ISSN NO.2395-0692
IJAHMS International Journal of Arts, Humanities and Management Studies

Law in the time of Covid-19- Cyber Law

Kavita Singh

Assistant Professor, Kotilya Law College, Jaipur.

INTRODUCTION-

The spread of the Novel Corona virus (COVID-19) pandemic across the world is creating fear exponentially, but the health risks are not the only bane that comes from this catastrophic event. It has been noticed that this period of social distancing and misinformation also gave an opportunity to the dark elements of the society.

"Working from home" has become the order of the day during lockdown. The way of accomplishing the tasks has drastically changed, with working from home as the viable option. One's dependence on the internet has increased manifold since the COVID-19 pandemic has caused restrictions on physical gesticulations. Online traffic has escalated due to jaked-up video conferencing/meetings, online classes and chatting. The use of apps like Paytm, Google Pay, BHIM, Phonepe, etc. as a mode of making payments has witnessed a surge.

During lockdown, along with the working habits, the modus operandi of the crimes has also changed. No doubt the crime rate has subsided as people are staying back but online frauds have seen an upsurge. Apart from being interaction/communication interfaces, sometimes these also serve as platforms for criminal elements and eventually end up being the epicentres of immeasurable security concerns. This working from home has now become an opportunity for cybercriminals to exploit the people through e-mail scams, hacking passwords, phishing, ransom attacks and online sexual harassment etc.

CYBERCRIME AND CORONAVIRUS-

There has been an influx of fake apps, domain names and websites capitalizing on two facts, first, the fear among the general public and their search for information related to this pandemic and secondly, the companies across the globe are turning to "work from home" via the online/virtual medium. We will deal with both the scenarios one by one.

Exploiting The Fear Among Public-

Everybody who has been trapped inside their house amidst lockdown is trying to stay on top of any information related to COVID-19 in an attempt to remain safe and away from infected people. The authors of malwares are taking advantage of this situation.

One such app which was available in Google Play Store was "Corona Live 1.1", which claimed to be a live tracker of cases of Coronavirus. The people using the app were of the view that they are keeping a track of the pandemic, but the malicious app was actually invading their privacy such as

getting access to the device's photos, videos, contacts, location and camera. The information collected can be used in multiple ways, they can be used to compromise bank accounts/transactions or even blackmail the owner of the pictures and videos.

The Android Play store removed many such apps and also have set rules for these types of apps and have put all such apps in the 'sensitive events' category.

Now the apps are available on fake websites, one such being 'coronavirusapp.site', where the link to download the app is listed. These instances adequately demonstrate the rise in cybercrime on account of coronavirus.

Exploiting the 'work from home' policies-

Every organisation, have been compelled to work remotely due to the lockdown. This will lead to increase in security risk as the proprietary data's being accessed from laptops and home PCs that may or may not have the same level of firewall and security as an in-office setup.

We may have noticed that an increase in the number of emails in our Junk Folder, pretending to an advisory relating to the COVID-19. These emails will entice the user to open the attachments, which are malicious/fraudulently in nature and the moment we open them the malware author will be able to access your system.

Once, the malware has attacked one of the systems, there is a potential risk of the security of the systems of your colleagues also being compromised. This can affect the whole grid of systems by which the organization is staying connected and there can be a huge loss of confidential data. Thereby, leading to a spurt of cybercrime cases due to the coronavirus outbreak in India and worldwide.

At such times, the organisations can rely on the ISO/IEC 27000 family. The ISO/IEC 27000 is a global benchmark certificate which is given to the organisations which follow the Information Security Management System (ISMS). In addition to providing improvements in structure and focus of the organisations, the ISMS helps you to safeguard you and your client's confidential data from cyber-attacks.

How to keep ourself safe-

We can keep yourself safe from such scams and frauds with a help of Vigilance and Diligence. Here are a few pointers which should be kept in mind while accessing the abovementioned data:

- Check the App details on Play store before downloading it, this includes, details of the developer, their website (if any), reviews and ratings given by other users.
- Avoid downloading apps from third-party stores and websites, and download the apps only available in App Store for Apple IOs users and Google Play store for Android users.
- Use reliable mobile and desktop antivirus, these can prevent fake and malicious apps from being installed.

Advisories are also issued by the Delhi Police and WHO due to rise of such frauds. Some of the DO's and DON'T's from the said advisories are as follows:

- Do not open email attachments that we have not asked for. In case we so receive an attachment, it is always safer to open the same from WHO's official website and not the attachment in the mail.
- Always pay attention to the type of personal information you are asked to share. There is always a reason why our personal information is needed. In no circumstances, there would be a need for our passwords.
- Do not believe any emails that come with a sense of panic. Legitimate organizations will never want us to panic and they always take the processes step by step.
- Do not believe that WHO or any other organization conducts lotteries or offer prizes, grants or certificates through emails.

Steps to check authenticity of website-

- HTTP = Bad, HTTPS = Good: The 'S' in https:// stands for 'secure'. It indicates that the website uses encryption to transfer data, protecting it from hackers.
- Check for easy markers such as spelling mistakes, typos and broken links. It is highly improbable for a legitimate business to have such mistakes on their website.
- Domain age: The imposters usually register a domain name just for a few months before changing the name of the domain and registering a new one. We can search engines such as Whois.com to look up the information such as the date of registration of the Domain name.
- Look for reliable contact information: Try to do background check. There is no harm in double checking with the company itself through alternate contact numbers.
- If we are a good Samaritan of the society and want to donate and help the needy then always donate only to the websites/apps whose authenticity is corroborated by the Government.

Prevalent Cyber- Crimes

Though cyber-crimes have been increasing continuously, there has been an upsurge during the lockdown due to people doing all the official as well as un-official work from their laptops or phones. Besides hackers directly attacking the systems, fake websites are being created to trap the users.

1. **Phishing:** -

Phishing is the cybercrime where the criminal accesses the information and details of the user through a link or e-mail that seems legitimate but is in fact, fraudulent. Phishing attacks have mushroomed to a large number during this lockdown. Spy-attacks and Ransom attacks are posing a threat to people submitting personal information online. Spyware steals the personal information and account details of the users, whereas a ransom attacker dominates and takes over the login credentials of the user. An app called 'Covid lock' is used as ransomware to target the anxious population, misrepresenting the same as an app to keep track of the spread of coronavirus.

ISSN NO.2395-0692
IJAHMS International Journal of Arts, Humanities and Management Studies

2. **Hacking At Companies and Offices: -**

According to a recent report by Price Waterhouse Coopers, the number of cyber-attacks on various firms has increased manifold times since the corona outbreak. Companies have set up a VPN structure, to let the employees have access to all the information, which has become the target of the hackers. Hackers are trying to hack the software/apps of the companies in order to gain access to all their important details and data. The use of an already-made malware 'AZORult' has increased for phishing into the companies. There have been cases of unwanted software trying to infiltrate to the companies' systems for theft and malicious payloads.

Hackers have even attempted to hack the computers of the Indian State Tax Department to steal sensitive information of PAN Cards, GST numbers, phone numbers, and e-mails. There have been several attempts made by the hackers at banks and Stock Markets leading to the brokerage. PM's COVID fund has also been one of the targets of the Hackers.

3. **Patients At Risk**: -

There have been cyber-attacks not only at local hospitals or test centres but also at the World Health Organization (WHO) to steal the passwords of WHO workers. Ransomware attacks have been detected in hospitals and other test centres where the important files/records of the patients are taken and not returned till a particular amount of ransom is paid. Hospitals have been alerted about ransom sites that claim themselves to be government advised sites to keep a check on the corona patients but then hacks the system.

4. **Other Online Crimes Related to social media: -**

Social networking apps like Facebook, WhatsApp have become an important tool to spread fake/false information. The Digital infrastructure across the globe is immensely comprised of these international tech-giants like YouTube, Google, Facebook, Twitter. Instagram etc. The social world has witnessed a complete transformation by these corporations, without any regulation or accountability of their Modus Operandi. These fake news' triggers the people, as they blindly believe these reports, and reacting accordingly. Besides this, these online chatting apps are misused to sexually and economically harass people. It has become inevitable for the employees to stay in touch with each other, so they opt for these communication platforms and sometimes end up being exploited in some way or the other.

Existing Cyber Laws in India-

Information Technology Act, 2000 is the only specific actions we have which is the basis of cyber laws and provides for different cybercrimes, their punishment, and sufficient Remedies.

The ransomware attacks are punishable[i] under The Information Technology Act, 2000. Under section 43 of this act, Hacking is a civil offense but if committed in a fraudulent way the person is punishable with imprisonment under section 66-B. The offense of phishing is punishable with imprisonment up to 3 years and a fine up to 1 lakh under Section 66 C of this Act. Section 72 and 66 of the IT Act provides punishment for the crime of cyber-stalking and online harassment.

Besides IT Act, 2000, the Indian Penal Code, 1860 also provides punishments and remedies for cyber-crimes: Section 419 of IPC provides for the frauds by impersonation. Section 354 of IPC provides for the crime of cyber-stalking and online harassment and its punishment with imprisonment up to 2-3 years. The Criminal Law Amendment Act, 2013 contains several additions

ISSN NO.2395-0692
IJAHMS International Journal of Arts, Humanities and Management Studies

to the Indian Penal Code, such as to sections 354, 354 A, 354 B, 354 C & 354 D, with the assistance of these sections now the issues of MMS scandals, pornography, morphing, defamation can be dealt in proper manner. The persons spreading fake news can be arrested under Section 505 of the IPC and Section 54 of Disaster Management Act, 2005 and can be punished with imprisonment up to 3 years and fine up to 1 lakh or both.

Cyber Laws of Other Nations-

The cyber laws[ii] much more developed than those in India. U.S.A has a number of acts in this regard: - the Electronic Communications Privacy Act, Computer Fraud and Abuse Act, Cyber Intelligence Sharing and Protection Act all to deal with the issues of cyber-crimes. Moreover, all the states of the United States are given the power to enact more laws and policies according to the need of the hour.

Canada also has strict laws against cyber-crime. Separate Health Sector Privacy laws deals with online crimes against hospitals, test-canters, laboratories, and clinics. Personal Information Protection Act and Electric Documents Act are further enacted to prohibit phishing and hacking. Canadian Anti-Fraud Centre is established which works against the marketing frauds.

Most of the European Countries have signed the Budapest Convention on Cyber Crime is an important step towards strengthening of cyber-laws against online frauds. The objective of the convention is to criminalize the offenses against privacy breach, confidentiality, breaking into the computer systems and set proper procedures to investigate against these Crimes. Other countries including England, Russia and Brazil have efficient acts and systems to act against cyber-crimes.

India is even not a signatory to the Budapest Convention on Cyber Crime and has not set any particular procedures to be followed to catch the cyber-criminals. National Cyber Security Policy 2013 was aimed to form the workforce of 500,000 skilled cybersecurity professionals but the objective is still not achieved. The number of ethical hackers in India is far more than the number of skilled IT professionals associated with the cyber police.

Lacunae In the Existing Indian Cyber Laws-

The problem of cyber laws in India starts with not having any set definition of cyber-crime in any act or law. Though there are some laws and remedies in the IT Act, 2000 but there are a lot of grey areas. These include intellectual property rights including copyrights, infringement and trademark. Moreover, there are no specific inclusions or the scams against the big companies and hence have to be treated only under the sections of hacking and online fraud. No separate policies are enacted for handling the cybercrimes against the health care sectors.

Territorial Jurisdiction is another major issue which is not specifically dealt by any cyber law. Since cybercrimes are computer and internet-based crimes, the hacker is far-sitting and maybe in another state and hence determination of jurisdiction is difficult. Preservation of evidence is another problem. As most of the evidence and proofs are online and in systems, destruction of the evidence is easy.

Besides this, the already existing laws are limited only to the theoretical punishments as it is not easy to prosecute the criminal due to anonymity. There are no concrete measures to take actions against these online criminals and no strategy to find these criminals sitting far away in comfort away from the actual location.

ISSN NO.2395-0692
IJAHMS International Journal of Arts, Humanities and Management Studies

CONCLUSION AND SUGGESTION

The government must ensure the safety of the state digital network & systems which store important public information and must take concrete steps in this regard. The lockdown has exposed the weak point of cyber-laws and after about a 5 percent increase in cyber-crimes, the government has shifted some focus to this side and the cyber-centers and cyber-police have become active. The government is issuing an advisory to the public to not to fall prey to these only crimes and take precautions while filling their details and passwords on online sites. But the government also needs to come up with some stronger laws, procedures, and strategies to catch the hackers. Besides, there is a need to introduce some security applications to prevent the companies' systems and hospital computers from hacking.

It is certain that the security standards have deteriorated as many organizations were not ready to work remotely and a rise has been witnesses in cybercrime due to coronavirus. With a little vigilance and due diligence, we can protect our data and privacy. It is always better to stay on the side of precaution but if, even after taking all the precautions, we fall into a trap then a quick action can salvage the loss. It is advisable to lodge a complaint with the appropriate authority.

These are some of the short-term solutions during the lockdown but there also needs some reform in the current Information Technology Act, 2000 as it is a comprehensive act and does not include much of the other aspects which are affected by the cyber-crimes.

ENDNOTES:

[i] Section 66-E and 66-F

[ii] America and other European countries