ज्ञान-विज्ञान विमुक्तये

Pathshala पाठशाला

MHRD Govt. of India सत्यमेव जयते

Pathshala पाठशाला

A Gateway to all Post Graduate Courses

MHRD Govt. of India

An MHRD Project under its National Mission on Education through ICT (NME-ICT)

Subject: CRIMINOLOGY

Production of Courseware

- Content for Post Graduate Courses

Paper : CYBER CRIMINOLOGY & CYBER FORENSICS

Module : Cyber Offences under the Information Technology Act

ज्ञान-विज्ञान विमुक्तये

MODULE 28: CYBER OFFENCES UNDER THE INFORMATION TECHNOLOGY ACT

Component - I - Personal Details

Role	Name	Affiliation
Principal Investigator	Prof(Dr) G S Bajpai	Registrar National Law University Delhi
Paper Coordinator	Prof(Dr) K. Jaishankar	Professor and Head, Department of Criminology, Raksha Shakti University, Ahmedabad, Gujarat
Content Writer/Author	1. Prof(Dr) K. Jaishankar 2. Divya Priyadarshini	1. Professor and Head, Department of Criminology, Raksha Shakti University, Ahmedabad, Gujarat 2. UGC Senior Research Fellow, Department of Sociology Delhi School of Economics University of Delhi
Content Reviewer	Dr. Akshat Mehta	Associate Professor and Head, Department of Police Administration, Raksha Shakti University, Ahmedabad, Gujarat

Component - I (B) Description of Module

	Description of Module
Subject Name	Criminology
Paper Name	**Cyber Criminology and Cyber Forensics**
Module No.	28
Module Name/Title	**Cyber Offences under the Information Technology Act**
Pre-requisites	Computer, Cyber Space, Offences, Legislations, legal, Punishments
Objectives	• To understand the Information Act 2000, amended in 2008. • To study Cyber offences and Punishments for them as laid under the Information Technology Act 2000 amended in 2008. • To interpret and analyse the applicability of Information Technology Act, 2000 amended in 2008 to combat the increasing cyber crimes.
Keywords	Cyber Offences, Penalties, Punishments, Computer, Information Technology

Table of Contents

Learning Outcomes

After the completion of this module you will be able:

1. To understand the evolution of the Information Technology Act, 2000 amended in 2008

2. To study the various cyber offences laid down in the IT Act and the punishments and penalties for the same

3. To understand the significance of framing cyber laws so as to combat increasing cyber crimes.

4. To examine, interpret and analyse the applicability of the laws relating to Cyber Offences as laid down in the IT Act, 2000 amended in 2008.

Cyber Offences under the Information Technology Act

1. Introduction

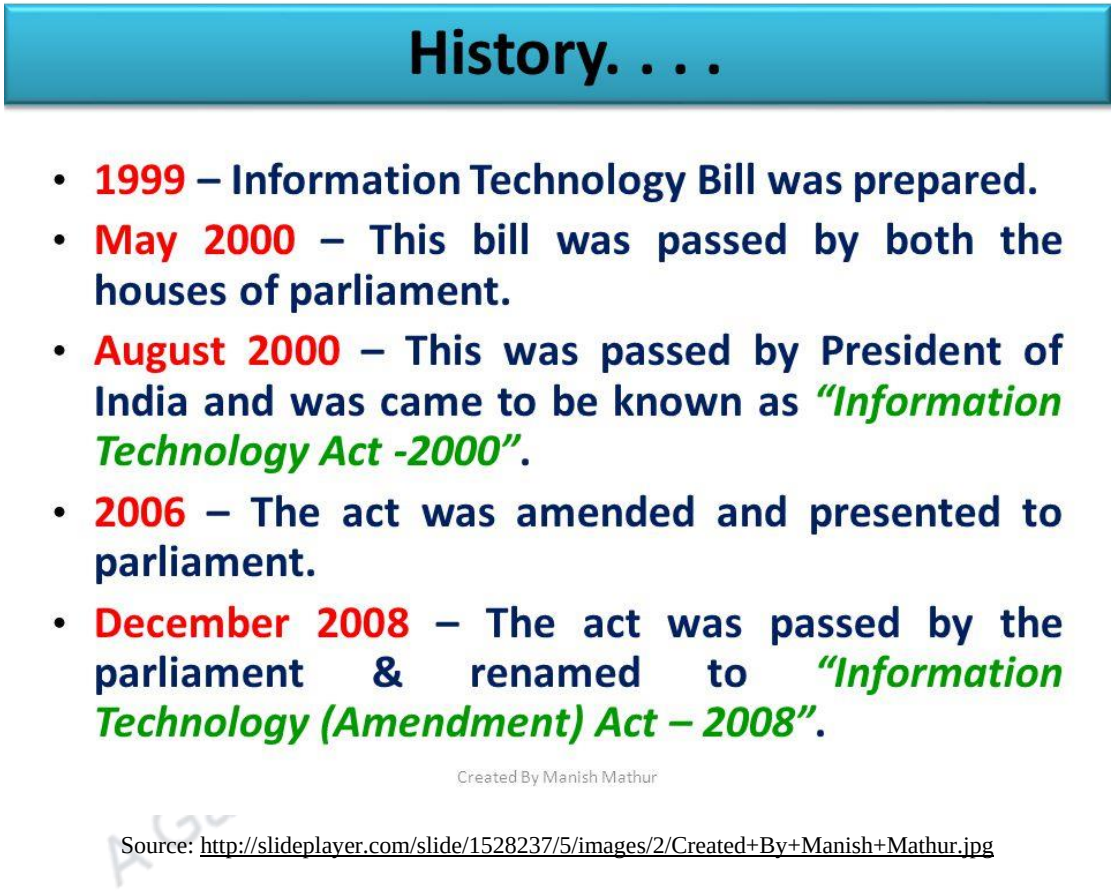
With the advent of technology the world today has shrunk into a micro chip and so has everyone's life. Computer, internet and e-communication have substituted paper based communication by digital and electronic communication. The United Nations Commission on International Trade Law (UNCITRAL) realizing the impetus being given to computerization adopted the Model Law on e-commerce in 1996. The General Assembly of United Nations passed a resolution in January 1997 inter alia, recommending all States in the UN to give favorable considerations to the said Model Law, which provides for recognition to electronic records and according it the same treatment like a paper communication and record. India was also a signatory to this Model Law and therefore became mandatory for it to revise its National Law as per the said Model Law. Therefore, in order to keep at pace with the requirements of the International Trading and also to allure industries into adopting this convenient way to transactions and storing data, the Information and Technology Act, 2000 was passed by both the Rajya Sabha and the Lok Sabha in May 2000 and the Act was amended in 2008 which came into force from 27th October, 2009. The preamble quotes:

> "An Act 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 Banker's Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto." (Information Technology Act, 2000)

2. Structure of the Information Technology Act, 2000

The Act in total has 13 chapters and 90 sections The Act begins with preliminary and definitions (Chapter 2) and from there on the chapters that follow deal with authentication of electronic records, digital signatures, electronic signatures etc. Elaborate procedures for certifying authorities (for digital certificates as per Information Technology Act -2000 and since replaced by electronic signatures in the Information Technology Act Amendment - 2008) have been spelt out. The civil offence of data theft and the process of adjudication and

appellate procedures have been described. Then the Act goes on to define and describe some of the well-known cyber crimes and lays down the punishments therefore. Then the concept of due diligence, role of intermediaries and some miscellaneous provisions have been described. Rules and procedures mentioned in the Act have also been laid down in a phased manner, with the latest one on the definition of private and sensitive personal data and the role of intermediaries, due diligence etc., being defined as recently as April 2011 (Pandurang, 2014).



Source: http://slideplayer.com/slide/1528237/5/images/2/Created+By+Manish+Mathur.jpg

3. Cyber Offences and Penalties under the Information Technology Act, 2000 as amended in 2008

Cyber crime or offences have not been defined in the Act explicitly but has been categorised in different sections along-with the sanctions. However, for understanding, cyber offences can be viewed as the unlawful acts which are carried in a very sophisticated manner in which either the computer is the tool or target or both (Pahurkar 2010). Cyber offences are usually generalised into three categories that are the ones committed against person, property and the government. Chapter 11 of the Act covers the offences and the Penalties that are

accrued upon when the law is threatened. The cyber offences as mentioned under the Information Technology Act, 2000 have been delineated below:

3.1. Section 65: Tampering with computer source documents

Any person who knowingly or intentionally conceals, destroys or alters, or causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable.

3.2. Section 66A: Punishment for sending offensive messages through communication service, etc. *(Now, not in existence as per Shreya Singhal vs. Union of India Case and it is struck down by the Supreme Court. Notably, experts like Halder (2013) feel that this section should be replaced with a new law or it should be amended appropriately).*

Source: http://indpaedia.com/ind/images/7/77/Information_technology_act.jpg

Source: http://www.hindustantimes.com/Images/popup/2015/3/gfx-Popup1-new.jpg

3.2. Section 66B: Punishment for dishonestly receiving stolen computer resource or communication device

Any person who, dishonestly received 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.

3.3. Section 66C: Punishment for identity theft

Any person who, fraudulently or dishonestly makes use of the electronic signature, password, or any other unique identification feature of any other person, shall be punished.

3.4. Section 66D: Punishment for cheating by personation by using computer resource

Any person who, by means for any communication device or computer resource cheats by personating, shall be punished.

3.5. Section 66E: Punishment for violation of privacy

Any person who, 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; 'Publishes' means reproduction in the printed or electronic form and making it available for public.

3.6. Section 66F: Punishment for Cyber Terrorism

A person commits the offence of cyber terrorism if he,

(i). with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people –

a. denies or causes the denial of access to any person authorized to access computer resource; or

b. attempts to penetrate or access a computer resource without authorization or by exceeding authorized access; or

c. introduces or causes to introduce any computer contaminant; and by means of such conduct causes or is likely to cause death or injuries to persons, or damage to or destruction of property, or knowing that it is likely to cause damage or destruction of supplies or services essential to the life of the community, or adversely affect the critical information infrastructure

(ii). Knowingly or intentionally accesses or penetrates a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations, or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise.

3.7. Section 67: Punishment for publishing or transmitting obscene material in electronic form

Any person who, 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;

3.8. Section 67A: Punishment for publishing or transmitting of material containing sexually explicit act etc. in electronic form

Any person who, publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct, shall be punished;

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

Any person who,

a. Publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

b. Creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

c. Cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

d. Facilitates abusing children online; or

e. Records in any electronic form own abuse or that of others pertaining to sexually explicit act with children shall be punished;

However, these provisions does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form which is proved to be justified as being for the public good on the ground that such material is in the interest of science, literature, art or learning or other objects of general concern;

3.10. Section 71: Penalty for misrepresentation

Any person who makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any licence or Electronic Signature Certificate shall be punished with imprisonment for a term which may extend to 2 years or with fine which may extend to Rs. 1 lakh or with both.

3.11. Section 72: Penalty for breach of confidentiality and privacy

If any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made there under, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person

concerned and discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to 2 years or with fine which may extend to Rs. 1 lakh or with both.

3.12. Section 72A: Punishment for disclosure of information in breach of lawful contract

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 3 years or with fine which may extend to Rs. 5 lakh or with both.

3.13. Section 73: Penalty for publishing Electronic Signature Certificate false in certain particulars

No person shall publish an Electronic Signature Certificate or otherwise make it available to any other person with the knowledge that –

a. The Certifying Authority listed in the certificate has not issued it; or

b. The subscriber listed in the certificate has not accepted it; or

c. The certificate has been revoked or suspended, unless such publication is for the purpose of verifying a electronic signature created prior to such suspension or revocation

Any person who contravenes above provisions shall be punished with imprisonment for a term which may extend to 2 years or with fine which may extend to Rs. 1 lakh or with both.

3.14. Section 74: Publication for fraudulent purpose

Any person, who knowingly creates, publishes or otherwise makes available an Electronic Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to 2 years or with fine which may extend to Rs. 1 lakh or with both.

3.15. Section 75: Act to apply for offence or contravention committed outside India

The provisions of this Act shall apply also to any offence or contravention committed outside India by any person irrespective of his nationality. However, for such liability the act or conduct constituting the offence or contravention should involve a computer, computer system or computer network located in India.

The table 1 briefly enumerates the cyber offences as laid under the IT Act, 2000 (Amendment 2008) with the punishments and penalties.

Table 1: Cyber Offences and Penalties and Punishments

S.no.	Section	Offence	Punishment
1.	65	Tampering with computer source documents	Imprisonment upto 3 years or fine upto Rs 2 lakh or both
2.	66	Computer related offences	Imprisonment upto 3 years or fine upto Rs 5 lakh or both
3.	66B	Dishonestly receiving the stolen computer resource and communication device	Imprisonment upto 3 years or fine upto Rs. 1 lakh
4.	65C	Theft of identity	Imprisonment upto 3 years
5.	66 D	Cheating by personation by using computer resource or communication device	Imprisonment upto 3 years and fine upto Rs. 1 lakh
6.	66E	Violation of Privacy	Imprisonment upto 3 years or fine upto Rs. 2 lakh or both
7.	66F	Cyber Terrorism	Life Imprisonment
8.	67	Publishing or transmitting obscene material in e-form	Upon 1st conviction with imprisonment upto 3 years and fine upto Rs 5 lakh; and upon 2nd or subsequent conviction with imprisonment upto 5 years and fine upto Rs 10 lakh.
9.	67A	Publishing or transmitting material containing sexually explicit act in e-form	Upon 1st conviction with imprisonment upto 5 years and fine upto Rs 10 lakh; and upon 2nd or

			subsequent conviction with imprisonment upto 7 years and fine upto Rs 10 lakh.
10.	67B	Publishing or transmitting material depicting children in sexually explicit act etc. in e-form	Upon 1st conviction with imprisonment upto 5 years and fine upto Rs 10 lakh; and upon 2nd or subsequent conviction with imprisonment upto 7 years and fine upto Rs 10 lakh.
11.	67C	Violating the directions to preserve and retain the information by intermediaries	Imprisonment upto 3 years and fine
12.	68	Violating the directions of Controller by Certifying Authority or his employee	Imprisonment upto 2 years or fine upto Rs 1 lakh or both
13.	69	Violating the directions of the Central Government or State Government to a subscriber to extend facilities to decrypt information	Imprisonment upto 7 years and fine
14.	69A	Violating the directions to block any information for access by the public	Imprisonment upto 7 years and fine
15.	69B	Violating the directions to monitor and collect traffic data or information	Imprisonment upto 3 years and fine
16.	70	Unauthorized access to a computer	Imprisonment upto 10 years and fine

	70A	system	
17.	70B	Violating the directions of the Indian Computer Emergency Response Team (CERT-IN)	Imprisonment upto 1 years or fine upto Rs 1 lakh or both
18.	71	Penalty for misrepresentation	Imprisonment upto 2 years or fine upto Rs 1 lakh or both
19.	72	Penalty for breach of confidentiality and privacy	Imprisonment upto 2 years or fine upto Rs 1 lakh or both
20.	72A	Disclosure of information in breach of lawful contract	Imprisonment upto 3 years or fine upto Rs 5 lakh or bo Upto 5 lakh.
21.	73	Penalty for publishing electronic signature certificate false in certain particulars	Imprisonment upto 2 years or fine upto Rs 1 lakh or both
22.	74	Publication for fraudulent purpose	Imprisonment upto 2 years or fine upto Rs 1 lakh or both

4. Summary and Conclusion

The legislation incorporates within its understanding the various cyber offences that the world is under the threat of in the contemporary era. Proper and timely implementation of the Act may help curb the cyber menace and also make the cyber space a more secure, safe and easy space for storage, transactions and definitely sharing. Its linkages with other Acts like the Indian Evidence Act, 1872 and the Bankers Book Evidence Act 1891 have made it a comprehensive and umbrella Act to deal with any kind of cyber crime. Its proper interpretation and implementation is what is the need of the hour.

References

Duggal, P. (2005). Cyber-Crime in India: The Legal Approach. In Broadhurst R. & Grabosky P. (Eds.), *Cyber-Crime: The Challenge in Asia* (pp. 183-196). Hong Kong University Press. Retrieved from http://www.jstor.org/stable/j.ctt2jc6s1.17

Halder, D. (2015). A retrospective analysis of S.66a: Could S.66a of the information technology act be reconsidered for regulating 'bad talk' in the internet? *Indian Student Law Review (ISLR), 3*, 91–118.

Pahurkar, P. (2010). Offences and Penalties under the IT Act, 2000. Retrieved from http://www.legalservicesindia.com/article/article/offences-&-penalties-under-the-it-act-2000-439-1.html on 26-4-2017

Pandurang, S. (2014). Intellectual Property Law. Goa: Govind Ramnath Kare College of Law The Information Technology Act, 2000 as amended in 2008.