International Journal of Law
ISSN: 2455-2194; Impact Factor: RJIF 5.12
Received: 19-07-2020; Accepted: 04-08-2020; Published: 20-08-2020
www.lawjournals.org
Volume 6; Issue 4; 2020; Page No. 269-271

Law`s challenge to curb growing cyber crime after Covid -19

Rup Kumar
LL.M. University Department of Law Tilka Manjhi Bhagalpur University, Bhagalpur, Bihar, India

Abstract
The digital frontier world has moved into the Coronavirus disease (COVID-19) pandemic era and into the digital maid. After the pandemic, when Lehenga has been minimized from the pitcher, and words like sachet distancing have been included in the routine of Lehenga. Like this, especially in a state like Bihar, from village to city, from the system to the people, they have come in virtual mode. Is studying online or is online meeting in the form of webinars. In banks, transactions have started taking more than e-banking and debit cards. In this case, there has been a big jump in the case of cybercrime in the crime dictionary. Cybercrime cases are increasing rapidly. But the system is not able to curb this. Nor has there been timely and expeditious research into such cases so that a quick trial of cases related to it can be done and the culprits can be punished. Due to this, the law has increased significantly in curbing cybercrime in today's time. Most of the cases are of online fraud. He is withdrawing from the bank accounts. The scope of this crime is increasing day by day by increasing the number of pilgrims and stealth. The feeling of cheating is coming when they are updating their account or the message of withdrawal of money on the mobile. Till then, the cyber thugs devour the field like a bird and there is no other option except to rub their hands in front of the laughen. There are cases of cyber frauds or online frauds that are not being reported in police stations. It is believed that in the next five years, the file of cybercrime from the police station to the court will be greatly compromised. And through the law for bars and benches, getting the contravention on this crime will be in the form of a change. In the COVID-19 pandemic, the movement of the people will be reduced during the lockdown, and instead of robbery and corruption, cyber miscreants started committing crimes online. The problem before the police is that in such cases in which online crime is committed, if the sections of the IT Act are added to it, only such cases can be investigated by the inspector level or above. Therefore, the police is also more interested in pressing such cases. Because even the police officers are neither fully aware of the cyber law nor the method of research of cyber case. Therefore, such cases in police stations become a headache for police officers. Therefore, in such cases better and scientific investigation is much less. In the manner in which cybercrime cases are increasing, it is decided that in the next five years, the government will have to set up cybercarts separately for cases related to cybercrime on the lines of speedy trials in other cases. At the same time, it is also an election in front of the bar and the bench to increase the speed of punishment in such cases so that cybercrime can be controlled. It will be a challenge for the new lawyers entering the law profession as the possibility of cybercrime increasing rapidly in the coming times. More and more the dependence of the people will increase on the mobile and the functioning of e-governance will be online and the crime will increase. The desires of the media to get involved and get connected to it are increasing all the time. Cyber crooks have also been active on Facebook, WhatsApp or on platforms related to the social media.

Keywords: information, cyber crime, digital, online information, cyber criminal, cyber space

Introduction
Cybercrime and related creaminals have no limit. Cybercrime is not easy to define because it has no limitations. New technologies create new criminal opportunities. Criminals do not need computers to commit fraud, child pornography and traffic to intellectual property, theft of an identity or violating someone's privacy. Cybercrime specifically represents crimes related to the Internet, computers and mobiles. Most cyber crime is an attack on the information of individuals, corporations or governments. An important aspect of cyber crime is its non-specific character. In workspaces they can be very vast and different from each other. This is a serious problem for law enforcement as earlier local or national crimes now require international cooperation. For example, if a person accesses child pornography on a computer in a country where child pornography is not banned, is that person committing a crime in a nation where such content is illegal. Cybercrime also includes crimes without money transactions, such as spreading viruses on other computers or posting private information of a business on the Internet. ybercrime is vastly growing in the world of tech today. Criminals of the World Wide Web exploit internet users' personal information for their own gain. They dive deep into the dark web to buy and sell illegal products and services. They even gain access to classified government information. Cybercrimes are at an all time high, costing companies and individuals billions of dollars annually. What's even more frightening is that this figure only represents the last 5 years with no end in sight. The evolution of technology and increasing accessibility of smart tech means there are multiple access points within users' homes for hackers to exploit. While law enforcement attempts to tackle the growing issue, criminal numbers continue to grow, taking advantage of the anonymity of the internet.

Bank customers falling victim to cyber crime- The number of cyber frauds in public sector banks in Bihar has increased more than double. The officials of banks are trying to deal with them. Cyber fraudsters are taking advantage of leakage in online banking and technology based banking facilities.

State Level Bankers Committee (SLBC) has also raised concerns about banking cyber fraud. Significantly, there is a bank branch in the state with a population of about 16 thousand and there are about eight crore bank accounts.

167 cyber fraud cases were reported in the year 2019-20

According to the information, in the financial year 2018-19, 78 cyber fraud cases were reported in front of public sector commercial banks in Bihar. While the number of these cases has increased to 167 by the last quarter of the financial year 2019-20. According to SLBC, there was a cyber fraud of Rs 42.05 lakh in the financial year 2018-19. Of these, recovery of Rs 36.03 lakh is still pending in 48 cases. At the same time, in the cases of 167 cyber frauds in 2019-20, there was a mess of Rs 93.77 lakh. Recovery of Rs 83.58 lakh in 147 cases remains.

6 banks are victims of cyber fraud

In Bihar, six banks have been targeted by cyber criminals and made their victims. These include Canara Bank, UCO Bank, IDBI Bank, ICICI Bank and Syndicate Bank along with State Bank of India. No cyber fraud cases were reported in Syndicate Bank in the last financial year, but so far four cases have been registered in the current financial year.

SBI: 124 cases occurred in the current financial year

Bihar has reported the most cyber fraud cases with the State Bank of India (SBI). Where 22 cases were reported in SBI in the last financial year, it increased to 124 in the current financial year. Last year, there was a cyber fraud of 19.15 lakh rupees. It recovered only Rs 2.25 lakh in two cases. A total of 14 cases related to the remaining cases are lodged in police stations and a total of Rs 16.43 lakh is still stuck in these cases.

Cybercrimes can generally be divided into two categories

Crimes that target networks or devices - Crimes using devices to participate in criminal activities
Viruses Phishing Emails
Malware Cyberstalking
DoS Attacks Identity Theft

Categories of Cybercrime

There are three major categories that cybercrime falls into: individual, property and government. The types of methods used and difficulty levels vary depending on the category.

Property: This is similar to a real-life instance of a criminal illegally possessing an individual's bank or credit card details. The hacker steals a person's bank details to gain access to funds, make purchases online or run phishing scams to get people to give away their information. They could also use a malicious software to gain access to a web page with confidential information.

Individual: This category of cybercrime involves one individual distributing malicious or illegal information online. This can include cyberstalking, distributing pornography and trafficking.

Government: This is the least common cybercrime, but is the most serious offense. A crime against the government is also known as cyber terrorism. Government cybercrime includes hacking government websites, military websites or distributing propaganda. These criminals are usually terrorists or enemy governments of other nations.

Types of Cybercrime

DDoS Attacks

These are used to make an online service unavailable and take the network down by overwhelming the site with traffic from a variety of sources. Large networks of infected devices known as Botnets are created by depositing malware on users' computers. The hacker then hacks into the system once the network is down.

Botnets

Botnets are networks from compromised computers that are controlled externally by remote hackers. The remote hackers then send spam or attack other computers through these botnets. Botnets can also be used to act as malware and perform malicious tasks.

Identity Theft

This cybercrime occurs when a criminal gains access to a user's personal information to steal funds, access confidential information, or participate in tax or health insurance fraud. They can also open a phone/internet account in your name, use your name to plan a criminal activity and claim government benefits in your name. They may do this by finding out user's passwords through hacking, retrieving personal information from social media, or sending phishing emails.

Cyberstalking

This kind of cybercrime involves online harassment where the user is subjected to a plethora of online messages and emails. Typically cyberstalkers use social media, websites and search engines to intimidate a user and instill fear. Usually, the cyberstalker knows their victim and makes the person feel afraid or concerned for their safety.

Social Engineering

Social engineering involves criminals making direct contact with you usually by phone or email. They want to gain your confidence and usually pose as a customer service agent so you'll give the necessary information needed. This is typically a password, the company you work for, or bank information. Cybercriminals will find out what they can about you on the internet and then attempt to add you as a friend on social accounts. Once they gain access to an account, they can sell your information or secure accounts in your name.

PUPs

PUPS or Potentially Unwanted Programs are less threatening than other cybercrimes, but are a type of malware. They uninstall necessary software in your system including search engines and pre-downloaded apps. They can include spyware or adware, so it's a good idea to install an antivirus software to avoid the malicious download.

Phishing

This type of attack involves hackers sending malicious email attachments or URLs to users to gain access to their accounts or computer. Cybercriminals are becoming more established and many of these emails are not flagged as spam. Users are tricked into emails claiming they need to change their password or update their billing information,

giving criminals access.

Prohibited/Illegal Content

This cybercrime involves criminals sharing and distributing inappropriate content that can be considered highly distressing and offensive. Offensive content can include, but is not limited to, sexual activity between adults, videos with intense violent and videos of criminal activity. Illegal content includes materials advocating terrorism-related acts and child exploitation material. This type of content exists both on the everyday internet and on the dark web, an anonymous network.

Online Scams

These are usually in the form of ads or spam emails that include promises of rewards or offers of unrealistic amounts of money. Online scams include enticing offers that are "too good to be true" and when clicked on can cause malware to interfere and compromise information.

Exploit Kits

Exploit kits need a vulnerability (bug in the code of a software) in order to gain control of a user's computer. They are readymade tools criminals can buy online and use against anyone with a computer. The exploit kits are upgraded regularly similar to normal software and are available on dark web hacking forums.

COVID-19 pandemic and many similars in cybercrime

covid 19, both a disease caused by cybercrime and corona virus, is incurable. Just as people resort to social distancing to avoid corona, similarly, distancing from strangers should be maintained on social media. On the other hand, we wash our hands for 20 seconds in Corona, in the same way any matter of cybercrime, or social media must think 20 seconds before doing anything. Many educated people have also been victims of this. There is a lack of awareness and awareness towards this crime. Up to Rs 65 lakh was cheated by an alleged American citizen from an officer couple in Bihar. At present, Jamtara in Jharkhand has become the capital of cybercrime.

Conclusions

Need to make cyber law more difficult

In order to make cyber crime more effective and to make the Act of 20 years ago in the country, it needs a lot of reform and improvement. At the same time, there is a need to increase the punishment and penalty fixed in different sections of this act. According to the manner in which cybercrime cases are increasing in Bihar, the speed of punishment is quite negligible. Penalty for different offenses up to section 65, 66, 66B, 66C, 66D, 66E, 66F, 67, 67A, 67B, 67C, 68, 69, 70 and section 71 of the Information Technology Act 2000 and imprisonment for three to five years There is a provision of In changing times, they seem relevant and weak. Also, there is a need to open a cyber station to investigate such cases separately in every district. Only then can there be effective control over this crime. In times to come, this crime will prove to be a headache for the system, governance and justice system. And it will bring mental and economic problems in the way that will increase the problem.

Suggestion-

Age limit should be fixed on social media

Just as the age limit has been set for voting, marriage, the age limit is also required on social media platforms. This case is still under consideration in the Supreme Court. It is being seen that people also create Facebook accounts for children between five and eight years of age, or the children are also given free exemption to use mobile-like devices by parents, which is wrong.

40 percent of the time is spent in download uploads

Presently, the youth of India are spending 40 per cent of their time on social media, downloads, uploads, which is a fact worth pondering and pondering. It is necessary to reduce it.

There are eight people in 10 lakh victims of cybercrime

Just as a fisherman throws nets to trap fish in a river, pond, sea, similarly some cyber criminals set up nets to trap people. In the trap thrown among 10 lakh people, only eight people get caught in the trap of cyber criminals, but cyber criminals also spend a lot of money in this.

To avoid cybercrime, five sources need to be implemented. Since childhood, cyber education should be made compulsory, people who use cyber should always keep safety and security in mind. In any case, you should not fall into greed, never believe any object in any cyber matter. Until now, capacity was judged by position and money, but in the cyber age, capabilities are being assessed through information. The one who has the most information and is as powerful and effective

You can be a victim of cybercrime in the free Wi-Fi affair

HTTP should be browsed on double slash only. If you are getting free Wi-Fi anywhere, then know that using it is not safe under any circumstances. Also, attention should be paid to end to end encryption.

Measures to avoid cybercrime

- Browse every secure website
- Never click a tempting message or email
- Never keep a simple password and do not save it on the computer
- Do not share your personal information with anyone
- Do not make people unknown to friends on social media platforms Facebook etc.

References

1. Mayur sachdeva Rajasthan Law House, Diglot Edition The Information Technology Act 2000
2. Cyber Crimes And Torts Book - Indira Gandhi National open University
3. Hindustan Newspaper Patna