NATIONAL JUDICIAL ACADEMY

WORKSHOP ON CYBERCRIME AND ELECTRONIC EVIDENCE FOR ADDITIONAL DISTRICT JUDGES

[P-1271]

27TH & 28TH NOVEMBER, 2021

PROGRAMME REPORT

PROGRAMME COORDINATORS: KRISHNA SISODIA & ANKITA PANDEY
FACULTY, NATIONAL JUDICIAL ACADEMY,
BHOPAL

OVERVIEW OF THE PROGRAMME

The National Judicial Academy organised two day online Workshop on Cybercime and Electronic Evidence for Additional District Judges on 27th and 28th November, 2021. The objective of the course was to familiarize judges with the ever-expanding threat of cybercrimes and the complex legal issues involved therewith. The workshop aimed to augment the knowledge of participant judges about the *modus operandi* of cybercrimes, potential targets and emerging threats and explore the contours of cyber security and data protection in light of national and international legal framework. The workshop facilitated deliberations on jurisdictional issues and appreciation of electronic evidence in the adjudication of cybercrimes; contemporary issues i.e. use of social media in offences involving threat to national security; and evolving methods to safeguard judicial institutions from cyber-attacks. The deliberations enabled clinical analysis of statutory provisions, case studies and critical consideration of relevant judgments.

DAY 1

Session 1 - Cyber Crimes: Role of Courts

Session 2 - Jurisdictional Issues in Adjudication of Cybercrimes

DAY 2

Session 3 - Admissibility and Appreciation of Electronic Evidence

Session 4 - Safeguarding Judicial Institutions from Cyber-attacks

DAY – 1

Session 1

Theme - Cyber Crimes: Role of Courts

Panel – Dr. Pavan Duggal & Ms. N.S. Nappinai

The session commenced with the assertion that in view of our increased dependency on technology the rate of cyber-crime is on the rise and we knowingly or unknowingly may have become victim of such crimes. A perpetrator of cybercrime focuses primarily on greed and fear of its target. With the advent of Covid-19 and the fear/panic associated thereto, financial crimes percolated to tier II and III cities where digital literacy is understandably low. It was remarked that the responsiveness in this regard is often without conformity to the standards, processes and procedures before adaptation of any technology. Also, it was stressed that post Covid era is likely to bring a new Cyber World Order wherein large amount of electronic data is created and cybercrime and cyber security breaches will be the default normal. As electronic evidence becomes more and more significant judges will be required to adjudicate upon its veracity, authenticity and admissibility as legal evidence in various cases.

The cases of an international paedophile racket operating through WhatsApp and child pornography crackdown by Kerala Police based on an InterPol report were referred to. Also, the alarming statistics of child sexual abuse material and violent imagery of women online was presented while reflecting upon the functioning of social media and the manner in which law enforcement agencies deal with online crimes. It was expressed that the current legal scenario is not adequate to deal with the intricacies of the cyber world. Law is tasked with the tough job of having to use out-dated processes which may not be well equipped to deal with technology moving at a breakneck speed. In this context, it is significant to find ways to utilize the existing legal remedies in a more effective manner.

In ***In Re: Videos of Sexual Violence and Recommendations***[1] use of innovative solutions such as artificial intelligence, machine learning, deep learning, hash technology and expanding use of

[1] (2018) 15 SCC 551

crawler technology as a tool to fight such crimes was focused upon in order to curb rampant circulation of gang rape/child pornography content on social media. The consensus proposal between the social media platforms and the governing body appointed by the Supreme Court was captured as order of the court. One of the most significant impacts of the *Prajwala* case has been in terms of improvement in the reporting mechanism of such content to the service providers and India has led the way for social media platforms to change their architecture across the globe. The setting up of the website cybercrime.gov.in in 2017 was another landmark associated to the outcome of this case. It has also been instrumental in bringing about *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. The following can be considered as contribution of *Prajwala* to the Rules: (a) expeditious takedown of explicit material within 24 hours; (b) appointment of grievance officer; and (c) deployment of automated tools for identifying and removing content particularly pertaining to offences against women and children.

While discussing the issue of liability of intermediaries the Communication Decency Act, 1996 (USA) and its absolute safe harbour under Section 230 which provides immunity to website platforms with respect to third party content beyond their control was highlighted. In this regard, the Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act, 2019 (Australia) and the extent of intermediary protection provided thereunder was also referred to. In the Indian context, it was clarified that Section 79 of the Information Technology Act, 2000 (IT Act) is a qualified right in view of subsection (2) and (3) dealing with the conditions of exemption. It was opined that when an intermediary is involved in moderating, modulating, verifying or censoring content it ceases protection under the existing legal framework.

The usage of artificial intelligence in tackling the menace of fake news and hate speech with its implication on free speech was also deliberated upon. Some significant cases such as ***Tehseen Poonawalla v. Union of India[2], Kodungallur Film Society v. Union of India[3],*** and ***Alakh Alok Srivastava v. Union of India[4]*** were referred in this context. Further, the warning, flagging and restraint procedure adopted by Facebook and WhatsApp in view of the *'Infodemic'* was taken note of during the course of discussion.

[2] (2018) 9 SCC 501
[3] (2018) 10 SCC 713
[4] 2020 SCC OnLine SC 345

While referring to some recent high profile cases featuring the headlines it was stated that as per *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* if in any matter electronic evidence becomes of crucial necessity the law enforcement agencies and the courts can direct any electronic evidence which is in the custody or possession of the service provider to be preserved till such time the matter is pending. Reference was made to the adoption of a Second Additional Protocol to the Budapest Convention in November, 2021 to enhance co-operation in disclosure of electronic evidence in fighting cybercrime. It was pointed that since India is not party to the Budapest Convention, 2001 reliance is heavily on the mutual legal assistance treaty route which in most cases prove ineffective primarily for want of electronic evidence. A recent phenomenon of 'deepfake' evidence was discussed particularly in respect of family law matters. It was apprehended that as court proceedings through video conferencing have become a new norm some portion of such hearing could also become electronic evidence in courts of law.

Session 2

Theme - Jurisdictional Issues in Adjudication of Cybercrimes

Panel - Mr. Sidharth Luthra & Mr. Sajan Poovayya

The session focussed primarily on harnessing extraterritorial evidence and developing internationally acceptable paradigms and parameters so as to deal with transnational cybercrimes. While delineating on the subject of territoriality it was specified that there are broadly two issues involved i.e. the court having jurisdiction over the dispute and the law to be applied. Giving a historical insight on the issue of extraterritorial evidence the celebrated judgments of the US Supreme Court and the intersection of views expressed in ***Rose v. Himely***[5]***, Hudson & Smith v. Guestier***[6] and ***American Banana Co. v. United Fruit Co.***[7] were discussed.

The challenges in determination of place of suing, territorial jurisdiction and intricacies involved in extra territoriality of evidence were highlighted through a series of illustrations drawing a contrast between the contours of crimes committed in the physical and virtual world. The scenario of artificial intelligence transacting particular aspects on the internet and the difficulty in

[5] 8 U.S. 241 (1808)
[6] 10 U.S. 281 (1810)
[7] 213 U.S. 347 (1909)

attributing jurisdiction in such cases was also deliberated. In ***Zippo Manufacturing Company v. Zippo Dot Com, Inc.***[8] the issue was of determining jurisdiction in cases of interactive websites and transactions on the internet. The *"Minimum Contact"* and *"Purposeful Availment"* tests were held not applicable in this case and the court brought about *"Sliding Scale"* test under which the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the website. However, subsequently the courts implicitly rejected this test criticizing the level of interactivity and commercialism sufficient to justify purposeful availment. The decision in ***Banyan Tree Holding (P) Ltd. v. A. Murali Krishna Reddy & Anr.,***[9] attempted to arrive at a balance in this regard and it was held that when there is a passive interaction or usage on the internet where information is received a court should loathe to assume jurisdiction. However, if it is shown that there is a purposeful availment of the jurisdiction by the person offering the service with instantaneous communication and transaction a court can assume jurisdiction.

Further, sections 1 and 4 of the Indian Penal Code (IPC) read with sections 1 and 75 of the IT Act and the impact of technology on litigatorial avenues were reflected upon. In this regard, the decision in ***M/S SIL Import, USA v. M/S Exim Aides Silk Exporters, Bangalore***[10] was cited wherein the court highlighted the need for giving a wide interpretation to the existing statutes while dealing with internet disputes till the time there is a specific legislation, or unless India becomes signatory to an International Treaty under which the jurisdiction of domestic courts can be ascertained. Further, the decision in ***World Wrestling Entertainment Inc. v. M/S Reshma Collection & Ors***[11] and ***Impresario Entertainment & Hospitality Pvt. Ltd. v. S & D Hospitality***[12] were deliberated at length.

It was stressed that the determination of parties and place of suing are preliminary considerations in any dispute. In this regard, Section 177 and its exception, 178-184, 188 and 189 of the Code of Criminal Procedure (CrPC) were highlighted. Section 179 which constitutes the *Effects Test* was briefly touched upon. The interplay between Section 1(2) and 75 of the IT Act with specific reference to active and passive involvement in cybercrime matters was explained. In ***Swami***

[8] 952 F. Supp. 1119
[9] (2018) 246 DLT 337
[10] (1999) 4 SCC 567
[11] (2017) 237 DLT 197
[12] (2010) 42 PTC 361

Ramdev & Anr. v. Facebook Inc. & Ors.[13] Section 75 of the IT Act has been interpreted to propound that the Act does have extra territorial application to the offences or contraventions committed outside India so long as the uploading takes place from India or the information/computer resource is located in India. While dealing with the issue of extra territorial evidence in terms of obtaining, handling, accessing and utilising the same it was stressed that there are large number of complexities involved in collection of material from overseas when the servers are not located in India especially in the context of cloud computing.

Post 2018, the issue of extraterritoriality has gained impetus especially with the proliferation of data and the manner in which it is being stored. In ***United States v. Microsoft Corp.***[14] Microsoft complied with the request of giving data stored in the United States but not data stored in Ireland. The issue involved was whether the Stored Communications Act (SCA) permits access to data located in servers of another country and whether the request for access is a legally unjustified extra territorial reach. The CLOUD Act of 2018 amended the SCA providing that the request for access is to be honoured irrespective of the location of the data. It was further pointed that the test under the CLOUD Act of reasonable justification based on articulable and credible facts do not find conformity with Sections 91 and 93 of the CrPC. Therefore, there is a need to relook at the IT Act, Indian Evidence Act (IEA) and CrPC especially in view of the fact that India does not have a bilateral arrangement with the US nor is a signatory to the Budapest Convention. Also, the scope of Sections 188 and 189 of the CrPC is not wide enough to deal with cybercrimes having a global colour. It was stressed that the IT Act is a traditionally ill equipped legislation which is not competent enough to effectively deal with interactive e-commerce models, social media intermediaries etc. and attribute responsibility in an instantaneous communication on the internet.

[13] (2019) 263 DLT 689
[14] 584 U.S. (2018)

DAY – 2

Session 3

Theme - Admissibility and Appreciation of Electronic Evidence

Panel - Justice Raja Vijayaraghavan V. & Mr. Harold D' Costa

The session commenced with the assertion that in today's "age of access" technology encompasses every aspect of modern life and digital devices are used as tool, target or both in the commission of crime. The meaning and scope of 'electronic evidence' as provided under the explanation to Section 79A of the IT Act was discussed. Further, it was pointed that the challenge in modern times is that since digital evidence has wider scope it is sensitive, mobile and requires special tools to retrieve with cautious collection and preservation to be worthy to be admissible in a court of law. It was emphasized that if identified, collected and analysed in a forensically sound manner, electronic evidence can prove crucial to the outcome of civil, criminal and corporate investigations. Volatile and non-volatile evidence and their manner of acquisition were discussed with the aid of illustrations.

The session focussed upon certain investigation techniques by providing live demonstration of WhatsApp chat modification, message date/time modification, RT-PCR certificate modification and location spoofing. The discussion further pertained to preservation/retention of electronic data as well as ascertaining its authenticity. The procedure for proper collection of cyber evidence in terms of pre investigation assessment; evaluation of scene of crime; collection of physical evidence and digital evidence; forensic duplication; seizure of digital evidence; packaging, labelling and transportation; legal procedure to be followed; and gathering information from various agencies was elaborated upon.

While referring to the Locard's Exchange Principle it was highlighted that each user's interaction with digital devices leaves both user data and certain remnants of digital data that is contained in the device. Further, the process of documentation of digital evidence was traced from identification/preparation; search and seizure; preservation; examination; analysis; reporting and finally presentation in court. In this regard, it was stated that since electronic evidence can be altered or damaged it is necessary for the court to ascertain that chain of custody is properly

maintained without which it would be difficult to prove the integrity of the evidence. The Secure Hash Algorithm (SHA) must also accompany the chain of custody form.

Further, it was iterated that any documentary evidence by way of an 'electronic record' can be proved only in accordance with the procedure prescribed under Section 65 of the IEA. The changes brought about to the IEA vis-à-vis 'electronic records' was discussed with reference to Sections 3(a), 5, 17, 22A, 39 65A and 65B of the Act. Section 81A and 84A was also discussed in relation to presumptions regarding digital evidence. Section 65B which deals with the admissibility of electronic record requires special procedure for presenting such material as admissible evidence in a court of law. It also provides for technical and non-technical conditions to be complied with in this regard. While dealing with the interpretation of Section 65B ***Anvar P.V. v. P.K. Basheer***[15] was referred. It was pointed that post the decision in ***Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal & Others***[16] it has been mandated that all the conditions specified under Section 65B (2) of the IEA must be fulfilled in contrast to the earlier position wherein the fulfilment of any of the conditions of sub-section (2) would suffice as per Section 65B (4) (c) of the Act. Therefore, certificate under Sections 65B (4) (a) and (b) is no longer needed. The Supreme Court reiterated that the certificate required under Section 65B (4) is a condition precedent to the admissibility of evidence by way of an electronic record and that oral evidence in place of such certificate would not suffice. It was also clarified that certificate under Section 65B (4) is unnecessary when the original document itself is produced.

The session concluded with the remark that judges' understanding and awareness in recognising, appreciating and assimilating the complexities of digital evidence is crucial to ensure that they are appropriately prepared to deal with new challenges in the field of computer crime, forensics and the law relating to it.

[15] (2014) 10 SCC 473
[16] (2020) 7 SCC 1

Session 4

Theme - Safeguarding Judicial Institutions from Cyber-attacks

Panel - Justice A. Muhamed Mustaque, Justice Suraj Govindaraj & Mr. Debasis Nayak

The session commenced by reflecting upon the need for stricter safeguards to be undertaken in relation to the protection of judicial data and the institution itself from cyber-attack. It was interestingly pointed that it is not a question of 'if' but 'when' there may be a cyber-attack on any of the court's IT infrastructure. It was highlighted that *threat* exploits *vulnerability* which leads to *risk*, damaging the assets of an organisation and it can be safeguarded by adopting suitable counter measures. While setting the context of the subject it was stated that judiciary has experienced a sharp increase in cyber incursions in US and Europe over the past years with 24 million attempts in 2019 as compared to 9 million attempts of cyber-attacks in US alone. Similar instances from Atlanta, Alabama, Colorado, Minnesota, Dallas, etc. were shared. Institutions which are significant in the governance of a nation such as administration, defence and judiciary may be targeted to sow chaos and destabilise a regime. It was pointed that network security is often overlooked in the judicial institutions and personnel involved therein are not always adept to best practices in keeping the system safe from cyber-attacks. It was emphasized that any unregulated entry point may provide unfettered access to all connected systems and large amount of crucial data such as encryption, bank details, aadhar/biometrics, victim identification, medical reports, IP and trade secrets, other confidential information not available in public domain etc.

Further, the various categories of cyber-attacks such as System Attack, Network Attack, Web Application, Human Base/Social Engineering Attack, Advanced Persistent Threat (APT), Code-injection, DoS and DDoS Attacks, Pop-ups, etc. were listed. In this regard, the session entailed discussion on phishing, spoofing, web defacement, bot/botnet, trojan/backdoor, ransomware etc. with the aid of illustrations and their potential threat on the judicial institution. The modus of the Pegasus software was explained stating that once installed on a mobile phone as a backdoor it can take control of the messaging app, determine and extract location, record video/audio, extract contact details etc. and send the data to the NSO group in Israel.

The discussion focussed upon the components of the information security system i.e. (a) People (court, judicial officers, court staff, vendors, lawyers, litigants etc.); (b) Processes (steps to

accomplish the objective of strengthening cyber security); and (c) Technology (developing appropriate and adequate network infrastructure). The primary control in this regard is the Information Security Policy so as to provide direction to the management and support for information security within an infrastructure. It was emphatically laid that organisation of information security is achieved by introducing framework provided in ISO 27001 and advised that every High Court and District Court network must be audited for the implementation of the same.

The discussion also explored the basic security domains in terms of (a) Proactive services: technical audit, compliance audit, red team audit, security management and security consulting (b) Active services: security operations centre and real time monitoring (c) Reactive services: CERT-IN or ICERT, digital forensics and cyber investigation. In this regard, reference was made to the National Cyber Security Policy prepared by the Ministry of Electronics and Commerce which must be adopted and implemented at all levels of the judiciary. On the issue of artificial intelligence and machine learning it was stressed that these can be used to ensure cyber security as also to commit data breach therefore, preparedness by judicial institutions becomes much relevant.

On issue of Privacy and Data Protection reference was made to Section 43 A of the IT Act which provides that entities handling Sensitive Personal Data or Information (SPDI) must implement reasonable security practices and procedures to protect it. The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 have been notified. Section 70 of the IT Act was deliberated which deals with Protected System which is essentially Critical Information Infrastructure and is defined as a computer resource destruction of which would debilitate national security, economy, public health or safety. It was iterated that a computer resource becomes a protected system when it is notified as such in the official gazette and the appropriate government would further authorise personnel to access such system. Any access or attempt to access without authorisation is punishable with upto 10 years imprisonment and fine. It was opined that the National Judicial Data Grid (NJDG) be declared as a protected system so as to enable necessary deterrent under the said provision.

Some preventive measures which were emphasized during the course of discussion were: (i) Creating awareness amongst the personnel regarding best practices and SoP; (ii) Setting up a dedicated IT professional team to manage the systems in addition to ensuring that software is

updated and all security patches are installed; (iii) Storage systems to ensure safe and secure copy of all important data in an event of cyber-attack; (iv) Regular threat assessment of the system to ensure all safety measures are functioning in optimal condition; (v) Using a variant of Linux which is less likely to be vulnerable to an attack in comparison to windows operating system; (vi) Audit of Information Security Management System through ISO 27001 framework; and (vii) Systematic update of all software and systems.
