**National Judicial Academy, Bhopal**


# REPORT

***Cyber Laws & Appreciation of Digital Evidence Special Program for High Court Judges (e-committee)***

**[P-1346]**

**13th May, 2023**

*Sumit Bhattacharya*

Academic Coordinator & Research Fellow
National Judicial Academy, Bhopal

**Cyber Laws & Appreciation of Digital Evidence Special Program for High Court Judges (e-committee) [P-1346]**

***13th May, 2023***

**PROGRAMME REPORT**

**Programme Coordinators –Sumit Bhattacharya Research Fellow, National Judicial Academy, Bhopal**

A single day special program for High Court judges on cyber laws and appreciation of digital evidence (in compliance to the proposal by the e-committee of the Apex Court of India) was organised at the Academy. The programme aimed to sensitise and enable the High Court Justices to the novelties and ephemeral nature of the cybercrimes. The objective was to enable a contemporary judge, by highlighting the necessity for acquiring a cross-disciplinary knowledge of law and technology. It offered a platform to explore the law and procedure to appreciate digital evidence, considering the increasing impact of such evidence in contemporary litigation. Examination of challenges posed by digitization, sometimes leading to conflicting Constitutional Rights *viz*. "freedom of expression" *vis-à-vis* "right to be forgotten" formed part of the discourse. The seminar accentuated on the need to deal with the fast mutating forms of digital evidence and issues relating to their admissibility.

The discourse was kindly guided and navigated by Justice Muhamed Mustaque (judge High Court of Kerala); Senior Advocate Mr. Sajan Poovayya; Justice Joymalya Bagchi (Judge Calcutta High Court) and; Justice Sanjeev Sachdeva (judge Delhi High Court).

The program schedule was carefully divided into three Sessions dedicated to cover three major areas delving into certain evolving areas such as:

**SESSION 1**

**Cybercrimes: Emerging Jurisprudence & Role of Courts**

***Scope of discussion:***

- ✓ Evolving jurisprudence including –
  - Digital Personal Data Protection Bill, 2022
  - New forms of Injunctions
- ✓ Conflicting Constitutional Rights –
  - Doctrine of Right to be Forgotten (RTBF) *versus* Freedom of Speech & Expression
  - RTBF (Right to Privacy) *versus* Public Rights
- ✓ Case Law jurisprudence

**SESSION 2**

**Jurisdictional Issues in Adjudication of Cybercrimes**

***Scope of discussion:***

- ✓ Determination of Parties, Place of Commission & Place of Suing

- ✓ Tests to determine jurisdiction
- ✓ Challenges relating to extraterritorial evidences

**SESSION 3**

**Admissibility & Appreciation of Digital Evidence**

***Scope of discussion:***

- ✓ Relevancy, authenticity and admissibility of electronic records
- ✓ Digital forensics; search and seizure of electronic records
- ✓ Contours of Section 65-B in light of *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*

**Session 1: Cybercrimes: Emerging Jurisprudence & Role of Courts**

The session commenced by contextualising, the interface of science, technology, cyberspace, digitization, to enhance compatibility and improve justice delivery. Resting on the conviction that technology is going to pervade and rule for forthcoming decades, it becomes incumbent upon the "new-gen" judges to keep pace and effectively deal with its impact. The key objective of the exercise includes sensitization and capacity building of the judiciary to the evolving techno-legal environment not only vertically but also horizontally (i.e. all stakeholders). It was sounded that one of the most rewarding thing owing to technology is raising the bar of efficiency. Embracing technology has consistently helped in better judicial management. Whereas one of the drawbacks is that the pace of change in technology sets in redundancy much faster. Hence, chances of crystallization of process as a dependable precedence is very low. This leads to much lower chances of reliance on processual precedence. The concepts of "cyberspace" and "cybercrime" was examined. The inevitable embracement of digital identity for societal progress brings with it, its own set of discomfort. Since, the laws of the recent past were made to address the physical space, the dimensions and orientations of the digital space with a limitless and unbound horizon has given an existential shock, rendering the extant laws otiose, redundant and resistant. Often they are square peg in a round hole. Resultant conflicts not only exposes the impotency of extant laws (suited for physical space), it flouted a new set of emerging issues i.e. conflict between Constitutional Rights. The novel issues *viz.* the "Right to Privacy" (which recently graduated as a Fundamental Right in India) appears to be susceptible to certain public rights as it militates with the "Right to Free Speech and Expression" or "Right to Information" (RTI) as it enters the paradigm of digital space. Such dynamic tempero-spatial issues demands a new prescription, an evolving area of jurisprudence which is quite ephemeral and malleable. The problems of "Right to be Forgotten" (RTBF) as against public rights *viz.* "Public Rights to Court Records" or the records of proceedings in judicial matters (especially for the Courts of Record) were chased in the debate. The claim to RTBF or RTE should not be isolated and be exclusively seen through the lenses of private rights only. Simply because it is often intertwined with public interest. It must be considered that RTBF proximately affects the records of judicial proceedings (a public law domain) wherein the "Courts of Record" (a Constitutional Creation through Aricle(s) 129 and 215) are liable to maintain, protect and reproduce such public records on a legitimate situation, to the extent of responding to a fundamental right to a citizen. The fundamental right to privacy not being an absolute right, would yield to certain other fundamental rights *viz.* public policy, and

public records, investigation of a crime etc. Therefore, once again the RTBF cannot be considered to prevail indiscriminately or be raised to an unequivocal immutable stature.

Contemplating the massive change that shall be driving the law when fused with technology, it was underscored, that today we are onto a threshold wherein courts are expected to find a legal solution to a technological problem; as against the long treaded convention of finding a technological solution to a technological problem. The transition from the all static web 1.0 to today's interactive version of web 2.0., and now progressively to web 3.0 was discussed. In web 2.0 normally we can say that the static web is now transformed to a dynamic and more interactive web. One can see that the data is centralized, *viz.* Google which is one of the biggest platform has got its huge servers located in US, which is essentially the hub of data preservation and trafficking. Importantly, the centralized data is now regulated to certain extant by municipal laws *viz.* data protection laws etc. and is governed by compliances to international norms etc. Due to which India (in a given situation) can still have a chance to request for evidence from Google through diplomatic channels (since India has an MLAT with US).

There is a potent assumption that the world is at least onto the hyper interactive (to the extent of Internet of Things (IoT)) version of web 3.0. One of the biggest evidence of transition of the world from web 2.0 to 3.0 is the transition of centralized data management from a few geopolitical locations to national level. This is the movement which is called "data-localization". India is pioneering the drive for "data localization". It would enable a court or a law enforcement agency to exercise jurisdiction on such data. One can have a Sec 91 CrPC notice served on the company owning the server, or have a court order calling for such evidence etc. Enforcement of RTBF or RTE would be much easier. Execution of injunction orders would be facilitated.

The evolving domain of "FinTech" including online financial transactions formed part of the discourse. The massive operations and pervasive transactions including the India specific and Indian pioneered Unified Payments Interface (UPI) platform, and its techno-legal aspects were examined and prognosis was attempted. The case of "Cookies" was exemplified as yet another example. India as on date do not have any regulations for cookies. However, in EU has the General Data Protection Regulation (GDPR) and the "EU Cookie Law" to regulate them. In EU therefore cookies are regulated as the "essential cookies" (permitted by law), and "non-essential cookies" (permitted by consent), generally an opt-in under EULA. It may be noted that the cookies are also a function of web 2.0.

While discussing the issues relating to jurisdiction, the meaning and scope of "national", "transnational", and "international" were discerned. The substantive statutory provisions dealing with cybercrime was traced to the Indian Penal Code, 1860 (hereinafter "IPC") and Information Technology Act, 2000 (hereinafter "IT Act"). A brief snap-shot of the provisions were shared.

| IT Act | IPC |
|---|---|
| Sec 43 - Damage to computers/ computer systems | Sec 420 - Cyber frauds |
| Sec(s) 66B – 66D – Data Theft & Hacking (contain provisions pertaining to offences ranging from identity theft to violation of privacy) | Sec 463 - Email spoofing |

| IT Act | IPC |
|---|---|
| Sec 66E - Cyberterrorism | Sec 499 - Defamation through email |
| Sec 67 – Obscenity (penalizes publishing or transmitting of obscene material in electronic form) | Sec(s) 292 – 294 - Obscenity |
| Sec 67B - Child pornography or child sexually abusive content | Sec 354D - Staking which included cyberstalking |

The various theories of jurisdiction were discussed which included "Subjective Territoriality" and "Objective Territoriality or Effects Jurisdiction". The distinction and the significance of Doctrine of Nationality" *vis-à-vis* "Doctrine of Passive Nationality or Passive Personality" w.r.t. applicability of statutory provisions was discussed.

Clarifying the jurisdictional validity and position of the "Doctrine of Protective Principle" (as reflected by a participant during the discourse), it was held not to be a preferred principle of jurisdiction, as it involves sovereignty of other nation(s). Whereas, in the "Universal Principle" it is upon any State to have a jurisdiction in a cybercrime case. The concepts were explained with the help of a few case law which included *Yahoo!, Inc. v. La Ligue Contre Le Racisme*, 433 F.3d 1199 (9th Cir. 2006); United States v. Microsoft Corp., 584 U.S. (2018), 138 S.Ct. 1186.

The discourse thereafter phased-in the aspects of extra territorial jurisdiction pertaining to cybercrimes with special focus on the extant position of the municipal laws of India. A comparative examination of Sec 4(3) IPC, Sec(s) 1(2) and 75 of the IT Act was done to understand the scope and application. It was asserted that the Sec 75 of the IT Act provides a wider scope than Sec 4(3) of IPC. A synergistic application of the corresponding provisions under CrPC *viz.* Sec(s) 179 & 182 was probed into by the participative delegation. The interoperability of the aforementioned provisions were explained w.r.t. *Ajay Agarwal v. Union of India*, 1993 AIR 1637; and *Lee Kun Hee v. State of U.P.*, 2012 (3) SCC132. The applicability of Sec 188 CrPC was delved into.

The potential for rise in the conflicting constitutional rights *viz.* RTBF a privacy domain, as against "Freedom of Speech and Expression" or "Right to Information" (RTI) a public domain provoked interesting interventions during the course of the session. *R. Rajagopal v. State of Tamil Nadu*, 1994 SCC (6) 632 was cited, wherein the apex court has laid down the test to be applied in the cases of such conflicting rights. It was held that "public records" would trump "privacy rights" (more specifically defamatory charges). The "Doctrine of Digital Immortality" in the digital age was considered as a massive challenge to be negotiated. The situation is aggravated with the advent of Artificial Intelligence (*hereinafter* AI). The algorithm which is used to train a set of data in machine learning (ML) remains as a "shadow" even after it is deleted or removed. Such digital footprints become digitally immortal. It was heralded that RTBF or "Right to Erasure" (RTE) are new solutions contemplated by the global legal systems including EU, US and India. But, these could at best serve as a panacea to the local (national level), as against the real controlling switch moving to the hands of operator(s) who are global (transnational). Hence, at best such infantile solutions would switch-off the lamp without impacting the electric supply. What is needed is how does one pulls-off the plug from the nesting generator, or stop the power supply generation. Would a *Mandamus* to RTE or a "Global Injunction" to erasure serve the purpose?

A typical hypothesis was discussed wherein a judge is faced with a case of adultery. Wherein a complainant husband charges adultery against his legally wedded wife (in his bedroom) adducing CCTV camera footage as digital evidence. The accused wife in opposition defends for her right to privacy. The discourse also delved into distinguishing between "anonymity" and "privacy". Wherein the former involves an act of masking the personal details as against the later which is much deeper and involves personal choices and fundamental rights.

The circuitous issues relating to intermediary (ISP) liability was discussed. It was asserted that the common debate while praying for an injunction before a court to take-down some contested material from the website, is faced with the defence from the ISP is based on the argument citing *Shreya Singhal v. Union of India,* AIR 2015 SC 1523 ruling that a web content has to be brought down by the ISP in compliance to a court order. Therefore, ISP can be held liable only once the courts hold them to be. Until then even for an objectionable material adversely impacting ones' reputation or equity, ISP can't be forced a take it down. The issue is so circuitous that even if the alleged content is taken down by an ISP in compliance to a court order the same would be uploaded by some other (proxy) server. The role of an "Evolving Injunction" was discussed. The problem with such an injunction is that the ISP contests that such an injunction demolishes its limited role as an intermediary. The ISPs contest that the "traffic data" is proprietary and therefore can't be shared. There are provisions and procedure prescribed for monitoring and collecting "traffic data". The session culminated with the thoughts and future challenges which will have to be dealt by Indian courts wherein:

1. Information will be "tokenized" Often NFTs
2. Information will be "decentralized" or "localized"
3. Control would be shifting to individuals from institutions
4. There is a transition from "Internet of Information" to "Internet of Things"

Therefore, in a country like India with largest numbers of smartphone uses, having exceptionally high internet and bandwidth usage, having at least three times more financial transactions processing than US it becomes imminent for India to evolve localized solutions rather than looking outwards. Therefore, it was suggested that the judges must be appraised more on the technology involved to evolve delivery of justice rather than extant law which is already fairly known to them. It will enable judges to mould the resultant justice by bridling the optimum and legal use of technology.

**Session 2: Jurisdictional Issues in Adjudication of Cybercrimes**

The session unfolded with the discussions on the theoretical and practical principles and applications of law relating to "extraterritorial jurisdiction" of a court of law, especially while it deals with "cybercrimes" and amasses "electronic evidence". The scope and nature of Section 4 of IPC, 1860 and Section 75 of the Information Technology Act, 2000 was examined. Section 179 of the CrPC was contemplated for the determination of the jurisdiction of a court w.r.t. to the aforementioned substantive offences referred under IPC and ITAct. The theories of jurisdiction and the substantive and procedural law applicable therein was discerned. It was explained that:

1. Under the theory of "subjective territoriality" i.e. if a cybercrime or cyber-attack takes place within the territorial jurisdiction of a nation (India) then Section 2 of IPC would apply.
2. However, elucidating the "Effect Doctrine" it was explained that in the event when the action takes place outside the territory of a forum State, but the primary effect/consequence of that activity is within the forum State, then it is considered as a case of "objective territoriality" and

the "effects theory" comes into play. Section 179 of CrPC therein allows an Indian court to assert jurisdiction.

3. The principle of "ubiquity" under the IPC was also contrasted with the "effects theory".

A comparative view of application of Section(s) 171 & 181 of CrPC was undertaken in the backdrop of a cybercrime, where a conspiracy is hatched in country A, using a computer resource of country B, to have an impact in country C. Section 181 deals with the place of trial, the provisions deal with an offence done by a non-Indian in a foreign land, having consequences in India. They determine jurisdiction of Indian courts to try such overlapping, consequential jurisdictions in India.

A situation wherein a foreign individual, in a foreign land, uses a computer, having a foreign network and IP (Internet Protocol) with the help of a foreign cloud server not situated in India, was examined. Wherein but for Section 179 CrPC, neither Section 4(3) of IPC nor Section 75 IT Act would apply for invoking jurisdiction on a foreign individual. This is because the wrongful loss is suffered by an Indian in effect. Section 188 CrPC was also discussed with the view that the *proviso* to the Section puts a rider that without the prior approval of the Central Government of India no trial or inquiry can be initiated under any of the provisions covered under Chapter 13 of CrPC. While explaining Section 188 an example of a foreign national who marries and Indian and thereafter subjects her to cruelty in a foreign land was discussed. The moment the foreigner husband comes back to India Section 188 will be invoked.

Another example was cited wherein Section 75 of the IT Act assumes a much wider scope than under Section 179 CrPC was discussed. A US citizen uses an Indian network to upload material to cause injury to individuals in Europe. Therefore in this case the consequence is not in India, but an Indian networking system is involved by a US citizen. In such a case the Indian Courts by virtue of Section 4(3) IPC and Section 75 IT Act will have jurisdiction. It was agreed that Section(s) 4(3) IPC, and 179 CrPC should be read with 75 of IT Act to enable widest amplitude to prosecute such a crime.

The "extra territoriality" principle is invoked on the "theory of nationality". Under this theory it was explained that Jurisdiction will be national where the domestic legislation grants jurisdiction to the courts within the country. The offence is defined as a crime in a nation, who prosecutes the crime, and who eventually punishes individuals who violate this national law.

An issue was considered when something which is considered to be a "hate speech" in India is considered to be a "free speech" in US. Under such a situation if a crime is committed by an US citizen in US (using a US server and network) but having adverse consequences in India raises red flags. In such a situation even on having an extradition treaty or MLAT US may not be willing to cooperate to comply with an order of an Indian Court. On the point of collection of evidence from foreign country in such a typical case, the court orders would fail to apply the "long arm" principle to enable collection of evidence. The example of *Microsoft Case* (*Microsoft Corp. v. United States*, known on appeal to the U.S. Supreme Court as *United States v. Microsoft Corp*., 584 U.S. ___, 138 S. Ct. 1186 (2018)) was cited which led to the enactment of the "Cloud Act" (Clarifying Lawful Overseas Use of Data Act)[1] It was asserted that it is important for India (one of the world's biggest data producers) to have a data protection

[1] The CLOUD Act amended the Stored Communications Act (SCA) of 1986 to allow federal law enforcement to compel US based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data are stored in the U.S. or on foreign soil.

legislation. The new data protection Bill, 2022 must rope-in provisions to regulate the social media intermediaries through the existing telecommunication legislations to be licensed as the other ISPs. The sensitive data must be docketed and maintained in the local servers in India. Recognition of personal and private data with the individuals it relates to and assigning ownership is imperative.

While discussing the jurisprudence of jurisdiction in cyberspace the "sliding scale test" or the "zippo test" determined in the d *Zippo Mfg. Co. v. Zippo Dot Com, Inc*., 952 F. Supp. 1119 (W.D. Pa. 1996) and the "effects test" or "calder test" determined in *Calder v. Jones*, 465 U.S. 783 (1983) were discussed. It was suggested that in the cases of cyber defamation or hate speech etc. '*Calder Test'* should be preferred over zippo. It was further asserted that in US the case law jurisprudence is consistently drifting away from *zippo* to *calder*. It was further suggested that owing to the issues of executing a court order in form of an injunction after assuming jurisdiction, it is preferable and more effective to issue an order under Section 69A of the IT Act, in form of a direction to the Government asking to block the indicated websites containing identical matters in public interest, in addition to injunctions. It was also asserted that ascertaining jurisdictions and moulding a relief under the criminal jurisprudence seems to have more clarity as against civil issues. *World Wide Wrestling Entertainment Inc. M/s Reshma Collections*, 2014 SCC OnLine Del 2031 and *Impresario Entertainment & Hospitality v. S & D Hospitality*, 2018 SCC OnLine Del 6392 were cited and compared on the point of assuming territorial jurisdiction of a court. Wherein, the later judgement distinguished the reason from the former one and held:

> [E}ven if the defendant has been able to attract customers from other jurisdiction including by way of Zomato and Dine-Out, the services of the defendant cannot be availed unless the customers go to Hyderabad. Through Zomato and Dine Out the customers will only be able to invite a customer and resume a table at the restaurant of the defendant at Hyderabad. The commercial transaction would take place only on the customer availing the services of the defendant at Hyderabad. Claim of the plaintiff is that at least one customer through the website booked the table at defendant's restaurant from Delhi believing that it was a restaurant of the plaintiff. On the basis of a solitary transaction, through internet plaintiff cannot claim that cause of action having arisen at Delhi this Court will have territorial jurisdiction to entertain the suit. Facts pleaded in the plaint do not pass the tests laid down by the Division Bench of this Court in *Banyan Tree Holding (P) Ltd. v. A. Murali Krishna Reddy*, 24 (1983) DLT 129.

On law relating to ISP liabilities it was contested that although Section 79 of the IT Act absolves the intermediaries as having hands-off owing to the fact that they do not have any active role in content selection or targeting, hence not liable, the courts have slowly started to take an opposite view, establishing the involvement of intermediaries in content selections and targeting using various tools including AI and other algorithms. The Intermediary Rules 2021, amended in 2022 (under contest pending in the Supreme Court of India) has attempted to address this innocent hands-off position taken by them under Section 79 and *quoting Shreya Singhal v. Union of India*, AIR 2015 SC 1523 for conditional compliance only on a court order. The caselaw cited was *acebook v. Delhi Legislative Assembly*, (2022) 3 SCC 529. The court went on to hold at page 606 that:

> [T]he vast and influential role of an intermediary like Facebook. In this modern technological age, it would be too simplistic for the petitioners to contend that they are merely a platform for exchange of ideas without performing any significant role themselves — especially given their manner of functioning and business model. Debate in the free world has shown the concern expressed by

Governments across the board and the necessity of greater accountability by these intermediaries which have become big business corporations with influence across borders and over millions of people. Facebook today has influence over one-third population of this planet! In India, Facebook claims to be the most popular social media with 270 million registered users. The width of such access cannot be without responsibility as these platforms have become power centres themselves, having the ability to influence vast sections of opinions. Without undermining the role performed by Facebook in giving a voice to various sections of society across the world, it has to be noted that their platform has also hosted disruptive voices replete with misinformation. These have had a direct impact on vast areas of subject-matter which ultimately affect the governance of the States. It is this role which has been persuading independent democracies to ensure that these mediums do not become tools of manipulative power structures. These platforms are by no means altruistic in character but rather employ business models that can be highly privacy intrusive and have the potential to polarise public debates. For them to say that they can sidestep this criticism is a fallacy as they are right in the centre of these debates.

Facebook as a platform is in the nature of a mass circulation media which raises concerns of editorial responsibility over the content circulated through its medium. The width of the reach of published material cannot be understated or minimised. Facebook has acknowledged in their reply that they removed 22.5 million pieces of hate speech content in the second quarter of 2020 itself, which shows that they exercise a substantial degree of control over the content that is allowed to be disseminated on its platform. To that extent, a parallel may be drawn with editorial responsibility cast on other mass circulation media.

**Session 3: Admissibility & Appreciation of Digital Evidence**

The session was strategically divided into two halves. While the first half dealt with the technical or technological aspect, the second half was devoted to the legal intricacies. To set the context it was thought prudent to prime the discussion with exposing the fact that how important for a contemporary judge it is, to know and keep abreast with the evolving technology, as they perform their judicial roles today in fair dispensation of justice. The ice was broken with inquiring if Section 65B of the IT Act a solution or even a means for achieving the results of proving a particular document. An "electronic evidence" is any probative information being transmitted or stored in digital form that can be used in a trial. What is an IP address? It was examined with examples. Any instrument which processes data and is connected to an internet network is assigned an IP address which is four sets of numbers separated by a period mark, but are unique. The IP addresses are of two types 1) internal and 2) external (used in World Wide Web). How to locate the IP address of an electronic device and treat it as an electronic address was demonstrated by exemplification. It was underscored that in digital world we are blind anything which can digitized (e.g. pictures, biometrics, texts, other physical substances etc.) is stored and transmitted by a computer in binary codes. The source of information and the method of extracting an information is of paramount importance. It enables a judge to understand, validate, authenticate and evaluate such information as a digital evidence. How to verify a digital signature for its authenticity was discussed. It was asserted that the concept of "digital immortality" has its own effects and side effects. While the data can be retrieved to enable a criminal investigation on one hand, misuse of personal data when it falls on wrong hands exhibits the darker side or disadvantage of indelible digital footprints. Deciphering of a digital file as an electronic evidence was discussed with the help of "meta data".

The importance of electronic evidence may not necessarily be limited for trial and proving of a crime, as it pervades at every stage of transaction owing to the wave of digitization of physical

documents into "electronic records" and simultaneous paradigm shift from physical to digital world in all aspects of life. Today one can say that the courts are by and large concerned with oral or electronic evidence. Documentary evidences being slowly but surely getting extinct. The nature of electronic evidence was examined. The transition and conversion renders mutability, fragility and hearsay effect to the "electronic records", making it vulnerable and ephemeral. Hence, a slightest of change in the binary data or the process (including the machine or the software involved) will change the "electronic record" rendering it highly susceptible.

The claim by the Supreme Court that Section 65A and 65B being a complete Code may need qualifications or riders. It can be called a complete Code w.r.t. admissibility of "electronic records", but not in the sense of its "probative value". A brief account of the case law jurisprudence in terms of the evolution of law from *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600, to the departure taken by the apex court to hold the mandatory nature of a 65B certificate in *Anvar P.V. v. Basheer P.K.*, (2014) 10 SCC 473 formed part of the discourse. A subsequent, spinning-off in *Shafi Mohammad v. State of Himachal Pradesh*, (2018) SCC OnLine HP 799, wherein the court held that in the event of absence of possession of original source, 65B certificate would not be mandatory.

"Electronic record" is defined as a document under Section 65B(1) of the IEA. The importance of the definition is that the documentary evidence of yesterday is now replaced by the electronic record of today. It was probed as to whether an "electronic record" is to be considered as a document or material object? Since, if the record is within a memory drive etc. it is a material object unlike a document when considered as in the form of an email.

The inconsistencies in law leading to operational confusion in admissibility of electronic evidence was highlighted by citing the contradictory positions between Section 161 and 162 of CrPC. It was asserted that whether the bar imposed under section 161 CrPC needs a reconsideration in the wake of the amendment made to Section 161 w.r.t. creation of an electronic record. Section 145 and 154 of the IEA states that the same can only be used for either contradicting or corroborating.

Yet another downside of the relevance of Section 65B certificate was discussed. It was considered to be important in the course of ordinary business to prove authenticity of an "electronic record" for admissibility. It was argued that with the exponential growth of the sources and usage of "electronic records" insistence of mandatory 65B certificate may not be a wise choice as it may not at all be relevant or sufficient. It is an archaic and fossilized legislative requirement which may be absolutely an unnecessary procedural bottleneck in the revolutionary advances in digitization across the domains. It was asserted that such a procedural road block was actually weeded out from the parent legislations of UK even prior to India's borrowing of the foreign wisdom. Referring to the Canadian legislation[2] i.e. Section 31.5[3] for standards to be observed for admissibility of an electronic document it was

[2] Canada Evidence Act, R.S.C., 1985, c. C-5

[3] Standards may be considered -

> 31.5 For the purpose of determining under any rule of law whether an electronic document is admissible, evidence may be presented in respect of any standard, procedure, usage or practice concerning the manner in which electronic documents are to be recorded or stored, having regard to the type of business, enterprise or endeavour that used, recorded or stored the electronic document and the nature and purpose of the electronic document.
> 2000, c. 5, s. 56

underscored that similar certificates would not be required, if it is proved that such electronic data is preserved and preserved, maintained appropriately by the third party no such certification would be necessary. It was asserted that the party who produces the evidence must provide metadata to establish that the authenticity and integrity of the document is preserved. A metadata extraction and production must fall in the domain of the investigating agency and should not be a judicial exercise because the same would push the court into an inquisitorial practice wherein it attempts to reach out to the evidence, thereby completely divorcing its adversarial, umpire-like role. It was reaffirmed that the role of a judge is akin to a gate keeper, just to check whether what is admitted is authentic, reliable etc. The judge has to order for an audit-trail of the electronic record with the metadata from the inception and creation of the data to support its qualifications and worthiness. It was clarified that for the purposes of examination of an electronic evidence, Section 45A of the IEA does not limits such examiner only to be a Central Government notified agent or body (in compliance to Section 79A of IT Act) but, any other private body or person found fit by the court. Similarly in the US under the provisions of the evidence legislation empowers a party to prove the evidence through other means. Hence, none of the major legal systems UK, US or Canada make certification a mandatory prerequisite for admissibility. They maintain that certification is *a* process and "may" be adopted, however it is not *the* way. Other forms of adducing electronic evidence for admissibility is not ruled out *per se.*

It was accentuated that reliability of an evidence is not exclusively dependent on admissibility. It is authenticity, and integrity, apart from relevance, which is important for relying on an evidence for its probative value of proving a fact or a relevant fact in issue. (2003) 3 SCC 123 since, electronic record is a document, if it is used to prove a fact, it is mandatory under law i.e. Section 207 read with 173 (6) of CrPC to supply such documents to the accused to enable a "fair trial". However, portions may be redacted, muted, or masked (as may be deemed necessary by the court in the interest of justice) prior to handing over such a copy. At least a gist of the documents must be given to the accused, *P. Gopalkrishnan v. State of Kerala,* (2020) 9 SCC 161 was cited in support of the same.

The conflict of rights arising out of "search and seizure" of a property *versus* privacy particularly in the case of electronic devices for electronic data was discussed. It was asserted that in the absence of any legislation in place and apex court decision the necessity of judicial oversight was is a must with an intervention under Section 94 CrPC. prior to the access and analysis of such data. The Supreme Court in *State of Bombay v. Kathi Kalu Ogadh*, (1962) 3 SCR 10 provides a guideline. The Karnataka High Court in *Virendra Khanna v. State of Karnataka,* 2021 SCC OnLine Kar 5032, held that such access under notice from authorities during the course of investigation will not implicate a commission of crime, or proves a guilt, and therefore does not militates with Article 20(3). It clarifies that a notice upon a suspect to share certain personal details may not be considered to be conflicting with Article 20(3). Reference was made to the UK legislation of The Regulation of Investigatory Powers Act 2000 (RIPA), wherein under Section 49 it provides for "notice requiring disclosure", wherein it empowers the investigating agencies upon showing probable cause and on non-availability of any other alternative means of securing access to the relevant material or data to call upon a suspect to share an encrypted key to the agency to enable investigation. The UK Court held that the electronic key, or the access code or the password is just like an ordinary key to open a locked drawer (signifying the computer equipment). The key is neutral and does not have to

do anything with the contents inside the computer or the drawer. Therefore, it may not be equated to be incriminating, as even in the case of any adverse evidence incriminatory to the owner of the computer or the drawer is found, the same has to be separately established in trial.

Hence, whether disclosure of a passcode under compulsion by police was in question. Section 175 of the IPC creates a mandate to share electronic record, failing which creates penal consequences. Therefore, the question that arises is whether Section 175 IPC if applied to fetch password, can be denied? Does it militates with Article 20(3)? and therefore be considered as self-incriminatory? In the above context the position taken by the Karnataka High Court in *Virendra Khanna v. State of Karnataka*, 2021 SCC OnLine Kar 5032, could be critically contemplated to be narrower w.r.t. production of documents and material protected by passwords.