Programme Report: P- 1299

NATIONAL JUDICIAL ACADEMY

NATIONAL SEMINAR ON CYBER CRIME & ELECTRONIC EVIDENCE
20th & 21st August, 2022

Programme Coordinators

Mr. Yogesh Pratap Singh, Research Fellow & Mr. Prasidh Raj Singh, Law Associate,
National Judicial Academy

Overview of the Programme

The National Judicial Academy organized a two-day National Seminar on Cyber Crime for the District Judiciary on 20th & 21st August, 2022. The objective of the course was to familiarize judges with the ever-expanding threat of cybercrimes and the complex legal issues involved therewith. The programme facilitated deliberations among participant judges on contemporary issues and recent developments in cyber laws. The seminar explored the contours of Cyber Crime– emerging trends, modus, intentions, threats, Jurisdictional Issues in Adjudication of Cyber Crime, Safeguarding Judicial Institutions from Cyber-Attacks, Admissibility and Appreciation of Electronic Evidence, and Scientific Evidence & Expert Testimony.

Session 1
Cyber Crime – Emerging Trends, Modus, Motivations, Intentions, Threats
Speakers: Mr. Sidharth Luthra & Dr. Harold D'Costa

It outlined contemporary issues and recent developments in cyber laws and also underlined complex legal issues. The topic was introduced briefly with explaining the nature of cyberspace and its trans-national reach. It was stated that access to internet- 'universal basic internet' is now being touted as the new human right. The expressions viz. cloud computing, hash values and dark web were explained and discussed in detail. Deliberating on evidence in cyber-crimes and ever-evolving technology, it was stated that technology is not static and, therefore primary known principles may not be sufficient to deal with evolving technology due to issues relating to access of remotely stored data and similar issues. This was further explained with the example of blockchain technology, wherein the data is spread over multiple computers all over the world and keeps growing. With reference to Section 65B of the Indian Evidence Act, the scope of admissibility of evidence was discussed. It was stated that the principles of admissibility depend upon the technology being susceptible to tampering or alteration as well as on the principles of original and secondary evidence. Referring to latest judgements, the meaning & scope of primary and secondary evidence, requirement of certificate and its admissibility in context of electronic evidences was discussed. Deliberations were also made on liabilities of intermediaries within the scope of Information Technology Act, Information Technology (Intermediaries Guidelines) rules, 2011 and The Information Technology (intermediary guidelines and digital media ethics code) rules, 2021. As the electronic records are more vulnerable to alteration, tampering, excision, the legitimacy of the electronic evidence was discussed and explained through practical demonstration & multiple examples.
The judgements; Justice K.S. Puttaswamy v Union of India (2017) 10 SCC 1; United States v. Lizarraga-Tirado, the Ninth Circuit 789 F.3d 1107; Google India (P) Ltd. v. Visaka Industries, (2020) 4 SCC 162; Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473; Arjun Panditrao Khodkar Vs. Kailash Kushanrao Gorantyal and Ors Civil Appeal No.20825-20826 of 2017; Avnish Bajaj v. State (NCT) of Delhi, 2004 SCC OnLine Del 1160; Shreya Singhal v. Union of India, (2015) 5 SCC 1 were also discussed & refereed during the session.

Session 2

Jurisdictional Issues in Adjudication of Cyber Crime

Speakers: Justice A. Muhamed Mustaque & Mr. Sidharth Luthra

It was delineated that Cyber-crime transcends national and international borders and raises jurisdictional issues that one nation alone cannot address and therefore, it has changed our sense of place or duration as well as "the unity of time, place, and action that informed the notion of actus reus in the criminal law" giving rise to jurisdictional issues in investigation and trial of cyber-crimes. The expressions under Cyber Jurisdiction viz. National, Transnational or International were explained. Test to determine jurisdiction was discussed. Following reasons as to why there could be jurisdictional issues in cybercrimes were pointed out;

- Material posted on the internet has worldwide audience;
- It is easy to move website from one territory to another;
- A website can be hosted on one area, but directed at users in another geographic location;
- Parts of a website may be hosted in one area, while other parts of the websites are hosted in another location; and
- It is not always possible to determine where a website or user is located.

Theories of jurisdiction viz. the territorial principles (subjective & objective), the nationality principle, the protective principle, the universality principle and the passive personality principle were also discussed. It was stated that as Internet facilitates remote control across national borders, the fundamental assumptions of territorial criminal jurisdiction often fail. Deliberating on Statutory Framework on Jurisdiction in India, it was stated that Section 166A and Section 105K of Code of Criminal Procedure, 1973 (CrPC), Section 57 and Section 61 of Prevention of Money Laundering Act, 2002 (PMLA), Section 12 of Fugitive Economic Offenders Act, 2018 (FEOA), etc., lay down the procedure of sending 'letter of request' through Competent Court on the request of Investigating Officer. Further, the procedure for execution of a request received from a foreign Court or Competent Authority has been enshrined in Section 166B and 105K of CrPC, Section 58 of PMLA. On transnational evidence gathering, it was stated that access to electronic evidence in foreign jurisdictions is primarily governed by mutual legal assistance (MLA) arrangements, however, there may be situations where the origin of an attack is unknown, where servers in multiple jurisdictions are involved, or other 'loss of location' situations where the principle of territoriality is not applicable. Elaborating further on MLA, it was explained that it is a mechanism whereby countries cooperate with one another in order to provide and obtain formal assistance in prevention, suppression, investigation and prosecution of crime to ensure that the criminals do not escape or sabotage the due process of law for want of evidence available in different countries. The judgements; United States v. Jones 565 US 400; Ajay Agarwal v. Union of India 1993 AIR 1637; Lee Kun Hee & Ors. v. State of U.P. & Ors 2012 (3) SCC 132; Neha V Vibhor Garg CR No. 1616 of 2020 and CR No. 2538 of 2020 (O&M); State of Maharashtra v. Praful Desai (2003) 4 SCC 601; Roshni Biswas v. Union of India 2020 SCC Online SC 881; Internet & Mobile Assn. of India v. RBI, (2020) 10 SCC 274; were also discussed & refereed during the session.

Session 3

Safeguarding Judicial Institutions from Cyber-Attacks: Cyber Security and Data Protection

Speakers: Justice A. Muhamed Mustaque & Dr. Harold D'Costa

Debilitating on cybersecurity in courts, it was stated that Indian organisations witnessed a 218% increase in ransomware attacks in 2021, making the nation the tenth most targeted country globally. It was stressed that with the move towards digitization of Indian Judiciary - judiciary has become recipient of an enormous amount of data including personal and sensitive data of litigants. Referring to Justice K.S. Puttaswamy v Union of India (2017) 10 SCC 1, the right to privacy as a fundamental right was discussed & pointed out that any data leak or data theft would violate the right to privacy. Citing some recent incidents of cyber-attacks on judicial system, it was highlighted that Courts across the world have seen data breaches. In early 2020, a breach was reported in the US Court's document filing system. The U.S. Courts system put out a statement in January 2021 acknowledging that its Case Management/Electronic Case Files system, had been compromised as part of the massive breach. In context of India, it was pointed out that India currently does not have data protection legislative framework to protect against such cybersecurity breaches, however, the Information Technology Act, 2000 can be resorted to- Section 43.

Deliberating on Strategies to prevent and respond to cyber-attacks, it was discussed that the Data Security Council of India has come out with the "National Cyber Security Strategy 2020"; It was suggested that the strategy focuses on a three-fold approach; 1. Secure- the cyberspace by large scale digitisation of public services; use of advanced technology, crisis management; 2. Strengthen- by promoting research and technological development, budgetary allocation for cybersecurity; 3. Synergise- by improving internet infrastructure, cybercrime investigation, and cyber diplomacy amongst nations. In addition, following suggestions were made and discussed during the session;

- Developing institutional capability for assessment, evaluation, certification, and rating of the core devices;
- Timely reporting of vulnerabilities and incidents;
- Map the potential threat surfaces- points where an attacker could gain virtual or physical access to systems and data;
- Ensure physical security of server rooms, devices;
- Limited access to systems, processes and data;
- Invest in cybersecurity;
- Training of staff in requisite cybersecurity best practices and softwares.

Session 4

Admissibility and Appreciation of Electronic Evidence

Speakers: Justice A. Muhamed Mustaque & Dr. Debasis Nayak

It was highlighted that various forms of electronic evidence are increasingly being used in both civil and criminal litigation. It was emphasized that the definition of documentary evidence has been amended to include all documents, including electronic records produced for inspection before the court. A reference was made to Section 2(t) of the Information Technology Act 2000 to underline the ambit and scope of electronic record which includes, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche. With regard to section 65B it was highlighted that print outs, copies of electronic records shall be considered documents, making it primary evidence, if the following conditions are fulfilled:

- At the time of the creation of the electronic record, the computer produced must have been in regular use,
- The kind of information contained in the electronic record must have been regularly and ordinarily fed in to the computer,
- The computer was operating properly; and,
- The duplicate copy must be a reproduction of the original electronic record

It was accentuated that Section 65B performs the same function for electronic records Section 61 does for documentary evidence. It creates a separate procedure, distinct from the simple procedure for oral evidence, to ensure that the adduction of electronic records obeys the hearsay rule. During the course of discussion it was pointed out that firstly it must be proved that the computer output is documentary evidence as per Section 65B(2) and it should be accompanied with a certificate confirming its authenticity as per Section 65B(4). Thereafter the party can rely on that computer output and cannot be compelled to produce the original electronic record in the Court. It is only after the stage of relevancy and admissibility of the evidence, that the genuineness, veracity, or reliability is seen by the Court A reference was made to the case of *Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473 wherein it was held that the very admissibility of such a document, i.e. electronic record which is called as computer output, depends on the satisfaction of the four conditions under Section 65B(2). The court further held that only if the electronic record is duly produced in terms of Section 65B of the Evidence Act, the question would arise as to the genuineness thereof and in that situation, resort can be made to Section 45A opinion of examiner of electronic evidence. Further, the judgment in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal and Ors* (2020) 7 SCC 1 was deliberated upon wherein the apex court held that Section 65B(1) differentiates between the 'original' electronic record, which is contained in the computer in which the information is first stored, and the secondary copies that are made from the primary electronic record. The certificate under Section 65B(4) shall have to be obtained only when the secondary copies of the electronic record are produced before the Court.

During the course of discussion simple copy and forensic copy with regard to identification of deleted file was discussed upon with reference to file allocation table. In this connection the importance of forensic image and forensic cloning was also conversed. It was emphasized that the process of acquisition of file, followed by authentication and analysis is vital to complete the procedure and thereafter produced it before the court under Section 65 of the IT Act. The definition of hash function was highlighted which means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as ―hash result such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible to derive or reconstruct the original electronic record from the hash result produced by the algorithm. It was stressed that the size of the file is immaterial but the output of the file will always remain in the fixed length. Lastly, it was accentuated that by comparing the hash output, authenticity of the document can be identified that whether it is altered or changed.

Session 5
Scientific Evidence and Expert Testimony
Speakers: Justice Atul Sreedharan & Dr. Debasis Nayak

It was emphasized that a basic knowledge of scientific evidence is essential for judges to understand the nuances attached to scientific and expert testimony. With regard to scientific evidence it was stated that a living man can lie, but dead man don't highlighting the importance of post-mortem report. It was emphasized that post-mortem report is of high significance for conviction or acquittal in a trial. During the course of discussion various case studies were cited to emphasize upon the prominence of scientific evidence in justice dispensation.

Participants were demonstrated how morphed frames obtained by morphing procedure as result of the automatic retouching process is used to remove visible artefacts. Challenging expert opinion by way of impeaching the credit of a witness such as; questioning expertise, making witness admit lack of expertise and compelling witness to give 'yes' or 'no' answers were some areas deliberated upon during the session. A reference was made to Section 79A of the Indian Evidence Act which provides that the Central Government may, for the purposes of providing expert opinion on electronic form of evidence before any court or other authority, specify by notification in the Official Gazette, any Department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence. With regard to Section 79A, it was highlighted that no private agency has been identified by the central government or state government as examiner of electronic evidence. This majorly contributes to pendency of cases considering the limited number of agency to examine electronic evidence. It was highlighted that Arsenal Consulting forensic report which found that computer was hacked using malicious software was used as primary evidence in the charge sheet filed in *Bhima Koregaon case*. A reference was made to Section 45A of the Indian Evidence Act to point out that when in a proceeding, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion of the Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000 is a relevant fact.

A reference was further made to the case of *Vinu v. Rebin Sunny & Ors.*, Kerala HC in Mat. Appeal. No. 302 of 2012 (A). It was highlighted that any person who, from his circumstances and employment, possess special means of knowledge and has given the subject attention and is more than ordinarily conversant with its details, will be considered especially skilled for the purposes of Section 45 of the Indian Evidence Act. Following judgments were also pointed out during the course of discussion *R. v. Silverlock*, [(1894) 2 QB 766]*; Dahibai v. Soonderi Damji*, (1907 (9) Bombay Law Reporter (819); *and The State of Bombay v. Kathi Kalu Oghad and Others* 1961 AIR 1808