NATIONAL JUDICIAL ACADEMY, INDIA

NATIONAL SEMINAR ON CYBERCRIME & ELECTRONIC EVIDENCE [P-1348]

Date: 22nd - 23rd July 2023

PROGRAMME REPORT

PROGRAMME COORDINATOR: SUMIT BHATTACHARYA & PRASIDH RAJ SINGH, FACULTY, NATIONAL JUDICIAL ACADEMY, BHOPAL

Session 1 - Cybercrime – Emerging Trends, Modus & Threats: The Session covered certain major premises including: Transnational reach of the cybercrime cases; Cyber technology: Cloud computing, hash values and the dark web; and Liability of intermediaries. Why the area of law should be bothering India and Indian judiciary was underscored by citing the facts, that India in terms of internet penetration is one of the largest jurisdiction, securing the second largest position globally in terms of usage of broadband and non-broadband based internet users. The vehicle of data carriage i.e. the telecommunication capability (atleast upto 4G levels) puts India to a prominent position. India actually beats China when it comes to telecom penetration. India secures the top position when it comes to digital financial transactions in the world (curtesy UPI). Therefore, renders a virgin ground and serves as a ready recipe for potential cybercrimes. It was highlighted that one of the challenges posed to the judiciary while dealing with cybercrimes is the paradigm of being meta-physical. The typical attunement and training to consider and look for physical facts (as in cases of any other crime in the physical world) blurs the visions of the judiciary and the law enforcement agencies to distinguish a cybercrime. It confuses a typical legal set-up which is otherwise prepped-up for physical crimes. So the difficulty to convert the essentials of a cybercrime to meet the standards laid down (both substantive and procedural) for dealing with crime in a physical world was pointed out to be major interstice. References were made for "Dark Web" and "Deep Web". It was narrated that a typical transaction in dark-web, of an illegal weapon, a consignment of narcotic drugs, or a contract to kill can be operated, by making the online payment in virtual currency. Once such initiation is rooted in the dark-web, a physical crime may result in the form of a terrorist activity, rape, financial embezzlement, cheating or murder. While adjudicating such a case, the trouble is located on the virtual side of the spectrum rather than the well-developed and settled law (through statutes and case law jurisprudence) of the physical world. The capability of a bit-coin mixer to disable virtual footprints of an illegal transaction was illustrated. Therefore, it was insisted that harping upon the minimum necessary knowhow about the emerging technologies and the trends becomes inevitable for the judges and the law enforcement agencies. The second most important takeaway underscored is a sequel to the first one, and is to ask a right and relevant question(s) (regarding and including the evidence(s)), to deal with the issue in *lis.* On the other hand there are certain genre of cybercrimes which are not necessarily conducted using Deep Web. A simple malware injected into a closed network system (especially in that of a financial institution *viz.* banks, treasury etc.) may perpetually syphon out

money using a "Salami software". In such a case amassing reliable electronic evidence of innumerable and insignificant transaction details to prove a case of a million dollar continuing *fintech* scam is not an easy proposition. The transition from web 1.0 to web 3.0 was discussed. The inability and incapacity of law to establish liability on an Artificial Intelligence (AI), thereby forecasting the impairedness of the extant legal system to address such novel and fractured areas of cyberlaws was underscored. Elucidating a hypothetical situation it was illustrated that while the Information Technology Act, 2000 (IT Act) might hold a malware programmer liable, a programmer of AI-algorithm-which in turn programed a malware responsible for a cybercrime can certainly not be held liable. (S)he cannot be generally held vicariously liable, or be held responsible by lifting the veil as typical in the case of a company which is an inanimate person. Because the company on its own volition cannot be said to flout a law or do a crime, whereas an AI instead, is capable of independently do the same Nor can the AI algorithm be held liable, owing to the fact that there exists no jurisprudence to hold such an independent and inanimate person in an AI liable. Online gaming and gambling (e.g. online rummy) was discussed. It was discussed that every High Court in the South of India has held Online gaming of rummy contested on account of Art. 19(1)(g) to be a "game of skill" and not a "game of chance" and therefore a fundamental right. Reliance on several judgements could be made including: *State of Bombay v. R. M. D. Chamarbaugwala*, AIR 1957 SC 699; *State of Andhra Pradesh v. K. Satyanarayana*, AIR 1968 SC 825; *M.J. Sivani v. State of Karnataka*, 1995 6 SCC 289; *Dr. K.R. Lakshmanan v. State of Tamil Nadu*, AIR 1996 SC 1153. However, if an online game is played by a bot using AI, then how should the Courts respond? Does such a game remain a game of skill anymore? Under a similar situation if a defamatory libel is published by an AI (say using a program *viz*. ChatGPT), who is to be sued? Or against whom an injunction be brought? [55:15]

Session 2 - Jurisdictional Issues in Adjudication of Cybercrime: The session started with the thought that, technology should wind-up making the judges and the justice delivery system as a better human being working in a perpetually qualitatively evolving system. However, a caution was sounded as to the fact that, technology if not being reasonably bridled might bring about perverse impact creating ripples in the society (e.g. vast outreach and pervasive use of social media could stir-up an environment of insecurity and a feeling of unjust society, in an unbelievably quick turnaround time). It was in this pretext the boundaries, scope and capacity of a court (jurisdiction) to deal with such militating and unsettling ideas was thought to be vital to be discussed. While

discussing jurisdiction for adjudicating the relevant statutory provisions from Indian Penal Code, 1860 (IPC); Information and Technology Act, 2000 (IT Act), The Code of Criminal Procedure, 1973 (CrPC); Code of Civil Procedure, 1908 (CPC); Indian Evidence Act, 1872 (IEA); and certain International Conventions and Covenants were considered. The triangular interplay and application of Section 4 of IPC, Section 75 of IT Act, Section(s) 188 CrPC was discussed. The various permutations of probabilities of an Indian or a foreigner committing a cybercrime in India or outside India was discussed w.r.t. the jurisdiction of an Indian court with the help of the relevant statutory provisions was discussed. While discussing a hypothetical scenario of a foreign citizen, using foreign computer resources, commits a cybercrime in India, it was debated and then summarily explained that Section 1(2) read with 75(2) of IT Act. It was further elaborated while the discourse enabled the test for jurisdiction in a cybercrime, as to how to determine which court in India shall be having such jurisdiction to try? The various relevant provisions of Chapter XIII of the CrPC were discussed. The interaction of Section 182 of CrPC read with Section(s) 1(2), 13 & 75 of the IT Act was discussed to clarify the place or court having jurisdiction in cases of e-mails or other electronic communications leading to a cybercrime. The application of "access" *versus* "purposive availment" tests evolved by the various case law *viz. Zippo Manufacturing Company v. Zippo Dot Com, Inc* 952 F. Supp. 1119; *Banyan Tree Holding (P) Limited v. A. Murali Krishna Reddy*, (2010) 42 PTC 361; *Casio India Co. Ltd. v. Ashita Tele Systems Pvt. Ltd*., 2003 (3) RAJ 506*; Independent News v. Indi a Broadcast Live,* 2007 (35) PTC 177 Del (contrast view taken by the Delhi HC as against *Casio Case* relying upon the foreign wisdom as laid down in *Compuserve Inc. v. Patterson*, 89 F.3d 1257 (6th Cir. 1996)). It was underscored that the issues relating to the civil jurisdiction of a court in cases of cyber wrongs seems to have substantially been developed and settled. However, that relating to the criminal jurisdiction is a "work in progress". In criminal jurisdictions the court might consider using the various tests (*viz.* sliding scale test, effects test, purposive availment test etc.) but with the view that it enables and doesn't logically disables (merely technically) the dispensation of justice. The dichotomy of scope and extent of fixing Intermediary Liability in case of online publications (e.g. defamation etc.) and its fluid state of evolution in law was posited. It was discussed to discern between a conventional print publication, to DTP (Desk Top Publication), to an online publication in a typical "social media platform" including a forwarding of a document (a republication situation). Republishers' liabilities should not be confused to those of mere "distributors", instead they are akin to those of

the first publishers'. Distinctions between "geoblocking" *versus* "global injunction" was drawn. The concepts of MLAT (Mutual Legal Assistance Treaties), Extradition Treaty, and "*Letters Rogatory*" was dealt with citing examples.

Session 3 - Safeguarding Judicial Institutions from Cyber-Attacks: Cyber Security and Data Protection: The session commenced with an exploration of the practical aspects of handling cybersecurity issues, emphasizing that much of the operational responsibility falls on the court staff. The importance of not merely locking away instruments but adopting effective measures to ensure data security was pointed out. The discussions highlighted the need for judges to remain vigilant, especially in cases where their data may be at risk, such as when judgments are uploaded to the system but not yet delivered. The discussion focused on the formidable challenges encountered by the judicial system regarding cybersecurity. Several incidents were cited to illustrate these challenges. One such incident involving a cyber-attack on the court was discussed, where data and information were flooded onto a specific email account, causing a temporary collapse of its operations. The hacking of data from the All India Institute of Medical Sciences was also highlighted. These examples underscored the critical need for robust cybersecurity measures.

The session emphasized that these incidents are valuable lessons and showcase the evolving nature of cyber threats. It was pointed out that, in the realm of cybercrime, the adversaries, whether scientists or criminals, are often at the forefront of technological advances. This creates an ongoing challenge for the judicial system to keep up and continually adapt to emerging threats.

A significant portion of the session revolved around the role of judges and court administrators in enhancing cybersecurity. The discussion raised important questions about judge's knowledge of using technology, with a particular focus on whether they should become proficient in computer science. The balance between workload and technical proficiency was a key concern. The session emphasized the judge's role in safeguarding data, even when operational aspects may be delegated to support staff. The need for proactive measures, negotiation, and threat management was highlighted to effectively address cyber threats.

Further, the session delved into the practical aspects of handling data within the judicial system. The discussion highlighted the importance of hash values in the context of cybersecurity, emphasizing their role in ensuring data authenticity and preventing unauthorized alterations. Hash values were defined as unique alphanumeric strings generated by applying a hash function to data.

They act as digital fingerprints, verifying the integrity of data and detecting any changes or tampering.

Legal implications of hash values were also highlighted during the session. It was explained that during proceedings, the presentation of hash values could be pivotal in linking digital evidence to a specific individual or event. Furthermore, the discussion stressed the importance of retaining hash values for digital evidence, as the failure to produce hash values during a trial could engender disputes and challenges regarding the authenticity of digital evidence.

Session 4 - Admissibility and Appreciation of Electronic Evidence: The Session started by enquiring about what is electronic evidence? In simpler language it is any probative information which is created, stored, or transmitted in a digital form is an e-evidence. A caution was sounded about the issuance of digital signatures based on the ones' email ID. The process subjects immense risk, as it exposes the fact that anyone with someone else's email ID can get a digital signature of the person who's email ID has been shared. It is only now that the digital signatures are being issued as against biometrics. The three concepts "Relevancy" (Sections 5 – 16 & 32 of the IEA); "Admissibility" (Section 65B(4) of the IEA); & "Reliability" of an electronic evidence was discerned. It was clarified that although while undertaking a trial all the three are important and inter-dependent, but one does not necessarily addresses or proves the other (*viz.* Section 65B(4) certificate only enables "Admissibility" of an electronic evidence (which is "secondary" in nature), but certainly does not ensures "Reliability" of such evidence. Moreover, whether an "Admissible" electronic evidence is of "Relevance" to the facts in issue needs to be separately ascertained. *Rahul v. State of Delhi*, (2023) 1 SCC 83 was discussed wherein the apex court held that the scientific evidences including the electronic evidence must be proved by the prosecution by leading cogent, clinching and clear evidence to establish the guilt of an accused. It was asserted that even an expert evidence is only an opinion-evidence and the report submitted by him/her must be properly examined (in fact the expert needs to be present before the court with his/her "rough notes" which may be referred by/before the court to validate the basis of an expert's opinion). The doctrine of "Individualization fallacy" was discussed. It was underscored that the role of a judge while admitting, appreciating, and seeking for the reliability of an electronic evidence, has to be more proactive, self-driven, innovative to at least do the small but essential bits for themselves, rather that squarely depending on documents produced by the investigation reports, expert reports et. A

judge can for himself/herself ascertain the veracity by use of metadata, match the reported DNA conclusions to ascertain the common follies (*viz.* Erroneous reporting of cent percent matching of the DNA of blood or semen samples of the victim in his/her inner wears, or a much lower degree of matching is clinically ascertained say merely ~60% match to be concluded and reported as "matched"). Therefore, a caution was marked to consider an experts or a mechanical report as just an "opinion" and not conclusive. It is the duty of a judge to ascertain further the extent and validity of such submissions or depositions. The lack of legislation regulating "biometric data" was discussed.

Session 5 - Scientific Evidence and Expert Testimony: The session commenced by revisiting the foundational principles enshrined in Sec. 3 of the Indian Evidence Act. It was reiterated that Sec. 3 offers definitions that form the bedrock for admissibility and reliability of evidence. Sec 65B of the IEA can be conservatively seen to be only a provisional mechanism to ascertain a admissibility of an 'electronic record' (Sect 2(1)(t) of IT Act) which is a 'computer output' as a document which is a 'secondary evidence'.

The crucial role of expert evidence in legal proceedings was underscored. It was stressed that expert evidence, like any other form of evidence, is subject to scrutiny by the court. The Indian Evidence Act, particularly Sec. 45, was referenced to establish that expert evidence may or may not be believed, with the court having the discretion to assess its credibility. The session underscored the fact that courts turn to expert testimony when they face issues that they cannot readily understand or ascertain. It was pointed out that in such cases, the court relies on experts to provide insights and clarification. However, the determination of whether a person qualifies as an expert or whether their testimony is reliable can be subject to cross-examination and challenges during proceedings.

The discussion touched upon the challenges and limitations of expert testimony. It was highlighted that, like all forms of evidence, expert evidence is not infallible and can be subjected to scrutiny and rebuttal. Specific examples were cited to illustrate the challenges faced in accepting expert evidence unequivocally. Ballistics and DNA analysis were mentioned as areas where expert evidence can be contentious. Differences between rough notes and final reports were noted as potential sources of doubt. The session emphasized that, the court's role is to analyze and assess

the credibility and reliability of expert testimony, ensuring that it aligns with legal standards and the weight of evidence presented.

During the discussion several challenges were brought to light when assessing the credibility of expert witnesses. Notably, the session raised concerns about experts who venture outside their field of expertise. For instance, a data science expert providing testimony on biological forensics may not be deemed an expert in that domain. The importance of defining the scope and limits of an expert's field of expertise was stressed to ensure their testimony's relevance and credibility. It was underscored that expert opinions, even when presented in court, do not mandate automatic acceptance. The court is not bound to accept an expert's opinion instead, it reserves the right to exercise its own judgment and record its reasons for doing so. This approach emphasizes that expert testimony, although valuable, is not an absolute authority and is subject to critical evaluation

The session brought forth several challenges associated with electronic evidence. One key issue raised was the marking of electronic evidence, particularly Compact disks (CDs), as exhibits in court. It was argued that marking a CD as an exhibit without verifying its content can lead to potential issues, as the content may not align with expectations. This is especially significant when the content includes multimedia elements, such as videos or images, as opposed to written documents. Participants in the session challenged this practice, highlighting the potential pitfalls of marking an electronic document as an exhibit without verifying its content. Practical issues like difficulties in playing the electronic content and discrepancies between the stated content and the actual content were also reflected upon.