for some entities and certain kinds of data processing.

The "Right to be forgotten" Personal Data Protection Bill, 2019, Act

The following are the provisions in the Personal Data Protection Bill, 2019 that concern the right to be forgotten:

- Chapter V of the Personal Data Protection Bill mentions the right to be forgotten as a right of a data principal under Clause 20. According to Clause 20(1), the following are the grounds for claiming the right to restrict disclosure of any personal data:

1. once the purpose has been achieved, or
2. when the data principal's consent has been withdrawn, or

3. when the disclosure was made in an unlawful manner, the data principal can restrict the disclosure of the concerned personal data.

- The Bill also provides for the appointment of an Adjudicating Officer by the Union Government. In order to avail the right under Clause 20, it is necessary for the data principal to show that his claim meets one of the three aforementioned conditions to the Adjudicating Officer and demonstrate how his right to be forgotten overrides the right to information and freedom of speech and expression of other citizens, as per Clause 20(2).
- Clause 20(3) lays down the factors that must be considered by the Adjudicating Officer before issuing an order on the claim of right to be forgotten of a data principal, and they are the following:

1. Sensitivity of the personal data;
2. The extent of disclosure and accessibility that the data principal seeks to restrict;
3. Importance of the data principal's role in public;
4. Relevance of the personal data to the public;
5. The nature of the disclosure and activities of the data fiduciary, especially whether the data fiduciary systematically facilitates access to personal data and whether the restriction of the disclosure would significantly affect them.

- As per Clause 20(4), if any other person finds the order unreasonable and uncalled for, can apply for a review of the order to the Adjudicating Officer.
- Data principals can also appeal against the decision of the Adjudicating Officer to the appellate board, as per Clause 20(5).
- As per Clause 21, the right to be forgotten, unlike the other rights of the data principal, does not require the data principal to request the data fiduciary to restrict or prevent the disclosure of any personal data. The data principal is only required to make an application to the Adjudication Officer to enforce this right.

The Personal Data Protection Bill, 2019 restricts the right to be forgotten to only the disclosure of personal data. The Draft Data Protection Bill, suggests including the processing of personal data as well to the scope of the right to be forgotten. This suggestion may or may not be taken into consideration.

Provision of Personal Data Bill 2019, Act

There are also some provisions in the Bill that essentially supplements the right to be forgotten, which are the following:

- Clause 18 deals with the 'right to correction and erasure', which tends to slightly overlap with the right to be forgotten. This includes correction of inaccurate or misleading personal data and erasure of personal data that is no longer necessary for the purpose for which it was processed. Wherever the data fiduciary makes such a correction or erasure, the individuals and entities to whom such data was disclosed must be notified by the data fiduciary.

- As per Clause 9, a data fiduciary cannot retain any personal data beyond the particular period for which it was required, unless it is explicitly consented to by the data principal or there is compulsion by law. Data fiduciaries are also obligated to undertake a periodic review to determine whether it is necessary to retain the personal data or not.
- Clause 36(b) states an exception to the right to restrict disclosure of personal data, wherever the personal data is required for enforcing a legal right or claim, to defend charges, for receiving legal advice, etc.

4. **Intellectual Property Rights Law in Cyber Law:** Intellectual Property encompasses the rights involving the original expression of work and inventions in a tangible form that has the capacity to be duplicated multiple times. The protection of such property against unfair competition is essential to the rights of the human endeavour in its intellectually innovative form. Resources and skills are invested in intellectual property, where the creator stimulates research and development to achieve economic development and technological advancements for the country and society at large. Intellectual property rights engrossed itself as a strong tool to keep intellectual endeavours intangible medium.

With the onset of cyber technology, global markets have benefited copyright owners. This is true, but beyond the considered benefits, the risks loom large, if the consequences of emerging trends are left unaddressed. Like any desired invention, cyber technology has its pitfalls. Unlicensed use of trademarks, trade names, service marks, images, codes, audios, videos, literature content by way of illegitimate practices of hyperlinking, framing, meta-tagging, spamming, and the list is endless, emerge as the regular infringements to the new universe of intellect and skills in the cyber domain.

Protection of Intellectual Property: It is clear from the above that protection of data in cyberspace accompanies myriad issues, but the common point of interpretation segregating the levels for copyright infringement may be based on ‘intent’. Dishonest intentions ought to lead to reading the legal and regulatory provisions in more stringent forms to derive the capability to disallow any of the copyright infringements seemingly permissible or at the least sitting over the fence on the superficial. Rampant violations of copyright rights on the internet affecting a larger mass, call for sharper legal protections. The responsibility is not restricted to the lawmakers or the law enforcement systems, but also to the copyright owners and software companies. Copyright notices and displays of licenses and warnings with limited permissions on the websites by the copyright owners need to be ensured. Blanket prohibitions may no longer serve the purpose, as technology is rapidly evolving and copyright may not seem to be affected if judged cursorily, especially where control over serious indirect violations are the emerging possibilities.

Special Rights of Broadcasting Organization and Performers’ Rights: Broadcasting organization, such as radio and television also popularly known as electronic media play vital role in the society. They are powerful media for entertainment, dissemination of information, knowledge, art and culture. The Copyright

(Amendment) Act, 1994 has substituted section 37 and made provision for special right known as “broadcast reproduction right”

Broadcast Reproduction Rights and Infringement (Section 37):

(a) rebroadcasting the broadcast

(b) causes the broadcast to be heard or seen by the public on payment of any charges;

(c) makes any sound recording or visual recording of the broadcast;

(d) sells or hires to the public or offers for sale or hire, any such sound recording or visual recording.

Conclusion: In the realm of cyber law is a dynamic and critical aspect of modern legal frameworks, especially given the rapid evolution of technology and its profound impact on society. This research article delves into various acts and rules pertinent to cyber law, shedding light on key areas such as authentication of electronic records, electronic commerce, personal data protection, and intellectual property rights.

The analysis of India's cyber law landscape reveals a concerted effort to adapt legal frameworks to the digital age. From provisions ensuring the legal recognition of electronic records to regulations governing electronic commerce contracts and personal data protection, India's legal system demonstrates a proactive approach to address the complexities of cyberspace.

Furthermore, the emphasis on intellectual property rights underscores the importance of safeguarding creators' innovations while navigating the challenges posed by digital infringement. The discussion on special rights for broadcasting organizations also highlights the evolving nature of media and the need for legal frameworks to keep pace with technological advancements.

In essence, the study underscores the significance of cyber law in fostering a secure and responsible digital environment. It calls for continuous evolution and harmonization of legal frameworks at both domestic and international levels to address emerging challenges and promote innovation while protecting individual rights and societal interests in cyberspace.[i]

---

i ***Adhila Muhammed Arif*****,** Personal Data Protection Bill, 2019 and the right to be forgotten, **Personal Data Protection Bill, 2019 and the right to be forgotten - iPleaders, March 11, 2022**

ii ***Divjot Arora,*** Analysis of laws/regulations pertaining to digital Intellectual Property Rights, **Analysis of laws/regulations pertaining to digital Intellectual Property Rights - iPleaders, March27, 2021**

iii Andreas Rahmatian, Cyberspace and Intellectual Property Rights, **Cyberspace and Intellectual Property Rights by Andreas Rahmatian :: SSRN, June 15, 2015**

iv *Apoorva Dixit, Role of intellectual property in Cyber law,* **Role of Intellectual Property in Cyber Law - Enhelion Blogs, September 1, 2022**