iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** VI **Month of publication:** June 2020

DOI: http://doi.org/10.22214/ijraset.2020.6058

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: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

Study on Cyber Law's of India

Ms. Nisha Tikariha Vaishnav[1], Dr. Snehlata Barde[2]
[1]*Research Scholar,* [2]Associate Professor, *MSIT,* MATS University, Raipur, Chhattisgarh

Abstract: ***In this present age all the things are depends on internet like online dealing or transaction. As we know internet is vast source of knowledge, so it's easy to access by anyone from anywhere. Some people used internet technology for criminal activities like unauthorized access, scams etc. Above unlawful activities or the offense through internet is come under cyber crime. The term "Cyber Law" was introduced for prevention of cyber crimes. Cyber law is the part of legal systems that conciliation the legal issues of internet related crime. Cyber Law helps to prevent or reduce criminal activities, for example freedom of expressions, access to utilization of the online, and online security or online privacy. Cyber crime is also known as law of web.***

Keywords: Net, Access of authorization, Web, TI Act, Cyberspace, Awareness, Imprisonment.

I. INTRODUCTION

The origination of Internet/web has made the lifetime of humans easier, it's been using starting from the individual to large organizations across the word . Most of us utilizing the Internet for the wrong purposes either for itself or for other's benefits. This is the origin of "Cyber Crime". This encourage to busy in unlawful activities which are illegitimate to the society. We will define Cyber Crime as crimes committed using computers or network and are usually happen over the cyberspace especially internet .Cyber laws are the laws that control cyber area. we understood Cyber Crimes, digital electronic signatures, data protections and privacies etc through Cyber Law. The primary IT Act of India was endorsed by UN's General Assembly which had its origin from "United Nations Model Law on Electronic Commerce" (UNCITRAL). Section II shows cyber crime scenario in India. Importance of cyber crime, awareness programs and IT Act of India 2000 in section III. Section IV describe cyber law in India and eventually section V shows the conclusion.

II. CYBER CRIME'S SCENARIO IN INDIA

"Cyber Crime" are often a criminal offense where transmission or information systems are involved, including any of these devices or the web or both. "Cyber law" is taken legalized matter that are associated with utilize of communication, literally "cyberspace", i.e. the web.

The term "Cyber Crime" was proposed by Sussman and Heuston within the year 1995. Cyber Crime is a set of acts or illegal behave. It's supported the fabric offence object that affects the info or systems. In cyber crime computer system / device or data system may be a tool or a target or vice versa. The cybercrime is additionally referred to as electronic, electronic device crimes, e-crime, high-tech crime, modern era crime etc.

A. Some Case study

1) *The Bank NSP Case:* In this bank management trainee's got engaged. Both are chatting with each other by using bank's mail id/system. Because of some reason they had breakup .The girl created some fake e-mail id like "Indian bar associations" and sent mails through bank system to the boy's foreign clients. Her boyfriend lost his clients and client sue the bank. The bank was held responsible for the e-mails sent using the bank's computer.
2) *Bazee.com Case:* The Chief military officer of Bazee.com was arrested in December 2004 because he was selling a compact disc with offensive data on the web site and even compact disc was also compositely sold-out within the market of Delhi. The Delhi and Mumbai Police take action and after a sometime CEO was bail out.
3) *Parliament Attack Case:* In this case a laptop from a surprise attack on Parliament on December 13, 2001 was seized. The seized laptop was sent to Computer Forensics Division of BPRD. CFSL analyze that system had lots of evidence like Home Ministry sticker, fake ID card, scanned national emblems (of the three lions) , seal and residential address of Jammu and Kashmir. All these evidence proof the terrorists intentions. However detection proved that it had been all forged and made on the laptop.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

III. CYBER LAW

Cyber Law is gazetted for controlling Cybercrimes. In cyber law we got definitions, punishment details as well as legal issues and privacy for use of communication or technology.

A. Importance of Cyber Law

Cyber law role is extremely important in new technology. it's important because it cares to most aspects of activities and transactions that happen either on internet or communication devices. whether we are conscious of it or not, but there are some legal and cyber-legal issue of every action and every reaction in cyberspace.

B. Cyber Law awareness Program

Awareness of cybercrime/cyberlaw is must for every single citizen. That are follows:-

1) Knows cyber law.
2) Essential information to use Internet and Internet's security.
3) Read cyber crime's cases.
4) Secure application from trusted site (as HTTPS://) are often used for cover of information or data.
5) Influence of Technology on crime.
6) Smartly use smart mobile phones.

C. The Information Technology Act of India, 2000.

The Information Technology Act, 2000 (the ITA-2000, or IT Act), is an act of the Indian Parliament (no 21 of 2000), it had been notified on October 17, 2000,(4)

On 30 January 1997, the General Assembly of the United Nations recommended the Electronic Commerce 1996 (UNCITRAL Model) was based on the United Nations Model Law.

This Act is amendment in 2008, it gives legal authorities for monitoring, interception nobs and encryption or decryption of computer resources and communication devices.

D. Some of the key points of the IT Act

1) E-mail is now regarded as a legitimate and legal communications.
2) It gives legitimacy to Digital signatures.
3) It started new environment to companies to become Certifying Authorities by providing digital certificates.
4) It gives legal power to issuing notices through e-governance.
5) The exchange of information between the companies or between the company and the government.
6) Addressing the issue of cyber security is the most important feature of this Act.
7) Act have provision of compensation to companies in case of loss by criminals.

IV. CYBER LAW/ IT ACT 2008 (INFORMATION TECHNOLOGY ACT 2008)

A. Section 65- Tempering with Computer source Documents.

Whoever intentionally or knowingly destroy, conceal or change any computer's source code that is used for a computer, computer program, and computer system or computer network. Punishment: Any person who involves in such crimes could be sentenced upto 3 years imprisonment or with a fine of Rs.2 lakh or with both.

B. Section 66- Hacking with Computer System.

Whoever with the intention to cause or knowing he is likely to cause wrongful loss, damage or to destroy, delete or to alter any information that resides in a public or any person's computer resource. Mitigate its utility, values or affects it injuriously by any means, commits hack.

1) *Punishment:* Any person commits shall be sentenced upto 3 years imprisonment, or with a fine that may extend upto 2 lakhs rupees, or both.

C. Section 66A

Extinguished

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue VI June 2020- Available at www.ijraset.com

D. Section 66B- Receiving stolen Computer's resources or Communication Devices Dishonestly.

Receiving or retaining any stolen computer, computer's resources or any communication devices knowingly or having the rationale to believe an equivalent .

1) *Punishment:* Any person who involves in such crimes could be sentenced either description for a term that may extend upto 3 years of imprisonment or with a fine of rupee 1 lakh or both.

E. Section 66C- Identify theft

Using of digital or electronic signature or password or any other unique identification of any person is a crime.

1) *Punishment:* Involvement could be sentenced either with a description for a term which may extend upto 3 years of imprisonment along with a fine that may extend upto rupees 1 lakh.

F. Section 66D- Cheating by Personation by the use of Computer's Resources

Whoever tries to cheats by personating through any communication devices or computer's resources.

1) *Punishment:* Involvement should be sentenced either with a description for a term that may extend upto 3 years of imprisonment along with a fine that may extend upto rupees 1 lakh.

G. Section 66E- Privacy or violation

Whoever knowingly or with an intention of publishing, transmitting or capturing images of private areas or private parts of any individual without his/her consent, that violations of privacy.

1) *Punishment:* Person shall be punished with3 years of imprisonment or with a fine not exceeding more than 2 lakhs rupees or both.

H. Section 66F- Punishment for Cyber Terrorism

1) Anyone intentionally threatened the integrity, unity, sovereignty or security or strike terror among the people or group of people by-
2) Deny to any people to access computer's resources.
3) Attempting to break in or access a computer resource without any authorization or to exceed authorized access.
4) Introducing any computer's contaminant, and through such conducts causes or is probable to cause any death or injury to any individual or damage or any destruction of properties or disrupt or it is known that by such conduct it is probable to cause damage or disruptions of supply or services that are essential to the life of people or unfavourably influence the critical information's infrastructure specified under the section 70 of the IT Act.

By intention or by knowingly tries to go through or tries to gain access to computer's resources without the authorization or exceeding authorized access, and by such conducts obtains access to the data, information or computer's database which is limited or restricted for interest of the security of the state or foreign relations, or any restricted database, data or any information with the reason to believe that those data or information or the computer's database obtained may use to cause or probably use to cause damage the interest of the independence and integrity nation.

a) Punishment: Shall be sentenced to life time imprisonment.

I. Section 67- Transmitting or Publishing Obscene Materials in Electronic Form.

Whoever publishes or transmits or cause to publish any kind obscene materials in electronics form. Any material that is vulgar or appeal to be lubricious or if its effect is for instance to tends to corrupt any individual with respect to all relevant circumstances to read or see or hear the matter that contained in it.

1) *Punishment*

a) First convict with either description for a term that may extend upto five years of imprisonment along with a fine which may extend upto 1 lakh rupee.

b) Second or subsequent convict it can be sentenced either description for a term that may extend upto ten years along with a fine that may perhaps extend to two lakhs rupees

J. Section 67A- Transmitting or publishing of Materials that Contains Sexually Explicit act, etc., in Electronics form

1) Punishment

a) 1st convict Sentences for either description for a term which may extend upto 5 years or imprisonment along with a fine that could extend to 10 lakhs rupees.

b) 2nd convict sentenced for either description for a term that could extend upto 7 years of imprisonment along with a fine that may extend upto 20 lakhs rupees.

K. Section 67B- Transmitting or publishing of materials that depicts children in sexually explicit act etc in electronics form.

1) Punishment: Sentenced for either description for a term which can reach 5 years of imprisonment with a fine that would reach rupees 10 lakhs on the primary conviction. And within the event of second conviction criminals might be sentenced for either description for a term that would reach 7 years alongside a fine that would extend to rupees 10 lakhs.

L. Section 67C- Retention and Preservation of Information by Intermediaries

1) Intermediaries shall retain and preserve such information that might specify for such period and in such a format and manner that the Central Government may prescribe.

2) Any intermediaries knowingly or intentionally contravene the provision of the sub-section.

a) Punishment: Whoever commits such crimes shall be sentenced for a period that may extend upto 3 years of imprisonment and also liable to fine.

M. Section 69- Power to issue Direction for Monitor, Decryption or Interception of any Information Through Computer's Resources

1) Where the Central government's or State government's authorized officers, as the case may be in this behalf, if fulfilled that it is required or expedient to do in the interest of the integrity or the sovereignty, the security defence of our country India, state's security, friendly relations with the foreign states for preventing any incident to the commission of any cognizable offences that is related to above or investigation of any offences that is subjected to the provision of sub-section (II). For reasons to be recorded writing, direct any agency of the acceptable government, by order, decrypt or monitor or cause to be intercept any information that's generated or received or transmitted or is stored in any computer's resources.

2) The safeguard and the procedure that is subjected to such decryption, monitoring or interception may carried out, shall be such as may be prescribed.

3) The intermediaries, the subscribers or any individual who is in the charge of the computer's resources shall call upon by any agencies referred to the sub-section (I), extends all services and technical assistances to:

a) Providing safe access to computer's resources, receiving, transmitting, generating or to store such information .

b) Decrypting, intercepting or monitoring the information.

c) Providing information that is stored in computer.

d) The intermediaries, the subscribes or any individual who fails to help the agency referred in the sub-section (III),

4) *Punishment:* Sentenced for a period that may extend upto 3 years of imprisonment and also liable to fine.

There are many other sections in the IT Act, 2000 among them a few important sections one should know are as follows:

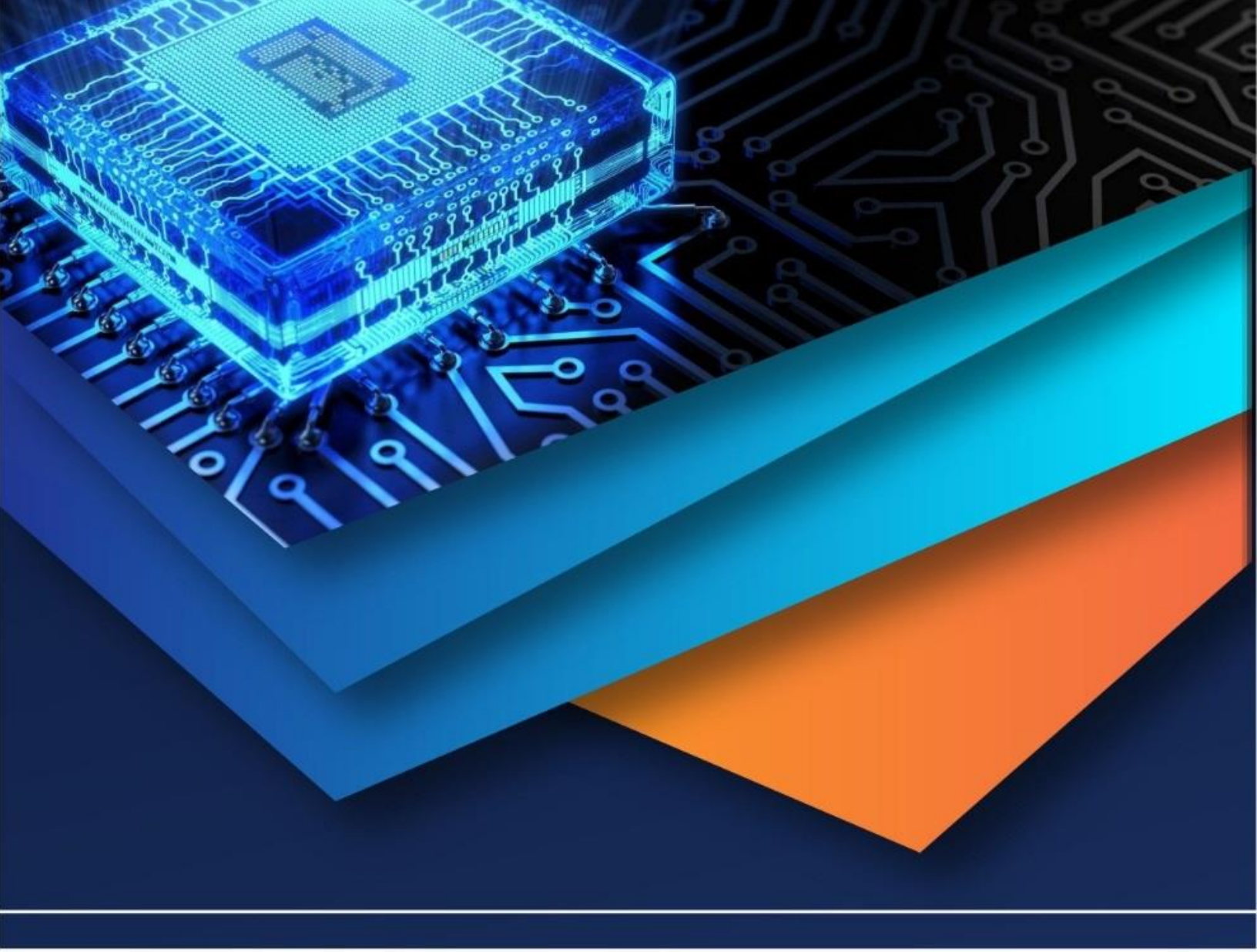
- In section 43, damage to computer, computer system etc.
- In section 69A, power to issue direction for blocking from public access of any information through any computer's resources
- In section 69B, power to authorize to collect traffic information or data and to monitor through any computer's resources for cyber security
- In section 70, un-authorized access to protected system.
- In section 71, penalty for misrepresentation.
- In section 72, breach of confidentiality and privacy.
- In section 73, publishing False digital signature certificates.
- In section 74, publication for fraudulent purpose.
- In section 75 , act to apply for contravention or offence that is committed outside India.
- In section 77, compensation, confiscation or penalties for not to interfere with other punishment.
- In section 77A, compounding of Offences.
- In Section 85, offences by companies.

V. CONCLUSIONS

The present period is moving towards a technological era. In which every person is constantly involved in the use of internet and other technical equipment from morning to night. Due to lack of knowledge about cybercrime and cyber laws, people commit crimes or fall prey to it. Cybercrime has been hazard to humanity. Therefore, in today's age, children, elders, officers, employees, rich, poor (every one) should know what is cybercrime and its imprisonment . Information related to all the above facts and why cyber law is important and its provision of punishment, has been contained in this paper. Cyber security is possible only by compliance with cyber law. Know or inadvertently the graph of crime is increasing, which will be difficult to stop due to lack of cyber law. Awareness is only key to avoid cyber crimes. Cyber crime could be committed from anywhere, it does'nt have any national boundary. It is must to get the crimes committed in and around you will discuss with your family or police. IT Act 2000 has been amendment in 2008 as the "IT Act 2008" because increasing graph of cybercrime and new type of internet related crime.

REFERENCES

[1] Ms. Nisha Tikariha Vaishnav, "CYBER CRIME PROBLEMS AND PREVENTION EFFECT ON SOCIETY" Journal of Information and Computational Science, Vol. 13, Issue 1,No29-36, 2020.
[2] Marco Gercke, "Understanding cybercrime: Phenomena, challenges and legal response". Book Page no 2 (1.3), 2012.
[3] Animesh Sarmah, "A brief study on Cyber Crime and Cyber Law's of India ", International Research Journal of Engineering and Technology (IRJET), Vol. 4, No 6, 2017.
[4] https://en.wikipedia.org/wiki/Information_Technology_Act,_2000
[5] Nadine Touzeau," Behavioral Cybercriminals Differentiations between the Real World and the Virtual Space" J Forensic Res, an open access journal, Vol. 8, Issue 6, No.1-2,2017



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY