iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 12 **Issue:** I **Month of publication:** January 2024

DOI: https://doi.org/10.22214/ijraset.2024.58030

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue I Jan 2024- Available at www.ijraset.com

AI and Cyber Security with Reference to Information Technology Act, 2000 and other Laws in India

Dr. Swapnil Choudhary
Assistant Professor of Law, VES Law College, Mumbai

Abstract: ***The term artificial intelligence (AI) is prominent in today's world of technology. In so many ways, it is still a developing science considering the problems presented by the twenty-first century. AI use has been established in daily life. Since AI has such a significant influence on human existence now, it is difficult to comprehend a world without it. Simply define, artificial intelligence (AI) is the study of how people think, work, learn, and decide in every situation in life, whether it is connected to problem-solving, learning something new, thinking logically, or coming up with a solution, etc. If Artificial Intelligence mostly connected with the daily life of the human being it must be protect the relationship between the human being and society people and there should be remedy to the peoples in case of violation of laws by AI machines.***

Cyber security and cyber law already new concept in the development of modern laws of the country. Cybercrimes are becoming common and frequently reported in the news. It is a global challenge, not simply one that affects one nation. AI is meaningless without strong security measures since it may be readily accessible by outsiders. Governments, banks, and global corporations now face a serious threat because of cyber security threats. Hackers use a lot of private and business data to their advantage, which poses a serious threat to the online community.

Keyword: Cyber Security, Computer Program, Information technology, Modern Laws in India, Criminal Liability.

I. INTRODUCTION

This modern world is called the world of Information Technology and Cyber culture out of that the new concept innovated by the Scientists (AI). Artificial intelligence (AI) is the ability of machines to replicate or enhance human intellect, such as reasoning and learning from experience. Artificial intelligence has been used in computer programs for years, but it is now applied to many other products and services. For example, some digital cameras can determine what objects are present in an image using artificial intelligence software. In addition, experts predict many more innovative uses for artificial intelligence in the future, including smart electric grids.[1]

Artificial Intelligence is the most trending field of computer science. However, with all the new technology and research, it's growing so fast that it can be confusing to understand what is. Furthermore, there are many different fields within AI, each one having its specific algorithms. Therefore, it's essential to know that AI is not a single field but a combination of various fields.[2]

The present article aims to cover the following areas:

1) To find the law in the legal statutes, subordinate legislations, andjudicial precedents:

The present study examines the following aspects of the law inspecific relation to Cyber Crime:

a) Information Technology Act, 2000
b) Indian Penal Code, 1860 (relevant provisions)
c) Indian Evidence Act, 1872
2) Aims at consistency and certainty of laws.
3) To some extent look into the purpose and policy of law that exists. The study examines the intent and purpose of the enactment of cyber laws and the social purpose behind it.

The Information Technology Act, 2000 (IT Act, 2000) is an outcome of theresolution dated 30th January 1997 of the General Assembly of the United Nations, which adopted the Model Law on Electronic Commerce, adopted the Model Law on Electronic Commerce on International Trade Law.

[1] Wolfgang Ertel; 'Introduction to Artificial Intelligence' Springer Publications Edn.2018
[2] Rajiv Kapur; AI made simple:A beginers Guide to Generative Intelligence;Rinity media Publishers Edn.2023

©IJRASET: All Rights are Reserved

This resolution recommended, inter alia, that all states give favorable consideration to the said Model Law while revising enacting new law, so that uniformity may be observed in the laws of the various cyber-nations, applicable to alternatives to paper based methods of communication and storage of information. The Department of Electronics (DoE) in July 1998 drafted the bill. However, it could only be introduced in the House on December 16, 1999 (after a gap of almost one and a half years) when the new IT Ministry was formed. It underwent substantial alteration, with the Commerce Ministry making suggestions related to e-commerce and matters pertaining to World Trade Organization (WTO) obligations. The Ministry of Law and CompanyAffairs then vetted this joint draft.[3]

After its introduction in the House, the bill was referred to the 42-member Parliamentary Standing Committee following demands from the Members. The Standing Committee made several suggestions to be incorporated into the bill. However, only those suggestions that were approved by the Ministry of Information Technology were incorporated. One of the suggestions that was highly debated upon was that a cyber café owner mustmaintain a register to record the names and addresses of all people visiting his café and also a list of the websites that they surfed. This suggestion was made as an attempt to curb cybercrime and to facilitate speedy locating of a cyber-criminal. However, at the same time it was ridiculed, as it would invade upon a net surfer's privacy and would not be economically viable.[4]

The Union Cabinet approved the bill on May 13, 2000 and on May 17, 2000, both the houses of the Indian Parliament passed the Information Technology Bill. The Bill received the assent of the President on 9th June 2000 and came to be known as the Information Technology Act, 2000. The Act came into force on 17th October 2000. The Information Technology Act, 2000 is India's mother legislation regulating the use of computers, computer systems and computer networks as also data and information in the electronic format. This legislation has touched varied aspects pertaining to electronic authentication, digital (electronic) signatures, cybercrimes and liability of network service providers.

The objective of the IT Act, 2000 as stated in the preface to the Act itself is as follows:
"to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper- based 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, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto."

The Act essentially deals with the following issues:
1) Legal Recognition of Electronic Documents
2) Legal Recognition of Digital Signatures
3) Offenses and Contraventions
4) Justice Dispensation Systems for cybercrimes.

II. CYBER CRIME AND CYBER SECURITY

India does not have a dedicated cyber security law. The IT Act, 2000 read with the rules and regulations framed thereunder also deals with cyber security and the cybercrimes associated therewith. Thus, IT Act, 2000 only provides legal recognition and protection for transactions carried out through electronic data interchange and other means of electronic communication, but it also contains rules that are aimed at safeguarding electronic data, information or records, and preventing unauthorized or unlawful use of a computer system and proper conduct and procedure. Rules framed by the Central Government in exercise ofits rule making power under Section 87 of the IT Act, 2000 are as follows:

1) *Information Technology (The Indian Computer Emergency Response Teamand Manner of Performing Functions and Duties) Rules 2013(the CERT Rules):*

These rules provide for the establishment of the Computer Emergency Response Team (CERT-In) as the nodal agency responsible for the collection, analysis, anddissemination of information on cyber incidents and taking emergency measures to contain such incidents.

[3] Jank Minker: 'Logic based Artificial Intelligence' Springer Publications,Edn.2000
[4] David Brown: 'Artificial Intelligence' Kindle Edn.

2) Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules 2011 (the SPDI Rules):

These rules prescribe reasonable security practices and procedures to be implemented for collection and the processing of personal or sensitive personal data.

These rules require specific information security measures to be implemented by organizations that have protected systems, as defined under the IT Act. Moreinformation on protected systems is provided in 'Scope and jurisdiction.'

3) Information Technology (Intermediaries Guidelines) Rules,2011 (the Intermediaries Guidelines):

These rules require intermediaries to implement reasonable security practices and procedures for securing their computer resources and information contained therein. These guidelines have been superseded last year by the 2021 Rules:

4) Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Under the newly framed Rules intermediaries are supposed to provide a two-level in-house complaints adjudication procedure for self-regulation.

III. ACTS AMENDED BY THE INFORMATION TECHNOLOGY ACT,2000:

The IT, Act 2000 also amended existing laws as follows:

A. The Indian Penal Code,1860

Normally referred to as the IPC, this is a very powerful legislation and probably the most widely used in criminal jurisprudence, serving as the main criminal code of India. Enacted originally in 1860 and amended many times since, it covers almost all substantive aspects of criminal law and is supplemented by other criminal provisions. In independent India, many special laws have been enacted with criminal and penal provisions which are often referred to and relied upon, as an additional legal provision in cases which refer to the relevant provisions of IPC as well IT Act, 2000 has amended the sections dealing with records and documents in the Indian Penal Code, 1860 (IPC, 1860) by inserting the word '**electronic**' thereby treating the electronic records and documents on a par with physical records and documents. The sections of the IPC, 1860 which deal with false entry in a record orfalse document (such as sections 192, 204, 463, 464, 464, 468 to 470, 471, 474,476 etc) have all been amended to include 'electronic record' and 'electronic document' within the ambit of crimes under the IPC, 1860. Accordingly, all crimespertaining to electronic records and electronic documents are crimes just likephysical acts of forgery or falsification of physical records.[5]

In practice, however, the investigating agencies file the cases quoting the relevant sections from IPC, 1860 in addition to those corresponding in IT Act, 2000 like offences under IPC 463,464, 468 and 469 read with the ITA/ITAA Sections 43 and 66, to ensure that a conviction can be secured in at least either of the two (or both) the legislations easily.

B. The Indian Evidence Act 1872

Prior to the passing of IT Act 2000, all evidence presented in a Court was supposed to be in the physical form only. However, with the IT Act 2000 giving legal recognition to electronic records and documents, it has become necessary that the provisions for evidentiary legislation also be amended in tune therewith.Accordingly in the definitions part of the Indian Evidence Act itself, the term "all documents including electronic records" were substituted. Words like 'digital signature', 'electronic form', 'secure electronic record' 'information' as usedin the IT Act, 2000 were inserted to make them part of the evidentiary mechanism during any kind of trial.

The IT Act, 2000 lead to amendment of the Indian Evidence Act, 1872 with the insertion of Section 65-B. This section describes evidence produced from a computer or electronic device and lays down that any information contained in an electronic record printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be treated like a document, without further proof or production of the original, if the conditions like these are satisfied:

1) The computer output containing the information was produced by the computerduring the period over which the computer was used regularly by lawful persons;
2) The information derived was regularly fed into the computer in the ordinarycourse of the said activities; and
3) Throughout the material part of the said period, the computer was operatingproperly and a certificate signed by a person responsible etc.

[5] S.N. Misra; 'Indian Penal Code' Central Law Publication, 23rd Edn. 2023

To put it in simple terms, courts can now take in evidence information in the form of print outs from computers or electronic storage devices as long as the conditionsstipulated in Section 65-B are complied with.

C. The Bankers Books Evidence (BBE) Act 1891

The Amendment to this Act has been included as the third schedule in IT Act, 2000. Prior to the passing of IT Act, 2000 any evidence from a Bank that was required to be produced in a Court necessitated production of the original ledger or other register for verification at some stage with the copies of such ledger or register being retained in the Court records as Exhibits. With the passing of the IT Act, 2000 the Section 2(3) of the Act pertaining to the definition of Banker'sBooks stood amended as: "*'Bankers' books' include ledgers, day-books, cash- books, account-books and all other books used in the ordinary business of a bank whether kept in the written form or as printouts of data stored in a floppy, disc, tape or any other form of electro-magnetic data storage device".*

Thus, when the Bankers' Books consist of printouts of data stored in a floppy, disc, tape etc. a printout of such entry certified in accordance with the provisions to Section 65-B of the Indian Evidence Act, 1872 will make it legally admissible in evidence.

D. The Reserve Bank of India Act,1934

The IT Act, 2000 brought about amendment in section 58 of the Reserve Bank of India Act, 1934 through the addition of a clause (pp) to Section 58(2), relating to the regulation of fund transfer through electronic means between the banks or between the banks and other financial institutions, including the laying down of the conditions subject to which banks and other financial institutions shall participate in such fund transfers, the manner of such fund transfers and the rights and obligations of the participants in such fund transfers.[6]

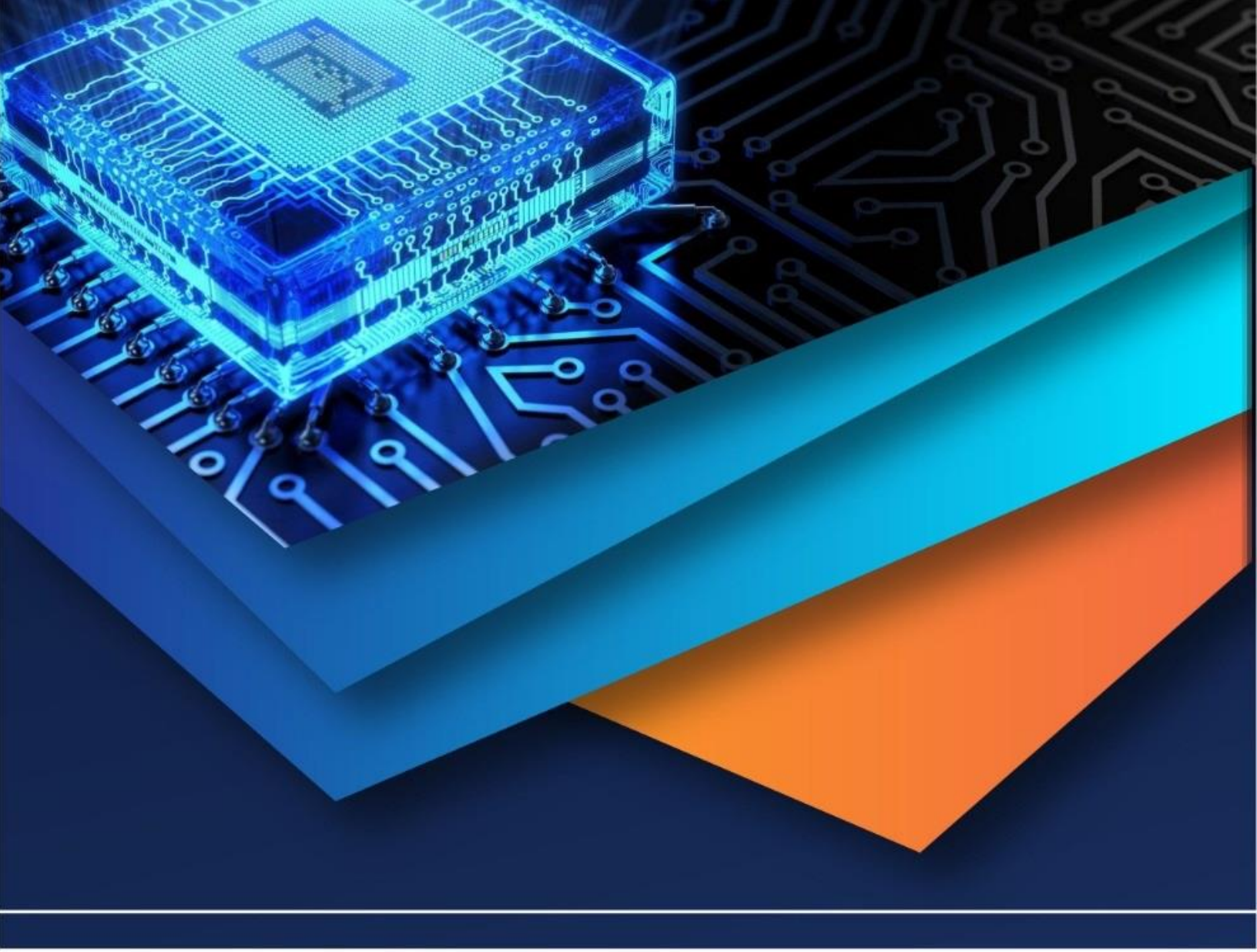
IV. CONCLUSION

In view of the analysis of the scope of the Artificial Intelligence and Cyber Security in India the above-mentioned laws are sufficient but with respect to future of IT sector in India there should be special laws must be enacted by the Indian Legislature for the purpose of Maintenance of rights of the Individuals and companies.

WEBLIOGRAPHY

[1] Ministry of Electronics & Information Techology (Mity): https://www.meity.gov.in/
[2] National Crime Records Bureau:
[3] Indian Cyber Crime Coordination Center (I4C) Scheme: https://www.mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C- Scheme
[4] National Cyber Crime Training Center: https://cytrain.ncrb.gov.in/
[5] Mumbai Police Cyber Cell: https://mumbaipolice.gov.in/CCC
[6] Wikipedia: https://en.wikipedia.org/wiki/Main_Page
[7] Vikaspedia: https://vikaspedia.in/
[8] Indian Computer Emergency Response Team: https://www.cert-in.org.in/
[9] Crime & Criminal Tracking Network & Systems: https://ncrb.gov.in/en/crime-and-criminal-tracking-network-systems-cctns
[10] National Digital Police Portal: https://digitalpolice.gov.in/

[6] Reserve Bank Of India Notifications and Guidelines,2023



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)