NATIONAL JUDICIAL ACADEMY

REFRESHER COURSE FOR CBI COURTS

PROGRAMME REPORT [P-1125]

(12th-14th October, 2018)

PROGRAMME COORDINATOR:

MR. KRISHNA SISODIA, LAW ASSOCIATE

NATIONAL JUDICIAL ACADEMY, BHOPAL

RAPPORTEUR:

MS. ASHITA GAUR

1ST YEAR, LL.M, CAREER COLLEGE OF LAW, BHOPAL

OBJECTIVE OF THE COURSE –

The course was structured to facilitate deliberations on investigation procedures adopted by the CBI, prosecution of civil servants, economic offences and sentencing practices. The sessions also enabled discussions on contemporary themes such as appreciation of electronic evidence, forensic evidence and the *Modus Operandi* of Cyber Crimes. The objective of the course is to provide a forum for participants to discuss, deliberate amongst themselves and share experiences, knowledge and best practices in exercise of jurisdiction evolving new horizons of relevant law and jurisprudence.

The following were the sessions:

- CBI: Why is this a Preferred Investigation ?
- Prosecution of Civil Servants : Sanction for Prosecution
- Prosecution of Civil Servants : Arrest and Investigation
- Economic Offences : Banking and Corporate Frauds
- Cyber Frauds in Banks : *Modus Operandi* of Crime
- Electronic Evidence : Collection, Appreciation and Preservation
- Forensic Evidence in CBI Cases
- Sentencing Practices in Corruption Cases.

DAY – 1

SESSION 1

CBI: WHY IS THIS A PREFERRED INVESTIGATION ?

SPEAKERS

MR. M. MALAKONDIAAH

MR. UMA MAHESHWARA RAO

CHAIR

JUSTICE A.M. THIPSAY

The conference commenced with a warm welcome of the participants and the eminent panelists by the Hon'ble Director, NJA. In his introductory remarks Justice Raghuram gave a brief about the CBI Courts and emphasized as to how imperative it was for the High Court Justices to elucidate on the subject.

The first speaker elaborated upon the background of CBI Courts by mentioning about the origin of CBI in which he said that the CBI- Central Bureau of Investigation traces its origin to Special Police Establishments (SPE) which was set up in 1942 by the Government of India. The Delhi Police Establishment Act (DSPE Act) was then brought into force in 1946. The Delhi Police Establishment later was popularly known as the Central Bureau of Investigation (CBI), through a Home Ministry Resolution dated 01.04.1963.

It was further emphasized that the CBI is an anti-corruption agency having jurisdiction over the Public Servants of Central Government and Central Public Sector Undertakings. The CBI has set up separate wings namely Special Crimes Wing, Economic Offences Wing, Banks Securities & Frauds Cell to investigate into conventional offences. It was also mentioned that as per Delhi Special Police Establishment Act, 1946, the jurisdiction of CBI stretches over the Union Territory however as per Section 5 of the DSPE Act, the Central Government may extend the jurisdiction of CBI to any State. Thus, CBI is a Specialized Investigating Agency that can exercise powers and jurisdiction in the Union Territories and the States.

A question was raised by a participant as to **why is CBI preferred for investigation ?**

This was very beautifully answered by the learned speaker who mentioned that CBI is preferred for investigation as CBI has a set of Standard Operating Procedures (SoPs) in every aspect of investigation and they are open to radical changes that take place in criminal law and judicial system. The best part is that the investigators conduct a free and fair investigation also the investigation is reviewed by the supervisory officers at least once a month. Besides this, all the cases have a multi-layered supervision which means that the cases are scrutinized at multiple levels, which enables the quality investigation as well as free and fair investigation. Whereas, in Police organizations, major work is to maintain law and order, hence time for investigation is compromised. A very beneficial point to note in the working of CBI is that all the instructions

are in writing and well documented hence, informal and oral instructions do not have any place in its functioning. The officers of CBI are posted on deputation for a tenure of 5 to 7 years therefore they are normally away from their parent cadre due to which the influence of politicians on their decision making is almost zero. CBI being an agency of the Central Government having jurisdiction throughout India has a better coordination with other organizations like Interpol, Enforcement Directorate, Income Tax, SFIO, SEBI etc. for conducting investigation. During investigation, CBI lays great emphasis on usage of science and technology, it is well equipped with Technical and Forensic Support Units (TAFSU) with latest technological advancements. The most important thing which enables CBI to conduct its investigations so well is that it has the luxury of investigating less number of cases, it investigates 1400 cases per annum on an average therefore the quality increases due to the reduction of quantity. CBI has an exclusive Pairvi Section, which handles services of summons an execution of warrants unlike the State Police. There is no corruption in CBI as there is very strong internal vigilance under which the officers are monitored continuously to ascertain any corrupt deeds/ misdeeds. CBI is isolated from external influence and also the powers of investigation are not misused by the officers and the notable part is that it has certain specializations in human trafficking, wildlife conservation, money laundering cases etc, hence it is preferred for investigation.

After answering the query of the participant, the **reasons for acquittal in CBI** were discussed briefly. The grounds of acquittal in CBI are hostility of crucial witnesses, non-availability of documents in old cases, settlement of dues by the borrowers to the financial institutes, disproportionate assets and the mistakes committed by the Sanctioning authorities while according sanction for prosecution.

The speaker also highlighted that the cases are transferred for investigation to the CBI, they are transferred so late that almost all of the evidences are lost as a case does not come directly for investigation to the CBI hence the purpose off investigation is lost due to the delay in transferring of cases as was seen in **Arushi Talwar's Murder Case**. There is also a lack of training and coordination between the prosecution and the investigating forces.

SESSION 2 & SESSION 3

PROSECUTION OF CIVIL SERVANTS: SANCTION FOR PROSECUTION
PROSECUTION OF CIVIL SERVANTS: ARREST & INVESTIGATION

PANEL
JUSTICE A.M. THIPSAY
MR. UMA MAHESWARA RAO

The second session began with reference to section 4 (4) of the Prevention of Corruption (Amendment) Act, 2018 in which it is mentioned that a trial of the offence shall be held on a day-to-day basis as far as possible on which it was discussed by the learned speakers that does this provision apply to the cases which come in the Courts for trial after

26.07.2018 or it also applies to the cases prior to the amendment. The answer to the extent was since it is a procedural provision, it will apply prospectively.

Further discussions lead in context to Section 197 of the Code of Criminal Procedure, 1973 which tells about the prosecution of Judges and public servants stating that no Court shall take cognizance of any offence punishable under Section committed by a Judge or public servant without previous sanction. Section 19 of the Prevention of Corruption Act,1988 was discussed which emphasizes that no court shall take cognizance of any offence punishable under Section 7,10,11,13 and 15 alleged to have been committed by a public servant, except without previous sanction. Thereafter, recent amendments to the Prevention of Corruption (Amendment) Act, 2018 were discussed at length main focus being on Section 17 A of the Act which deals with enquiry or inquiry or investigation of offences relatable to recommendations made or decision taken by public servant in discharge of official functions or duties. It was highly debated by the participant judges that the provision is treading the dangerous path of immunity vs impunity.

DAY - 2

SESSION 4

ECONOMIC OFFENCES: BANKING AND CORPORATE FRAUDS

SPEAKER

MR. RAJIV AWASTHI

CHAIR

JUSTICE SANJEEV SACHDEVA

The session began by the speaker giving a brief of the background and origin of the Prevention of Money Laundering Act, 2002 –

In 1992 – Brussels Convention FATF (Financial Action Task Force) gave recommendation for a money laundering act to be created.

In 1998 – India Standing Committee approved the legislation.

In 2002 _ The Prevention of Money Laundering Act, 2002 was formulated.

On 01.07.2005 – The Prevention of Money Laundering Act, 2002 came into force.

In 2007 – First case was registered under the act. It was very slow but started taking its flow within the passing of time. The first provisional attachment was made by attaching 287 properties.

The session continued further by emphasizing on the **Prevention of Money Laundering Act, 2002** in which **Section 3, 4, 5 and 8** of the Act were briefly discussed. It was also mentioned that money laundering is a scheduled offence which involves concealment of origin of illegally obtained money typically by means of transfers involving foreign banks or legitimate businesses.

Further a thin line of difference was drawn between **Section 5 (1)** and **section 8 (1)** of the Prevention of Money Laundering Act, 2002. Section 5 (1) makes an officer duty bound to investigate and record the reasons to believe that such person has committed the offence in writing. Whereas, Section 8 (1) does not make an officer duty bound to record the reason to believe in writing.

The purpose of the Prevention of Money Laundering Act, 2002 was thrown light upon stating that it was created with the objective to make everyone who commits a crime, liable to attachment. It was further told that **Section 4** of the act prescribes punishment which makes any person found guilty of the offence of money laundering liable to a punishment for rigorous imprisonment for a term of three years which may extend to seven years and in some cases to 10 years.

There was an important amendment in Section 8 of the act which previously enabled the power to provide only after the completion of trial but after amendment, the power to provide relief is available during the trial also. The five major amendments to the act were made in the years 2005, 2007, 2009, 2013 and 2018.

A question was raised by a participant asking whether a privy authority is also a police officer and what is the procedure for producing a person before a Magistrate?

It was aptly answered by the speaker saying that Section 19 of the Prevention of Money Laundering Act, 2002 gives the power to arrest and the arrest in this act is different from the arrest by a police officer which is governed by Section 65 of the Act. Later, Section 43, 44, 45 of the act were briefly discussed. There was a recent amendment in the provisions of attachment which stated that charge sheet is not a must for the purpose of attachment, which was a pre-requisite condition for attachment before the amendment. Further various discussions in light of Section 17 (1) of the act took place in which every participant put forward his views and also cleared their queries with the speaker.

The speaker gave an important point by telling everyone that if any transaction exceed Rs. 100 Crore or Rs. 200 Crore then it is definitely a case of money-laundering. A famous scam, the IPO Scam of Ahmedabad was given brief of by the speaker in which SEBI (Securities and Exchange Board of India) had found many irregularities in 21 IPOs from2003 - 2005 due to which unlawful gains of about Rs. 41.34 Crore were reallocated by 1.27 million investors.

After this, the next speaker took the lead of the session by discussing about corporate fraud and how it impacts businesses. He said that a corporate fraud is sophisticated, complex and difficult to investigate. Mainly the stock market, commodity market, banking sectors are prone to these frauds. Frauds are usually done by ‘shell companies’. Shell companies are the companies that are legitimate legal entities that do not possess actual assets or run business operations, they particularly functions as vehicles for variety of firms. These companies later introduce ‘seed’

money as capital in one shell which is then passed on to other shells in a single day in a single branch. Each of these company gets identical sums as capital which is then lent or invested in another company. This exercise is repeated several times to create an illusion of real transactions and multiplying money. Often many such shells have common registered address with 'dummy' directors who may be real persons but are untraceable and unrelated to the business.

Further the Modus Operandi of such companies was thrown light upon in which the speaker mentioned that the modus operandi of such companies is to suddenly raise shares in one year in a 'synchronized manner' and when they are spotted, they simply vanish. These type of companies deal with 'account takeover'. An 'account takeover' can happen when a fraudster or computer criminal poses as a genuine customer, gains control of an account and then makes unauthorized transactions. This includes banks, credit cards, email and other service providers. Online banking accounts are usually taken over as a result of phishing, spyware or malware scams. Then there are also 'Government Agency Frauds' in which the fraudsters send official letters similar looking to original letters to scam people and get their information.

SESSION 5

CYBER FRAUDS IN BANKS: MODUS OPERANDI OF CRIME

SPEAKER

DR. HAROLD D'COSTA

CHAIR

JUSTICE SANJEEV SACHDEVA

The next speaker continued the session by going into a new world that is created by the humans known as the **'Cyber World'**. He laid great emphasis on the characteristics of this world by stressing upon the fact that cyber world is a world with no boundaries, it's a world of limitless potential. There are no laws, no legal orders, no countries, no names, no addresses, no states, no rules, no public order governing life or property. In this world people have no identities, they create their own identities which gives them the power to misuse and create fake accounts enabling them to do frauds. This world was not created by the Government but by corporate bodies for business purposes. The internet was introduced was the first time in the United States of America but after the Indians got familiar with this new technology of internet, they even left the inventors behind. India is the biggest consumer for the developers of internet. A notable point was put forward stating that on 31.07.1995 the Chief Minister of West Bengal made India's first cellular phone call hence inaugurating Modi Telstar's Mobile Net Service in Calcutta.

The speaker gave information to everyone present in the conference regarding 'identity theft' in which he told that identity theft means when knowingly or unknowingly we post huge amount of personal data on social networking sites, this information is subject to a risk to our safety and privacy which means the data we post can be used by unauthorized people against us. Further the speaker asked does anyone know who owns the content we post and who controls it? He then told that every data that we post is owned and controlled by the social media platform, if we carefully read the 'terms and conditions' of the social networking site, there is a clause in every app or network according to which whatever a person uploads on a social network, is their

property hence they can commercially exploit us and we can not say anything against it as we ourselves agreed to their terms and conditions therefore one should be very careful in what he posts on the social media platform. Sometimes, this may also lead to disclosure of confidential information due to which trade secrets may be disclosed by an employee or other party.

The next speaker took over the session and told everyone that there are around 50 Crore internet users as on 30.06.2018. The service of internet came in our country in 1994. The main question is that who owns the internet and who runs it? The answer to this is that nobody owns the internet, it is an intangible concept rather than a tangible entity. The internet is run by **Internet Corporation for Assigned Name and Number (ICAAN).** It is a globally distributed computer network comprising of various voluntary interconnected autonomous works. It has over 108 Crore domains out of which 8 – 8.5 Crore are Indian domains. Before 21.09.2018, ICAAN was under the governance of United States of America but now it is an independent body. It has a total of **13 root servers** distributed as follows –

- 10 root servers – United States of America
- 1 root sever – Netherland (Amsterdam)
- 1 root server – Sweden (Stockholm)
- 1 root serer – Japan (Tokyo).

A point to keep in mind is India does not have a root server of its own which means the data of India is controlled by the root server of some other country.

After giving a brief about the internet, the speaker made everyone aware of **'phishing scams'** which means an attempt to obtain sensitive information such as usernames, passwords and credit card details, often for malicious reasons by disguising as a trustworthy entity in an electronic communication.

The speaker in his session highlighted about the **COSMOS Bank Fraud** in which the 'switch software' which is used to identify whether a card being inserted is genuine or spoof or fake was made a proxy due to which fake cards were signaled as genuine by the ATM, due to this **13,329 cards** were generated between **28 countries** worldwide and around **78 Crore** was ciphered from **11.08.2017 – 11.08.2018**. This was possible only because the bank did not comply with the provisions of the Information Technology Act, 2000 and hence the onus was on the bank.

A device named **'skimming device'** was given information about in which the perpetrators steal the card owner's authentication data by the use of a device called **'skimmer'**. The stolen data is then used to make counterfeit cards that are used to draw money from the victim's account. Most of the cards are compromised at petrol pumps. If there is a chip in the card, it is difficult to duplicate it but if the software is compromised, then even a chip cannot protect the card from duplication.

SESSION 6

ELECTRONIC EVIDENCE: COLLECTION, PRESERVATION AND APPRECIATION

PANEL

JUSTICE SANJEEV SACHDEVA

DR. S. MURUGAN

The next speaker led the session by giving a description about electronic evidence. An electronic evidence is any probe in information started or transmitted in electronic devices. It is of binary form. Anything and everything a person does on the internet leaves a trace on the computer which can be used as an evidence. A participant asked that **where can an evidence be found ?**

The speaker replied to this by saying that an evidence can be found in internal devices, external devices or on digital platform. It was also told by the speaker that in the digital world we are blind as everything is in the form of binary i.e., '01010101' format which is not readable by any person except the computer.

A brief was given about digital footprint also known as digital evidence. When anyone uses a device, he leaves a footprint, everything that a person posts on the internet is watched. Every time we log on, we leave a mark this mark is known as 'digital footprint'. **Digital footprint** or evidence is difficult to delete and is very easy to modify and duplicate. No data can ever be deleted even if it delete it from the concerned folder, it is still present somewhere in the metadata of the computer and can be easily accessed by a person who has even a little knowledge about computers. A metadata is a data which gives data about other data. Metadata in case of a –

- Digital photo is the camera used for taking the photo and description of the lens used.
- File is the author and the number of characters in the file.

The conference continued on its path which was led by another speaker who gave a definition of cyber crime as a crime in which an electronic communication device is the object of the crime, or used as a tool or target to commit an offence. Cyber criminals may use information technology to access personal information, business trade secrets or use the internet for malicious or exploitive purposes. A computer may be used both as a target and a tool, a computer is used as a target for unauthorized use of data, identity theft etc. whereas a computer as a tool is used for phishing, lottery fraud, credit card frauds and also using e-mail for threat or harassment.

The speaker further quoted **Edmond Locard's Theory** which states that "anyone, or anything entering a crime scene takes something of the crime scene with them. They also leave something of themselves behind when they depart" similarly when a person enters a social network he always leaves something behind which may be later used by fraudsters for malicious activities. Edmond Locard was the Father of Forensic Science.

Later a distinction was given between conventional crimes and cyber crimes. The speaker said that the traditional criminal techniques have now turned into cyber crimes with the growth in technology and development. The crime of burglary has changed into hacking, deceptive callers

have turned to phishing, extortion has now become internet extortion, fraud has converted into internet fraud however, identity theft and child exploitation still remain the same.

The speaker gave a brief about evidence and characteristics of electronic evidence. The term evidence should always be treated as evidence regardless of whether the evidence is physical evidence, trace evidence, biological matter or electronic evidence, all evidence must be treated in a similar manner. An electronic evidence on the other hand is any information and data of value to an investigation that is stored on, received on or transmitted by an electronic device. The main characteristic of an electronic evidence is that it is invisible and can be altered, modified and destroyed easily. Later the emphasis was laid on as to **where is an electronic evidence stored ?** An electronic evidence can be stored in any storage device like Computers, CDs, DVDs, Floppy Disks, Hard Drives, Thumb Drives, Electronic Cameras, Memory Sticks, Memory or SIM Cards, Fax Machines, Answering Machines, CCTV etc.

The session continued further with reference to **Section 2 (1) (v), Section 3** and **Section 4** of the **Information Technology Act, 2000**. **Section 22 A, 62 and 64, 63** and **65** of the **Indian Evidence Act, 1872** were also referred to which deal with oral evidence and documentary evidence. There are mainly two types of evidence – primary evidence and secondary evidence where primary evidence means the document itself and secondary evidence means copies made from the original by a mechanical process.

The speaker opined that every forensic investigator shall always have an **Electronic Forensic Kit** with him which should contain the following:

- An electronic camera
- Sterilized removable media
- Forensic Computer
- Hardware write-blocking devices
- Forensically sound boot disks
- Mobile device acquisition tools
- Tool kit (screw drivers, etc.)
- Evidence packaging materials.

A brief about the process of **'Chain of Custody'** was given which means a process that tracks the movement of evidence through its collection, safeguarding, and analysis by documenting each person who handled the evidence, the date or time when it was collected or transferred and also the purpose for which it was so transferred.

The speaker elaborated on the topic of **Deleting a file** which means when a file is deleted it is simply deleted or zeroed { i.e. alterations are made to the FAT (File Allocation Table) or MFT (Master File Table) } so that at the logical level the file does not appear to the user, but at the physical level the file data is still intact on the media and may be recovered anytime. **Wiping a file** means the entity of the file is overwritten by a known random hex character or pattern

rendering it unrecoverable. A term called 'hash values' was defined. **Hash Values** can be treated as fingerprints for files, they are a way to represent a piece of electronic data with a unique numerical value by applying a mathematical algorithm to the data. There are various social media issues which were also thrown light upon namely harassment, humiliations, cyber bullying; use, misuse and abuse of **Article 19** of the Constitution of India i.e. **'Freedom of Speech'** ; issues related to **Section 506, 153 A and B, 354 A,B,C and D** of the **Indian Penal Code, 1860.** The speaker highlighted a very important aspect of Google stating that 'Google knows you better than you know yourself; Google does not forget; Google does not delete and Google has 254 products and services', the list of which was also circulated to the participants.

DAY – 3

SESSION 7

FORENSIC EVIDENCE IN CBI CASES

SPEAKER

DR. SUDHIR GUPTA

CO-CHAIR

JUSTICE S. TALAPATRA

JUSTICE ATUL SREEDHARAN

The session began with discussion of the meaning of **forensic science**, it was elaborated that forensic science is the application of sciences to matters of law, it can help investigators understand how blood spatter occurs (physics), learn the composition and source of evidence such as drugs (chemistry) or determine the identity of an unknown suspect (biology). The origin of Forensic Science can be traced back to the 6th Century. The session continued further with an elaboration on the role that forensic evidence plays in criminal investigations. Forensic evidence helps in criminal investigations by proving that a crime has been committed or establishing key elements of the crime, places the suspect in contact with the victim or crime scene, establishes the identity of persons connected with the crime, corroborates a victim's testimony and mainly assists in establishing the facts of what actually occurred. The **two recent scientific and technological advances** were brought in light – (i) **DNA typing** which facilitated body fluids to be individualized and (ii) **Computerized database of DNA**, fingerprints and firearms which can be stored and retrieved when required. Sometimes, the DNA profile may not match the suspect thereby exonerating the suspect from the crime. A latent print can match a suspect but further investigation may reveal that the suspect can explain why his prints were at the scene and give proof that he was not at the scene when the crime occurred. Hence, forensic evidence is not mathematics which can be clearly stated 2+2 = 4 but it is a means to arrive at the nearest possible outcome.

It was further told that sudden unnatural death of a person raises suspicion regarding the manner of death, not only among the family members but also in the society. When such reasonable suspicion occurs, only forensic science can properly investigate and give answers to the questions of the family members of the deceased.

Various cases were elaborated by the speaker which were related to the investigation done by the forensic department of the CBI. The five major cases that were discussed were –

1. **The case of Pramila Gandhi, Bengaluru** dated 27.03.2009 in which the manner of death had to be determined.

2. **The case of Sara Singh, Ferozabad** dated 09.07.2016 in which the cause of death of the victim was to be determined.

3. **The case of Tannu Jaiswal, Shimla** dated 20.06.2009 which dealt with determination of the manner of death of the victim.

4. **The case of Puja Mishra, Greater Noida, U.P.** dated 01.08.2015 which was a case related to the investigation of manner of death.

5. **The case of Geetanjali Garg, Gurgaon** dated 17.07.2013 which revolved around investigation of the manner of death of the victim.

The session was concluded by the speaker by giving some **important points relating to forensic investigation –**

- The first and foremost point to keep in mind is that the opinion of a forensic expert should be in 'gold standard' i.e. an opinion which can be read and easily understood even by a person who is from a non-scientific branch.

- Secondly, forensic experts should be updated about the latest scientific and technological developments in their field.

- Thirdly, no forensic expert shall ever form an opinion in a haste.

- Fourthly, it is very important for a forensic expert to record the postmortem findings in an objective manner.

- Fifthly, every forensic expert shall while investigating and making a report of any case keep both the circumstantial and direct evidences in mind to form proper and accurate report.

- At last, an expert medical opinion shall always be based on facts and findings as available at the time of making medical opinion.

SESSION 8

SENTENCING PRACTICES IN CORRUPTION CASES

PANEL

JUSTICE S. TALAPATRA

JUSTICE ATUL SREEDHARAN

The last session of the conference was based on the sentencing practices in corruption cases wherein the speaker mentioned that in corruption cases, there is always a pre meditation of having an intention as corruption is not something which occurs at the spur of the moment rather it is a pre-planned process. Section **13 (1d), Section 16 , Section 18 and Section 20** of the **Prevention of Corruption (Amendment) Act, 2018** and also **Section 235 (2) and 248** of the **Code of Criminal Procedure, 1973** were laid stress upon and a discussion with reference to the same took place between the participants and the speaker. The conference before concluding had an interactive session of the participants and the speakers in which they discussed various topics relating to the subjects of the conference and also cleared certain queries.

The three day long course was concluded with a warm thanks and expression of gratitude to the learned speakers and all the participants by the Additional Director, National Judicial Academy. He also thanked the speakers for taking time out of their busy schedule and coming over to Bhopal for sharing their vast knowledge of the subjects with everyone. The speakers also thanked the Additional Director, NJA saying that it was an opportunity for them to share their knowledge and they were highly obliged.