

CYBER CRIME UNDER THE PROVISIONS OF IPC

AUTHOR:

Mrs. K.KALISELVI B.A.,B.L.,LL.M.,

RESEARCH SCHOLAR

SAVEETHA SCHOOL OF LAW

SAVEETHA INSTITUTE OF MEDICAL TECHNICAL SCIENCES (SIMATS)

SAVEETHA UNIVERSITY

kaliselvi5118@gmail.com

CO-AUTHOR:

SHIVANI MOAHAN

REGISTER NUMBER-131801011

SAVEETHA SCHOOL OF LAW

SAVEETHA INSTITUTE OF MEDICAL AND TECHNICAL SCIENCES (SIMATS)

CHENNAI-77

Email Id: shivani.mohan00@gmail.com

Abstract:

Law provides a cure against the vast majority of the common digital violations. 'Digital wrongdoing' is certainly not a characterized term however a catch-all expression inferable from any offense including a web gadget. The vast majority of the digital violations are recorded under the Information Technology Act (IT Act), 2000, which was amended in 2008 and 2012. Nonetheless, this lucidity vaporizes with the acknowledgment that IT Act isn't the main authorization covering digital wrongdoing. The Indian Penal Code (IPC) could likewise be brought in to start arraignment against digital violations or to enhance the arrangements of the IT Act. For example, offenses like hacking, information burglary, infection assaults, refusal of administration assaults, unlawful altering source codes including ransomware assaults could be indicted under S.66 r/w S.43 of the IT Act. Instances of producing a credit or debit .The IT Act to give legitimate acknowledgment to exchanges did by methods for electronic information trade and different methods for electronic correspondence, regularly

alluded to as "electronic business", which include the utilization of choices to paper-based strategies for correspondence and capacity of data, to nusta altering electronic recording of reports with the Government organizations and further it has it provisions under the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and support matters associated there with or coincidental thereto. Even Though with sufficient laws we are still facing lot of cyber crime suits and for this the researcher had undergone a study with 1579 samples . This paper focuses on the concept of cyber crime and its provision with IPC. The online criminal activities is widespread throughout the world. From the analysis, the paper sort to conclude that the null hypothesis . There is an association between the dependent and independent variables.

KEYNOTES: Cybercrime, Computer, Punishments, Conventional crime, Indian Penal Code and Criminal law.

Introduction

In order to prevent the various crimes in cyberspace, India adopted and placed the Information Technology Act 2000. It was the first step towards controlling and curbing cybercrimes. The act contains the rules to prevent and control cyber crimes to regulate superhighway, to protect data and cyber world from any wrongful act or damage. The act was amended through the Information Technology Amendment Act 2008 and it provides additional focus on information security. It has added several new sections on offences including cyber terrorism. Thus the solution for cyber crime is the need for the hour.

In the literal sense, cyber was a word coined by William Gibson in his 1984 fictional novel 'Neuromancer'. Cyber is the prefix relating to the worldwide field of electronic communication. Crimes involving stealing, fabricating, leaking or circulating forbidden digital information is collectively branched under the umbrella term cyber-crime. Cyber-crime is classified broadly into three basic categories – data related crimes, physical crimes and software crimes.

Data related crimes involve fraudulent input of data in the hierarchy of levels – encoding, examining, checking, storing, converting and transporting data to be entered into the computer. Which also includes software related crimes. Software crime is the use of viruses or other such damaging software such as Trojan Horse, Time Bombs and Logic Bombs. Trojan Horse is a spy program that will stalk spy and corrupt files in computer forcing them to send

signatures on the progress of system processing to a designated path of device or telecom line. Logic Bombs are designed to carry out certain unwarranted commands on encountering pre-designated data or logic in a system.

All Cyber Crimes do not come under the Information Technology Act, 2000. For other type of crimes such as cheating, fraud, forgery, threat, misappropriation, defamation, etc committed by using computer IPC and other special laws to be invoked.

Indian Penal Code was amended by infusing the term “electronic”. Thus all the electronic documents and records were made commensurate with the physical documents and records covered within the ambit of the IPC. Further the following offences were made punishable under IPC.

The following are the 14 most common cyber crime which has its provisions under IPC.

1) Harassment via fake public profile on social networking site: A fake profile of a person is created on a social networking site with the correct address, residential information or contact details but they are labelled as a ‘prostitute’ or a person of ‘loose character’. This leads to harassment of the victim.

Provisions applicable: Sections 66A, 67 of the IT Act and Section 509 of the Indian Penal Code.

2) Online hate community: Online hate community is created inciting a religious group to act or pass objectionable remarks against a country, national figures etc.

Provisions applicable: Section 66A of IT Act and 153A & 153B of the Indian Penal Code.

3) Email account hacking: If victim’s email account is hacked and obscene emails are sent to people in the victim's address book.

Provisions applicable: Sections 43, 66, 66A, 66C, 67, 67A and 67B of the IT Act.

4) Credit card fraud: Unsuspecting victims would use infected computers to make online transactions.

Provisions applicable: Sections 43, 66, 66C, 66D of IT Act and section 420 of the IPC.

5) Web defacement: The homepage of a website is replaced with a pornographic or defamatory page. Government sites generally face the wrath of hackers on symbolic days.

Provisions applicable: Sections 43 and 66 of the IT Act and Sections 66F, 67 and 70 of IT Act also apply in some cases.

6) Introducing viruses, worms, backdoors, rootkits, trojans, bugs: All of the above are some sort of malicious programs which are used to destroy or gain access to some electronic information.

Provisions applicable: Sections 43, 66, 66A of IT Act and Section 426 of Indian Penal Code.

7) Cyber terrorism: Many terrorists are using virtual (G-Drive, FTP sites) and physical storage media (USB's, hard drives) for hiding information and records of their illicit business.

Provisions applicable: Conventional terrorism laws may apply along with Section 69 of IT Act.

8) Online sale of illegal articles: Applicable when the sale of narcotics, drugs weapons and wildlife is facilitated by the internet.

Provisions applicable: Generally conventional laws apply in these cases.

9) Cyber pornography: This is among the largest businesses on the internet. Pornography may not be illegal in many countries, but child pornography is.

Provisions applicable: Sections 67, 67A and 67B of the IT Act.

10) Phishing and email scams: Phishing involves fraudulently acquiring sensitive information through masquerading as a trusted entity. (E.g. Passwords, credit card information)

Provisions Applicable: Section 66, 66A and 66D of IT Act and Section 420 of IPC

11) Theft of confidential information: Many business organisations store their confidential information in computer systems. This information is targeted by rivals, criminals and disgruntled employees.

Provisions applicable: Sections 43, 66, 66B of IT Act and Section 426 of Indian Penal Code.

12) Source code theft: A source code generally is the most coveted and important “crown jewel” asset of a company.

Provisions applicable: Sections 43, 66, 66B of IT Act and Section 63 of Copyrights Act.

13) Tax evasion and money laundering: Money launderers and people doing illegal business activities hide their information in virtual as well as physical activities.

Provisions applicable: Income Tax Act and Prevention of Money Laundering Act. IT Act may apply case-wise.

14) Online share trading fraud: It has become mandatory for investors to have their demat accounts linked with their online banking accounts which are generally accessed unauthorized, thereby leading to share trading frauds.

Provisions applicable: Sections 43, 66, 66C, 66D of IT Act and Section 420 of the IPC.

Hence the person committing these crimes will not only be liable under the IT Act but also under IPC. The aim of the study is to have an in depth knowledge about IT Act and IPC and cyber crime’s provision under IPC. The aim of the paper is to have an in depth knowledge about cyber crime and how far it is connected with conventional crimes.

OBJECTIVES:

1. To understand about cybercrime.
2. To analyses and use the preventive measures available to control cyber crime
3. To know the reason for cyber crime.
4. To study about the cyber crime under the provision of IPC.

Review of literature

The Information Technology (IT) Act, 2000, determines the criminal demonstrations. (Stephen 1872; Nappinai 2017; Sharma, n.d.; Gandhi and India 2006; Ormerod, Smith, and Hogan 2011; Richardson 2019; Halder and Jaishankar 2016; Commonwealth Secretariat 2001; Koops and Brenner 2006; “IPC. IPC Releases ‘F’ Revision of IPC-A-600” 2000; Gajjar 2017; Ictsd, ICTSD, and IPC 2009; World Intellectual Property Organization, n.d.;

Hayden 2012; World Intellectual Property Organization et al., n.d.; Sood 2007; American Contractors Exam Services and Prince 2015; Jung et al. 2019; Bogdanovic et al. 2019; Gaur 2019; Sinha 2015; Isebrands and Richardson 2014) Nonetheless, as the essential goal of the Act is to make empowering condition for business utilization of I.T., certain exclusions and commissions for culprits with utilization of PCs have not been incorporated. With the lawful acknowledgment of Electronic Records and the changes made in the few areas of the IPC vide the IT Act, 2000, a few offenses having bearing on digital field are likewise enlisted under the proper segments of the IPC. (Stephen 1872; Nappinai 2017; Sharma, n.d.; Gandhi and India 2006; Ormerod, Smith, and Hogan 2011; Richardson 2019; Halder and Jaishankar 2016; Commonwealth Secretariat 2001; Koops and Brenner 2006; "IPC. IPC Releases 'F' Revision of IPC-A-600" 2000; Gajjar 2017; Ictsd, ICTSD, and IPC 2009; World Intellectual Property Organization, n.d.; Hayden 2012; World Intellectual Property Organization et al., n.d.; Sood 2007; American Contractors Exam Services and Prince 2015; Jung et al. 2019; Bogdanovic et al. 2019; Gaur 2019; Sinha 2015; Isebrands and Richardson 2014; Li et al. 2019) Of the 738 cases enlisted for Cyber Crimes under IPC, greater part of the violations fall under 3 classifications viz. Criminal Breach of Trust or Fraud (510), Forgery (167) and Counterfeiting (59). However, these offenses fall under the customary IPC wrongdoings, the cases had the digital tones wherein PC, Internet or its related perspectives were available in the wrongdoing and subsequently they were sorted as Cyber Crimes under IPC. (Stephen 1872; Nappinai 2017; Sharma, n.d.; Gandhi and India 2006; Ormerod, Smith, and Hogan 2011; Richardson 2019; Halder and Jaishankar 2016; Commonwealth Secretariat 2001; Koops and Brenner 2006; "IPC. IPC Releases 'F' Revision of IPC-A-600" 2000; Gajjar 2017; Ictsd, ICTSD, and IPC 2009; World Intellectual Property Organization, n.d.; Hayden 2012; World Intellectual Property Organization et al., n.d.; Sood 2007; American Contractors Exam Services and Prince 2015; Jung et al. 2019; Bogdanovic et al. 2019; Gaur 2019; Sinha 2015; Isebrands and Richardson 2014; Li et al. 2019; Gao et al. 2019) During 2002, 2 occurrences of False Electronic Evidence has likewise been accounted for. Curiously, number of cases under Cyber Crimes identifying with Counterfeiting of cash/Stamps remained at 49 wherein 124 people were captured during 2002. Of the 46,271 cases detailed under Cheating, the Cyber Forgery (167) represented 0.4 percent. (Stephen 1872; Nappinai 2017; Sharma, n.d.; Gandhi and India 2006; Ormerod, Smith, and Hogan 2011; Richardson 2019; Halder and Jaishankar 2016; Commonwealth Secretariat 2001; Koops and Brenner 2006; "IPC. IPC

Releases ‘F’ Revision of IPC-A-600” 2000; Gajjar 2017; Ictsd, ICTSD, and IPC 2009; World Intellectual Property Organization, n.d.; Hayden 2012; World Intellectual Property Organization et al., n.d.; Sood 2007; American Contractors Exam Services and Prince 2015; Jung et al. 2019; Bogdanovic et al. 2019; Gaur 2019; Sinha 2015; Isebrands and Richardson 2014; Li et al. 2019; Gao et al. 2019; Pignot 2019)Of the all out Criminal Breach of Trust cases (14,027), the Cyber fakes (510) represented 3.6 percent, of the Counterfeiting offenses (1522), Cyber Counterfeiting (59 out of 1522) offenses represented 3.9 percent.Of the 738 cases enlisted for Cyber Crimes under IPC, greater part of the violations fall under 3 classifications viz. Criminal Breach of Trust or Fraud (510), Forgery (167) and Counterfeiting (59). However, these offenses fall under the customary IPC wrongdoings, the cases had the digital tones wherein PC, Internet or its related perspectives were available in the wrongdoing and subsequently they were sorted as Cyber Crimes under IPC(Stephen 1872; Nappinai 2017; Sharma, n.d.; Gandhi and India 2006; Ormerod, Smith, and Hogan 2011; Richardson 2019; Halder and Jaishankar 2016; Commonwealth Secretariat 2001; Koops and Brenner 2006; “IPC. IPC Releases ‘F’ Revision of IPC-A-600” 2000; Gajjar 2017; Ictsd, ICTSD, and IPC 2009; World Intellectual Property Organization, n.d.; Hayden 2012; World Intellectual Property Organization et al., n.d.; Sood 2007; American Contractors Exam Services and Prince 2015; Jung et al. 2019; Bogdanovic et al. 2019; Gaur 2019; Sinha 2015; Isebrands and Richardson 2014; Li et al. 2019; Gao et al. 2019; Pignot 2019; Pu et al. 2019; Wang et al. 2019). During 2002, 2 occurrences of False Electronic Evidence has likewise been accounted for.(Stephen 1872; Nappinai 2017; Sharma, n.d.; Gandhi and India 2006; Ormerod, Smith, and Hogan 2011; Richardson 2019; Halder and Jaishankar 2016; Commonwealth Secretariat 2001; Koops and Brenner 2006; “IPC. IPC Releases ‘F’ Revision of IPC-A-600” 2000; Gajjar 2017; Ictsd, ICTSD, and IPC 2009; World Intellectual Property Organization, n.d.; Hayden 2012; World Intellectual Property Organization et al., n.d.; Sood 2007; American Contractors Exam Services and Prince 2015; Jung et al. 2019; Bogdanovic et al. 2019; Gaur 2019; Sinha 2015; Isebrands and Richardson 2014; Li et al. 2019; Gao et al. 2019; Pignot 2019; Pu et al. 2019) Curiously, number of cases under Cyber Crimes identifying with Counterfeiting of cash/Stamps remained at 49 wherein 124 people were captured during 2002. Of the 46,271 cases detailed under Cheating, the Cyber Forgery (167) represented 0.4 percent. Of the all out Criminal Breach of Trust cases (14,027), the Cyber fakes (510) represented 3.6 percent, of the Counterfeiting offenses (1522), Cyber

Counterfeiting (59 out of 1522) offenses represented 3.9 percent.(Stephen 1872; Nappinai 2017; Sharma, n.d.; Gandhi and India 2006; Ormerod, Smith, and Hogan 2011; Richardson 2019; Halder and Jaishankar 2016; Commonwealth Secretariat 2001; Koops and Brenner 2006; “IPC. IPC Releases ‘F’ Revision of IPC-A-600” 2000; Gajjar 2017; Ictsd, ICTSD, and IPC 2009; World Intellectual Property Organization, n.d.; Hayden 2012; World Intellectual Property Organization et al., n.d.; Sood 2007; American Contractors Exam Services and Prince 2015; Jung et al. 2019; Bogdanovic et al. 2019; Gaur 2019; Sinha 2015; Isebrands and Richardson 2014; Li et al. 2019; Gao et al. 2019; Pignot 2019; Pu et al. 2019; Wang et al. 2019; Agreli et al. 2019)

Research Questions

- 1.Do you think that cyber crime is punishable?
- 2.Are you aware that cyber crime is an element from conventional crime?

RESEARCH HYPOTHESIS

Ho: There is no significant association between age and cyber crime

H1: There is a significant association between age and cyber crime

RESEARCH METHODOLOGY AND METHOD

The present paper was analysed through the non-doctrinal research methodology and empirical and descriptive method of research was used. The present analysis was made through random sampling method where the survey was taken from common public, professionals, etc. The sample size 1597 in the present analysis is samples, the independent variable is in the analysis is gender and the dependent variables is reliable on the statement that whether they are aware of technical barriers set on imports and exports or not. The research tools used in the present paper such as cross tabulation, chi-square and case summary and graphical representation was also used to analyse the study. Data for this research is collected from primary and secondary sources.Data collection methods are:

- Books and articles
- Magazines
- Journals

ANALYSIS and Suggestions

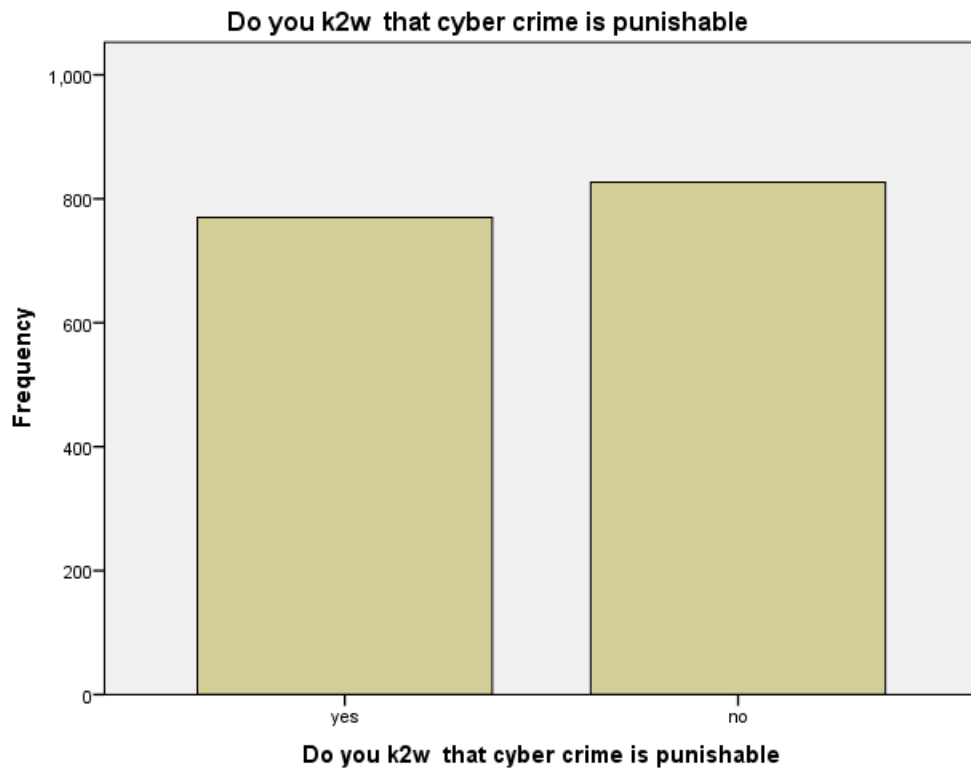
Table 1.1: Age of sample

age

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid below 20	226	14.2	14.2	14.2
21-30	518	32.4	32.4	46.6
31-40	336	21.0	21.0	67.6
41-50	302	18.9	18.9	86.5
above 50	215	13.5	13.5	100.0
Total	1597	100.0	100.0	

Do you know that cyber crime is punishable

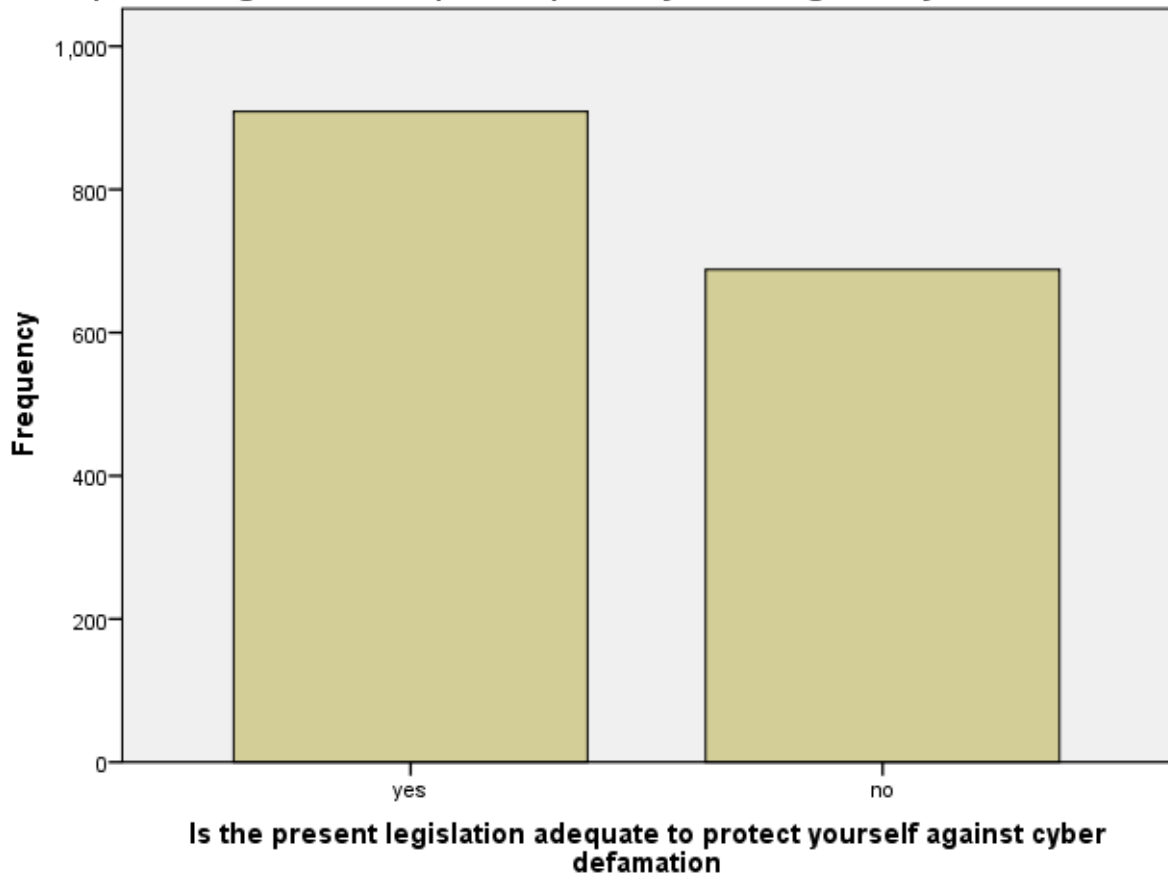
	Frequency	Percent	Valid Percent	Cumulative Percent
Valid yes	770	48.2	48.2	48.2
no	827	51.8	51.8	100.0
Total	1597	100.0	100.0	



Are you aware that cyber crime is an element from conventional crime

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid yes	721	45.1	45.1	45.1
no	876	54.9	54.9	100.0
Total	1597	100.0	100.0	

Is the present legislation adequate to protect yourself against cyber defamation



age * Do you know that cyber crime is punishable?

	Value	Asymptotic Standardized Error ^a	Approximate T ^b	Approximate Significance
Interval by Interval Pearson's R	-.106	.025	-4.276	.000 ^c
Ordinal by Ordinal Spearman Correlation	-.094	.025	-3.765	.000 ^c
N of Valid Cases	1597			

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.

c. Based on normal approximation.

TABLE 1.4:CYBER Crime with provisions under IPC

	Value	Asymptotic Standardized Error ^a	Approximate T ^b	Approximate Significance
Interval by Interval Pearson's R	.010	.025	.381	.703 ^c
Ordinal by Ordinal Spearman Correlation	.007	.025	.281	.779 ^c
N of Valid Cases	1597			

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.

c. Based on normal approximation.

Since the Pearson Chi-Square value is 0.000 is less than 05 there is a significant relationship between dependent variable and independent variable.If the Chi-square value is greater than 0.05 then there would be no significant association between dependent and independent variable. Hence alternative hypothesis is accepted.

DISCUSSION

It can be observed from the above table that the percentage of people of above 20 years who have responded to the survey questions is 14.2% and people between 21-30 years are about 32.4%.Within the age group of 31-40 years 21.0% of people have responded.Finally 18.9% people have responded under the age group of 41-50 and above 50 is 13.5%. Since the Pearson Chi-Square value is 0.000 is less than 05 there is a significant relationship between dependent variable and independent variable. The Chi-square value is greater than 0.05,there is no significant association between dependent and independent variable. Hence alternative hypothesis is accepted.

CASE LAW ANALYSIS:

The case of **State of Tamil Nadu v. Suhas Katti** can be considered as a landmark case in the history of Cyber Crime Management in India. This was the first case in India wherein the offender was convicted under S.67 of the IT ACT 2000 of India.

Judgement- On November 5 2004, the accused was found guilty by the magistrate of the offence under the section 469 509 of IPC and 67 of It Act 2000. The offender was sentenced with 2 years of rigours imprisonments under the section 469 of IPC and one year imprisonment and Rs 500 fine under section 509 of IPC.

The case of **Nascom v. Ajay Sood and Others** is another landmark judgement delivered in March 2005, in which the Delhi High Court declared ‘**Phishing**’ on the internet to be an illegal act. Though there is no specific legislation in India to penalise phishing, the court defined it under Indian Law as “a misrepresentation made in the course of trade leading to confusion as to the source and origin of the email causing immense harm not only to the consumer but even to the person whose name, identity or password is misused”.

New multimedia and technology have become part of our daily lives in contemporary society and has made our life easier, quicker and cheaper in many ways. Such tremendous utility of Information Technology encourages the terrorists and other deviants in the society to sometimes use it as a tool or target to achieve their wrongful ends. This is not only a national issue of concern but a global one. Hence regulations must be made stringent to combat it.

Judgement-The Delhi HC stated that even though there is no specific legislation in India to penalise phishing, it held phishing to be an illegal act by defining it under Indian law as “a misrepresentation made in the course of trade leading to confusion as to the source and origin of the email causing immense harm not only to the consumer but even to the person whose name, identity or password is misused.” The court held the act of phishing as passing off and tarnishing the plaintiff’s image.

SUGGESTION

Several initiatives have been taken to ensure awareness among police and judiciary. These exercises have to be balanced with sensitisation programmes to ensure that the persons involved in the system understand the effects of cyber crime and act expeditiously. There are, however, many old systemic problems. Also, there is rampant abuse and misuse of the provisions of the IT Act due to its opacity. Lack of awareness among users merely aggravates this problem. Absence of awareness either of the laws or of their applicability makes people

vulnerable to cyber crime. Until the legal system demonstrates robustness, even irrespectively . Hygiene in the digital world is as important as again as in the real and may protect each and every individuals the harm that a cyber attack may cause.

Recommendations

- Awareness should be created among the public.
- Punishments can be increased for cognizable offence.
- Service providers should be held responsible.
- Computer knowledge and awareness should be increased and created.
- Cyber crime can be reduced if the punishments are classified more clearly

CONCLUSION

The intense volume of information and an easy way of transferring it on the Internet makes it a critical source for cyber crime. After researching on the aforesaid topic, it can be said that the present scenario of India regarding laws do not have an adequate approach towards cases of cyber crime. Also, IPC provisional laws should be sufficiently flexible to be applied to all sections. As the IPC laws in the era of the Internet, it becomes practically impossible to apply the principle of 18th and 19th-century cases to the issues arising on the Internet in the 21st century. Despite the fact that the IPC existed long before the internet was created, it is still applicable to govern the law on cyber crime in certain situations. Nonetheless, the complexity of online crime and its materials must be taken into account and any restrictions must be clearly set out in laws, be based on compelling grounds, be proportionate and necessary. Thus there is a pressing need for new amendments to be made to the IPC and the IT Act, especially with regard to the publication rule and defences available for online Harassment.

Reference

1. Agreli, Heloise, Fiona Barry, Aileen Burton, Sile Creedon, Jonathan Drennan, Dinah Gould, Carl R. May, et al. 2019. "Ethnographic Study Using Normalization Process Theory to Understand the Implementation Process of Infection Prevention and Control Guidelines in Ireland." *BMJ Open* 9 (8): e029514.
2. American Contractors Exam Services, and Christopher Prince. 2015. *DEWALT*

- Plumbing Licensing Exam Guide: Based on the 2015 IPC.* Cengage Learning.
3. Bogdanovic, Jasmina, Serge Petralito, Simone Passerini, Hugo Sax, Tanja Manser, and Lauren Clack. 2019. "Exploring Healthcare Providers' Mental Models of the Infection Prevention 'Patient Zone' - a Concept Mapping Study." *Antimicrobial Resistance and Infection Control* 8 (August): 138.
 4. Commonwealth Secretariat. 2001. *Law in Cyber Space.* Commonwealth Secretariat.
 5. Gajjar, Parmesh. 2017. "IPC Quick Start Guide: IPC Programming for Inspect-X." <https://doi.org/10.3927/59340663>.
 6. Gandhi, B. M., and India. 2006. *Indian Penal Code.*
 7. Gao, Hanfei, Yuchen Qiu, Jiangang Feng, Shuang Li, Huijie Wang, Yuyan Zhao, Xiao Wei, et al. 2019. "Nano-Confined Crystallization of Organic Ultrathin Nanostructure Arrays with Programmable Geometries." *Nature Communications* 10 (1): 3912.
 8. Gaur, Krishna Deo. 2019. *Commentary on the Indian Penal Code: As Amended by the Criminal Law (Amendment) Act, 2018 (Act No. 22 of 2018).*
 9. Halder, Debarati, and K. Jaishankar. 2016. *Cyber Crimes against Women in India.* SAGE Publications India.
 10. Hayden, Mary. 2012. *Taking the IPC Forward: Engaging with the International Primary Curriculum.* John Catt Educational Ltd.
 11. Ictsd, ICTSD, and IPC. 2009. "ICTSD-IPC Platform on Climate Change Agriculture and Trade." https://doi.org/10.7215/ag_ib_20091001.
 12. "IPC. IPC Releases 'F' Revision of IPC-A-600." 2000. *Circuit World.* <https://doi.org/10.1108/cw.2000.21726cab.005>.
 13. Isebrands, Jud G., and Jim Richardson. 2014. *Poplars and Willows: Trees for Society and the Environment.* CABI.
 14. Jung, Anna, Felix Arlt, Maciej Rosolowski, and Jürgen Meixensperger. 2019. "Early Prognostication after Traumatic Brain Injury: Specific Validation of the IMPACT Prognostic Calculator in a Level 1 Trauma Center." *Journal of Neurological Surgery. Part A, Central European Neurosurgery*, August. <https://doi.org/10.1055/s-0039-1685137>.
 15. Koops, Bert-Jaap, and Susan W. Brenner. 2006. *Cybercrime and Jurisdiction: A Global Survey.* T.M.C. Asser Press.

16. Li, Zhuang, Shengzi Zhang, Wenhao Xing, Zheshuai Lin, Jiyong Yao, and Yicheng Wu. 2019. “BaSrPbOCl: The First Alkali-Earth Metal Lead(ii) Oxyhalide with an Intriguing Multimember-Ring Layer.” *Dalton Transactions* , September. <https://doi.org/10.1039/c9dt02839k>.
17. Nappinai, N. S. 2017. *Technology Laws Decoded*.
18. Ormerod, David, John Cyril Smith, and Brian Hogan. 2011. *Smith and Hogan's Criminal Law*. Oxford University Press.
19. Pignot, G. 2019. “[Role of the nurse in the implementation of enhanced recovery after surgery].” *Progres en urologie: journal de l'Association française d'urologie et de la Société française d'urologie*, August. <https://doi.org/10.1016/j.purol.2019.08.269>.
20. Pu, Ya-Lou, Zhuang-Shuang Li, Xiao-Xu Zhi, Yi-An Shi, Ai-Feng Meng, Fang Cheng, Ali Ali, Cheng Li, Hong Fang, and Cheng Wang. 2019. “Complications and Costs of Peripherally Inserted Central Venous Catheters Compared With Implantable Port Catheters for Cancer Patients: A Meta-Analysis.” *Cancer Nursing*, August. <https://doi.org/10.1097/NCC.0000000000000742>.