International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 6 1256 – 1260

Cybercrime and Cyber Law Pertaining to India: An analysis

Shinde Kashmira Jayvant
Assistant Professor, BCA,
vnsgu,
Surat, Gujarat, India
kashmira25.89@gmail.com

Rekha P.
Assistant Professor, BCA,
vnsgu,
Surat, Gujarat, India
rekha.sarnoth1208@gmail.com

Abstract—No stones are untouched by technology which gives rise to various refined crimes performed by so called intellectual criminals. The crimes performed using technology is termed as cybercrime. This paper tries to give insight on the broader areas effected by cybercrime in India. It also tries to associate various laws under various sections of IT Act 2000 which can be levied upon the culprit. It focuses on three categories of crime, viz. crime against individual, crime against property and crime against government. The paper tries to give insight on the loopholes as well as statistics of various cybercrimes in India.

Keywords-*cybercrime, cyber law, cyber bullying, ransomware, hacking*

*****

I. Introduction

We live in an era where growth of technology has given liberty to connect ourselves to anybody around the globe. This has also led to various types of crimes using new and highly sophisticated technological tools. The use of technology to commit a crime where a computer is a target or a tool is called cybercrime. Cybercrime may range from anything as simple as downloading illegal music files to stealing millions of dollars from online bank accounts. In India, according to Information Technology Amendment Act 2008 (ITAA - 2008), cyber-security has been defined as "Cyber-Security means protecting information, equipment, devices, computer, computer resource, communication device and information stored therein from unauthorized access, use, disclosure, disruption, modification or destruction". Thus from this we can infer that, anything that interrupts our information stored in computer system or interrupts computer itself is breaching the system security. The device may be used as tool to perform crimes such as Harassment via E-Mails, Cyber-Stalking, Dissemination of Obscene Material, Hacking, E-Mail Spoofing, Child Pornography, Internet Phishing, Cyber Squatting, Cyber Vandalism, Virus, Cyber Terrorism, Distribution of pirated software, Possession of Unauthorized Information. The intensity with which the above crimes are affecting our lives has increased the momentum of creating affective laws to combat against these crimes. The government of various countries have enforced laws known as cyber laws and in India these laws are contained under Information Technology ACT 2000 (IT Act 2000), which was effective from October 17, 2000.

Widely effected areas 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

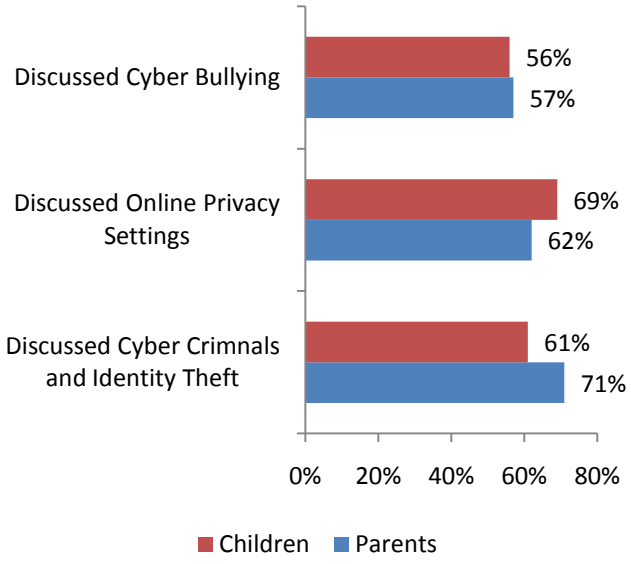
ISSN: 2321-8169
1256 – 1260

various steps so that the criminals behind such act can be punished.

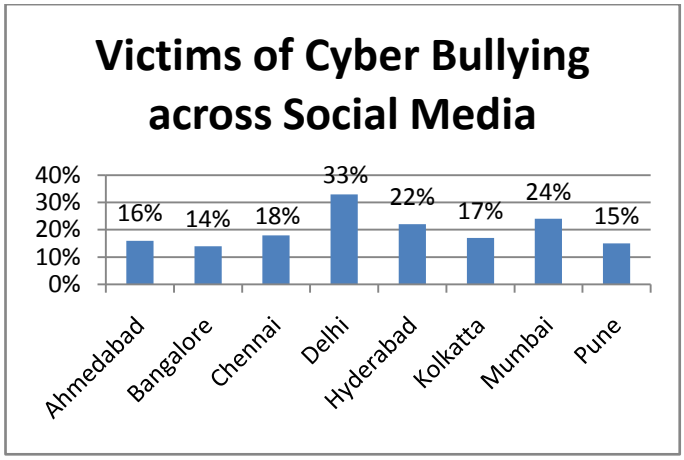
Cyber bullying is defined as use of any communicating device to bully any individual by sending messages which are threatening or daunting in nature. The intension of cyber bullying is to harm person's reputation, his state of mind or to humiliate him socially or personally where victim suffers adverse 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.

Based on the survey conducted by global research company Ipsos, 32% parents complain their child as victim of cyber bullying. This is much higher compared to countries around the world where12% parents complain the same. The same survey reveals that frequency of cyber bullying in India – 32% is much higher than other countries like US – 15%, UK – 11 % while Japan – 7% of children are affected. According to another study carried out by Intel Security's "Teens, Tweens and Technology Study – 2015", about 81% of the users of age group eight to sixteen are active on social media networks of which 22% have being bullied over network which places India on fourth position in Cyber bullying. 52% of Indian Children have bullied people over social media was also resulted in this study. It was also found that victims were being bullied more than once. The survey of Ipsos reports that 60% of bullying has been carried out through social networking sites like Facebook while 42% says it is through some electronic communicating device as cellular phone. The online chat rooms contribute to 40% of cyber bulling and 32% through emails are the major contributor forms in cyber bullying. The study shows that India has 57% people concerned about cyber bullying which is lower than other countries like Australia with 88% people concerned with cyber bullying, USA 80% and Singapore 71% people concerned about it.

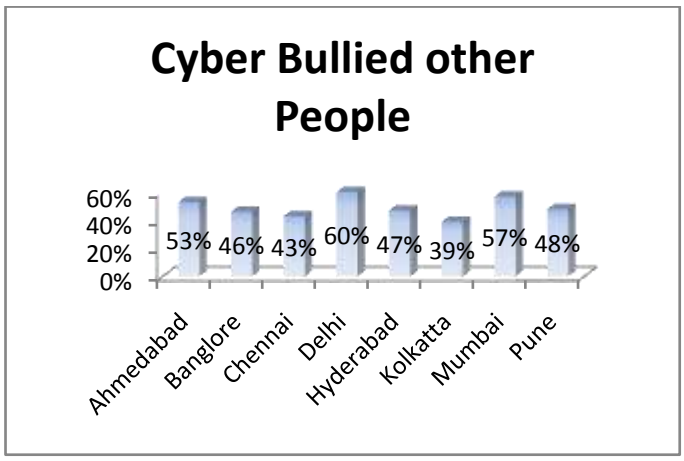
The chart predicting the most discussed topic in India for parents and children based on Intel's survey



Cyber Bullying experienced on social media's across different states

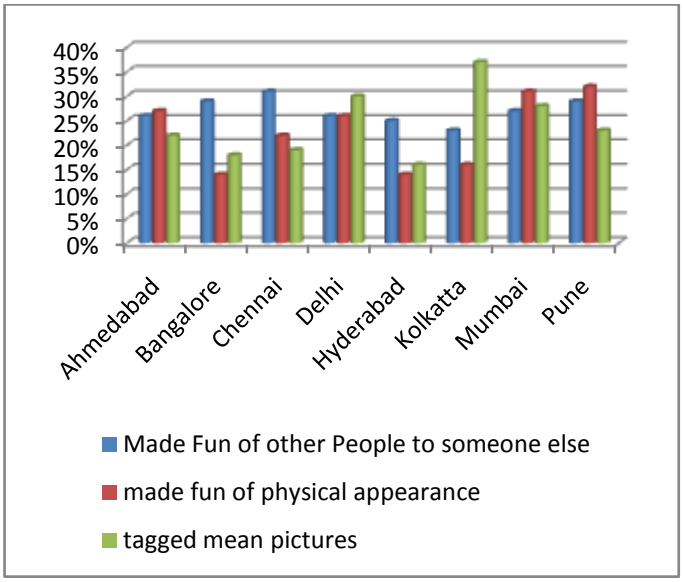


Children bullied people over social media



 ISSN: 2321-8169
1256 – 1260

Contribution Factorsof bullying over social media



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.

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.

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.

- 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.
- 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.
- 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.
- 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.

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.

 ISSN: 2321-8169
1256 – 1260

- 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 fearof 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

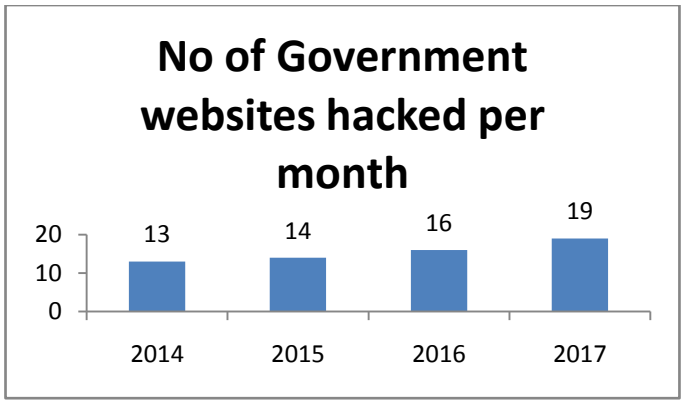
Hacking is to exploit any computer resources or any computer on a network by gaining unauthorized access to the system or network. As India is moving towards digitization, government has taken steps to digitize many of the government related works which means that the public data is maintained online. 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.

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 hackers left the warning message to Indian Cyber Army claiming to hack many other websites.
- Indian Army - In April 2015, the principle comptroller of defence 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.

 ISSN: 2321-8169
1256 – 1260

According to government agencies, 8348 persons were arrested under different provisions of cyber law, of which 315 were convicted.

II. Conclusion

These were just the few instances of the various cybercrimes faced by the users of the country. This shows the lack of awareness and security measures being taken by technocrats. While writing this paper we encountered many pit holes in the Indian Cyber Laws which could be further improved by providing cyber law for every specific crime. It is the need of the day for special cyber courts giving verdicts for cybercrimes in supersonic speed. We also suggest that governments of various countries follow some standard laws and combat against cybercrime. We conclude that cybercrime is a great threat to mankind, if not addressed with strict cyber rules, the day is not far where world will be at the verge of cyber war. On a positive note we are glad to note that Prime Minister's Office (PMO) has recently proposed ₹1000 crore to be utilised over a period of four years to push India's cyber security efforts.

References

[1] http://timesofindia.indiatimes.com/india/over-700-government-websites-hacked-from-2013-to-2016/articleshow/57029456.cms
[2] https://yourstory.com/2012/01/legal-action-against-hackers-and-data-theft/
[3] http://www.indiainfoline.com/article/news-top-story/kids-in-india-worst-affected-by-cyberbullying-ipsos-survey-113103005078_1.html
[4] http://www.cyberlawtimes.com/articles/105.html
[5] http://www.ijli.in/assets/docs/AshnaRishabh.pdf
[6] http://ncrb.nic.in/
[7] http://devgan.in/ipc/?a=ipc&q=extortion
[8] https://blog.ipleaders.in/ransomware-attack/
[9] The Information Technology Act, 2000, http://www.dot.gov.in/sites/default/files/itbill2000_0.pdf
[10] The information Technology Act, 2008, https://cc.tifrh.res.in/webdata/documents/events/facilities/IT_act_2008.pdf
[11] P M Bakshi, Hand book of Cyber & E-Commerce, Bharat Law House Pvt Ltd