LAB Manual

PART A

(PART A: TO BE REFFERED BY STUDENTS)

**Experiment No: 10**

**A.1 Aim:**

To study cyber laws in India.

**A.2 Prerequisite:**

Fundamentals of web security.

**A.3 Outcome:**

**After successful completion of this experiment students will be able to** 1. Understand cyber security laws.

**A.4 Theory:**

We can categorize Cyber crimes in two ways

The Computer as a Target :-using a computer to attack other computers.

e.g. Hacking,Virus/Worm attacks,DOS attack etc.

computer as a weapon :-using a computer to commit real world crimes.

e.g. Cyber Terrorism, IPR violations,Credit card frauds,EFT frauds, Pornography etc.

Cyber law (also referred to as cyberlaw) is a term used to describe the legal issues related to use of communications technology, particularly "cyberspace", i.e. the Internet. It is less a distinct field of law in the way that property or contract are as it is an intersection of many legal fields, including intellectual property, privacy, freedom of expression, and jurisdiction. In essence, cyber law is an attempt to integrate the challenges presented by human activity on the Internet with legacy system of laws applicable to the physical world.

The IT Act 2000 attempts to change outdated laws and provides ways to deal with cyber crimes. We need such laws so that people can perform purchase transactions over the Net through credit cards without fear of misuse. The Act offers the much-needed legal framework so that information is not denied legal effect, validity or enforceability, solely on the ground that it is in the form of electronic records.

In view of the growth in transactions and communications carried out through electronic records, the Act seeks to empower government departments to accept filing, creating and retention of official documents in the digital format. The Act has also proposed a legal framework for the authentication and origin of electronic records / communications through digital signature.

From the perspective of e-commerce in India, the IT Act 2000 and its provisions contain many positive aspects. Firstly, the implications of these provisions for the e-businesses would be that email would now be a valid and legal form of communication in our country that can be duly produced and approved in a court of law.

Companies shall now be able to carry out electronic commerce using the legal infrastructure provided by the Act.

Digital signatures have been given legal validity and sanction in the Act.

The Act throws open the doors for the entry of corporate companies in the business of being Certifying Authorities for issuing Digital Signatures Certificates.

The Act now allows Government to issue notification on the web thus heralding e-governance.

The Act enables the companies to file any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in electronic form by means of such electronic form as may be prescribed by the appropriate Government.

The IT Act also addresses the important issues of security, which are so critical to the success of electronic transactions. The Act has given a legal definition to the concept of secure digital signatures that would be required to have been passed through a system of a security procedure, as stipulated by the Government at a later date.

Under the IT Act, 2000, it shall now be possible for corporates to have a statutory remedy in case if anyone breaks into their computer systems or network and causes damages or copies data. The remedy provided by the Act is in the form of monetary damages, not exceeding Rs. 1 crore.

**Also Read Important Cyber Law Case Studies**

https://www.cyberralegalservices.com/detail-casestudies.php

**Task: (Read the PDF Given)**

Find out

1. Define cyber security
2. What are the functions of controller in certifying authority?
3. What is the Punishment for sending offensive messages through communication service?
4. What is the Punishment for dishonestly receiving stolen computer resource or communication device?
5. Explain violation of privacy and mention the punishment for the same.
6. What is meaning (as per Indian laws)
7. transmitting obscene material
8. cyber terrorism
9. What is the punishment for
10. publishing or transmitting of material containing sexually explicit act
11. publishing or transmitting of material depicting children in sexually

explicit act

1. Mention the importance of Act 66 D.
2. Define the term ‘cybercrime against Governmnet’

PART B

(PART B : TO BE COMPLETED BY STUDENTS)

***(Students must submit the soft copy as per following segments within two hours of the practical. The soft copy must be uploaded on the Portal or emailed to the concerned lab in charge faculties at the end of the practical in case the there is no portal access available)***

|  |  |
| --- | --- |
| Roll. No.: N049 | Name: Tarun Tanmay |
| Class: MBATech CE | Batch: B3 |
| Date of Experiment: | Date of Submission: 26/09/20 |
| Grade: | |

**B.1 Theory written by student:**

1. Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security. ... A compromised application could provide access to the data its designed to protect.
2. The Controller may perform all or any of the following functions, namely:   
   * + exercising supervision over the activities of the Certifying Authorities.
     + certifying public keys of the Certifying Authorities.
     + laying down the standards to be maintained by the Certifying Authorities.
     + specifying the qualifications and experience which employees of the Certifying Authorities should possess.
     + specifying the conditions subject to which the Certifying Authorities shall conduct their business.
     + specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key.
     + specifying the form and content of a Digital Signature Certificate and the key.
     + specifying the form and manner in which accounts shall be maintained by the Certifying Authorities.
     + specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them.
     + facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems.
     + specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers.
     + resolving any conflict of interests between the Certifying Authorities and the subscribers.
     + laying down the duties of the Certifying Authorities.
     + maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public
3. any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.
4. Whoever dishonestly receive or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.
5. Invasion of privacy is the intrusion upon, or revelation of, something private[i]. One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his/her private affairs or concerns, is subject to liability to the other for invasion of privacy[ii]. . Section 66E (Punishment for violation of privacy): Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.
6. a.) Obscenity when considered as an offence it is not defined in any acts in India, however certain laws state that ‘obscenity’ in certain situations establishes it as an offence. Indian Penal Code, 1860 and Information Technology Act, 2000 are the two legislations in India which recognizes obscenity as an offence or crime in certain circumstances. However nor the Information Technology Act, 2000 or the Indian penal code has defined the word obscene or obscenity, but as per section 67 of the Information Technology Act, 2000 and section 292 of the Indian Penal Code, 1860 elaborates and explains Obscenity as “anything which is lascivious or appeals to the prurient interest or if its effect is tend to deprave and corrupt persons.”[3][4]  
   b.) The Indian Information Technology Amendment Act 2008 lays down Section 66F as a specific provision dealing with the issue of cyber terrorism that covers denial of access, unauthorized access, introduction of computer contaminant leading to harm to persons, property, critical infrastructure, disruption of supplies, ‘sensitive data’ thefts, acts which are punishable with imprisonment which may extend to imprisonment for life.
7. a.) Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.  
   b.) There is no enhanced punishment for producing and transmitting child pornography. The punishment is up to five years imprisonment and ten lakh rupees fine for the first offence and seven years imprisonment and ten lakh rupees fine for the second or subsequent offence, both for adult as well as child pornography. Child pornography must be viewed as a more harmful and serious offence.
8. Accordingly, section 66D of the Act has specified the list of services consisting of 16 heads of services which is termed as ‘Negative List’. In a comprehensive tax regime, this ‘Negative List’ is of paramount importance because every activity not covered under this list is chargeable to service tax.
9. A crime against the government is also known as cyber terrorism. Government cybercrime includes hacking government websites, military websites or distributing propaganda. These criminals are usually terrorists or enemy governments of other nations.

**B.2 Conclusion:**

Through this experiment I’ve learned about cybercrime which prevails in today’s world, the laws and acts associated with cybercrime and the punishment imposed on the guilty.