National Judicial Academy, Bhopal

REPORT

National Workshop for High Court Justices

[P-1295]

23rd & 24th April, 2022

Sumit Bhattacharya & Shruti J. Eusebius

Program coordinator & Research Fellow
National Judicial Academy, Bhopal

National Workshop for High Court Justices

[P-1295]

23rd & 24th April, 2022

PROGRAMME REPORT

Programme Coordinators –Sumit Bhattacharya & Shruti J. Eusebius, Research Fellow, National Judicial Academy, Bhopal

A two day "National Workshop for High Court Justices" was organised at the Academy on virtual platform. The online course sought to sensitize the participating justices from pan India on the key aspects and contours of role of judiciary in dealing with the fast changing scenario owing to aspects of cybercrime. The essence of the national workshop was schematically subsumed in four sessions accreting to a deeper understanding of the underlying policy framework through the pragmatic and operational challenges faced in adjudication in the domain. An enabling capsule of best practices evolved through the case law jurisprudence formed part of discourse. The pedagogy and the discourse stimulated intense discussions on appreciation of electronic evidence by the courts in the ever changing modes of cybercrimes *vis-à-vis* global best practices and principles of law evolved therein. A designated session dealing with interstices in safeguarding judicial institutions from cyber-attacks formed part of the course.

The discourse was kindly guided and navigated by Hon'ble Justice Talwant Singh (judge Delhi High Court); Mr. & Dr. Harold D'Costa (Independent Consultant and Domain expert); Hon'ble Justice A. Muhamed Mustaque (Judge Kerala High Court); Mr. Debasis Nayak (Advocate and Academician in cyberlaws); Hon'ble Justice Suraj Govindaraj (Judge Karnataka High Court); Mr. Anand Venkatnarayanan (Independent Consultant and Domain expert).

Session-wise Programme Schedule

Day-1

Session 1 - Cyber Crimes: Role of Judiciary.

Session 2 - Appreciation of Electronic Evidence.

Day-2

Session 3 - Territoriality and Jurisdictional Issues in Cyber Crimes.

Session 4 - Safeguarding Judicial Institutions from Cyber-attacks.

Session 1
Theme: Cyber Crimes: Role of Judiciary

Speaker: Justice Talwant Singh & Dr. Harold D'Costa

The session commenced with a discussion on virtual crimes, its pervasive nature, evolving modus of commission and the motivations of offenders. The major types of cybercrimes were identified. The seriousness of the issue was highlighted by referring to two recent news reports regarding firstly, the presence of child abuse material on the internet and secondly, the practice of internet scapegoating. The fact that most websites which upload offending content are based outside India was stated to be the major challenge in the investigation and adjudication of cybercrimes. The rise of new issues with the use of video conferencing was highlighted including the commission of obscene acts which are inadvertently broadcasting on the video conferencing forum, and which hitherto would not amount to an offence since the same was committed in the privacy of one's home or office.

In light of the increasing prevalence of cybercrimes, emphasis was placed on the need for a security audit of the judicial system and for the need to prioritise digital security for the judiciary. It was stated that the judiciary is a potential target for cyber criminals. There is a need to determine policy of data protection and virtual security for the courts. Measures must be undertaken as a matter of priority to secure the court in the virtual world and to secure data, files, apps etc. of the judiciary. The use of pirated softwares was flagged as an issue for consideration and emphasis was placed on the need to ensure that verified softwares are used in courts, legal services authorities, and state judicial academies. The need for the creation of a database of judgments by the judiciary was also emphasised as a necessary step to make judgments accessible to the public and to reduce dependence on external agencies. The need was expressed for measures to secure data in the judicial system to ensure that sensitive and confidential information is protected. Unauthorised access to judgment drafts was also flagged as a concern. It was stated that the judiciary generates large volume of

data in the form of judgments and orders which contains details like names, addresses etc. This data can potentially be used to improve the judicial system. The right to be forgotten was emphasised as a pertinent consideration in this regard. The challenges in enforcing orders for takedown of content was discussed. The right to privacy in the digital era and the intrusions into the privacy of an individual by digital devices including smartphones was discussed. The collection, appropriation and misuse of personal data was highlighted as an issue impacting the right to privacy.

Emphasis was placed on the need for cyber forensics training for judges and also for other stakeholders including advocates, police and public prosecutors. It was also suggested that security and virus protection softwares must be purchased and installed on devices including smartphones and reliance on free softwares should be avoided. Caution should also be exercised while installing applications and softwares, and the terms and conditions of these applications and softwares must be carefully read while installing. Discussions also touched upon the Dark Web and the challenges in regulating the same and investigating transactions undertaken on the Dark Web. The use of drones for commission of offences was also pointed out

Discussion was undertaken on the Internet as a medium for the commission of cybercrimes. In this regard it was stated that the internet is not owned nor controlled by any single entity, it is largely self-regulated; hence it is a challenge to regulate activities on the internet. Further, the fact that all root servers, which are a critical part of the internet infrastructure, are located in other countries was highlighted as a challenge in investigation of cybercrimes. Emerging trends in Cyber law were discussed and the following emerging challenges were highlighted –

- Determination of jurisdiction in cybercrimes.
- Challenges in understanding the behaviour of cybercriminals and their modus
- Lack of training of law enforcement
- Location of servers outside India
- Absence of dedicated law or legal policy on the regulation of mobile communications devices.
- Need for policy on cybersecurity

- Need for creation of a culture of cybersecurity through awareness building measures
- Need for legal remedies to address cloud computing incidents, data security and privacy issues, to determine jurisdiction in cloud computing cases.
- Rise in litigation relating to social media including defamation, cyber harassment, cyberstalking, and identity theft.
- Need for effective legislative provisions to address spam.

Emphasis was placed on the need for a strong legal regime for data protection in India to protect privacy rights and to build awareness. In this context, the various data stored by third parties (personal data, engagement data, behavioural data and attitudinal data) and its misuse was pointed out citing examples of data leaks, and social media misuse. Challenges in determining jurisdiction was discussed at length and it was stated that determination of location of main server is a major challenge which in turn determines the jurisdiction. Further, the lack of uniform policy on storage of data by service providers was also identified as a challenge in investigating and adjudicating cybercrimes. Faulty biometrics was also pointed out as a matter of concern which would pose challenges in adjudication of cybercrimes. Morphing of data and the challenges in detecting morphed and fake data were discussed with a live demonstration of morphing. Discussions were also undertaken on intermediary liability citing Section 79 of the Information Technology Act, 2000 (IT Act). Victimisation in cybercrimes was also touched upon.

Session 2
Theme: Appreciation of Electronic Evidence

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

The session commenced with discussion on the appreciation of evidence and the assessment of probative value of the evidence with the concerns of spoofing in mind. Reference was made to the judgments in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal,* (2020) 7 SCC 1, *Shafhi Mohammad v. The State of Himachal Pradesh*, (2018) 2 SCC 801 and *Anvar P.V. v P.K. Basheer*, (2014) 10 SCC 473. The admissibility of

electronic evidence and the interpretation of Section 65B post the judgment in *Arjun Panditrao Khotkar* was discussed.

Major issues in the appreciation of electronic evidence were discussed. Firstly, consideration was given to the challenge in enforcement of the right to privacy in cases where electronic evidence produced before the court may pertain to private matters of the parties which may be intrusive, non-consensual or may have be acquired through illegal means. The admissibility of such evidence was considered and the judgement in *US v. Jones* 615 F. 3d 544 was discussed. Secondly, the challenges in securing evidence in other jurisdiction and the options available including Mutual Legal Assistance Treaties were discussed. Thirdly, the issue of testimonial compulsion in electronic evidence *vis-à-vis* Article 20(3) of the Constitution of India was emphasised. The judgments in *P. Gopalkrishnan v. State of Kerala*, (2020) 9 SCC 161 and *Virendra Khanna v. State of Karnataka*, 2021 SCC OnLine Kar 5032 were discussed in this context.

The compromising of evidence was discussed referring to the US Door Frame case and Logic Bombs. Methods of forensic examination of electronic devices was elaborated upon and it was stated that the forensic examination should reveal the softwares used and their versions, the hash results and the details of the storage media. Emphasis was placed on the maintenance of a chain of custody log which authenticates the electronic evidence. This log must necessarily provide the following details i.e. the person(s) who took possession of the device/evidence; the description of evidence; the places where it was taken; the time and date it was taken; and the purpose for taking the evidence.

The Omega case was discussed to detail the methods in which cyberattacks are committed and the evidence in such cases. The basic requirements to establish guilt in a cybercrime case was discussed viz. – the correct procedure is followed by Investigating Officer; the function of the 6 line program (expert opinion); and determination of the fact the software or program could only have been installed by the suspect. The evolving nature of digital evidence was highlighted and the major types of devices from which evidence can be acquired was discussed. Internet based

cybercrimes were discussed at length. The major internet based cybercrimes (DNS spoofing, web defacement, FTP attacks, bogus websites, web spoofing, and website based launch of malicious code, cheating or fraud) were explained. The fundamentals of investigation of internet based cybercrimes was delineated and it was stated that the IP Address key to almost all web based crimes. The method to identify and locate IP Addresses was demonstrated.

Evidence in phishing cases was discussed and the details required while collecting evidence was specified –

- The victim's internet service provider
- Whether there is a copy of the email
- The purported sender
- Domain name and IP address of the suspect site
- When and where the site was visited by the complainant
- Bank accounts to which payments were made
- Any contact email address
- Relevant service providers
- Whether headers have been examined.

Admissibility of digital evidence was discussed referring to Section 65B, IT Act and the conditions to be satisfied under Section 65B were discussed –

- Computer output was produced by a computer regularly used to store or process information.
- File type that was being regularly fed into the computer is similar to the evidence in question.
- Computer was operating properly. If not operating properly, it has not affected the creation of secondary evidence.
- The computer was ordinarily used for storing/processing such file types containing the primary evidence.

The certificate under Section 65B(4), IT Act and is requirements were highlighted in the discussion. The certificate is required to–

- Identify the electronic record and describe the manner in which it was produced.
- Provide particulars of the devices involved.
- Provide all information required under Section 65B(2)
- Signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities

It was stated that Section 65B(4) certificate is not an expert opinion report, rather it only makes the evidence admissible. Subsequent to this, the evidentiary value of the evidence need to be examined through an expert opinion. Discussions on Section 65B also included a consideration of the judgments in *State (NCT of Delhi) v. Navjot Sandhu,* (2005) 11 SCC 600; *Anvar P.V. v P.K. Basheer; Shafhi Mohammad v. The State of Himachal Pradesh; Tomaso Bruno v. State of U.P.,* (2015) 7 SCC 178; and *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal.*

Examiner of Electronic Evidence under Section 79A, IT Act was discussed and it was pointed out that the examiner of electronic evidence can only be a governmental agency. It was opined that this limitation acts as a restriction against employing the services of private agencies with proven competence, and contributes to the delay and pendency. In this context, the Pegasus matter and its linkage to the Bhima Koregaon case was discussed. In the Bhima Koregaon case, the report of Arsenal Consulting revealed the presence of Pegasus spyware in the phone and Netwire malware in the laptops of the accused. However, such report is not admissible as evidence under Section 45A of the India Evidence Act as it is provided by a private agency. The discussions on admissibility of evidence also included discussions on *Virendra Khanna v. State of Karnataka*; *Magraj Patodia v. R.K. Birla*, (1970) 2 SCC 888; *Pooran Mal v Director of Inspection,* (1974) 1 SCC 345 and *State (NCT of Delhi) v. Navjot Sandhu*. The issue of testimonial compulsion was also discussed in relation to cases where accused persons are compelled to provide their passwords, and it was considered whether such act of compulsion would be violative of Article 20(3) of the Constitution of India.

Session 3
Theme: Territoriality and Jurisdictional Issues in Cyber Crimes

Speakers: Justice N. Kotiswar Singh, Justice Talwant Singh, Mr. Debasis Nayak

The session kicked-off by tracing the intersecting nebulous created owing to the fast evolving technology deeply pervading the society and poses operational challenges to the extant legal setup. Such interfaces of techno-legal disruptions accretes novel and evolving procedural bottlenecks and saturates the potency of a legal system to grapple with such issues on one hand and squarely address them on the other. It was highlighted that the very nature of the virtual world enabling electronic transactions, transcending national boundaries make them ungainly in terms of fixing jurisdictions, and often pernicious to institutions and nations. Jurisdictional scope of cybercrimes may be classified international (i.e. trans-national beyond the geopolitical reach of a nation), and intra-national (wherein the pecuniary jurisdiction is hit by the huge cost involved therein). The involvement of multiple sovereign State jurisdiction gravitates the complexity in cybercrimes. Jurisdiction of a court is its competency to hear and decide issues by rendering enforceable judgments was emphasised in light of Section 188 Code of Criminal Procedure, 1978 (CrPC), Section 4 of Indian Penal Code, 1860 (IPC) and Section 75 of the Information and Technology Act, 2000 (ITAct). A brief account of the provision under Section 75 of the ITAct with its ingredients was given. It was however sceptically asserted that the scope of Section 75 does not immutably and squarely addresses the evolving and mutating panoply of novel territorial issues. It was underscored that the transcendental nature discussed above also offers the advantage of application of the jurisprudential principles evolved in one part of the globe to another, owing to the fact that the underlying causative technology involved remains the similar or comparable. Few such principles which have been globally evolved and locally applied (by Indian courts) include the "minimum contacts and a purposeful availment" to determine territorial jurisdiction of a court. *Asahi Metal Industry Co. v. Superior Court of California,* 480 U.S. 102 (1987) was referred. The genesis of the "minimum contact test" was traced back in *International Shoe Co. v. Washington*, 326 U.S. 310 (1945) way before computers or at least cybercrimes came to existence. Similarly, the "sliding scale" or the popularly known "zippo test" was cited as yet

another principle. The test is a three-prong test to establish jurisdiction over a website based on three categories namely: active, passive, and interactive websites. It was evolved by District Court of Western District of Pennsylvania, US in *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 1119 (W.D. Pa. 1997). It was held therein that "the likelihood of constitutional exercise of personal jurisdiction is directly proportional to the nature and quality of commercial activity that an entity conducts over the internet". Hence the more the activity the scale slides more towards the higher possibilities for invoking the personal jurisdiction. A third test discussed was the "effects test" wherein an operating website intends and causes an effect in a particular forum (or sometime State), in such a case it avails the privilege of doing business there for purposes of assumption of jurisdiction of a relevant court. The "effects test" was evolved in *Calder v. Jones*, 465 U.S. 783 (1984). It has been further ascertained in *Dudnikov v. Chalk & Vermilion*, 514 F.3d 1063 (10th Cir. 2008), that the "effects test" is often found to be useful when the exact nature of the defendant's internet activities is to be assessed *vis-à-vis*, injury caused to a resident elsewhere, in a different State. The European position was discussed by citing "Brussels Convention on Jurisdiction and Enforcement of Judgments in Civil and Commercial Matters, Regulation 44/2001 (Dec. 22, 2000). In EU the Article 5(3) allows for two jurisdictions – the place of domicile of the defendant or the place where the harm has occurred. *Handelskwekerij G J Bier B. V. v. Mines de Potasse d'Alsace SA*, Case 21/76 [1976] E.C.R. 1735; and *Shevill & Ors. v. Presse Alliance S.A.*, Case C-68/93 [1995] 2 W.L.R. 499 were referred.

A few Indian case law emulating the aforementioned principles were discussed which included*: Independent News Service Pvt. Limited v. India Broadcast Live LLC*, 2007 (35) PTC 177 (Del.); *Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy*, CS (OS) No. 894/2008. It was pointed out that the case had its own limitations and is not a "one size fits all". While a strong precedence may be drawn for IPR issues and online transactions, it leaves torts *viz.* defamation uncovered. The jurisprudence on "cause of action", was discussed to be at a place where the customer carried out his part of transaction citing *World Wrestling Entertainment Inc v. M/s. Reshma Collection,* 2014 (60) PTC 452 Del (DB) wherein the court laid down the jurisdiction based on the

spontaneous nature of online transactions (i.e. offer and acceptance and payment of consideration). The issue of scope and extent of jurisdiction of an Indian courts to order a "global takedown" or "geo blocking" or "global injunction" was discussed w.r.t *Swami Ramdev v. Facebook, Inc.*, CS (OS) 27/2019 of Delhi High Court. The conflicting judgments asserting a "global injunction" in *Subodh Gupta v. Herdscene,* CS(OS) 483/2019, Delhi High Court (Order dated 18th September, 2019); and opposing such a concept in *You Tube v. Geeta Shroff*, FAO 93/2018, Delhi High Court (Decided on 17th May, 2018) was put to rest in *Swami Ramdev case.* The question as to "what would constitute removal or disabling access within the meaning of Section 79 of IT Act. Can removal or disabling access be geographically limited or should it be global?" was mooted in *Swami Ramdev case*, wherein the court held that:

> The interpretation of Section 79 as discussed hereinabove, leads this Court to the conclusion that the disabling and blocking of access has to be from the computer resource, and such resource includes a computer network, i.e., the whole network and not a mere (geographically) limited network. It is not disputed that this resource or network is controlled by the Defendants. When disabling is done by the Platforms on their own, in terms of their policies, the same is global. So, there is no reason as to why court orders ought not to be global. All offending material which has therefore, been uploaded from within India on to the Defendants‟ computer resource or computer network would have to be disabled and blocked on a global basis. Since the unlawful act in case of content uploaded from India is committed from within India, a global injunction shall operate in respect of such content. In case of uploads which take place from outside India, the unlawful act would be the dissemination of such content in India, and thus in those cases the platforms may resort to geo-blocking.

The session resonated with inquisitive inquiries and small but effective local practices adopted by the courts to deal with the dynamic and ever mutating cybercrime cases brought before the courts.

Session 4
Theme: Safeguarding Judicial Institutions from Cyber-attacks

Speakers: Justice Justice A.M. Mustaque, Justice Suraj Govindaraj, Mr. Anand Venkatnarayanan

The session started with an upfront and honest confession of ignorance of the subject matter to the judges in a judicial system to deal with the potential threat. The ignorance might be classified to include issues relating to the contours, anatomy, scope, impact assessment, qualitative and technical knowhow, operational bottlenecks, or of such other myriad dimensions including essence of being current or that of being obsolete and redundant. It was urged upon the justices to take voluntary initiatives and run meticulous awareness programs to enable the judges from the District Judiciary to understand, respond to, and deal with cyber-attacks. It was acknowledged that the pandemic challenged the conventional court system of justice dispensation and catalysed the adoption of the virtual operations of the judicial system by compulsion eclipsing and overtaking the sceptical and tardy rate of transition to virtual processes, otherwise adopted by choice. As any reactive and impulsive adoption would have its own problems, things as basic as choosing an appropriate video conferencing platform had its own abrasive issues. While enlisting the teething problems, unpreparedness to adopt an IT implant into the judicial system posed a formidable challenge. The natural inertia to resist change owing to stereotypical mind-set was identified to be yet another stumbling block. It was underscored that the last decade and a half of IT and related reforms in the Indian judiciary had been phenomenal in scale though, but had seen its rainy days as implementation impediments. The dissatisfaction was also attributable considering the volume of resources spent therein including financial & human resources.

It was highlighted the aforementioned systemic issues might be considered as the moot vulnerabilities facing cyber-attacks once the Indian judiciary slowly and progressively aligns to complete digitisation. It was cautioned that the threat of prospective cyber-attacks is neither very far nor imaginary. It is real and proximate enough. Judicial institution would not be auto-immune or impregnable by mere figment of assumptions. Hence, realistically the right question is not “If” but “when”

there could be a cyber-attack on the judicial infrastructure. It was resounded that the false sense of security looms only at the peril of facing such an attack. The lack of preparedness on the pretext of not having cyber security engineers, network security engineers and such important sentinels even at High Court levels poses a serious sense of insecurity against imminent cyber-attacks. Judicial data is a precious commodity worth stealing or guarding as a goldmine. Involvement and role of judiciary facing cyber-attacks can be said to have two paradigms: as an administrator and dispenser of justice to victims of cyber-attacks; and as a victim itself.

It was asserted that while addressing cyber-security issues, it would not be out of context to consider the analogy of conventional security (*viz.* national security), wherein the phrase "offence often is one of the best form of defence" is popular. It was asserted that schematically dividing the understanding of nature and scope of cyber-attacks and designing certain best practices to armour the judicial institution to shield against it could be done by separately understanding four sub-domains: Nature of Internet which enables optimum understanding of certain operational issues as to how and why a cyber-attack is performed and more; Internet Service Providers (ISPs) since they play a key role in controlling and sharing sensitive inputs; Passive Intelligence, which essentially is a sort of Data Analytics at national, institutional, personal scale, particularly on network defence. It was stated that an overall birds eye-view would generally reveal a pattern that the operations at national, or organisational, or personal level would have many commonalities and least common factors; and lastly delve into the sub-domain of control mechanism wherein, access control and device control mechanisms need to be granularly understood to prevent a prospective cyber-attack. The session ended with sharing experiences and limitations faced in implementing IT related court reforms.