Report on

WEBINAR ON "CYBER LAWS AND ELECTRONIC EVIDENCE"

Held on: 5th-6th February, 2021

Organized by: Rajasthan State Judicial Academy, Jodhpur

Resource Person(s):

- Mr. Mukesh Choudhary (Cyber Law Expert, Jaipur)
- Mr. Nisheeth Dixit (Cyber Law Expert, Jaipur)

Report prepared by: Shubham Shandilya (Research Scholar)

- One of the greatest and most revolutionary inventions of mankind has been the proliferation of computers and digitalization. As with other spheres of human life, the cyber space has not been free from dangers and commission of crimes. The diversity of content and information available on the cyber space along with the ease of accessibility and wide reach, has also led to a tremendous increase in its misuse.
- When we talk of the word 'cyber', it automatically takes us to the thought of internet, technology and virtual world. In a nut shell they include anything and everything which has its roots in technology or is somewhere related to the generic term 'computer' and its offshoots. All these things are collectively and generically called 'cyber space'.
- The criminals are using these high end technologies to commit such crimes which are beyond the reach and understanding of a layman. A person unskilled in this art cannot fancy tracing the roots of the crime. In recent years it has given us a new term called cyber-crime. It is a crime in which a computer (cyber, in general) is used either as a tool or a target.
- In a crime involving the use of technology, the evidences so furnished will also be in some electronic form. At times it becomes difficult to test the veracity of such evidences, in absence of an expert. Here comes the role of cyber forensics. Forensics generally means the use of science and technology to establish facts in courts of law. When prefixed by the word cyber, it obviously connotes the relation with cyber space. Etymologically we term them as 'electronic evidence'.
- Objective of Rajasthan State Judicial Academy is to educate and sensitize its officers and other stake holders about the latest laws and procedure to achieve the constitutional mandate of securing the "Rule of Law".
- Making full use of the advances in the field of technology and keeping up with its constitutional mandate in mind, The Rajasthan State Judicial Academy on **5th-6th February, 2021** organized a **Webinar on "Cyber Laws and Electronic Evidence"** at **3.00 pm** (both days), which was presided over by Mr. Mukesh Choudhary (Cyber Law Expert, Jaipur) and Mr. Nisheeth Dixit (Cyber Law Expert, Jaipur).
- The webinar was conducted under the aegis and guidance of **Hon'ble Mr. Justice Sandeep Mehta (Judge, Rajasthan High Court and Chairman, Rajasthan State Judicial Academy),** under whose able leadership the series of webinars for providing in-service training to the Judicial Officers of the State of Rajasthan was envisaged and implemented.
- The webinar saw a participation of 268 Judicial Officers (Additional District and Sessions Judge and Senior Civil Judge cum Chief Judicial Magistrate) across the various Judgeships of the State of Rajasthan.
- **Ms. Poonam Durgan** (Additional Director [Academic], Rajasthan State Judicial Academy) welcomed **Hon'ble Mr. Justice Sandeep Mehta** (Judge, Rajasthan High Court and Chairman, Rajasthan State Judicial Academy); Mr. Mukesh Choudhary (Cyber Law Expert, Jaipur) and Mr. Nisheeth Dixit (Cyber Law Expert, Jaipur) on the webinar.
- The webinar subsequently began with the deliberations by the Resource Persons.

5th February 2021

- **Emerging Technologies**
- **Recent Frauds and new modes of operations in Cyber Crimes with case studies and counter measures**
- **Investigation of Social Media Crimes, Credit/Debit Card and E-Wallet frauds.**
- **Handling of Electronic Evidence.**

By

Mr. Mukesh Choudhary (Cyber Law Expert, Jaipur)

- The Resource Person started the deliberations by discussing the major problems encountered in the investigation of Cyber Crimes in the Country. Some of these include:
    a) Poor know-how of handling cybercrime investigation
    b) Handling of Digital Evidence
    c) Poor know-how of IT infrastructure and advancement in crime rate and technology.
- The recent trends in Cyber Crimes were also discussed with the participants in detail, with the help of illustrations and case studies. Some of the trends that were discussed included:
    a) Cases of Fake Profiles and Impersonation
    b) Impersonation over voice communication carried out using the Internet Protocol (Voice over Internet Protocol)
    c) Call Spoofing
- The Resource Person also provided the list of counter measures to be taken by the participants, so as to not become a victim of the above mentioned incidents. The discussion then moved on to the concept of Networking Fundamentals, wherein the Resource Person explained the various types of networks to the participants.
- Networking is defined as a method of connecting devices such that they can communicate or interchange data. The various types of computer networks include:
    a) Local Area Network (LAN)
    b) Metropolitan Area Network (MAN)
    c) Wide Area Network (WAN)
- The abovementioned network types were explained to the participants in detail. The Resource Person also discussed the concepts related to "Port". A port is defined as application-specific or process-specific communication endpoint in a computer's host operating system. Ports are divided into two parts:
    a) Physical Ports
    b) Virtual or Internal Ports
- The classification of the Internal Ports based on their respective range was also explained to the participants along with well-known examples such as FTP (File Transfer Protocol), DNS (Domain Name Service), HTTP (Hyper Text Transfer Protocol) etc.
- The Resource Person then discussed the fundamentals of an IP Address with the participants. An Internet Protocol address is a logical and unique identity address of a system. The format of the IP Address depends on its version. There are basically two types of IP addresses:

a) Static IP Address
b) Dynamic IP Address

- The basic concepts related to a proxy server, Virtual Private Network (VPN) were also discussed with the participants. The session concluded after discussing case studies related to whatsapp/facebook based incidents and the difficulties and challenges of investigation that arise in such cases wherein social media has been used as a weapon to commit a crime. The security measures that can be taken to prevent such cyber-crimes were also explained to the participants.

6th February 2021

- **Objective and scope of IT Act**
- **Applicability and non-applicability of IT Act**
- **Cyber Contraventions and adjudication process**
- **Cyber Offences with case studies**
- **Admissibility of Electronic Evidence**

By

Mr. Nisheeth Dixit (Cyber Law Expert, Jaipur)

- The Resource Person started the deliberations by discussing the meaning of Cyber Criminology. Cyber criminology is defined as ***"the study of causation of crimes that occur in the cyberspace and its impact in the physical space."***
- The term "Cyberspace" literally means 'navigable space' and the word "Cyber" is derived from the Greek word "kyber" which means, to navigate.
- "Cyber-crime" is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It broadly includes:
  a) Crimes where a computer is the **target of the crime**,
  b) Crimes where a computer is a **tool of the crime**, and
  c) Crimes where a computer is **incidental to the commission of the crime.**
- The broad categories of cyber-crimes that were discussed with the participants includes:
  a) Data Crimes
  b) Network Crimes
  c) Access Crimes
  d) Content related crimes
- It was brought to the attention of all the participants that cybercrime is estimated to cost the world US$6 Trillion annually by 2021 based on projections by various think tanks.
- The categories of cyber criminals and the motives of cyber-crimes were also explained to the participants. The various issues encountered in investigation of cyber-crimes were also discussed with the participants, some of these include:
  a) Difficulty in Detection of Crimes
  b) Masking of Identity–Anonymity

c) Lack of awareness of Technology(Cyber Security, Forensics SOPs)
d) Issues pertaining to jurisdiction–Territorial limits, different levels of legal protection in different countries, extra-territorial Jurisdiction, MLAT etc.

- The discussion then moved on to the Information Technology Act, 2000 and the Resource Person explained the different sections of the IT Act pertaining to specific cyber-crimes/cyber offences, along with the relevant case laws concerning the same.
- The Hon'ble Supreme Court in **Sharat Babu Digumarti v. Govt. of NCT of Delhi AIR 2017 SC 150**, held that: "*If legislative intendment is discernible that a latter enactment shall prevail, the same is to be interpreted in accord with the said intention. Once the special provisions having the overriding effect do cover a criminal act and the offender gets out of the net of the Indian Penal Code and in this case, Section 292.* ***The electronic forms of transmission are covered by the IT Act, which is a special law.*** *It is settled position in law that a special law shall prevail over the general and prior laws.*"
- In **Syed Asifuddin and Ors. v. The State of Andhra Pradesh and Ors. 2005 CriLJ 4314**, the Hon'ble High Court of Andhra Pradesh held that a cell phone fulfilled the definition of a computer under the IT Act and the tampering of the unique numbers i.e. computer source codes/ ESN(Electronic Serial Number) attracted Section 65 of the IT Act.
- The Hon'ble High Court of Kerala in **Vijesh v. The State of Kerala and Ors. 2018 (4) KLJ 815**, held that: *"In a case in which a mobile phone is used for the commission of the crime, the first and foremost thing the officer should have done was to secure the phone to prevent the destruction/manipulation of data. Given the nature of evidence to be copied, maintaining the evidential continuity and integrity of the evidence that is copied is of paramount importance."*
- Further, with regards to Admissibility of Electronic Records, the Hon'ble Supreme Court in **Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal and Ors. AIR 2020 SC 4908**, held that: *"Required certificate under Section 65B(4) is unnecessary if the original document itself is produced. This can be done by the owner of a laptop computer, computer tablet or even a mobile phone, by stepping into the witness box and proving that the concerned device, on which the original information is first stored, is owned and/or operated by him. In cases where the "computer" happens to be a part of a "computer system" or "computer network" and it becomes impossible to physically bring such system or network to the Court, then the only means of providing information contained in such electronic record can be in accordance with Section 65B(1), together with the requisite certificate under Section 65B(4)."*
- The Resource Person also discussed the concepts related to Cyber Contraventions. A cyber contravention refers to a civil wrong under IT Act, 2000. It is important to note that the Law of Torts provide remedies for civil wrong, where affected person can compel the wrong doer to pay damages by way of compensation. However, for cyber contraventions damages are provided under Sections 43-45 of IT Act, 2000.

- The webinar concluded with a vote of thanks by **Ms. Poonam Durgan (Additional Director [Academic], Rajasthan State Judicial Academy**) thanking **Hon'ble Mr. Justice Sandeep Mehta (Judge, Rajasthan High Court and Chairman, Rajasthan State Judicial Academy)** for His Lordship's guidance in conducting the webinar. **Additional Director (Academic, Rajasthan State Judicial Academy**) further extended her most sincere gratitude to Mr. Mukesh Choudhary (Cyber Law Expert, Jaipur) and Mr. Nisheeth Dixit (Cyber Law Expert, Jaipur) for imparting their valuable knowledge with regards to **"Cyber Laws and Electronic Evidence"**; the webinar concluded after expressing the most sincere gratitude to all the participants for making the webinar an interactive and fruitful discussion.
