CAPACITY BUILDING SEMINAR TO HANDLE CYBER CRIMES (P-967)

29TH- 31ST JANUARY, 2016

PROGRAMME REPORT

PREPARED BY- PRAGYA AISHWARYA, LAW ASSOCIATE, NJA

INTRODUCTION

In the present era, Information and Communication technology (ICT) have creeped into almost every aspect of human life. The increasing reliance and dependency on ICT has made societies vulnerable to threats of cybercrime, that is, crime committed against or through computer data and systems. Cyber world being very dynamic, emergence of new facets of cyber crime and internet related offences is common occurrence. Spurt in internet usage has directly affected the rate at which cyber offences have grown. Offences unheard a few years ago have become frequent reality of the present era. Currently, the cyber crimes in India is nearly around 1,49,254 and is likely to cross 3,00,000 mark by 2015, growing at compounded annual growth rate of about 107 per cent, a recent study has revealed. Given the increasing rise in cyber crimes and internet related offences, there is need for the judges dealing with such offences to be well versed with essential technical and legal aspects to play an essential role in providing justice to victims of such crime.

With this underlying object, the NJA organized **'Capacity Building Seminar to handle Cyber Crimes'** from 29th-31st January 2016, for the High Court judges. This seminar, aimed to acquaint on essential skills necessary to cope with computer and internet-related offenses. Simultaneously new developments, new conventions and new protocols developed in the field governing cybercrimes were part of the conference.

DAY 1

The 1st day of the seminar comprised of 3 technical sessions followed by hands on session.

The 1st session started with basics of cybercrime. The theme of the session was **"About cybercrime Why worry about cybercrime? What is cybercrime? Challenges for judge"**. The main focus of this session was to bring before the participants the very basics of cyber crimes, distinguish it with normal crimes and to make the participants aware about the challenges which they might face while dealing with a case concerning such crimes.

The speakers for this session were Ms. Nappinai and Mr. Deepak Maheshwari. Ms. Nappinai started the session with the discussion on enactment of the Information Technology Act and the subsequent amendments which have taken place. She said that when the IT Act was enacted it did not come into place to deal with cybercrime, it was primarily concerned with regulation of e-commerce but today the focus of the Act is all on cybercrime. Moving further she discussed how cybercrime is different from other crimes, because of its borderless domain. Talking about definition of cybercrime, she brought to notice that most nations have shied away from defining the term cyber crime. They have resorted to keep it open ended and leave it to either the provisions to dictate whether it is a crime or cybercrime or for enforcement authorities to decide where it would lie. Talking about Cyber Crime in India, she said that when we look at cybercrime from the Indian perspective we start off with the first step of presumption that we do not have a definition for cybercrime. The second step is then how do we deal with this concept of cybercrime because it's an undefined term, we have to look beyond the IT Act, we have to look most importantly beyond the traditional concepts of crime, the basic differences or the basic intent or purpose behind crime which used to be a need has now become want. Elaborating on this she explained few cases where the offenders were young and desperate for recognition, which prompted them to try their hands on cyber crimes. Many times it is seen that the offender do not know the serious nature of the crime they are committing. Ms. Nappinai mentioned names of some very prominent figures like Bharkha Dutta, Sagarika Ghosh, Chinmay who have been victims of cyber stalking and cyber bullying. All the cases on 66A are not dead with the death of section 66A. Moving back to the definition of cyber crime, she discussed a definition given by Kerala government circular to the police which very succinctly captures what a cybercrime is, it just says that, it is a crime committed against computer, where the computer is the victim or by using a computer where the computer is the weapon. Further she discussed broad structure of IT Act and some of the major provisions. In the course of deliberations, Shreya Singhal's case was also discussed. Moving towards hacking, Ms. Nappinai discussed the case of Sony, where its entire database was hacked, another instance of hacking in 2011 where 12000 email id of government officials, who were dealing with DRTO was discussed. Then she discussed different modes through which a computer is hacked. These days it is done mostly by sending false mail in the name of user's bank or play store etc, which prompts the user to click on some link through which Trojan is download in the system. If there is Trojan in a computer, the moment when the user enters his password, through those keystrokes it can capture it and send it back to the person who has hacked into his account. There has been instances where most kids keep their computers in the bedroom so

what happens is this Trojan activates the camera randomly, captures all the private details and they are uploaded for no reason except that they can do it. The next type of cyber crime discussed by the speaker was denial of service attack. She explained a case from Cambridge where the attacker did the crime just to gain attention and because of his desperation for recognition.

The second session themed **"National law and international standards"** proceeded as a continuation of the first one. The main aim of this session was to make the participants aware about the increasing ambit of internet, its increasing user base, existing domestic legislation on cyber crime, and the international conventions in place. Ms. Nappinai started the session by deliberating on the issues and challenges that would come up while dealing with cybercrime. She said that one of the primary issue that comes up with hacking is jurisdictional issues because every incident may happen from our neighbour or from any part of the world. Mr. Maheshwari added that it often happens with remote tools, without knowledge of the person that his system has been hacked. Mr. Maheshwari further explained how a computer can be accessed and controlled by another computer system which is situated at a very distant place from it. He explained that it happens because of nature of internet, every computer is connected to other computer just like our phone network. Ms Nappinai explained that hackers get access to any computer from a long distance through the internet, when both computers are matching connected to net at the same time, they can from the IP address get into target computer. She cautioned that for that to happen the hackers need an open door from where they can get into our system. For every single action that happens, whether it is virus or hacking etc., everything is done through a software programme, it is a code written to break into others computer. The speaker then threw some light on Dark Net on being questioned about it by one of the participants. Mr. Maheshwari talked about changing land scape of cyber crime. He brought before the participants, some of the latest data's which showed the glaring pace at which internet users are increasing worldwide and in India. He stated four characteristic of internet, for which he used 4 Ss, Speed, Scale, Skills, and Spread. He stated that the problem lies in the fact that internet and technology is global while the legislations are territorial. In India cyber criminals are moving faster, investigators and other agencies are not able to catch the pace. He further discussed what are the tools for dealing with cyber crimes in the present era. He talked about the Budapest Convention, which is the first global treaty to deal with cyber crime. He said that though India has not ratified the convention, it has aligned its legislation in line with the convention after the 2008 amendment. The speaker further said that more effective

international cooperation is needed for dealing with cyber crime. The main cause for rise in such crimes is that the law enforcement is not very well equipped, both in terms of technology and knowledge. Number two, lot of these hackers are operating from safe heavens, from countries where they are enjoying protection. So to keep a check on rising cyber crimes, three most essential points are that there should be capacity building and awareness among the users, there is a need for synchronizing domestic and international systems and third aspect is to bring about regulatory consistency in India.

The third session was themed **as "Technology Functioning of the internet (basic notions): Glossary of terms Protocols".** This session focused on the very basics of internet, how it works and basic internet protocol. Important terms and few technical concepts associated with the functioning were explained to the participants through theoretical as well as practical demonstration. This session was taken by a team of experts from PwC (Pricewaterhouse Coopers). The main speaker for this session was Mr. Murali. He first of all explained how the internet evolved from 1968 onwards. He then talked about how cables are laid around the world which provides internet connectivity around the globe. Then the discussion moved towards explaining some of the very basic concepts about computer system like BIOS, RAM, Mother Board, LAN, Wifi and other related concepts. The PwC team supplemented the explanations with practical demonstration wherever it was possible. Later a video was played which explained how a packet data travels and brings information on click of a button. The speaker answered some very basic queries of the participants regarding the functioning of internet and working of computers. Concepts like Internet of Things, Free basics were also taken up during the course of discussion.

The fourth session was themed as **"Offences against computer data and systems, Computer related fraud and forgery, Content-related offences, Intellectual property-related offences"** The speaker for this session was Justice Yatindra Singh. He divided the session into two parts, first half consisting- Offences against computer data and systems, Computer related fraud and forgery and Content-related offences, and the second half consisting of IP related Offences. He started off with following questions What is cyber laws, what are the violations of cyber laws, what is cybercrime, its remedies and punishments?. He then discussed about computer technology, cyber space and moved towards Information technology Act. He stated that the legislatures are enacting laws, government are making rules and regulations, courts are fine tuning the guidelines or framing the laws where there is no such law, all these solutions

put together, are known as information technology laws or computer laws or cyber laws. He also talked about amendments done to IT Act and subsequent enactment to other legislations: Indian Penal Code, Indian Evidence Act, RBI Act and Banker Book's Evidence Act. He said that violations of cyber laws can be divided into two parts, one in the field of IPR and second in fields other than IPR. Cyber Crime can be of two types: one when the computer is targeted or other when the computer is used as an object. He stated broad sections under the IT Act that deals with computer as object or target. He then talked about remedies for cyber crimes: civil and criminal remedies. He talked about sections 43, 43 A of the IT Act, damages and penalties under the Act. Talking about appeal he said that appeal lies to appellate tribunal, cyber appellate tribunal and the second appeal lies to the High Court. He explained differences between section 43 and 66A of the IT Act and said that the difference lies just in the mens rea, mens rea of dishonestly or fraudulently. He then talked about some more provisions like cyber terrorism under section 66F, section 70-securing or attempting to secure access of protected system, sections which were covering affecting human body and person, section 66 A and 66E, child pornography, cyber stalking and provisions. Moving on to second part the speaker talked about IP offences. He said that there are number of different kinds of IPRS. WTO conceives it as 7. There are much more than these 7. So far as IT is concerned five of them are relevant:

1. Trade Mark
2. Trade Secret
3. Copyright
4. Patent
5. Lay Out Design, Integrated Circuits

He talked about ten kinds IP- Internet related offences

1. Domain name dispute
2. Cyber squatting and typo squatting
3. Protest Violations
4. Copyright Violations on Internet
5. Linking
6. Image linking
7. Framing
8. Meta tagging and Key Word
9. Selling of Trade Mark

10. Peer to Peer file Sharing

At the end of 1st day sessions, an hour was allotted for practical demonstration session by the PwC team. The team explained how investigators should proceeded with an electronic device so as to prevent loss or tampering of data. They carried out an imaging activity before the participants showing how imaging from a mobile device is done during the course of investigation.

DAY 2

The second day was chaired by Justice Muralidhar. Speakers for this session were Mr. Pravin Anand and Mr. Vakul Sharma. It was themed as "**About electronic evidence: definitions and characteristics.**" Mr. Anand started the session explaining how the evolution in technology has taken place. He started by saying that it is important to understand when electrical became electronic. He said that the term cyber was used only when the internet came, so cyber essentially meant internet related, today the meaning of cybercrime has broadened. Because of overlapping technology, and various devices' multiple activities involving entering contracts, transferring money, buying selling, listening to music, seeing films, reading books, all this is now covered under cybercrime. He then explained the difference between internet service provider and telecom provider. He talked about computer softwares, use of internet and mobile technology, different ways of file sharing like P to P and P to C. Touching upon IP related offences he said that, in classic IP law, there is a distinction between the person who makes and the person who distributes, but on internet this distinction gets blurred, you click a button, and automatically a copy is produced and it is disseminated. He explained the difference between transmissions as it takes place in IP related cyber crimes, He said that that is why now there is a new right which is called making available right, when you are not just making your content available, rather distributing your content or transmitting it. Further he talked about principle of ephemeral reproduction, it meant that unlike books, when you read them you do not photocopy a part of the book in your mind, in the computer, you necessarily copy when you are running the programme, just by running it you are copying it in the RAM Chips of the computer, so you are making a copy into the computer and that is reproduction. But that is reproduction only till the time you are running the programme that is why it is called ephemeral reproduction. Mr. Vakul Sharma then started his part of discussions. He started by explaining that what is electronic evidence and when we are looking into an electronic evidence what kind of evidence we are looking into. He said that when one is looking at electronic evidence which is presented before the court of law, first thing is collection, followed by analysis then

its presentation before court of law. The text messages sent and received, the WhatsApp or any kind of chat platform in form of text, , video, images, , emails, digital photographs, ATM transaction records, call records in form of CDRs all this form part of electronic evidence. On being questioned by one of the participants, the speaker talked about allocation of IP address through use of Wifi and dongles. He talked about static and dynamic IP address. The participants then discussed with the speakers some of the practical issues which they face while dealing with cases on cyber crime before them.

The speakers for next session, session 6, were MS. Nappinai and Mr. Pravin Anand. The session was themed as **"Procedural law/ investigative measures: Jurisdiction and territorial competencies, Expedited preservation of computer data, Production orders/ warrants."** Mr. Anand started the session by talking about efficient facilities available in Delhi High Court for recording electronic evidences. He further said that for things to work smoothly it is important that judges should be well versed with technology. He then talked about software piracy, Anton Pillar order, John Dow order, Section 76 of the IT Act. He further moved the discussions towards jurisdictional issues and the challenges faced therein. He then touched upon two decisions by the Delhi High Court in Banyan Tree and the WWE case. Himalayas Drug Companies case was discussed in some detail by the speaker. He then talked about concept of phishing and Delhi High Court's NASSCOM case. Ms Nappinai started her part of discussion by dwelling upon how a case proceeds. She said that there are three aspects of how a case proceeds: first is where we have a problem we approach a court, the procedural aspect which court has to follow, second is an order which is issued to protect the rights of the litigant but the third part is implementing Court's orders. Ms. Nappinai then talked about electronic signature and its various aspects. She then discussed, some of the challenges that electronic medium has brought before us and moved towards discussing criminal jurisdiction pertaining to the cybercrimes. She then closed the discussions by talking about 65 B, Dharmbeer case and Anwar vs Basheer.

Session 7 was themed as **"Requirements of electronic evidence**". The speaker for this session was Mr. Vakul Sharma. The participants requested him to cover two important issues in this session which were: 1) How do you prove a CCTV footage? 2) How do you prove a tapped mobile conversation? Mr. Sharma started off with the first question. He explained that in most of the cases the CCTV footage is in a very granular manner it is a grainy picture, and once you are looking into a grainy picture, the persons face may not come out as a clear picture of an

accused person. So the first thing that has to be seen is the record retention policy of the place where such CCTV has been installed. The next point he said which should be looked into is whether CCTV is linked to direct electricity line or not, whether there is a backup, electricity back up in that particular building or not. Next thing which has to be seen is whether that CCTV is having, some sort of time or date stamping or not. Whether the time date stamping that comes on the screen is there or not, it is another crucial aspect to be looked into. On the question of how to prove CCTV footage Mr. Sharma said that the first thing that has to be complied with is the requirements of section 65 B. He said that in most of the cases CCTV footages are being stored in a hard disk, whether that hard disk is apart of computer system or a computer resource, that thing has to be seen, only then section 65 B certificate will come into play. Then the discussions moved towards when 65 B certificate will be required and when it is not required. The speaker then discussed some of the land mark cases- Trimax International, Shakti Bhog foods limited vs kola shipping ltd, Gajraj case, Shamsher Singh vs state of Haryana, with the participants.

The next session was themed as **"Computer Forensics".** The session was taken by PwC team. Mr. Sachin started the discussion with definition of digital forensics and its 4 different principles. Having explained that he moved towards the process of digital forensics. He explain it in the following steps: First is to identify source of data, a particular source of data. Then experts carry out some kind of preservation mechanism, one mirror image is preserved as it is to present in the court of law and second one which is working copy, the analysis is done on the working copy. Then the experts follow their report mechanism, they do certain set of analysis based on the case and then prepare report which can be given before the court of law, produced as an evidence. If required they testify before the court as expert witness. One of the speakers then talked about different memories in a computer system: cache memory, RAM memory. The speakers then explained how different memories can be retrieved using forensic tools by experts. If a file is deleted from the recycle bin, how can it be re structured by forensic experts was explained through practical examples given by the speakers based on their experiences? How criminals are tracked and traced through IP address, sent mails, telephone conversations etc was discussed. Chain of custody form was shown to the participants and the speakers told the participants that proper chain of custody form is not maintained most of the time, details are just written on piece of paper that is why lot of confusion takes place. Various challenges while dealing with electronic evidences were discussed. Next they discussed types of analysis which can be done on any digital media.

At the end of 2nd day's session, an hour was allotted for practical demonstration session by the PwC members.

DAY 3

The sessions for the third day were chaired by Justice Muralidhar. Speaker for the 9th session were Mr. Ashok Dohre and Mr. Rabindranath Patil. The session was themed as "**Search and seizure of computer data: The interception of traffic and content data."** Mr. Dohre initiated the sessions. He demonstrated some practical softwares used by Government of India for interception of data. In the course of demonstration he discussed some concepts related to transfer of data in computer like packet shifting, transmission, IP sniffing. He further discussed legal issues related to electronic evidence like the provisions of Evidence Act involved, requirement of electronic certificate, how to ensure integrity of electronic data etc. Mr. Patil discussed few real life cases which he has dealt with relating to search and seizure of electronic data. Two main cases which were taken up by him during the course of discussions were: the investigation of 26/11 Mumbai terror attacks by Indian agencies and the second case was of intelligence operation which lead to arrest as well as conviction of David Coleman Headley.

The last session of the conference, i.e. session 10 was themed as **"Safeguards".** The speaker for this session was Mr. Pavan Duggal. He started the session by saying that there is no magical formula for safeguards. During the course of discussions he shared some important cases and incidents that have happened which are very serious in terms of way forward as safeguards, they were The Pathankot attack case was the first case that was taken up in the course of discussion. Subsequently he gave various examples of incidents of cyber defamation, cyber pornography, hacking, IP offences and mentioned the challenges which the court faces in each of such type of offences. Issued discussed in Avnish Bajaj, Anvar vs Basheer, certificate under 65 B etc were taken up during the course of discussions.