International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

Criminal Law in India and Cybercrimes: Problems and New Perspectives

Dr Manoj Kumar Sadual

Associate Professor, P.G. Department of Law, Utkal University, Bhubaneswar, Odisha, India

Abstract: ***As a center for information technology, India is also growing into a significant location where cybercrimes against innocent users of new technologies are becoming more commonplace on a daily basis. In such circumstances, it becomes imperative to defend citizens' rights against lawbreakers who prey on the gullibility of the general public. The cyber world has caused all technology solutions to evolve to the point where there is now a generational divide between those who have grown up with these and those who have not. India has a widening gap between its rich and poor populations, as well as greater than average levels of poverty and poor education. Consequently, for these reasons, the generation gap widens even further. As a result, it is the duty of both legislators and law enforcement to establish effective legal frameworks to handle cybercrimes that occur in virtual environments, which are very challenging to police using physical means. Thus, the purpose of this paper is to evaluate the legislative structure and determine how effective it is at regulating cybercrimes in India.***

Keywords: Cybercrime, Criminal Law, Cyber Law, Challenges, Information Technology

1. Introduction

Since the invention of Internet, its users are increasing day by day across the globe. in India too, the number of internet users are increasing and surprisingly India surpassed the number in US where US users amounts to only 4.4% population of global internet users while India amounts to 17.2% of total global users. Majority of the population using internet in India belongs to age group of less than 30 years which indicates that the workforce in India is basically dependent on IT based technologies as a result of which IT and Business Process Outsourcing Industries have gained global prominence in India. However, we must also acknowledge that this internet has also created a virtual world with no borders and to some extent with very limited regulatory control across the world. Many activities can take place through internet where the actors might not get recognized. In such cases it becomes quite difficult to regulate criminal activities and to secure the virtual world with legal rules that are fit for real world but may not suit the virtual world. This Article therefore will make an attempt to analyze the Indian legal framework over the matter of regulating cyber-crimes in the virtual cyber world especially at such a time when the process of digitalization has increased to a significant level.

Briefly conceptualizing cybercrimes

Cybercrimes in a narrow sense refers to all those illegal activities committed through a set of electronic operations targeting the security of either the computer systems or the data possessed by them.[1] While in a broader sense, cyber-crimes can be referred to all illegal behavior or activities committed in relation to a computer system or network that even includes possessing, offering, distributing or sharing of information through the means of such computer systems or network. The Budapest Convention is the first International Legal Instrument that was adopted primarily with the objective of introducing a uniform set of regulations at the international level for combating various forms of cyber offences. It even became the first legal instrument to connect cyber offences with human rights violations.[2] The principal categories of cyber offences as defined by this Convention are - data interference, illegal access, misuse of devices, illegal interception, computer related fraud or forgery, offences related to copyright, neighboring rights and child pornography. Later publication of any content with racist or xenophobic propaganda was also made a criminal offence by an Additional Protocol to this Convention. At present even cyber terrorism has also been included within the scope of this Convention. From these facts, it can be argued that the scope of cyber offences is much broader to even include all activities that are illegally committed through a computer system, mobile phones, networking, or any electronic device and even may include those illegal activities that are not committed through electronic devices or networking as such but are committed in order to target such devices. There is no universally acceptable definition of cybercrime and also, in India no clear definition of cybercrimes or offences has been provided under any of the laws including IT Act of 2000 and 2008.[3] It is therefore essential to analyze the provisions of various laws that deal with cyber offences along with their different categories that have taken place or have been committed in India.

Highlights of Cyber Laws in India

1) Information Technology Act, 2000

Indian cyber laws are governed by the Information Technology Act, which was implemented in 2000. This Act's major purpose is to provide secure legal protection for ecommerce by making it easy to register real-time records with the government. A number of changes were made as cyber criminals got cleverer, as well as the human proclivity

[1] Boruah, Jayanta, Cyber Crimes and Its Legal Challenges in India (October 17, 2020). The Journal of Legal Methodology Policy and Governance, Volume 2 Issue 1, ISSN: 2581-8554), Available at SSRN: https://ssrn.com/abstract=3819497

[2] Kumar, R., Pattnaik, P. K., & Pandey, P. (Eds.). (2017). Detecting and Mitigating Robotic Cyber Security Risks. IGI Global. https://doi.org/10.4018/978-1-5225-2154-9

[3] A Reyes et al, Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement , and Prosecutors. (1st Edn, Rockland, Syngress. 2007) p. 24

Licensed Under Creative Commons Attribution CC BY

to misuse technology. The ITA emphasizes the heavy sanctions and penalties that protect the e-governance, e-banking, and e-commerce businesses, which were passed by India's Parliament. ITA's scope has been broadened to encompass all of the most contemporary communication devices.

The IT Act is the most significant; as it directs all Indian legislation to strictly regulate cybercrime:

a) Section 437 [Penalty and compensation] for damage to computer, computer system, etc.–If any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network.
b) Section 668 Computer related offences - If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakhs rupees or with both.
c) Section 66B9 Punishment for dishonestly receiving stolen computer resource or communication device - 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 lakhs or with both.
d) Section 66C10 Punishment for identity theft– Whoever, fraudulently or dishonestly make use of the electronic signature, password, or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakhs.
e) Section 66D11 Punishment for cheating by personation by using computer resource- Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

2) Indian Penal Code (IPC) 1980

The Indian Penal Code (IPC), 1860, and the Information Technology Act of 2000 are both used to prosecute identity theft and related cyber offences.

"The primary relevant section of the IPC covers cyber frauds:

a) Forgery (Section 464)
b) False documentation (Section 465)
c) Forgery pre-planned for cheating (Section 468)
d) Reputation damage (Section 469)
e) Presenting a forged document as genuine (Section 471)

Categories of cybercrime and cyber laws in India

As the world is moving towards being a single interconnected web with highly sophisticated digital devices, people have indulged in executing even more sophisticated crimes which are easy to commit, hard to detect and even harder to locate in judicial terms. In India, cybercrime has been majorly targeted to the following broad categories:

- Cybercrime against Individual
- Cybercrime against Property
- Cybercrime against government

Each category here undertakes various methods for its implementation which can be different for each criminal. With the increased use of technology, the thrust to misuse the technology has amplified to its peak level resulting in new strict laws being enforced to regulate the criminal activities. Indian Parliament has passed its Information Technology Act, 2000 followed by Information Technology Amendment Act, 2006, Information Technology Amendment Act, 2008 and Information Technology (Intermediaries guidelines) Rules, 2011 to fill up the loopholes in previous laws. Information Technology Act, 2000 deals with the technology in the field of e-commerce, e-governance, e-banking as well as penalties and punishments in the field of cybercrimes.

Cybercrime against Individual Cyber Bullying

This category of cybercrime includes cyber stalking, cyber bullying, distributing pornography, trafficking and grooming. Today government has been actively taking various steps so that the criminals behind such act can be punished.

Cyber bullying is defined as use of any communicating device to bully any individual by sending messages which are threatening or daunting in nature. The intension of cyber bullying is to harm person's reputation, his state of mind or to humiliate him socially or personally where victim suffers adverse effects. The person committing this crime can be a known person of victim or he can be completely unknown to him. The act uses technological advancement like internet, group chat rooms, messaging services, e-mails, social media, etc. It can be executed in form of posting obscene photos or writing defamatory texts or sending e-mail with obscene content. The effect of cyber bullying is mostly found in teenagers and unfortunately many of these harassers are also found under age. The statistics based on different survey shows that India is among top five countries that are affected by this crime and also a country having highest criminals.[4]

Existing Law to deal with Cyber Bullying

Cyber bullying is one of the cruel acts which leave its mark upon the victim for his entire life. As the victims are bullied over cyber space which spreads the message swiftly and to places the impacts on their life, mentally and emotionally, can be grave. So there is a need for a strict law to be enforced so that the offender can be punished and fair justice could be availed.[5]

The ITAA – 2008 includes the remedies under which a case can be registered, but there is no particular act against cyber bullying. Cyber bullying can take place in various forms so based on the form of bullying; action against the bully could be taken.

[4] Halder, Debarati & Karuppannan, Jaishankar. (2012). Cyber Crime and the Victimization of Women: Laws, Rights and Regulations. 10.4018/978-1-60960-830-9.

[5] Preventing Bullying Through Science, Policy, and Practice, Academies of Sciences, Suzanne Le Menestrel, Frederick Rivara, National Academies Press, 2016

Licensed Under Creative Commons Attribution CC BY

Section 66A deals with sending offensive messages through communication device where the victim is send offensive information or false information or information pointing out the character of victim is send with an intension of antipathy, enmity etc. Here if the victim is sent email or any other form of message through computer, mobile or other communicating device which is belligerent in nature then action could be taken against the person under this act. If the person is found guilty, then punishment up to three years of imprisonment or fine or both could be levied.

Similarly, sending obscene material in any electronic form is dealt under section 67 of the ITAA – 2008. Offenders posting mean pictures on social media or in any electronic form could be charged under this section. If found guilty, then punishment is imprisonment up to five years and fine up to ₹5,00,000. Subsections of Section 67 can also be charged based on the obscene material transmitted. Section 67A deals with the transmitting of material containing sexually explicit act whereas Section 67B which specifies of transmitting material depicting children in sexually explicit act in an electronic form can be taken into account based on offense carried out. Although these laws exist there are some loopholes which need to be addressed by the law makers and Supreme Court of India.

a) IT Act -2000 or its amendments do not specify anywhere the provisions or judicial procedures for crime like cyber bullying. It has to be handled under the existing sections of IT Act.
b) There is no law mentioning proper age for usage of electronic device like mobile phones which are used for sending offensive messages to other people.
c) The Anti-Ragging Act prevalent in many states of India can deal with the bullying but there is no uniform law around India for the same.
d) IT Act 2000 does not specify any provision for safeguarding of children.

Cybercrime against Property Data theft

Data theft is a deep penetrating problem in cyber world. The problem is related to the act of stealing computer based information. One of the recent types of data theft encountered is ―Ransomware, a type of Trojan virus which usually infects your device through fake software updates, in the form of phishing email or spam. Post infection the device is held as hostage by encrypting data and demanding ransom payment for decrypting the same. Payment is demanded in the form of bitcoin. Wannacry ransomware attack one of its kind usually attack Microsoft OS. The target of this crime has been mostly business and public institutions.[6]

Laws that can be enforced on the attacker of ransomware in accordance with the types of crime committed under various sections are

- Section 72 - Breach of confidentiality and privacy - Ransomware is a clear act against right to privacy and henceforth the culprit can be convicted under this law. According to section 72 under information act 2000, which states that any person who has secured access to any electronic record, book, register document information without the consent of concerned person shall be considered liable to punishment. Punishment: imprisonment for a term which may extend up to 2 years or a fine which may extend to 1 lakh or both.
- Section 66 - Hacking with computer system, data alteration - The attacker of ransomware can also be found guilty under this law as well which states that any person trying to destroy, delete or alter any information that resides on public or person's computer thereby decreasing its utility by any means commits hacking. Punishment: Any person involved under this type of crime could be sentenced up to 3 years of imprisonment or a fine that may extend 2 lakh or both.
- Section 383- Extortion - This section states that whoever intentionally puts any person in fear of any injury to that person, or to any other, and thereby dishonestly induces the person so put in fear to deliver to any person any property, or valuable security or anything signed or sealed which may be converted into valuable security, commits Extortion.
- Ransomware can also be a type of extortion as the victim is put to fear of loss of data which forces him/her to forcefully deliver his/her financial resource in terms of bitcoin. Punishment: person found guilty shall be punished with imprisonment which can extend up to 3 years or with a fine or both.

Cybercrime against Governments Hacking of government sites

Hacking is to exploit any computer resources or any computer on a network by gaining unauthorized access to the system or network. As India is moving towards digitization, government has taken steps to digitize many of the government related works which means that the public data is maintained online. Despite of various security measures the statistics suggest that there is an increase in cases registered for hacking of government sites which causes panic in public to be a part of digitization. This vulnerability in terms of security puts India down in the race of future digitization. This calls for the government to impose strict cyber laws as well as increase the security of the existing data.[7]

According to the statistics, approximately 707 websites including state and central government have been hit due to security lapse in the past four years. According to minister of state of home affairs, website of NSG – National Security Guard which handles the counter terrorism force was hacked as reported on January 1, 2017. The hackers posted abusive messages on the site on account of which the site was blocked with immediate effect. Major cases which were reported earlier were:

- Indian Space Research Organization – ISRO - The official site was hacked and users visiting the site were deviated to some buying portal. Later a 404 error was encountered on the webpage.
- Central Bureau of Investigation – CBI - The hackers have made a sarcasm being able to hack India's premiere investigating agency CBI in December 2010. The

[6] Leonidas Deligiannidis, Charlie Wiseman, Mira Yun, Hamid R. Arabnia, Emerging Trends in ICT Security, Elsevier Inc. Chapters, 2013

[7] Akash Kamal Mishra, An Overview on Cybercrime & Security, Volume - I, Notion Press, 2020

Licensed Under Creative Commons Attribution CC BY

hackers left the warning message to Indian Cyber Army claiming to hack many other websites.

- Indian Army - In April 2015, the principle comptroller of defense accounts (PCDAO) was reportedly hacked creating a panic among the army officers who failed to access their crucial data from the site.

The trend has shown a consistent increase over the years for hacking of government websites.

In 2014, a total of 155 government websites were hacked. In 2015, the number rose to 164. Last year, it was 199. This year, the number could reach 250 at current rates.

Laws applicable for Hacking

Section 66 of Information Technology Act 2000 specifies that hacking with computer system, data alteration is an offence. This section describes that whoever with the purpose or intension to cause any loss, damage or to destroy, delete or to alter any information that resides in public or any person's computer is an offender. Diminish its utility, values or affects it injuriously by any means commits hacking. There is no alternative law specifying the hacking related to government sites, the above stated law is applied.

Any person found guilty is liable for a three year imprisonment or more with a fine that may extent up to one lakh. According to government agencies, 8348 persons were arrested under different provisions of cyber law, of which 315 were convicted.[8]

2. Conclusion

No one can deny the positive role of the cyber space in today's world either it be political, economic, or social sphere of life. But everything has its pros and corns, cyber terrorists have taken over the technology to their advantage. To curb their activities, the Information Technology Act 2000 came into existence which is based on UNICITRAL model of Law on e-commerce. It has many advantages as it gave legal recognition to electronic records, transactions, authentication and certification of digital signatures, prevention of computer crimes etc. but at the same time is inflicted with various drawbacks also like it doesn't refer to the protection of Intellectual Property rights, domain name, cyber squatting etc. This inhibits the corporate bodies to invest in the Information technology infrastructure. Cryptography is new phenomenon to secure sensitive information. There are very few companies in present date which have this technology. Other millions of them are still posed to the risk of cyber crimes.

There is an urgent need for unification of internet laws to reduce the confusion in their application. For e.g. for publication of harmful contents or such sites, we have Indian Penal Code (IPC), Obscenity Law, Communication Decency law, self regulation, Information Technology Act 2000 , Data Protection Act, Indian Penal Code, Criminal Procedure Code etc but as they deal with the subject vaguely therefore lacks efficient enforceability mechanism. Due to numerous Laws dealing with the subject there lays confusion as to their applicability, and none of the Law deals with the subject specifically in toto. To end the confusion in applicability of Legislation picking from various laws to tackle the problem, I would suggest unification of laws by taking all the internet laws to arrive at Code which is efficient enough to deal with all the problems related to internet crimes. Although these legislations talk about the problem but they don't provide an end to it. There's need for a one Cyber legislation which is co-ordinated to look after cyber crimes in all respects. With passage of time and betterment of technology in the present date, has also resulted in numerous number of Information technology related crimes therefore changes are suggested to combat the problem equally fast.

Crucial aspect of problem faced in combating crime is that, most of the countries lack enforcement agencies to combat crime relating to internet and bring some level of confidence in users. Present law lacks teeth to deter the terrorist groups for committing cyber crimes if you see the punishment provides by the Act it's almost ineffective, inefficient and only provides punishment of 3 years at the maximum. Harsher laws are required at this alarming situation to deal with criminals posing threat to security of funds, information, destruction of computer systems etc. Data protection, by promotion of general principles of good information practice with an independent supervisory regime, would enable the law to maintain sufficient flexibility to achieve an appropriate balance between the need to protect the rights of the individuals and to have a control over the way their personal information have been used would be helpful in this increasingly networked economy. Just having two provisions in the Information Technology Act, 2000 for protection of data without any proper mechanism for to tackle the crime makes their mention in the Act redundant.

Information Technology Act is applicable to all the persons irrespective of their nationalities (i.e. to non-citizens also) who commits offence under the Information Technology Act outside India, provided the act or conduct constituting the offence or contravention involves computer, computer systems, or computer networks located in India under Section 1 and Section 75 of the Information Technology Act, but this provision lacks practical value until and unless the person can be extradited to India. Therefore it's advised that we should have Extradition treaties among countries. To make such provisions workable.

It's like "eye for an eye" kind of situation where the technology can be curbed only by an understanding of the technology taken over by cyber terrorists. Even if the technology is made better enough to curb the computer related crime there is no guarantee if that would stay out of reach of cyber terrorists. Therefore Nations need to update the Law whether by amendments or by adopting Sui generic system. Though Judiciary continues to comprehend the nature of computer related crimes there is a strong need to have better law enforcement mechanism to make the system workable.

[8] M. Dasgupta, Cyber Crime in India: A Comparative Study, Eastern Law House, 2009

Licensed Under Creative Commons Attribution CC BY