NATIONAL JUDICIAL ACADEMY, INDIA

National Workshop for High Court Justices on Cyber Laws [P-1352]

12th & 13th August 2023

PROGRAMME REPORT

PROGRAMME COORDINATOR: SUMIT BHATTACHARYA & PRASIDH RAJ SINGH, FACULTY,

NATIONAL JUDICIAL ACADEMY, BHOPAL

Session 1: Regulating the Cyber Space: National and International Jurisprudence - The session initiated by discerning law from the substratum on which it applies, especially in the case of cyber space and operation of internet. It is important to consider and examine them distinctly because of the fundamental change of application of law to a new set of environment which is digital, beyond the conception of physical boundaries, its characteristics of being all pervasive, and its potential to impact specifically and generally. The potential loss of privacy owing to voluntary sharing of one's data (either out of compulsion, ignorance or avarice) was discussed. The regular and carefree susceptibility of personal data by casually entering into an e-contract by 'click wrapping' and 'browse wrap' was cited. The massive relinquishment of personal data to large corporations having deep and pervasive digital presence, vis a vis sense of insecurity to share private data with government agencies were contemplated in the light of potential vulnerabilities including deep-fakes. Interestingly it was stated that compelling a corporate to protect private data through ethics or regulations is a farfetched idea. It is secondary to the fact that the sheer nature of outreach of internet and its deep pervasive character, disables it so much so, that it makes it near impossible even for the corporate houses (viz. Twitter) to locate the exact location of the datum in the first place, what to speak of its protection. The other extreme of the position is that, too much access is available on too many systems, and to too many employees, making it nearly impossible for the corporation to monitor illegal or unsolicited access within its ecosystem by its own employees. Thus, rendering privacy at an unguarded risk. Discussing the major principles of data protection law, a few principles which are fundamental were underscored. These include "collection limitation"; "data quality"; "purpose specification"; "use limitation"; and "security for data preservation" principles. The importance of 'consent' and role and liabilities of a 'data fiduciary' was discussed in the light of the proposed Digital Personal Data Protection statute of 2022. The role of authority like 'Data Protection Board of India', and 'Data Protection Officer' to adjudicate disputes between 'Data Principal' and 'Data Fiduciary' was briefly touched upon. The scope of rights and duties of the 'principle' and the 'data fiduciary' were briefly accounted for. The objective of the legislation was simplified and narrated as a balancing act of protecting the individual rights to personal data of the data principle (in a digital world) and its consensual access, use etc. for legitimate purposes by a data fiduciary. The necessity of a 'warrant' to enable access to personal data was contemplated, wherein the difficulties of service of such warrant, circumvention of such warrant, and apparent conflict of fundamental right against self-

incrimination was examined. The role of international law (especially in terms of State liability) in cases of cybercrimes owing to its characteristics of posing jurisdictional challenges to a typical national law was examined. It was emphasized that State responsibility is an established position of law as founded in the United Kingdom v Albania (Corfu Channel Case) (1949) ICJ Rep 244, ICGJ 201 (ICJ 1949), and White Industries Australia Ltd. v. Coal India Ltd. (India –Australia BIT Award Case), IIC 529 (2011). The principles of 'subjective' and 'objective' territoriality was clarified while discussing the issues relating to jurisdiction fixation in cybercrime cases.

Session 2: Jurisdictional Issues in Adjudication of Cybercrimes - The session unfolded with dispelling certain pre-conceived notions relating to the popular terminologies *viz*. 'cyber', 'cyberspace', 'cyber-issues', and 'cybercrimes'. It was clarified that all cyber related issues are not to be construed as cybercrimes. Cybercrimes are only criminal offences committed in cyber space. Whereas, there are other civil wrongs and misconducts which occupies the cyberspace. Yet another oft mistaken presumption is that cybercrimes or cyber issues are essentially and necessarily international in nature. Whereas, cyberspace by its virtue being boundary-free can be intra-national. Therefore, territoriality does not necessarily has to imply international. However, when we refer to 'extra territoriality' of an offence as codified under penal provision, refers to international offences. The session delved into the issues relating to the determination of jurisdiction by a court in India for an offence which is either committed by an Indian citizen or a foreign national in India or outside India. The contours of extra-territorial jurisdiction provisioned under atleast the three major statutes i.e. Indian Penal code, 1860 (IPC); Information Technology Act, 2000 (ITA); and Criminal Procedure Act, 1973 (CrPC) were examined with various permutations and combinations. While it was asserted that in cases of cybercrimes the enabling provision under Section 4(3) of IPC provides for extra-territorial jurisdiction to the Indian courts to try, it is Section(s) 1(2) and 75 of the ITA which synergizes the scope and compensates for the interstices. The pertinent provision for trying the aforementioned issues were explained in the light of Section 188 of CrPC. Role, scope and application of "Letters Rogatory" and Mutual Legal Assistance Treaty (MLAT) was discussed. Explaining Regarding investigation of a cybercrime wherein a foreign State is involved, and there is a necessity to investigate and collect evidences from the foreign soil (especially in the event of the fact that, the police or the concerned authority of such foreign State denying cooperation) the Court can under Section(s) 105K and 166A, and reciprocally respond back to a request from a foreign Court or authority under Section(s) 105K

and 166B of CrPC. A brief account of rise in cybercrime in India was projected. It recorded as 5693 in 2013 and had swollen to 50,035 cases by 2020, a darting kilo quantum jump. Only to account for reported cybercrimes, steadily discounting the massive fraction of those which remain unreported. The explosive matrix depicted the pervasive outreach of the crime indicative of the massive adjudicatory quantum in its imperative making. One of the most troubling issues in adjudicating cybercrimes is determination of Parties. Due to the pervasive, indeterminate, multi-locative and transient nature, it becomes extremely difficult to pin down accurately who is/are accused, accomplice(s), and the intermediaries responsible and liable, or to personify victim(s) etc. Yet another difficulty is determination of 'place of commission' and/or 'place of suing' (i.e. jurisdiction). For ease of understanding the case of 'dark-net' was considered. In fact, the situation could be equated with a time when there is 'no law' or a jurisprudential green field with scarce precedence, and a relatively undetermined ballpark for interpretation. The positive of the takeaway would be a great opportunity for original thinking, to pave the path for novel and dynamic jurisprudence. For a court to exercise its jurisdiction the principle of 'localisation' was discoursed. It enables the courts to have jurisdiction akin to the question of having a deeming fiction. The tests propounded by the US jurisprudence includes 'minimum contacts' test; the 'purposeful availment' test; the *Zippo* 'sliding scale' test and the 'effects' tests. A brief comparative between Section 20 CPC and Clause 12 Letters Patent was done. Clause 12 of the Chartered High Courts relating to leave to sue was discussed. Under this Clause of the Letters of Patent, it was held to confer jurisdiction upon the Court, with regard to suits other than suits for land, in the first instance in relation to the cause of action, which jurisdiction is not exercised "in personam", because even though the defendant may not be within its jurisdiction, the Court can exercise its jurisdiction in relation to the subject-matter of the suit.

Session 3: Examining Other Potential Adjudicatory Challenges - The session flagged-off with the briefly revisiting the genesis of the notion of 'Right to be Forgotten' RTBF. The discourse traced the milestones pegged by the said concept to traverse from a notion to be considered as a legal right , to subsequently attaining the status of being recognised as a Constitutional Right, ultimately culminating to be raised to the level of being recognized as a (derived) Fundamental Right . Simply explained RTBF can be traced from the French term le droit à l'oubli which was recognized by the French courts in 1965, in a conventional non-digital context. It implied to forget the past and live in the present preserving the individuals' dignity. *Google Spain v. AEPD*,

ECLI:EU:C:2014:317, Case No. C-131/12 was referred to be one of the pioneering case on the concept in the internet age. Although the CJEU decided in favour of the individual against Google, but the decision was based on the Data Protection Directives 95/46. After the advent of GDPR, 2016 there are specific provision regarding Right to Erasure, RTBF *viz*. Article 16, & 17. While dealing with RTBF it was narrated that in an 'open court' system RTBF firstly cannot operate while a lis is live. One cannot demand a live-streaming to be stopped under his/her privacy accounts as it hits transparency. However, if a person has already being absolved, the absence of any legislation the court needs to adjudicate on the balance between public interest versus private interest. It was underscored that the court has to decide on case-to-case basis. The recent statute on Data Protection Act, 2022 does not addresses RTBF. Next the concept of Non Fungible Tokens (NFT) was explained and its role was discussed. NFT like DLT issues a unique ownership to the property (including IPR). It is a secured system for transaction. A non-fungible token is a unique digital identifier that is recorded on a blockchain, and is used to certify ownership and authenticity. It cannot be copied, substituted, or subdivided. The ownership of an NFT is recorded in the 'Blockchain' and can be transferred by the owner, allowing NFTs to be sold and traded but not divisible or multipliable. An overview of the Digital Personal Data Protection Act, 2023 was given. An analysis between "data fiduciary" and "data principal" was done. A detailed discussion on "Global Injunctions & worldwide interlocutory injunctions" formed part of the discourse. Case law jurisprudence discussed included, *Google Inc. Appellant v. Equustek Solutions Inc*. Supreme Court, District British Columbia, [2017] 1 S.C.R. 824; *Swami Ramdev v. Facebook*, CS(OS) No. 27/2019, decision dated October 23rd, 2019; Eva *Glawischnig-Piesczek v. Facebook Ireland Limited*, Case C-18/18, 3 October 2019.

Session 4: Admissibility & Appreciation of Digital Evidence - The session commenced by highlighting the relevant provisions of the Indian Evidence Act, 1872, and the Information Technology Act, 2000, which plays a pivotal role in defining electronic records and establishing their status as admissible evidence. It was pointed out that Sec. 3 of the Indian Evidence Act is an instrumental in this regard, as it explicitly defines "evidence" to encompass all documents, including electronic records. It was stated that this broad definition sets the stage for recognizing electronic records as a distinct category within the evidentiary framework. Subsequently, a reference was made to Section 2(t) of the Information Technology Act, 2000, which provides a specific definition of "electronic record." It characterizes electronic records as data, records, or

data generated, images, or sounds stored, received, or sent in an electronic form or in microfilm or computer-generated microfiche. It was emphasized that this definition within the IT Act serves as a complementary source for understanding the nature of electronic records and the contexts in which they exist.

A reference was made to the case of *State of Bihar v. Radha Krishna Singh*, AIR 1983 SC 684 wherein it was held that admissibility of a document is one thing and its probative value is another and these two aspects cannot be combined. It was opined that a document may be admissible, and yet may not carry any conviction and weight or its probative value may be nil. With regard to relevancy of electronic record various cases were relied upon *viz. Kundan Singh v. The State* 2015 SCC OnLine Del 13647; *Dhruben Guraldas Balani v. State of Gujarat* 2022 GLH 1 680; *Shyam Sunder Prasad v. Central Bureau of Investigation* 2023 (122) ACC 851; *Saidai Sa. Duraisamy v. Stalin M.K and Ors*. 2016-5-LW448

The contours of Sec. 65-B of the Evidence Act were explored, with a reference to the case of *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* 2020 7 SCC 1. It was emphasized that electronic records, when used as documentary evidence under the Indian Evidence Act, must adhere to specific procedures. It was underlined that the presentation of electronic records as evidence follows the process outlined in Sec(s) 65A and 65B of the Evidence Act, providing for both technical and non-technical conditions and the method for presenting electronic records as admissible evidence. These conditions extend to both the nature of the information and the integrity of the computer system involved. If these conditions are met, the computer-generated output, be it printed or stored, becomes eligible for introduction as evidence in a court of law. It was emphasized that adherence to the conditions outlined in Sec. 65-B of the Evidence Act is essential to ensure the admissibility of electronic records in court proceedings, and participants were encouraged to stay updated with evolving legal interpretations and precedents in this area.

The discussion shed light on the pivotal questions, specifically, whether Sec. 65A and 65B of the Evidence Act constitute a comprehensive code or not. It also delved into the circumstances under which a certificate under Sec. 65B (4) can be waived and the trial stage at which a party can furnish the certificate. In this context it was underscored that the certificate under Sec. 65B (4) is a prerequisite for the admissibility of electronic record evidence and Oral evidence cannot replace the certificate, as Section 65B (4) is a mandatory requirement. It was emphasized that certificate

under sub-section (4) of Sec. 65B is not required if the original document itself is presented. With regard to the stage of production of the certificate it was highlighted that Sec. 65B does not specify the exact stage at which the certificate must be furnished to the court. So long as the hearing in the trial is not yet over, the certificate can be directed to be produced by the judge at any stage

During the course of discussion various cases were referred and deliberated upon including, State (NCT of Delhi) v. *Navjot Sandhu @ Afsan Guru* AIR 2005 SC 3820; *Anvar P.V. v. P.K. Basheer* (2014) 10 SCC 473, *Tomaso Bruno v. State of U.P.* [(2015) 7 SCC 178]; *Shafhi Mohammad v. State of Himachal Pradesh* (2018) 2 SCC 801; *State of Maharastra v. Praful B. Desai JT* (2003) 3 SC 382; *U.S. v. Hassan*, 742 F.3d 104 (4th Cir. 2014); and *Harpal Singh and Ors. v. State of Punjab*, (2017) 1 SCC 734

Session 5: Safeguarding Judicial Institutions from Cyber Attacks - The session commenced by discussing the emergence of the concept of "cyber" in the late 1980s and early 1990s, propelled by a cultural fascination with technology and computers. It was highlighted that this period marked the mainstream recognition of the term as technology and computers began to dominate popular culture. The discussion explored the elements that characterize the cyber realm, focusing on the culture of computers, information technology, and virtual reality.

Various types of cyber-attacks were delineated, including malware attacks, phishing and social engineering, denial of service (DoS) and distributed denial of service (DDoS) attacks, man-in-the-middle (MitM) attacks, SQL injections, insider threats, advanced persistent threats (APTs), cryptojacking, and ransomware attacks. The comprehensive list emphasized the multifaceted nature of cyber threats. The discussion referred a range of cyber-attacks on courts globally, citing instances in various countries such as Georgia, Ukraine, European Court of Human Rights, Montenegro, and Argentina. These examples served to underscore the potential risks posed to the international judicial institutions.

Subsequently, it was underscored that a comprehensive judicial digital data management policy should incorporate key figures such as implementation officers, compliance officers, grievance redressal officers, and a committee. It was opined that such policy should serve as the cornerstone for safeguarding the security and integrity of judicial digital repositories. The importance of regular cybersecurity audits was stressed, as they are imperative for the proactive identification of vulnerabilities, security risks, and other potential issues within the judiciary. The role of the

compliance officer was highlighted as pivotal in conducting these audits and provide findings and recommendations. It was suggested that the audit report & findings should be expeditiously disseminated to the grievance redressal officer and the implementation officer.

It was suggested that a more advanced security system should be implemented to prevent data breaches in the court. Participants were advised to adopt strong and unique passwords, employ multi-factor authentication, utilize trustworthy security software, and maintain a regular monitoring and audit. Moreover, the importance of encrypting all electronic communications and data exchanged within the court system using robust encryption protocols were highlighted. This encompassed emails, documents, and other forms of communication. It was recommended that a secure document management system, ensuring the confidentiality and integrity of court documents, be adopted.

The discussion underscored the necessity for comprehensive cybersecurity training for judges, lawyers, court staff, and other court personnel. It was highlighted that such training is vital for keeping them informed about the various facets of cyber threats, including social engineering tactics and best cybersecurity practices. The session emphasized the imperative of bolstering cybersecurity measures within the judicial system to protect sensitive data, preserve the integrity of court operations, and defend against the evolving landscape of cyber threats. Lastly, the need for tailored incident response plans for courts, outlining the necessary steps to be taken in case of a cybersecurity incident were suggested.