SE-08: Workshop on Cybercrime for High Court Judges and Principal District Judges [In collaboration with CEELI Institute, Prague and Federal Judicial Center (FJC), Washington], November 12-15, 2021

VIRTUAL – FACILITATED FROM THE CEELI INSTITUTE

Report prepared by: Prasidh Raj Singh & Nitika Jain, Law Associates, Faculty, NJA

The National Judicial Academy (NJA), India concluded a workshop in collaboration with the Central and East European Law Initiative (CEELI Institute), Prague, and the United States Federal Judicial Center (FJC) in Washington, DC to promote exchanges between U.S. judges, subject experts, and Indian Judges on areas relating to the adjudication of Cybercrime cases and cases involving issues relating to cyber security. The workshop was facilitated virtually through CEELI Institute. The workshop had mixed participation of High Court Justices and judicial officers from District Courts of India. A total of 30 participants including 16 High Court Justices and 14 Principal District & Sessions Judges were nominated from different jurisdictions, out of which 29 judges attended the workshop (*Annexure-I*). The workshop included 9 sessions spread across four days which were summarized in the last session by Mira Gur Arie, Director, International Judicial Relations Office, FJC; Claire Smearman, Senior Judicial Education Attorney, Judicial and Legal Education, FJC and; Justice A.P. Sahi, Director, NJA. Details of the deliberations in each session are briefed in this report.

Artificial Intelligence as Evidence (Pre-recorded Session)

Speaker: Hon. Paul Grimm, Judge, U.S. District Court for the District of Maryland; & Dr. Maura Grossman (J.D., Ph.D.), David R. Cheriton School of Computer Science, University of Waterloo, Ontario, Canada

The session was a pre-recorded session that focussed on the relevance of AI in an ever-changing landscape of litigation and modern forms of evidence for lawyers and judges. The areas covered during the session included fundamentals of AI, encompassing how AI works, how it is being used in the legal industry and elsewhere, and some of the issues AI implicates. The session also addresses issues pertaining to the admissibility of evidence introduced through AI and machines. A descriptive analysis of the pertinent rules of evidence that may or may not apply in the case of AI evidence also formed part of the session.

Friday, November 12, 2021

Overview of Cybercrimes & Cyber-Enabled Crimes – Admissibility of Digital Evidence: An Overview of Practice in the United States

Speaker: Hon. Paul Grimm, Judge, U.S. District Court for the District of Maryland

The session covered a deliberation on evidentiary concepts under the United States Federal Rules of Evidence and evidentiary principles that govern electronic evidence from a global experience. The session commenced by the speaker highlighting that the greatest challenge regarding the admissibility of electronic evidence in cybercrime cases is requiring party introducing the electronic evidence to authenticity it; that whether the evidence that was collected from the accused in the course of investigation has remained untainted and has not been manipulated till the time it is placed before the court for assessment. It was highlighted that digital evidence is everywhere including cell phone records, location data, forensic images of digital devices, text messages, emails & tweets, social media

& websites, photos, audio, and video, etc. It was pointed out that in the coming times Artificial intelligence will also be a form & source of electronic evidence.

The speaker highlighted Preliminary consideration in the US rules of evidence under following provisions:

- Rule 104(a) - court decides preliminary questions re: admissibility, qualification of experts, and, existence of privilege
- Rule 104(b) – Conditional Relevance: when relevance of evidence depends on existence of fact, it is admissible subject to/conditionally upon proof of that fact.

It was highlighted that the rules of evidence in the US are also predicated on the assumption that the default fact finder in a criminal case will be jury and the overwhelming majority of the cases while it is not unusual to have criminal cases tried before a single judge in case of a misdemeanor for felonies. As a result, the rules of evidence impose a great deal of protections and charge a trial judge with making preliminary determinations to ensure that the information that is allowed to be considered by the jury who will decide the facts of the case is authentic and not irrelevant to the issues and not excessively prejudicial. It was also pointed out that in the US judges are not specialty judges but are general judges who have to be familiar with technical evidence whether dealing with medical issues or issues involving science or technology.

The session focussed on the relevancy of evidence wherein Rule 104(b) on conditional relevance was deliberated upon. Particularly functional in the jury system. In order to prove the evidence is relevant, there is a need to establish a disputed fact. It was highlighted that in the US legal system in most cases a judge will make the gatekeeping decision about whether evidence is admissible in both judge and trial before a jury. Further, the session included a presentation on various aspects of what is 'relevant' viz. whether evidence has any tendency to prove a fact of consequence to litigation and should not be confused with the weight /credibility of evidence [Rule 104 (e)]; Authenticity [Rule 901(a)] as a key issue and how it is to be proved; and, Excessively prejudicial rule [Rule 403].

It was highlighted that in the US legal system there are 24-25 different examples of how evidence can be authenticated which are non-exclusive and are only illustrative [provided under Rules 901(b)(1), 901(b)(3), 901(b)(4), 901(b)(9)]. The rules providing for self-authentication under the US Federal Rules of Evidence were also elucidated upon [provided under 901(1)- (4): domestic/foreign public records; 902(5): official publications (need not be testified); 902(6): newspaper, magazine (the editor of the newspaper can authenticate); 902(7): trade inscription (uniquely identifiable with that source is self-authenticating); 902(11)-(12): certified copies of domestic/foreign business record and; 902(13): certified records generated by electronic process producing reliable results; 902(14): certified data copied from electronic device, file, storage medium, etc.]. Some ways of certification under the US legal system were pointed out under the above-mentioned rules. The original writing rule/ or the concept of best evidence rule as provided under Rules 1001-1008 of the US legal system were also emphasized upon. It was pointed out that in case no original/duplicate evidence is available then secondary evidence is allowed and that in the US if the evidence is voluminous then a summary of evidence can be provided as per Rule 1006. It was emphasized that like in India the US also has the rule of presumption of innocence i.e. 'to establish guilt beyond reasonable doubt'.

Cyber technologies: A Primer – Digital Investigative Analysis

Speaker: Ovie Carroll, Director, U.S. Dept. of Justice Computer Crime and Intellectual Property Section Cybercrime Lab

The speaker commenced the deliberation while identifying the three major types of cyber-attacks starting from phishing, malware, and distributed denial-of-service (DDoS). It was highlighted that the rapid growth of invention and the availability of information is unprecedented as compared to any time in the past. It was underlined that children consumed more information as compared to their parents since the flow and accessibility of information is remarkably tranquil. It was emphasized that the future of investigation depends on the ability to quickly identify, preserve and analyze digital evidence. A reference was made to the various terminologies such as; gigabyte, terabyte, petabyte, exabyte, zettabyte, and yottabyte in connection with the creation and replication of data. The speaker identified and explained the value of digital evidence involved in the investigation phase such as; pre-search, search, post-search investigation, and trial. It was highlighted that cloud storage is the new paradigm shift from in-house memory storage to the cloud server. It was further emphasized that many social media websites along with mobile technology such as; location services and privacy sometimes often help to mitigate the possibility of convicting the innocent.

It was pointed out that investigating agencies find it difficult to preserve the electronic evidence during search and seizure and suggested that preservation of digital evidence is of paramount importance wherein search should be conducted in a way to gather all the digital and forensics artifacts without losing the credibility to appreciate before the court.

The session dwelt upon some other areas viz. the random access memory, network connection, malware, potential browser activity, FTK imager, dumplt, and pgp encrypted. It was highlighted that the hash value (of any file) will remain unchanged even though its identity and source location have been tampered with. The session lastly involved inputs on the methods and tools through which data can be recovered and restored as a part of digital investigation.

Saturday, November 13, 2021

Path of a Cyber Investigation

Speaker: Ovie Carroll, Director, U.S. Dept. of Justice Computer Crime and Intellectual Property Section Cybercrime Lab

The session commenced, while identifying the role of the forensic examiner, and emphasized that every forensic artifact is an independent witness in digital cyberspace. It was highlighted that forensic examiners do not give any type of independent opinion, their report is based on the finding and evidence collected or drawn during the forensic examination of any digital device. The concepts of *"opinion testimony", "expert witness", and "investigative mindset"* were formed part of the deliberation. A reference was made to Locard's evidence transfer principle wherein every contact leaves a trace. It is generally understood that with contact between two items, there will be an exchange. It was highlighted that forensic examiners ordinarily consider the following aspects such as; application run and action, location of the device, communication, storage of the device, browsing history, and knowledge access while examining the digital device.

The speaker further dwelt upon the phased approach methods while preparing and analyzing the digital device and application. It was highlighted that the phased approach consists of three stages;

triage, identification, and deep analysis relating to case user attribution and exculpatory data which were explained to all the participants. The session threw light upon the authenticity of an electronic record and the identification of tampered devices during the investigation. It was highlighted that the possibility to tamper with the digital device after confiscation is rare since experts create a forensic image immediately with the help of hash value and any change thereafter in the hash value will lead to derailing the authenticity of the forensic device and report based on it.

A reference was made to the metadata which provides information about one or more aspects of the data, also referred to as "*Data about Data*". It was highlighted that to check the authenticity of the metadata it is essential to assess various aspects of application activity of such device such as; compass activity i.e. number of times application used, activities conducted (dates/times when used), communication programme (bandwidth in/ out by application) and, counter forensics (user responsible). The speaker also emphasized the importance of file knowledge directory navigation, windows registry, and world wheel query on Microsoft while examining any digital device to help analyze the authenticity of the evidence.

The speaker further demonstrated the tools and techniques to gather information from the link file, which shows the time and duration of files last opened, last directory location, volume number, and volume serial number which help in collecting the digital evidence and provide genuineness and legitimacy to the forensic report. Lastly, the session included deliberation on the methods through which the information may be culled out from the hard drive and USB confiscated from the crime scene which can be used for investigation. A reference was also made to the surface web, deep web, and dark web during the course of the discussion.

Electronic Evidence and Digital forensics

Speaker: Amit Janju, Senior Managing Director, Ankura

During the session, the speaker covered the following areas of data volumes, challenges faced with regard to electronic evidence & digital forensics, data sources, professional skepticism, and case studies with real examples on the subject. The speaker gave an insight into the statistics of large volumes, velocity, and variety of data available on the internet at present and highlighted that it is difficult to calculate how much data is generated daily. It was pointed out that over the period as technology has become more accessible and more advanced due to which the challenges with technology are also increasing. When a large matter has a criminal angle or involves financial fraud or business email compromise then the source of the incident, potential suspect, source of data, kind of data, etc. are all important aspects to be looked into.

It was highlighted that with the exponential growth of electronic devices over the years, there are more and more data sources from which meaningful data can be used to gain insights into an investigation. A large amount of data poses greater challenges and requires the following areas to be addressed, such as - data source, data collection, data integrity, data processing, data privacy, and governance. It was pointed out that one of the biggest challenges with Electronic evidence is the overlay of data across geographies having different processing rules and standards making investigations complicated. It was stated that linking logs, evidence, and data sets from different sources in an automated but still forensic manner is one area where AI and machine learning can be made use of.

Fraud, data theft, and cyber-attacks were areas that were deliberated upon at length wherein it was emphasized that the source for evidence to be looked into in such matters includes various gadgets like smartwatches, handheld devices, laptops, mobile and social media websites, dark web, etc. It was stressed that the exponential growth of electronic devices over the years, has created more and more data sources from where meaningful data can be used to gain insights into an investigation. It was also mentioned that gaming apps & platforms like 'Pokemon Go' is a wealth of location-based information & create electronic records which can be useful for investigation and likewise apps like Instagram, Facebook, Twitter, etc. Some other sources which could be useful for investigation in case of cybercrimes including tracking location with the help of metadata were areas explained during the session. It was stressed that the most crucial aspect of any investigation is its data integrity, data availability, and the ability of the examiner to look beyond the obvious. In this regard, the session involved discussion on how easy it is to manipulate, tamper and destroy evidence related to any cyber or fraud investigation; and, how to identify if a WhatsApp message is modified or manipulated. Further, the speaker explained various case studies in reference to WhatsApp chat Manipulation; Email Manipulation, Business Email Compromise or payment Fraud, Ransom attack, Source code theft at a gaming company, and, the false allegation in a joint venture to highlight the practical approaches and challenges faced in such cases.

Following suggestions along with a word of caution were pointed out: that participant judges were suggested to be cautious and carefully examine the records of chat messages when a WhatsApp chat is produced as evidence. It is important to analyze the authenticity of the WhatsApp chat through its source; whether the screenshots are being produced or whether the mobile phone itself is produced; and unless a mobile phone is produced it is difficult to check the authenticity of a WhatsApp chat. With regard to Email Manipulation, some key points of discussion included analyzing the information post-acquisition to verify the integrity of email messages: checking - server metadata, message metadata (size and body), MIME boundary delimiters, and header fields is essential. Few notable instances and examples of Ransom attacks and business email compromise were highlighted. The speaker also elucidated upon how hackers operate and the difference between different types of hackers was such as white, black, and grey hat hackers. Lastly, geopolitical challenges such as data privacy and adequacy agreements also formed part of the deliberation.

Rise of Digital Currency and Related Issues

Speaker: Rayan Rubin, Senior Managing Director, Ankura (London)

The speaker initiated the discussion by highlighting the emergence of digital currency and its prodigious worldwide growth. The session threw light upon the various facets of bitcoin, which is a decentralized digital currency without central or single administration. It was emphasized that bitcoin transactions do not require any intermediaries rather it is user to user on the peer-to-peer bitcoin network. It was further underlined that transactions are verified by network nodes through cryptography and recorded in a public distributed ledger called a "Block chain". A reference was made to Ethereum, which is home to innumerable forms of digital money, global payments, and applications. The speaker dwelt upon various merits of cryptocurrency such as – high liquidity, no physical barriers of government or central authority; and demerits such as – price volatility, scalability, and lack of legal regulation.

The speaker further highlighted the advent of "smart contracts" which is a self-executing contract, where the terms of the agreement are written as lines of computer code that may automatically monitor, execute and/or enforce performance of the agreed terms. Further, the generally accepted principle of contract law was discussed to streamline the binding nature of such smart contracts.

During the course of the discussion it was highlighted that in the year 2018, the Reserve Bank of India banned financial entities dealing with cryptocurrency. A reference was made to the case of *Internet and Mobile Association of India vs. RBI*, (2020) 10 SCC 274 where the Apex court held that under the existing law, the RBI does not have the power to restrict individuals dealing with cryptocurrency. It was accentuated by the speaker that the unregulated sphere of cryptocurrency and its interconnected link with terrorism financing and Anti-national activities will remain a key concern before giving the final nod. It was emphasized that offences including crypto theft, crypto payment disputes, money laundering sanctions, market manipulation, insider trading, pump & dump scheme, and asset recovery requests will soon inundate the court with such types of complex issues involving digital currency.

During the deliberation, it was pointed out that cryptocurrency can be obtained from an exchange, where fiat currency is traded for Cryptocurrency. A reference was made to various platforms to acquire cryptocurrency or exchanges viz. Coin switch, e-Kuber, Coin DCX, Zebpay. A comparative reference was drawn and highlighted by the speaker with regard to the regulation of cryptocurrency in the United Kingdom, United States of America, and China. Multiple regulations such as; Anti Money Laundering and Countering Terrorist Financing (AML/CTF), Bank Secrecy Act (BSA) formed part of the discussion. Lastly, the speaker highlighted various crypto cybercrimes such as; Pump and Dump, Ponzi Schemes, Misappropriation of funds, Crypto thefts, Investor Fraud, Ransomware Payments, Crypto Mining, Extortion requiring Crypto payments, Money Laundering, and Exchange/Defi Hacking which requires immediate attention to encounter such digital frauds.

Sunday, November 14, 2021

Legal Framework: India

Speaker: Hon. Joymalya Bagchi, Judge, Calcutta High Court

This session focussed on Indian legislation addressing cyber-enabled crimes, including the Information Technology Act of 2000, its associated rules alongside relevant provisions of the India Penal Code. The session gave an insight into how Indian law addresses some of the challenging issues that arise in cybercrime cases, including extra-territorial jurisdiction over parties and criminal conduct and the use of expert testimony. Participant judges were given practical fact patterns on real incidents of cybercrimes & related issues including discussion on how to address the challenges they present.

Jamtara phishing incidents were mentioned to point out the growing concerns of crimes on the internet. The instances and statistics pertaining to increasing the rate of cybercrime in the country were highlighted. Some probable reasons for the increase in cybercrime reported in India were mentioned such as India being the second largest number of internet users in the world and poor knowledge/ awareness of cyber security. Participant judges discussed the number of cases reported in their court pertaining to cybercrimes wherein it emerged that in some jurisdictions more than 10 cases of cybercrimes are reported regularly.

Various types of cybercrime in India along with relevant provisions under IPC and IT Act were discussed upon at length including Hacking [Sec. 66 r/w 43 (a) of IT Act]; Cyberstalking [Sec 354D IPC]; Breach of Privacy [Sec. 66E of IT Act]; Obscenity [Sec. 292 of IPC & Sec. 67, 67A of IT Act]; Child Pornography [Sec 67A, 67B of IT Act]; Financial Frauds [(Sec 66, 66B, 66C, 66D of IT Act]; Identity Theft/ Impersonation [66B, 66C and 66D of the IT Act]; Salami Attacks [Sec 66B, 66C, 66D]; Phishing/Vishing [Sec 66B, 66C and 66D of IT Act]; Spoofing [66C and 66D of IT Act]; Skimming [Sec 66B, 66C and 66D of IT Act]; Malware [Sec 65, 66 r/w 43 (c) to (f), (i), (j) of IT Act]; IP Crimes [Copyright Act, Patents Act]; Cyber Squatting [Trademarks Act 1999]; Cyber Terrorism/Warfare [Sec 66F]; Espionage [Sec 66F of IT Act], etc. Different categories of Cybercrime with relevant provisions under the IT Act were also mentioned. It was stressed that there is an overlap with regard to the offences under the IPC, IT Act and other laws and the overriding effect of the Acts. The following judgements were cited during the discussion *Google India Pvt. Ltd. vs. Visaka Industries,* (2020) 4 SCC 162 and, *Sharat Babu Digumarti vs. Government (NCT of Delhi),* (2017) 2 SCC 18 on the issues pertaining to the liability of intermediary.

A comparison was drawn between Sec. 79 under the old Information technology Act of 2000 and the IT Act of 2008 which has got a wider definition of intermediary and has undergone a significant change. Further, a deliberation was also made on the extraterritoriality of offences under the IT Act as provided in Sec. 75 on extraterritorial jurisdiction. An emphasis was drawn upon the unique difference between a crime committed in the cyber world and a crime otherwise prosecutable is that the crime does not have a special place of occurrence. Sec. 179 of the CrPC was also referred to in this regard. It was pointed out that cybercrime is wholly based on the internet and by way of the use of data on the internet. Therefore, without proof of electronic data, the very aspect of proof of cybercrime will not be achieved. In this regard, Sec. 3 of the Indian Evidence Act and Sec. 2(t) of the IT Act were mentioned.

It was also presented that electronic evidence is unique and different from real evidence since it is intangible, mutable, and fragile and participant judges were asked to share their experiences with regard to the introduction of electronic evidence during proceedings. Further, the session involved an insight into the admissibility of electronic evidence wherein oral evidence when relevant was discussed upon. Sec. 22A, Sec. 59, Sec. 65A Sec. 68B, and, Sec. 65B(4) of the Indian Evidence Act were highlighted. Intangibility, mutability, and fragile characteristics are very important with regard to the aspects of admissibility, reliability, preservation, and probative value of electronic evidence. Admissibility with regard to the Indian Evidence Act was discussed at length with the help of various provisions under the IT Act. Nature of Certification under Sec 65B(4) with the help of a series of interpretations in important judicial pronouncements were discussed upon. Some judgement cited during the session includes *State (NCT of Delhi) vs. Navjot Sandhu* (2005) 11 SCC 600; *Anvar vs. P.K. Basheer and Ors.* (2014) 10 SCC 473; *Harpal Singh vs. State of Punjab* (2017) 1 SCC 734; *Vikram vs. State of Punjab* (2017) 8 SCC 518; *Sonu vs. State of Haryana* (2017) 8 CC 570; *Shafhi Mohammad vs. State of U.P* (2018) 1 SCC (Cri) 860; *State of Karnataka Lokayukta Police Station, Bengaluru vs. R. Hiremath,* (2019) 7 SCC 515; and, *Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal* (2020) 7 SCC.

International Cooperation: MLATs

Speaker: Hon. John Tunheim, Chief Judge, U.S. District Court for the District of Minnesota

It was highlighted that cybercrimes in present times involve multiple jurisdictions and it is difficult to investigate as there is dissimilarity in national laws coupled with the privacy policy. A reference was made to the United Nations Convention against Transnational Organized Crime and it was emphasized that the purpose is to encourage national authorities to work together to combat and prosecute transnational organized crime. It was underlined that under the convention the state parties shall afford one another the widest measure of mutual legal assistance in investigations, prosecutions, and judicial proceedings in relation to the offences covered by this Convention. It was suggested by the speaker that where the domestic or national law is unclear or in ambiguity, it is possible to take reference from international treaties since they are legally binding to the member states.

A reference was made to the mutual legal assistance treaty between USA and India, through which states seek and assist with gathering evidence for use in criminal cases. It was emphasized that there are a few challenges such as; lengthy processes, the difference in legal traditions but certainly, it is a well-organized and simplified procedure as compared to the other mode of assistance. A reference was made to dual and multilayer mutual legal assistance treaty in criminal matters which include; taking of evidence or statement, effective service of a judicial document, executing search and seizure, examining object and sites, seizure for the purpose of confiscation, and facilitating the appearance of a witness. It was emphasized by the speaker that the extradition is both treaty and non-treaty based and that countries must show the reasons for extraction such as; the seriousness of the crime, the event is a crime in both the countries and the penalty involved is proportionate to the crime. The speaker also highlighted the reasons and possibilities for refusing the extradition such as; evidence presented is not authentic, the possibility of torture in another country, no fair trial in the requesting country, and cruel or inhuman treatment.

During the course of discussion, a reference was made to the concept of "*Letter Rogatory*", which forms part of the formal request from a court in which an action is pending, to a foreign court to perform some judicial act such as; requests for taking the evidence, service of summon, subpoenas, execution of civil judgment, and other legal notice. Further, the difference in the law regarding the admissibility of witness statements, evidentiary standards, judgments in absentia, non-extradition of nationals, and dual criminality was discussed at length.

Monday, November 15, 2021

Judicial Management of Complex Criminal Cases

Speaker: Hon. John Tunheim, Chief Judge, U.S. District Court for the District of Minnesota

The session was commenced by elucidating on the complexities involved in adjudicating cyber-crime cases other than technology such as; lack of direct evidence, different location of accused and witnesses, multiple defendants, non-availability of physical evidence, jurisdictional issues, and delays in receiving the evidence. The speaker pointed out that multiple defendants makes a criminal case even more complex with more challenges coming across different issues which a judge has to decide. Another challenge highlighted was to control many more people in the courtroom and to keep the courtroom in order. It was emphasized that multiple witnesses from different countries often delay the judicial proceedings. A reference was made to *"remote testimony"* to easily accommodate the jurisdictional challenges attached with multiple witnesses. The session further dwelt upon the

credibility of witnesses, language translator, and the issue of security. During the course of deliberation, a reference was made to some of the goals and objectives of judicial case management such as; to enable fair, timely, and effective justice, reducing delay, eliminating excessive expense, and managing judicial workload. Some goals and objectives of Judicial case Management and elements of case management were highlighted such as early and consistent judicial involvement; mandatory case conferences - pre-trial; firm deadlines; classification of facts and legal issues etc. The session focussed deliberations on framing of charges in complex criminal matters which is an important stage in the trial process; that there are voluminous documents in complex matters and this is where technology can play a major role in sorting them out and keeping a record maintainable.

The session accentuated the importance of expediting trial through effective use of technology, court management, avoiding unrequired adjournments, time management, and victim and witness protection as some of the cornerstones to managing complex criminal cases. It was highlighted that court staff should be trained to facilitate case management coupled with court technology such as; electronic filing, video conferencing, software to facilitate legal research, and courtroom technologies to facilitate the trial process & presentation of evidence. The speaker further stressed the importance of courtroom security and periodic inspection. A reference was made to high-profile cases involving intense media interest and controversy which calls for a security plan inside and outside the courtroom. It was also pointed out that difficult lawyers often cause disruption in trial proceedings which causes delay and this is common in both jurisdictions as discussed.

Lastly, the participant judges were presented with a fact pattern involving various issues faced by judges in complex criminal trials. Thereafter, participants were divided into groups to review the cybercrime fact patterns and discuss some important aspects to be looked into while handling such cases. Topics such as; initial pretrial conference, digital evidence to be considered, trial by media, and, security plans were some aspects that formed part of the discussion.

Pulling it all Together

The last session was a summarization of the ten workshop sessions addressing the many varied facets of cybercrime litigation that offer an overwhelming amount of new information to process. The session included a discussion on the central ‘takeaways’ for judges and some reflection upon how to integrate new knowledge and practices while handling similar matters. Lastly, the workshop was concluded by closing remarks from the Director, NJA deliberating upon the role of judges in addressing the complexities of criminal cases, the immense leap of technology and its role in the present times along with global challenges posed, complexities revolving around the use of cryptocurrency and its legal implications, case management fixing timelines, judge’s role in enforcing production of witnesses who are infirm or not able to reach the court especially in complex crimes, and handling bar particularly in criminal cases.