NATIONAL JUDICIAL ACADEMY

P-1273

NATIONAL WORKSHOP FOR HIGH COURT JUSTICES

DECEMBER 11 & 12, 2021

Programme Report

PROGRAMME CO-ORDINATORS

Paiker Nasir & Krishna Sisodia

Faculty, NJA

The National Judicial Academy organised a two day online Workshop for High Court Justices on cybercrime and electronic evidence on 11th and 12th December, 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, emerging threats and exploring 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.

DAY-1

Session 1

Cyber Crimes: Role of Judiciary

- *Evolving Concerns & Challenges: National & International Perspective*
- *Use of social media in connection with offences related to national integrity and sedition*
- *Liability of intermediaries*

Speakers: ***Dr. Harold D'Costa & Mr. Rushi Mehta***
Chair: ***Justice A. K. Menon***

The session commenced by providing an overview of the *modus operandi* of different types of cybercrimes viz., online financial frauds, sextortion, online harassment, cyber stalking, cyber loan sharking, hacking, ransomware, data theft, website defacement, spying mobile devices etc. It was iterated that a typical organised cybercrime involves encrypted phones, hi-tech payment gateways, intentlinks, neobanks, rented companies, rented/fake accounts, fake KYC simcards, VPN, darkweb, cryptocurrency, advertisement platforms and server hosting on fake companies. It was pointed that broadly, cyber criminals in India are either professional with deep tech expertise (hackers) or they are illiterate with social engineering skills (Jamtara).

Further, the session dealt with certain investigation techniques by providing live demonstration of WhatsApp chat modification, SMS 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. 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.

Session 2

Appreciation of Electronic Evidence

- *Relevancy, authenticity and admissibility of electronic records*
- *Digital Forensics vis-à-vis acquisition, authentication, analysis and documentation of data*
- *Contours of Section 65-B in light of Arjun Panditrao Khotkar vs Kailash Kushanrao Gorantyal*
- *Challenges relating to extraterritorial evidence*

Speakers: ***Justice Sanjeev Sachdeva & Dr. Debasis Nayak***
Chair: ***Justice Kurian Joseph***

The session initiated by defining electronic evidence as any probe in information started or transmitted in electronic devices. It was pointed that everything a person does on the internet leaves a trace on the computer which can be found in internal devices, external devices or on digital platform. It was suggested that whenever anyone uses a device, it leaves a footprint, known as 'digital footprint'. It was asserted that digital evidence is impossible to delete, however, easy to modify and duplicate. No data can ever be deleted even if it is deleted from the system. The deleted data remains as the metadata and can be retrieved with the help of advanced softwares. 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 Indian Evidence Act (IEA). Thereafter, *P. Gopalkrishnan v. State of Kerala and Anr., (2020) 9 SCC 161, State by Karnataka Lokayukta, Police Station, Bengaluru v. M.R. Hiremath, (2019) 7 SCC 515, Shamsher Singh Verma v. State of Haryana, (2016) 15 SCC 485, Gajraj v. State (NCT of Delhi), (2011) 10 SCC 675* were cited tracing the vitality of electronic evidence.

Further, while dealing with the interpretation of Section 65B of the Evidence Act, *Anvar P.V. v. P.K. Basheer (2014) 10 SCC 473* was referred. It was pointed that post the decision in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020) 7 SCC 1* 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. Thereafter, intermediary liability as contemplated in Section 79 of the Information Technology Act was discussed in light of *Shreya Singhal vs. Union of India (2015) 5 SCC 1*, wherein it was held that if an intermediary fails to expeditiously remove or disable access to explicit materials on knowledge of the court order or on being notified by the appropriate government or its agency will be held liable.

Further, 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.

DAY- 2

Session 3

Territoriality and Jurisdictional Issues in Cyber Crimes

- *Statutory Framework*
- *Cyber Jurisdiction- National, Transnational or International*
- *Tests to determine jurisdiction*
- *Extradition – Mechanisms for international co-operation*

Speakers: *Prof. Ellen S. Podgor & Mr. Sajan Poovayya*
Chair: *Justice G.S. Patel*

The session commenced by accentuating that essentially everything that we do in cyberspace retreats the traditional geographical precincts. It is substantial to comprehend that almost everything is trans-border in cyberspace and the most critical issue that arises thereof is jurisdiction. While discussing general principles of extraterritoriality it was stressed that jurisdiction is to be considered by three diverse constituents i.e., *jurisdiction to prescribe* which refers to legislations, *jurisdiction to adjudicate* means the person should be physically present else (s) he could not be adjudicated and *jurisdiction to enforce* that denotes prosecutors, investigative agencies, judiciaries who have the ability to enforce and lead the adjudication. While discussing the national approach of the United States in dealing with extraterritorial jurisdiction it was highlighted that cybercrimes can be seen in three different echelons i.e., statutes focused on international conduct, statutes with extraterritorial provisions and judicial interpretation.

The international principles with respect to territoriality as applied in the US were elaborated viz. *territorial principles,* these are applicable to acts committed within the domestic territory of a country. On the other hand, objective territoriality takes it beyond this territorial principle and it focuses on whether or not the conduct affects the country. In cases of drug trafficking, money laundering etc. objective territoriality principle is applied. The other principle is of *active* *personality* i.e., essentially whether the perpetrator of the crime is the national of the US or not. Another principle is of *passive personality* which refers to the nationality of the victim. An additional expanding principle is the *protective principle* which is based on the idea of protecting the country. The last principle is of *universality or human rights*. It was stressed that these principles are referred by courts when the legislation is not clear whether it has extraterritorial application or in situations when the judges are dealing with an older statute. The US Supreme Court jurisprudence with respect to extraterritoriality in the light of *Morrison v. National Australia Bank LTD* 561 U.S. 247 (2010), *Kiobel v. Royal Dutch Petroleum Co.* 569 U.S. 108 (*2013*) and *RJR Nabisco v. European Union* 579 U.S.__ (2016) was briefly discussed.

Subsequently, considerations that are crucial while determining cybercrime jurisdiction were expounded as follows:

- ✓ Meaning of cybercrime and whether it is a national, transnational, or international problem?
- ✓ Is there a need to examine cybercrime from the perspective of the core criminality, like-theft or pornography, or else it is a crime that entails exclusive examination?
- ✓ Should the crime determine whether the remedy should be one in the national, transnational, or international realm?
- ✓ How to deal with procedural issues that accompany cybercrime (e.g., what are the constitutional rights afforded to individuals storing materials on computers)?
- ✓ Who should prosecute the cybercrime, the country where the keystroke occurs, the country where the harm occurs, or the country through which the computer signal passes?
- ✓ When more than one jurisdiction can prosecute a computer crime, who should have priority?
- ✓ Should we treat perpetrators the same: such as juveniles who use their computers to infiltrate a security concern, adults who commit a crime for financial gain, and governments that act for political reasons?

While discussing territoriality and jurisdiction in the Indian context the focus was laid on the perspective of cyber conflicts committed within the territory of India, how they are dealt with and in what manner international manifestation of these conflicts are handled. Examples were cited with regard to defamation cases, financial frauds, data theft etc. To understand the granularity while looking into the jurisdictional aspect it was stressed that when it comes to identity theft and data theft to comprehend the abrasiveness of the jurisdiction aspects becomes difficult. Although India has a unified judiciary, criminal legislations are common that apply across the country, prosecution and investigation is local but still the question of which court will have the jurisdiction keeps coming up. It was stressed that in India, with respect to criminal jurisprudence in cybercrimes, acquittals are based on technical reasons due to the lack of sufficient evidences and it is high time that we come up with techniques and processes to handle this issue. Various hypothetical instances were floated to brainstorm jurisdictional aspects in cybercrimes. It was underscored that our legislative actions needs to be in pace with the contemporary needs since they are far behind when it comes to data protection legislations.

Session 4

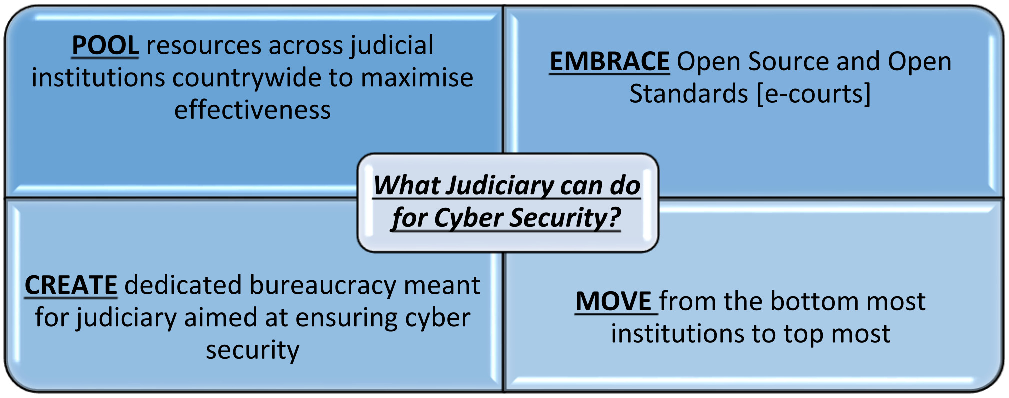
Safeguarding Judicial Institutions from Cyber-attacks

- *Cybersecurity and data protection*
- *Cybersecurity in courts*
- *Liability of internet service providers*
- *Strategies to prevent & respond to cyber-attacks*

Speakers: ***Mr. Pierluigi Perri & Mr. Anand Venkatnarayanan***
Chair: ***Justice A. Muhamed Mustaque***

The last session emphasised that the judiciary is a goldmine of data and hence, it is certain to be attacked. It was underscored that in the past few years there has been a rise in cyber-attacks on the judiciaries across the globe especially in Europe and United States. In US alone around 24 million cyber-attacks have been attempted in 2019 as compared to 9 million such attempts in 2016. Prominent reasons for susceptibility of judicial institutions to cyber-attacks as highlighted during the discussion are- network security is usually overlooked; weak links with unguarded entry points especially in large networks may provide unfettered access to all the connected systems; not updated individual systems tend to be non-supportive of the running operating systems; non-involvement of personnel working with judiciaries who are not continuously skilled in best practices involved for keeping the systems safe; and most importantly, a single cyber-attack may give access to a substantial amount of crucial data. Later rules on live-streaming and recording of court proceedings were briefly discussed. Subsequently, approach of the Europeans Union [*hereinafter EU*] on the protection of personal data, security measures that can be used in cyber security were highlighted. It was accentuated that the EU has developed a holistic approach to cybersecurity that includes security of systems and data by taking into consideration all components of an information viz. hardware, software and human ware. In order to keep the system secure adequate technological and organizational measures are adopted for every component. Various enactments, regulation and directives to regulate complexities involved in cybersecurity as developed by the EU were also discussed.

Consequently, reasons why cyber security fails were highlighted. The first reason being the jinx of unpredictability in cyber security because things have become convoluted and due to which it impossible to recognise the ends and secondly, the offense of cyber breach although is technical in nature but the defense is political which implies exactly how organizations are structured. It was stressed that cyber defense is fundamentally driven by budgets, bureaucracy, organizational structures, standard operating procedures, people, processes etc. While discussing ways to defend institutions from cyber-attacks it was emphasised that first and foremost it is significant to- reduce complexities; allocate sufficient budgets; have rapid reaction forces and to have an agile bureaucracy. Uniquely Indian issues associated to cyber security as identified during the discussion are – budget allocations, no deep understanding of privacy and lack of cyber security being a culture. All these reasons make it hard to institutionalize cyber security. Therefore, it was highlighted that the role of the judiciary in such a scenario becomes all the more significant. It was suggested that the judiciary can- pool up the resources across the judicial institutions countrywide to maximise effectiveness; embrace open source and open standards since this will allow us to at least ensure that the components are minimal and can help in watching what the vulnerabilities are; move from the bottom most institution to upwards because attacks occurs on the fringe and then the hackers learn how the fringe operates and thereafter these attackers move up on the chain and finally, to it is important to ensure that there is a creation of a dedicated bureaucracy to the extent the available budgets allow which is meant for judiciary aimed at cyber security.



What Judiciary can do for Cyber Security?

POOL resources across judicial institutions countrywide to maximise effectiveness

EMBRACE Open Source and Open Standards [e-courts]

CREATE dedicated bureaucracy meant for judiciary aimed at ensuring cyber security

MOVE from the bottom most institutions to top most

The session further emphasised that the Indian judiciary needs a secured e-corridor that will have solutions to the problems that are ever increasing in an era where judicial governance is concerned with almost every facet of life whether it is criminal, commercial, transnational and personal life of an individual.