Journal of Multi-Disciplinary Legal Research

Level Of Cyber Crimes During Covid-19 Pandemic

Lavanya Pandiyan

ABSTRACT

Cybercrime can have a great impact on present generation during this pandemic era. The use of cyber world has increased in worldwide and everything goes in online. When cyber defences lowered due to the shift of focus on health crisis and over dependency on technology during 'Covid-19' pays way for enemies against world power. Cybercrime now become a million-dollar business. As there are freely available and downloadable tools on the internet even script kiddies can download and run against any vulnerable target without understanding what the tools does. There have been reports of scams impersonating public authorities such as the World Health Organization, supermarkets and airlines targeting support platforms and offering Covid-19 cures and many other ways victims are targeted. Especially they target the public, who are now socializing and spending more time online in general, as well as the increased number of people who are working from home. Thus, technological challenges impact the security, victims' time and finances, and also packs an emotional punch, anger, stress, vulnerability, powerlessness and violation.

Journal of Multi-Disciplinary Legal Research

INTRODUCTION

"Virus of cyber-crime has been changing with the corona-virus in the city"

Though Internet makes the life so speedy and fast, but hurled under the eclipse of threat from the deadliest type of criminality termed as 'cybercrime' without computers, entire businesses and government operations would almost cease to function. This proliferation of cheap, powerful, user-friendly computers has enabled more and more people to use them and, more importantly, rely on them as part of their normal way of life. Starting from children to aged persons are being victims to cyber crime in this lock down period as we are constrained to stay in home and do most of the things in online. Hence research in this topic become mandatory at present to be in safe for future environment.

BACKGROUND OF THE STUDY

Pandemic pays way for social networking sites are more of a demerit as compared to merit if both the parameters are evaluated; The youth is addicted towards fields of entertainment other than relevant information derived sources due to overutilization of social networking sites.[1] Cybercrime is a new category of crime especially during health crisis, requiring a comprehensive new legal framework to address a unique nature of emerging technologies and the unique set of challenges that traditional crime do not deal with such as jurisdiction, international cooperation, intent and the difficulty of identifying the perpetrator (Hackers & Crackers). Research suggests that the frequency of internet usage shares a positive association with cybercrimes and victimization. Limiting internet use is not a plausible solution to the problem of being a victim of cybercrime. Thus, there is a need for examining the roots of the problem.[2]

Journal of Multi-Disciplinary Legal Research

ISSUES

Suicide incidents, mental-illness, cyber-bullying, child exploitation, data theft or identity theft cases have increased widely. Cyber crime will bring new challenges for the Indian Government and policy makers due to - anonymity; Global reach (including issues of jurisdiction, disparate

[1] Patton, D. U., Hong, J. S., Ranney, M., Patel, S., Kelley, C., Eschmann, R., & Washington, T. (2014). Social media as a vector for youth violence: A review of the literature. Computers in Human Behavior, 35, 548-553.

[2] Marcum, C. D., Higgins, G. E., & Ricketts, M. L. (2020). Potential factors of online victimization of youth: An examination of adolescent online behaviors utilizing routine activity theory. Deviant Behavior, 31(5), 381-410.

criminal laws and the potential for large scale victimization); The speed at which crimes can be committed and unable to follow-up complaints in this pandemic situation; The volatility or transient nature of evidence, including no collateral or forensic evidence such as eyewitnesses, fingerprints, trace evidence or DNA; and the high cost of Investigations.

AIMS AND OBJECTIVES

To determine the negative usage of social networking sites during Covid-19 Pandemic and it's proximate and remoteness of damage vested within it; To analyze the credibility over the information received from social networking sites; To take control of online victimization; To study the influence of social networking sites on the personal and professional life of the people; To find motivation of the cybercriminals, a way of reducing cybercrime activities and it's effect; To focus on deterrent measures like recommending maximum and appropriate punishment for offenders, when prevention and control is not totally possible; To review the existing law and suggest amendments where necessary, develop a detail and acceptable measures of tracking the cyber criminals.

SURVEY OF WORK

According to Norton Life Lock's 2021 *Norton cyber safety insights* report, which gathered responses from over 10,000 people in Australia, France, Germany, India, Italy, Japan, Netherlands, New Zealand, the UK and the US to establish current consumer attitudes to cyber security. During this Pandemic the researcher found that 74% of respondents from the samples believed the new culture of universal remote working had made it far easier for cyber criminals to take advantage of them, while 59% were more worried than before about becoming a victim of cyber crime, and 62% were concerned their identity would be stolen. All over the world the two million people impacted by identity theft in the past 15 months alone, this means a lifetime of vigilance for suspicious activity on their accounts or against their name. WhatsApp, You tube, Facebook, Instagram, and online games impact the youngster into great risk as 40% of the people chatting with strangers and the extensive use of social media can actually cause addiction and negative effects.[3] At the present situation we are facing the challenges of environment complexity, new technologies, new threats and exploits, limited focus on security, limited budget for security, shortage of qualified security experts and security of our assets, network infrastructure, network resources, integrity, confidential personal data and protection

[3] O'Keeffe, G. S., & Clarke-Pearson, K. (2011). The impact of social media on children, adolescents, and families. Pediatrics, 127(4), 800-804.

against exploitation are in danger. Can the attacks be detected and solved, is a big tragedy in this lock down period due to lack of skilled personnel in cyber security, hard to detect the criminals, unable to contact and pursue the complaint progress as the authorities are busy in health crisis, lack of evidence, dragging of cases and no geographical boundaries in implementing cyber laws. In some cases, people don't even know if they have been a victim of cybercrime activities or not. Hence, we are in need of secure our cyber space and to ensure that offenders are punished accordingly.

MILLION-DOLLAR BUSINESS

Nation wide lock downs have led increased use of digital technologies and people around the world have adjusted the new way of life and work. Left with no option mostly people are prone to use internet and internet-based services to communicate, interact and continue with their job. Compared to pre-lockdown period internet services have risen from 40% to 100%. Likewise, video conferencing usage has increased into ten times greater than before. Cities like Chennai, Bangalore, etc., have seen a 100% increase in internet traffic. Police records show that cybercrime pattern has been changed in pandemic. While people are trying to adopt and overcome this pandemic situation, taking advantage of health crisis the cyber criminals are doing crimes as a full-time job for financial gain. **The increased number of crimes** are:

a. As per report of 'National Crime Record Bureau', online fraud, scams, intrusions and security breach for extracting money or data/information have increased up to 64%.
b. Privacy violation, phishing, online sexual harassment have increased up to 70%
c. **Brute force attacks** against remote desktop protocol (RDP) in March 2020 jumped from 93.1 million to 277.4 million in worldwide
d. **Data breach** at the payment firm Mobikwik and other services like Airtel, Bigbasket, Juspay, Unacademy which affected 3.5 million users exposing know your customer documents such as addresses, mobile number, Aadhar card, PAN card and so on.
e. Cyber frauds put online advertisements offering lucrative returns on investment and disappear after money has been credited to their account
f. **Fake profiles** of prominent persons are made by criminals on social media and ask money from friends of that prominent persons (Identity theft of 2 million people in 2020)
g. Frauds posing as cop or defence personel
h. Cheaters contact house owner for rental accommodation and ask for bank account number and OTP from owner to transfer rent amount and siphon money

Journal of Multi-Disciplinary Legal Research

i. Cheating by uploading **fake job vacancy**. Some gangs contact job aspirants who are fresher or who lost their job and offer them employment in good company. Here aspirant is asked to deposit Rs.1000/- towards registration fees
j. Some people began **offering Covid vaccines** to online users, they sought advance money and disappeared
k. Most important thing is financial frauds through digital transactions, where new users of net banking and internet users were targeted[4]
l. Many people started placing online shopping of groceries, liquor, masks, medicines, N-95 face masks in bulk, hand sanitizers and thermal scanners, etc., to avoid venturing out of their home.
m. Increased number of **fake apps, domain names and websites**. (E.g: google play store "corona live 1.1" which claimed to be a live tracker of cases of corona. But malicious app was actually invading their privacy, getting access to device's photos, videos, location, camera, used to compromise your bank accounts and then black mail the victims)
n. Exploiting the **work from home policies**. Every organization compelled to work remotely due to lockdown, which increased security risk as the proprietary data is being accessed from laptops and personal computers may or may not have same level of firewall and security as in office. The hackers send the mail regarding covid-19 cures with an attachment of malwares/virus. We simply open the mail without knowing the truth at the moment itself malware author access your system which might affect the whole organization.
o. By using spy attack or ransom attack hackers take over log in credentials and threat people to submit their personal data or money.
p. Hackers attempted to hack computers of Indian State Tax Department, Banks, Stock Market, Prime Minister COVID fund and Individual's sensitive information like pan card, GST no, Phone no, email, etc.,
q. **Patients at risk:** cyber attacks not only at local hospitals or test centers but also at World Health Organization to steal passwords of WHO workers by using ransom ware attacks, imported files of patients are taken and not returned till the amount of ransom is paid.

[4] Kunz, Michael and Wilson, Patrick (2004) Computer Crime and Computer Fraud, University of Maryland Department of Criminology and Criminal Justice [Online] available from [March 29, 2011].

r. **International tech-giants** like You tube, Google, Twitter, Facebook, WhatsApp, etc., have become important tool to spread information or for communication. Which are also being platform for exploitation, fake news, sexual harassment by way of online chatting.[5]

LAWS RELATED WITH CYBER CRIME

1. Information Technology Act, 2000
2. of Indian Penal Code, 1986
3. Section 54 of Disaster Management Act, 2005
4. National Cyber Security Policy 2013
5. International and Regional Conventions
6. Constitutions of India, 1950
7. Intellectual Property Rights
8. Computer Misuse Act, 1990

LACUNAE

- No proper definition for cyber crime
- Grey areas in IT Act includes copy right and trademark infringement under IPR
- No separate policies are enacted for handling cybercrimes against "health care sector"
- Territorial jurisdiction not specifically dealt by any cyber laws
- Determination of jurisdiction is difficult
- Preservation of evidence is a great problem
- As most evidence and proofs are online based or in system hence destruction of evidence is easy
- Existing laws are limited only to the theoretical punishments as it is not easy to prosecute the criminal due to anonymity[6]
- The lock down has exposed the weak cyber laws and increased in cyber crimes
- High cost of investigation
- Unable to follow up the cases in this pandemic

Journal of Multi-Disciplinary Legal Research

[5] Hale, C. (2002). Cybercrime: Facts & figures concerning this global dilemma. Crime and Justice International, 18(65), 5-6.

[6] Eric J. Sinrod and William P. Reilly (2000) cybercrimes: a practical approach to the application of federal computer crime laws; Santa Clara university school of law Journal vol16, number 2 [Online] available from < http://www.sinrodlaw. com/CyberCrime.pdf> [April 30, 2011].

RECOMMENDATIONS

Research is to provide effective information security awareness delivery methods and web-based training materials. Individuals should avoid disclosing any information like photos, credit card number, passwords and always use latest security programme and update anti-virus software to guard against virus attacks. Keep a watch on the sites that your children are accessing to prevent any kind of harassment or depravation in children. Webasite owners should watch traffic and check any irregularity on the site and block pornographic sites on the Internet and to initiate "trans-border cooperation".

CONCLUSION

The criminals are always draw their own priorities, pleasure and fix on to which ones are most important and how. Similarly during this crisis, we are all rely more than ever on computer systems, mobile devices and the internet to work, communicate, shop, share and receive information and otherwise mitigate the impact of social distancing. Through social networking sites criminals are getting quick information about what goes around in their near and dear ones' lives through the source of social networking sites offering them a ground to updates, which ease them to commit crime. Criminal justice authorities need to engage in full cooperation to detect, investigate, attribute and prosecute the above offences and bring to justice those exploited in midst of COVID-19 pandemic. If we aware of virtual crimes and take measures to safeguard ourselves, will make constant progress possible or even give us victory in the fight against cybercrime during this pandemic situation by developing security consciousness among public. Thereby internet will be a better and safer place for transactions and young users will be better informed of security tips for the safety of their personal matters and would not be victim for cyber crimes.[7]

[7] Oksanen, A., & Keipi, T. (2013). Young people as victims of crime on the internet: A population-based study in Finland. Vulnerable children and youth studies, 8(4), 298-309.