DE JURE NEXUS LAW JOURNAL

Author:

Monika Gupta

Jyoti Vidyapeeth Women's University, Jaipur.

Law Graduate, 2020.

CYBER CRIME IMPACTS ON YOUNGESTERS

Being the second most populous country have its own perks, India is ranked 23rd among the most dangerous countries in the world. After having the largest democracy in the world, ***50% MPs(approx.)*** *in the* ***Lok Sabha*** *have criminal records. India is acknowledged worldwide for its crimes in Racketeering, Drug trafficking, Dacoity, Smuggling, Extortion, Loan sharking, Human trafficking, Money Laundering, Gambling, Murder and a new introduction in this never-ending list is* ***CYBER CRIME.***

INTRODUCTION

Cyber Crime or internet fraud. It is a new introduction in the crime list of India, it requires a computer, a network and most importantly an unsound mind. Cybercrime is a criminal activity carried out by hackers or cyber criminals to make money. It uses computer as a tool for committing fraud, Human trafficking in child (by online mode), Pornography, violating privacy or stealing Identities.

New technology often creates new criminal opportunities like earlier one must require a computer in committing hideous crimes but with upgraded technologies criminal do not need a computer to do illegal activities. Most cybercrimes are often committed to attack on personal information's, business privacy or government cooperation's. Although the attacks do not take place on a physical body instead targets the personal or virtual body.as a planet-spanning

network, the internet offers criminals multiple hiding places in the real world as well as in the network itself.

Cyber Crime comes under Information Technology Act,2000 and Indian Penal Code Act,1860 which Provides Framework for Cyber Crime Which Includes Sections 43 & 66 for hacking and data theft (which comes under IT act), Section 378,424,425, 426(which comes under IPC).

CYBER CRIME CASES IN INDIA

According to the national Crime record bureau data cybercrime cases piles up to 44,546 cases in 2019 compared to 28,248 in 2018. In 2019 India exceeded huge increased of cybercrime cases which is 63.5%

1. [1]Some ex-employees of Mphasis ltd under BPO arm breakdown US customers of CITI bank to the extent of 1.5 Crores. It was one of those crime cases that Includes the role of "DATA PROTECTION" The fraud was versatile enough to accommodate list of illegal activities such as "cheating", "conspiracy", "breach of trust" etc. According to the section 66 and 43 under IT act 2000 the persons involved are contingent for imprisonment as well as payment of the damage to the victims.
2. [2]India saw its First ever cybercrime case judgement in 2013 which arise after a complaint was filed by Sony India Pvt Ltd. In May 2002, the accused locked into the website using the identity of Barbara Campa and Ordered a Sony color television set plus a cordless headphone set. After one and a half months of the transaction which was carried by the credit card payment was alleged to be an unauthorized transaction as the real owner had denied having made the purchase. After the immediate registration of complaint about online cheating under section [3]418, 419 and 420 of the IPC Act, the matter was Investigated and Arif Azim was arrested. Later he confessed gaining illegal access to the credit card no. Of an American national which he misused on the company side.

TEENAGERS INVOLVEMENT IN CYBER CRIME

The Latest study in 2015 conducted by National Crime Agency in UK reveals that 61% of computer hackers Identified begin their activity before the age of 16. In Spain more than

[1] Pune citi bank MPhasis Call center fraud
[2] Sony.sambandh.com CASE
[3] sec 418 to 420- cheating and dishonesty

300 youngsters under the age of 15 have been investigated or detained every year for Cybercrimes. It is concluded that roughly 1 out of every 6 individuals in the UK admitted that they have attempted some kind of internet hacking.

There are many other small-scale tools for hacking so, the teenagers are easily hacked the program and involve themself in cybercrime. There are many other videos in which people teach you how to hack or how to use someone personal information.

HOW CYBER CRIME IS AFFECTING YOUNGSTERS?

Internet is becoming very popular and very habitual for everyone. Everyone wants be digital with the new technology, Fewer skills are required to commit a cyber-crime. As people need not to be a programing or computer expert to do the deed, the IT industries are aware enough of the surroundings to depict the need of low-cost variety hackers' tools. People who knows handling a simple gadget (like mobile phones, tablets, laptop, computer etc.) can easily brows the hacking tutorials on YouTube or on similar platforms.

In this time the young generation are so involved in gadget world that they also forget the outdoor activities. Also, we can say that in order to make their reel world more interesting and fake than real world unknowingly they get involved in cybercrime. For example, youngsters can reach extreme limits to win people love and affection and also for video games and try to adopt shorter ways to reach their goals fast and other useless stuff. So, these are the most common reason why youngsters get involved into all this.

To understand the impact further let's look into a general theory of crime by Gottfredson and Hirschi. This theory explains that people who are more damaged to commit a crime are those who have extreme low self-control, in different words individuals whose control is out of their hands or their emotions or undesirable behavior. The external and internal pressure of possession, usually articles of snob appeal, represents expenditure cost which is not within everyone reach through lawful channels which if coupled with high ego which is usually present at these ages, results in some teenagers try to obtain such possessions through illegal methods.

An example to explain young behavior is that supposed some young people feel to own latest gadgets and technologies because they are influenced by their peers rather than by adults, they use it as a bench mark and try to imitate the behavior they see in their equals. This behavior is known as akers' Social learning theory. According to which criminal

behavior is learnt like any other. It justifies that if a group of equals carries out re enforces criminal conduct, the individual is more likely to imitate the same behavior specially if the output of such act means more benefit than bashing.

CONCEQUENCES OF CYBER CRIME

There are usually two types of hackers-

1. **White hat hackers:** they are appointed by companies to improve their security or finding information or avoid any mishandled of their network by hacking into their computers in a legal way
2. **Black hat Hackers:** they are considered as online dacoits from which people need two secured their valuable or personal information because they illegally break into their networks for their own pleasure.

People need to wisely choose amongst these two options of hacking career. Legal hacking would be the best option because illegal hacking has its worst consequences. Section 77A of the IT act, dictates that the breaching the words stated by IT act would directly result in imprisonment for up to 3 years, most of the cybercrimes which lies under the IT act are punishable with imprisonment of 3 years or less.

The computer fraud and abuse act- this act is a leading anti-hacking organization which was originally came into force for providing security to US government financial institution and legal entities, furthermore it was expended later on to secure all computers in the country. The act serves as a powerful frame work to ensure the best punishment for those who tries to not abide by the law. Such as, breeching national security information can end up with 10 years minimum and 20 years maximum imprisonment, someone intentionally damaging by knowing transmission could serve for 5 to 10 years conviction, trafficking in passwords can lead and individual towards maximum 10 years conviction.

Even in India, penalty for committing heinous act can held the accused for the imprisonment of 3 years, where the penalty amount can vary from crime to crime. For example, tempering with computer source course can end up with imprisonment for 3 years and fine up to Rs 2 lakhs. Whereas identity theft, dishonestly receiving stolen computer resource, cheating by personation by using computer resource can end up with 3 years imprisonment and fine up to Rs 1 lakh. However, some extreme level of hacking like cyber terrorism can result in imprisonment for life.

Leading states in cybercrime cases?

According to 2018 survey, **UTTAR PRADESH** holds the greatest number of cybercrime cases in India which counts up to 6300 cases. Whereas, Kerala now records the highest number of cybercrimes during lockdown, as Kerala also tops the higher number of literacies in India so it is likely expected that because of unemployment during lockdown brilliant minds which would have chosen to keep their mind distracted because of lack of work. The economic times report states that in Kerala places like Kannur, Kollam, Kochi, Kottayam saw the largest hits with 236, 374, 147 and 462 attacks respectively while Kerala is a whole state suffered 2000 attacks, the highest thus far in the country. This was followed by Tamil Nadu with 184 attacks and Punjab with 207.

HOW TO REDUCE CYBER CRIME IN INDIA?

The basic and the most common factor that leads not only cybercrimes but also increasing every type of illegal crimes is **heavy rate of unemployment.** As we all know how not 1000 but millions of people lost their job during the lockdown. However, the pandemic is not the only reason behind job crises in the country but also the decreasing GDP, increasing Imports, decreasing exports and etc. When India was glooming. In 2016 to 2017 it earned the tag of fastest growing economy in the world, though the worst for the country was yet to come when the country suffered crores of unemployment, exploitation of labors, the farmers, misuse of skills and underutilization of resources. ‘

1. We can point out the unawareness of people to the one of the reasons though, central government and state government has taken effective steps to spread awareness about cybercrime, issue of alerts, training of legal IT hackers, improving cyber forensic facilities etc. Our government has also launched the online cybercrime reporting portal, www.cybercrime.gov.in for immediate and online reports and complaints covering up child pornography/young sexual abuse, rape, computer hacking etc. The government steps include: 1. national critical information infrastructure protection center (NCIIPC) for procuring internal and critical information infra structure of the country.
2. Various organization came into force providing digital services have been instructed to report cybercrime incidents to **CERT-In.**

3. Cyber swachhata Kendra has been launched for perception of malicious program and free measurements to remove such programs.
4. **CERT-IN** has issued activeness and counseling groups regarding cyber threat.
5. Government has taken effective part in conducting regular training events for system/network administrator and chief information security officer of government to secure the IT infrastructure and frequent cyber-attack.

CONCLUSION

In our research we have concluded that in this era might be not all people are the sufferer to cybercrime, but they are still at the risk of losing everything they might have built from dust to glory. Nowadays people lack knowledge and acknowledgment on ongoing threat posed up on their online personal information. Criminals committing crime through computers varies, as they not always occur behind computers, but only needs to be executed by them. Hackers can live 7 continents away from there victim and can still continue its heinous crimes without letting its victims have any slightest idea about what they are onto. With increasing technology and advance systems robbers do not need to visit banks or any other institutions to rob them, they just need to sit on a sofa and have everything required on their lap plus genius mind. Their weapons don't consist of guns or knives anymore, they attack with keyboard, mouse, and passwords.

Committing cyber-crime includes consequences that not only the victims suffers but also does great damages to the accuser as well. they will not only serve life detention but self-guilt will degrade the mental health too. Doing harm to innocents is neither acceptable by the society nor by the inner conscience of an individual. Instead of using great minds in heinous crimes choose the better path in the same line of interest. Rather than working illegally use your talent in helping others like working in a company or helping them grow in IT sector, serve our nation by contributing help in security system of the country. This not only will help in earning good numbers but also gives a feeling of success and peace. People can change their lives only by the matter of choice, lives of many people depends upon some people for what they choose either they can be the reason for someone's misery or can be the reason for someone's merry. So, choose wisely because difference do exist.