LEXKHOJ RESEARCH JOURNAL OF LAW & SOCIO-ECONOMIC ISSUES

ISSN: 2456-4524

VOLUME I ISSUE III

Website:www.lexkhoj.com

E-mail:lexkhoj@gmail.com

LEXKHOJ PUBLICATIONS

EDITORIAL NOTE

Lexkhoj Publication is committed to bring the highest quality research to the widest possible audience through an unparalleled commitment to quality and reliability. It is established with the objective of promoting academic research and fostering debate on contemporary legal issues all across the world. Lexkhoj Publications collectively bring together leading scholars in the field to cover a broad range of perspectives on all the key issues in national and international law.

Lexkhoj is delighted to announce the Third Issue of the Lexkhoj Research Journal of Law and Socio-Economic Issues which is an international journal, publishing critical approaches to socio-legal study and multi-disciplinary analysis of issues related to law and socio-economic. The journal will strive to combine academic excellence with professional relevance and a practical focus by publishing wide varieties of research papers, insightful reviews, essays and articles by students, established scholars and professionals as well as by both domestic and international authors. Authors should confirm that the manuscript has not been, and will not be, submitted elsewhere at the same time.

The Journal provides a forum for in-depth analysis of problems of legal, social, economic, cultural and environmental transformation taking place in the country and word-wide. It welcomes articles with rigorous reasoning, supported by proper documentation. The Journal would particularly encourage inter-disciplinary articles that are accessible to a wider group of Social activist, economist, Researcher, policy makers, Professionals and students.

This quarterly issue of the journal would like to encourage and welcome more and more writers to get their work published. The papers will be selected by our editorial board that would rely upon the vibrant skills and knowledge immersed in the paper.

Needless to say, any papers that you wish to submit, either individually or collaboratively, are much appreciated and will make a substantial contribution to the early development and success of the journal. Best wishes and thank you in advance for your contribution to the Lexkhoj Research Journal of Law and Socio-Economic Issues.

EDITORIAL BOARD

TRAINING ON CYBER LAW: A NEW CHALLENGE FOR THE POLICE

Palvi Mathavan[*]

Research Scholar, Department of Law, University of Jammu

ABSTRACT

Information and Communication Technologies (ICTs) are progressively being adopted in Police work with the aim of nurturing greater accountability and a contrivance to check cyber crime. The knowhow about cybercrime is also inadequate among a significant section of the officers. The training programmes on cyber crime and its detection is only made available to a selected few, while the rest remain in darkness. As the number of victims of cybercrimes is increasing day by day, the policemen (even at the root level) must be aware and conscious of the nuances of cybercrime so that they can capably guide the people and counter the menace. In this regard the present paper seeks to address the predicament of cyber crime in the State of J&K and provide certain suggestions to help the police officials in dealing with cyber crimes and to check the peril.

Keywords: ICTs, cybercrime, Policemen, ecrimes

INTRODUCTION

Cyber Crime has become one of the major problem to country's law enforcers. Virtually, the person using the computer for crime will be leaving no trace of his activities if he and the computer comes in perfect consonance, that means the man using the Computer knows in and outs about Hardware and Software. This brings to fore an urgent need to educate police officers, who are investigating frauds, embezzlements and cheating in the conventional way as new and new areas in banking, insurance and finances including Stock Exchanges are being computerised. With the computerisation of such financial institutions the rate of electronic frauds has increased, Electronic embezzlement and electronic cheating will give a new name of electronic criminal to the perpetrator. Two families in Delhi recently received a rude shock when people started calling and visiting them in response to advertisements about sexual services reportedly offered by a young wife and a female college student inserted

[*] Research Scholar, Department of Law, University of Jammu
Lecturer, KC Law College, Jammu

deliberately in the internet to harass them. This is just the one of the thousands of cases of Cyber pervert criminals.

There is another area of theft of information which is also done using computers. Theft of Information is of more potential value and damage than theft of money[1]. Theft of information will leave a irreparable damage therefore this threat has to be taken care of very seriously. One such case of theft of information by computer came to the light in USA at United Energy Agency. One of the employee of the Computer Centre before retiring had established contact of the computer with his house telephone. The work of that computer was to keep secret information and tell them on being asked through telephones. With Cyber Law now in position, that is going to be a major challenge to the law enforcement agencies to understand it and enforce it. Even with Cyber Laws a crackdown on such Cyber Criminals would be extremely difficult for want of proper training and sensitisation. More often they tend to get away with impunity.

Today's Police is expected to provide multi-dimensional service to the people in a proactive way. This entails that they are to be equipped in the best possible way to establish them as a people friendly police force. To provide the best of services it has been found that the police force has failed to come out of its cocoon and most of the officers remain unpragmatic and uneasy towards the recent developments. ICTs are providing multifaceted array of tasks not only to the masses but also to the police. In addition to this, the abuses of ICTs have also challenged the police to a newer form of crime – cyber crime. The paper is an attempt to delve into the infrastructure and technical skills that the Police of Jammu & Kashmir should offer to the people to combat cyber crime.

TYPES OF CYBER CRIMES

Cyber crimes can be of the following nine types:

(a) Cyber Pornography

(b) Cryptography

(c) Cyber Fraud

(d) Cyber Stalking/ E-mail threats

[1] Castells, M. 1999. 'The Information Age: Economy, Society and Culture'

(e) Cyber terrorism/ Hacking/ Information War

(f) Cyber theft

(g) Economic Espionage

(h) Obscene Materials

(i) Software Piracy and Electronic funds transfer fraud[2] .

Furthermore, they can also be classified as the following:

(1) Denial of service attacks:

It is an attack on a web server with false requests for pages. The server spends so much time trying to process these requests that it cannot respond to legitimate requests and may crash.

(2) Viruses, worms, trojans and other forms of malicious code:

Malicious code is a general term for programs that, when executed, would cause undesirable results on a system; Computer viruses are computer programs that can replicate themselves and harm the computer systems on a network without the knowledge of the system users. Viruses spread to other computers through network file system, through the network, Internet or by the means of removable devices like USB drives and CDs. Computer viruses are after all, forms of malicious codes written with an aim to harm a computer system and destroy information. Writing computer viruses is a criminal activity as virus infections can crash computer systems, thereby destroying great amounts of critical data.

(3) Unauthorized Entry:

The activity of breaking into a computer system to gain an unauthorized access is known as hacking. The act of defeating the security capabilities of a computer system in order to obtain an illegal access to the information stored on the computer system is called hacking. The unauthorized revelation of passwords with intent to gain an unauthorized access to the private communication of an organization of a user is one of the widely known computer crimes. Another highly dangerous computer crime is

[2] http:// www.crime.hku.hk/cybercrime.htm visited on 12.6.2017

the hacking of IP addresses in order to transact with a false identity, thus remaining anonymous while carrying out the criminal activities.

(4) Information Tampering:

Intruding into and damaging information stored in different storage devices of the computer.

(5) Cyber stalking:

The use of communication technology, mainly the Internet, to torture other individuals is known as cyber stalking. False accusations, transmission of threats and damage to data and equipment fall under the class of cyber stalking activities. Cyber stalkers often target the users by means of chat rooms, online forums and social networking websites to gather user information and harass the users on the basis of the information gathered. Obscene emails, abusive phone calls and other such serious effects of cyber stalking have made it a type of computer crime.

(6) Spamming

Sending unsolicited bulk email.

(7) Mouse-trapping

Clicking the browser's back button with the mouse does not lead out of the unwanted site but only to the viewing of further unwanted pages eg. pornography. To escape the user may need to close the browser or even restart the operating system.

(8) Phreaking :

Breaking into the telephone network illegally to tap phone lines;

(9) Computer Damage:

Injuring the hardware of the computer.

(10) Phishing:

The act of attempting to acquire sensitive information like usernames, passwords and credit card details by disguising as a trustworthy source. Phishing is carried out through emails or by luring the users to enter personal information through fake websites. Criminals often use websites that have a look and feel of some popular website, which makes the users feel safe to enter their details there.

(11) Identity Theft:

This is one of the most serious frauds as it involves stealing money and obtaining other benefits through the use of a false identity. It is the act of pretending to be someone else by using someone else's identity as one's own. Financial identity theft involves the use of a false identity to obtain goods and services and a commercial identity theft is the using of someone else's business name or credit card details for commercial purposes. Identity cloning is the use of another user's information to pose as a false user. Illegal migration, terrorism and blackmail are often made possible by means of identity theft.[3]

Cyber Crimes can be committed against persons, against property and against Government. Cyber Crimes committed against persons would include harassment of a person with the use of a computer such as e-mail. Cyber Stalking and Transmission of Pornography with the help of computer and internet a cyber criminal can cause maximum harm and harassment to society in general through the threat, trafficking distribution, posting and dissemination of Obscene Material including Child Pornography, Indecent Exposure and Pornography. A Cyber Criminal, if he chooses to, can continuously harass any person or a group of persons through Electronic Mail, access to website or through the popular chat programmes.

Cyber Crimes can also be committed against property such as Computer Vandalism using cyberspace to trespass computer, transmission of harmful programmes and unauthorised possession of computerised information. Basically, Cyber Crimes against property are of 5 types, such as Hacking, Cracking, Viruses, Software Piracy and Stealing of Intellectual Property Rights.

[3] B.Etter,"Critical Issues in High-Tech Crime", available at http://www.acpr.gov.au/pdf/ Presentations/apmedec02.pdf visited on 14.4.2010 and http://www.buzzle.com/articles/ types-of-computer-crimeshtml visited on 13.8.2012.)

CYBER CRIME AND LAW ENFORCEMENT

The development of new technology invites the establishment of new institutions to supervise policing, and value driven design may enable new legal procedures that are better equipped to hold policing accountable. The new policing aims to prevent and pre-empt crime rather than to prosecute it[4]. By predicting when, how, and by whom a crime will be committed, it aims to enable efficient intervention. Law enforcement has recognized in virtual space a toolkit of restraints on criminal behaviour. These restraints include law, technological features, network typology, and the social construction of particular uses of computers.m[5] .

India was one of the very first countries to enact a full fledged Act dealing with e-commerce, e-governance and cyber crimes, known as Information Technology Act, 2000. The Act was basically framed to facilitate e-commerce but, later on, some penal provisions were added to prevent misuse of trade on-line. Now, there are two strong schools of thought. One school is in favour of separate Act defining various types pf cyber crime procedures to collect digital evidence, its admissibility in Court of Law and other aspects covering the future changes in technology. The second school is of the opinion that some amendments should be made in the present IT Act, IPC and other Acts can suffice the needs of law enforcement agencies[6].

IT Act, 2000 was enacted in June and enforced on 27th October, 2000. Contrary to the popular belief, the Act has been quite effective and has emerged as an enabling piece of legislation. First and foremost it performed the much required function of declaring the e-documents equivalent to paper documents and digital signatures to a natural signatures made on a piece of paper. It also brought far-reaching changes in the legal system with the corresponding changes in the CrPC and Evidence Act. It introduced accountability by attributing e-records to the originator. It also provided a framework as a result of which the whole of the infrastructure of Controller of Certifying Authorities and Licensing of Certifying Authorities started functioning. The two main objectives of the Act i.e. e-commerce by enabling conclusion on contracts and creation of rights and obligations through electronic medium and e-governance by

[4] Policing India in the New Millennium.New Delhi:Allied; 989-1000.
[5] . Oxford Grabosky, P.N. 1998. 'Crime and Technology in The Global Village', Paper presented at the conference: Internet Crime held in Melbourne, 16-18February1998, by the Australian Institute of Criminology Kozlovski 2007: 108-114).
[6] India's Communication Revolution: From bullock Carts to Cyber Marts. New Delhi: Sage Publications

enabling use and acceptance of e-records and digital signatures have been well achieved. As far as the tackling of cyber crime is concerned, there are still several grey areas.

Law enforcement officials throughout the world are severely handicapped in tackling the new wave of Cyber Crimes. The biggest impediment they faced is total anonymity which the internet provides to an intelligent cracker. Getting internet account in fake name is easy. Moreover accounts can be used and discarded even before the authorities know that a criminal attack has taken place. This renders the problem more intractable for the law enforcements. Furthermore, there is an international connotation to computer crime. The hackers are not hampered by borders and geographical imputations. Traditional jurisdictions don't mean anything any more.

Today in its brawl against cyber crime the law enforcement agencies face a number of challenges: First, procedural resistance hinder law enforcements's ability to find and indict criminals operating online. Second, laws defining computer offences and the legal apparatus needed to probe criminals using the internet, cannot match up with the fast scientific and societal developments. Finally, there is a dearth of well trained, well equipped investigators and prosecutors to detect high tech crime. There are not enough law enforcement officers who are trained to combat computer crime. There is also the problem of acute storage of component investigating officers and almost no Prosecutors are capable enough in prosecuting Computer Crime. So, what are law enforcement officers to do? A former FBI computer specialist suggests that, "you either have to take a cop and make him a computer expert or take a computer specialist and make him a cop" and I fully agree with this view and we must start harnessing our available talents in this regard.

To counteract these emergent cyber threats, the role of the police in India should be redefined and the force should be professionalized to perform its tasks in cyber space through various organizational and structural changes in order to re-institutionalise the existing occupational culture, which is the main impediment of the force in combating cybercrimes (Thomas 2002:999). However the police alone cannot maintain their domain or jurisdiction over cyberspace nor can they fully exercise cybercrime patrolling. The success of fighting cybercrimes depends on the support that it gets

from the legal systems and the cooperation of community and the users of new technologies in cyberspace.

CYBERCRIME IN THE STATE OF J&K

Cybercrime is on the rise in the state of J&K. Internet has become one of the easiest way and source of exploitation, where anybody can do anything, sitting at the comfort of one's home. The Internet has pioneered not only new ways of reaching customers, but also new ways of exploiting them. Moreover with the advent of information technology and internet, cybercrimes with all the benefits of anonymity, reliability and convenience have become a global phenomenon. As per United States report on Internet and computing trends , Indians are the second largest sharers of personal information over the Internet after Saudi-Arabians. With increasing popularity of chat rooms and vulnerability of personnel data to criminal access, women in India have become soft targets to variety of cybercrimes such as pornography, sexual defamation, morphing, spoofing etc[7].

The researcher for the purpose of study has visited Cyber Cell, Jammu for collection of statistical data, where it was found that, 67% of the police reported cases of intimidation on the internet sre from women and young girls[8]. Around 70% of the cases are relating to cyber morphing and cyber pornography and the recent sensation of social media such as Facebook, Instagram has increased the cases of Defamation also, where various fake accounts are being made to defame a women and to send filthy, vulgar messages. According to the National Crime Records Bureau incidents of sexual exploitation of women has increased by 63.7% i 2016 as compared to 2015.

In September, 2016, the internet sex racket that rocked Jammu, came to the fore when Mukesh Nanda S/O Parshottam Lal Nanda R/O Rehari Colony, Jammu lodged a written complaint at Police Station Janipur. The complaint went to effect that during Google search Nanda found a few phone numbers on certain websites which offered sex services. Titles such as 'seeking sex with excellent model girls offered from Jammu' were common on these pages along with the numbers. The number clearly depicted that these services are provided by some locals of Jammu, who have

[7] Public Safety United States, 2005. National Strategy to combat women exploitation on the internet.
[8] Statistical data provided by the Cyber Cell Jammu for the past five years (2012-2016) relating to cybercrimes against women.

mentioned their phone numbers on such websites. They manage girls for illegal menace/Prostitution and provide to customers, locals as well as non-locals. On this complaint an instant case was registered and investigation into the matter was taken up. During the course of investigation, three people were arrested who were the brokers also. The trio disclosed the names of others brokers as well as sex workers, and names of various big shots of Jammu were disclosed.

The cases relating to credit card fraud has also increased significantly after the demonetisation. As our country is going towards digitization, cyber frauds and credit card scams are increasing. In an another case relating to cyber morphing in Jammu, where one girl namely Zainab R/O Old Town, Baramulla, lodged a written complaint in Police Station, Baramulla, stating that one of its friend , with whom she has shared her pictures has misused them, and circulated those on social media after they fell apart on some issue. She also alleges that some of those pictures were photoshopped and morphed to put her life in danger by putting them on porno portal websites. Based on her complaint case was registered and investigation was taken up. During the course of investigation it came to know that one Abrar Ahmad Mantoo S/O Raqeeb Ahmad Mantoo had morphed the photographs and uploaded on Facebook.

In the last 5 years statistical data of cybercrime in Jammu region, total 31 cases were registered, out of which 3 cases are not admitted, 3 un-traced, 5 challaned and 20 cases are still under investigation. Cyber Crime Cell, Jammu is not a full fledged Cyber Police Station till now. It just provide assistance. Investigation, filling of caes is done by the regular police only. Cyber Cell is a part of the expert cell. The Cyber Cell has 6 cyber experts. Most of the cases are relating to fake ids, character assassination, credit card frauds etc.

Jammu being multi religious and multi lingual city is very sensitive and vulnerable to cyber posts of communal nature and therefore such a related communal offences have the potential of causing serious law and order problems. It is also expected that the impact of cyber crime in contest of socio-legal dimension will be a challenge for the police to a large extent.

Therefore, there is a magnificient increase of cyber crime cases in J&K. Its very difficult to regulate and control such crimes as these crimes only effect the individual virtually and no physical harm is done to an individual, and not much expertise staff is

available to deal and crack such crimes. These crimes are still taken very leniently and most of the time these cases are dealt under as regular crimes. To fight these crimes we need to have some expertise staff and lot of awareness among the people.

SUGGESTIONS & RECOMMENDATIONS

1. A Cyber Crime Cell/Police Station should be developed to handle cases dealing with computer offences.

2. A Cyber Forensic Laboratory with all updated technologies should be endorsed to detect computer crimes.

3. A team of specially trained officers expert in detecting cybercrimes should be reared in the model of 'Cybercops' of Andhra Pradesh Police. A special group of officers must be skilled in collection, storage, and, retrieval of digital evidence. Laboratory and skill development to maintain digital evidence is a need of the time.

4. The Police Commissionerate should take initiatives to have information about the recent new police technologies that are being used by police in Bangalore, Mumbai, Delhi, Chennai and Kolkata with special emphasis to cyber crimes. They should also take note of police organizations in developed countries. This will help them to keep pace with new challenges of policing and establish itself as a high tech police force.

5. The local police stations (20 police districts each for Bhubaneswar and Cuttack) should keep a vigil on the cyber cafes of their respective localities. It should be ensured that no one will be allowed to use the cyber café without valid proof of identity. The time limit for surfing in the cyber cafes should also be restricted. Recently the State Government of Odisha has made cyber café registration mandatory. The order ensures that apart from asking for valid identity proof, the cyber cafes will maintain a record of the visitors and also prohibit surfing of websites containing pornography, obscenity, terrorism and other objectionable materials.('Cyber café Registration Mandatory', The Sunday Express, 19th August, 2012, p.4)

6. The website of the Police Commissionerate of Bhubaneswar and Cuttack should provide information to the city dwellers about the precautionary measures that should be taken to check cyber crimes. Awareness among the public about rising e crimes should be

made by the city police through the website, advertisements and sensitization programmes in educational institutions.

7. The Contact Number of police personnel dealing in Cyber Crime should also be mentioned in the official website.

8. The new generation policemen should be trained in the application of ICTs in police work to help them to carry forward the legacy of the police organization successfully. Policemen who are new entrants must be imparted training in ICTs at the inception of training programme to enable them to understand its importance in police work. In addition to this will reduce the inhibitions in using computerized technologies. They will also be sensitized about the abuses of computer technologies.

9. All complaints of cyber crimes should be given importance. Special directions should be given to local police stations so that they can properly guide the people if they come with complaints of cyber crimes.

10. The Crime Statistics of the cities of Bhubaneswar and Cuttack does not show any data on cyber offences. This should be included as a separate category in the list and should not be merged with other traditional forms of crime. (See http:// bhubaneswarcuttackpolice.gov.in/ crimestatistics.php visited on 5.8.2012.)

11. Awareness programmes should be carried out to sensitize police officers about the Information Technology Act, 2000/2008.

12. Since the number of educational institutions is increasing in Bhubaneswar and Cuttack with a regular flow of students from all over India, the Police Commissionerate should be extra vigilant and sensible towards the youth. Since the offenders and victims of cyber crime are mostly the young generation the police should take a constructive and reformatory approach while dealing with them.

13. Sensitization programmes on cyber crimes should be organized by the Police Commissionerate in educational institutions to spread awareness about computer abuse among students. Students should also be updated about the provisions of the Information Technology Act, 2000/ 2008.

14. Community Policing Programmes should also be initiated to check cyber offences. The people's participation can be of great help in combating cyber crime.

15. The Police Commissionerate needs to provide access to technologies especially wireless handsets, computers, internet, and mobile telephones to all ranks of policemen to make them adept in handling ICTs....

CONCLUSION

The Police authorities of Jammu & Kashmir has to match steps with other capital cities like Hyderabad, Bangalore, Mumbai, Delhi and Kolkata in so far as protection against cyber crime is concerned. The police of the twin cities has to initiate noteworthy measures to combat computer crimes. A Proper full fledged Cyber Police Station must be set up in the state. The Cyber Police Station should have a separate wing of 'Cyber Crime Investigation & Training Cell '. The abuses of ICTs is on the rise and with so many educational and industrial developments going on, it is the need of the hour to develop a more proactive safety measure to check the peril. Since the victims as well as the offenders of cyber crime are mainly the younger generation it is important that they should be adequately sensitised about the legal directions against cyber crime. With the recent regulations on cyber cafes the police officer not below the rank of an inspector has to be assigned the responsibility to check or inspect cyber cafes and computer resource or network established at any time to comply with the Technology (Guidelines for Cyber Cafes) Rules, 2011 as issued by the Ministry of Information Technology. In this regard the Police Commissionerate can play a notable role. More so, the police officers including those working at the grass root especially in the local police stations if adequately informed can be active in combating cybercrime. Proper Hardware and Software required for the training of the Police personnel must be purchased. Also, proper education should be imparted to others who are associated with the Criminal Justice System, i.e. the prosecution process, such as the Public Prosecutors, as well as the members of the judiciary and Police officers,etc. Regarding Cyber Law and Cyber Crime Investigation. The insinuations to the Police Commissionerate have come with the hope, that if implemented can make the police of the twin cities more high tech and agile in combating cyber crime.