S.Balu,
Addl. Superintendent of Police (Retd)
Tamil Nadu.

79 A IT (A) Act 2008

"This Paper was presented by the author in the 40TH ALL INDIA CRIMINOLOGY CONFERENCE ON DIMENSIONS OF CRIME AND CRIMINAL JUSTICE SYSTEM: CONTEMPORARY ISSUES AND CHALLENGES held on 19th - 21st January 2018 at Gujarat National Law University, Gandhinagar."

Abstract :

" This paper focuses the wrong perspective on the provision of "79A of Information Technology Amendment Act (IT (A)), 2008*1, by most of the literates. It stipulates that the Central Government may, for the purposes of providing expert opinion on Electronic form Evidence before any court or other authority specify, by notification in the official Gazette, any department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence. The objective of this section is to help the Judiciary/Adjudicating officers in handling technical issues. The above provision was inserted in the amended Act IT (A), 2008. It came Into effective from 27th October 2009, by a Gazette notification*2. Subsequently on 2nd January 2017, the Government of India came out with a notification under Section 79A of IT (A) 2008 on a pilot scheme for notification *4 of Government organizations as "Electronic Evidence Examiners". The notification is under process. At the moment the above provision is quite inoperative as no agency has been notified. Recently during the trial of a hacking case investigated by me , which was mainly depended upon the evidences of Forensic Assistants and their reports,the accused counsel argued that since the Tamil Nadu State Forensic lab/ Scientific Assistants have not been notified under section 79A as an Examiner of Electronic Evidence, their reports and evidences have to be ignored. The court accepted the defence argument and acquitted the accused placing it as a prime reason. Now the appeal is before the Madras High Court. This paper is to project the objectives of 79A of ITA 2008 and envisage the wrong perspective by the Literates. "

Introduction:-

There are many laws for regulating the human activities in the Physical world. But we have not witnessed either major misuse or amendments/scrapping in the enacted Laws. For instance the major criminal law, The Indian Penal Code, which was enacted in the year 1860 has undergone only very few changes in the last 157 years. Very few crimes have been added to the initial list of crimes and declared punishable. But the only Law 1,"The Information Technology Act, 2000", which was enacted to regulate the human activities in the Cyber Space, has faced major amendments in the year, 2008 and also a penal provision i.e. 66A has been scrapped by the Supreme Court of India in the year 2015*3. The law is not suiting to all the situations and some of the legal provisions are being misunderstood and misused. Why in a short span of time, the said Act has been amended and one of the penal provisions scrapped? Because, even now, we have not experienced all the situations in the Cyber Space. Each and every minute we are meeting with a new experience in Cyber Space. This causes persistent anxiety.

Background

Let us see the background for the introduction of the above new provision and situations caused me to present this paper. After the enactment of Cyber Law, the Forensic Labs under the control of the Central Government and State Government have started establishing Computer Forensic Labs and commenced procuring of latest Cyber Forensic Tools. The Qualified Scientific Assistants of the Labs are also placed to undergo various Forensic Trainings. They have been accepting the digital storage Medias from the Law Enforcements through the Courts for digital analysis and submitting their reports in the courts. They are also attending the courts for deposing their evidences as their opinions are legally admissible according to the provisions U/s. 45 of Indian Evidence Act and Section 293 of Cr.P.C.

However, considering the complexities and constant changing of the Cyber Crime, the legislators felt the utmost need of experts exclusively for handling the electronic evidences and periodical updating of computer forensic tools and the knowledge of Experts in the Centre and State computer Forensic labs.The services of expert will be required to explain to the Judge in the court the evidence adduced, since much computer-derived evidence is unintelligible to the normal person. The person will generally be primarily concerned with the properties of the Information and Communication Technologies (ICTs) from which the evidence is derived, rather than the content of the retrieved material.

An expert essentially acts as an interpreter, addressing those matters likely to be outside the experience of and knowledge of a judge. As such, the role of an expert is not simply to present facts, but also to offer opinions and interpretations on matters on which he has expertise. Indeed, the ability to state opinions distinguishes an expert from the general rule applicable to witnesses that they should only give evidence of facts they have perceived, although it must be clear to the court on what facts any expert opinions are based.

In the adversarial common law system, both the prosecution and defence teams will need to make use of the services of expert witnesses. In civil law systems, such as in France and Germany, an official expert will be nominated by the court that has a different status from a witness. In view of the necessity and importance,as additional facility, this provision was inserted. It directs the Central Government to notify the Government organizations as Examiner of Electronic Evidence to assist the Courts and adjudicating officers. The notifications will be followed by allocating the required resources to make the existing Forensic Labs and the Scientific Assistants as strong and updated to face any changing situations in the cyber space.
Wrong Perspective.

In this regard after explaining the provision, I would like to place three cases, including a case investigated by me to show the wrong perspective by the Advocates in all the cases and by the Judicial in one case, in which I was the Investigating officer.

What is 79 A? -Central Government to notify Examiner of Electronic Evidence.

The Central Government may, for the purposes of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the official Gazette, any department, body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Explanation:- For the purpose of this section, "Electronic Form Evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, digital fax machines". In the above section we have to note, the use of the word "may" instead of "Shall". The words may and shall are distinct in meaning, while one confers a discretionary power, the latter one pelts the mandatory direction. The provision indirectly expresses the followings:-

- Existence of some system for the intended purpose.
- Notification is neither mandatory nor urgent.
- It is only an additional facility
- It is mainly for any court or other authority specify.

The above section was inserted in the Information Technology (Amendment) Act, 2008 and the amended Act came into effective from 27 October 2009 by a Gazette notification. On 2nd January 2017, the Government of India came out with a notification under Section 79A of ITA 2008*4, on a pilot scheme for notification of certain Government organizations under Section 79A as Examiners of Electronic Evidence.

In line with the above requirement, MeitY has formulated a scheme for notifying the Examiner of Electronic Evidence. The objective of the scheme is to ascertain the competence of all the desiring Central Government or a State Government agencies and to qualify them to act as Examiner of Electronic evidence as per their scope of approval through a formal accreditation process. Once notified such Central, State Government agencies can act as the Examiner of Electronic Evidences and provide expert opinion of digital evidences before any court.

The scheme is based on international standards like ISO/IEC 17025 (A Standard on General requirements for the competence of testing and calibration laboratories) and ISO/IEC 27037 (A Standard on Information technology -Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence). The evaluation process includes examination of the technical, skilled professional manpower in digital forensics, licensed tools and equipment,

availability of suitable environment to carry out such evaluation as also the availability of a proper quality management system and reasonable experience to demonstrate their overall competency in this area. Hence notification of Examiner of Electronic Evidence is only under process. At the moment we need not think of an Examiner of Electronic Evidence. Since the Government Labs are only going to be notified, automatically the law enforcements will be benefited. The procedures said in the criminal procedure code have not changed and the Police will continuously Utilize the services of experts as prevailing. This will not discourage the private forensics experts in India as they will get support from the private industry. No doubt in US, there are different categories of experts viz., Loaned Govt. employee, retained private consultant, court appointed expert etc.

The primary objectives for notifying the Govt. organizations are to ensure the confidentiality and integrity. The law enforcements are also having their labs for investigation purpose. For instance in a hacking case the investigating officer is suspecting, the theft of information from a particular system. The system hard disk was seized and sent to the Lab through court. As in traditional crime the I.O. had no opportunity of observing the hard disk /scene of crime and to tell the expert to look for any foreign Finger print in a particular place or in an object. The I.O. should keep a copy of the hard disk to observe by utilizing the lab set up by the Police for investigation purpose and to frame questions. Otherwise the investigation will be defective and the I.O. could not take a lead from SOC.

Defense counsels try to exploit the absence of any central notification about the Examiner of Electronic Evidence. The legal aspects of Digital Evidence in India are covered under Indian Evidence Act and Information Technology Act 2000 (amended in 2008). 45A. Opinion of Examiner of Electronic Evidence.-When in a proceeding, the court has to form an opinion on any matter relating to any information transmitted or stored in any computer resource or any other electronic or digital form, the opinion of the Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000(21 of 2000)., is a relevant fact. This section has reference to section 79A of the IT Act 2000.In the absence of notifying of Examiner of Electronic Evidence under the IT Act 2000 by the Central government, the section 45A of the Indian Evidence has no relevance.

Case 1*5:-

Tamil Nadu-The High Court of Chennai in criminal case K. Ramajayam @ Appu Vs. The Inspector of Police, T-4, Maduravoyal Police Station, Chennai stated In fine, we approve the method adopted by the Police in sending the Digital Video Recording (MO-2) itself to the Tamil Nadu Forensic Sciences Laboratory for the computer experts to view the recordings and give a report of the events in the nature of Ex.P-10. Similarly, the morphological study of the photographs of the accused that has been obtained by the Police from two sources, by Pushparani (PW-24), Scientific Officer, and her Report (Ex.P-12) stands accepted by us to infer that the assailant seen in the CCTV footage is the accused. It is axiomatic that the opinion of an expert, which is relevant under Section 45 of the Indian Evidence Act, 1872, when accepted by the Court graduates into the opinion of the Court.

The Central Government has not yet issued notification under Section 79A of the Information Technology Act, 2000 on account of which Section 45A of the Indian Evidence Act, 1872 remains mute. Therefore, the methods evolved by Kala (PW-23) and Pushparani (PW-24), Scientific Officers of the Tamil Nadu Forensic Sciences Department to analyze and give their opinions on the electronic data, are correct and cannot be faulted.

Case 2*6:-

Odisha -The recent judgment- delivered by the Sub-divisional judicial magistrate, Puri in G.R. Case number 1739/2012, the defense counsel had argued that the evidence given by the CFSL, Kolkata cannot be admitted given the fact that there is no official notification from the Central government declaring CFSL as Examiner of Electronic Evidence. But the trial court rejected the argument of the defence and delivered the orders in favour of testifying the experts under section 45 of Indian Evidence Act and section 293 of the CrPC.

Relevant portion of the Judgment :

The learned defence counsel argued that the evidence of P.W.13, L. Nato Singh the Scientific Officer of C.F.S.L., Kolkata is not admissible as it has not complied the mandatory provision of Section 79(A) of Information Technology Act. He further argued that the C.F.S.L., Kolkata has not been declared or notified either by the Central Government or State Government for examining as an expert required U/s. 79(A) of Information Technology Act. Considering the argument of learned A.P.P. and the defence counsel the court admitted the evidence of P.W.13 as per the provision of U/s. 293 Cr.P.C..

Neither the Central Government nor the State Government has yet to declare or notify any institution for the purpose of providing expert opinion. It does not mean any type of evidences which are produced as a secondary piece of evidence for which the expert opinion is required and in absence of the notification from the side of the Government such evidences stand uncorroborated and the prosecution shall be bewildered on the context of seeking notification from the side of Government. When the opinion of any Scientific Officer is complied with the provision U/s. 45 of Indian Evidence Act and Section 293 of Cr.P.C. then such opinion can be considered as an expert opinion. Even if, the notification U/s. 79(A) of I.T. Act is not available yet it is admissible and the opinion of the expert complied with Section 45 of the Indian Evidence Act 1872 and Section 293 of Cr.P.C. is a relevant fact.

On perusal of the Exts. 32 and 33 it has been noticed that the prosecution has complied the mandatory provision required U/s. 65(B) of the Indian Evidence Act as it was certified by the Nodal Officer, D.G.M., B.S.N.L., Orissa, Bhubaneswar. Having regards to above discussion the evidence of both P.W.12 and P.W.13 are admissible by treating them as the expert. The prosecution can rely upon Section 45 of the Indian Evidence Act and Section 293 of Code of Criminal Procedure which states as follows:

45 IEA
Opinions of Experts

When the Court has to form an opinion

upon a point of foreign law or of science or art,
or as to identity of handwriting [or finger impressions],

the opinions upon that point of persons specially skilled in such foreign law, science or art, [or in questions as to identity of handwriting] [or finger impressions] are relevant facts. Such persons are called experts.

45-A. IEA
Opinion of Examiner of Electronic Evidence.

When in a proceeding, the court has to form an opinion

on any matter relating to Electronic Form Evidence (any information transmitted or stored in any computer resource or any other electronic or digital form,)

the opinion of the Examiner of Electronic Evidence referred to in section 79A of the Information Technology Act, 2000(21 of 2000) is a relevant fact.

293. Reports of certain Government scientific experts.

(1) Any document purporting to be a report under the hand of a Government scientific expert to whom this section applies, upon any matter or thing duly submitted to him for examination or analysis and report in the course of any proceeding under this Code, may be used as evidence in any inquiry, trial or other proceeding under this Code.

(2) The Court may, if it thinks fit, summon and examine any such expert as to the subject- matter of his report.

(3) Where any such expert is summoned by a Court and he is unable to attend personally, he may, unless the Court has expressly directed him to appear personally, depute any responsible officer working with him to attend the Court, if such officer is conversant with the facts of the case and can satisfactorily depose in Court on his behalf.

(4) This section applies to the following Government scientific experts, namely:-

(a) any Chemical Examiner or Assistant Chemical Examiner to Government; ,(b) the Chief Inspector of Explosives;

(c) the Director of the Finger Print Bureau; ,(d) the Director, Haffkeine Institute, Bombay;

(e) the Director , Deputy Director or Assistant Director of a Central Forensic Science Laboratory or a State Forensic Science Laboratory;,(f) the Serologist to the Government.

Case -3*7:-

Tamil Nadu- CBCID Cyber Crime Cell-It is submitted that the accusation against the accused is that the accused an employee in Vigilance & Anti Corruption with his services being located in the building NCB 23, on 01.04.2008 and 02.04.2008 entered the building NCB 21 were the legal adviser and other officials are stationed and having access to NCB 21 building under the guise of going to meet official PW 43 unobtrusively gained access to the computer of the legal adviser in the ground floor and meddled with his computer using the pen-drive of that of his sister Sujatha and deliberately caused the publication of confidential nature transpired between the Chief Secretary of Tamil Nadu Govt. and the Director of V&AC, information being in store for exclusive use of PW 43. The accused/respondent deliberately copied the information in store. The careful investigator in substantiating the originator of the crime examined as many as 54 witnesses and seized and marked 110 documents besides material objects in all 26 numbers. Prosecution tendered as many as 45 witnesses.

Relevant portion of the Judgment :

While so on perusal of the entire material objects marked by the prosecution the original audio file recorded in the office of the PW43 has not been recovered and marked by the prosecution to prove the charges levelled against the accused . While so Tr.S.Balachandar, Senior net work Engineer You Telecom IndiaPrivate Limited Chenna.34 has been examined as PW8 ,and Tr.N.Thiyagarajan, ServiceEngineer HCL , Nandanam ,Chennai has been examined as PW25 , and M.Asokan, Audio Visual Technician (Photographer)CBCID , Chennai 32 has been examined as PW27 , and Mr. K.Manivannan , Scientific Assistant Gr.II Computer Forensic Unit, TNFSD,Chenani.4 has been examined as PW30 Tr.D. Robert ,Manager , HCL, Anna Nagar Chenai 45 has been examined as PW37 , and Tr. CH.E. Sai Prasad , Assistant Central Intelligence, Officer,Gr.IComputer , Forensic
Division, GEQD, Ramanthapur, Hyderabad has been examined as PW38 . They gave evidence about the tampering of computer by using pen drive and the Learned Public Prosecutor argued that the evidence of above said experts can be used against the accused for commission of offence.

At this juncture on perusal of the information Technology Act Section 79 A reveals that " the Central Government may, for the purpose of providing expert opinion on electronic form evidence before any court or other authority specify, by notification in the official Gazette, any Department , body or agency of the Central Government or a State Government as an Examiner of Electronic Evidence.. ."But in this case no such notification was issued in respect of Forensic Agency to state or Central Government .Hence the evidence given by the PW8, PW25, PW27 , PW30, PW37 andPW38 are not acceptable evidence and it will not be used against the accused as per section 79A of Information Technology Act. It is pertinent to say there is no eye witness in this case to prove the charges against the accused. But there are circumstantial evidence who had deposed before this court but it is not continuation of events to prove the charges against the accused. To sum up everything the prosecution has not proved the charges leveled against the accused beyond all reasonable doubts . In the result the accused found not guilty U/s 66, 70 & 72 I.T. Act, and acquitted u/sec.235(1) Cr. PC. M.O.1. to MO26 are ordered to be confiscated to state after appeal time is over. Now the appeal is pending before the High court of Madras.

Conclusion:- I would like to express my concluding message through a wall picture appended below:-

It is a story of a group of blind men, who have never come across an elephant before, learn and conceptualize what the elephant is like by touching it. Each blind man feels a different part of the elephant body, but only one part, such as the side or the tusk. They then describe the elephant based on their partial experience and their descriptions are in complete disagreement on what an elephant is. In some versions they come to suspect that the other person is dishonest and they come to blows. The moral of the parable is that humans have a tendency to project their partial experiences as the whole truth, ignore other people's partial experiences, and one should consider that one may be partially right and may have partial information.Most of the Netizens have not understood the cyber law and Cyber Crime in proper perspective and similar to the description of an Elephant by six blind Men.
I have not come to above conclusion only on the basis of wrong Perspective on 79 A, but I have more instances with regard to other provisions and cybercrime. I have placed a few instances below:-

1) Hacking Case 2005 – Wrong perspective by the accused: - Arrested Ex-Employee engineer for the theft of a Vehicle's design from a Company. Accused claimed that it was his design since he designed while he was working in the company. Imagine if a Cook who prepared food takes away the food by telling that it's her/his preparation.

2) Hacking-Case-2007. Wrong perspective by the Advocate:- Information theft by the employee in an MNC was charge sheeted for information theft under section of 66 I.T.Act 2000. While crossing the defense counsel questioned me Do you know that the information which was charged to have stolen by the client is easily available in the internet? Have you investigated on those lines? I told that the information which was possessed by the company was stolen by the accused and the same was established by CC TV Footage, Duty Access card logs, Time stamp logs etc. and it is similar to caught red handed case. Whether the same information is available in the internet or not, is immaterial for the case. Let us imagine copies of Thirukural books kept in a School office was stolen by a visitor and the thief was caught red-handed,During trial, can accused take the Defence as the Thirukural books are easily available in the market?

3) Hacking case (2008) Wrong perspective by the Court: - i.e. information theft case, the accused was charge sheeted for downloading a particular audio file from a hard disk in a pen drive. When the case was under trial the accused filed a petition in the High court for furnishing copy of all the information in the hard disk to defend the case. High court ordered the trial court not to furnish all the information but to provide the information which he was charged as stolen. Accordingly the trial court furnished. Let us imagine if it is a case of Servant theft of one lakh cash. In such scenario, if the accused asked to provide the cash of one Lakh, for defending the case, Will the court issue order to give one Lakh rupees?

In fine I would like to suggest that "a detailed debate on the applicability of Section 79A and other provisions of IT Act & Cyber Crime have to be conducted repeatedly with intensity for creating awareness among the Advocates &Judiciary to analyse in proper perspective for a just decision. However as the framers of the amendment did not clarify the effect to be given to such amendment as a result of which courts are in dilemma to conclude that notification as mandate under section 79A not being issued ,the need to resort to take evidence of Scientific Asst. not acceptable.The absence of implementation drive to conclude that expert evidence of forensic science could not be acted upon and as such a lacunae is created causing disadvantage to prosecution.

On 26.3.2018, the Ministry of Electronics And Information Technology notified the Forensic labs at New Delhi, Gujarat & CFSL Hyderabad as Examiner of Electronic Evidence within India. Now the situation is different because of 3 notified Labs in India. What will be the status of the States including Tamil Nadu, which do not have notified Labs, is a present question before us? With this I conclude my article.

References:

1. *1Information Technology Amendment Act (IT (A)), 2008 http://www.eprocurement.gov.in/news/Act2008.pdf
2. *2 Gazette notification for (IT (A)), 2008 http://www.naavi.org/naavi_comments_itaa/ita_2008/ita_2008_notification.pdf
3. *3 66A scrapped by the Supreme Court of India in the year 2015*3 https://www.scribd.com/document/259756539/The-Section-66A-judgment
4. *4 Notification under Section 79A of ITA 2008 http://meity.gov.in/notification-pilot-scheme-notifying-examiner-electronic-evidence-under-section-79a-information
5. *5 Case 1: https://indiankanoon.org/doc/179639914/
6. *6 Case 2: https://www.naavi.org/wp/court-in-puri-debates-section-65b-iea-and-section-79a-ita2000/

★