# Use, Admissibility and Proof of Electronic Evidence, in Investigation and Trial; A Critical And Empirical Study with Special Reference to the State Of Goa.

A THESIS SUBMITTED IN PARTIAL FULFILLMENT FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

IN LAW

Manohar Parrikar School of Law, Governance and Public Policy

GOA UNIVERSITY

GOA


BY

Pooja Chandrakant Kavlekar

V M SALGAONCAR COLLEGE OF LAW

Research Centre-Miramar

December 2022

# DECLARATION

I, Ms. Pooja Chandrakant Kavlekar, hereby declare that this thesis represents work which has been carried out by me and that it has not been submitted, either in part or full, to any other University or Institution for the award of any research degree.

Place: Taleigao Plateau.

Date : 31-12-2022 Pooja Chandrakant Kavlekar

# CERTIFICATE

I,Dr. K.S. Rao, hereby certify that the work was carried out under my/our supervision and may be placed for evaluation.

Dr.K.S.Rao

Research Guide

V.M.Salgaocar College of Law,

Miramar, Panaji, Goa.

# ACKNOWLEDGEMENT

The God almighty, who kindness has bestowed this day upon me. This is one of his countless blessings and I begin with praises and gratitude to the divine force that has been with me throughout my life.

I extend my profound and deepest gratitude to my guide Dr K. S. Rao for his continuous support and guidance for my Ph. D study. Sir has been the epitome of humility and a fountainhead of immense knowledge. Words cannot express my gratitude Hon'ble Dr Rao for his invaluable patience, guidance and feedback. In true sense of the term "guide" sir has been beacon that has shown me the way towards completion of these thesis.

I am extremely grateful to Dr P.D. Sebastian for always being there when I needed his support, reviewing my progress constantly, and guiding me through my PhD studies. His insight into the subject of technology is remarkable. A soft spoken, amiable personality was generous enough to adjust his travel schedules to suit my non working days.

My gratitude also goes out to Dr Shabbir Ali, Principal V M Salgaoncar College of Law who took his time to read the draft and prolifically shared with me the wisdom gathered from his wide research studies. I thank him for teaching me the nuances of research methodology and for all the support.

I could not have undertaken this journey without the constant support of my colleagues in the judiciary and particularly Hon’ble Principal District Judges officiating from the year 2015 to 2022 in the North and South Goa Districts.

I would also like to extend my thanks to the advocates of the North and South Goa bar and prosecutors in the State of Goa for enthusiastically sharing their experiences on the subject of electronic evidence and painstakingly answering the questionnaires.

I am also grateful to the Police Department particularly the Police Inspectors of Cyber Crime Police station and the Director and Scientific Officers of GFSL Verna for having assisted me in the field work.

I thank the Editorial Board of the CMR Journal of Innovation and Research, Bangalore for considering my research paper worthy of publication.

Special thanks to Ms. Bhakti Naik, Dr. Shruti Dalal, Dr. AndyrushaD'Costa, and Adv Emidio Pinho, who were always there for discussions about anything that I was unsure on. Thank you for being so generous and giving.

The foundation is at the bottom, but holds the entire edifice. My roots, my foundation, the essence of my very existence, my father Shri Chandrakant Kavlekar and my mother Mrs. KundaKavlekar, thank you will be too small of a word for all that they have done for me. I dedicate my entire life and existence in gratitude to them. They continue to inspire me every single day.

I am deeply indebted to my father in law Mr. Kiran Naik and my mother in law Mrs. Disha Naik who have put up with a very unconventional, academically inclined, daughter in law and have always encouraged me to soar high.

This endeavour would not have been possible without my best friend for life, the wind beneath my wings, my husband Mr. Amey Naik, on whose insistence I ventured on this journey. Thank You for holding on to me when I was at my weakest. This thesis would not be possible without his unconditional support and help during my PhD journey.

I thank my dear friends in the judiciary who have always had my back.

I am also thankful to the staff of the Libraries of VM Salgaoncar College of Law, North and South Goa District court and the Maharastra Judicial Academy for assisting me in reference of books and journals.

Last but not the least I thank each and every person who has helped me in every small which way.

*Pooja C.Kavlekar*

# Contents

## CHAPTER – 1

## Introduction

## CHAPTER- 2

## The Scope of Admissibility And Proof Of Electronic Evidence Under The Indian Law

## CHAPTER- 3

## International Conventions and Model Laws on Electronic Evidence and Genesis of Indian Law.

## CHAPTER- 4

## Seizure, Production and Evidentiary Aspects of Electronic Evidence.

## CHAPTER- 5

## Data Analysis and Findings: Comparison of Idealism with Practical Reality

## CHAPTER 6

## Conclusion and Suggestions

# List Of Tables

# List Of Figures

## List Of Cases

| Sr. No. . | Name of case with Citation |
|---|---|
| 1 | Brijnandan Sinha v. Jyoti Narain AIR 1956 SC 66 |
| 2 | Sharad Birdi Chand Sarda vs State Of Maharashtra 1984 AIR 1622 |
| 3 | In Hanumat's v. State of M.P. [1953] SCR 1091 |
| 4 | Subramaniam v. Public Prosecutor, (1956) 1 WLR 965 |
| 5 | Rabindra Nath Thakur v. Union of India, 1998 SCC OnLine Pat 580 |
| 6 | Sudhir Engineering Company v. Nitco Roadways Ltd. 1995 IIAD Delhi 189 |
| 7 | Baldeo Sahai v. Ram Chander&Ors., AIR 1931 Lahore 546; |
| 8 | Smt. Dayamathi ..Vs.. K. M. Shaffi, A.I.R. 2004 S.C. 4082 |
| 9 | Hemendra Rasiklal Ghia & Oths Vs. Subodh Modi & Oths2008 (6) Mh.L.J., 886 |
| 10 | Kali Ram v. State of Himachal Pradesh [(1973) 2 SCC 808 |
| 11 | Shafi Mohammad vs. The State of Himachal Pradesh,(2018) 2 SCC 801 . |
| 12 | Hemendra Rasiklal. Ghia v. Subodh Mody.; 2009(3) ALJ 69) |
| 13 | Unmesh Diwakar Raotevs.The Municipal Corporation of Greater Mumbai,C.S.T.&Ors.MANU/MH/2261/2018, |

| | |
|---|---|
| 14 | Faim and others v. The State of Maharashtra(MANU/MH/3080/2015) |
| 15 | Rangammal v. Kuppuswami, (2011) 12 SCC 220 |
| 16 | Saki Ammal @ Chitra vs. Veerabhadra @ Kumar (MANU/TN/1419/2012) |
| 17 | Anvar v. P. K. Basheer (2014) 10 SCC 473 |
| 18 | Utkal Contractors & Joinery Pvt. Ltd. v. State of Orissa AIR 1987 SC 2310 |
| 19 | Union of India and Anr., v. G.M. Kokil and Ors1984 AIR 1022 |
| 20 | Chandavarkar Sita Ratna Rao v. Ashalata S. Guram1986 4 SCC 447 |
| 21 | K. Vs. Maqsud Ali [1965] All. E.R. 464. |
| 22 | R.M. Malkani Vs.State of Maharashtra 1973 Cri.L.J. 228 |
| 23 | R.K. Anand Vs. Registrar, Delhi High Court, (2009)8 SCC 106. |
| 24 | Ram Singh and Ors. Vs. Col. Ram Singh 1985 (Supp) SCC 611 |
| 25 | N. Sri Rama Reddy Vs. V. V. Giri, 1971 (1) SCR 399. |
| 26 | S.Pratap Singh Vs. The State of Punjab, AIR 1964 SC 72 |
| 27 | Ziyauddin Burhanuddin Bukhari Vs. BrijmohanRamdass Mehra, (1976) 2 SCC 17 |
| 28 | Yusufalli Esmail Nagree Vs. State of Maharashtra, (1967) 3 SCR 720 : 1968 Cri.L.J. 103 |
| 29 | State (NCT of Delhi) v Navjot Sandhu AIR 2005 SC 3820 |

| | |
|---|---|
| 30 | Ratan Tata v. Union of India Writ Petition (Civil) 398 of 2010 before Supreme Court of India. |
| 31 | Lorraine v. Markel American Insurance Company 241 FRD 534 (D. Md. 2007) |
| 32 | Anvar P. V. vs. P.K Basheer &Ors AIR 2015 SC 180 |
| 33 | Tomaso Bruno and another v. State of Uttar Pradesh(2015) 7 SCC 178 |
| 34 | Sonu @ Amar v. State of Haryana 2017 SCC Online 765 |
| 35 | Arjun PanditraoKhotkar v. Kailash KushanraoGorantyal 2020 SCC OnLine SC 571 |
| 36 | K. Ramajayam alias Appu v. Inspector of Police 2016 (2) CTC 135 |
| 37 | Jagjit Singh v. State of Haryana (2006) 11 SCC 1. |
| 38 | K.K. Velusamy v. N. Palanisamy (2011) 11 SCC 275 |
| 39 | Mohd. Arif v. State (NCT of Delhi), (2011) 13 SCC 621 |
| 40 | Dharambir Vs. C.B.I(2008) ILR 2 Del 842 |
| 41 | State of Maharashtra Vs. Dr. Praful B. Desai AIR 2003 SC 2053 |
| 42 | Salem Advocate Bar Association AIR 2003 SC 189 |
| 43 | Twentieth Century Fox Film Corporation and anr. Vs. NRI Film Production Associates (P) Ltd AIR 2003 Kar. 48 |

| | |
|---|---|
| 44 | Shilpa Chaudhary v. Principal Judge And Others AIR 2016 ALL 122 |
| 45 | SirangiSobha Shoba Munuri vs SirangiMuralidharRao AIR 2017 AP 88 |
| 46 | Dr.KumarSaha Vs. Dr.Sukumar Mukherjee (2009) 9 SCC 221, |
| 47 | Suvarna Rahul Musale v/s Rahul Prabhakar MusaleWrit Petition No. 6514 of 2014 (Bombay High Court) |
| 48 | Kishan Tripathi vs The State MANU/DE/0434/2016 |
| 49 | SheebaAbidi Vs. State 113 (2004) DLT. 125. |
| 50 | Bodala Murali Krishna Vs. Smt. Bodala Prathima MANU/AP/0973/2006 |
| 51 | Mohd. Arif @ Ashfaq Vs. State of NCT of Delhi (2011) 13 SCC 621 |
| 52 | Bhupesh v. State of Maharastra 2018(3) BomCR(Cri)12 |
| 53 | Mohammad Ajmal Kasab AIR 2012 SC 3565 |
| 54 | Gubinas and Radavicius v HM Advocate, High Court at Aberdeen (2017) HCJAC 59 |
| 55 | C. Ramajayam@Appu Vs Inspector of Police 2016 (2) CTC 135 |
| 56 | Rahul Adiwal v. State of Haryana CRM-M-31490-2020 (O&M) Date of decision: 11.12.2020 the Punjab and Haryana High Court |
| 57 | A2Z Infraservices Ltd. Versus Quippo Infrastructure Ltd. (Now Known AsViom Infra Ventures Ltd.) SLP(C) No. 8636/2021 |

| | |
|---|---|
| 58 | Ritu versus State 2018 SCC ONLINE DEL 2914 |
| 59 | National Lawyers Campaign for Judicial Transparency and Reforms and others versus Union of India MANU/DE/1475/2017 |
| 60 | Ambalal Sarabhai Enterprise vs Ks Infraspace LLPLimited CIVIL APPEAL NO(s). 9346 OF 2019 |
| 61 | Imran Ilyas Dalla vs State OfMaharastra Criminal Application (BA) No.183 of 2020 |
| 62 | Samsung (India) Electronics (P) Ltd. v. MGR Enterprises, 2019 SCC Online Del 8877 |
| 63 | Mukul vs State Of PunjabCrl. Revision No. 570 of 2016 (O&M)theHonble Punjab-Haryana High Court |
| 64 | State of Punjab and others Vs. M/s Amritsar beverages Ltd and others AIR 2006 SC 2820 |
| 65 | M/S ICICI Bank Limited V/S Kapil Dev Sharma 2018 Latest Caselaw 652 Del. |
| 66 | Om Prakash v. Central Bureau of Investigation 2017 VII AD (Del) 649 |
| 67 | State of MP v. Paltan Mallah (2005) 3 SCC169 |
| 68 | Deepti Kapur v. Kunal Jhulka 2020 SCC Online Del 672 |
| 69 | Neha vs Vibhor Garg CR No. 1616 of 2020 and CR No. 2538 of 2020 (O&M) |

| | |
|---|---|
| 70 | HavoiSetna v. KersiGustadSetna AIR 2011. Bom. 283 |
| 71 | X v. Z AIR 2011. Bom. 283 |
| 72 | AchleyYadhav v. State014 (8) LRC. 236 (Delhi) DB |
| 73 | Kundan Singh vs The State MANU/DE/3674/2015 |
| 74 | Abdul Rehman Kunji v. State of West Bengal 2016 CrLJ 1159 |
| 75 | Smt Bharathi V Rao v. Sri Pramod G Rao MANU/KA/3243/2013 |
| 76 | Fatima Riswana Vs State and others AIR 2005 SC 712 |
| 77 | Amulya Kumar Panda Vs State of Orissa 2008 CRI. L.J. 1676 |
| 78 | G Shyamala Ranjini Vs. M.S. Tamizhnathan AIR 2008 Mad 476 |
| 79 | Preeti Jain vs Kunal Jain &Anr 2016 SCC OnLine Raj 2838 |
| 80 | S.K. Saini &Anr vs C.B.I.Crl. A. No.159/2005(Delhi High Court) |
| 81 | Raj Kumar v. State CRL.A. 232/2016 (Delhi High Court) |
| 82 | Sanju v. State of M.P 2019 SCC OnLine MP 2070 |
| 83 | Surendra v. State of MPM.Cr.C. No.15796/2020 (M.P. High Court) |
| 84 | Ark Shipping Co. Ltd. Vs. GRT Shipmanagement 2007 (6) Bom.C.R. 311. |
| 85 | Avadut Waman Kushe Vs. State of Maharashtra, 2016 SCC Online Bom 3256 |

| | |
|---|---|
| 86 | Brajesh Tiwari vs The State Of Madhya Pradesh Writ Petition 4834/2015 |
| 87 | Paras Jain v. State of Rajasthan (2016) 2 RLW 945 (Raj) |
| 88 | Kundan Singh v. State 2015 SCC OnLine Del 13647 |
| 89 | Avadut Waman Kushe v. State of Maharashtra 2016 SCC Online Bom 3256. |
| 90 | Kamal Patel v. Ram Kishore Dogne 2016 SCC OnLine MP 938 : (2016) 1 MP LJ 528 |
| 91 | State v. MR Hiremath AIR 2019 SC 2377 |
| 92 | Union of India and Others v CDR Ravindra V Desai (2018) 16 SCC 272. |
| 93 | State of Rajasthan through the Special P.P. Vs. Sri Ram SharmaCrl. Misc. Petition No. 4383/2016 dt. 02.09.2016 |
| 94 | Ignatius Topy Pereira Vs. Travel Corporation (India) Pvt. Ltd and another2016 SCC Online Bom 97 |
| 95 | J R Gangwani v. State of Harayana 2012 SCC Online P&H 19890 |
| 96 | Amrik Singh Juneja v. State of Punjab 2013 SCC Online P & H 3506; Rajaram Kabnure v. GunwantiDhulappaKetkale 2011 SCC Online 1275. |
| 97 | Shreya Singhal Vs. Union of India AIR 2015 SC 1523 |
| 98 | Syed Asifuddin And Ors. vs The State Of Andhra Pradesh 2005 CriLJ 431 |
| 99 | State of Punjab v. Amritsar Beverages Ltd (2006) 7 SCC 607 |

| | |
|---|---|
| 100 | Dr. (Smt.) Nupur Talwar vs State Of U.P. Crime Appeal No. - 293 of 2014 Allahabad High Court. |
| 101 | Om Prakash v. Central Bureau of Investigation 1999 (48) DRJ 686 |
| 102 | State of U.P. v. Raj Narain AIR 1975 SC 865 |
| 103 | Bibhabati v. Ramendra AIR 1947 PC 19 |
| 104 | Ram Bihari Yadav v. State of Bihar AIR 1998 SC 1850 |

## List of Abbreviations

| | | |
|---|---|---|
| 1. | UN | United Nation |
| 2. | UNO | United Nations Organisation |
| 3. | No. | Number |
| 4. | S.C. | Supreme Court |
| 5. | SCC | Supreme Court Cases |
| 6. | BOM | Bombay |
| 7. | SCC | Supreme Court Cases |
| 8. | MhLJ | Maharashtra Law Journal |
| 9. | AIR | All India Reporter |
| 10. | UOI | Union Of India |
| 11. | IO | Investigating Officer |
| 12. | Anr | Another |
| 13. | CBI | Central Bureau Of Investigation |
| 14. | Cr.P.C. | Criminal Procedure Code |
| 15. | POCSO | Protection of Children From Sexual Offences |

| | | |
|---|---|---|
| 16. | IPC | Indian Penal Code |
| 17. | RBI | Reserve Bank Of India |
| 18. | Cri.L.J | Criminal Law Journal |
| 19. | Del | Delhi |
| 20. | SC | Supreme Court |
| 21. | SCW | Supreme Court Weekly |
| 22. | SC | Sessions Case |
| 23. | SCORS | Sessions Cases Others |
| 24. | CS | Civil Suit |
| 25. | NI | Negotiable Instrument |
| 26. | UNCITRAL | The United Nations Commission on International Trade Law |
| 27. | CPC | Civil Procedure Code |
| 28. | CD | Compact Disk |
| 29. | All. E.R. | All England Reporter |
| 30. | Supp | Supplement |

Ouriginal

## Document Information

| | |
|---|---|
| **Analyzed document** | phd_final_29.12.0222_without_footnotes.docx (D154618107) |
| **Submitted** | 12/29/2022 12:42:00 PM |
| **Submitted by** | Nandkishor B. |
| **Submitter email** | asstlib2@unigoa.ac.in |
| **Similarity** | 1% |
| **Analysis address** | asstlib2.unigoa@analysis.urkund.com |

30/12/22

## Sources included in the report

| | | |
|---|---|---|
| W | URL: https://www.lawyerservices.in/Jisal-Rasak-Versus-The-State-of-Kerala-Represented-by-Public-Pro...<br>Fetched: 4/21/2022 10:30:07 PM | 13 |
| W | URL: https://www.livelaw.in/columns/the-law-of-electronic-evidencethe-error-continues-161892<br>Fetched: 12/12/2020 6:48:30 AM | 5 |
| W | URL: https://www.srdlawnotes.com/2018/04/electronic-evidence-admissibility-of.html<br>Fetched: 2/24/2021 9:55:36 AM | 4 |
| W | URL: https://www.ijrra.net/Vol4issue3/IJRRA-04-03-57.pdf<br>Fetched: 6/22/2022 10:43:33 AM | 15 |
| W | URL: https://ijcrt.org/papers/IJCRT2205188.pdf<br>Fetched: 12/19/2022 10:31:10 AM | 1 |
| W | URL: https://www.zeusip.com/admissibility-and-perplexity-of-electronic-evidence.html<br>Fetched: 7/29/2021 11:23:47 AM | 2 |
| W | URL: https://vipslawblog.wordpress.com/2022/02/28/digital-evidence-and-cyber-forensics/<br>Fetched: 12/5/2022 10:30:52 AM | 2 |
| W | URL: https://www.lawweb.in/2018/09/landmark-judgments-of-supreme-court-on.html<br>Fetched: 5/3/2022 7:38:53 AM | 1 |
| W | URL: https://lawtimesjournal.in/electronic-evidence-bnder-indian-evidence-act-1872/<br>Fetched: 4/27/2022 12:41:15 PM | 2 |
| W | URL: http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S1727-37812019000100015<br>Fetched: 11/26/2021 11:51:23 AM | 1 |

### Entire Document

Chapter 1 Introduction
1.1 Introduction

# Chapter 1

# Introduction

## 1.1 Introduction

Evidence constitutes the edifice of the justice delivery system. The various stages of its discernment, seizure, preservation, production, authentication and appreciation forms the entire gamut of the adjudicatory process.

When the existence of a fact is asserted by one person and denied by other, the fact has to be proved by evidence. Such chain of relevant facts provide resolution to the issue in dispute before the court of law. With rampant intervention of technology in our lives, proof of a fact no longer needs to be restricted to the human and documentary mode. The law makers recognised the potent ability of the Indian Evidence Act to prove a fact as a result the archaic 1972 law of Evidence was amended in consonance with the Information and Technology Act 2000. The Indian Evidence Act primarily recognised two kinds of evidence namely oral and documentary. As per amended Section 3(2) of Indian Evidence Act "electronic evidence" is added in the category of documentary evidence[1].

The Indian Evidence Act does not define the word electronic record however provides that the term "electronic record" shall be given the same meaning as is given in the Information Technology Act. Section 2(t) of The Information Technology Act 2000 defines electronic record as any data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche.

[1] Section 3(2) of the Indian Evidence Act provides that all documents including electronic records produced for the inspection of the Court, such documents are called documentary evidence.

It was in the year 2000 that the Indian Evidence Act was amended to incorporate special provisions which would be needed in the matter of admission and appreciation of electronic record as evidence[2].

The present study therefore takes a bird's eye view of the use, admissibility and proof electronic evidence in the State of Goa at the stage of investigation and trial. Here the term "Use" is given a restricted meaning so as to imply that production and utility of electronic records to prove a fact. The present study is restricted to the cases and statistics pertaining to the State of Goa. The study will be conducted in the socio- legal conditions unique to the State of Goa. To the best of the knowledge of the researcher there has been a serious dearth of legal and analytical research on the core theme of these thesis in the context of cases arising in the State of Goa.

### 1.2 Brief Overview of the Problem

A fact is proved by production of evidence which may be of myriad forms. A fact may be proved by adducing material proof by direct evidence, or by adducing discursive and intuitive proof based on circumstantial evidence. As a matter of fact all these forms of evidence overlap at a certain degree. This understanding of evidence makes it possible to see at once the difference in the roles of persons who produce evidence and the persons who access or apply that evidence. The former is required to establish evidence and the latter is required to appreciate it. In both cases however it is important for them to understand the genesis of the evidence sought to be produced. The conventional form of evidence is simple and hence can be obtained and processed at both these levels with ease. The difficulty lies when the evidence is relatively non conventional, fairly vulnerable and essentially abstract, requiring the assistance of technology to make it readable. These attributes aptly describe the new breed of evidence called "electronic

[2] The second schedule of the Information Technology Act 2000 contains the list of amendments made to the Indian Evidence Act 1872.

evidence".

The first foremost point that needs to be highlighted is the level of comfort that both these functionaries have with “Electronic evidence”. This will be determined by their familiarity with the subject. Familiarity will essentially arise out of its frequent usage. Frequent usage will help in identifying flaws of in procurement, seizure, preservation and appreciation of electronic evidence. The most arduous part of this process is that the person producing electronic evidence and proving the same is pitted against the person assessing it. In the existing adversarial system, the latter cannot assist the former in any manner to ensure that best evidence is produced to prove a fact. Simply stated a Judge cannot guide police or a prosecutor when an electronic record is not properly admitted or proved. It can only reject the same as inadmissible and not proved.

The second aspect is that conventional form of evidence was not vulnerable in and therefore there was no excessive importance given to the aspects procurement, seizure, preservation in the matter of its appreciation. Evidence to prove a fact in court is not expected to be immaculate. However it needs to the highest degree of credence. Conventional form of documentary evidence by its nature is essentially infallible, because the instance of tampering can easily be detected. However an electronic record is different from the form it manifests itself in. Therefore the chain of its custody right from its generation, transmission, procurement, seizure, preservation becomes a relevant fact. Ultimately the question whether the electronic record produced in the court has been tampered with will depend upon the correlativity of all these factors.

Thirdly, considering its wider scope to record and reproduce facts without intervention of the fallibilities human mind, electronic evidence has greater potential to prove a fact then the conventional forms of evidence. For this wide potential to be tapped there needs to be a clear and functional legislation that prescribes methods of its admissibility and mode of proof. Therefore in the light of the above, the researcher intends to unearth the challenges faced in use, admissibility and proof of electronic evidence.

The Impediments that possibly exists in the seamless functioning of the above three processes can broadly be divided into two categories:

1. Impediments at procedural level of legislation.
2. Impediments at substantive level of legislation.

### 1.2.1 Impediments at Procedural Level

A cursory look at the codes of procedure and the rules of evidence in the light of latest technological advances makes it manifest that there is a gap between conceptual idealism and experimental reality. Some of the paradoxes in the law are examined as under:

1. *Conventional machinery for investigation is ill equipped with the tools required to procure, preserve and extract relevant electronic evidence.*
2. *There is lack of knowledge and sufficient training of all stakeholders in matters relating to electronic evidence.*
3. *Usage of electronic evidence is infrequent as formal nature of proof requisitioned in the court a major discouraging factor.*
4. *There is lack of infrastructure to process, validate and preserve electronic data.*

### 1.2.2 Impediments at Substantive Level

The term substantive used here implies, the legislation that governs production, admissibility and proof electronic evidence. The researcher found that there were hurdles, some insurmountable, for using electronic evidence to prove a fact before the court of law. These hurdles essentially emanated from the shortcomings or paradoxes in the existing laws. These shortcomings are briefly stated as under:

1. *Electronic evidence is a new breed of evidence requiring a specialised law*

*governing and regulating the same.*

2. *The amendments made to the Indian Evidence Act by the Information Technology Act making secondary evidence of electronic record is essentially vague and is of no significant assistance in the matter of admissibility of electronic evidence.*
3. *The only mode of proving an electronic record whose authenticity is disputed appears to be the assistance of an expert which is expensive and arduous.*
4. *Existing legislations ignore the potent ability of electronic evidence to conclusively prove facts.*
5. *Lack of awareness and knowledge of electronic form of evidence amongst judges advocates, police and other stakeholders create bigger challenges in appreciation of evidence.*
6. *Traditional doctrinaire procedures relating to judicial process are not in consonance with the requirement special conditions needed for handling of electronic evidence.*

### 1.3 Objectives Of Study

The study endeavours to achieve the following objectives:

1. To decipher the gap between conceptual idealism and experimental reality.
2. To understand and elucidate the two stages that electronic evidence needs to pass namely, admissibility and mode of proof by studying the existing rules, regulations pertaining production and appreciation of electronic evidence and examine judicial precedents on the subject of electronic evidence and examine its efficacy in dealing with challenges relating to electronic evidence.
3. To trace the genesis of Indian Law on electronic evidence vis-a-vis International Rules and conventions and investigate the impact of amendments made by the

Information and Technology Act to the Indian Evidence Act and other laws.

4. To explore the process in seizure, preservation transit, production of electronic record at pre-trial(Investigation)and trial stage with case studies.
5. To identify, substantive and procedural impediments, in the existing legislation and examine its impact on cases in which on electronic evidence is produced or proposed to be produced and to examine the fitness of prosecuting agencies and judiciary to tender and appreciate electronic evidence respectively.
6. To suggest ways and means to make optimum use of available resources, by providing insights and mode for strengthening and streamlining the existing rules of evidence and procedure.

**1.4 Research Questions**

1. Whether there is limited use of methods of investigation using electronic evidence due of lack of information, knowledge and Training?
2. Whether the present rules of procedure contain a full proof mechanism for making optimum use of electronic evidence in all types of cases?
3. Whether there is adequate infrastructure available in the State of Goa that would assist the law enforcing agencies in proper seizure, preservation, production and authentication of electronic evidence in court?
4. Whether electronic evidence being new breed of evidence requires a specialised law of procedure governing and regulating the same and the amendments to the Indian Evidence Act are fit to cover all cases involving proof of electronic records?
5. Whether proper use and authentication of electronic technology will lead to complete demystification of the adjudicatory process ensuing transparency, clarity, better accessibility and certainty?

## 1.5 Hypothesis

1. There is limited use of methods of investigation using electronic evidence due of lack of information, knowledge and training.
2. The present rules of procedure are obsolete and do not contain a full proof mechanism for making optimum use of electronic evidence.
3. There is inadequate infrastructure available in the State of Goa that would assist the law enforcing agencies in proper preservation, production and authentication of electronic evidence in court
4. Electronic evidence being new breed of evidence require a specialised law of procedure governing and regulating the same and the amendments to the Indian Evidence Act are cryptic and unfit to cover all cases involving proof of electronic records.
5. Proper use and authentication of electronic records will lead to complete demystification of the adjudicatory process ensuring transparency, clarity better accessibility and certainty in evidence.

## 1.6 Methodology

The research is essentially critical, empirical and doctrinal. The researcher adopted the survey method, interview method, case study method, participant and non participant observation technique and use of empirical data from custodian primary sources for research. The researcher has used unstructured interview technique and structured questionnaires. Secondary data for the study has been collected using Law books, bare Acts articles on law journals and magazines, dictionaries, Government Notifications, Official Gazettes, information published on Government websites and other relevant websites.

### 1.6.1 Survey Method

For the survey method the entire population of stake holders was divided into four categories. The researcher used the random stratified sampling method so as to indentify the smaller homogenous group existing within the population. These fourfold stake holders are judicial officers, prosecutors, police, lawyers . This method was employed by using both structured and open ended questionnaires. The questionnaires were distributed to the respondents either physically or digitally using Google forms.

For conducting survey into this homogenous group the researcher employed the random sampling techniques. The stratified random samples of the four stake holders were administered different questionnaires. Although substantively the questionnaires had common questions however to some extent they were customised keeping in mind the role that each stake holder played in the matter of production/seizure, admission and appreciation of electronic evidence. The questionnaire was a combination of closed as well open ended responses. However as the data which was to be obtained from the questionnaire was to be analysed there were higher number of closed questions. Some questions in the questionnaire were used inform of rating scale so as to ascertain the extent of comfort and interaction of the respondents with electronic records.

### 1.6.2 Interview Method

The researcher interviewed a select few from amongst the stakeholders. The persons selected for interview were persons who had essentially dealt with cases relating to electronic evidence and had firsthand experience in handling cases with electronic evidence. From amongst the survey population, employing partly the convenience sampling method and partly the purposive sampling method the researcher has interviewed some eminent persons, from amongst the survey population, consisting of Police, Judges, Lawyers, Prosecutors and even Litigants. These persons may or may not have constituted the sample used in the survey method for administration of the questionnaires. The researcher also interviewed computer forensic experts from various

reputed computer forensic laboratories in the country who were not a part of the survey population.

Considering that this research is not purely empirical the researcher conducted an unstructured interview as it provided a high degree of flexibility to both the interviewer and the interviewee in questioning and responding. For the interview method the researcher used the non probability sampling technique and purposive and convenience sampling sub technique.

### 1.6.3 Participant and Non Participant Observation Method

The researcher is a judicial officer having about 15 years experience first as a trial court judge and presently as a sessions court judge. The researcher therefore was in the most advantageous position whereby the researcher would purposefully and carefully watch the process of use, admission and proof of electronic evidence to draw out factual statements with adequate evidence. The observation was primarily participant and non structured. However when using the interview techniques and case study methods or whilst conducting field study at forensic labs, Police stations and Malkhanas the observation was non participant observation.

### 1.6.4 Case Study Method

Based on these interviews as well as by resorting to participant and non participant research, the researcher has conducted case studies of relevant cases pending in the court of North and South Goa district. The purpose was to ascertain the manner in which certain forms of electronic evidence is produced in these cases. In the process the researcher also found certain civil cases where some intriguing questions on the manner in which electronic evidence is produced and appreciated in those cases. For case study method the researcher used the non probability sampling technique and convenience sampling sub technique.

### 1.6.5. Empirical Data from Custodian Primary Sources

The research needed foundational data essentially, empirical in nature, from various stakeholders and Government Departments. Here the researcher with the aid of Right to Information Act and request letters has obtained the same form the various legal custodians of that data. These Departments include, the Police Headquarters, Cyber Crime Cell, Goa Forensic Science Laboratory, North and South Goa District Courts, Directorate of Prosecution, Goa. Directorate of Information and Technology Goa.

### 1.6.6 Doctrinal Research Method

Doctrinal Research was conducted by studying Legislations namely the Indian Evidence Act 1872, Indian Penal Code 1860, Criminal Procedure Code 1973, Information Technology Act 2000, Bankers Book Evidence Act 1891, and Criminal and Civil Manual. In addition to that the researcher referred to articles in law journals and magazines, dictionaries, Government Notifications, Official Gazettes, Information published on Government websites and other relevant websites. The researcher also studied Judgements delivered by the Hon'ble Supreme Court and various high courts of India on the subject of electronic evidence.

## 1.7 Scope of Study

The present study was limited to the State of Goa. Goa covers an areas of 3702 square kilometers and comprises of two revenue districts namely North Goa and South Goa. The North Goa revenue district consists of 6 talukas and South Goa revenue district consists of 6 talukas.

Judicially, Goa is again divided into two districts. North Goa judicial district consisting of talukas, Tiswadi, Bardez, Bicholim, Pernem, Valpoi and Ponda and Darbandora. There is no seperate court for Darbandora Taluka and it falls within the jurisdiction of

Ponda Taluka. The South Goa judicial district consists of 5 talukas namely, Salcete, Quepem,Sanguem, Canacona and Vasco. The district headquarters of North Goa district is Panaji. Whereas the district headquarters of South Goa district is Margao. In the present research, survey statistics were gathered with respect to the entire State of Goa. The area covered for the field survey is based on random sampling method and the researcher does not claim to have taken a representative sample of every taluka. This however has no impact on the authenticity of the results as the yardstick for the results are not demographic or geographical considerations. The study has been carried out for a period of 7.6 years ranging from February 2015 to June 2022.

### 1.8 Review of Existing Literature

The researcher reviewed five relevant thesis and articles. The access to thesis was obtained from the Shodganga website[3] that is the authorised repository of thesis submitted and published by various universities in India. The researcher also reviewed five articles that were available for reading on reputed online legal journals.

#### 1.8.1 Research Papers and Thesis.

*Sarma, Archana*[4], in her research examines the fitness of Computer forensics as a new branch of forensic science in resolving the challenges in admission of electronic evidence in courts in India. The researcher has discussed in detail the procedure adopted by computer forensic investigators in forensic laboratories and has tried to ascertain whether this is uniformly done in compliance with rules of evidence. She has focused on the application and use of forensic science in the process of admission of electronic evidence in courts. The researcher has also discussed various case laws and has tried to

[3] https://shodhganga.inflibnet.ac.in
[4] Sarma, Archana, *Computer Forensics in Criminal Investigation And Admissibility Electronic Evidence In India*, National Law University Delhi 2019. *http://hdl.handle.net/10603/351813* accessed on 12th December 2020 at 10.00 pm.

examine the challenges that are faced by law enforcement agencies in India in the process of handling electronic evidence. Lastly, the researcher has suggested legislative changes and set of guidelines for all agencies to ensure better utility of electronic evidence in courts

The research of *Shri M.Ramasubramani*[5] is exclusively based on cyber crimes and the role of Tamil Nadu Police in investigating cyber crimes. The researcher has gathered statistics of cyber crimes and has resorted to case study method to enunciate the different kinds of cyber crimes and how they were investigated. The perspective of the research is essentially socio legal in nature and therefore the conclusions drawn and the suggestions made tilt towards reduction of cyber crimes.

*Ramrao, Wagh Jitendra*[6] has conducted an analytical study on the concept of cybercrimes specifically. As the title suggests this research is confined to cyberlaws and cyber crimes. The thesis innovatively dwells into the aspect of criminological analysis of cyber crimes. In addition to carrying out critical and doctrinal research the researcher has used case study method to illustrate how courts in India have handled issues of cyber crimes.

*Chaudhary, Arvindeka*,[7] in his thesis has confined himself broadly to the use of scientific techniques of investigation and specifically the use of Narco-analysis, Polygraph and Brain Mapping. The researcher has studied the status of admissibility of 'Scientific Evidence' under Indian Evidence Law with the help of case studies and further examined the constitutional validity of all these techniques vis a vis the right of the accused. The researcher has done a comparative analysis of the law in this regard

---

[5] Shri M.Ramasubramani, *A Study On Police Administration Of Tamil Nadu With Specific Reference To Cybercrime Management In Chennai City*, Department Of Public Administration, University Of Madras *http://hdl.Handle.Net/10603/272740* accessed on 12th December 2020 at 10.30 pm.

[6] Ramrao, Wagh Jitendra, *Analytical Study On The Concept Of Cybercrimes Under The Criminal Law Of India With Reference To Information Technology Act 2000*, Department Of Law Department Of Law Swami Ramanand Teerth Marathwada *University http://hdl.Handle.Net/10603/217733 Accessed On 13th December 2020 At 10.00 Pm.*

[7] Chaudhary Arvindeka, *Admissibility of Scientific Evidence under Indian Evidence Act 1872* Department of Law, Guru Nanak Dev University *http://hdl.handle.net/10603/102549 Accessed On13th December 2020 at 11.00 pm.*

vis a vis the position in foreign countries. There is however no reference to electronic form of evidence.

*Kumar, Naresh*,[8] has essentially confined himself to cyber crimes only. The researcher has critically analyzed cyber crime legislations not on in India but has also considered it from international perspective. At the outset the researcher examines the definition of cyber crime and thereafter goes into the aspect of its classification and characteristics. The researcher touches upon the quintessential issue of global reach of cyber crimes and the issues of jurisdiction. The researcher thereafter introspects how regulating a cyber crime is a global challenge and how various authorities such as G8, UN, European Union, etc have attempted to tackle it. The researcher finally calls out for global cooperation in harmonizing laws relating to cyber crime and the need for better enforcement of the Information Technology Act.

### 1.8.2 Research Articles.

*Vikas Upadhyay* and *Prakash Upadhyay* [9] in their research paper trace the interpretation of section 65B that deals with admissibility of electronic evidence since its enactment by the courts of law. The Article examines the challenges that the section originally posed and how the challenges where explored by the Hon'bble Supreme Court of India in their various precedents. The article exposes the paradoxes that are encountered as a result of the overruling of the previous judgment of the Supreme Court that made electronic records admissible without a certificate under section 65 B of the Indian Evidence Act.

---

[8] Kumar, Naresh, *Control Of Cyber Crimes - A Study Of Cyber Legislations In India*, Department Of Law Jagannath University *Http://hdl.Handle.Net/10603/130487 Accessed On 12.5.2016 At 11.00 Pm.*

[9] Vikas Upadhyay And Prakash Upadhyay, *Changing Facades Of Law On Admissibility Of Electronic Evidence*. 2021 SCC Online Blog Op Ed 53 *https://ww.scconline.Com/Blog/Post/2021/03/13/Electronic-Evidence/ As On 21.5.2021*. Accessed On14th May 2021 At 11.30 pm.

*Ashwini Vaidialingam*[10] in her article makes a critical review the judgment of the Hon'ble Supreme Court in P.V. Anvar v. P.K. Basheer[11] and its application to pending cases. The article gives a step by step insight on how the judgment will have repercussions on the different issues relating to production of electronic evidence. According to the author the judgment has not stated the position of law correctly although the intent of the judgment was right. The dictum of the Hon'ble Supreme Court that certificate under section 65B is the only method to admit secondary evidence of an electronic record is found to be flawed by the author in her article and she has raised points in support of her argument.

*Dubey V.*[12], in this article discusses the concept of evidence under the Indian Evidence Act and proceeds to enunciate the concept of electronic evidence. The article discusses various judgements of the Supreme Court that have interpreted the meaning and import of section 65B of the Indian Evidence Act. The article is basically elucidative or explanatory in nature.

*Nibras Salim Khudhair*[13] traces the issue of admissibility of electronic evidence in India through case laws and further makes a comparative analysis of the same in jurisdictions of United Kingdom, United States of America and Canada. The author has appreciated the Canadian system of admissibility and proof which has a system-integrity in matter of issuance of a certificate this is particularly useful when the original is in possession of a neutral third party.

---

[10] Ashwini Vaidialingam, *Authenticating Electronic Evidence: §65B, Indian Evidence Act, 1872*, 8 NUJS L.Rev. 43 (2015) *Http://Nujslawreview.Org/2016/11/06/Authenticating-Electronic-Evidence/65b-Indian-Evidence-Act-1872/* Accessed On 02.01.2016 at 10.00 pm

[11] 2014 10 SCC 473

[12] Dubey V. "*Admissibility Of Electronic Evidence: An Indian Perspective*" Forensic Research & Criminology International Journal *eISSN:2469-2794: 10.15406/frcij.2017.04.0010* Accessed On 02.01.2016 at 11.30 pm.

[13] Nibras Salim Khudhair, *Revisiting the Admissibility of Electronic Evidence: Indian Jurisdictions & Notes from Other Countries* PSYCHOLOGY AND EDUCATION (2021) Volume 58(5), ISSN 1553 - 693 *on http://psychologyandeducation.net/pae/index.php/pae/article/view/5462/4711* Accessed on 21.11.2021 at 1.00 am

*Shweta and Tauseef Ahmad,*[14] have enunciated the Indian law on admissibility of evidence. The author has discussed the amendments brought about by the Information Technology Act. She has also done a comparative analysis with the laws of UK and US and had discussed judgments of various courts.

### 1.8.3 Summary of Literature Review

At the outset it would be relevant to state that when the researcher submitted her first chapter there were a very few thesis and articles on this subject. However before the final submission the researcher relooked for the existing work of other research scholars and have also reviewed the same. Most of the theses were accessed from the repository of thesis of University Grants Commission "Shodganga". The articles are from online legal journals of repute.

Except one thesis that makes an attempt to touch upon evidentiary aspects of electronic evidence the researcher found that there is no research made in India till date on the subject of use admissibility and proof of electronic record in courts. That research emphasized on the forensic aspects of electronic evidence. The researcher has made an honest attempt to bridge this gap and look at the practical aspects and challenges with regard to production of electronic evidence in Courts. The research though empirically is restricted to the State of Goa nonetheless certain propositions deduced herein will have universal application.

## 1.9 Utility of the Research

The research is conducted for suggesting legislative and administrative changes for effective use of electronic evidence in investigation and trial. It is also conducted to as far as possible provide solutions to contemporary problems with use of available

[14]Shweta and Tauseef Ahmad, *Relevancy and Admissibility Of Digital Evidence: A Comparative Study* 2018 IJLMH | Volume 2, Issue 1 | ISSN: 2581-5369 *https://www.ijlmh.com/relevancy-and-admissibility-of-digital-evidence-a-comparative-study* Assessed on 21.5.2020 at 10.00 pm

resources and legislation. The larger endeavour of the researcher is to commence a debate on this novel subject that does not seamlessly trade the path of justice as is done by conventional form of evidence.

### 1.10 Chapterisation

In an attempt to underscore and analyse the time gap between the existing laws and advent of electronic technology, this research paper has been organised into 6 chapters including introduction and conclusion.

### Chapter 1: Introduction

This chapter shall give a concise yet fairly comprehensive exposition of the concept of evidence in general and then proceed to explain how electronic evidence is different from regular forms of evidence. It shall provide an insight of the nature of the subject that the researcher proposes to study.In the end, this chapter shall also outline the reasons behind this research, the objectives of the study, the research methodology and the scope of study, utility of research and further give a brief overview of all the chapters.

### Chapter 2: The Scope of Admissibility and Proof of Electronic Evidence under the Indian Law

This chapter traces the change in the judicial outlook towards the use of electronic evidence in India by discussing case laws on section 65B of Indian Evidence Act. The chapter shall begin with a discussion on types of evidence recognised under the Indian Evidence Act, concepts of relevancy, admissibility and mode of proof. Thereafter there shall be a brief discussion on the concept of electronic evidence and the significance of the introduction of the word electronic record in definition of a "documentary

evidence". The chapter shall examine the role of section 65B in proving secondary evidence of primary electronic record and shall conclude with a study of judicial precedents on this subject.

**Chapter 3: International Conventions and Model Laws on Electronic Evidence and the Genesis of Indian Law.**

This chapter shall trace the evolution of the law on electronic evidence expressed globally in Conventions and treatises. There after the chapter shall briefly assess its impact on the Indian law of electronic evidence when it was enacted. Lastly the chapter shall succinctly discuss the Information Technology Act 2000 the enactment of which gave statutory recognition to the concept of electronic evidence.

**Chapter 4: Seizure, Production and Evidentiary Aspects of Electronic Evidence**

This chapter shall discuss the manner in which electronic evidence is produced and proved in the court. The chapter shall begin with the modes employed by the Police for seizure of electronic record as that constitutes the edifice of the entire superstructure of admissibility and mode of proof. Thereafter the next part of the chapter will take a cursory look at evidentiary aspects of various forms of electronic records and the modes used by the courts to admit and authenticate electronic records. This part of research is based on interviews taken, participant and non participant observation and lastly case studies. The Chapter shall end with case studies of sample size cases tried in courts in Goa involving electronic evidence.

**Chapter 5: Data Analysis And Findings: Comparison Of Idealism With Practical Reality.**

This chapter shall contain an analytical scrutiny of the data obtained. In this chapter an

assessment shall be made of the factors that cause impediments in optimum use and authentication of electronic evidence at substantive and procedural levels. This chapter shall test research questions and hypothesis and shall examine the roadblocks that are encountered in the optimum use of scientific and electronic evidence at pre trial and trial stage.

**Chapter 6: Conclusion and Suggestions**

This chapter shall consist of inferences and conclusions drawn based on the research undertaken. In the later part of the chapter the researcher shall suggest changes in approach, perspective and law if needed for effective use of electronic evidence in investigation and trial.

**1.11 Limitations of Study:**

It is clarified that stakeholders, namely lawyers, Judicial Officers, Prosecutors and Police who face difficulties may technologically challenged or their technical knowhow may be limited to day to day use of computers only. The researcher too falls in this category. Thus an attempt is consciously made to refrain from digressing into technical aspects of electronic evidence that may require expertise in information and technology. The research traces the journey of an “electronic record” as a potent form of evidence from the time it is seized by the Police, till the point it is appreciated in evidence by the Court. In this journey two more stakeholders namely prosecutors and lawyers assist in making the electronic record admissible and appreciable.

The present thesis is therefore confined to only that facet of electronic evidence that deals with its seizure, production and appreciation in evidence as a part of court process. Considering that the concept of electronic evidence calls out for a need of technical expertise and knowledge of computers, the researcher is conscious that the research is conducted in the field of law, therefore there is a deliberate attempt to keep the technical references as minimal as possible. The research is conducted from a point of view of a

jurist, as the intent is to make it beneficial to the class of persons who have to routinely deal with issues pertaining to electronic evidence, but have very limited knowledge of its technical aspects.

In the course of research it was found that the legislature while amending the Indian Evidence Act 1872 in par with the second Schedule of the Information Technology Act 2000 has ensured that there are no unwelcome references to technical terminology which is often associated with the study of computers. That is why all technical definitions are kept in the Information Technology Act, 2000 itself and have to be read there from.

Secondly, the study is also not extended to the operation and enactment of the Information Technology Act, Cyber laws or Cyber crimes. This domain is completely distinct to what is researched herein. There may be some portions of the Information Technology Act at have been incorporated into these thesis, but reference to these portions was imperative in view of the fact the Information Technology Act introduced amendments to the Indian Evidence Act one of which is section 65B, which forms the edifice of this research work.

Thirdly, the study is confined to attributes of justice delivery system in State of Goa. Since a part of this research is doctrinal some of the assumptions made and the principles deduced may have universal application. This is because the legislations studied by the researcher and the precedents analysed have binding authority all over the country. However the endeavour is to confine the study to the actual state of affairs that exist in the State of Goa due of time constrains and financial limitations.

Fourthly, as this study is not a comparative study. The researcher has not referred any law, rules and regulations followed by different countries on the issue of use admissibility and proof of electronic record. There is however an independent chapter dedicated to Global Conventions as these conventions have often served as a precursor for enactment of local legislations on the subject of electronic evidence.

The next chapter shall be an edifice for the superstructure of research that shall underscore the gamut of law of Evidence in India and the scope of electronic evidence under that law.

# Chapter 2

# The Scope Of Admissibility And Proof Of Electronic Evidence Under The Indian Law

## 2.1 Concept of Evidence and its Classification under the Indian Law

### 2.1.1 Definition and Scope of the term "Evidence" under the Indian Law:

Having chalked out a roadmap in the foregoing chapter this chapter elucidates the law applicable for admissibility, proof and appreciation of evidence in Courts in India.

Evidence is the usual means of proving or disproving a fact or a matter in issue. The law of evidence provides an insight into what facts a party can lawfully introduce to prove the existence of a relevant fact and also what standard of proof is imperative (quality and quantity) in proof of that fact. In short the law of evidence governs the means and manner in which a party substantiates his own case and refutes the case of another[15]. The law that governs matters relating to evidence in India is the Indian Evidence Act 1872. Evidence in the widest sense includes everything that is used to determine or demonstrate, the truth of an assertion. Giving or procuring evidence is a process of using those things that are either (a) presumed to be true or (b) were themselves proven by evidence, to demonstrate an assertion of truth[16].

Indian Evidence Act 1872, gives an inclusive definition to the term "evidence"[17]. This definition of the word evidence is not exhaustive and therefore it is not to be extended where such an extension is not warranted[18].Evidence under the Indian Law therefore

[15] Halsburys " Laws of England", 4th Edition, Vol 17, page 1
[16] Ram Jethmalani & D S Chopra, " The Law of Evidence, Commentary on Evidence Act 1872" Vol I page 28
[17] Section 3 of the Indian Evidence Act defines Evidence as .— " Evidence" means and includes—
(1) all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry, such statements are called oral evidence;
(2) all documents including electronic records produced for the inspection of the Court, such documents are called documentary evidence.
[18] Brijnandan Sinha v. Jyoti Narain AIR 1956 SC 66.

signifies only instruments by means of which relevant facts are presented before the court through witnesses and documents. The court will take into consideration statement of witnesses, contents of documents, surrounding circumstances and probabilities. Appreciation of evidence may also include inference to be drawn from a fact.

Evidence is produced to prove the existence or non existence of a fact. The Indian Evidence Act defines a "fact" to mean and include any, thing, state of things or relation of things, capable of being perceived by the senses[19]. Fact in issue, is a fact that is asserted by one party and denied by the other and the proof of which would determine the course of the finding given by the court[20].

### 2.1.2 Concepts of Relevancy and Admissibility

Evidence can only be given of relevant facts. The Indian Evidence Act does not define what a relevant fact is. It provides that a fact is said to be relevant to another when one is connected with the other in any of the ways referred to in the provisions of Indian Evidence Act relating to relevancy of facts[21]. Section 5 to Sec.55 of Indian Evidence Act provides several ways in which one fact may be connected with other facts for it to be relevant.

Facts should not be received in evidence unless they are found to be relevant and admissible[22]. Inadmissible evidence cannot be admitted in evidence even by consent of the parties[23].

Admissibility of evidence is often confused with the term relevancy. Admissible

[19] Section 2 of the Indian Evidence Act,1782
[20]Section 3 of the Indian Evidence Act defines "Facts in issue" as. —The expression "facts in issue" means and includes— any fact from which, either by itself or in connection with other facts, the existence, non-existence, nature, or extent of any right, liability, or disability, asserted or denied in any suit or proceeding, necessarily follows. Explanation.— Whenever, under the provisions of the law for the time being in force relating to Civil Procedure, [3] any Court records an issue of fact, the fact to be asserted or denied in the answer to such issue, is a fact in issue
[21] Section 5 of the Indian Evidence Act.
[22] State of U.P. v. Raj Narain AIR 1975 SC 865
[23] Bibhabati v. Ramendra AIR 1947 PC 19

evidence is that evidence that law *permits* to be produced in proof of a fact. Admissibility concerns form rather than substance. Relevancy is a substantive question of fact and is invoked to prove the existence or non existence of a fact. When on one hand, admissibility is the duty of the court to decide whether any evidence should be received by the court, on the other hand it is the primary duty of the person producing evidence to show relevancy. Relevancy is based on logical probability whereas admissibility is not based on logic, but on law and strict rules.

Relevancy is a concept that is associated with facts whereas admissibility is a concept which is associated with evidence. A fact may be relevant, but by its nature may be inadmissible. In most cases the two words admissibility and relevancy are used interchangeably with each other but their legal implication is very different. This is because often vital facts such as communication between the spouses in marriage are relevant, but not legally admissible[24]. Likewise a confession made before the police may be relevant but is inadmissible. Thus, all evidence that is admissible is relevant, but all that is relevant is not necessarily admissible. The concept of relevancy therefore is the genus of which admissibility is a species[25].

Evidence can be given only of relevant facts provided that the evidence is admissible**.** The word `evidence' is used in common parlance in three different senses: (a) as equivalent to relevancy (b) as equivalent to proof and (c) as equivalent to the material, on the basis of which courts come to a conclusion about the existence or non-existence of disputed facts.

The main function of rule of evidence is to narrow down the scope of dispute before the Court to the facts relating to that matter which have logical probative value in determining a fact and to prevent giving judgments based on illogical conclusions or prejudices. These rules aid in proper administration of justice.

---

[24] Ram Bihari Yadav v. State of Bihar AIR 1998 SC 1850

[25] Certain classes of facts which, in ordinary life, are relied upon as logically relevant are rejected by law as legally irrelevant. See sections. 91-99, sections. 115-117 and sections121-130 of the Indian Evidence Act.

### 2.1.3 Classification of Evidence Under the Indian Evidence Act

Broadly speaking, evidence has been classified in five independent categories i.e. (a) direct and circumstantial evidence (b) original and hearsay evidence (c) oral and documentary evidence, (d) primary and secondary evidence and (e) real and presumptive evidence.

### (a) Direct And Circumstantial Evidence

"Direct evidence" means that evidence that supports the existence or non existence of a fact on its own without the need of drawing inference. For example the testimony of an eyewitness that he has seen the happening of the event in question, or production of a document containing affirmation of a fact in question. Whereas "circumstantial evidence" consists of a group of facts, necessary to draw an inference about the existence or non existence of a fact in issue.

Direct evidence is ordinarily stand alone evidence. Whereas, circumstantial evidence, requires the support of several facts, so connected with each other, so as to lead to a particular inference. Judicial pronouncements have coined the word "chain of circumstances" to identify this phenomenon. It is well settled by various pronouncement of the Hon'ble Supreme court that the circumstances from which the inferences of guilt are drawn should be fully established. The Judgement in the case of ***Sharad Birdhi Chand Sarda***[26]is a leading authority on this point.

---

[26] Sharad Birdhi Chand Sarda vs State Of Maharashtra 1984 AIR 1622, 1985 SCR (1) 88 it was held that *"A close analysis of this decision would show that the following conditions must be fulfilled before a case against an accused can be said to be fully established: (1) the circumstances from which the conclusion of guilt is to be drawn should be fully established. It may be noted here that this Court indicated that the circumstances concerned "must or should" and not "may be" established. There is not only a grammatical but a legal distinction between "may be proved" and "must be or should be proved" as was held by this Court in Shivaji Sahabrao Bobade v. State of Maharashtra (1973) 2 SCC 793 where the observations were made : [SCC para 19, p. 807 : SCC (Cri) p. 1047] "19. .....Certainly, it is a primary principle that the accused must be and not merely may be guilty before a court can convict and the mental distance between 'may be' and 'must be' is long and divides vague conjectures from sure conclusions. (2)*

Direct evidence is clear and tangible and certain. Circumstantial evidence is hazy and therefore considered to be a weak form of evidence[27]. Any discovery of a relevant fact (weapon of assault) upon disclosure from the accused when combined with factors such as last seen previous enmity can be used to build a chain of circumstances to infer that the accused may have committed the crime. Direct evidence proves existence of facts in issue, without any inference or presumption.

**(b) Original And Hearsay Evidence**

Direct evidence is sometimes called original evidence arising from the personal knowledge of the witness. The antonym to this form of evidence is hearsay evidence. Every act done or spoken which is relevant on any ground must be proved by someone who saw it with his eyes and heard it with his ears. Hearsay[28] means evidence of a person who is not directly involved with the fact about which he is deposing. The information that he is giving has been obtained by him from a source whether human or otherwise[29]. This form of evidence is inadmissible in court except under circumstances enunciated under section 6, 17-23,32 and 33 of the Indian Evidence Act.

There is another term "percipient evidence" which is a term given by some authors to direct evidence having a slightly distinct meaning. It is said that this term not only

---

*the facts so established should be consistent only with the hypothesis of the guilt of the accused, that is to say, they should not be explainable on any other hypothesis except that the accused is guilty, (3) the circumstances should be of a conclusive nature and tendency, (4) they should exclude every possible hypothesis except the one to be proved, and (5) there must be a chain of evidence so complete as not to leave any reasonable ground for the conclusion consistent with the innocence of the accused and must show that in all human probability the act must have been done by the accused."*

[27] In Hanumat's v. State of M.P. [1953] SCR 1091 it was held that these five golden principles constitute the panch-sheel of the proof of a case based on circumstantial evidence and in the absence of a corpus deliciti.

[28] Merriam Websters dictionary defines hearsay as evidence based not on a witness's personal knowledge but on another's statement not made under oath

[29] Subramaniam v. Public Prosecutor, (1956) 1 WLR 965 which was referred to in Rabindra Nath Thakur v. Union of India, 1998 SCC OnLine Pat 580 it was held that Evidence of a statement made to a witness by a person who is not himself called as a witness may or may not be hearsay. It is hearsay and inadmissible when the object of the evidence is to establish the truth of what is contained in the statement. It is not hearsay and is admissible when it is proposed to establish by the evidence, not the truth of the statement, but the fact that it was made.

avoids any possibility of confusion but is also more appropriate to describe the opposite of hearsay evidence. "Percipient evidence" is evidence of fact which a witness personally perceives using any of his senses. "Indirect evidence" also known as substantial evidence is that which gives rise to a logical inference that such fact exists. "Substantial evidence" may be either "conclusive" or "presumptive". It is conclusive when there is connection between principal fact and the evidentiary fact. The effect of substantial evidence on consideration must be such as not to admit more than one solution and must be inconsistent with any explanation that the fact is not proved. By direct or presumptive evidence one may say that other facts are disapproved from which existence of given facts may be logically inferred.

**(c) Oral And Documentary Evidence**

The idea of best evidence is implicitly ingrained in the Indian Evidence Act. Evidence consists of statements made by a witness ( oral evidence) or contained in a document(documentary evidence). Infact the definition of the term "Evidence" under the Indian Evidence Act defines the terms oral evidence and documentary evidence.

The Indian law only permits direct oral evidence as admissible. Therefore in case of oral evidence, the Act requires that only that person, who has actually seen, heard, felt or opined a particular fact has to depose about that fact for the fact to be admissible[30]. If the fact is deposed by a person whose source of information is not firsthand the evidence is rejected as heresay. There are however exceptions to this rule contained in

[30] Section 60 of the Indian Evidence Act states that "Oral evidence must, in all cases whatever, be direct; that is to say-- If it refers to a fact which could be seen, it must be the evidence of a witness who says he saw it; If it refers to a fact which could be heard, it must be the evidence of a witness who says he heard it; If it refers to a fact which could be perceived by any other sense or in any other manner, it must be the evidence of a witness who says he perceived it by that sense or in that manner; If it refers to an opinion or to the grounds on which that opinion is held, it must be the evidence of the person who holds that opinion on those grounds: Provided that the opinions of experts expressed in any treatise commonly offered for sate, and the grounds on which such opinions are held, may be proved by the production of such treatises if the author is dead or cannot be found, or has become incapable of giving evidence, or cannot be called as a witness without an amount of delay or expense which the Court regards as unreasonable: Provided also that, if oral evidence refers to the existence or condition of any material thing other than a document, the Court may, if it thinks fit, require the production of such material thing for its inspection."

section 32 and 27 of the Indian Evidence Act.

The term Document[31] and documentary evidence[32] has been given two separate definitions under the Indian Evidence Act. The term "document" as per section 3 means a matter that is expressed or described on any substance by use of letters, figures or marks, for the purpose of recording the matter whereas Documentary evidence means all documents produced for the inspection of the Court. Documentary evidence includes electronic records. The definition of the term documentary evidence is inclusive.

**(d) Primary And Secondary Evidence**

The law enjoins that contents of a document may be proved by the primary or secondary evidence[33]. In case a fact is sought to be proved through documentary evidence, the Indian Evidence Act requires that ordinarily the original should be produced. Section 62 defines what is Primary evidence [34]. The Indian Evidence Act uses the word "primary" only in the context of documentary evidence.

---

[31] Section 3 of the Indian Evidence Act defines the word "document" as "Document" means any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter. *Illustrations* A writing is a document; Words printed lithographed or photographed are documents; A map or plan is a document; An inscription on a metal plate or stone is a document; A caricature is a document.

[32] Section 3 defines evidence as " Evidence" means and includes—(1) all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry, such statements are called oral evidence; (2) all documents including electronic records produced for the inspection of the Court], such documents are called documentary evidence

[33] Section 61 of the Indian Evidence Act

[34] Section 62 of The Indian Evidence Act defines primary evidence as : Primary evidence means the document itself produced for the inspection of the Court. Explanation 1.—Where a document is executed in several parts, each part is primary evidence of the document; Where a document is executed in counterpart, each counterpart being executed by one or some of the parties only, each counterpart is primary evidence as against the parties executing it. Explanation 2.—Where a number of documents are all made by one uniform process, as in the case of printing, lithography, or photography, each is primary evidence of the contents of the rest; but, where they are all copies of a common original, they are not primary evidence of the contents of the original. Illustration A person is shown to have been in possession of a number of placards, all printed at one time from one original. Any one of the placards is primary evidence of the contents of any other, but no one of them is primary evidence of the contents of the original.

Secondary Evidence is defined under section 63 of the Indian Evidence Act[35]. If primary evidence is not available, the law permits production of secondary evidence under the circumstances mentioned under section 65 of the Indian Evidence Act[36]. The idea of introducing section 65 in the Indian Evidence Act is to ensure that the best evidence is not left out due to the rigor of section 62 of the Indian Evidence Act.

Next issue is the proof of contents of a document. Proof of document involves two

---

[35] 63. Secondary evidence.—Secondary evidence means and includes—
(1) Certified copies given under the provisions hereinafter contained
(2) Copies made from the original by mechanical processes which in themselves insure the accuracy of the copy, and copies compared with such copies;
(3) Copies made from or compared with the original;
(4) Counterparts of documents as against the parties who did not execute them;
(5) Oral accounts of the contents of a document given by some person who has himself seen it.
Illustrations
(a) A photograph of an original is secondary evidence of its contents, though the two have not been compared, if it is proved that the thing photographed was the original.
(b) A copy compared with a copy of a letter made by a copying machine is secondary evidence of the contents of the letter, if it is shown that the copy made by the copying machine was made from the original.
(c) A copy transcribed from a copy, but afterwards compared with the original, is secondary evidence; but the copy not so compared is not secondary evidence of the original, although the copy from which it was transcribed was compared with the original.
(d) Neither an oral account of a copy compared with the original, nor an oral account of a photograph or machine-copy of the original, is secondary evidence of the original.

[36] Section 65. Cases in which secondary evidence relating to documents may be given.—Secondary evidence may be given of the existence, condition, or contents of a document in the following cases:—
(a) When the original is shown or appears to be in the possession or power— of the person against whom the document is sought to be proved, or of any person out of reach of, or not subject to, the process of the Court, or of any person legally bound to produce it, and when, after the notice mentioned in section 66, such person does not produce it;
(b) when the existence, condition or contents of the original have been proved to be admitted in writing by the person against whom it is proved or by his representative in interest;
(c) when the original has been destroyed or lost, or when the party offering evidence of its contents cannot, for any other reason not arising from his own default or neglect, produce it in reasonable time;
(d) when the original is of such a nature as not to be easily movable;
(e) when the original is a public document within the meaning of section 74;
(f) when the original is a document of which a certified copy is permitted by this Act, or by any other law in force in 1[India] to be given in evidence; 1[India] to be given in evidence;"
(g) when the originals consists of numerous accounts or other documents which cannot conveniently be examined in Court, and the fact to be proved is the general result of the whole collection. In cases (a), (c) and (d), any secondary evidence of the contents of the document is admissible. In case (b), the written admission is admissible. In case (e) or (f), a certified copy of the document, but no other kind of secondary evidence, is admissible. In case (g), evidence may be given as to the general result of the documents by any person who has examined them, and who is skilled in the examination of such documents

aspects. First is the proof of its genuineness and second is the proof of its contents. Where the document itself is produced before the court no further proof of its genuineness is required. However if the original document is destroyed, lost, or cannot be conveniently produced a copy thereof may be admissible in case the same is produced in compliance with section 63-65 of the Indian Evidence Act, in such a case its genuineness has to be proved under the Indian Evidence Act.

When a document is produced in evidence it passes through two stages. One is the stage when all the documents on which the parties rely are filed by them in Court. The subsequent stage is when the documents are tendered in evidence by the witness. It is at this later stage that the Court has to decide whether they should be admitted or rejected. If they are admitted the court marks the document as an exhibit and endorses on the document that the document is admitted in evidence[37]. In case the document is inadmissible it is rejected by putting an endorsement on the document and returned to the party.[38]. The court admits only primary documentary evidence. Secondary evidence is admitted only when it complies with the diktat of section 65 and 66 of the Indian Evidence Act.

Evidence either oral or documentary is tendered by the witness in the court. When such evidence is tendered the court has a twofold responsibility. Firstly to gauge the form of evidence produced and determine its admissibility and thereafter examine whether the evidence tendered is sufficiently proved.

---

[37] In Sudhir Engineering Company v. Nitco Roadways Ltd. 1995 IIAD Delhi 189 it was held that Any document filed by either party passes through three stages before it is held proved or disproved. These are : First stage : when the documents arc Filed by either party in the Court; these documents though on file, do not become part of the judicial record; Second stage: when the documents are tendered or produced m evidence by a party and the Court admits the documents in evidence. A .document admitted in evidence becomes a part of the judicial record of the case and constitutes evidence. Third stage: the documents which are held 'proved, not proved or disproved' when the Court is called upon to apply its judicial mind by reference to Section 3 of the Evidence Act. Usually this stage arrives 31 the final hearing of the suit or proceeding.

[38] Baldeo Sahai v. Ram Chander & Ors., AIR 1931 Lahore 546; see also Order 13 Rule 4 Civil Procedure Code

There cannot be further proof of a fact that is orally stated on oath[39]. Whereas when a fact is contained in a document it has to be proved in the manner as provided under the Indian Evidence Act. At this juncture it may be pointed that a thorough discussion on this aspect is necessary in the context of this research because an electronic record is classified as documentary evidence by the law makers.

For a document to be admissible in evidence the document has to either be primary or secondary. When a document is tendered in evidence, an objection to the admissibility of evidence should be taken when it is tendered and not subsequently. The objections as to admissibility of documents in evidence may be classified into two classes: (i) an objection that the document is inadmissible in evidence; and/or (ii) the objection that the party does not dispute the admissibility of the document in evidence but disputes its contents. In other words the contents of the document have to be proved as per law.

The former objection has to be decided by the court at that instance itself before marking the document in evidence whereas the later objection being a question of fact can be postponed for decision till the culmination of trial. A necessary corollary to this principle therefore is that objection to the proof of a document has to be taken at the first instance, if not taken the objection will have to be deemed to have been waived. An objection as to the mode of proof being procedural can be waived and therefore it cannot be taken for the first time in appeal[40]. The Hon'ble High court of Bombay set to rest the conflicting decisions on the admissibility, proof and impounding of documents in the case of ***Hemendra Rasiklal Ghia*** .[41]

In that case the court formulated two questions, the first being at what stage the court should consider objection as to admissibility and or proof of a document has to be raised by a party and considered by the court and the second was at what stage objections as to the admissibility and relevancy of evidence contained in affidavit in evidence under

---

[39] Section 59 Indian Evidence Act,- All facts expect contents of a documents and electronic records have to be proved by oral evidence

[40] Smt. Dayamathi ..Vs.. K. M. Shaffi, A.I.R. 2004 S.C. 4082,

[41] Hemendra Rasiklal Ghia & Others Vs. Subodh Modi & Oths 2008 (6) Mh.L.J., 886

Order XVIII Rule 4 of CPC should be considered by the court[42].

The genuineness of a document produced as secondary evidence is established by resorting to the process established by sections 67 to 73 of the Indian Evidence Act, and its contents is proved by means of independent direct or circumstantial evidence. The contents of a document can be proved by admission[43], examination of the author/signatory of the document[44], examination of persons who have witnessed the execution/generation of the document where the document has to be attested by law[45], examination of persons who are conversant or acquainted with the signature or handwriting[46], where the signature and handwriting is a fact in issue, comparison by the court of the admitted and disputed signature[47] and lastly by examining an handwriting experts[48]. Contents of public documents[49]may be proved by producing certified copies thereof[50]. Documents of which the court can take judicial notice need not be proved[51].

Though, under section 17 of the Indian Evidence Act , an admission can be oral or written, under S.22 an oral admission as to the contents of the document is not permitted unless(a) the party proving the document shows that he is entitled to prove them by secondary evidence or (b) the genuineness of the document is in question. Likewise oral admissions as to the contents of electronic records are also not relevant, unless the genuineness of the electronic record produced is in question[52].Section 65 (b) of the Indian Evidence Act requires that the admission must be a written one. Under S.70,

---

[42] In Hemendra Rasiklal (supra) it was held that (i) objection to the document sought to be produced relating to the deficiency of stamp duty must be taken when the document is tendered in evidence and such objection must be judicially determined before it is marked as exhibit;(ii) Objection relating to the proof of document of which admissibility is not in dispute must be taken and judicially determined when it is marked as exhibit;(iii) Objection to the document which in itself is inadmissible in evidence can be admitted at any stage of the suit reserving decision on question until final judgment in the case.
[43] Section 58 of Indian Evidence Act provides that facts admitted need not be proved.
[44] Section 67 of Indian Evidence Act 1872
[45] Section 68 Ibid
[46] Section 47 ibid
[47] Section 73 ibid
[48] Section 45 ibid
[49] Section 74 of the Indian Evidence Act defines Public document documents.
[50] Section 77 of the Indian Evidence Act.
[51] Section 56 and 57 ibid
[52] Section 22A ibid

admission by the party of the execution by himself dispenses with the proof of its attestation.

**(e)Real And Presumptive**

The next category of evidence is real and presumptive evidence. Real evidence is the evidence produced in court to prove a fact. Presumptive evidence is a fiction of law which presumes a fact to be true unless proved as false. Sections 79 to 90 of the Indian Evidence Act deal with presumptions genuine of certain categories of documents[53]. These presumptions are not substitute to the requirement of proof. These presumptions only displace the burden. A presumption is an inference of a fact drawn from a known or proved fact. Presumptions are of two types namely rebuttable presumptions and irrebutable presumptions also known as "conclusive proof"[54]. The Indian Evidence Act uses two forms of rebuttable presumptions, "shall presume" and "may presume". The former are in the nature of compelling presumptions or presumptions of law and the later are in the nature of permissive presumptions or presumptions of fact. Raising a presumption dispenses with proof, the extent of which depends upon the type of presumption.

[53] Section 79. Presumption as to genuineness of certified copies, Section 80. Presumption as to documents produced as record of evidence Section 81. Presumption as to Gazettes, newspapers, private Acts of Parliament and other documents. Section — 81A. Presumption as to Gazettes in electronic forms Section 82. Presumption as to document admissible in England without proof of seal or signature. Section 83. Presumption as to maps or plans made by authority of Government. Section 84. Presumption as to collections of laws and reports of decisions. Section 85. Presumption as to powers-of-attorney. Section 85A. Presumption as to electronic agreements. Section 85B. Presumption as to electronic records and 5[electronic signatures]. Section 85C. Presumption as to 6[Electronic Signature Certificates]. Section 86. Presumption as to certified copies of foreign judicial records, Section 87. Presumption as to books, maps and charts. Section 88. Presumption as to telegraphic messages. Section 88A. Presumption as to electronic messages. Section 89. Presumption as to due execution, etc., of documents not produced. Section 90. Presumption as to documents thirty years old.

[54] Section 4 of the Indian Evidence Act - "May presume" Whenever it is proved by this Act that Court may presume a fact, it may either regard such fact as proved, unless and until it is disproved, or may call for proof of it. "Shall presume".—whenever it is directed by this Act that the Court shall presume a fact, it shall regard such fact as proved, unless and until it is disproved. "Conclusive proof.—When one fact is declared by this Act to be conclusive proof of another, the Court shall, on proof of the one fact, regard the other as proved, and shall not allow evidence to be given for the purpose of disproving it.

### 2.1.4 Burden Of Proof:

A discussion on the concept of evidence is incomplete without addressing the concept of burden of proof. Burden of proof simply means the primary responsibility in chronology, during a trial, to prove a fact. In an adversarial system which involves assertion of a fact by one party and the denial of a fact by another, it is imperative to identify on whom the burden to prove a fact lies. Burden of proof[55] is defined under section 101 of the Indian Evidence Act. The general rule is that the burden to prove a case lies on the person who will fail if no evidence is led from either side[56]. Section 102 to 114 A of the Indian Evidence Act deal with various presumptions.

Since the researcher has essentially based her research only on criminal cases one of the cardinal principles of burden of proof in criminal cases is that an accused is always presumed to be innocent unless proved guilty. This presumption is a presumption of practice as the level of proof required in criminal cases is beyond reasonable doubt, unlike civil cases where a fact could be proved on balance of probabilities.

There are certain cases in which statutory presumptions that can be raised in criminal cases in respect of certain facts. But even in such cases the burden is upon the prosecution to prove the existence of facts which have to be present before the presumption can be drawn[57]. Once those facts are shown by the prosecution to exist, the Court can raise the statutory presumption and it would be for the accused to rebut the presumption. Even in such cases the onus upon the accused is not as heavy as is normally upon the prosecution to prove the guilt of the accused. If some material is brought on the record consistent with the innocence of the accused which may

[55] Section 101 of the Indian Evidence Act defines burden of proof as "Whoever desires any Court to give judgment as to any legal right or liability dependent on the existence of facts which he asserts, must prove that those facts exist. When a person is bound to prove the existence of any fact, it is said that the burden of proof lies on that person".
[56] Section 102 of the Indian Evidence Act.
[57] The only exception to this proposition are cases based on conclusive proof.

reasonably be true, the accused would be entitled to an acquittal[58].

Therefore the entire law of evidence is a catalyst in the quest of justice. It is through the auspices of the rules of evidence, the conundrum of facts reach its comprehendible form so as to enable to court to give a finding on conflicting issues.

## 2.2 Concept Of Electronic Evidence:

### 2.2.1 Meaning and Scope

Until the year 2000 the Indian Evidence Act catered to the requirement of proof of fact by oral and documentary evidence only. The emergent usage of technology and its production in its myriad tangible forms as evidence in court, created a need for a statutory torchlight that would simply and lead us to the path of easy appreciation and application in the course of trial. The Information Technology Act in the year 2000 amended the definition of "documentary evidence" in Indian Evidence Act to include in it the term "electronic records". This amendment has opened the portals of the old Indian statutory law to a new breed of evidence and has paved a way for development of a new perspective on the issues of admissibility and mode of proof.

In common parlance the term electronic evidence and digital evidence[59] are used interchangeably. Neither the term digital evidence nor electronic evidence is statutorily defined in India. The Information Technology Act defines the term electronic record. This observation is essential because in the year 2009 the word “digital” that was incorporated by amendments in the year 2000 in the Indian Evidence Act was replaced with the word “electronic”. Electronic in the context of a computer is anything that is generated, created or stored electronically by a computer or magnetic or optical storage

[58] Kali Ram v. State of Himachal Pradesh [(1973) 2 SCC 808

[59] Digital evidence or electronic evidence is any probative information stored or transmitted in digital form that a party to a court case may use at trial .Casey, Eoghan (2004). Digital Evidence and Computer Crime, Second Edition. Elsevier. ISBN 0-12-163104-4. *https://en.wikipedia.org/wiki/Digital_evidence* Accessed at 4.30 pm. on 16.01.2020.

devices.

The word computer herein has to be used in the widest possible sense. And must include any electronic device that stores manipulates or transmits data.

Some insight into the term digital is necessary at this juncture. Wikipedia defines digital system as a system that stores data in a discreet way. This discrete way could be the use of binary numbers (1,0), non numeric symbols such as letters or icons, for input, processing, transmission, storage or display, rather than continuous spectrum of values.

The word digital is often used in computing and in the field of electronics, in which readable data is converted to binary numeric forms. Here data could mean audio as well as videographic data which can be discerned by the human mind and is indiscreet. The term often meant by the prefix "e" as in email and e-book even though not all electronic systems are digital[60].

Likewise there is a profound difference between the term Electronic signature and digital signature. The main difference between the two is that digital signature is authorised by statutory certification authorities and is mainly used to secure documents and whereas an electronic signature is electronic process which may be a symbol, or sound representing the intention of a party to sign a contract. For example a digital signature will have a public and private key issued by certifying authorities under the Information Technology Act, whereas a classic case of electronic signature is when we click “yes” or “ok” on a licensed of an application downloaded on our computer.

Therefore to sum it up electronic evidence or digital evidence is any data that is generated, transmitted or stored using a computer which data is a relevant fact in issue in a trial of a case. The data referred herein covers a combination of numbers that represent information held in digital format such as text image audio and video files.

[60] Dr Gupta and Agarwal, “Electronic Evidence (Law and Practice)” Premier Publishing Company 2018.

### 2.2.2 The Difference Between Physical and Electronic Evidence.

At the outset it is clarified that physical evidence herein means conventional documentary evidence and may also refer to any physical object.

**a. Not created in human readable format**

Before the advent of the digital era, evidence in physical form did not offer much challenges in its interpretation and presentation. The highlight of physical evidence, whether documentary or in form of an object, is that this evidence is "human readable". The data contained in physical evidence is generated in the form in which it had been created. Whereas the data in digital format is not created in a "Human readable" format. For it to be understood by the human mind the data requires an interpreter. This interpreter is the hardware and software.

Illustratively stated when a physical document is generated by writing. The document as seen to the human eye was created in the same form. Whereas when a electronic record, say an email, is generated by typing on the keyboard. The entire process involves creation of data and meta data in binary or numeric form, which cannot be seen by the human eye. What is seen as English alphabets to us is actually a overt presentation of data created and stored in digital form ordinarily in binary format.

**b. Electronic evidence is dual in essence**

Secondly, therefore digital evidence is dual in essence**;** the form in which it is generated is not the form in which it is presented. Therefore there is a huge cloud on its dependability. Its latent form being different from the patent forms makes it vulnerable to tampering which cannot be detected by the human eye by mere observation or scrutiny. Its authenticity and integrity therefore can be easily questioned. As against this the tampering with physical evidence can easily be detected, or atleast with comparably less effort.

c. **Electronic evidence is perishable its preservation is difficult**

Thirdly, preservation of electronic evidence is a difficult task as it is ordinarily generated and stored on magnetic tapes that are prone to a greater risk of wear and tear as compared to a piece of paper. Here it is pertinent to note that if an electronic record is not used or opened for long there is always a risk of it being rendered unreadable. In the course of the research, the researcher noted that audio and video recordings stored on mobiles are produced in the court as evidence. The mobile is kept unused and unattended for a long period of time until the matter comes up for trial. At the stage of trial even if the mobile is plugged to a power source, the mobile does not switch on and valuable piece of evidence is lost. Keeping in mind the vulnerable nature of electronic evidence, certain safeguards need to be adopted to preserve its contents. Interalia if proper documentation of its contents is made in form of detailed panchanamas etc the injury caused by damage to the device will be offset to a substantial extent.

**d. Relies heavy on Technology.**

Likewise, electronic evidence, unlike physical evidence, depends upon technology to make it readable at all times. The technology used in operating systems, application software and hardware changes rapidly. As a result the data contained in an electronic record may reach a point where it cannot be read. If technology becomes obsolete there may be a problem that will affect disclosure and discovery. This problem also arises where a data (say document or audio file) has been saved in a particular format and an application for software no longer supports that format. This problem also arises in respect of hardware. The best examples are floppy disks which have now become obsolete. The non use is prevalent to such an extent that the manufactures have stopped manufacturing computers with a floppy drive.

e. **Electronic Evidence can be copied, altered, updated or deleted much easily**

Fourthly, digital evidence as compared to physical evidence can be copied, altered, updated or deleted much easily as compared to physical evidence. This alteration is so

precise and similar to the original that it cannot be easily detected without intervention of a forensic expert.

**f. Modification of Electronic Evidence can easily be detected**

However the flipside of this point is that electronic evidence leaves discernable footprints can be intercepted easily by a forensic expert, therefore the detection of this alteration, updation or deletion is fairly easy.

### 2.2.3: Advantages And Disadvantages Of Electronic Evidence Over Physical Evidence

**a) Advantages:**

i. Electronic Evidence Cannot be easily destroyed or permanently deleted.

ii. Most electronic records have a time stamp which can give an indication of the date time and modification of that record.

iii. Use of electronic records can leave a trial that can be detected through forensic techniques.

iv. Electronic records are easy to store as a bulk of the data can be compressed and saved on a small storage device.

v. Electronic records are easy to present in court (provided that they pass the test of admissibility) as they can be printed on paper.

vi. Encrypted and Hidden Data contained in an electronic record can assist in investigation.

**b) Disadvantages or Challenges:**

i. Electronic Evidence is Volatile.

ii. Electronic Evidence can be easily deleted or overwritten and cannot be retrieved easily by a non technical person.

iii. Electronic Evidence is difficult in handling requires training and tools.

iv. Electronic Evidence requires technology to make it readable.

v. Forgery and tampering of Electronic Evidence cannot be detected by human eye easily.

vi. Electronic Evidence poses challenges in production before court being new breed of evidence.

vii. Electronic Evidence is Fragile.

viii. Difficulty to prove chain of custody of Electronic Evidence.

ix. Internet investigations are the most difficult in matters pertaining to Electronic Evidence.

x. Electronic evidence is dynamic

### 2.2.4 Appreciation/Evaluation Of The Electronic Evidence.

The appreciation of electronic evidence involves consideration of five important factors namely, Relevancy, Challenge, Admissibility, Authenticity And Integrity Or Accuracy. While the first three attributes are common for physical as well as electronic evidence. The authentication, integrity or accuracy which will come under the umbrella of “mode of proof".

**a. Relevancy**:

The most vital and foremost factor that the court needs to consider is whether the electronic record is relevant to prove the fact in issue. The law relating to relevancy is contained in section 5 to section 55 of the Indian Evidence Act.

In a court case for custody of a child pending in the Court of CJM Panaji, it was seen that several bills, that were electronically generated from a grocery shop billing counter, were produced to prove that when the child was living with the father he would spend money on her. Several attempts were made to have resort to the judgement in the case of ***Mohd Shafi***[61] ( which at the relevant time was not overuled) to prove that the document is a third party document and that the same has to be accepted without a certificate. In deciding such applications the court has to consider whether such a document would be relevant in the first place in a child custody matter. If the court concludes that the electronic evidence is not relevant the same can be discarded and precious time of the court in proving the same would be saved.

**b. Challenge**

Before going into admissibility and authentication the court has to first examine whether the fact that is sought to be produced by way of electronic evidence is challenged. In civil cases the admissions are in writing in form of pleadings. Similar is the advantage in private criminal cases. Whereas in criminal cases there is no stage in the Criminal Procedure Code that requires the accused to admit documents produced, except if an application is filed by the prosecutor under section 294 of CrPC. Therefore the burden lies on the prosecution at all times to make electronic records admissible and prove them in accordance with law. Suggestions put by the accused to the witnesses and his stand taken in his 313 statement may become relevant but they cannot shift the

[61] *S*hafi Mohammad vs. The State of Himachal Pradesh,(2018) 2 SCC 801 .

onus. At the same time any admission of an electronic record made in a document proved as per law also becomes valuable.

Likewise if it is found that there is no challenge to the authenticity of electronic record produced or any of its parts or attributes, then the court can proceed to examine other aspects considering that these attributes are proved. A challenge to an electronic record can be to the authenticity of the record itself or a copy thereof. The former refers to the issue of mode of proof and the later to the issue of admissibility.

**c. Admissibility**

If no admission of the electronic record or a copy thereof is found documented in trial, nor can it be discerned from the any inference drawn out of the oral evidence produced, the court will be duty bound whether the electronic record or its copy can be admitted in evidence.

Electronic records are classified as documentary evidence. Therefore the rule that contents of documents may be proved either by primary or by secondary evidence applies to electronic documents as well. For an electronic record to be admissible in evidence, it must either be primary or secondary evidence. Strictly speaking this exercise of categorising an electronic record as primary or secondary has to be done at the time when the electronic evidence is tendered in evidence[62]. If not at this stage at least at the time of appreciation of evidence it is imperative for the court to be satisfied that the electronic evidence produced has passed the test of admissibility.

When the original electronic record is produced in evidence, no further proof of its admissibility in form of a certificate is required. However for a copy of the electronic record which is either printed or copied on a magnetic tape such as a Compact Disk, to be admissible a certificate under section 65B[63] is necessitated. As a copy by its nature is

[62] Hemendra Rasiklal. Ghia v. Subodh Mody.; 2009(3) ALJ 69 supra
[63] Section 65A of the Indian Evidence Act provides that The contents of electronic records may be proved

a secondary evidence of the original it cannot be admissible without complying with the statutory requirements[64]. Later in this chapter the researcher shall examine the import of section 65B of the Indian Evidence Act and analyse the safeguards it contains to make electronic records admissible in evidence. Suffice it to state at this point that the Hon'ble Supreme Court has time and again held that section 65A and Section 65B Indian Evidence Act is a complete code in itself and the principle of substantial compliance by resorting to other provisions of law would not be applicable to it.

**d. Proof of electronic record**

Once the court is satisfied that the electronic evidence is admissible in evidence the court will have to now satisfy itself on the aspect of its authenticity, integrity and accuracy. These aspects together come under the umbrella of the subject of "proof of electronic record".

All these phrases can be interchangeably used for the purpose of appreciation of evidence because they only intend to testify that the document is not tampered with. This issue is therefore trickiest one. There is no statutory obligation on the person producing an electronic record to prove at the time of its production that the document

---

in accordance with the provisions of section 65B (w.e.f. 17-10-2000)

[64] Unmesh Diwakar Raote vs. The Municipal Corporation of Greater Mumbai,C.S.T. & Ors. MANU/MH/2261/2018, the question was whether the photographs taken from mobile phone and downloaded in a compact disc are admissible as evidence in absence of certificate u/s 65B of IEA, 1872 or not? Considering the arguments advanced it was held that The compact disc and photographs constitute documentary evidence. However, in this case the prosecution has not furnished certificate u/s 65B of IEA, 1872 so as to prove the photographs taken from mobile phone as well as compact disc. The mandatory requirement of producing such a certificate as laid down in Anwar P.V. v. P.K. Basheer has not been adhered to, and therefore, the photographs and compact disc both were declared to be inadmissible pieces of evidence. Proof of such electronic record is not permitted by oral evidence unless and until requirements of Section 65B of the Indian Evidence Act is first and foremost complied with. Further in Faim and others v. The State of Maharashtra (MANU/MH/3080/2015). The court disallowed production of Call records in the absence of certificate under section 65B. Here the presiding judge has to meticulously examine and ascertain whether the certificate contains all the vital affirmations of section 65B(2) of the Indian Evidence Act. And further satisfy itself that the certificate issued by the person having lawful control over the computer that was used for the process of copying or transmission. Even though a cryptic of a bad certificate is a curable defect nonetheless, this precaution has to be taken at the time when the certificate is tendered in evidence.

is not tampered. The burden may be on the person alleging that the document is tampered to prove that circumstances exist for the court to have recourse to the opinion of an expert. This principle of ordinary prudence and is applied in all cases relating to proof of documentary evidence.

### 2.2.5 Burden to Prove Tampering Of Records:

When a person alleges existence of a fact the burden is on him to prove it. This is the mandate of section 101 and 102 of the Indian Evidence Act.

In the case of ***Rangammal***[65] it was held that the Evidence Act has clearly laid down that the burden of proving a fact always lies upon the person who asserts it[66].

Tampering with an electronic record is equivalent to forgery of a paper document. The term forgery is not defined in any statutes pertaining to civil law. It is defined under the Indian Penal Code which also contains certain provisions deal with making of false documents. Section 465 of the Indian Penal Code prescribes punishment for forgery. "Forged document" is defined in Section 470 Indian Penal Code while Section 471 Indian Penal Code deals with the crime of using as genuine, the forged document[67].

As the Information Technology Act has not made any significant amendments to the Indian Evidence Act in this regard, the modes of proving the integrity of the contents of a conventional document will also apply to an electronic record.

The Indian Evidence Act does not mandate that every allegation of forgery of a

---

[65] Rangammal v. Kuppuswami, (2011) 12 SCC 220

[66] It was held by the Hon'ble Supreme court in Rangammal that "Until such burden is discharged, the other party is not required to be called upon to prove his case. The court has to examine as to whether the person upon whom the burden lies has been able to discharge his burden. Until he arrives at such conclusion, he cannot proceed on the basis of weakness of the other party

[67] In Stroud's judicial Dictionary, Fifth Edition Vol. 2 the term Forgery has originated from the French word "Forger", which signifies: "to frame or fashion a thing as the smith doth his work upon the anvil and it is used in our law for the fraudulent making and publishing of false writings to the prejudice of another man's right. Webster Comprehensive Dictionary, International Edition, "Forgery' is defined as: "The act of falsely making or materially altering with intent to defraud; any writing which, if genuine, might be of legal efficacy or the foundation of a legal liability."

document has to be tested on the touchstone of expert evidence under section 45 of the Act. Whether to resort to section 45 and the consequent burden to solicit the services of an expert will depend on the interplay of section 101 and section 102 of the Indian Evidence Act as against the facts of the that case. Therefore even though the board principle is that whoever alleges forgery will have to prove the same, whether it is imperative upon him only to resort to section 45A of the Indian Evidence Act in case of electronic evidence will depend upon the facts and circumstances of the case.

In ***Saki Ammal @ Chitra***[68]***,*** A man filed a divorce petition alleging cruelty. He claimed that, his wife abused him in filthy language over the cell phone, which he had recorded on cell phone and downloaded on Compact Disc (CD). The trial Court allowed the petition of husband and held that the court had powers to compare and identify voice recorded in the CD. His wife filed appeal. The question that arose before the court was whether an expert opinion is relevant in identification of voice recorded in CD? The Court held that it is petitioner who has to prove by competent witnesses the time; place and accuracy of the tape-recordings and the voice must be properly identified.

There is a difference between admissibility of a document and its mode of proof. Section 65 B relates to admissibility. And section 45A relates to mode of proof.

Section 65B makes secondary evidence of an electronic record admissible in evidence. When the issue of mode of proof of an electronic record arises, we need to fall back on the conventional form in which any document would be proved.

In the course of research the researcher found that in matters relating to electronic evidence, the integrity of the tangible electronic record may not always be a fact in issue. In deciding as to who has to prove the electronic record, the court has to first ascertain whether the fact in issue is (a) creation of the record( Who created it?) or(b) transmission ( who sent it?) of the same or (c) its receipt(who received it?) or (d) its contents (what did it contain?).

[68] Saki Ammal @ Chitra vs. Veerabhadra @ Kumar (MANU/TN/1419/2012

Illustratively stated, a girl files a police complaint that she received a nude image from the mobile of B over whatsapp. The fact in issue is not the contents or integrity of the image. Relevant for the purpose of investigation is the factum of creation, transmission and receipt. In order to ascertain who transmitted the data, the Investigating officer may have to never prove the integrity of the image received.

However in another illustration if a person files a complaint stating that he received a call from the accused for extorting money from him. He the accused admits the call but denies the substance of conversation to be morphed. Here the contents or integrity of the voice recording is a fact in issue.

Thus burden of proof of proving an electronic record unlike physical evidence which is only confined to authorship and contents, depends upon the facts in issue. The researcher upon her interaction with the experts at the computer forensic laboratories in Chandigarh, Delhi and Goa found that the questions that the investigation officer refers along with the muddemal attached for forensic analysis are the most crucial to make the report of the expert of some significance under section 45A of the Indian Evidence Act. For that the understanding what are the facts in issue is the most crucial.

For achieving greater clarity on this aspect electronic record can be divided into two broad categories.

A. Electronic record created by a human agency

B. Electronic record created by an automated mechanical process. Eg. CCTV Recording, Telephone voice tapping using a device, Saving details of call records, etc.

**A. Electronic record created by a human agency**

An electronic record created by a human agency is a record that is made using human intervention. The intervention may be at the stage of creating the record or transmitting

the same.

For example when an electronic record is an email the author of the email will have to prove the same. When the electronic evidence is a digital photograph the photograph will have to be proved by the photographer clicking the same. Likewise a video recording will have to be proved by a person who recorded the video. In other words were electronic record is created by a human agency the same will have to be proved by examining the creator.

Some of such electronic record however by its essence is intended to be transmitted electronically to one or several recipients. In such cases the recipient of the record is generally the victim. How would the IO therefore prove such electronic evidence? The researcher in the course of the research, examined the evidentiary aspects of the most commonly found electronic records created by human agencies in the subsequent chapters.

**B. Electronic record created by an automated mechanical process.**

Electronic record may be created by an automated process such as IVR, Call records, CCTV footage etc. Here a device is designed to create images, logs or videos under a certain protocol. The question sometimes arises as to who has to prove such images and logs. There is no statutory provision as to who has to prove such electronic record. Therefore by commonsense and by application of conventional law of evidence it would be imperative that such record is proved by the person who has lawful control over the machine or the device that has generated the record.

When we say that such record is to be proved by the person having lawful control of the machine, his testimony cannot be equated to an author of the document. He has to only testify about the setting up of the device by him and state the circumstances that would make the court believe that the device was working property when the electronic record was generated.

As the role of the person who has lawful control over the device is limited, most often or not he is cited as a witness. If the process of seizure of the original electronic record or a copy thereof is properly done, the burden would shift on the person who claims that there is tampering to prove it.

Ordinarily, when electronic record created by an automated mechanical process, the record is stored on the memory of the device that cannot be easily moved. Invariably therefore a copy thereof in form of printouts or CD recording is produced before the court. These copies are admitted by production of certificates under section 65B. However many a times the process by which the copy is obtained itself is challenged under the law. Also the process of copying without use of any forensic tools makes the hash value of the original data prone to alteration. It therefore becomes imperative on the Investigating Officer to preserve the original electronic record. In the foregoing chapters the researcher has studied the safeguards that an Investigating officer has to adopt to ensure that the electronic evidence is properly proved in the court and the impediments in achieving these safeguards.

## 2.3 Secondary Evidence Of Electronic Records

### 2.3.1 Demystifying Section 65B.

Primary evidence is the original evidence produced for the inspection of the court. Electronic record is documentary evidence[69]. When the original document itself is produced for the inspection of the court, the document is admissible in evidence However in case of electronic evidence it is difficult to read the evidence in its native

[69] The Indian Evidence Act has been amended by virtue of Section 92 of Information Technology Act, 2000 (Before amendment). Section 3 of the Act was amended and the phrase "All documents produced for the inspection of the Court" were substituted by "All documents including electronic records produced for the inspection of the Court". Regarding the documentary evidence, in Section 59, for the words "Content of documents" the words "Content of documents or electronic records" have been substituted and Section 65A & 65B were inserted to incorporate the admissibility of electronic evidence.

form. Therefore there is a need to make it presentable, in a form that can be read and comprehended by the human mind.

The Indian Evidence Act contains provisions under which secondary evidence of a fact is admissible. After the enacting the Information Technology Act, the Parliament introduced section 65B of the Indian Evidence Act that made secondary evidence of primary electronic record admissible upon fulfilment of certain conditions. These conditions are contained in section 65B of the Indian Evidence Act.

The question therefore arises as to how the provision would make an electronic record admissible in evidence. Electronic evidence by its nature is distinct from the conventional form of evidence. The yardstick for admissibility of a copy thereof cannot be the same as conventional documents. The legislature has introduced section 65A and 65B which lays down conditions for admissibility of secondary evidence of primary electronic record. Section 65A is an enabling provision that lays down that the contents of electronic records may be proved in accordance with the section 65B of the Indian Evidence Act.

Section 65B gives conditions in which original electronic record can be transformed into “Computer Output” and made admissible as evidence. The Section 65B makes the copy in the form of computer output comprising of printout or the data copied on electronic/magnetic media admissible in evidence subject to certain conditions.

The “Computer Output” referred to in the Section 65B are of two types namely “Printed on Paper” or “Copied on a Media”. This section does not deal with the original electronic record, but only its computer output.

The researcher has dissected section 65B into questions so as to provide maximum clarity about its ambit and applicability. The questions help in gauging important points and phrases and avoid unnecessary long sentences and the confusion created by use of strong legal language.

**QUESTION 1.**

WHY/WHEN DO YOU HAVE TO PRODUCE A CERTIFICATE UNDER SECTION 65B?

When the original electronic record cannot be produced in evidence

**QUESTION 2**

WHAT IS ADMISSIBLE UNDER SECTION 65B?

Any **information** contained as above is **admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original .**

**QUESTION 3**

WHAT INFORMATION IS ADMISSIBLE?

The information must be a computer output which is

1. printed on a paper

   or

2. stored, recorded or copied in optical or magnetic media

**QUESTION 4**

WHAT ARE THE CONDITIONS REQUIRED TO BE FULFILLED BY THE DEVICE/ COMPUTER THAT IS USED TO PRINTED, STORE, RECORD OR COPY ?

1. The computer was regularly used to store and process such information.
2. The computer was used by a person having lawful control over the computer.

3. The information that is contained in the electronic record was regularly fed in computer in the ordinary course of the activities.
4. The computer was operating properly during the period when the electronic record was printed, stored, recorded or copied, and even if not, the defect was not such as to affect the accuracy of the contents of the electronic record; and
5. Information reproduced is the same as it is fed into computer in the ordinary course of activity.

All the above conditions relate to the computer used in processing the information. Emphasis is more on the words "regularly fed" and "ordinary course of its activity" as this word is used in two conditions. The word computer[70], information[71] and electronic record[72] is defined by the Information Technology Act and must be construed in terms of the said definitions. It is pertinent to note that the definition of the word information is not substantive and but inclusive. The most important requirement is that the computer which is used to generate the output must be in lawful control of the person certifying the conditions.

**QUESTION 5**

WHAT HAPPENS WHEN THERE ARE SEVERAL COMPUTERS USED FOR

[70] 2(i) of the Information Technology Act defines "computer" means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic,and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network

[71] 2(v) of the Information Technology Act defines information ‖includes data, message, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche

[72] 2(t) of the Information Technology Act defines information ―electronic record means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche;

PROCESSING THE INFORMATION?

Section 65B(3) takes care of this eventuality and provides the computers operating over that period of time shall constitute as single computer in case of

1. combination of computers; or
2. different computers operating in succession; or
3. different combination of computers operating in succession; or
4. information processed in any manner involving the successive operation over that relevant period of time, in whatever order, of a single or more computers and of a single or more combinations of computers.

**QUESTION 6**

WHAT IS REQUIRED TO MAKE THE COMPUTER OUTPUT ADMISSIBLE?

Certificate as per section 65B.

The researcher randomly examined about 30-40 files in the courts of north Goa and South Goa and found earlier about five years ago, the trend was to produce the printout or the CD without a certificate. The system of producing the certificate along with the copy of the electronic record has been started only around the year 2014 after the judgement of the case of ***Anvar v. P. K. Basheer*** [73] (supra)along with the copy of the electronic record at the first instance.

**QUESTION 7**

WHAT HAS TO GIVE THE CERTIFICATE?

The certificate has to be given by a person who is occupying a responsible official

[73] (2014) 10 SCC 473

position in relation to the operation of the concerned device or the management of the concerned activities. He has to state that the contents of the certificate are to the best of his knowledge and belief.

Here it is relevant to note that the section does not require the only the maker of the copy of the electronic record to sign the certificate. In other words there is no weightage given to the mechanical process by which the certificate was made.

**QUESTION 8**

WHAT MUST THE CERTIFICATE CONTAIN?

(a) The certificate must have clear identification of the electronic record

(b) It must describe manner in which the copy was produced;.

(c) It must give particulars of any device involved in the production of that electronic record as may be appropriate.(the purpose is to show that the electronic record was produced by a computer).

(d) Must certify the fulfilment of conditions mentioned in sub-section (2) as may be applicable.

While reading the entire section 65B, one must keep in mind that the certificate must emphasize on the process of creating the "Computer Output" and not the process of "Creating the Electronic Document".

### 2.3.2 Salient Features Of Section 65A and 65B:

Section 65 A and 65B was introduced by the Information Technology Act by way of an amendment in the year 2000. The amendment was prompted on account of uniqueness of electronic records as documentary evidence even though it is classified as documentary evidence. The researcher has therefore enlisted following salient feature of

section 65A and section 65B.

**a. The provision is independent of section 61 to 65.**

Whereas in almost all provisions of the Indian Evidence Act where the word "document" occurs, the word "document" has been replaced by the word "Electronic documents" or "content of electronic documents". However that is not the case in Section 61 to 65, the word "Document or content of documents" have not been replaced by that phrase. Thus, the intention of the legislature is clear not to bring electronic records with the ambit of section 61 to 65 of the Indian Evidence Act.

It is the cardinal principle of interpretation is that if the legislature has omitted to use any word, the presumption is that the omission is intentional. It is a cardinal principle of interpretation that the Legislature does not use any word unnecessarily. The Apex Court in ***Utkal Contractors***[74] has laid down that the Parliament is not expected to express itself unnecessarily. When the parliament uses a word or a phrase it is presumed that the word of phrase is used intentionally.

b. **Stand alone mandatory provision:**

It is noted that Section 65A & 65B begins with a non obstante clause. "Notwithstanding anything contained in this Act", further strengthens the fact that the legislature had intended the production or exhibition of the electronic records shall be only by the medium of Section 65A & 65B of the Indian Evidence Act.

A non-obstante clause rules out the applicability of any other law. It is ordinarily

[74] Utkal Contractors & Joinery Pvt. Ltd. v. State of Orissa AIR 1987 SC 2310 it was held that "Parliament is also not expected to express itself unnecessarily. Even as Parliament does not use any word without meaning something, Parliament does not legislate where no legislation is called for. Parliament cannot be assumed to legislate for the sake of legislation; nor indulge in legislation merely to state what it is unnecessary to state or to do what is already validly done. Parliament may not be assumed to legislate unnecessarily.

appended to a provision with a view to give the enacting part of the Section, in case of conflict, an overriding effect over any provision in the same or any other Act[75].

c. **Does not prescribe any standard or special procedure for procuring electronic evidence.**

In case of secondary evidence of conventional documents, the issue of custody and possession of the original becomes relevant. Whereas the issue of custody of the original electronic record, is not relevant for applicability of section 65B.

**d. Does not distinguish between private and public electronic record when produced as third party evidence:**

Electronic record may be produced by a third party who is neither the author/ generator or receiver of the same. Such form of electronic record may be(1)substantive evidence (or evidence of contents), in form of e-mail or documents in digital format, SMS, photographs or videos that are not made publicly available and which are stored on a server. Or (2) Evidence from publicly available websites, such as blog postings and images uploaded to social networking websites. Section 65A and 65B does not distinguish between the two forms. And hence does not prescribe any protocol for authentication of electronic records by third-party.

[75] The aforesaid principles of interpretation with respect to the non-obstante clause in form of "Notwithstanding anything contained in this Act" is further supported by the Hon'ble Apex Court in *Union of India and Anr., v. G.M. Kokil and Ors* 1984 AIR 1022 observed "It is well-known that a non obstante clause is a legislative device which is usually employed to give overriding effect to certain provisions over some contrary provisions that may be found either in the same enactment or some other enactment, that is to say, to avoid the operation and effect of all contrary provisions." Further, the Hon'ble Apex Court in the case cited as *Chandavarkar Sita Ratna Rao v. Ashalata S. Guram 1986 4 SCC 447*, explained the scope of non-obstante clause as "…It is equivalent to saying that in spite of the provision of the Act or any other Act mentioned in the non obstante clause or any contract or document mentioned the enactment following it will have its full operation…"

## 2.4 Evolution Of Law On Electronic Evidence Through Judicial Pronouncements

### 2.4.1 Era Of Tape Recorded Conversations

Before the law makers coined a statutory definition to the term electronic evidence, evidence in form of tape recorded conversation was admitted and proved. Although this form of evidence could not be strictly classified as electronic evidence, this contained data that was stored on an electro-magnetic device by following a mechanical process.

There was no statute in India that contained provisions governing admissibility and mode of proof of this form of evidence, however certain principles came to be developed as standard operating procedures on the production of tape recorded evidence by the courts. The researcher has traced the evolution of electronic evidence starting from tape recorded conversations as they are similar in attributes to electronic records and are distinct from paper documents. In case of tape recorded conversations the form in which data is generated and transmitted is different from what is manifestly seen and made admissible.

In ***Maqsud Ali***[76] a question arose as regards the admissibility of tape recorded evidence and the courts in England held that there can be no question of laying down any exhaustive set of rules by which the admissibility of such evidence should be judged as there seems to be no difference in principle between a tape recording and a photograph. However the court cautioned that such evidence must be admitted with caution and assessed in the light of the circumstances of each case[77]. However the Indian Supreme Court in the landmark judgement in the case of ***R.M. Malkani***[78], held that the essential

[76] K. Vs. Maqsud Ali [1965] All. E.R. 464.

[77] ibid. The Hon'ble Court further laid down In saying this we must not be taken as saying that such recordings are admissible whatever the circumstances, but it does appear to this Court wrong to deny to the law of evidence advantages to be gained by new techniques and new devices, provided the accuracy of the recording can be proved and the voices recorded properly identified; provided also that the evidence is relevant and otherwise admissible, we are satisfied that a tape recording is admissible in evidence. Such evidence should always be regarded with some caution and assessed in the light of all the circumstances of each case. There can be no question of laying down any exhaustive set of rules by which the admissibility of such evidence should be judged.

[78] R.M. Malkani Vs.,State of Maharashtra 1973 Cri.L.J. 228 See also R.K. Anand Vs. Registrar, Delhi High Court, (2009)8 SCC 106.

conditions which, if fulfilled or satisfied would make a tape recorded statement, admissible otherwise not are that the Tape recorded conversation must be relevant to the matter in issue; secondly, the voice of the speaker has to be clearly indentified; and, thirdly, the accuracy of the conversation must be proved by eliminating every possibility of erasure.

Subsequently thereafter the Hon'ble Supreme court laid down exhaustive guidelines in ***Ram Singh and Ors.***[79] for admissibility of tape recorded conversations [80].

After this judgement the Hon'ble Bombay High Court framed Rules for production, use and recording of the tape record evidence in court[81].

---

[79] Ram Singh and Ors. Vs. Col. Ram Singh 1985 (Supp) SCC 611

[80] ibid. The court laid down the following guidelines: 1) The voice of the speaker must be duly identified by the maker of the record or by others who recognise his voice. 2) The accuracy of the tape recorded statement has to be proved by the maker of the record by satisfactory evidence direct or circumstantial. 3) Every possibility of tampering with or erasure of a part of a tape recorded statement must be ruled out otherwise it may render the said statement out of context and, therefore, inadmissible. 4) The statement must be relevant according to the rules of Evidence Act. 5) The recorded cassette must be carefully sealed and kept in safe or official custody. 6) The voice of the speaker should be clearly audible and not lost or distorted by other sounds or disturbances.

[81] Criminal Manual Chapter 6 Para 24; Rules for production, use and recording of the Tape Record Evidence in Court.24. The Honourable the Chief Justice and Judges, with the previous approval of the Governor under Article 227 of the Constitution of Indian, are pleased to make the following rules regarding recording of the tape-record evidence in Court :-

(1) These Rules may be called the Rules for the Production, Use and Recording of the Tape-Record Evidence in Courts.

(2)These Rules came into force with effect from 1st August, 1978.

(3) The party producing the tape-recorded evidence shall also produce the transcript of the tape record along with the tape.

(4) The Court or its authorised officer who is to accept the tape should accept only such tapes as are under the seal of the party producing them.

(5) Court or such officer shall hear the tape record in order to verify whether the transcript produced alongwith the tape is correct or not and endorse such verification on the transcript record under his signature with date.

(6) The tape shall be kept in safe custody in a cover under the seal of the court. In case the tape is replayed or the seal is broken for any reason, the tape shall be re-sealed.

(7) The notice of production of the tape together with the transcript shall be served on the other side through the court.

(8) Any party to the proceeding may apply to the Court to hear the tape-record.

(9) The tape-record would be played within the hearing and sight of an officer appointed by the Court for that purpose and as far as possible in the presence of the other side or its Advocate. The Court on receipt of application may grant the necessary permission. However, the tape shall ordinarily not be played on 3rd or 4th occasion, unless the Court specifically permits hearing of the same. The Court while granting

Therefore at the point at which technology stood then, when it was disputed whether a person made a particular statement there could be no more direct or better evidence of it, than its tape record, provided that its authenticity was duly established. Just like a previous statement, tape recorded statement, can be used not only to corroborate the evidence given by the witness in Court but also to contradict the evidence given by him. It can be used to test the veracity of the witness as well and also to impeach his credit[82]. Continuity, clarity and coherence are the three principles that are required for fair and reliable assessment of the conversation.

Possibility of tampering was held to be no ground to ignore tape records by Indian courts. The reason being that even paper documents could be easily tampered. Hence it was laid down in several cases that the above factor would have a bearing only on the weight to be attached to the evidence and not affect its admissibility[83].

Therefore without any legislative amendments tape records became "documents", as defined by Section 3 of the Evidence Act, which stood on no different footing than photographs, and that they were admissible in evidence on satisfying certain

---

such permission should bear in mind that repeated use and play of the tape may affect the tape and its audibility. The Court may also permit any party to record the voice on the tape, produced in Court, on another tape.
(10) Every Court shall maintain a record showing as to how, when and why the seal of the tape -record has been resealed. Such record shall be kept in the proceedings alongwith the tape record and its transcript.
(11) The tape in a sealed cover together with its transcript shall be given a separate exhibit.
(12) In Criminal cases where appeal lies to the High Court and when the tape record is not in English, either wholly or in part, the transcript must be accompanied by an agreed or official English translation of the said transcript or part thereof, as the case may be.
(13) In case of discrepancy or doubt, the court may direct the tape to be replayed and the transcript record shall be corrected if the Court so directs.
(14) While preparing the paper-book for appeal to the High Court the Lower Court shall include therein the transcript in English under Rule 12, and a copy of record referred to in Rule 10 above.
(15) The rules as to the production, preservation and destruction of them court record should mutatis mutandis apply to the tapes.
(16) The above rules (Rules Nos.1 to 15) are framed for guidance of the Courts and they should be followed as far as possible and subject to the provisions of the Evidence Act and Code of Civil Procedure.

[82] N. Sri Rama Reddy Vs. V. V. Giri, 1971 (1) SCR 399.

[83] S.Pratap Singh Vs. The State of Punjab, AIR 1964 SC 72

conditions[84].

The process of tape recording offers an accurate method of storing conversations and later reproducing whenever needed. Just like a photograph, a contemporaneous tape record of a relevant conversation is a relevant fact under Section 7 or even under section 5 of the Indian Evidence Act[85].

### 2.4.2 Evolution Of Principle Of Rule Against Substantial Compliance Of Section 65B.

Due to passage of time tape recorded conversations did not remain the sole repository of electronic evidence. Magnetic tapes came to be replaced by digital tapes. With the advent of computers every form of data could now be generated and stored in electronic form. The growing use of the communication and information system through the internet and computers, led to certain new legal issues. The laws existing prior to the Information Technology Act proved insufficient to deal with the emerging challenges. The United Nations Commission on International Trade Law' (UNCITRAL) enacted the 'Model Law on Electronic Commerce‘. by its resolution dated 30.01.1997. This led to the passage of the Information Technology Act 2000 in India. With the passing of this law India opened its portals to a new perspective to examine the way evidence was adduced and authenticated in the court of law.

---

[84] In Ziyauddin Burhanuddin Bukhari Vs. Brijmohan Ramdass Mehra, (1976) 2 SCC 17 it was held that : (a) The voice of the person alleged to be speaking must be duly identified by the maker of the record or by others who knew it. (b) Accuracy of what was actually recorded had to be proved by the maker of the record and satisfactory evidence, direct or circumstantial, had to be there so as to rule out possibilities of tampering with the record. (c) The subject matter recorded had to be shown to be relevant according to rules of relevancy found in the Evidence Act. As regards the shorthand transcripts of the tape records, the evidence of their makers is there, it is certainly corroborative inasmuch as it only goes to confirm what the tape records contained. The tape records were the primary evidence of what was recorded. The transcripts could be used to show what the transcriber had found recorded there at the time of the transcription. This operated as a check against tampering.

[85] Yusufalli Esmail Nagree Vs. State of Maharashtra, (1967) 3 SCR 720 : 1968 Cri.L.J. 103

This law made an honest attempt to set to rest all legislative bewilderment on the aspect of electronic evidence. The highlight of this Act is that this Act gave legal recognition to the transactions carried out through electronic communication, commonly known as "electronic commerce". It also gave legal recognition to the electronic signature. Its primary objectives was facilitate electronic filing of documents with the Government agencies and for protecting the information access, privacy, communications, intellectual property and freedom of speech related to the use of the internet, websites, email, computers, cell-phones, software and hardware, such as data storage devices. It enacted penal provisions to that defined cyber crimes and made them punishable. The Act also made amendments to existing statutes such as The Indian Penal Code, The Indian Evidence Act, 1872, The Banker's Books Evidence Act, 1891, The Reserve Bank of India Act, 1934.

The most important amendment that it made to the Indian Evidence Act, is introducing the concept of electronic records in it. It made computer output of any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer, admissible only upon the production of a certificate in terms of section 65B of the Indian Evidence Act.

Section 65B is the bedrock of law relating to admissibility electronic evidence. It is the first hurdle that every electronic record that is tendered in evidence has to pass through. The question whether certificate under section 65B is mandatory, for the first time was raised in the landmark case of ***Navjot Sandhu***[86] in that case the court examined the import of section 65B of the Indian Evidence Act and its relevance when coexisting with other provisions relating to secondary evidence under the Indian Evidence Act.

In this case there was an appeal against conviction following the attack on Parliament on December 13 2001. The question was as regards the proof and admissibility of mobile telephone call records details.

It was argued on behalf of the accused that no reliance could be placed on the mobile

[86]State (NCT of Delhi) v Navjot Sandhu AIR 2005 SC 3820

telephone call records, because the prosecution had failed to produce a certificate under Section 65B of the Indian Evidence Act before tendering the Call record details in Evidence. The Supreme Court noted that computerized record furnished by the cellular service providers, and the covering letters were signed by their nodal officers who were examined as witnesses. These persons were competent witnesses who were acquainted with the functioning of the computer during the relevant time. The printouts of the call records were taken by following a mechanical process. Therefore the electronic record stood proved and admitted by section 63 and 65 of the Indian Evidence Act and this was sufficient to prove the call records even without a certificate under section 65B of the Indian Evidence Act[87].

This case however was found flawed in many respects and was a subject of criticism by both the experts in cyber laws as well as the jurists. The case directly breached the principle of inadmissibility of heresay evidence. It failed to recognise the meaning and import of section 65B as a facilitator of secondary evidence in true sense.

The Indian Evidence Act mandates a special procedure for electronic records precisely because printed copies of such information are vulnerable to manipulation and abuse. This is what the defence counsel, pointed out in ***Navjot Sandhu***[88] where there were discrepancies in the CDRs led in evidence by the prosecution. Critics argued that despite these infirmities, which should have disqualified the evidence until the State demonstrated the absence of mala fide conduct, the Supreme Court stepped in to certify the secondary evidence itself against the mandate of law. The court did not compare the

[87] On the question of the defence's challenge to the authenticity and accuracy of certain call data records (CDRs) that the prosecution relied on, which were purported to be reproductions of the original electronically stored records, a Division Bench of Justice P. Venkatarama Reddi and Justice P. P. Naolekar held: "*According to Section 63, secondary evidence means and includes, among other things, "copies made from the original by mechanical processes which in themselves ensure the accuracy of the copy, and copies compared with such copies". Section 65 enables secondary evidence of the contents of a document to be adduced if the original is of such a nature as not to be easily movable. It is not in dispute that the information contained in the call records is stored in huge servers which cannot be easily moved and produced in the court. That is what the High Court has also observed at para 276. Hence, printouts taken from the computers/servers by mechanical process and certified by a responsible official of the service-providing company can be led into evidence through a witness who can identify the signatures of the certifying officer or otherwise speak to the facts based on his personal knowledge.*"

[88] Ibid page 148

printed CDRs to the original electronic record. Essentially, the court allowed hearsay evidence[89].

The finding of the court that irrespective of the compliance of the requirements of Section 65B, there can be no bar for adducing secondary evidence under the other provisions of the Evidence Act, namely, Sections 63 and 65 was found to render the amended Indian Evidence Act redundant.

The case of ***Ratan Tata***[90]followed the suit. This was a case where a CD containing intercepted telephone calls was admitted in evidence without following the procedure laid down under section 65B of the Evidence Act.

In 2007, the United States District Court for Maryland decided the issue of electronically stored information (ESI) in ***Lorraine v. Markel American Insurance Company***[91]. That case raised the question of admissibility and proof of emails as evidence of a contract. These emails were not tendered in evidence per the Federal Rules of Evidence relating to electronically stored information. Rejecting this evidence the court held that in admitting ESI as evidence the court has to consider the special characteristics of electronically stored records and the need to establish its accuracy and reliability. Therefore the American federal courts took a contrast view to the lenient view taken by its predecessors[92]. The trend therefore was to recognise electronic evidence as a special breed of evidence requiring separate rules for its admissibility and authentication. It discouraged the process of its admissibility and authentication in the same manner as traditional documentary evidence.

---

[89]Bhairav Acharya "*Anvar v. Basheer and the New (Old) Law of Electronic Evidence* https://bhairavacharya.net/ published by Law and Policy in India on September 25, 2014. Accessed on 17.8.2019 at 10.30 pm

[90] Ratan Tata v. Union of India Writ Petition (Civil) 398 of 2010 before Supreme Court of India.

[91]Lorraine v. Markel American Insurance Company 241 FRD 534 (D. Md. 2007)

[92] Judge Grimm discussed five evidence standards ESI evidence must satisfy: (1) is the ESI relevant (under Rule 401); (2) is it authentic (under Rule 901(a)); (3) is it hearsay (under Rule 801) and, if so, does it constitute an exception under Rules 803, 804 and 807, (4) does it comply as an original or duplicate under the original writing rule or, if not, can it be admitted pursuant to the admissible secondary evidence rules 1001- 1008 to prove the content of ESI and (5) is the probative value of the ESI substantially outweighed by the danger of unfair prejudice or another factor identified by Rule 403 of the Federal Rules of Evidence

Taking a cue from the progression of law in the United States in ***Anvar P. V.***[93], the Supreme Court overruled the decision in the case of ***Navjot Sandhu,(supra)*** and redefined the concept of admissibility of electronic records to correctly reflect the letter and spirit of the amended provision and harmoniously interpreting sections 63, 65 and 65B of the Indian Evidence Act. The court applied the maxim generalia specialibus non derogant ("the general does not detract from the specific"),

In this case, P.V. Anwar had filed an appeal contending that his opponent P. K. Basheer, MLA had defamed him. The defamatory content that contained electronic propaganda, interviews and recordings of public meetings where recorded on a mobile phone and video cameras. This electronic record was copied on CDs which were produced as evidence without a certificate under section 65B of the Indian Evidence Act. This evidence was challenged on the ground that it is secondary evidence as the original cell phone or camera on which it was recorded has not been produced. Here infact the person who recorded some of the speeches was also examined as a witness.

However the Supreme Court declined to accept the view that the courts could admit electronic records as prima facie evidence without certificate under section 65B. It was held that section 65A and 65B are a complete code in itself exclusive of the other provisions of the Indian Evidence Act and therefore an electronic record cannot be admitted by resorting to other provisions relating to secondary evidence[94].

Despite this view taken by the Hon'ble Supreme Court declaring section 65A and B a self contained code, the practical challenges faced in admissibility of electronic record,

---

[93] Anvar P. V. vs. P.K Basheer &Ors AIR 2015 SC 180

[94] Justice Kurian Joseph authoring the judgement laid down that "*Any documentary evidence by way of an electronic record under the Evidence Act, in view of Sections 59 and 65A, can be proved only in accordance with the procedure prescribed under Section 65B. Section 65B deals with the admissibility of the electronic record. The purpose of these provisions is to sanctify secondary evidence in electronic form, generated by a computer. It may be noted that the Section starts with a non obstante clause. Thus, notwithstanding anything contained in the Evidence Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be deemed to be a document only if the conditions mentioned under sub- Section (2) are satisfied, without further proof or production of the original. The very admissibility of such a document, i.e., electronic record which is called as computer output, depends on the satisfaction of the four conditions under Section 65B(2)".*

made subsequent judgements water down the effect of Anwar P V (supra).

In the case of ***Tomaso Bruno***[95]**,** the Hon'ble Supreme Court held that Secondary evidence of contents of an electronic record can also be led under Section 65 of the Evidence Act. In that case it was held that the omission to produce CCTV footage, which is the best evidence, raises serious doubts about the prosecution case. The Court, drew an adverse inference against the prosecution under Section 114 (g) of the Evidence Act, and conviction was, therefore, set aside.

Further in of ***Sonu @ Amar***[96]**,** a question arose whether CDRs which were produced without a certificate under section 65B of the Indian Evidence Act could be read in evidence. The Hon'ble SC relied on the basic principle of admissibility and mode of proof as would be applicable for conventional documents and held that the objection as regards admissibility had to be raised at the stage when the copy of the electronic record was produced at the first instance by the prosecution before the trial court. Admittedly, no objection was taken when the CDRs were adduced in evidence before the Trial Court. The court therefore held that the CDRs could be admissible in evidence without the certificate[97].

A two-Judge Bench of the Apex Court in ***Shahfi Mohammad***[98], was required to consider a situation where the certificate under section 65B could not be produced on account of the original record being in possession of a third party[99]. In this case the

[95] Tomaso Bruno and another v. State of Uttar Pradesh (2015) 7 SCC 178

[96] Sonu @ Amar v. State of Haryana 2017 SCC Online 765

[97] The Supreme Court reasoned that the crucial test in such a case is whether the defect could have been cured at the stage of marking the document. Upon an objection relating to the mode or method of proof, the Courts holds that in the present case if an objection was taken to the CDRs being marked without a certificate, the Court could have given the prosecution an opportunity to rectify the deficiency. It holds that the mode or method of proof is with connected appeals procedural and objections, if not taken at the trial, cannot be permitted at the appellate stage. It holds that if the objections to the mode of proof are permitted to be taken at the appellate stage by a party, the other side does not have an opportunity of rectifying the deficiencies. An example was taken as to the statements under section 161 of the Code of Criminal Procedure, which fall under the category of inherently inadmissible evidence and CDRs do not fall in the said category of documents.

[98] Shahfi Mohammad v. The State of Himachal Pradesh Special Leave Petition (CRL.)No.2302 of 2017

[99] After hearing submissions of the parties and clarifying the legal position on the subject on the admissibility of the electronic evidence (especially by a party who is not in possession of device from

court was considering the utility of videography in investigation and the potential roadblock of section 65B in respect of electronic record which is not in possession of the party producing its secondary evidence. After considering the rival submissions it was held that if the original record is in possession of third party, the party intending to produce its copy is exempted from producing a certificate under section 65B. This however does not mean that the copy of the electronic record can be directly read in evidence. It was held that the evidence so produced has to be tested on the touchstone of sections 61 to 65 of the Indian Evidence Act.

The Hon'ble Apex Court in the case of **A*rjun Panditrao Khotkar***[100]attempted to clear the deadlock to some extent.

Since the passing of judgment in the case of ***Mohd Shafi(supra)***, two more decisions came from Hobn'ble High courts. The Madras High Court in ***K. Ramajyam***[101] which held that oral evidence can be given through a person who was in-charge of a computer device in the place of the Certificate. In . ***In Tomaso Bruno(supra),***it was held that that Sections 65A and 65B cannot be held to be a complete Code on the subject, directly contrary to what was stated by a three Judge Bench in Anvar P.V. (supra). It was further

---

which the document is produced) the Apex Court (in reference to aforesaid judicial decisions) made the following observations: i. Electronic evidence is admissible under the Act. Section 65A and 65B are clarificatory and procedural in nature and cannot be held to be a complete code on the subject. ii. If the electronic evidence so produced is authentic and relevant, then it can certainly be admitted subject to the court being satisfied of its authenticity. The procedure for its admissibility may depend on the facts such as whether the person producing the said evidence is in a position to furnish a certificate under Section 65B (h). iii. The applicability of the procedural requirement under Section 65B(4) of the Act of furnishing a certificate is to be applied only when such electronic evidence is produced by a person who is in a position to produce such a certificate being in control of the said device and not of the opposite party. iv. In a case where electronic evidence is produced by a party who is not in possession of a device, applicability of Sections 63 and 65 of the Act cannot be held to be excluded. In such cases, procedure under the said provisions cannot be held to be excluded. v. A person who is in possession of authentic evidence but on account of manner of proving, such document is kept out of consideration by the court in absence of certificate under Section 65B(4) of the Evidence Act, which party producing cannot possibly secure, will lead to denial of justice. vi. A party who is not in possession of a device from which the document is produced cannot be required to produce a certificate under Section 65B (4) of the Act. Thus, the requirement of certificate under Section 65B is not always mandatory.

[100] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal 2020 SCC OnLine SC 571

[101] K. Ramajayam alias Appu v. Inspector of Police 2016 (2) CTC 135

clarified that the requirement of a certificate under Section 64B(4), being procedural, can be relaxed by the Court wherever the interest of justice so demands. One circumstance in which the interest of justice so justifies would be where the electronic device is produced by a party who is not in possession of such device, as a result of which such party would not be in a position to obtain the requisite certificate.

In **A*rjun Panditrao Khotkar (supra)*** the fact in issue were video recordings produced by the Election Commission, without a certificate from the person incharge of the device generating the record under section 65B of the Indian Evidence Act. In this case filing of nomination papers was challenged on the ground that they were filed beyond the time limited by the election commission. The petitioner sought to rely upon the video recordings available at the office of the Returning Officer. However despite several correspondence made the Returning Officer who was the incharge of the record refused to give a certificate under section 65B of the Evidence Act. Although the VCD were already on record there was no certificate under section 65 B produced to support them. If the contents of the aforesaid VCDs could be proved, then the petitioners were bound to succeed in the case. The Honble High Court then observed that the CDs that were produced by the Election Commission could not be treated as an original record and would, therefore, have to be proved by means of secondary evidence.

The question however was whether the VCDs could be admitted as secondary evidence in the absence of a certificate?. Finding that no written certificate as is required by Section 65-B(4) of the Indian Evidence Act was furnished by any of the election officials, and more particularly, the Returning Officer, the High Court then held that the substantive evidence, in form of cross examination of Smt. Mutha, which testifies all the requirements of section 65B of the Evidence Act is sufficient to admit the electronic record.

The Hon'ble court held that she was incharge of the management of the relevant activities and her evidence can be used and needs to be used as substantial compliance of the provision of section 65-B of the Evidence Act and hence based on this evidence the election of the Returning Candidate was therefore was declared void in the

impugned judgment.

This order of the Hon'ble High Court was challenged before the Hon'ble Supreme Court. The argument was that as there was no certificate under section 65 B the electronic record in form of CD could not be admitted in evidence. Reliance was placed on the judgement in the case of ***Anvar P.V. (supra)***, and argued that the theory of substantial compliance that is laid down by the court is contrary to this judgement and hence has to be set aside.

Per contra it was argued that the testimony taken down in the form of writing, which witness statement is signed by the Returning Officer, would itself amount to the requisite certificate being issued under Section 65B(4).

On behalf of the intervener it was argued that the case of that ***Anvar P.V. (supra)*** required to be clarified to the extent that Sections 65A and 65B being a complete code as to admissibility of electronic records, and define as to what is to be done when it is not possible to produce a certificate under section 65B.

The Hon'ble Supreme Court considered the origins of section 65B of the Indian Evidence Act, and particularly the non obstante clause and held since section 65A and 65B were particularly introduced in view of the information Technology Act it is a complete code in itself and cannot be supplanted or modified by any other provisions of law. It however did not still clear the air about third party electronic records and held that it is the need of the hour for the legislature to relook at the law relating to third party electronic records[102].

[102] The reference is thus answered by stating that:(a) Anvar P.V. (supra), as clarified by us hereinabove, is the law declared by this Court on Section 65B of the Evidence Act. The judgment in Tomaso Bruno (supra), being per incuriam, does not lay down the law correctly. Also, the judgment in SLP (Crl.) No. 9431 of 2011 reported as Shafhi Mohammad (supra) and the judgment dated 03.04.2018 reported as (2018) 5 SCC 311, do not lay down the law correctly and are therefore overruled.
(b) The clarification referred to above is that the required certificate under Section 65B(4) is unnecessary if the original document itself is produced. This can be done by the owner of a laptop computer, computer tablet or even a mobile phone, by stepping into the witness box and proving that the concerned device, on which the original information is first stored, is owned and/or operated by him. In cases where the "computer" happens to be a part of a "computer system" or "computer network" and it becomes

Therefore the law that stands as on date is that for copy of any electronic record to be admissible in evidence a certificate under section 65B is mandatory.

### 2.4.3 Early Perspective Of The Hon'ble Supreme On Electronic Evidence

The earliest judgement of the Hon'ble Supreme court on the issue of electronic evidence was the judgement in the case of ***Jagjit Singh***[103]**.**In this case the issue was as regards admissibility of electronic records contained in television recording. The court held that electronic record was certified by the television agencies or its authorised representative and in the absence of a specific allegation that the record was doctored mere vague denials would not suffice. It was therefore held that the speaker has rightly relied upon other documentary evidence along with the electronic evidence to hold that the members of the Legislative Assembly were liable to be disqualified for misconduct. In that case the television news channels had produced the original CDs that contained the original recordings before the court along with the certificate under section 65B. This case was one of those first cases decided by the Honorable Supreme Court much before ***Navjyot (supra).***

---

impossible to physically bring such system or network to the Court, then the only means of providing information contained in such electronic record can be in accordance with Section 65B(1), together with the requisite certificate under Section 65B(4). The last sentence in Anvar P.V. (supra) which reads as "…if an electronic record as such is used as primary evidence under Section 62 of the Evidence Act…" is thus clarified; it is to be read without the words "under Section 62 of the Evidence Act,…" With this clarification, the law stated in paragraph 24 of Anvar P.V. (supra) does not need to be revisited.

(c) The general directions issued in paragraph 62 (supra) shall hereafter be followed by courts that deal with electronic evidence, to ensure their preservation, and production of certificate at the appropriate stage. These directions shall apply in all proceedings, till rules and directions under Section 67C of the Information Technology Act and data retention conditions are formulated for compliance by telecom and internet service providers.

(d) Appropriate rules and directions should be framed in exercise of the Information Technology Act, by exercising powers such as in Section 67C, and also framing suitable rules for the retention of data involved in trial of offences, their segregation, rules of chain of custody, stamping and record maintenance, for the entire duration of trials and appeals, and also in regard to preservation of the meta data to avoid corruption. Likewise, appropriate rules for preservation, retrieval and production of electronic record, should be framed as indicated earlier, after considering the report of the Committee constituted by the Chief Justice's Conference in April, 2016.

[103] Jagjit Singh v. State of Haryana (2006) 11 SCC 1.

The case of ***K.K. Velusamy*** [104]was also one of the earliest cases, where the Honorable Supreme Court was confronted with the admissibility of electronic record that is contained in a compact disc. In this case the plaintiff wanted to produce a tape recorded conversation which was recorded on a compact disc (electronic record) which would show the liability of the respondent towards a loan transaction. The respondent resisted the application contending that the voice was not his. It may be noted that the Honorable Supreme Court was considering the dismissal of a recall of witness application. The Honorable Supreme Court considered that section 3 of the Indian Evidence Act also includes electronic record which is defined under Section 2(t) of the Information Technology Act of 2008 and also includes a compact disk containing an electronic record of a conversation and further that such a conversation is relevant under Section 8 of the Indian Evidence Act, in view of the previous judgement of the Supreme Court in the case of ***RM Malkani (supra)*** wherein the Supreme Court had made it clear that tape recorded conversation is relevant. However it was held that it is open to the trial court to consider the authenticity and admissibility of the electronic record.

In ***Mohd. Arif***[105] there was no direct reference to section 65B of Indian Evidence Act nonetheless in this case the court considered the valuable role that call record details and tower location details play in intercepting the location of the accused and connecting the accused with the crime.

### 2.4.4 Subcutaneous Memory And Its Relevance.

In ***Dharambir***[106], it was held that a hard-disk is an electronic record. There are two levels of electronic records. One is the hard-disk which once used itself becomes an electronic record in relation to the information regarding the changes the hard-disk has been subjected to and which information is retrievable from the hard-disk by using software. The other level of electronic record is active accessible information recorded

[104] K.K. Velusamy v. N. Palanisamy (2011) 11 SCC 275
[105] Mohd. Arif v. State (NCT of Delhi), (2011) 13 SCC 621
[106] Dharambir Vs. C.B.I(2008) ILR 2 Del 842

in the hard-disk in the form of a text file or sound file or video file etc. Such information can be converted or copied to another storage device. Even a blank hard-disk, which was once used for recording information can also be copied by producing a mirror image.

### 2.4.5 Evidence Through Video Conferencing

In ***State of Maharashtra Vs. Dr. Praful B. Desai***[107], it was held that recording of evidence in presence of accused (S. 273, Cr.P.C.) does not necessarily mean physical presence. It may be presence through video conference. Hence, recording of evidence through Commissioner or through the video conference is permissible. In ***Salem Advocate Bar Association***[108], the Hon'ble Supreme Court ruled that Order XVIII Rule 4 (3) C.P.C. provides for recording of evidence in writing or mechanically. The word mechanically indicates that the evidence can be recorded with the help of electronic media, audio or audio-visual. In fact, whenever, the evidence is recorded by the Commissioner, it will be advisable to record it simultaneously through audio recording of the statement of the witness so as to obviate any controversy at a later stage.

In ***Twentieth Century Fox Film Corporation and anr.***[109], the Hon'ble Karnataka High Court gave some guidelines for recording evidence through audio-video link. They include supply of same set of documents to the witness also for reference purpose.

In ***Shilpa Chaudhary v. Principal Judge And Others***[110] The court noted that family courts in matrimonial matters increasingly see a number of cases where one of the parties are abroad it is difficult for them to undertake a trip to india. In such cases the courts can resort to technology such as skype and permit a party to lead evidence. Presence does not necessarily mean physical presence. All statements indicated under

[107] AIR 2003 SC 2053
[108] AIR 2003 SC 189
[109] Twentieth Century Fox Film Corporation and anr. Vs. NRI Film Production Associates (P) Ltd AIR 2003 Kar. 48
[110] Shilpa Chaudhary v. Principal Judge And Others AIR 2016 ALL 122

section 3 of the Indian Evidence Act can include statements made by witnesses through video conferencing and requirement for a witness to be present physically in the court can be dispensed with. There is thus no need to resort to the old practice of engaging a power of attorney to depose on behalf of the principle.

In ***Sirangi Sobha Shoba Munuri***[111] the question before the Andhra Pradesh High Court was whether can the mere possibility of prompting or altering a witness be a ground for denial of recording evidence through skype?. The court dismissed this apprehension holding that the Apex court in a number of leading cases have laid down guidelines on the manner in which such evidence is to be recorded and further held that the trial court while recording evidence can record the demeanour of the witness and shall note the objections as well if raised during recording of evidence.

In ***Sheeba Abidi***[112] it was held by the Delhi High Court that it can also be used where the Court on facts and circumstances do not want the witness to personally attend the Court and answer. It can happen in cases where the witness (victim) is a child who has been sexually exploited or in case if the child has suffered from unnatural offence.

The party, who intends to avail the facility of V.C., shall be under an obligation to meet the entire expenditure[113].

### 2.4.6 CCTV Evidence:

CCTV is the short form of the term “closed-circuit television". The term Closed-circuit is used because the broadcasts are confined to a limited (closed) number of monitors, in contrast with “regular” TV.

A CCTV is extremely useful in crime detection and the recording made on the DVR

---

[111] Sirangi Sobha Shoba Munuri vs Sirangi Muralidhar Rao AIR 2017 AP 88, see also Dr.Kumar Saha Vs. Dr.Sukumar Mukherjee (2009) 9 SCC 221,, Suvarna Rahul Musale v/s Rahul Prabhakar Musale · Writ Petition No. 6514 of 2014 (Bombay High Court.

[112] Sheeba Abidi Vs. State 113 (2004) DLT. 125.

[113] Bodala Murali Krishna Vs. Smt. Bodala Prathima MANU/AP/0973/2006.

serves in gathering evidence relating to the act in question " actus reus" and or serves the purpose of identifying the accused. The issue of identity of the accused is relevant under section 9 of the Indian Evidence Act and was conventionally established by oral or circumstantial evidence. The investigation officers would often resort to methods like test identification parade to establish the identity of those accused who were seen by witnesses for a sporadic second[114]. However courts now have realised the potent ability of CCTV footage to serve that purpose with greater accuracy.

In ***Kishan Tripathi vs The State***[115] the court convicted the accused based on ocular evidence corroborated by CCTV evidence. It was argued that the CCTV footage is not admissible without certificate under section 65B. Rejecting this argument the court held that since the original hard disk was produced, it being primary evidence there was no need of a certificate under section 65B to admit it in evidence. The court opined that since CCTV footages are images captured by a mechanical process its reliability is even greater than the ocular version given by eye witnesses. In such cases a CCTV camera becomes the eyes that views the incident[116]. The court however cautioned that the

[114] Test identification parade has its own limitations. these are the passage of time between the incident and the procedure, the time for which the accused was visible to the witnesses, the surrounding conditions that would affect the ability of the witness to identify the accused State of Maharashtra v Syed Umar Sayed Abbas & Ors., the incident of firing occurred in broad day light, however not much time was there with the witnesses to clearly see the accused and there was delay in TIP, hence the Court acquitted the accused on the ground that it is highly doubtful whether the eye witness could have remembered the face of the accused after such a long time.

[115] Kishan Tripathi vs The State MANUDE04342016

[116] At para 14 it was held that "*The CCTV footage is captured by the cameras and can be stored in the computer where files are created with serial numbers, date, time and identification marks. These identification marks/ details are self generated and recorded, as a result of pre-existing software commands. The capture of visual images on the hard disc is automatic in the sense that the video images get stored and recorded suo-moto when the CCTV camera is on and is properly connected with the hard disc installed in the computer. It is apparent in the present case from the evidence led that no one was watching the CCTV footage when it was being stored and recorded. The recording was as a result of commands or instructions, which had already been given and programmed. The original hard disc, therefore, could be the primary and the direct evidence. Such primary or direct evidence would enjoy a unique position for anyone who watches the said evidence would be directly viewing the primary evidence. Section 60 of the Evidence Act states that oral evidence must be direct, i.e., with reference to the fact which can be seen, it must be the evidence of the witness, who had seen it, with reference to the fact, which could be heard, it must be evidence of the witness, who had heard it and if it relates to the fact, which could be perceived by any other sense or any other manner, then it must be the evidence of the witness, who says who had perceived it by that sense or by that manner. Read in this light, when we see the CCTV footage, we are in the same position as that of a witness, who had seen the occurrence, though*

CCTV must pass through a twofold test of system integrity and record integrity. The court must rule out any possibility of manipulation, fabrication or tampering. In this case the court held that it was satisfied but the integrity of the electronic record[117].

When we see the CCTV footage, we are in the same position as that of a witness, who had seen the occurrence, though crime had not occurred at that time when the recording was played, but earlier. Electronic evidence of CDR for determination of movement of a

---

*crime had not occurred at that time when the recording was played, but earlier. HG wells in his book "The Time Machine" had said "Now I want you clearly to understand that this lever, being pressed over, sends the machine gliding into the future, and this other reverses the motion. This saddle represents the seat of a time traveler. Presently I am going to press the lever, and off the machine will go. It will vanish, pass into future Time, and disappear. Have a good look at the thing. Look at the table too, and satisfy yourselves there is no trickery." Time machine is friction, albeit seeing the CCTV footage with your own eyes as a judge gives you an insight into the real world in the past. In the present case, the court has itself seen the CCTV footage, and has travelled back in time to the time when the occurrence took place and thereby has seen the occurrence in the same position as that of a witness, who would have seen the occurrence, if he was present. There cannot be a more direct evidence. This video recording which captures the occurrence, would be per se and mostly discerningly reliable and compellingly conclusive evidence, unless its authenticity and genuineness is in question.*

[117]At para 16 it was observed that ." *We would accept the genuineness and authenticity of the CCTV footage played before us, for good and sound reasons. System integrity test is satisfied by ocular testimonies of Rakesh Bhargawa (PW-4), Ram Milan (PW-15) and police officers H.C. Rajpal Singh (PW-7) and Inspt. B.S. Rana (PW-18). System was working and contemporaneously storing data. They had viewed the data. On record integrity, i.e., contents of the record have remained unchanged, we were anxious as it was noticed that the list of documents at Sr. No. 27, filed with the charge-sheet, mentions compact disc (CD) indicative that the hard drive had been examined and secondary evidence was created. Examination of the police case file had revealed that the CD was created at the behest of the public prosecutor, before the charge-sheet was filed. This was certainly a lapse and the hard disc sealed and deposited in the malkhana should not have been opened, even for the purpose of making copies of the video files. However, in the facts of the present case, this transgression and deviation would not unsettle and nullify the authenticity of the CCTV footage for there is no evidence or even a suggestion that the appellant Kishan Tripathi was at any time under compulsion or force, was asked to enact the crime at the place of occurrence. Moreover, the CCTV footage was seen on 23rd February, 2009 by Rakesh Bhargava (PW-4) and the police officers HC Rajpal Singh (PW-7), Insp. B.S. Rana (PW-18) and Ram Milan (PW-15) who had operated and played the CCTV footage. We are satisfied that the recorded CCTV footage has not been interpolated or tampered in the light of the original hard drive, which has been played before us. The footage recorded consists of 405 files starting from 2:06 P.M. on 21.02.2009 till 2:14 P.M. on 23.02.2009, with self generated numbers. Time and date are mentioned on the files and the video. These are not one, two or three files, but more than 400 files, created over a span of several hours. This "internal evidence" establishes its genuineness. Hard disk in the present case is not only a physical object, but a document within the meaning of section 3 of the Evidence Act [See Shamsher Singh Verma Vs. State of Haryana, 2015 (12) Scale 597]. The Supreme Court in Mobarik Ali Ahmed Vs. State of Bombay, AIR 1957 SC 857, has held that execution of a document can also be proved by the "internal evidence" contained in the contents of the document. The circumstantial evidence enforces our belief that the original document, i.e. hard drive, is original and authentic."*

person on the basis of mobile phone has been accepted[118].

The case of ***Bhupesh*** [119]was decided by the Bombay High Court on the point of admissibility of CCTV footage. In this case there was a murder at seven Hills Bar and Restaurant Nagpur. The accused were convicted by the Court of Sessions. Most of the eye witnesses examined by the prosecution had turned hostile. The prosecution had attached CCTV footage from the scene of offence and in cross examination these eye witnesses were confronted with the CCTV footage which clearly identified the accused. In this case the prosecution had engaged the services of a forensic computer expert who had copied the original electronic record onto a CD and DVD. In addition to that the original hard disk of the DVR containing original electronic record was also attached. However witnesses that were examined before the court were confronted only with the secondary evidence of CDs and DVDs containing the CCTV footage. It was argued by the learned counsel appearing for the accused to that the CD and DVD would not be admissible in evidence against the accused because the certificate under section 65B should have been provided by either the owner of the restaurant or the manager who had a responsible position vis a vis the electronic record. The Hon'ble Bombay High Court considered the decision of the Hon'ble Supreme court in the case of ***Anwar PV (supra***) and summarized the law on electronic evidence holding that not all conditions laid down by the case of ***Anwar PV (supra***) where complied in the instant case. However in the instant case the prosecution produced both the primary as well as secondary evidence of the electronic record. Infact, the prosecution had attached the original hard disk containing the CCTV footage from the DVR. Although the witnesses were not confronted with the original hard disk nonetheless there were no objections raised at the time when they were being confronted with the CDs and DVDs. The court found that the primary as well as secondary evidence of the electronic record is produced and the secondary evidence produced is a true and genuine copy of the primary evidence.

[118] Mohd. Arif @ Ashfaq Vs. State of NCT of Delhi (2011) 13 SCC 621
[119] Bhupesh v. State of Maharastra 2018(3) BomCR(Cri)12

In the case of ***Mohammad Ajmal Kasab***[120], the electronic evidence of VoIP, CCTV footage etc. was extensively adduced by the prosecution and accepted by the Court.

A question may arise as to what will be the status of CCTV footage when the recording and the testimony of eye witness are not corroborating with each other? In both the situations, if the CCTV footage is proper and clear and the origin of the CCTV is proved beyond reasonable doubt, it will be enough to establish the actus – reus at the instance of the accused person.

The case of ***Gubinas and Radavicius***[121], discusses the issue of genuineness of CCTV Footage. The court observed that even if all the witnesses say one thing and CCTV shows something else, then the electronic evidence will be relied upon and not the ocular evidence given by the witnesses. This observation although made by the Foreign Court makes it clear that the contents of CCTV footage is considered sufficient to establish the commission of crime and for identification of accused person.

In the case of ***C. Ramajayam@Appu Vs Inspector of Police***[122]; the facts of the case were that Dhanaram and Gunaram were brothers who owned and operated "Balaji Pawn Brokers," a pawn broking and jewellery shop. Around 8:00 a.m., the deceased Gunaram opened the store. Dhanaram arrived around 9:00 a.m. and stayed for a while before leaving for another job. He was surprised to see his brother lying in a pool of blood when he returned to the shop around midnight. He sounded the alarm, and nearby shop owners arrived. Apart from the homicide, 935 grams of gold were stolen. The accused was convicted by the trial court. The Hon'ble Madras High Court upheld the conviction. But what is novel in the matter is that in this case the Hon'ble Madras High Court had viewed the CCTV footage. In this regard, the Madras High Court has laid down guidelines by holding that during the hearing of the case the Hon'ble Court has noted

---

[120] AIR 2012 SC 3565

[121] Gubinas and Radavicius v HM Advocate, High Court at Aberdeen (2017) HCJAC 59 discussed in Prachi Agarwal, CCTV footage: A silent witness – The Criminal Law Blog *at https://criminallawstudiesnluj.wordpress.com*_Accessed on 21.9.2017 at 10.00 pm

[122] 2016 (2) CTC 135.

that the trial court has not played the DVR and has not seen the CCTV footage in the presence of the accused. To ensure that the mistake is not repeated in future the court directed that every case where a magistrate receives an electronic record he may himself view it and back it up ensuring the integrity of the source is not disturbed, in CD or a pen drive or any other gadget, by drawing a proceeding. The backup can be kept in safe custody by wrapping the same in an antistatic cover and it should be sent to session's court at the time of committal. The magistrate can avail service of an expert during this process. It was further held that articles such as Harddisk, CD, memory card, pen drive etc containing relevant electronic record are documents under section 3of the Indian Evidence Act and albeit making them as material evidence. Court has power to view CCTV footage in the presence of the accused and satisfy itself about the correctness of the facts deposed. The trial Court should also specifically put questions to the accused when he is examined under section 313 of CrPC about his overt acts. In ***Tomaso Bruno & Anr. V. State Of U.P*** [123]the court considered non production of the best available evidence namely the CCTV footage which captured the incident as a fatal defect in the case of the prosecution and acquitted the accused on that count. The court applied section 114 of the Indian Evidence Act to draw an adverse inference in that case. The second question that may arise is what is primary and secondary evidence in case of CCTV footage. Ordinarily CCTV footage is produced in form of CDs in the court of law. These CDs are accompanied by a certificate under section 65B of the Indian Evidence Act. However infact a CCTV camera records an image and this image is converted to digital form through a Digital Video Recorder (DVR). A DVR stores the electronic data and is the primary evidence. If the DVR is produced in the Court, it will be primary evidence. However, if it is not possible to produce the DVR in that case the Investigating officer copies the relevant contents on a CD by documenting the process under a panchanama and produces the same in the court. This CD has to be accompanied by a certificate under section 65B of Indian Evidence Act obtained from the person who has generated this computer output namely the CD.

[123] (2015) 7 SCC 178

In ***Rahul Adiwal***[124] court has issued directives to the police to seize any CCTV footage that is claimed to be available and ensure that copies are made and requisite certificate under Section 65B of the Indian Evidence Act, 1872 obtained in accordance with law. In case of the investigating officers omit to do so the court has directed registration of FIR under Section 166-A of the IPC against the defaulting Investigating Officer.

### 2.4.7 Whatassp Chats

Generally speaking WhatsApp chats like any other regular form of electronic record would be admissible in evidence if properly proved however the recent observation by of the Honorable Supreme Court holding that popularity is not a measure of reliability and WhatsApp messages cannot be the basis to conclude that a fact is proved has created a doubt over the admissibility of WhatsApp messages as piece of evidence. The Supreme Court asserted that anything can be created and deleted on social media these days and therefore the bench does not attach any value to WhatsApp messages[125]. The observation of Honorable Supreme Court was based on the fact such messages could be easily forged and fabricated. However prior to this observation made by the Honorable Supreme Court, in the case above, different high courts have taken contrary views.

The Hon'ble Haryana High Court in ***Rakesh Kumar Singla***[126] has held that reliance can be placed on WhatsApp messages as primary evidence for investigation provided that they are proved by producing certificate under section 65B however in that case the

[124] Rahul Adiwal v. State of Haryana CRM-M-31490-2020 (O&M) Date of decision: 11.12.2020 the Punjab and Haryana High Court

[125] A2Z Infraservices Ltd. Versus Quippo Infrastructure Ltd. (Now Known As Viom Infra Ventures Ltd.) SLP(C) No. 8636/2021The Apex court on July 14, 2021, held that What is the evidential value of WhatsApp messages these days? Anything can be created and deleted on social media these days. We don't attach any value to the WhatsApp messages.""Prima facie we are not satisfied with the HC direction for depositing the money in an escrow account. We are not considering the purported admission in WhatsApp messages. If it is not late, then go before the arbitrator and parties would be bound by the arbitrator's award.

[126] Rakesh Kumar Singla versus Union of India CRM-M No.23220 of 2020 (O&M) Punjab and Haryana High Court

prosecution has produced WhatsApp messages without a certificate under section 65B and hence the court held that those messages were inadmissible.

Further in the case of ***Ritu v. State*** [127], Delhi High Court upheld the acquittal of a rape accused based on WhatsApp chats.

In ***Ambalal Sarabhai Enterprise Ltd***[128], the Supreme Court observed that WhatsApp messages which are virtual verbal communications are a matter of evidence with regard to their meaning and its content is to be proved during the trial by evidence in chief and cross-examination".

In case of ***National Lawyers Campaign for Judicial Transparency and Reforms and others***[129]it was held that a WhatsApp forward without original cannot be treated as a document under the Indian Evidence Act. Here the petitioner wanted the police to register an FIR based on a whatsapp forward. The court noted that the learned counsel for the petitioner was unable to state what is the source of the alleged information based on which the petition was filed. The learned counsel for the petitioner stated that this information was received on social media WhatsApp platform however he was unaware of the identity of the sender or of the receiver. Notwithstanding observations made by the various High Courts as per article 141 of the Constitution of India and obiter dictum of the Supreme Court is binding and therefore the view taken by the Honorable Supreme Court on the evidentiary value of WhatsApp chats will be binding. This view however can be distinguished by holding that the view taken by the Hon'ble Supreme Court was taken in the context of business agreements which require a certain degree of formality in its transactions.

---

[127] Ritu versus State 2018 SCC ONLINE DEL 2914

[128] Ambalal Sarabhai Enterprise Ltd. v. KS Infraspace LLP Limited and Another (Civil Appeal No. 9346 of 2019)

[129] National Lawyers Campaign for Judicial Transparency and Reforms and others versus Union of India MANU/DE/1475/2017

In ***Ambalal Sarabhai Enterprise(supra)***[130] the Hon'ble Supreme Court granted injunction in a matter where the court held a prima facie case in favor of the plaintiff based on whatassp messages[131].

Similarly ***Imran Ilyas Dalla***[132]**.**the Hon'ble Bombay High Court relied upon screenshots of WhatsApp chat between the applicant accused and other accused persons to prima facie show his involvement in crime. Based on this his bail application was rejected.

In ***Mukul vs State Of Punjab***[133] relied upon a whatassp chat to come to a conclusion that the proposed accused was actually supporting the victim and not the accused and hence he could not be arraigned under section 319 of CrPC.

### 2.4.8 Electronic Ledger

In ***Samsung (India) Electronics (P) Ltd*** [134]the petitioner produced ledger statement of account of the respondent firm maintained by them for a certain period in order to show their liability. This statement was in form of a computer printout. Admittedly no certificate under section 65B of the Indian Evidence Act was attached to the said printout. For the first time in appeal an objection was raised that the document is inadmissible in evidence as there is no certificate under section 65B.Per contra it was argued that since no objection was raised when the copy of electronic ledger was admitted in evidence the objection cannot be entertained now. The Honble High Court noted that if a document is inherently inadmissible in law (in this case for want of a certificate under section 65B) it cannot be read in evidence. Though an objection as to the mode of proof can be waived an objection as to the admissibility of a document goes

---

[130] Ambalal Sarabhai Enterprise vs Ks Infraspace LLP Limited CIVIL APPEAL NO(s). 9346 OF 2019 (Supreme Court)

[131] It was held that the negotiations were widespread over time both by WhatsApp messages and exchange of emails. These collectively have correctly been interpreted to hold a prima facie case in favour of the plaintiff. The terms and conditions of payment, were all finalized which prima facie reflect the existence of a concluded contract.

[132] Imran Ilyas Dalla vs State Of Maharastra Criminal Application (BA) No.183 of 2020

[133] Crl. Revision No. 570 of 2016 (O&M)the Honble Punjab-Haryana High Court

[134] Samsung (India) Electronics (P) Ltd. v. MGR Enterprises, 2019 SCC OnLine Del 8877,

to the root of the matter can be raised at any stage of the proceedings.

In ***M/s Amritsar beverages Ltd and others***[135]***, s***ection 14 (3) of the Punjab General Sales Tax Act provided for inspection of books, documents and accounts and their seizure. As per the said Act the officer seizing the books, accounts, registers or document had to grant a receipt, retaining a copy, affixing signature and seal of the officer on the document and return of the books to the dealer. But, the seized record was cash book, ledger and other registers maintained in a hard disk. Hence, it was not possible to put signature and seal of the official on the seized hard disk. The court therefore directed the department to make a copy of the hard disk and return the original to the party.

### 2.4.9 Bank Records

Books of accounts and Bank records, that are maintained in the daily course of business in electronic form or are relevant[136]. For them to be admissible in the court of law in addition to a certificate under section 65B of the Indian Evidence Act a certificate under section 2A of Bankers Book Evidence Act should also be produced. On April 24th, 2009 RBI published a notification advising State and Central Co-operative Banks to comply with the provisions of Banker's Books Evidence Act, 1891 while furnishing certified copies and computer printouts to courts. The notification further says that if such statutory certification is not complied with, the courts will not be obliged to admit the document in Evidence without any further proof[137].

In ***M/S ICICI Bank Limited V/S Kapil Dev Sharma***[138] it was held that if a record submitted is inadmissible, it will remain inadmissible whether an objection was raised or not, or whether it was marked as an exhibit or not.

---

[135] State of Punjab and others Vs. M/s Amritsar beverages Ltd and others AIR 2006 SC 2820
[136] Section 34 of the Indian Evidence Act 1872
[137] Notification No. RBI/2008-09/457 read with RPCD.CO.RF.BC.No. 100 /07.38.03/2008-09 Dated 24.04.2009
[138] M/S ICICI Bank Limited V/S Kapil Dev Sharma 2018 Latest Caselaw 652 Del.

The Delhi High Court in Court in ***Om Prakash v. Central Bureau of Investigation*** [139] held that a conjoint reading of Section 34 of the Indian Evidence Act with Sections 2(8), 2A and 4 of the Banker's Book Evidence Act and the judgememts of the Supreme Court held that the prosecution has to lead admissible evidence to prove the entries in the books of accounts and link the same with other evidence on record to prove the offence beyond reasonable doubt. Thus the statements of accounts are admissible in evidence only if they are accompanied by certificate as envisaged under Section 2A of the Bankers' Books Evidence Act. As regards objection to admissibility and mode of proof the Hon'ble court held that an objection as to the competence of the person exhibiting the statements of account has to be taken at the time when the statements are admitted in evidence however if the statements of accounts have been exhibited without certificate under Section 2A of the Act, then the document is inadmissible and cannot be read into evidence and this objection can be taken at anytime even in appeal.

### 2.4.10 Electronic Evidence In Matrimonial Cases:

Although the scope of this research is not civil cases none the less matrimonial disputes can escalate into domestic violence, dowry harassment or adultery cases. Under these circumstances it would be apt here to take a cursory look at the judicial trend in admitting electronic evidence produced in matrimonial disputes.

In matrimonial disputes evidence may be produced in form of photographs, videos or chats on social media or social media posts. Some of this evidence may be obtained with consent and some has been stealthily obtained. It is a settled principle of law under the Indian Jurisprudence that evidence that is relevant cannot be rejected on the ground that it was obtained through illegal means[140].

---

[139] Om Prakash v. Central Bureau of Investigation 2017 VII AD (Del) 649

[140] In the case of *State of MP v. Paltan Mallah (2005) 3 SCC169 it was held that* It may also be noticed that the Law Commission of India in the 94th Report suggested the incorporation of a provision in Chapter 10 of the Indian Evidence Act, 1872. The suggestion was to the effect that in a criminal proceeding, where it is shown that anything in evidence was obtained by illegal or improper means, the

In the case of ***Deepti Kapur v. Kunal Jhulka***[141]The question was relating to admissibility of a CD containing audio video recording of a conversation between the wife of the applicant and her friend in which she allegedly spoke in a very derogatory manner about the applicant's family which according to the applicant constituted cruelty. The wife opposed the production of the CD on two counts. Firstly, that the contents of the CD have been tampered with and second that the production of the CD violated her right to privacy. In view of his objection filed by the wife the husband filed an application before the family court for referring the CD to FSL to assess the genuineness of the recording. The application was allowed. Hence a petition was filed before the High Court challenging the order of the Family Court. After considering the rival submissions and various judgements cited the court upheld the judgement of the family court. The Hon'ble High Court observed that in this case the husband had clandestinely fitted a CCTV in the bedroom of the wife. No doubt this conduct had to be deprecated and all legal consequences for that act would follow, however the court noted that there is nothing in the law that makes evidence that is obtained by illegal means inadmissible only on that ground. If the evidence is properly proved by filing certificate under section 65B of the Indian Evidence Act, the same could be used to prove a relevant fact.

However the Punjab and Haryana High Court in ***Neha vs Vibhor Garg***[142] held that recording a conversation of the wife without her knowledge is infringement of her

---

court, after considering the nature of the illegality or impropriety and all the circumstances under which the thing tendered was obtained, may refuse to admit it in evidence, if the court is of the opinion that because of the nature of the illegal or improper means by which it was obtained, its admission would tend to bring the administration of justice into disrepute. The Commission also quoted the various circumstances surrounding the proceedings that may entail the exclusion of such evidence but the suggestion of the Law Commission was not accepted and no legislation was effected in line with the recommendations of the 94th Report of the Law Commission and the position continues to be that the evidence obtained under illegal search could still be admitted in evidence provided there is no express statutory violation or violation of the constitutional provisions. For example, if certain specific enactments are made and the search or seizure is to be effected in accordance with the provisions of such enactment, the authorities shall comply with such provisions. The general provisions given in the Criminal Procedure Code are to be treated as guidelines and if at all there is any minor violation, still the court can accept the evidence and the courts have got discretionary power to either accept it or reject it.

[141] 2020 SCC OnLine Del 672

[142] CR No. 1616 of 2020 and CR No. 2538 of 2020 (O&M)

privacy and the transcripts of such conversations cannot be admissible as evidence by Family Courts[143].

However this judgement of the Punjab and Harayan High Court is subjudice before the Honble Supreme Court[144].

In ***Havoi Setna v. Kersi Gustad Setna***[145] the issue as regards production and proof of tape recorded conversation between husband and wife had come up. In this case, in a divorce proceedings the husband wanted to produce a CD which contained recorded conversations between the husband and wife on certain dates. The wife objected to the production of the CD amongst other grounds that the husband had failed to produce the original instrument on which the original conversation was recorded and further that

---

[143] It was observed by Justice Lisa Gill that" *As an aside I would say that there are voice changing software available on the Net waiting to be downloaded to be applied in hiding or creating identities, creating true or false evidence, making room for impersonation, deceit and the like, which may be hard to crack without special detection by experts specially trained in this evolving field of investigation when experts are not easily found or available presently in courtrooms which remain severely handicapped and ill equipped with newfangled tools for use or misuse of modern science and technology and to easily apply to a case in hand the repercussions of which may be far reaching and beyond one's ken. It would be a rather dangerous trend to allow people to be fixed or exposed on Audio CDs obtained by malfeasance, in its object of collecting evidence and the secretive means adopted to achieve a lawful or an unlawful end. The computer age is a dangerous age. The mobile phone or electronic gadgets should not be readily allowed to be used as an instrument of torture and oppression against a wife in a matrimonial action unless the court in satisfied that it might tilt the balance between justice and injustice in its cumulative judicial experience, wisdom and discretion in decision making. A married woman too has a valuable right to her privacy of speech with her husband in the confines of the bedroom. Couples speak many things with each other unwary that every word would be weighed one day and put under the judicial scanner. Courts should be very circumspect in such matters before allowing such applications as presented in this case. The Courts cannot actively participate in approving mischief and invite invasion of privacy rights not called for in deciding a case where parties are free to adduce evidence which may or may not be sufficient to obtain a decree of dissolution of marriage. Fools rush in where angels fear to tread.Going ahead, the Bench then holds that:he caution which has been sounded is indeed to be heeded. To permit a spouse to record conversations with an unsuspecting partner and to produce the same in a court of law, to be made the basis of deciding a petition under Section 13 of the Act, would indeed not be feasible. It is rightly observed in Deepinder Singh's case (Supra) that couples speak many things with each other, unaware that every word would be weighed in a Court of law. Moreover, the court would be ill-equipped to assess the circumstances in which a particular response may have been elicited from a spouse at a given point of time, notwithstanding the right of cross-examination."*

[144]https://www.livelaw.in/top-stories/can-husband-produce-as-evidence-secretly-recorded-phone-conversations-of-wife-in-divorce-case-supreme-court-to-consider-189316 on 26.1.2022 at 12.30 pm

[145] AIR 2011. Bom. 283

the affidavit of documents is also not filed. The Hon'ble Court considered various judgements including that of R Malkani(supra) and held that the plaintiff can confront the defendants with the CD in cross examination, if the wife admits the contents, it could be read in evidence, if the wife disputes the contents, the husband will have to prove, its contents by direct or circumstantial evidence. In case the later happens the husband may produce the original electronic record itself and seek to play it before the Court to have the voice of the wife which is disputed be identified in Court. Or the husband may apply send the tape recorded conversation for forensic analysis to identify the voice of the wife through an expert by following due process of law, regarding obtaining voice samples from the wife.

In ***X v. Z***[146] the Hon'ble Delhi High Court has issued guidelines on how to handle evidence which is of sensitive nature and is likely to affect right of privacy in matrimonial matters. This type of evidence may include video clips, text messages chat details, emails, CCTV footage etc. If in the assessment of the lawyer of the party such evidence is of sensitive in nature, then the party can apply to the court to keep such evidence in a sealed cover and the court after considering the facts of the case can permit the same.

### 2.4.11 Call Record Details(CDR)

In ***Achley Yadhav***[147] Call record details were used for conviction where the accused who made ransom calls to the victim on his the mobile number as well as the landline number of his family. As per the prosecution two landline numbers were used to make a call. The prosecution produced call record details of all calls, however failed to produce certificate under section 65B of the Indian Evidence Act of the landline phones. The court held that in such evidence despite of call record details having been proved by examining the Nodal Officer, is not admissible and set aside the conviction. The court

[146] MAT.APP.(F.C.) 78/2015 (Delhi High Court)
[147] Achley Yadhav v. State 014 (8) LRC. 236 (*Delhi*) DB

remanded the case for retrial permitting the prosecution to produce certificate under section 65B of Indian Evidence Act.

In ***Kundan Singh[148] (Delhi High Court)*** the issue was as regards reliance of CDR where the section 65B certificate was produced subsequently in re-examination by the nodal officer. The court held that the trial court correctly admitted the CDR in evidence after taking certificate under Section 65B of the Evidence Act on record . Further the court relied on the said CDR to confirm that that after the death of deceased, his mobile was used to make a call. Based on this corroborative incriminating evidence against the accused the conviction against the accused was sustained.

### 2.4.12 EMAILS

The full form of an email is electronic mail[149]. An email consists of two components namely a header and a body. The header contains details such as the sender and recipients' email ids, the date and time of sending and receiving etc. In case of an email the original electronic record is stored on the servers, therefore invariably what is produced in courts are copies or printouts taken on paper.

---

[148] Kundan Singh vs The State MANU/DE/3674/2015 Here the court held that "*The effect of the aforesaid provisions is that when a certificate under* Section 65B *authenticates the computer output, it will only show and establish that the computer output is the paper print out or media copy, etc. of the computer from which the output is obtained. The court has still to rule out when challenged or otherwise, the possibility of tampering, interpolation or changes from the date the record was first stored or created in the computer till the computer output is obtained. The focus over here is not so much on the creation of the out-put as stipulated under sub-section (2) to Section 65B, but rather on the preservation and sanctity of the record after it was originally created. It extends beyond identification of the particular computer equipment and the process or equipment used for computer output, etc. It would relate to the policies, procedures for use of the equipment that stored the said information since creation and data base and integrity of the same. Questions which would arise and have to be answered is whether data base was protected and had no or limited access, which permits modification/alteration; whether the data base could be wrongly lodged or created or could be transferred or changed when the data base was transferred and stored in the backup systems. These are questions which are pertinent and have to be examined to ascertain whether or not there was possibility of change, alteration or manipulation in the initial or original data after it was created. The courts must rule out that the records have not been tampered and read the data or information as it originally existed. These are aspects which are not codified as such, for probative value is examined on the case to case basis keeping in mind the relevant facts"*.

[149] Britanica defines email, messages transmitted and received by digital computers through a network. An e-mail system allows computer users on a network to send text, graphics, sounds, and animated images to other users *https://www.britannica.com/technology/e-mailm on 12.1.2019 at 10.00 p.m.*

In ***Abdul Rehman Kunji v. State of West Bengal***[150] the Hon'ble High Court of Calcutta while deciding the admissibility of email held that an email downloaded and printed from an email account of the person can be proved by virtue of Section 65B r/w Section 88A of Evidence Act. The testimony of the witness to carried out such a procedure, downloaded and print the same is sufficient to prove the electronic communication.

In ***Smt Bharathi V Rao v. Sri Pramod G Rao,***[151] it was held that emails come under the definition 'electronic record' and are admissible in evidence.

### 2.4.13 Photos And Videos:

In ***Fatima Riswana***[152] the prosecution was relating to exploitation of certain men and women for the purpose of making pornographic photos and videos in various acts of sexual intercourse and thereafter selling them to foreign websites. The case was allotted to fast track court presided over by a lady judge. The accused applied for copies of the CDs. The trial court rejected that prayer. The High Court, also rejected such prayer by observing that if their copies are provided, they can be copied further and put into circulation. However, the High Court allowed viewing of the CDs in the chamber of the judge. It was contended on behalf of the accused that it may cause embarrassment to the lady judge. Hence, the matter was directed to be transferred to the court of a male judge. However the concern of the victim side was not considered. The apex court observed that a judicial officer be it a female or male is expected to face this challenge when call of duty required it. Hence that order was set aside.

In ***Amulya Kumar Panda***[153] a CD containing Section 27 statement of the Indian Evidence Act was exhibited without objection of the accused. The court allowed it to be played to the extent of S.27 statement that may be admissible in law.

---

[150] Abdul Rehman Kunji v. State of West Bengal 2016 CrLJ 1159
[151] Smt Bharathi V Rao v. Sri Pramod G Rao MANU/KA/3243/2013
[152] Fatima Riswana Vs State and others AIR 2005 SC 712
[153] Amulya Kumar Panda Vs State of Orissa 2008 CRI. L.J. 1676

In ***G Shyamala Ranjini***[154] it was held that a CD without S.65B certificate cannot be allowed in cross examination.

In ***Preeti Jain vs Kunal Jain***[155] a divorce petition was filed by the husband on the ground of adultery. He has relied upon evidence recorded on a pin hole camera. The original electronic record was produced without a certificate under section 65B. Wife filed an application under section 65B r/w section 122 of the Indian Evidence Act stating that the electronic record cannot be read in evidence as it is not properly certified and secondly that the same is a privileged communication between husband and wife. Rejecting the contention of the wife the court held that since the original electronic record was produced before the court it being primary evidence did not require the support of any certification. As regards section 122 of Indian Evidence Act.[156] It was held that the recording cannot be considered a privileged communication in view of the exception provided in the section itself and by virtue of section 14 of the Family Court Act 1987[157].

In ***S.K. Saini***.[158] it was held that the recording that was sought to be relied upon as evidence was carried out on a Micro-Cassette Recorder along with transmitter and a Micro Cassette from the same was sealed. The Original Micro Cassette has never been

---

[154] G Shyamala Ranjini Vs. M.S. Tamizhnathan AIR 2008 Mad 476 in that case a CD was produced at the time of cross examination without Sec.65B certificated, but the same was rejected by Hon'ble Court on the ground that, 'although the electronic record is admissible in evidence, but for that purpose the person who is producing the evidence has to satisfy the conditions mentioned under sub-section (2) of Sec. 65B of the Indian Evidence Act and is also required to produce a certificate as enumerated under sub-section (4) of Sec. 65B of Indian Evidence Act.'

[155] Preeti Jain vs Kunal Jain &Anr 2016 SCC OnLine Raj 2838 Decided on 27.05. 2016

[156] Section 122 of the Indian Evidence Act : Communications during marriage.—No person who is or has been married, shall be compelled to disclose any communication made to him during marriage by any person to whom he is or has been married; nor shall he be permitted to disclose any such communication, unless the person who made it, or his representative in interest, consents, except in suits between married persons, or proceedings in which one married person is prosecuted for any crime committed against the other.

[157] Section 14 in The Family Courts Act, 1987 Application of Indian Evidence Act, 1872.-A Family Court may receive as evidence any report, statement, documents, information or matter that may, in its opinion, assist it to deal effectually with a dispute, whether or not the same would be otherwise relevant or admissible under the Indian Evidence Act, 1872 (1 of 1872). -A Family Court may receive as evidence any report, statement, documents, information or matter that may, in its opinion, assist it to deal effectually with a dispute, whether or not the same would be otherwise relevant or admissible under the Indian Evidence Act, 1872 (1 of 1872

[158] S.K. Saini & Anr vs C.B.I.Crl. A. No.159/2005 decided on 19.08.2015(Hon'ble Delhi High Court)

produced before the Court and has not even been sent for CFSL examination. The Court noted that as per the report dated 8th March, 2002, a copy of the original cassette was made prior to sending it to the SSO Division. This copy is not accompanied by a certificate under section 65B and therefore recording could not be read in evidence.

In ***Raj Kumar***[159] the Hon'ble Delhi High court admitted a mobile phone which contained the original photograph without certificate under section 65B in evidence. In ***Sanju v. State of M.P***[160], the order of the trial court by which it was held that a tape recorded conversation without a certificate under section 65B of Indian Evidence Act could be produced in evidence was it was challenged by the petitioner. The conversation was recorded on the mobile of Haresingh and was copied on a CD and pendrive by one Banesingh which CD and pendrive was intended to be produced in evidence. The court examined the effect of the judgement of the Honorable Supreme Court in the case of Anwar and Mohammed Shafi and held that since the person producing the tape recorded conversation was also the author of the Cd and the Pendrive that contained the conversation it was mandatory for him to produce a contemporaneous certificate under section 65B without which the electronic record could not be made admissible. In other words the certificate under section 65B should be prepared on the same date when the CD and the pendrive was prepared.

In ***Surendra***[161] an application was filed by the accused for bail raising a plea of alibi. The accused relied on a photograph, the metadata of which showed that the photograph was taken at a distance of 60 to 70 kms from the scene of the offence the photograph was forensically examined. The court considered this electronic evidence and noted that digital forensic evidence and metadata of a photograph is a big tool in the hands of the forensic expert and courts are expected to scrutinise this tool with care and deep study. Meta data photos etc and report of digital forensic expert should carry due certification as per the Indian Evidence Act.

---

[159] Raj Kumar v. State CRL.A. 232/2016
[160] Sanju v. State of M.P 2019 SCC OnLine MP 2070
[161] Surendra v. State of MP M.Cr.C. No.15796/2020

### 2.4.14 Sample Certificate Under Section 65B

A sample certificate u/s. 65B of the Evidence Act is available in the reported case of ***Ark Shipping Co. Ltd.***[162]**.** It was held that certificate can be filed at the time the electronic record is tendered in evidence and need not be necessarily produced at outset[163].

### 2.4.15 Competency To Sign The Certificate

In ***Brajesh Tiwari*** [164]the case of the petitioner was that the prosecution has relied upon call record details and they could not be admissible without a certificate under section 65B of the Indian Evidence Act as such it was necessary to issue direction to the witness Rajiv Bhadoria to produce a certificate under section 65B of Indian Evidence Act. The Honorable Court noted that Rajiv Bhadoriya was in charge of Cyber Cell Superintendent of Police Patna. He was not an officer of Bharti Airtel Limited in whose servers the call record details were saved and therefore he did not fall in the category of the person occupying a responsible official position in relation to the operation of the relevant device or management of relevant activity. As such he would not be competent to issue a certificate as required under section 65B of the Indian Evidence Act.

### 2.4.16 Stage For Producing Certificate Under Section 65B.

In the case of ***Paras Jain*** [165] the Rajasthan High Court was confronted with the issue of whether a "contemporaneous certificate" under Section 65-B is required for admissibility of a CD in evidence. The Court relied upon *Anvar P.V(supra) and* opined that such certificate is not required to be filed with charge-sheet and the only

[162] Ark Shipping Co. Ltd. Vs. GRT Shipmanagement 2007 (6) Bom.C.R. 311.
[163] Avadut Waman Kushe Vs. State of Maharashtra, 2016 SCC Online Bom 3256 see also Paras Jain Vs State of Raj decided on 4.07.2015 by Rajastan HC Nyati Builders Pvt Ltd v Mr Rajat Dinesh Chauhan, 2015 SCC OnLine Bom 7578
[164] Brajesh Tiwari vs The State Of Madhya Pradesh Writ Petition 4834/2015 Madhya Pradesh High Court.
[165] Paras Jain v. State of Rajasthan (2016) 2 RLW 945 (Raj).

requirement is to ensure that the certificate is produced before the issue of admissibility of evidence is considered by the court. Held that just like how the court has powers to permit additional evidence even after the filing of the charge sheet if the court of the opinion that additional evidence is essential for the trial of the case, how can it be said that a certificate under section 65B cannot be permitted to be subsequently produced merely because it was not produced along with the charge sheet. This view was affirmed by the Hon'ble Supreme court in ***Arjun Panditrao Kotkar (Supra).***

The Hon'ble Delhi High Court as well in ***Kundan Singh***[166] applying the ratio of *Anvar P.V(supra)* held that the law does not require a simultaneous or contemporaneous certification under section 65B of the Indian Evidence Act. The High Court opined that admissibility and authenticity are two different aspects and Section 65-B pertains to only admissibility and is not about authenticity of the electronic record produced.

In ***Avadut Waman Kushe***[167] the Honble High Court of Bombay decided the question as to whether certificate under Section 65-B(4) must necessarily be filed simultaneous with the electronic record or whether it can be filed at any subsequent stage of proceedings. Answering the said question the High Court independently observed that Section 65-B does not specify the stage of production of certificate. It can be filed when the record is tendered in evidence as subsequent filing of the certificate does not reduce its effectiveness.

The Madhya Pradesh High Court however has taken a contrary view. In ***Kamal Patel***[168] it was held that a contemporaneous certificate under section 65B is mandatory when an electronic record is produced in evidence. It was further held that that where the record is subsequently transferred on a number of occasions a contemporaneous certificate at the time of each transfer is necessary.

---

[166] Kundan Singh v. State 2015 SCC OnLine Del 13647
[167] Avadut Waman Kushe v. State of Maharashtra 2016 SCC Online Bom 3256.
[168] Kamal Patel v. Ram Kishore Dogne 2016 SCC OnLine MP 938 : (2016) 1 MP LJ 528

Although till date there is no judgment of the Hon'ble Supreme court answering this pointed question as to at what stage a certificate under section 65B has to be filed, in ***State v. MR Hiremath***[169], the Hon'ble Supreme Court held that the High Court had erred in coming to a conclusion that the accused was entitled to be discharged because the prosecution had failed to produce a certificate under section 65B of the Indian Evidence Act along with the chargesheet when it relied upon a Spy Camera in a trap case. The Honorable Supreme Court held that the need of a certificate would arise only when the electronic record is tendered in evidence. The Supreme Court relied upon the judgement in the case of ***Union of India and others v. Commander Ravindra V Desai***[170], where it was held that non production of a certificate under section 65B of the Indian Evidence Act is a curable defect.

In ***State of Rajasthan through the Special P.P. Vs. Sri Ram Sharma*** and others, S.B.[171], the Hon'ble High Court of Rajasthan allowed prosecution application filed under Sec. 311 Cr.P.C. for submitting certificate under Sec.65B, prepared by investigation officer after closing of defence evidence, regarding electronic evidence of conversation between complainant and accused, relating to illegal gratification.

In ***Ignatius Topy Pereira Vs. Travel Corporation (India) Pvt. Ltd and another***[172]**,** If the certificate under S.65B, Evidence Act which was produced was rejected as not in consonance with the Section 65B a fresh certificate may be produced.

This chapter therefore gives a succinct description of Indian Law on electronic evidence and further demonstrates as to how proactively the law has been explained, interpreted and developed by judicial precedents.

In the next chapter the researcher has studied Global conventions and Models laws that influenced the in enactment of the Indian Legislature on electronic evidence. As this

[169] State v. MR Hiremath AIR 2019 SC 2377
[170] Union of India and Others v CDR Ravindra V Desai (2018) 16 SCC 272. ( 2018) 16 SCC 272
[171] State of Rajasthan through the Special P.P. Vs. Sri Ram Sharma Crl. Misc. Petition No. 4383/2016 dt. 02.09.2016
[172] 2016 SCC Online Bom 97

research is strictly confined to electronic evidence, there is no must emphasis in studying the Information Technology Act 2000. However a reference to the Act is imperative as the Information Technology Act 2000 has led to the statutory recognition of electronic evidence.

# Chapter 3

# International Conventions And Model Laws On Electronic Evidence And Genesis Of Indian Law.

## 3.1 Introduction

Despite of the researcher elucidating the concept of electronic evidence under the Indian law in chapter 2, a study on this subject would be incomplete without studying the global evolution of electronic evidence and its impact on the Indian law.

Before embarking into this chapter one must understand the concept of cyberlaw and its connection with the present subject of research namely: use admissibility and proof of electronic evidence. Simply put cyberlaws are laws governing cyber spaces. The matters covered by cyber laws are cyber crime, electronic commerce, Data Protection, Data Privacy and may also include intellectual property rights in as much as they relate to cyber space. The Conventions that are proposed to be discussed in this chapter essentially fall within the domain of the concept of cyber laws that is not strictly the subject matter of the present research however all the law that governs the admissibility and mode of proof of electronic evidence has emanated from these conventions. The primary source of cyber law in India which is the Information Technology Act 2000, is heavily influenced by some of these conventions, which called upon nations to enact legislations to recognise electronic means of communications. These conventions brought electronic form of communication in par with paper documents. Hence most of its provisions have been replicated in the Indian Law. Thus a study on electronic evidence is incomplete without a reference to these conventions and subsequently a reference to the Indian Cyber law namely the Information Technology Act, 2000.

## 3.2 International Conventions and Model Laws

The United Nations Organization as a global body noted somewhere in the late 80's that in the last generation or two, there is enormous expansion of rapid communication by

electronic means. The diversity of national laws made matters relating to electronic mode of communication complicated. E- commerce has had a dramatic impact on the way business was done globally. There was as a serious dearth of legal rules governing the same. Hence the United Nations mooted an idea of a global law that would set up a protocol on electronic correspondence. Hence the UNCITRAL Model Law on Electronic Commerce was enacted in the year 1996.

### 3.2.1 UNCITRAL Model Law On Electronic Commerce 1996

This Model Law was enacted in response to a major shift in the means by which communications are made between parties using computerized or other modern techniques in doing business. The Model Law was adopted with an intent that it would serve as a model to countries for the modernization of certain aspects of their statutes and practices in the field of commerce involving the use of computerized or other modern techniques, and for the enacting a relevant legislation in that regard, where none presently exists.

The Model Law on Electronic Commerce (MLEC) purports to serve as a template that would facilitate commerce conducted by use of electronic means with a set of internationally acceptable rules. In particular, it was intended to overcome the hurdles that arise from statutes by providing equal treatment to paper-based communication and electronic communication.

The MLEC was the first legislative text to adopt the fundamental principles namely of (a) non-discrimination, (b) technological neutrality and (c) functional equivalence which principles are regarded as the founding elements of modern electronic commerce law. The principle of non-discrimination guarantees that no document shall be denied of legal effect, validity or enforceability solely on the grounds that it is in an electronic form. The principle of technological neutrality requires States to adopt such provisions which are neutral in respect to technology used in electronic communication. The aim was to accommodate any future developments without any further legislative amendments. The functional

equivalence principle lays out criteria in for electronic communications to bring it in par with to paper-based communications.

The law has enacted rules for the formation and validity of contracts concluded by electronic means, for the attribution of data messages, for the acknowledgment of receipt and for determining the time, place for dispatch or receipt of data messages.

The UNCITRAL after acknowledging that the use of automatic data processing (ADP) is about to become firmly established throughout the world felt the need for a unification of the rules of evidence for the use of computer records in international trade and commerce. Accordingly the model law was adopted on 16th December 1996.

The model law is divided into two parts. The first part contains general provisions relating to e-commerce, enunciating the above three principles. The second part deals with Electronic Commerce in specific areas such as carriage of goods.

The model law applies only to data messages[173]which relate to international commerce and it does not override any rule of law that is intended to protect the consumers. Further the model law provides that the signatory States may wish to extend the applicability of the law to any kind of information in form of data message.

The key definition under this Act is of the term data message. A data message means information generated, sent received or stored by electronic, optical or similar means including but not limited to electronic data interchange(EDI) electronic mail, telegram, telex and telecopy. The model law defines terms such as Electronic data interchange, originator addressee, intermediary and information system[174]. The highlight of the model law is that the law recognizes "a data message" as a valid mode of communication for dispensing information.

The model law gives recognition to digital signatures and presentation of information in

[173] Model Law on Electronic Commerce 1996Artilce 2(a) "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy
[174] Article 2(b) ibid

original digital form. It urges the States to devise a method which guarantees that the integrity of the data is preserved[175].

The model law further provides that in any legal proceedings, nothing in the application of the rules of evidence, shall apply so as to deny the admissibility of a data message in evidence solely on the ground of it being a data message or on the ground that it is not in original form if it is the best evidence that the person in whose possession it is could obtain[176]. In this process due weightage has to be given to the reliability of the manner in which the data message was generated, stored or communicated, the manner in which its integrity was maintained and to the manner in which its originator was identified. Also to any other factor found relevant[177].

As regards retention of data messages the model law provides that where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that (a) the information contained therein is accessible so as to be usable for subsequent reference; and (b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and (c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received[178]. The Model Law further contains provisions relating to retention of data messages[179], formation and validity of contracts electronically[180], attribution of data messages, issues of its dispatch, receipt, the time and place of dispatch and its receipt[181]. The Information Technology Act 2000 which is an Indian legislation is substantially based on this Model law.

[175] see Article 6, Article 7 and Article 8
[176] Article 9
[177] Article 9
[178] Article 10
[179] Article 10
[180] Article 11
[181] Article 13, Article 14 and Article 15

### 3.2.2 UNCITRAL Model Law on Electronic Signature 2001:

With the advancement of technology all around the world, handwritten signatures were slowly be replaced with electronic authentication techniques (generally referred to as electronic signature). As there were divergent legislative approaches of various States in authentication procedure a need was felt to establish uniform legislative provisions. Building on the fundamental principles underlying Article 7 of the UNCITRAL Model Law on Electronic Commerce with respect to the fulfilment of the signature function in an electronic environment, a need was felt to design a new Model Law to assist States in establishing a modern, harmonized and fair legislative framework to address more effectively the issues of electronic signatures.

It was noted by the Commission constituted for enactment of this law that a number of issues remained unsolved even after the passage of the Model Law on Electronic Commerce, namely, the possibility to enable use of electronic communications in cases where a formal written requirement is mandated by another treaty, usually drafted before the widespread use of electronic means. Finally, it was felt that some of the provisions of the Model Law on Electronic Commerce and of the Model Law on Electronic Signature could be outdated and complemented[182]. The enactment of the Model Law on Electronic Commerce led to increased use of electronic means of communication and correspondence in international trade and commerce. With the advent of technology, authentication techniques also changed and the manual process of signatures now came to be replaced by digital/ electronic signatures. The use of electronic mail as standard mode of communication gave rise to issues relating to its authentication. The UNCITRAL Model Law on Electronic Signatures was adopted on 5 July 2001, as it appears in annexure II to the report of the United Nations Commission on International Trade Law in its thirty-fourth session, together with the Guide to Enactment of the Model Law. Just like the Model Law on Electronic Commerce the Model Law on Electronic Signature also provides that this law applies where electronic

[182] Alysia Davies, "The Development of Laws on Electronic Documents and E-Commerce Transactions", Parliament of Canada, Library of Parliament Research Publications, Background Paper No. PRB 00-12-E.

signatures are used in the context of commercial activities and does not override any rule of law intended for the protection of consumers. Article 2(a) of the Model Law defines electronic signatures[183]. The most important articles in this Model law are Articles 6, 7 and 8**.** Where the law requires a signature of a person, that requirement is met in relation to a data message if it is electronically signed and the conditions laid down by Article 6 have been satisfied[184].

The question arises however as to who will determine whether the conditions laid down in Article 6 have been satisfied. The Model Law on Electronic Signature provides that **a**ny person, organ or authority, whether public or private, specified by the enacting State as competent may determine which electronic signatures satisfy the provisions of Article 6 of this Law. Provided that any such determination shall be consistent with recognized international standards[185].Here the role of the signatory has been given vital importance. Article 2(d) defines a signatory as a person who holds signature creation data and acts, either on its own behalf or on behalf of the person it represents[186].

---

[183] Article 2(a) of the UNCITRAL Model Law on Electronic Signatures (2001) "Electronic signature" means data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained in the data message.

[184] Article 6. 1. Where the law requires a signature of a person, that requirement is met in relation to a data message if an electronic signature is used that is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement. 2. Paragraph 1 applies whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature. 3. An electronic signature is considered to be reliable for the purpose of satisfying the requirement referred to in paragraph 1 if: (a) The signature creation data are, within the context in which they are used, linked to the signatory and to no other person; UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001 3 (b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person; (c) Any alteration to the electronic signature, made after the time of signing, is detectable; and (d) Where a purpose of the legal requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable. 4. Paragraph 3 does not limit the ability of any person: (a) To establish in any other way, for the purpose of satisfying the requirement referred to in paragraph 1, the reliability of an electronic signature; or (b) To adduce evidence of the non-reliability of an electronic signature.

[185] Article 7

[186] Article 2(d) ibid

The Law lays down the responsibilities of certification service provider and enunciates the principle of trustworthiness in Article 10. Article 12 provides for recognition of foreign certificates and electronic signatures if it offers a substantially equivalent level of reliability.

### 3.2.3 The United Nations Convention on the Use of Electronic Communications In International Contracts

The United Nations has adopted a Convention namely "The United Nations Convention on the Use of Electronic Communications in International Contracts". The Convention addresses different policy goals:1) it removes obstacles arising from formal requirements contained in other international trade law treaties; 2) it provides a common substantive core to the law of electronic communications, thus ensuring a higher level of uniformity both in the legislative text and in its interpretation; 3) it updates and complements the provisions of the MLEC and of the MLES; 4) it provides core legislation on electronic communications to those States not having yet any, or having partial and insufficient provisions[187]. However as India has not ratified the convention the researcher does not propose to dwell further into it[188].

### 3.2.4 The UNCITRAL Model Law on Electronic Transferable Records, 2017

The UNCITRAL Model Law on Electronic Transferable Records ("MLETR") is a uniform model law that has been adopted by the (UNCITRAL) on 7th December 2017. It applies to the use of transferable documents and instruments[189] in electronic form.

---

[187] L. Castellani, 'The United Nations Electronic Communications Convention - Policy Goals and Potential Benefits', 19(1) Korean Journal of International Trade & Business Law 1 (2010), at 2.

[188] https://mea.gov.in/ Images/attach/lu6353.pdf *assessed on 14.5.2016 at 1.30 pm*

[189] Article 2 defines "Transferable document or instrument" as a document or instrument issued on paper that entitles the holder to claim the performance of the obligation indicated in the document or instrument and to transfer the right to performance of the obligation indicated in the document or instrument through the transfer of that document or instrument.

Examples of transferable documents are bills of lading, promissory notes , bills of exchange, warehouse receipts etc.

The Model law is divided into four parts namely: general provisions; provisions on functional equivalence; use of electronic transferable records; and cross-border recognition of electronic transferable records. The law applies to Electronic transferable record which are records that comply with the requirement of Article 10[190].

The Model Law provides for non discrimination of an electronic transferable record on geographical grounds.

Therefore summarily stated these Model Laws or international conventions lay down uniform rules for use of electronic records in international commerce and correspondence. Incidentally these model rules also served as a template for the passage of local laws on electronic records of its signatories.

### 3.3 Brief Overview of the Information Technology Act 2000

In the beginning of the 21st century, technology had started to knock the doors of Indian commerce. Its usage slowly and surely perpetrated into the lives of the people and just as was globally felt, the Indian Parliament felt the need for a law that would lay down definitions and recognise use of technology. In that process it also thought that it would to some extent give effect to the resolution by which the General Assembly adopted Model Law on Electronic Commerce adopted by the United Nations Commission on

[190] Article 10 provides that "Where the law requires a transferable document or instrument, that requirement is met by an electronic record if: (a) The electronic record contains the information that would be required to be contained in a transferable document or instrument; and (b) A reliable method is used: 10 UNCITRAL Model Law on Electronic Transferable Records (i) To identify that electronic record as the electronic transferable record; (ii) To render that electronic record capable of being subject to control from its creation until it ceases to have any effect or validity; and (iii) To retain the integrity of that electronic record. 2. The criterion for assessing integrity shall be whether information contained in the electronic transferable record, including any authorized change that arises from its creation until it ceases to have any effect or validity, has remained complete and unaltered apart from any change which arises in the normal course of communication, storage and display."

Trade Law.

As a consequence of which the Information Technology Act 2000 was passed which came into force on 17th May 2000. The Act states its objective to legalise e-commerce and further amend the Indian Penal Code 1860, the Indian Evidence Act 1872, the Banker's Book Evidence Act1891 and the Reserve Bank of India Act 1934[191]**.** The basic purpose was to incorporate the changes in these the existing laws so as to make them compatible with the Act of 2000[192].

The Information Technology Act, 2000, was passed as the Act No.21 of 2000[193]. By adopting this cyber legislation India became the 12th nation in the world to adopt a Cyber Law regime during 2000.The Act extends to the whole of India and except as otherwise provided, it also applies to any form of contravention which is committed outside India by any person[194]. The Act however does not apply to documents or transactions specified in First Schedule[195].

As per the Preamble of the Act, the Act envisaged to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication. The secondary purpose of enacting the Act was to amend the Indian Penal Code; the Indian Evidence Act, 1872; the Bankers' Books Evidence Act, 1891; and the Reserve Bank of India Act, 1934 and for matters connected to electronic data interchange and other means of electronic communication[196].

The original Act consisted of 94 sections, 13 chapters and 4 schedules. The Act was

---

[191] Preamble

[192] Shashirekha Malgi "Cyber Crimes under Indian IT Laws IJSER journal ISSN 2229-55182 *http://www.ijser.org*

[193] The Information Technology Act got President assent on 9th June 2000 and it was made effective from 17th October 2000.

[194] Section 1 of the Act

[195] These documents and transactions are 1.Negotiable Instrument (Other than a cheque) as defined in section 13 of the Negotiable Instruments Act, 1881;2.A power of attorney as defined in section 1A of the Powers of Attorney Act, 1882;3.A trust as defined in section 3 of the Indian Trusts Act, 18824.A will as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition5.Any contract for the sale or conveyance of immovable property or any interest in such property; 6.Any such class of documents or transactions as may be notified by the Central Government

[196] Preamble

subsequently and substantially amended by Information Technology Act Amendment Bill 2008 and the Act was renamed as Information Technology (Amendment) Act 2008. The Act gives an impetus to electronic governance by giving legal recognition to electronic records and digital signatures. It defines cyber crimes and prescribes penalties against persons committing them. It contemplates appointment of a Cyber Appellate Tribunal to resolve disputes arising from this new law.

### 3.3.1 Important Definitions under the Act

Section 2 of the Act contains several important definitions. It enlists the definitions of various relevant expressions. Interestingly the term cyber crimes have not been defined under the Act. In common parlance a cyber crime[197] is a crime that uses computer as a weapon for committing a crime or computer is the object on which a cyber crime is committed. "**Computer**" is defined under the Act as any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetical, and memory functions by adopting the process of manipulations of electronic, magnetic or optical impulses[198]. The definition of the word computer is broad enough to include any data processing device.

"**Data**" has been defined as a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared or processed in a

[197] An interesting definition of cyber crime was provided in the "Computer Crime: Criminal Justice Resource Manual" published in 1989. According to this manual, cyber crime covered the following: (1) computer crime i.e. any violation of specific laws that relate to computer crime (2) computer related crime i.e. violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution (3) computer abuse i.e. intentional acts that may or may not be specifically prohibited by criminal statutes. Any intentional act involving knowledge of computer use or technology is computer abuse if one or more perpetrators made or could have made gain and / or one or more victims suffered or could have suffered loss.

[198] Section 2(i) defines computer as computer means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer system or computer network;

formalized manner..

"**Electronic Record**" is defined as any data generated, image or sound that is stored, received or sent in an electronic form or micro film or computer generated micro fiche[199];

### 3.3.2 Digital Signature and Electronic Signature

The Act originally dealt with only "Digital Signature" defined as authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3[200].However vide the Amendment Act of 2006, the Act first introduced the term "electronic signature" as authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature[201]. The Act also defines Public key and Private Key in the context of digital certificates.

Section 3 recognises the use of digital signature to authenticate electronic records. It provides for the use of algorithm hash function to generate a hash result using public and private keys. After 2008 the Act also recognized electronic signature as a means of authenticating electronic document. The electronic authentication technique is specified in the Second Schedule of the Act[202].

### 3.3.3 Legal Recognition of Electronic Records

[199] Section 2(t) defines electronic record as data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche; Further section 2(r) defines "Electronic Form" with reference to information as any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device; section 2(v) defines information as information‖ includes 2 [data, message, text,] images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche;

[200] Section 2(r)

[201] Section 2(ta)

[202] Section 3A

The most important achievement of this Act is that it gives legal recognition to electronic records and makes electronic record in par with tangible documents. Section 4 of the Act provides that where any law provides that information or any other matter shall be in writing or in the typewritten or printed form, then, notwithstanding anything contained in such law, such requirement shall be deemed to have been fulfilled if that information is rendered or made available in an electronic form; and is accessible for a subsequent reference. The Act makes of electronic signatures in par with handwritten signatures[203].

The law further provides for filing of any form, application or any other document with any authority, or the issue or grant of any licence, permit, sanction or approval or the receipt or payment of money in electronic form[204].

On the aspect of retention of records the Act provides that where any law mandates that documents, records or information be retained for a specific period, then the requirement will be said to have been met if the documents are retained in electronic format and if the information contained therein remains accessible for subsequent reference in the format in which it was originally created, generated, sent or received and further the details which will help the identification of origin, destination, date and time of despatch or receipt of the electronic record is available in the electronic record. These conditions are not applicable to electronic documents which are generated automatically, solely for the purpose of enabling an electronic record to be dispatched and received. Likewise the law shall not apply to any provision that expressly provides for retention of documents, records or information in the form of electronic records[205].

Section 7A of the Act brings audit of physical documents in par with electronic documents.

The Act allows publication of rule, regulation, etc in electronic gazette thus bringing

[203] Section 5
[204] Section 6
[205] Section 7

them in par with official Gazettes[206]. Although the Act gives recognition to electronic records it does not however give a right to person to insist upon the State Government or the Central Government that it must accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.

The 2008 amendment also recognises the validity of contracts formed through electronic means[207] and empowers the Central Government to make rules in respect of electronic signature. Section 10A recognizes contracts formed by electronic means and provides that no such contract shall be deemed to be unenforceable only on the ground that it was found to electronically created.

### 3.3.4 Attribution Acknowledgement and Dispatch of Electronic Records.

Chapter 4 of the Act deals with attribution, acknowledgement and dispatch of electronic records. This is one of the most important chapters as it identifies certain aspects which are vital to the understanding and admissibility of electronic records in evidence.

Section 11 of the Act provides that an electronic record shall be attributed to the originator if it is sent by the him or by any person authorized by him or by any information system which is programmed by the originator to operate on his behalf automatically. In cases where the fact in issue is whether a particular electronic document has been sent by one person or not, this section plays a very important role. If it is shown by the prosecution that there is material to believe that the electronic record has been sent by the originator or any person authorized by him or any information system which is programmed by the originator a presumption can be drawn that he only has operated it.

Once the originator is identified. The quest would be to find out whether the record

[206] Section 8
[207] Section 10A.

reached its source. Hence there must be a clear legal provision that recognises a particular mode in which the receipt is acknowledged. This issue essentially arises in matters of contracts. Section 12 of the Act provides that where acknowledgement of electronic record has to be given in a particular form or a particular manner then the addressee has to acknowledge the of receipt of the electronic record, in such a case the addressee will acknowledge the receipt of the same either by communicating such receipt, through automated or other means; or in such a manner that the conduct of the addressee is sufficient to indicate to the originator that the electronic record has been received. The provision further deals with eventualities when the originator stipulates that the transaction will be binding only upon the receipt of an acknowledgement[208].

Where issues relating to emails arise, the time and place of dispatch is relevant. The originator and the addressee can agree to the time and place of receipt of the electronic record. Generally, when an electronic record enters a computer resource outside the control of the originator or when it enters the computer resource of the addressee, it is deemed to have been the time of receipt[209].

As regards the place of dispatch, an electronic record is deemed to be dispatched and received at the place of business of the originator or the addressee even if their computer resources are located at any other place. If neither of them have a place of business, their usual place of residence will be deemed to be the place of business[210].

### 3.3.5 Secure Electronic Records and Digital Signatures

Digital signature is defined under section 2(p) as a means authentication of any electronic record as per the provisions of section 3, of the Act[211]. Section 3 of the Act recognises the use of digital signature as a means of authentication of electronic records

[208] section 12 ibid
[209] Section 13 ibid
[210] Section 13(c)
[211] section 2(p) -digital signature means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3;

by its affixation on the electronic record. It provides for the use of asymmetric crypto system and hash function. While a unique private key is used to authenticate the electronic record, any person can verify the electronic record by the use of a public key. Section 3A recognises the use of electronic signature or electronic authentication technique for authentication any electronic record[212]. It is pertinent to note that section 3 or 3A does not derecognise electronic records that have not been authenticated by use of digital signatures. Practically is puts digital signatures or electronic authentication techniques in par with manual signatures.

Section 15 lays down when an electronic signature shall be deemed to be a secure electronic signature[213]. An electronic or digital signature can only be issued by a certifying authority[214]. Chapter VI deals with regulation of certifying authorities and appointment of controllers. Sections 21 to 25 deals with the procedure to apply for, grant, revoke, renew and suspend licence. Chapter VII deals with issuance of electronic signature certificates and chapter VII provides for duties of subscribers of digital certificates.

---

[212] section 3A of the Act provides that (1) Notwithstanding anything contained in section 3, but subject to the provisions of sub-section (2), a subscriber may authenticate any electronic record by such electronic signature or electronic authentication technique which— (a) is considered reliable; and (b) may be specified in the Second Schedule. (2) For the purposes of this section any electronic signature or electronic authentication technique shall be considered reliable if (a) the signature creation data or the authentication data are, within the context in which they are used, linked to the signatory or, as the case may be, the authenticator and to no other person; (b) the signature creation data or the authentication data were, at the time of signing, under the control of the signatory or, as the case may be, the authenticator and of no other person; (c) any alteration to the electronic signature made after affixing such signature is detectable; (d) any alteration to the information made after its authentication by electronic signature is detectable; and (e) it fulfils such other conditions which may be prescribed. (3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated. (4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the Second Schedule: Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable. (5) Every notification issued under sub-section (4) shall be laid before each House of Parliament.]

[213] Section 15 provides that An electronic signature shall be deemed to be a secure electronic signature if- (i) the signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and (ii) the signature creation data was stored and affixed in such exclusive manner as may be prescribed.

[214] section 2(g) of the Act defines Certifying Authority‖ means a person who has been granted a licence to issue a electronic signature Certificate under section 24;

### 3.3.6 Provisions Relating To Data Protection and Data Tampering.

Section 43 of the Act makes unauthorised access to a computer or a computer operating system culpable. Access also includes downloads, making copies extracting any data, introducing any computer contaminant, causing damage, causing disruption, denial of authorized access, providing assistance to any person to facilitate access in contravention of the provisions of this Act, rules or regulations made thereunder, charging the services availed of by a person to the account of another person by tampering with or manipulating any computer, destroying, deleting or altering any information residing in a computer, stealing, concealing, destroying or altering any computer source code used for a computer resource with an intention to cause damage. Such a person would be liable to pay damages by way of compensation to the person so affected[215]. The explanation to section 43 defines the terms computer contaminant, computer data-base, computer virus, damage, computer source code used earlier in the section.

Whereas damage to computer or computer system, failure to protect data by a body corporate is in possession, handling or dealing in sensitive personal data[216] or failure to furnish information return[217], etc is also made a civil wrong that makes the violator liable to pay compensation to the tune of crores of rupees if found culpable.

The Act expressly provides that a penalty imposed or compensation awarded or confiscation under the Act, will not result in avoidance of an award of compensation or imposition of any penalty or punishment under any other law. If no penalty is separately prescribed for contravention of the Act, then the person contravening will be liable to pay a compensation not exceeding Rs 25,000/- to the person affected by such contravention. Adjudication of penalties and compensation under Chapter IX shall be

[215] Section 43 ibid
[216] Section 43A
[217] Section 44

done by an adjudicating authority appointed under section 46[218].

### 3.3.7 Establishment of Cyber Appellate Tribunal

Chapter X of the Act provides for establishment of Cyber Appellate Tribunal that is empowered to hear appeals from the controller or an adjudicating officer under this Act. The Central Government is empowered to notify the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction[219].

### 3.3.8 Offences and Penalties:

As stated above the term cyber crime is not defined under the Act. In colloquial terms it means a crime where either the weapon or the victim of the crime is a computer[220]. A cybercrime can be committed against a person, property or the State.

Chapter XI of the Act deals with "offences". This chapter effectively covers the entire gamut of law on cyber crimes in the country. Earlier the substantive criminal provisions were less than ten under the 2000 Act.

Several trends in cybercrime, like virus attacks, denial of service(DOS) attacks, hacking in the usual technical sense, i.e. obtaining unauthorised access to a computer resource, to name a few, which preceded enactment of the Information Technology Act, were not covered under the criminal provisions of the Information Technology Act

[218] The Secretary of the Department of Information Technology of each of the States or Union Territories are normally not below the rank of Director and possess the requisite experience in the field of Information Technology and also possess legal/judicial experience as required, therefore the Secretary of Department of Information Technology of each of the States or of Union Territories is hereby appointed as Adjudicating Officer for the purpose of the Information Technology Act, 2000. *As per IT Act Notification No 240 The Gazette Of India Extraordinary Part II- Section 3, Sub-Section (I) Dated The 25th March, 2003.*

[219] Section 48

2000. Instead, they were listed as civil penalties under section 43 of the Information Technology Act 2000. It took till December 2008 for these provisions to be made into criminal offences punishable under the Information Technology Act.

Contrary to the established principles of criminal legislations, the Information Technology Act 2000(including amendments thereto of 2008) contains extremely open ended and broad based criminal penal provisions.

Several of these were drawn from UNCITRAL Model laws and or from Foreign Legislations. Apart from the errors in inclusions/modifications of substantive provisions, the amendments also brought about changes to the procedural aspects. It diluted the deterrent factor by making most offences bailable including pornography. There were also a provision that permitted compounding offences that was inserted.

### 3.3.9 Offences under the Information Technology Act

Below is a table that lists various penalties prescribed for violations under the Information Technology Act. It may be recalled that the Act prescribes Civil as well as criminal consequences. The table herein below deals only with offences and not civil liability.

**Table 1**

*Offences Under the Information Technology Act*

| **Sr. No.** | **Section** | **Offence** | **Punishment** |
|---|---|---|---|
| 1. | 65 | Tampering with computer source Code | Punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees, or with both. |

| | | | |
|---|---|---|---|
| 2. | 66 | Doing of an act prohibited under section 43. | Punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both. |
| 3. | 66A | Sending offensive messages through communication service, etc | Punishable with imprisonment for a term which may extend to three years and with fine. |
| 4. | 66B. | Dishonestly receiving stolen computer resource or communication device. | Punishable with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both. |
| 5. | 66C. | Identity theft. | Punishable with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh. |
| 6. | 66D | Cheating by personation by using computer resource | Punishable with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees. |

| | | | |
|---|---|---|---|
| 7. | 66E | Violation of privacy. | Punishable with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. |
| 8. | 66F | Cyber terrorism | Punishable with imprisonment which may extend to imprisonment for life. |
| 9. | 67 | Publishing or transmitting obscene material in electronic form. | Punishable with on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees |
| | 67A. | Transmitting of material containing sexually explicit act, etc., in electronic form. | Punishable with, on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to |

| | | | |
|---|---|---|---|
| | | | seven years and also with fine which may extend to ten lakh rupees. |
| 10. | 67B | Publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form. | Punishable with, on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees: |
| | 67C | Failure to Preserve and retain of information by intermediaries as per Government guidelines | Punishable with an imprisonment for a term which may extend to three years and also be liable to fine. |
| | 69 | Interception/Monitoring/decryption of data in computer resource. | Punishable with imprisonment for a term which may extend to seven years and shall also be liable to fine. |
| | 69A | Failure of intermediary to | Punishable with an imprisonment for a term which may extend to |

| | | | |
|---|---|---|---|
| | | Block computer resource from public access | seven years and shall also be liable to fine. |
| | 69B | Failure of intermediary to Monitor and collect data for cyber security. | Punishable with an imprisonment for a term which may extend to three years and shall also be liable to fine. |
| | 71 | Penalty for misrepresentation. | Punishable with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. |
| | 72 | Penalty for breach of confidentiality and privacy. | Punishable with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. |
| | 72A | Punishment for disclosure of information in breach of lawful contract. | Punishable with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both. |
| | 73 | Penalty for publishing Electron ic Signature | Punishable with imprisonment for a term which may extend to two years, or with fine which may |

| | | | |
|---|---|---|---|
| | | Certificate false in certain particulars. | extend to one lakh rupees, or with both. |
| | 74 | Publication for fraudulent purpose. | Punishable with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both. If any person knowingly creates, publishes or otherwise makes available a Electronic Signature Certificate for any fraudulent or unlawful purpose, he shall be punished with imprisonment upto two years, or with fine upto one lakh rupees, or with both. |

In ***J R Gangwani v. State of Harayana***[221] the Punjab and Haryana High Court refused to quash the proceedings under section 66 of the Information Technology Act where the accused created fake email ids and sent it to the customers of the complainant company with the malafide intent of maligning its image.

The substantial lapse of time between the passing of the amendments of the Information Technology Act in December 2008 and the actual date when they came into effect on 27.10.2009, has resulted in commencement of prosecutions, which are neither maintainable nor tenable. Initiation of criminal prosecutions under the amended section 66, before it came into effect, has been the most common folly with respect to the Information Technology Act. Following in the steps of innumerable Supreme Court

[221] 2012 SCC Online P&H 19890

judgements, the Punjab and Haryana High Court held in ***Amrik Singh Junejas***[222] that the petitioner could not be prosecuted for alleged offences committed on 29th February 2008 under the amended section 66, which came into effect in October 2009 and that the only remedy available to the aggrieved person was to seek civil redress for commission of any acts set out in section 43 of the Information Technology Act. The court quashed proceedings initiated under section 66 and 66A of the Information Technology Act and acquitted the accused.

In ***Shreya Singhal***[223] the Hon'ble Supreme Court struck down Section 66A of the Information Technology Act as ultra vires to the Constitution.

In ***Syed Asifuddin And Ors***[224] Reliance Infocomm Limited had launched CDMA digital phones. These phones were hacked by the staff of Tata Indicomm. FIR was filed under sections 102B, 409 and section 420 of IPC and section 65 of Information Technology Act. These phones came with an inbuilt tariff plan which was owned by Reliance Infocomm Limited. The question before the court was whether the act of Tata Indicomm employee of tampering with the mobile identification number (MIN) which was connected with the Electronic serial Number (ESN) that belonged to Reliance phone should be treated as altering the source code of the computer. It was argued that telephone handset would not fall within the definition of a computer and hence section 65b of the Information and Technology Act 2000 would not be attracted. The court went through the definition of computer, computer system and computer network under the Information Technology Act. The court held that a computer is any electronic, magnetic or optical device that is capable of receiving, processing and storing information in form of magnetic and electronic impulses. The court noted that section 65 of the Information Technology Act made tampering with source code and offence. The court arrived at the definition of computer source code so as to mean a series of instructions given to a

[222] Amrik Singh Juneja v. State of Punjab 2013 SCC Online P & H 3506; Rajaram Kabnure v. Gunwanti Dhulappa Ketkale 2011 SCC Online 1275.
[223] Shreya Singhal Vs. Union of India AIR 2015 SC 1523,
[224] Syed Asifuddin And Ors. vs The State Of Andhra Pradesh 2005 CriLJ 431

program to work. In this context it was held that as the mobile identification number(MIN) of Reliance is linked with electronic serial number(ESN) manipulation of this electronic serial number would amount to an offence under section 65 of the Information Technology Act or even under section 66(hacking) of the Information Technology Act. It was thus held that a telephone handset would also fall within the definition of a computer[225].

[225] The court held that all cell phone service providers like Tata Indicom and Reliance India Mobile have special codes dedicated to them and these are intended to identify the phone, the phone's owner and the service provider. To understand how the cell phone works, we need to know certain terms in cell phone parlance. System Identification Code (SID) is a unique 5-digit number that is assigned to each carrier by the licensor. Electronic Serial Number (ESN) is a unique 32-bit number programmed into the phone when it is manufactured by the instrument manufacturer. Mobile Identification Number (MIN) is a 10-digit number derived from cell phone number given to a subscriber. When the cell phone is switched on, it listens for a SID on the control channel, which is a special frequency used by the phone and base station to talk to one another about things like call set-up and channel changing. If the phone cannot find any control channels to listen to, the cell phone displays "no service" message as it is out of range. When cell phone receives SID, it compares it to the SID programmed into the phone and if these code numbers match, cell knows that it is communicating with its home system. Along with the SID, the phone also transmits registration request and MTSO which keeps track of the phone's location in a database, knows which cell phone you are using and gives a ring. The very definition of 'computer source code,' a) list of programmes; b) computer commands; (c) design and layout and d) programme analysis of computer resource in any form, is a 'computer source code' for the purpose of Section 65 of I.-T. Act. Going by the definition, ESN of Samsung N191 model cell phone handset or ESN of LG-2030 model cell phone handset exclusively used by the second respondent as well as SID of second respondent come within the definition of computer source code. Every cell phone operator is required to obtain SID from the licensor i.e., Government of India. Further, ESN is a permanent part of the phone whereas MIN and SID are programmed into phone when one purchases a service plan and have the phone activity. When a customer of second respondent opts for its services, the MIN and SID are programmed into the handset. If some one manipulates and alters ESN, as per the case of second respondent, Samsung/LG handsets which are exclusively used by them become usable by other service providers like TATA Indicom. Therefore, prima facie, when the ESN is altered, the offence under Section 65 of I.T. Act is attracted because every service provider like second respondent has to maintain its own SID code and also gives a customer specific number to each instrument used to avail the services provided. The submission that as there is no law which requires a computer source code to be maintained, an offence cannot be made out, is devoid of any merit. The disjunctive word "or" is used by the Legislature between the phrases "when the computer source code is required to be kept" and the other phrase "maintained by law for the time being in force" and, therefore, both the situations are different. This Court, however, hastens to add that whether a cell phone operator is maintaining computer source code, is a matter of evidence. So far as this question is concerned, going by the allegations in the complaint, it becomes clear that the second respondent is in fact maintaining the computer source code. If there is allegation against any person including the petitioners, certainly an offence under Section 65 of I.-T. Act is made out. Therefore, the crime registered against the petitioners cannot be quashed with regard to Section 65 of the I.-T. Act.The main allegation against the petitioners is that the MIN of Reliance phone is irreversibly integrated with ESN and the petitioners hacked ESN so as to wean away RIM customers to TATA Indicom service. The question is whether the manipulation of this electronic 32-bit number (ESN) programmed into Samsung N191 and LG-2030 cell phone instrument exclusively franchised to second respondent amounts to altering source code used by these computer handsets i.e., cell phone instruments. In the background facts, a question would also arise

***Suhas Katti v. Tamil Nadu***[226] is the first case in India where there was conviction was achieved in a the cyber crime of cyber staking and online harassment of a woman. In this case a woman complained that the accused was posting of obscene, defamatory and annoying message about her on yahoo messenger group. He also forwarded emails through a false e-mail account opened by him in the name of the victim. a charge Sheet was filed u/s 67 of IT Act 2000, 469 and 509 IPC before The Hon'ble Addl. CMM Egmore who convicted the accused this case is regarded as the first conviction under section 67 of IT Act [227].

### 3.3.10 Protection Of Intermediary

Intermediary with respect to any particular electronic record, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web hosting service providers, search engines, online payment sites, online-auction sites, online market places and cyber cafes[228].

Unless otherwise specifically provided to the contrary, an intermediary will be not liable for, any third party information, data or communication link made by him. This exemption is available only if (a)The intermediary's role is limited to providing access to a communication system over which third parties transmit information or temporarily store the same.(b)The intermediary does not, initiate the transmission, select the receiver of transmission or, modify the information contained in the transmission. The exemption would however stands withdrawn if intermediary conspires or abets the commission of an unlawful act or after having received the information from the

---

whether such alteration amounts to hacking with computer system? If the query answered in the affirmative, it is always open to the police to alter the F. I. R., or it is always open to the criminal Court to frame a charge specifically with regard to hacking with computer system, which is an offence under Section 66 of the IT Act. At this stage, we may read Sections 65 and 66 of the IT Act.

[226] C No. 4680 of 2004 before the Court of Chief Metropolitan Magistrate, Egmore

[227] *https://en.wikipedia.org/wiki/Suhas_Katti_v._Tamil_Nadu on 17.11.2017 at 19.30 pm*

[228] Section 2(w)

Government that any information, data or communication link residing in or connected with computer resources controlled by the intermediary, are being used to commit unlawful acts and such intermediary fails to act expeditiously in removing or disabling access to such link or resource[229].

### 3.3.11 Duty Of The Government To Notify An Examiner Of Electronic Evidence.

Section 79A empowers the Central Government to 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, for the purposes of providing expert opinion under section 45 A of the Indian Evidence Act, on electronic form evidence before any court or other authority. Until the submission of the pre synopsis the researcher has found that the lone forensic science laboratory in Goa has not been empanelled under this law. The List of Forensic Science Laboratories that have been notified till date as per the Ministry of Information Technology Website GOI are annexed hereto as **Annexure 1.**

### 3.3.12 Miscellaneous Provisions

Chapter XIII of the Act contains miscellaneous provisions. The Act empowers a police officer exercising jurisdiction under this Act to search any premises without a warrant[230]. It offers protection to acts done in good faith[231]. The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force. This however shall not restrict any person from exercising any right conferred under the Copyright Act 1957 or the Patents Act 1970[232]. The Act further empowers the State and the Central Government to make rules[233] and

[229] Section 79 inserted by way of amendment in 2006.
[230] Section 80
[231] Section 84
[232] Section 81
[233] Section 87

confers power of removal of difficulties[234].

### 3.3.13 Amendments By The Information And Technology Act To Other Acts

The Information Technology Act 2000 brought about many amendments in the Indian Penal Code 1860, The Indian Evidence Act, 1872, The Bankers' Books Evidence Act, 1891, The Reserve Bank of India Act, 1934.

For the purpose of the present thesis the amendment to the Indian Evidence Act is the most vital. The definition of documentary evidence was widened to include electronic records. Wherever evidence was stated to be in oral and documentary form, an additional category called electronic form was added. Broadly speaking electronic record or evidence in electronic form was given recognition throughout the Act.

In addition to the above following new sections were added to the Indian Evidence Act, namely section 22A[235], Section 45A[236] section 47A[237], section 65A[238], section 65B[239],

---

[234] Section 86

[235] Section 22A : When oral admission as to contents of electronic records are relevant. Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.

[236] Section 45A : 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. Explanation .—For the purposes of this section, an Examiner of Electronic Evidence shall be an expert;

[237] Section 47A : Opinion as to digital signature when relevant. When the Court has to form an opinion as to the electronic signature of any person, the opinion of the Certifying Authority which has issued the Electronic Signature Certificate is a relevant fact

[238] Section 65A: Special provisions as to evidence relating to electronic record: The contents of electronic records may be proved in accordance with the provisions of section 65B.

[239] Section 65B. Admissibility of electronic records:

Notwithstanding anything contained in this Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied in relation to the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence of any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:—

(a) the computer output containing the information was produced by the computer during the period over which the computer was used regularly to store or process information for the purposes of any activities

section 67A[240], section 73A[241], section 81A[242], section85A[243], section 85B[244], section 85C[245], section 88A[246], section 90A[247].The amendments are succinctly discussed as

---

regularly carried on over that period by the person having lawful control over the use of the computer;
(b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer in the ordinary course of the said activities;
(c) throughout the material part of the said period, the computer was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and
(d) the information contained in the electronic record reproduces or is derived from such information fed into the computer in the ordinary course of the said activities.
(3) Where over any period, the function of storing or processing information for the purposes of any activities regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by computers, whether—
(a) by a combination of computers operating over that period; or
(b) by different computers operating in succession over that period; or
(c) by different combinations of computers operating in succession over that period; or
(d) in any other manner involving the successive operation over that period, in whatever order, of one or more computers and one or more combinations of computers, all the computers used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer; and references in this section to a computer shall be construed accordingly.
(4) In any proceedings where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things, that is to say,—
(a) identifying the electronic record containing the statement and describing the manner in which it was produced;
(b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer;
(c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate) shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.
(5) For the purposes of this section,—
(a) information shall be taken to be supplied to a computer if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment;
(b) whether in the course of activities carried on by any official information is supplied with a view to its being stored or processed for the purposes of those activities by a computer operated otherwise than in the course of those activities, that information, if duly supplied to that computer, shall be taken to be supplied to it in the course of those activities;
(c) a computer output shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment. Explanation.—For the purposes of this section any reference to information being derived from other information shall be a reference to its being derived there from by calculation, comparison or any other process.]

[240] Section 67A . Proof as to digital signature.
[241] Section 73 A Proof as to verification of digital signature.
[242] Section 81A Presumption as to Gazettes in electronic forms.
[243] Section 85A Presumption as to electronic agreements.-
[244] Section 85B Presumption as to electronic records and digital signatures.
[245] Section 85C Presumption as to Digital Signature Certificates.-
[246] Section 88A. Presumption as to electronic messages

under:

**A. Amendment to section 3**

The most important amendment was the insertion of the phrase “including electronic records” in the definition of documentary evidence. The last definition in the definition clause has been of the term “India”. After “India” the amendment inserted expression such as : Certifying Authority", digital signature", "Digital Signature Certificate", "electronic form", "electronic records", "information", "secure electronic record", "secure digital signature" and "subscriber and provided that these expressions shall have the same meaning as assigned to them in the Information Technology Act, 2000.

**B. Amendment to section 17**

In section 17 an admission which is in electronic form in addition to the words "oral or documentary” has been made admissible.

**C. Insertion of to section 22 A**

The amendment has inserted section 22A which provides that Oral admission of contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.

**D. Amendment to section 34**

In section 34, for, entries in the books of account maintained in electronic form were brought in par with regular entries maintained in books of account. Whereas in section 35 for the word "record", is stated to include electronic record.

**E. Amendment to section 39**

For section 39 has been substituted to include electronic records. Section 39 permits evidence to be given only of the relevant portion of statement when it is a part of a

[247] Section 90A Presumption as to electronic records five years old.

longer conversation.

**F. Insertion of section 47A**

Section 47 A is a new section that was inserted to make opinion of certifying authority as regards the digital signature of any person a relevant fact.

**G. Amendment to section 59**

Section 59 Of the Indian Evidence Act provides that all facts may be proved by oral evidence expect the contents of documents. Now in addition to “documents” the legislature has inserted the word “electronic records".

**H. Insertion to section 65A and 65B**

Section 65A and 65B are new sections that were inserted containing special provisions laying down conditions under which secondary evidence of original record is admissible in evidence. The said section requires that in case a copy of electronic record is produced, which is referred to as computer output in that section, can be admissible in evidence if the same is produced by a person having holding a responsible official position in relation to the operation of the computer and certifying certain processes relating to the operation of the computer when the copy was produced.

**I. Insertion to section 67A**

After section 67 Section 67A has been inserted which provides that electronic signature which are not secure electronic signatures will have to be proved to have been affixed by the person whose signature it is claimed to be.

**J. Insertion to section 73A**

In continuation of provisions relating to digital signature section 73 A is introduced which provides what the court must do in case a question arises as to whether a digital signature is that of the person by whom it purports to have been affixed. In such a case

the court can direct the person signing, or the Controller or the Certifying Authority to produce the Digital Signature Certificate; or any ask the other person to apply the public key .

**K. Insertion to section 81A**

The newly added section 81A of the Indian Evidence Act creates a presumption of genuineness of official Gazettes preserved in electronic forms if they are kept substantially in the form required by law and if they are produced from proper custody.

**L. Insertion to section 85A**

The newly added section 81A of the Indian Evidence Act creates a presumption that an agreement containing the electronic signatures of the parties was concluded by affixing the electronic signature of those parties.

**M. Insertion to section 85B**

The newly added section 85B of the Indian Evidence Act creates a presumption that the court shall presume that a secure electronic signature was affixed with intention of signing or approving the electronic record;

**N. Insertion to section 85C**

The newly added section 85C of the Indian Evidence Act creates a presumption that the court shall presume that the information listed in a Electronic Signature Certificate is correct, except for certain kind of information.

**O. Insertion to section 88A**

The newly added section 88 A of the Indian Evidence Act creates a presumption that an electronic message forwarded through an electronic mail server corresponds with the message that is fed in the computer of the addressee for transmission. . But there shall be no presumption as to the person who sent this message.

**P. Insertion to section 90A**

The newly added section 90 A of the Indian Evidence Act creates a presumption that as regards electronic signature affixed on electronic record produced from its proper custodian .

**Q. Amendment to section 131**

Section 131 of the Indian Evidence Act provided that where a person is in possession of documents he cannot be compelled to produce them if any other person would be entitled to refuse to produce the same. However if the said person consents the court can order production of the same. After the word document the word electronic record has been added. It may be pertinent to note that again in the year 2009 there were amendments made to the these sections where primarily the word "digital signature" that appeared at various places was replaced by the word electronic signatures.

The Information Technology Act 2000 also amended other statutes. These amendments are enlisted in a tabular form as under:

**Table No. 2**

*Amendments made by the Information Technology Act to other statutes*

| Sr. No | Name of the Act | Details of Amendments | Remarks |
|---|---|---|---|
| 1. | Indian Penal Code 1872 | Section 29A, section 167, Section 172, Section 173 Section 175, Section 192 Section 204, Section 463 Section 464, Section 466 Section 468, Section 469, | Most of these provisions added the word electronic record after the word document that appeared in the respective section |

| | | | |
|---|---|---|---|
| | | Section 470, Section 471 Section 474, Section 476 section 477a | |
| 2. | Bankers' Books Evidence Act,1891 | Section 2(3), Section 2(8), Section 2A | Section 2(3) and 2(8) was substituted and section 2A was inserted. |
| 3. | Reserve Bank of India Act 1934 | Insertion of section 58(2)(pp) | |

Thus in this Chapter the researcher has made an earnest attempt to give a brief insight into international conventions that legitimised the use of electronic technology in day to day business and laid down principles with regard to its use.

In the next chapter the researcher shall look into the evidentiary aspects of electronic evidence and examine how it is tendered and appreciated in court. The chapter also looks at the rules of procedure that have to be followed by investigating officers in seizure of electronic evidence.

# Chapter 4

# Seizure, Production and Evidentiary Aspects Of Electronic Evidence.

## 4.1 Introduction

Electronic evidence is ephemeral and requires extreme care and caution in collation. Most of the times it appears as if there is either no trail or it is difficult one to find. Expeditious and effective action will ensure that the trial including every link in the chain of evidence is collected to establish a case. Mastering appreciation of and proving of evidence in trials is an art which most struggle to perfect. Electronic Evidence simply makes the task more difficult.

Time tested process for collation, retention and production of evidence are put to test when it comes to electronic evidence. The Supreme Court in ***Amritsar Beverages Ltd***[248] opined that the officers enforcing the IT Act faced new problems in dealing with new technologies which apply *pari passu* to the victims and courts also. The fable of six blind men describing an elephant and how far removed from the truth their explanation was, probably explains the understanding of electronic evidence, the most appropriate manner.

In this part of the thesis I shall discuss the conventional modes employed by various stake holders in the process of use, admissibility and proof of electronic record. The researcher noted that this entire process begins with the seizure of electronic record that constitutes electronic evidence either from the crime scene or from the possession of any person. For this reason there is a need to take a bird's eye view of the modes employed by the Police for seizure of electronic record at the outset. As would be discussed subsequently in this chapter the researcher found that the admissibility and

[248] State of Punjab v. Amritsar Beverages Ltd (2006) 7 SCC 607

the Mode of Proof of electronic record are widely determined by the process that is followed in seizure. Issues such as chain of custody, possibility of tampering and authentication is closely connected to this process. Therefore before discussing the modes used by the justice delivery machinery to admit and prove electronic records, the researcher shall first discuss the aspect of seizure.

Electronic records are produced both in Civil as well as criminal cases, however the researcher has restricted her research to the aspect use admissibility and proof of electronic evidence in investigation and trial. Therefore the foremost exercise shall be to determine the manner and mode in which the electronic evidence is seized, preserved and produced before the court. The internet consists of exhaustive material giving guidance to investigating officers all over the world on how to seize secure, preserve and handle electronic evidence. However there are no law/Rules in India that lay down SOP for handling electronic record.

## 4.2. Standards And Guidelines For Seizure Of Electronic Record

Electronic evidence produced in courts is produced in two forms (a) Patent electronic evidence and (b) Latent electronic evidence.

Patent electronic evidence is the electronic evidence that is readable or can be viewed in the form in which it was generated. For example electronic text documents, videos, photos, emails, account statements print outs, text and instant messages, social media posts, voice recordings, electronic transactions. The definition of electronic record is most suited to define this form of evidence. Whereas the term latent means that which cannot be seen readily, but it exists. A computer often stores information about its usage. Such as logs, locations of servers, history of internet surfing. Every electronic record created also has data saved at the time at which it was created and the IP address of the device that created it. If the record in question is an electronic message or email it will contain information about the sender and receiver. All this latent form of evidence may be relevant in cases where the fact in issue pertains to this information.

A call log on the mobile of a person is patent electronic evidence whereas the information about the location from where the call was made in the circle of GPS[249] or allied service activation on the mobile will be latent electronic evidence. So also photos or videos posted on social media may contain location information.

The reason this categorisation is made at the outset is because this distinction is the first thing that the Investigating Officer has to bear in mind when he proceeds to investigate a case that may involve electronic evidence. An electronic record maybe the muddemmal or the physical fact or it may be a piece of evidence to introduce, corroborate or rebut a particular fact. The researcher has enlisted the following stages based on her research undertaken by observation and interview technique. This practical assessment is primarily backed by study material gathered on this subject which is discussed later in this Chapter.

When the researcher visited the lone cyber crime police station in Goa, the Police Inspector incharge of the police station gave an insight into the manner in which an electronic record has to be seized. The researcher found that unlike acts such as the Narcotic Drugs and Psychotropic Substances Act, 1985 or the Prevention of Food Adulteration Act 1954 there is no law in India that lays down rules for seizure of electronic records. The Goa Police therefore falls back on the material supplied to them during their training sessions on cyber crimes and electronic evidence.

In the absence of legislation or an authoritative guiding manual of SOP over the internet the researcher has found the following standard procedures published by various organisations that may assist the investigating officers in the process of seizure of electronic records.

[249] Photos clicked with global positioning system (GPS) enabled device contain file data that shows when and exactly where a photo was taken.

### 4.2.1. ISO/IEC 27037:2012; Information Technology — Security Techniques — Guidelines For Identification, Collection, Acquisition And Preservation Of Digital Evidence.

ISO/IEC 27037:2012 has laid down guidelines for handling of digital evidence, namely on the aspects of identification, collection, acquisition and preservation which potential digital evidence can be of evidentiary value. These guidelines provide guidance to individuals in respect of common situations encountered by them in the process of handling digital evidence and assists organizations in their disciplinary procedures in facilitating the exchange of potential electronic evidence between various jurisdictions. These guidelines are published by the International Organization for Standardization (ISO) [250]in 2012. ISO/IEC 27037 was prepared by Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques[251].

These standards can be applied only if they are in compliance with national laws, rules and regulations. The purpose is not to replace specific legal requirements of jurisdiction of individual countries. Rather they serve as a practical guideline for investigations involving potential digital evidence.

The objective of these guidelines is to minimize manipulation of data, document all the events and changes incorporated in electronic evidence right from the stage of its collection till the point it is handed over to an expert for forensic analysis. The guidelines enlist commonly used terms in the context of handling digital evidence and gives its definitions. It lays down comprehensive details about collecting and handling

[250] ISO (the International Organization for Standardization) and IEC (the International Electro technical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

[251] https://www.iso.org/obp *accessed on 9.1.2020 at 10.30 pm*

of digital evidence and deals with key components such as chain of custody, identification and preservation of digital evidence.

### 4.2.2. The ACPO Good Practice Guide for Computer Based Evidence

These guidelines were developed by the Association of Chief Police Officers (ACPO) in the United Kingdom[252]. The highlight of these guidelines are the four principles that have been laid down regarding handing of electronic evidence[253]. These guidelines have been followed by a number of authors and research papers on the subject of electronic evidence. Succinctly stated these guidelines set out a plan for the Investigating Officer as to where digital evidence could be potentially found and should be looked for. It lays down guidelines as to how electronic evidence can be captured and cautions the investigating officers to weigh proportionality issues before seizure. It gives a practical list of do's and don'ts in data collection. Further the guidelines lay down principles for forensic analysis and interpretation of data. It also gives templates of how to prepare reports and statements. It emphasises on the need of training and education.

### 4.2.3. Electronic Crime Scene Investigation: A Guide For First Responders: The U.S. Department Of Justice (USDOJ, 2001)

[252] This best practice guide has been produced by the ACPO Crime Business Area and was originally approved by ACPO Cabinet in December 2007.*https://www.digital-detective.net/digital forensic documents ACPO_Good_Practice_Guide_for_Digital_Evidence_v5* assessed on 19.1.2020 at 11.00 p.m

[253] The principles are enunciated as follows Principle 1: No action taken by law enforcement agencies, persons employed within those agencies or their agents should change data which may subsequently be relied upon in court. Principle 2: In circumstances where a person finds it necessary to access original data, that person must be competent to do so and be able to give evidence explaining the relevance and the implications of their actions. 2.1.3 Principle 3: An audit trail or other record of all processes applied to digital evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result. 2.1.4 Principle 4: The person in charge of the investigation has overall responsibility for ensuring that the law and these principles are adhered to.

U.S. Department of Justice (USDOJ)[254] has created a guide for conducting electronic crime scene investigation by law enforcement agencies. The purpose of these guidelines is to assist State and local law enforcement and other first responders for recognizing, collecting, preserving and safeguarding digital evidence. The intended audience for this guide are anyone encountering, processing, supervising, and managing a crime scene that may involve electronic evidence. It enlists the type of electronic devices and gives guidelines as to how to extract evidence there from. It lays down what are the tools that the IO should be equipped with when approaching the crime scene. It explains how to secure and evaluate crime scene and thereafter how to document it. Further it gives guidelines as to how to handle crime scene. The novelty of this guide is that it enlists various devices and notes its primary uses and the potential evidence that may be found therein. It also provides how such evidence is to be packed, transported and stored.

### 4.2.4. CBI (Crime) Manual, 2005

Chapter 18 of the CBI Crime Manual deals with investigation of cyber crimes[255]. It gives guidelines as to what precautions should be taken at the search site, taking control of the location, reliance on experts, labelling, photography, keeping the power system down, dismantling of the system and seizing of documents and peripheral devices. It

[254] In May 1998, the National Cybercrime Training Partnership (NCTP), the Office of Law Enforcement Standards (OLES), and the National Institute of Justice (NIJ) collaborated on possible resources that could be implemented to counter electronic crime. NIJ established the Technical Working Group for Electronic Crime Scene Investigation (TWGECSI) to identify, define, and establish basic criteria to assist agencies with electronic investigations and prosecutions. In January 1999, planning panel members met at the National Institute of Standards and Technology (NIST) in Gaithersburg, Maryland, to review the fast-paced arena of electronic crime and prepare the scope, intent, and objectives of the project. During this meeting, the scope was determined to be too vast for incorporation into one guide. The final draft was then sent for content and editorial review to more than 80 organizations having expertise and knowledge in the electronic crime environment. The returned comments were evaluated and incorporated into the document when possible. At the end of the document are appendixes containing a glossary, legal resources, technical resources, training resources, and references, followed by a list of the organizations to which a draft copy of the document was sent. This guide is intended for use by law enforcement and other responders who have the responsibility for protecting an electronic crime scene and for the recognition, collection, and preservation of electronic evidence. *https://www.ojp.gov/pdffiles1/nij/187736.pdf*

[255] As per Para 18.4 of the Manual CBI has the following specialized structure to handle crimes: (i) Cyber Crimes Research and Development Unit (CCRDU); (ii) Cyber Crime Investigation Cell (CCIC); (iii) Central Forensic Science Laboratory (CFSL); and (iv) Network Monitoring Centre.

also makes references to data protection, packing and transportation of the material seized. It is peculiar to note that the guidelines are brief and barely run into 5 pages.

### 4.2.5. Cyber Crime Investigation Manual (DSCI-NASSCOM)

Upon interviewing Senior Police Officers in Goa it was found that the foremost cybercrime investigation Manual that is relied upon by the Police in Goa is the one that is prepared by the DSCI –NASSCOM[256]. The other publications of DSCI –NASSCOM include Cybercrime Training Material Level I Pocket Handbook on Cybercrime Investigation (2013), Cyber Forensics - Meeting the Challenges of Cybercrimes (2013) Cybercrime Training Material Level II (2015) FAQs on Information Technology Act 2008.

In addition to the above mentioned guidelines, the LNJN National Institute of Criminology and Forensic Science (NICFS) formulated a Guide titled "A Forensic Guide for Crime Investigators – Standard Operating Procedures" to strengthen the role of forensic science in criminal investigations.

## 4.3 Stages Involved In Crime Scene Investigation Involving Electronic Evidence.

After going through the international and local guidelines the researcher has enlisted the following stages and the standard expectation from the Investigating Officer in the processes involved in those stages as under:

### 4.3.1 Identification Of The Electronic Record/ Source.

[256] To standardize the operating procedures for cybercrime investigation, DSCI has prepared Cyber Crime Investigation Manual which is based on its experience of operating the Cyber Labs and working with the police in handling many of the cybercrimes over the last few years. The manual aims to bring a uniform and scientific approach in investigating these crimes and bringing them to the court of law. The manual covers a comprehensive list of Cybercrime topics including procedures for pre-investigation, evidence collection, and handling evidence. It will be a valuable resource in any field investigation, as it provides clear guidance to investigating officers on the procedures to be followed at crime scenes where digital media is involved. On https://www.dsci.in/content/publications *accessed on 12.12.2019 at 7.30 pm*

The person carrying out the act of seizure must have necessary authority under the law to carryout seizure. The Information Technology Act of 2000 provides that no person below the rank of a police officer can carry out investigation under the Act[257]. There is however no such embargo when investigating offences under any other penal statute, which involve use of electronic evidence. If the offence requires obtaining any search warrant it should be obtained well in advance. The search warrant must contain proper description of the offence and what is intended to be searched.

The first stage that an electronic record passes through at the commencement of investigation is identification of the electronic record/source. The most important responsibility of an investigation officer is to discern from the FIR as to what electronic evidence he needs to seize to prove the ingredients of an offence. Upon receipt of FIR the investigating officer has to first determine as to what are the ingredients of the offence and thereafter enlist facts that will have to be placed before the court to prove these ingredients. If the proof requires electronic evidence then the Investigating Officer should make a mental roadmap of what form of electronic record may have to be seized or gathered in proof of relevant facts. There must be clarity about what the record is and where it may be available.

Documentary evidence under the Indian Evidence Act includes electronic records produced for the inspection of the Court. An electronic record is defined under section 2(l) of the Information Technology Act meaning data, record or data generated, image or sound stored, received or sent in an electronic form. Therefore any electronic record to be admissible as evidence before the court has to be in form of a data. By necessary implication therefore a device such as a computer or a network of computer is not electronic evidence and its seizure alone will not suffice. At the most it can be classified as a source of electronic evidence. Hence what may be seen by the eye is not what legally admissible before the court.

[257] Section 78 of the Information and Technology Act.

That evidence which is relevant electronic record has to be made admissible and later authenticated by following due process of law. Equipment and software may be needed to make it readable before the court. As electronic evidence is fragile and can be easily damaged and altered therefore utmost precautions will have to be taken to ensure that there is no scope for doubt in the mind of the judge about a process followed at the time of seizure. Here the testimony of the Investigating Officer and the Forensic expert is of utmost relevance they may be called upon to state the process of seizure and its limitations.

The researcher found that in cases where the electronic record is contained in a mobile phone the Investigating Officer seizes the mobile phone simplicitor and produces it for the inspection of the court without extracting the data from the same. Here there has to be clarity in the mind of the Investigating Officer as to what is relevant evidence to prove a fact and how he will go about securing it.

The researcher has found that most Investigating Officers approach the device containing the electronic record without such a road map. Some officers are also not aware as to how to operate some devices so as to extract electronic evidence there from.

### 4.3.2 Preparation For Its Seizure.

The next step is preparation for seizure of electronic record. Electronic record unlike physical evidence is unique in its constitution. Experts believe improper handling of electronic evidence may also affect the integrity of data contained in it. Although the Indian Evidence Act classifies electronic record as documentary evidence, considering its unique nature it cannot be seized in the manner in which an ordinary document is seized.

In addition to this the researcher interviewed computer forensic scientists, Police officers and browsed the internet for information and enlisted the following principles that could be traced from the research made.

a) Before reaching the scene of offence preliminary planning is essential. The planning involves gathering information before hand about the type, location of the computer or computer network that is to be seized. Standalone computers or laptops can be seized by staff that have basic knowledge of computers however, in case of computer networks the investigating officer must have sufficient training in seizure of the electronic evidence.

b) Second is briefing the entire team which proceeds to the scene of offense about the purpose and the manner in which search and seizure will be conducted. Here training of all police personnel, including the one who is lowest in the rung, in handling of electronic evidence is imperative.

c) The investigating officer must make a list of equipment/ tools that have to be carried at the scene of offence. Tools such as screw drivers pliers, scissors etc may be required for the purpose of dismantling computer systems as well as their packaging and removal. Similarly, labels, tapes may be required for marking and identification. A spare hard disk or cartridges can be used if required by the forensic scientist to make copies of documents. Computer forensic experts suggest that where no services of an expert can be procured at the site, investigating officers shall invariably photograph and video graph the scene untouched and thereafter as far as possible photograph or video graph the process of seizure and the exhibits. These photographs and videos may not have much evidentiary value however it can assist a forensic scientist later when the exhibits are sent to him for forensic analysis. Packing material such as rubber bands, tape boxes, bubble wrap, anti static wrap should also be carried.

d) Taking into account the circumstances of the case and his/her own expertise in the matter the investigating officer may consider seeking assistance of a cyber forensic expert. All the above pre-planning is possible only when the investigation officer has prior knowledge of the existence of electronic evidence at a particular place. However investigating officer must give a thought of there being a possibility of unanticipated electronic evidence found at the scene of offence. For example on reaching a spot where murder was committed valuable evidence may be found on a laptop at the scene of

offence[258]. The researcher therefore suggests that a "computer evidence kit" must be made available at all times at the police station.

e) Lastly the person who will conduct the seizure must have adequate knowledge of computer hardware particularly of different kinds of storage devices.

### 4.3.3 Actual Seizure.

The next stage is actual seizure. It is important for the investigating officer to first know what to seize and how to seize. The following guidelines are generally found recommended by computer forensic experts:

a. When reaching the scene the Investigating officer must secure the scene and move people away from equipment and any power supply.

b. Check whether the device is Switched ON or connected to a network. If the device is switched off, forensic scientists recommend not switching the device ON and advice to remove the power supply cables and/or Battery Packs from the equipment. If the device is switched off forensic scientists recommend to immediately solicit expert intervention at the time of seizure. If expert intervention is not available it is recommended not to touch the keyboard. Investigating Officer must photograph and make note of what is on the display. In case of a laptop remove the battery. Check whether the computer is actually switched off or whether it is in sleep mode as a computer in sleep mode can be remotely operated.

[258] In the famous double murder case of Arushi and Hemraj the prosecution found that there was internet activity through the intervening night of the murder to show that the parents of the deceased remained awake on the night and had manually operated the computer the entries recorded in ISP log depicting IP address were produced as evidence see *Dr. (Smt.) Nupur Talwar vs State Of U.P. Crime Appeal No. - 293 of 2014 Allahabad High Court.*

c. After dismantling secure each part with proper labels so that the forensic expert can assemble the parts easily. Enlist details of all components that are separately seized. Preferably take photographs. If the printer in on, let the process of printing be over.

d. If the computer is switched ON first check whether it is connected to any network. Disconnect the modem if attached. Remove all the connection cables after properly labelling them. Record what is on the screen by taking a photograph or making a written note. If no expert is available it is advised to remove the power supply without shutting down the computer. Always remove the end that is attached to the computer and not to the power socket.

e. Experts caution from following unverified advice from suspects.

f. In case of handheld devices the same procedure is recommended except if the device is switched off it is recommended to change batteries. It is recommended by experts that in the absence of an expert forensic team it is important for the investigating officer to label and photograph/video the equipment at site. Investigating Officer should remove all other connection cables leading to wall sockets or other devices. The Investigating Officer must remove and package the equipment and further record all details on the search form. He must ensure that all the components have exhibit labels attached for later re-assembly.

e. If possible the Investigating Officer must search the scene for diaries or pieces of paper which may give a clue of passwords. In any case there are forensic tools that can help to find out the password however the process is too tedious and time consuming and such clues if available at site can come handy.

f. The seizure of equipment would depend upon what electronic record is needed for investigation. Ordinarily a CPU or the main unit of the computer suffices. But in investigation of certain cyber crimes the entire system including the leads, power supply units, modems etc may be needed. To ensure that the search and seizure happens seamlessly it is most essential to seek assistance of a cyber security expert.

In seizing mobile devices**,** devices should be turned off immediately and batteries removed, if possible. Turning off the phone preserves cell tower location, call logs and prevents the phone from being used which could change the data on the phone. In addition, if the phone remains ON, remote destruction commands may be used without the investigators knowledge. If the device cannot be turned off it must be isolated from its cell tower by placing it in a Faraday bag or other blocking material or set to airplane mode. Wifi Bluetooth or other communication system must be disabled. Digital devices should be placed in antistatic packaging such as paper bags envelopes and card board boxes. Plastic should be avoided as it can convey static electricity or allow build-up of condensation or humidity.

### 4.3.4 Transit And Handling

Transit and handling constitute an important aspect of investigation as it is often argued in defence that a lot of data is lost on account of mishandling of electronic record. The Investigating officer must take the following precautions at the time of transit and handling of electronic evidence.

#### a. Protecting data

The Investigating Officer should write protect the disks that he finds at the site of search in order to protect the data. Forensic scientists advise that placing a blank disk in the hard drive of a computer system will keep them from booting up from the hard drive if they are accidentally turned on.

**b. Packing for Transport.**

Once the Investigating Officer or the expert has dismantled the computer, it is ready to be packaged for transportation to the forensic laboratory. Computer parts being sensitive are easily damaged hence they have to be handled carefully. One should not wrap the computer components using Styrofoam and antistatic or bubble wrap is often preferred.

**c. Keep the system components together.**

The Investigating Officer must keep the components of each computer system together. This small organizational set can save lots of time when examiners are trying to reconstruct the system.

**d. Single Machine Single seizing Agent.**

If one person handles the seizure of a computer, that same person can depose and give evidence at the stage of trial.

**e. How to transport and store the system.**

Equipment should be kept safe of shocks and the resultant damage on account of transportation. The computer system should be secured in a way that would reduce vibrations that may make loosen any parts. The Investigating Officer should store the computer in secure, cool dry place away from any generations or others devices that emit electromagnetic signals.

### 4.3.5. Preservation and storage

The issue of preservation of electronic evidence is of global significance. Preservation of electronic record in its broader sense implies the act of fixing and keeping the original data evidence or its supplemental data such as hash values and abstracts in an way to prevent its deletion or modification and make the authenticated electronic record available at any stage of the proceedings in future. In the narrow sense, electronic evidence preservation only refers to the preservation of the source/ original electronic record.

The former is a subject of international research and debate where suggestions are made to resort to online preservation methods such as hash operation, time stamp, and block chain technology can effectively guarantee the authenticity and security of electronic data[259]. In the European Union there is a cyber notary authority appointed for such purpose but India there is no such legislation or law. This issue is discussed in detail in the last chapter as preservation of original electronic data is a big challenge as ordinarily cases take a significant time to attain finality. However the later can be assured to a great extent if the device or disk containing the original record is seized and stored properly and the data therein is extracted forensically.

To ensure the integrity of the data till the point it reaches a computer forensic laboratory for authentication the investigating officer must ensure that at all times during transport the devices were kept away from any magnetic fields. They were transported with utmost care and are stored away from excessive heat and humidity. As discussed above all components have to be labelled properly so as to facilitate its easy reassembly in the laboratory.

[259] Shang H, Qiang H. Electronic data preservation and storage of evidence by blockchain. J Forensic Sci Med [serial online] 2020 [cited 2021 F*eb 10];6:27-36. Available from: https://www.jfsmonline.com/text.asp?2020/6/1/27/280893*

### 4.3.6 Analysis Of Electronic Evidence

Although the research does not emphasise much on computer forensic aspect of electronic evidence nonetheless a basic understanding of some popular forensic methods to extract the data from the seized equipment is necessary. The need of forensic intervention arises for linking an activity with a specific user account or in establishing a timeline of events, breaking encryption, identifying relationships/connections between the suspect and victim, identifying websites that have been visited, determining whether certain files were opened or downloaded, identifying what search engine queries have been entered, locating contraband (such as child pornography),determining what applications have been installed or uninstalled, recovering deleted files, determining whether or not the system has been compromised in some way etc. It is also used for authentication of the evidence by comparison of Hash values of both source and destination media to make sure that both the values are same, which in turn ensures that the content of destination media is an exact copy of the source medium.

Digital forensics and the word Computer forensic are often used interchangeably. However the former has been given a wider meaning so as to cover investigation of all devices capable of storing digital data. The purpose of computer forensics is to examine digital media forensically with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the digital information. A relevant electronic record may be contained in a computer component (eg. hard disk, inbuilt device memory ROM) or a recording media (eg. magnetic tapes and optical disks). The following are some commonly used tools for forensic analysis.

**A. Disk Cloning:**

When any computer component or recording media is subject to forensic analysis it may involve loss of data thereby compromising with the integrity of the data. Hence Forensic scientists recommend creation of a clone of a seized hard disk. Cloning is a process of creating a bit by bit image of the hard disk. The cloned hard disk is fully

functional and in the event that it is swapped to replace the original drive, it will work like the original. If a computer, is booted using the cloned drive, its operations and data, will be identical to the original drive. The process involves using of a cloning device and a sterile hard disk preferably of a greater capacity then the original hard disk. As a thumb rule no forensic analysis is done by a forensic scientist on the original hard disk seized by the Investigating Officer.

It is recommended that the process of cloning should be done in the presence of panch witnesses or preferably the owner of the hard disk or to video graph the same so as to avoid any suspicion or doubt. Forensic scientists opine that minimum two cloned disks are prepared so as to facilitate giving of a copy to the accused. Some popularly used cloning devices are Image Master Solo4 from TCS, Encase, FTK. In order to prevent accidental write back of data, a write protector or write blocker is used. Some cloning devices have an inbuilt write blockers.

**B. Disk Imaging**

Imaging is the process of creating a byte-by-byte image, however the contents of the image may be compressed and archived by placing it on another drive. This compressed file acts like a big .zip file. Therefore with cloning, if the source drive crashes by replacing it with the cloned drive the computer can be restored as good as the old. The processes may be different but the end result is substantially the same. Imaging is cost effective and used particularly in cases where copies are to be made of the electronic record to be produced along with the chargesheet. The researcher asked a question to forensic scientist as to whether by creating a cloned image will there be no liability to preserve the original. All the forensic scientists answered in the negative.

**C. Hash Value Authentication**

A hash value is a numeric length that uniquely identifies data[260]. For example the hash value for a simple sentence like "admissibility of electronic evidence" will be say 11223344556677. Now if this sentence is tampered with even by a bit, by say even changing the font, the hash value will change 11223444556677. By this technique forensic scientists authenticate electronic records. This is considered as one of the most accurate method of authentication. A hash value is generally taken of the image copy before any examination and matched with the hash value of the original evidence, if the hash values are same, then the copy is treated the same as original. This is also called "The pre-acquisition hash". Other then authentication electronic data hash value can be used to authenticate the integrity of the data exchanged between the parties and any tampering would result into change in hash value.

**D. Network Forensics**

The term network forensics is used for study and analysis of computer network traffic for the purposes of information gathering, legal evidence or intrusion detection. Compared to computer forensics where evidence is usually preserved on disk, network forensics is more difficult as such data is volatile and unpredictable. There are many network monitoring tools used in network maintenance and information security management. These are helpful in extracting evidence. In order to ensure that evidence is extracted from network data traffic information is acceptable for judicial purpose, it is necessary that the forensic analyst adopts suitable procedure for observation as well as appropriate tools for the purpose of recording information. Some popular tools used for computer network forensics are "Wire Shark", Net scout etc.

[260] https://docs.microsoft.com/en-us/dotnet/standard/security/ensuring-data-integrity-with-hash-codes on 09.02 .2021 at 8.30 pm

**E. Memory Forensics**

Memory forensics is forensic analysis of volatile data contained in a computer's memory dump[261]. Its primary application is investigation of such computer attacks which are surreptitious to avoid leaving data on the computer's hard drive. Consequently, the memory (RAM) must be analyzed for forensic information. Volatile data is the data stored in temporary memory or the RAM of a computer while it is running. If a computer is powered off, volatile data is lost almost immediately. Volatile data is found in a computer's short term memory storage and can include data like browsing history, chat messages, and clipboard contents.

**F. IP Tracing**

One of the first requirements of an investigation of an internet based communication is to trace the IP addresses. " Trace Route" is one of such commonly used tools. As some service providers use proxy IP addresses with which the clients mails are forwarded it may be necessary for forensic investigator to get originating client IP address based on a query from a law enforcement agency.

**G. Mobile Forensics**

Mobile forensics is a part of digital forensics which deals with recovery of digital evidence from mobile devices. Electronic Evidence on a mobile can be extracted from different sources namely handset memory, SIM card, and attached memory cards such as SD cards, Memory Stick etc. Earlier mobile phone forensics was used to recover

[261] Memory forensics (sometimes referred to as memory analysis) refers to the analysis of volatile data in a computer's memory dump. Information security professionals conduct memory forensics to investigate and identify attacks or malicious behaviors that do not leave easily detectable tracks on hard drive data. https://digitalguardian.com/blog/what-are-memory-forensics-definition-memory-forensics

SMS and MMS, view call logs, contact lists and phone IMEI information. However, Android phones and smartphones provide a variety of services to the user such as web browsing, wirelessnetwork settings, geolocation information(including geotags containe d within image metadata), e-mail social networking service posts etc. Mobile phones can also be used to run applications which alter or modify electronic records. In other words a mobile phone nowadays can perform almost all functions that can be performed by a computer. Service provider logs and call data records are important supplementary evidences that may be collected through mobile forensics.

Once a computer is booted the program can then copy digital evidence sector by sector. When the digital evidence has been copied, data can be viewed physically or logically. Viewing data in logical view enables the user to examine the data as represented by the file system.

The possible sites where data and metadata that can be extracted are succinctly stated as under:

**(i) Passwords and encryption:**

A number of tools are available that are capable of removing passwords, and by passing or recovering passwords. Some tools are available to guess passwords. If the encryption keys are small enough and where it is not possible to defeat a password it is sometimes possible to search for encrypted versions of data in other areas of the hard disk.

**(ii) Logs, files and printing:**

When a user uses their computer he leaves traces of his actions across a range of data logs and files. A data log is capable of containing any type of data, depending on what the system is programmed to capture. For instance if a file is downloaded from the internet, a date and time stamp will be added to the file to demonstrate when the file was downloaded on the computer. When the file is moved opened or modified the time and date stamps will be altered to reflect these changes. In addition the meta data can also

help provide more information about the file, such as the location to which it was stored on the disk, the printer, the original time and the date when the file was created. When a file is printed, the computer tends to store the print job in a temporary file and then sends the file to the printer when the printer has to capacity to print the document. Once the command to print has been passed to the temporary store the user can continue to work with the application, for instance they can continue to type a new document whilst the previous document is waiting to be printed.

**(iii)Use of internet**

When a person obtains access to internet, a range of data is created and retained on a computer, including the websites that have been visited, the content a user has viewed and the newsgroups that they have obtained access to. Some systems also include a log of times and dates the modem was used.

**(iv) Browser cache/Cookies**

The browser retains an image of the page called cache. Many websites seek to keep a track of the visit by individuals to their websites by placing information in cookie files on their user computer.

**(v)Email and instant messaging**

It is possible to recover email message that have been deleted but has not been removed from the email file.

**4.3.7. Reporting:**

The findings and any conclusions made by the digital evidence specialist will have to be set out in a report. The report should include the following range of information that is pertinent to the case including but not limited to :

a) Notes prepared during the examination phase of the investigation.

b) Details about the way in which investigation was conducted.

c) Details about the chain of custody

d) The validity of the procedure used.

e) The details of what was discovered including but not limited to:

i) Any specific files or data that were directly related to investigation.

ii) Any files or data that support the conclusion reached by the specialist. This will include recovery of any deleted files and analysis of graphic files.

iii) The types of search conducted such as key word searches and the programs searched

iv) Any relevant evidence from the internet, such as emails and the analysis of websites visited and log files

v) Indications of names that might demonstrate evidence of ownership of software, such as to whom the software is registered abd

vi) Whether there is any attempt to hide date in a way and if so what are the methods used.

The reports need to reflect how the examination was conducted and what data was recovered. It may be that digital evidence specialist will have to give evidence about the conduct of examination and the validity of procedures and tools used.

### 4.3.8 Establishing Chain Of Custody:

The reason for taking particular care with digital evidence is that the nature of evidence is such that it can be easily altered. It is necessary to demonstrate the integrity of evidence and to show that it cannot be tampered with after being seized or copied. In a case involving a number of items of hardware and more then one computer it will be necessary to ensure that there is a clear link between hardware and digital evidence that is copied from that hardware. In this respect the record should address issues such as:-

a) Who collected the evidence.

b) How and where the evidence was collected.

c) The name of the person who took possession of the evidence.

d) How and where the evidence was stored.

e) What was the protection afforded to evidence whilst in storage.

f) The names of the people who removed the evidence from storage including the reasons for removing the evidence from storage.

The succinct description of the process of handling of electronic evidence by the police indicates the gamut of infrastructural change that may be required to make optimum use of electronic evidence. The analysis of the field research in the next chapter would indicate whether the State of Goa has braced its self to face the challenge.

### 4.4 Evidentiary Aspects Of Different Categories Of Electronic Evidence

Different forms of electronic records are produced before the court. All electronic records do not have the same physical structure or properties. Therefore no uniform rules can be laid down on the matter of their admissibility and the mode of proof. Just like every form of electronic record is unique in its makeup, the facts in issue in respect of that electronic record may be different in all cases. The researcher has divided the evidentiary aspects of different types of electronic evidence into 6 broad categories:

1.Data contained on Website

2.Social Network Communications and Postings

3.Email

4.Text Messages

5.Computer Stored and Generated documents

6.Photographs, videos and audio recordings.

Section 22A of the Indian Evidence Act states that oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question.

### 4.4.1. Data Contained On A Website

Information that is displayed on a website is often tendered as evidence in the court in form of a printout. The website in question may be a Government website or a private website.

Websites are of two types namely, Static websites and dynamic websites. Static websites are ones that are fixed. These websites contain the same content for every user. The interaction between the user and the website is minimal and only through URLs. Examples of a static website would be a website of a company or an organization which may contain information about their products, constitution business etc.

A dynamic website, is one which can display different content and provide user interaction, by using advanced programming and databases in addition to HTML. In contrast with static websites, which are purely informational, a dynamic website is more functional. It allows users to interact with the information and data which is available on the page. For eg. e-courts website or the website of the passport department where one can take appointments or upload information.

#### *A. Aspect Of admissibility Of Data Contained On A Website:*

When the data contained in a website is to be used as evidence in the court such data is ordinarily produced in form of a print out. When this printout is accompanied by a certificate under section 65B of the Indian Evidence Act, the printout becomes admissible in evidence. This certificate is in form of a template and needs to be modified as per the facts of the case. The original electronic record in this case is a web

page that is sought to be produced therefore the certificate must contain the following information so as to establish its identity.

a. Complete URL[262] of the website
b. The date and time when the witness logged into the site and viewed what was displayed
c. The date and time when the printout was taken.
e. Information if any whether the printout was directly taken or whether the web page was saved on any disk or device and the form in which it was saved.
f. Lastly all other standard clauses pertaining to the section 65B.

Section 65B assures that the printout fairly and accurately reflects what the witness saw. This is the same as in case of a photograph. Unless the opponent is able to point out from the cross examination that there is a plausible reason to believe that the witness is lying or is mistaken.

***B. Mode Of Proof Of Data Contained On A Website***

Next comes the issue of mode of proof and its authentication. Once the copy of the electronic record is admitted, any inferences regarding authenticity pertain to mode of proof and not admissibility. There are essentially three different categories of data contained on websites that may likely be a subject of an inquiry on the aspect of its authenticity.

a. Data posted by the owner of the website.

b. Data posted on a website by a third party with the consent of the owner.

c. Data posted on a website by a third party without the consent of the owner. Eg hacked accounts on social networking sites.

[262] URL stands for Uniform Resource Locator. A URL is nothing more than the address of a given unique resource on the Web

Ordinarily data from a website is produced in defamation cases. Very rarely the authenticity of the same is denied. Difficulty arises when public information of private individuals or processes are displayed on the website. For example information of incorporation of companies, electoral rolls, information regarding tenders, advertisement for jobs.

Some data on websites are self authenticating. The Indian Evidence Act lacks a provision akin to section 57 of the Indian Evidence Act in respect of electronic record that can make the certain kind of electronic data on a Government website self authenticating. It is often argued that it is very difficult and inconvenient if formal authentication is insisted upon, where a print out of information on a Government website is produced. Authentication or proof of this form of electronic evidence depends upon what information is published on the webpage. If it pertains to a record of which a certified copy can be obtained the same can be produced by obtaining a certified copy. Infact the researcher is of the humble view that the courts must never give a go by to section 74 of the Indian Evidence Act which makes only certified copies of public record admissible in evidence and no other, until it is amended to make data contained on Government websites self authenticating.

The person against whom the document is sought to be produced is free to challenge that same. The challenge can be threefold first that the exhibit does not accurately reflect the contents of the website, second that the information never existed or exists and third that the contents is not attributable to the owner of the site.

As regards the first two challenges it is observed that in considering whether a genuine issue as to trustworthiness is raised, the court will look into the following circumstances:

a) Whether there is a statement of the length of time the data was posted on the site?

b) Whether any witness has reported of having seen it?

c) Whether it is available at a later point of time on the website for the court to verify?

d) Whether data is a of a type ordinarily posted on same or similar websites ( eg financial information from corporations)

e) Whether the owner of the site or others have published the same data elsewhere?

f) Whether the data has been republished by others who identify the source of data as the website in question?

g) Whether there is a reasonable risk of hacking or manipulation.

Here an expert has no role to play. An expert report may be sought to note necessary technical details of the information in rare cases.

When the researcher interviewed a sample size of judicial officers in Goa it was found that none of the judicial officers had examined any expert when an extract of a website was produced before it.

The third objection that those contents are not attributable to the owner of the site, is a question of fact and has to be considered by following the same rules of evidence as any other form of conventional documentary evidence produced in the court.

### 4.4.2. Social Network Messages/Posts

The Merriam Webster's dictionary defines social network messages as forms of electronic communication through which its users create online communities to share information, ideas, personal messages, and such other content[263]. There are third party platforms through which its members can create a profile for identification purpose and posts are often made through these profiles. The post made in these profiles are intended

[263] https://www.merriam-webster.com/dictionary/social media at 1.30 pm. On 13.01.2021

to reach a larger section of audience unlike messaging which is confined to a target individual or individuals. In addition to general posts the members also put up their personal information, photographs and videos which information is available for public viewing.

### *A. Aspect Of admissibility Of Social network messages/posts*

The rules regarding admissibility of social networking messages and data contained on website is more or less the same. However the certificate under section 65B must essentially contain a brief description of the post or message that is cited as evidence.

### *B. Mode Of Proof Of Social Network Messages/Posts*

The mind boggling issue is typically one of authorship. Authorship of a post of social media cannot be discerned by gathering information about the profile. As fake profiles can easily be created. Likewise a genuine profile is also prone to hacking. Therefore the traditional rules of authentication of such of kind of evidence must be meticulously applied. Generally there must be circumstances sufficient to draw an inference that the purported sender was infact the author.

Profile pages on social network sites raise authentication issues analogous to those raised by website data. In examining the authenticity of the profile it is imperative to bear in mind that essentially anyone is free to create a profile page using whatever name they choose, so the mere existence of a profile page in someone's name does not necessarily reflect that the purported creator had anything to do with its creation. In the absence of significant corroboration courts often exclude social network messages stating their concerns with the websites security and the potential for access by hackers.

Upon interviewing judicial officers, advocates and police personnel on these aspects the researcher found these four common methods of authenticating social network profile or posting:

a) ADMISSION: Facts admitted need not be proved. Where there is an admission in the pleadings or by way of a statement or confession that the social network profile or post belonged to the user from the user himself. No further proof is required.

b) EVIDENCE TAKEN FROM THE DEVICE FROM WHICH THE PROFILE WAS CREATED: If the profile or the post has been created on a device belonging to the creator, seizure of his device and its examination by an expert will give valuable clues about creation of the profile or the post. This is because computers save its usage history and create logs of activity. Even if an activity is deleted, it can be retrieved by a computer forensic scientist.

c) ROGATARIES FROM THE SOCIAL NETWORKING SITE:A third way of obtaining information is directly seeking the information through service provider platform. Here the testimony of the owner of the platform plays a crucial role in authenticating the profile of the user. Platform such as facebook, twitter, instagram can provide information as to time date of creation of profile including the IP address and the location from where the profile was created. Where a social media post is relied upon as evidence in a case and the authorship of the profile is denied in criminal cases the police seek information of the account by writing to the service provider. This is the most challenging and a daunting task as the registered offices of these social networking cites are situated in foreign countries and are not bound by Indian Laws.

An application is made to the court under section 166A[264] of CrPC. The researcher undertook case study of one of such cases decided by the Court of

[264] Section 166A provides "*Notwithstanding anything contained in this Code, if, in the course of an investigation into an offence, an application is made by the investigating officer or any officer superior in rank to the investigating officer that evidence may be available in a country or place outside India, any Criminal Court may issue letter of request to a Court or an authority in that country or place competent to deal with such request to examine orally any person supposed to be acquainted with the facts and circumstances of the case and to record his statement made in the course of such examination and also to require such person or any other person to produce any document or thing which may be in his possession pertaining to the case and to forward all the evidence so taken or collected or the authenticated copies thereof or the thing so collected to the Court issuing such letter.The letter of request*

Chief Judicial Magistrate Panaji and interviewed the concerned Investigating Officer. In that case the accused has posted some objectionable content about the death of a political leader[265] on his Facebook Profile. The Crime Branch filed an application for rogatories under section 166A of the CrPC requesting the court to issue rogatories to FACEBOOK situated in a Foreign Country. Accordingly rogatories were issued seeking information about the account of the accused. The response to such letters essentially depends upon the existence of MLAT (Mutual Legal Assistance Treaty).Likewise authenticating a social media message or post is fairly difficult in Civil cases as no such provision like rogatories is available in case of civil cases.

d) EVIDENCE OF PERSONS WHO HAVE SEEN THE USER OF THE PROFILE AS PARTICIPANT IN A THEARD: When a public post or a post in a private group is made, it is seen by other users as well who respond to it. There is often a thread of replies by other users creating a virtual conversation. Ordinarily electronic conversations on a social networking sites can be authenticated by testimony from a participant in a conversation. The participant can testify on the following points

    a. That he or she knows the user on the social networking site and can identify his profile.

    b. That printouts of the conversation shown to him appear to be accurate records of his or her conversation with the person and

    c. The context of the communication is relevant only to the person or a group of people of whom the person in question is one.

e) OVER ALL CONDUCT OF THE AUTHOR ON SOCIAL MEDIA NETWORK: The court can also be urged to take note of the overall conduct of

---

*shall be transmitted in such manner as the Central Government may specify in this behalf.Every statement recorded or document or thing received under Sub-Section (1) shall be deemed to be the evidence collected during the course of investigation under this Chapter."*

[265] Crime No. 47/2018 under section 505(2) of IPC crime branch Ribander

the holder of the profile if the authorship of the post made by him in question is a fact in issue. The earlier posts made by him of facts or materials which are likely to be exclusively within his knowledge or acknowledgment of the existence of the profile on some other medium are relevant facts which the court can consider as corroborative evidence.

### 4.2.3.Email Messages:

An email[266] is short of Electronic Mail and is a form of electronic document transmission. The email has vital significance as form of evidence. Emails have become most widely used forms of communication considering the ease of usage. However emails can easily be forged or abused. When produced before the court relevancy of an email may arise in these three board categories:

1. The body or the text of the email may itself be a fact in issue.

2.The information about sender receiver or time may be a fact in issue

3.The path of the email i.e. information about logs, servers etc may be a fact in issue especially in cyber crimes such as phishing or sending spam or threatening emails.

As resolution of these issues may require an access to the original email it is imperative for the witness to preserve the original email. It may be noted that forensic tools can be used to retrieve an email that has been deleted.

E-mails contains two main parts namely, the message header and the message body. The header contains routing information about the e-mail, source and destination of the e-mail, the IP address of the sender and time related information. The message body is the

[266] www. merriam-webster dictionary defines email as means or system for transmitting messages electronically (as between computers on a network) at https://www.merriam-webster.com/dictionary/e-mail on 12.1.2021 at 10.00 pm.

actual message of the email message its subject matter. The body may also have attachments tagged to it.

A header is most relevant in Email forensics[267].An email can be traced by computer forensic experts by examining the header information contained in email messages. This information is found on an email either at the beginning or the end of e-mail messages. A thorough investigation of e-mail headers should include examination of the sender's e-mail address and IP address, examination of the message ID as well as the messaging initiation protocol (HTTP or SMTP). Time is very important in e-mail cases as HTTP and SMTP logs are archived frequently. Some e-mails have fake/forged headers in order to deceive investigators, so extreme caution and careful scrutiny should be practiced in investigating every part of the e-mail header[268].

[267] E-mail forensics refers to the study of email details including: source and content of e-mail, in order to identify the actual sender and recipient of a message, date/time of transmission, detailed record of e-mail transaction as well as the intent of the sender. Therefore, e-mail forensic investigation often involves analysis of metadata, keyword searching as well as port scanning, for authorship attribution and identification of cyber-crime. *http://cyberforensicator.com/wp-content/uploads/2017/01/SSARS2016-Charalambous.pdf on 13.2.2020 at 8.30 pm.*

[268] E-mail analysis begins from the recipient's mailbox which contains the e-mail message. The message is analysed to determine the source (originator and author). The analysis involves investigation of both control information (envelope and header) and message body. Mailbox, domain name, message-ID and ENVID are globally unique identities that are used in e-mail. The Mailbox is identified by an e-mail address and domain name is an identifier of an Internet resource. Message-ID is used for threading, aiding identification for duplications and Domain Name System (DNS) tracking. The ENVelope Identifier (ENVID) is used for the purpose of message tracking. E-mail message comprises of envelope that contains transit-handling information used by the Message Handling Service (MHS) and message content which consists of two parts namely Body and Header. The Body is text but can also include multimedia elements in Hyper Text Markup Language (HTML) and attachments encoded in Multi-Purpose Internet Mail Extensions (MIME) (Resnick 2001). The Header is a structured set of fields that include 'From', 'To', 'Subject', 'Date', 'CC', 'BCC', 'Return-To', etc. Headers are included in the message by the sender or by a component of the e-mail system and also contain transit-handling trace information. Further, the message also contains special control data pertaining to Delivery Status (DS) and Message Disposition Notifications (MDN), etc. The control information i.e. envelope and headers including headers in the message body that contain information about the sender and/or the path along which the message has traversed represents the metadata of an e-mail message. The analysis of this metadata called header analysis can be used to determine genuineness of a message. M. Tariq Banday Technology Corner Analysing E-Mail Headers for Forensic Investigation Journal of Digital Forensics, Security and Law, Vol. 6(2)*https://www.researchgate.net/publication/227859085_Technology_Corner_Analysing_E-Mail_Headers_for_Forensic_Investigation on 12.1.2021 at 10.30 pm.*

EXAMPLE OF AN EMAIL HEADER:

| | |
|---|---|
| from: | **ITR Filing** <newsletter@updates.informalnewz.com> |
| reply-to: | ITR Filing <reply@updates.informalnewz.com> |
| to: | "1983kcp@gmail.com" <1983kcp@gmail.com> |
| date: | Jan 13, 2021, 12:43 AM |
| subject: | Missed the income tax return deadline? You can still file it with a fine |
| mailed-by: | mail.updates.informalnewz.com |
| signed-by: | updates.informalnewz.com |

***A. Aspect Of admissibility of email messages***

An email can be produced in a court either in form of a print out or its digital copy can be produced on a CD or on pendrive. As these forms are in the nature of a copy it has to be accompanied by a certificate under section 65B. An email just like a web page when produced with a certificate under section 65B must contain the following information.

1. Complete email in its normal form as displayed on the computer complete with all information contained on its header.

2. Reference if any to the attachments

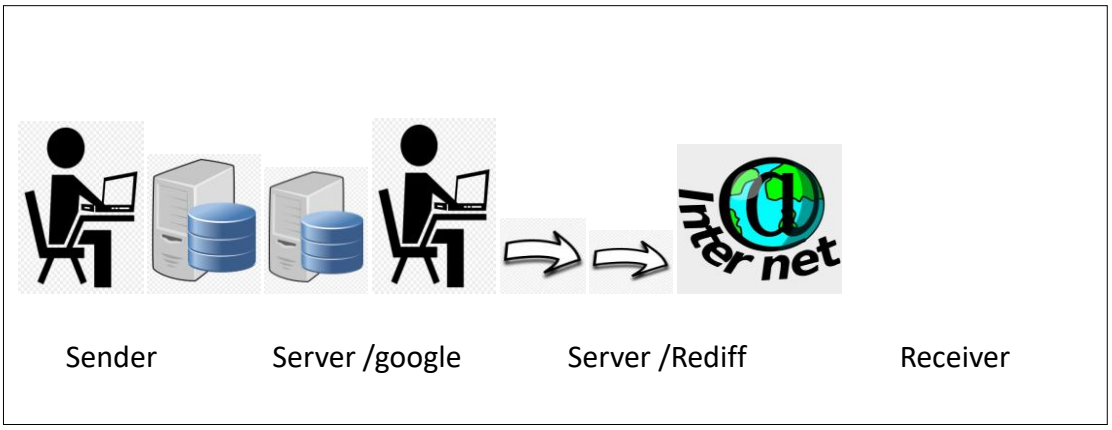
3. The date and time when the witness logged into the email account and obtained a print or copy.

4. Information if any whether the printout was directly taken or whether the email was saved on any disk or device and the form in which it was saved.

5. Whether the original electronic record is available as on the date of submitting the certificate.

5. Lastly all other standard clauses pertaining to the section.

The most intriguing question that arises here is as to who has to give certificate under section 65 B in respect of an email. The picture shown below illustrates the path of a typical email. Illustrative stated A sender A sends an email to receiver B through his google email id. The email travels from google server through the internet and is received by the receiver B on his rediffmail through rediff server.




There are four parties here namely 1. sender 2. receiver 3. ISP Google and 4. ISP rediff. Which of these four persons can or should give a certificate under section 65B ? Strictly speaking any of these four persons can give a certificate under section 65B.

A question may arise whether it is imperative for the internet service provider to give certificate under section 65B as the original mail is in their server?. The answer to this question is contained in section 88A of Indian Evidence Act which creates a presumption that an electronic message, forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission. This presumption however is a rebuttable presumption. Therefore in view of this presumption it is not imperative to examine the Internet Service Provider.

Here it would be apt to state that a certificate under section 65B can also be provided by a person who receives a copy of the email electronically.

In case of server based emails, the certificate has to come from the incharge of the computer servers. In all these cases, the preservation of 'meta-data' is extremely crucial[269].

What happens when the person producing the certificate is neither the sender nor receiver. In such a case it is often argued that any person who has a lawful access to the concerned mail box may produce a copy of the email.

This is where the paradox arises. Section 65B of the Indian Evidence Act permits a person occupying responsible position in connection with the device or management of relevant activities to give a certificate under section 65B. Considering the nature of an email, access to the mailbox becomes a relevant fact. The question therefore arises as to whether a third person who is neither the sender nor receiver producing a certificate under section 65B requires to satisfy the element of responsible position. In other words can a person who hacks email of another and prints it out can give a certificate under section 65B of the Indian Evidence Act.

If section 65B is read as a whole it appears that there is nothing in the section that would bar a hacker from giving such a certificate because the section does not use the term lawful access. This has to be read in the light of the fact that the law does not bar evidence that is unlawfully obtained[270]. The aggrieved may have other remedies against

[269] meta data is data about data and contains information relating to date/time/origin/authenticity/access date of the data, which goes on to strengthen, or destroy its evidentiary or believability quotient

[270] In Umesh Kumar vs State Of A.P. Criminal Appeal No.1305 Of 2013(Supreme Court of India) it was held that "It is a settled legal proposition that even if a document is procured by improper or illegal means, there is no bar to its admissibility if it is relevant and its genuineness is proved. If the evidence is admissible, it does not matter how it has been obtained. However, as a matter of caution, the court in exercise of its discretion may disallow certain evidence in a criminal case if the strict rules of admissibility would operate unfairly against the accused. More so, the court must conclude that it is genuine and free from tampering or mutilation. This court repelled the contention that obtaining evidence illegally by using tape recordings or photographs offend Articles 20(3) and 21 of the Constitution of India as acquiring the evidence by such methods was not the procedure established by law. (Vide: Yusufalli Esmail Nagree v. The State of Maharashtra, AIR 1968 SC 147; Magraj Patodia v. R.K. Birla & Ors., 1970 (2) SCC 888; R.M. Malkani v. State of Maharashtra, AIR 1973 SC 157; Pooran Mal v. Director of Inspection, Income-Tax, New Delhi & Ors., AIR 1974 SC 348; and State (NCT of Delhi) v. Navjot Sandhu alias Afsan Guru, (2005) 11 SCC 600)"

the third party producing such evidence nonetheless it cannot be discarded[271]. This issue is mostly raised in matrimonial cases where spouses plant cameras or spyware devices or obtain unlawful accesses to mail boxes. There is a need of a clear precedent that distinguishes between the term lawful access and responsible position. This issue calls for a critical analysis.

***B. Mode Of Proof Of E-Mail***

Now coming to the issue of mode of proof. Upon interviewing judicial officers, advocates and police personnel on these aspects the researcher found these four common methods of authenticating Emails:

1. ADMISSION.

Facts admitted need not be proved. Where there is an admission in the pleadings or by way of a statement or confession that the email account belonged to the user or the email was sent by the user himself. No further proof is required.

2. EVIDENCE OF THE SENDER/AUTHOR

An email ultimately is akin to any other ordinary mail. Therefore evidence of the author of the email that is duly admitted in evidence after complying with section 65B will suffice as proof of its contents when the contents of the email is a fact in issue.

3. APPEARANCE OF THE EMAIL IN CONJUNCTION WITH OTHER CIRCUMSTANCIAL EVIDENCE:

Even if there is no evidence of a direct participant of the communication, email can be authenticated by reference to its appearance, contents, email id, substance, internal

[271] Section 43(a), (b) and section 66 of the Information Technology Act makes accessing a computer resource and stored information without permission of the owner of the computer resource a punishable offence.

patterns and other distinctive characteristics taken in conjunction with circumstances. However because of the risk of manipulation of email headers these attributes must be cautiously handled. These attributes alone are not sufficient to authenticate an email as having been authored or sent by the opponent. There must be confirming circumstances sufficient enough to prove the factum of authorship.

4. EVIDENCE OF PERSONS WHO HAVE SEEN THE AUTHOR TYPE OR SEND THE EMAIL.

Just like any other conventional forms of evidence advocates are often seen examining witnesses to prove the authorship of an email by examination of persons who have seen the author, type and send it. This often happens in corporate transactions, where the actual author may have left the office. This mode again has to be cautiously used.

5.CIRCUMSTANTIAL EVIDENCE:

Additional circumstances that may suffice to establish that the email was sent by a specific person includes evidence that:

a. The email in question bears the customary format of an email including the addresses of the sender and the recipient.

b. The address of the recipient is consistent with the email address on other emails sent by the same sender.

c. The email contains type written name or nickname of the recipient ( and perhaps, the sender) in the body of the email.

d. The email contains the electronic signature of the sender.

e. The email recites matters that would normally be known only to a number of persons including this individual).

f. Following receipt of the email, the recipient had a discussion with the individual who purportedly sent it and the conversation reflected the individuals knowledge of the contents of email.

6. EVIDENCE OF COMPUTER FORENSIC EXPERT.

In the absence of circumstantial evidence of authenticity there are varieties of technical means by which email transmissions may be traced, such as identifying the encoded internet protocol from which or to which the email was sent. Knowing the IP address that enables one to contact the service provider who can identify the IP address of the sender and the recipient. Therefore if serious authentication issues arise a technical witness may be of assistance. This may be important in cases where a person or entity denies sending an email or denies receipt of email and there is no circumstantial evidence of sending or receipt of email or other electronic communication.

**4.4.4.Text Messages.**

This category of evidence essentially includes text Messages send from a Mobile phone. These messages could be sent using applications such as whatassp, telegram or any other application that enables sending of messages over the internet. Such messages could also be sent by SMS messaging, which allows the user to send text messages over the mobile network.

The foremost difference between an email and text messages was at one time the device that was used to communicate. However as technology has advanced an email can also be sent through a mobile phone and messages can be sent through a computer. Therefore the researcher has tried to gather the general principles relating to admissibility and authentication of text messages which will have to be mutatis mutandi applied vis a vis the device that was used for communication.

The general principles of admissibility of text messages is similar to email in most ways. The difference however for this type of electronic communication is predominantly, the mobile phone that is used.

Admissibility of text messages requires a certificate under section 65B either from the sender or receiver who has legitimate control over the device which was used to send or receive messages. If the original mobile itself containing the text messages is produced before the court there is no need to produce any certificate. However this does not ordinarily happen. Ordinarily text messages are produced in form of printouts. An android phone enables the user to take a screenshot of the text messages. This screenshot usually contains the phone number of the sender and the phone number of the receiver. The researcher found that the screenshot method was the most favoured method of producing evidence in form of whatsassp messages in court.

***A. Aspect Of admissibility of text messages***

When a text message is relied upon as evidence in the court in form of a print out or a copy it must be accompanied by a certificate under section 65B. This certificate must imperatively contain the following information.

1. Message should be ideally produced in form of a screenshot which displays relevant details like the phone number of the sender and the date and time of the message. If not all these details have to be stated.

2. The date and time when the printout was taken.

3. Information if any whether the printout was directly taken or whether the text message was copied and saved on any disk or device and the form in which it was saved.

4. Lastly all other standard clauses pertaining to the section.

***B. Mode Of Proof Of Text Messages***

If the text message is properly printed and a certificate under section 65 B of the Indian Evidence Act is appended to it containing all necessary details there cannot be any defence that the message is not authenticated. However the most intriguing question in respect of such text messages is its authorship. A question may be raised as to whether mere possession of the device or phone number standing alone is sufficient to show that the possessor authored messages sent from that device or number. The answer to this question is obviously negative because technology has advanced to a point where text messages can be remotely sent from a phone number without having physical custody of the device or the sim card. Therefore the proponent of such evidence must present some proof that the messages were actually authored by the person who allegedly sent them. Text messages may be proved by the following modes:

1. ADMISSION:

As in case of other forms of electronic evidence, if there is any judicial or extra judicial admission of authorship the same can be admitted in evidence by following law of admissions under the Indian Evidence Act.

2. IDENTIFICATION OF OWNER OF THE DEVICE AND THE PHONE NUMBER.

The first step in proving a text message is by identifying the owner / user of the phone number from which the message is send. In addition to this the details of ownership of sim card may also be relevant. Nonetheless such messages can be generated by a third person who gets the custody of the mobile of that person or who can electronically secure control over the device. Majority of the courts therefore have not equated evidence of these account user names or numbers as self authentication when taken singularly.

3. CIRCUMSTANCIAL EVIDENCE.

As in case of authentication of email, authorship can be determined by circumstantial evidence as well surrounding the exchange of messages their contents who had the background knowledge to send the message and whether the parties conventionally communicated by text message. Characteristics to consider in determining whether text message evidence has been properly authenticated include:-

a. Sequential consistency with another text message that may be sent by the alleged author or the receiver which is not in dispute.

b. Message having connection with other form of evidence or has been sent in context of a matter proved in other form of evidence.

c. Agreement or understanding between the parties in dispute that communication by way of text messages would be a accepted mode of communication. Especially in cases involving contracts.

d. Past conduct of the parties as may appear from pleadings or evidence on record that the dealings of the parties happened through text messages.

e. Whether the user of the mobile reported any unauthorized use of the mobile at any point of time.

d. Plausibility of unauthorized usage in the absence of any third party specifically named.

F. Inclusion or reference of text message made in any document or email by the alleged user

g. The reasonable probability of the message being generated by a third person who gets the custody of the mobile of that person or who can electronically secure control over the device.

A pertinent question may arise here is whether presumption under Section 88A can be applied to text messages. Section 88A of the Indian Evidence Act provides that the

Court may presume that an electronic message, forwarded by the originator through an electronic mail server to the addressee to whom the message purports to be addressed corresponds with the message as fed into his computer for transmission; but the Court shall not make any presumption as to the person by whom such message was sent. If literal interpretation is given to this provision it appears that it pertains to only electronic mail. However considering that a text message works on the same protocol this presumption should be made inclusive of all electronic messages which are adjusdem generis.

**4.4.5. Computer Records.**

The first question that needs to be clarified at this juncture is when every electronic record is generated by a computer why create a separate category for this kind of document. This question has been answered at the outset. This category includes all such electronic record that is generated or stored in a computer other then the types mentioned above. The emphasis of this category is on auto generated computer records its authentication and admissibility. This category excludes documents that are generated by a computer that is used as a typewriter.

Where law requires manual authentication of documents which may be printed from a computer, section 65B or the whole law of electronic evidence has no application. Such evidence may be authenticated by a witness in the same manner as a paper document. When a computer is simply used as a typewriter, computer stored documents should be proved in the same manner are a paper document. However where a witness denies of having created the document and if its origin can be traced to a computer, evidence can be produced to raise the probability of the witness being its author.

It can be proved by distinctive characteristics that establish a connection of a particular person to that document. The mere presence of a document in a computer will suffice as an indication of a connection with a person or persons having ordinary access to that

file. However how much will depend upon the surrounding facts and circumstances of each case. Ideally it cannot be made the sole basis of proof and it is reasonable to insist on corroboration.

For example, if the fact in issue is whether a particular email was sent at a particular time from a particular laptop having a internet connection of a particular address. The meta data stored in the computer such as the cache files, time stamps and IP address can be produced in the court as evidence. This kind of evidence will constitute computer generated records.

Before the researcher proceeds further on the aspect of admissibility and authentication of computer records, it is essential to explain the distinction between the term computer generated records and computer stored records.

There are two types of computer records, one that is created by a human agency on a computer and the second created by a program fitted in the computer. For eg a letter typed by a person on the computer will come in the former category whereas call logs will come in the latter. The former can be classified as Computer stored records whereas the latter can be called computer generated documents. Computer generated material is a product of the machine itself (not a person using that machine). A computer generated electronic record is essentially created by processing data by following a set algorithm or command. For example. Call record details, History of logs saved on a computer, data generated by an ATM Machine.

Shri Adam Wolfson in his article "Electronic Fingerprints" published in the Michigan Law Review Association[272] has explained the distinction between computer stored and computer generated records as under .

"*The crucial distinction courts should not ignore about computer records is that some records are computer stored while others are computer generated. In essence, computer*

[272] Adam Wolfson, '"Electronic fingerprints": Doing Away With The Conception Of Computer-Generated Records As Hearsay' (2005) 104 Mich Law Rev 165.

*stored records are human assertions stored in an electronic format. These records constitute: assertions because they are " the by product of a machine operation which uses for its input " statements" entered into the machine by out of court declarants. Examples of this type of record include : word processor files, spreadsheets, such as Microsoft excel files charts graphs and emails." Accordingly these records are statements and fit easily under the classic definition of hearsay. Computer generated records, on the other hand are records that are self generated by the computer. This is a sometimes deceptively simple definition because human interaction often triggers the computer processes which create the records; however, the crucial factor is whether the record is a mark of computer activity or if it is the electronically saved statements of a human user. A common example of this type of record is the trace report created by a telephone company computer when it monitors calls made to a specific phone number. When person dials that number, the computer automatically creates the report no human must assert that the call was made in order for the record to be generated. Other examples include ATM receipts, computer document " meta data" and internet protocol (IP) logs on computer network."*

The question arises as to whether both categories of documents can be authenticated in the same manner?. The answer to this question may be in the negative. Because in case of the former it suffices to examine the author of the document. Whereas in case of the latter a person having lawful control over the device will be able to testify about its operation.

In the latter case, that is in case of computer generated documents. It may so happen that the program may require the intervention of a human agency in feeding the data. Even in such cases testimony of a person having lawful control over the device even though he may have not actually fed in the data will suffice in the facts and circumstances of the case.

***A. Aspect Of admissibility of Computer Records.***

For a copy of the computer generated electronic record to be admissible in court it is imperative to produce a certificate under section 65B of the Indian Evidence Act. However in this category, when producing a certificate under section 65B of the Indian Evidence Act both the aspects below have to be covered in addition to the general points discussed above:

a. a description of the system or process to produce a particular result.

b. evidence showing that that the process or system produces an accurate result in ordinary circumstances.

***B. Mode of proof of Computer Records***

Computer generated records will have to be proved in the same manner as social network messages, *mutatis mutandi*. Infact the rigour of proving authorship does not exist in cases of computer generated records.

***C. Whether computer generated records are heresay evidence?***

As noted above since a computer generated record can be admitted through a person having lawful control over the same, who need not be the author of that document,a question may arise as to whether there is a possibility of it being classified as hearsay? There may be. However making such an interpretation will push every computer generated record to a very low pedestal.

***D. Arguments against treating computer generated records as heresay:***

The first argument is that computer is not a person but is a machine, therefore the margin of human error, tendency to improvise or concoct the facts in issue is virtually

impossible. On the contrary as the fact in issue is generated by the computer by following a algorithm or a command, the accuracy of the information so presented will be much higher then what is perceived by a human being using any of his senses and reproduced in the court even as firsthand account.

The second argument is that the fact in issue may not be a statement made by the computer. The fact may be a result of a process that the information fed in the computer may have undergone. Historically the courts have excluded animals and machines from the rule of heresay. Same analogy applies to computers.

Thirdly, the rule against hearsay was adopted on account of the accuracy level that can be attributed to first hand or direct evidence. In case of computer generated records the accuracy level is much higher even when compared to direct evidence of a human agency.

Fourthly, classifying computer generated records as hearsay may often frustrate the purpose of promoting accurate fact finding for computer crimes like electronic terrorism, internet stalking computer trespass etc because it may prohibit highly relevant and trustworthy evidence regarding crime.

Fifth is that the truth and falsity of the process of generating a record is subject to verification as long as the record is available, which is not the case when direct evidence is produced in the court especially, when the evidence is oral evidence.

### *E.* ***Electronic Fingerprint Test***

The electronic fingerprint test is premised on the hypothesis that computer generated records are like human fingerprints. When any surface is touched by a human being he leaves his fingerprints behind. Likewise when any computer is accessed or subjected to any kind of activity, the computer records that activity in form of meta data.

For example, when a phone is used for calling its service provider creates a log of all the calls made. Similarly, when the computer is used to access the internet the system will make a log of all the activities conducted. This process being mechanical its possibility of being manipulated is very less. And therefore the accuracy of this electronic fingerprint is very high. These fingerprints therefore are used to establish trail of a transaction. The difficulty however is the verifiability of the information presented in the court at the time of trial. The computer from which this information is derived may not be in working condition at the time when the matter comes up for trial. Or the person producing the information may not have lawful control over the computer from which the information is derived or that the information may have been deleted or wiped off.

To avoid a successful challenge to the authenticity of such electronic fingerprints it would be essential to adopt all safeguards of its proper seizure, forensic analysis and documentation of the entire process.

Photoshop images contain metadata which can be computer generated. This meta data records a wide variety of data. Illustratively stated details as to when the file was opened or modified, the user who assessed the file, the computer used, any actions taken with respect to the file ( such as printing or emailing it to another computer). A similar example is online journals which contain both types of data combined in one, the sites user created content may be rightfully excluded while computer generated logs of the website itself are admitted into record. Because of the computer evidences highly unified presentation, Judges and lawyers alike can miss the crucial distinctions that make parts of the evidence admissible and other parts barred[273].

[273] Electronic, Evidence by Dr Gupta Agarwal Premier Publication Company 2018

### 4.4.6. Digital Photographs, Video And Audio( Visual Or Audio Evidence)

Digital Photographs, Video and audio are the most commonly produced electronic records. This form of electronic evidence is also most susceptible to tampering. In other words it is simple to edit, rearrange the chronology of events depicted, distort the passage of time and show events out of sequence and context in this form of electronic record. The most prickly part is that this tampering cannot be easily discerned, thereby leading to misleading assumptions based on this form of electronic record. The digital recording process also involves compressing video data to save hard drive space, which can lead to data loss and affect image quality.

#### *A. Aspect of admissibility of Digital photographs, Video and audio*

Unlike other form of electronic evidence audio and video electronic record is not produced in form of printout. The data contained in electronic form is generally copied and stored on a pendrive or a compact disk. For this compact disk to be admissible in evidence it has to be accompanied by a certificate under section 65B of the Evidence Act. Photographs are ordinarily produced in court either in form of a CD or a printout or both. This certificate is in form of a template and needs to be modified as per the facts of the case. Therefore the certificate must imperatively contain the following information.

1. Brief description of the electronic record that is contained in the CD or pendrive particularly in case of audio and video evidence.

2. Time stamp of the relevant fact disclosed in case the audio and video evidence runs into several frames.

3. Details of creation access and chain of custody and all such details that may be necessary to clear all doubts in the mind of the judge regarding preservation of integrity of the data. Here it is pertinent to clarify that although section 65B does not make it mandatory to state these details however this is the best stage and opportunity to state them on oath.

4. Information if any whether the copy was directly made or whether it was first saved on any disk or device and the form in which it was saved.

5. Lastly all other standard clauses pertaining to the section.

***B. Mode Of Proof Of Digital Photographs, Video And Audio***

Visual or audio evidence will have to be proved in the same manner as any other electronic record mutatis mutandi, however in case of such evidence if the authenticity of the original is in dispute only expert evidence can certify that the electronic record has not been tampered with. The court has to apply general rules of evidence, probability and burden of proof before requisitioning services of an expert.

The advantage of this form of electronic record ( Digital photographs, Video and audio( Visual or audio evidence) is that the original electronic record can be conveniently produced before the court. If the original storage device is produced for the inspection of the court, there is no need to resort to section 65B of the Indian Evidence Act.

This has been the dictum of the practically all courts in India when interpreting section 65B. The researcher however finds an anomaly here. What is made admissible by the Indian Evidence Act is a document, a document presupposes that it is produced in the same form as it would be visible for the court to admit in evidence and assess its value. The court is not expected to subject the document to any process and thereafter view and assess the end result. When the original storage device(say the removable disk or memory card) is produced before the court, for the court to view its contents the device will have to be plugged to a source which would convert the form in which the data is stored to a form that is readable. In other words, if the fact in issue are photographs, a mere look at the memory card will not help the judge to assess the photographs that are produced as evidence. The judge will have to place the memory card in a card reader and view its contents on the screen. What the judge has seen on the screen in effect

constitutes relevant evidence. The form of evidence to be appreciated is what is seen on the screen and not what is seen in the envelope in form of a rectangular card.

Now if by producing the original the party is absolved from the liability of producing a copy, the relevant evidence in the form in which it has to be appreciated will never form a part of record. Every time this evidence is to be assessed the process of plugging it to a reading device will have to be followed. There will be serious repercussions to this exercise. Firstly handling the original constantly will cause data loss. Secondly, such is process of dealing with evidence is not recognized by any of our procedural codes. Thirdly and most importantly preservation of such electronic record which is essentially magnetically stored till a considerable period of time will be an impossibility.

***C. Difficulties faced in production of video evidence:***

1. **No specific time stamp of the fact or event in issue**.

In a lot of criminal cases video recording of a crime or an event is produced. Most of the times it is in the nature of a CCTV footages that runs into several minutes. The event that constitutes the bundle of relevant facts appears on the screen after a lot of unwanted material is played on the screen. The researcher therefore interviewed prosecutor and judges who have opined in unison that the Police have to put a time stamp to the relevant portion of the video either in the panchanama if any or in the memorandum along with which the video is produced. This therefore saves valuable time of the court.

2. **Lack of description of relevancy of the video**

When any evidence is produced in the court there has to be some means for the court to determine its relevancy before it is permitted to be tendered in evidence. In a criminal case the need is even more pressing, as the video recording sometimes is relied upon at the time of arguments before charge. In case of other documentary evidence, the perusal of the document itself, including photographs, indicates the nature of its contents. This is not the case in Video recordings. Sometimes there is nothing in the chargesheet for the prosecutor to have a clue as to what is there in the video recording.

This is because either the panchanama of seizure is not done or the panchanama is not descriptive enough to contain details of what the video depicts. Sometimes the device containing the original electronic record is seized and directly sent to CFSL for making copies. These copies are directly produced in the court without the Investigating Officer getting an opportunity to view it earlier. It is therefore essential that the investigating officer plays the copy of the video submitted in the court and documents the process by conducting a panchanama.

3. **Preservation of magnetic disks or electronic fiches when record produced in court.**

The most challenging aspect in respect of audio visual evidence is preservation of magnetic disks or electronic fiches when a record is produced in court. As per the data collected by the researcher no courts in Goa are equipped with an independent Malkhana or Muddemal room meant to keep electronic record. Most of the times such magnetic disks are stitched along with paper documents and are handled in the same manner as paper documents. Sometimes pendrives and CDs are kept in the safe custody of Nazir which again are stored in regular drawers or cupboards. This often leads to damage and wear and tear thus making the electronic record unreadable at the time when it may be required to be tendered in evidence.

**4. Intervention of an expert imperative where a video or photograph is subjected to forensic analysis.**

Sometimes the police resort to image enhancement to get more clarity especially if the image is taken in a dark mode. Here an expert can remove the graininess noise etc, revealing finer details hidden beneath what can be apparently seen by a naked eye. Such digitally enhanced videos or images have to be produced in evidence only through an expert. Because image enhancement comes with a risk. The more you enhance a video, the more admissibility of your final product can be challenged in court on the ground that the image has been altered and is no longer accurate or fair.

### 4.4.7. Bank Statements

In today's time practically every bank maintains its ledger in electronic form. Therefore when any bank statements are purported to be produced before the court they are produced in form of printout obtained from accounting software. Bank statements as evidence are governed by the Bankers Book Evidence Act. The objective of the Act was to streamline the process of maintaining bank records and to regulate its production in the court of law as evidence. The Act acquires significance particularly because it contains a provision that a certified copy of any entry in a Bankers Book shall be received as *prima facie* evidence of the existence of such entry, in all legal proceedings[274] . The word Bankers Book[275] and certified copy[276] has been defined under the Act.

---

[274] Section 4. Mode of proof of entries in bankers books .Subject to the provisions of this Act, a certified copy of any entry in a bankers book shall in all legal proceedings be received as *prima facie* evidence of the existence of such entry, and shall be admitted as evidence of the matters, transactions and accounts therein recorded in every case where, and to the same extent as, the original entry itself is now by law admissible, but not further or otherwise.

[275] Section 2(3): "bankers books" include ledgers, day-books, cash-books, account-books and all other records used in the ordinary business of a bank, whether these records are kept in written form or stored in a micro film, magnetic tape or in any other form of mechanical or electronic data retrieval mechanism, either onsite or at any offsite location including a back-up or disaster recovery site of both

[276] Section 2(3):(8) certified copy means when the books of a bank,

(a) are maintained in written form, a copy of any entry in such books together with a certificate written at the foot of such copy that it is a true copy of such entry, that such entry is contained in one of the ordinary books of the bank and was made in the usual and ordinary course of business and that such book is still in the custody of the bank, and where the copy was obtained by a mechanical or other process which in itself ensured the accuracy of the copy, a further certificate to that effect, but where the book from which such copy was prepared has been destroyed in the usual course of the banks business after the date on which the copy had been so prepared, a further certificate to that effect, each such certificate being dated and subscribed by the principal accountant or manager of the bank with his name and official title; and

(b) consist of printouts of data stored in a floppy, disc, tape or any other electro-magnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of section 2-A;]

(c) a printout of any entry in the books of a bank stored in a micro film, magnetic tape or in any other form of mechanical or electronic data retrieval mechanism obtained by a mechanical or other process which in itself ensures the accuracy of such printout as a copy of such entry and such printout contains the certificate in accordance with the provisions of section 2-A.]

Prior to its amendment by the Information Technology Act a Bank statement had to be produced accompanied by a certificate under section 2 of the Bankers Book Evidence Act certifying that this is a true copy of the entry, that such entry is contained in one of the ordinary books of the bank and was made in the usual and ordinary course of business and that such book is still in the custody of the bank, and where the copy was obtained by a mechanical or other process which in itself ensured the accuracy of the copy. If the book from which such copy was prepared has been destroyed in the usual course of the bank's business after the date on which the copy had been so prepared, a further certificate to that effect must be produced, each such certificate being dated and subscribed by the principal accountant or manager of the bank with his name and official title[277].

In respect of the books now being electronically maintained, an additional certificate is prescribed by inserting section 2A to the Bankers Book Evidence Act. Also section 2(8) was amended to incorporate electronic records**.** Section 2A**[278]** lays down conditions in

[277] Section 2 (8): "Certified Copy" means when the books of a bank,-a) are maintained in written form, a copy of any entry in such books together with a certificate written at the foot of such copy that it is a true copy of such entry, that such entry is contained in one of the ordinary books of the bank and was made in the usual and ordinary course of business and that such book is still in the custody of the bank, and where the copy was obtained by a mechanical or other process which in itself ensured the accuracy of the copy, a further certificate to that effect, but where the book from which such copy was prepared has been destroyed in the usual course of the bank's business after the date on which the copy had been so prepared, a further certificate to that effect, each such certificate being dated and subscribed by the principal accountant or manager of the bank with his name and official title; and

(b) consist of printouts of data stored in a floppy, disc, tape or any other electro-magnetic data storage device, a printout of such entry or a copy of such printout together with such statements certified in accordance with the provisions of section 2A.

(c) a printout of any entry in the books' of a bank stored in a micro film, magnetic tape or in any other form of mechanical or electronic data retrieval mechanism obtained by a mechanical or other process which in itself ensures the accuracy of such printout as a copy of such entry and such printout contains the certificate in accordance with the provisions of section 2A.

[278] Section 2A of Bankers Book Evidence Act: Conditions in the printout:

A printout of entry or a copy of printout referred to in sub-section (8) of section 2 shall be accompanied by the following, namely :-

(a) a certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and

(b)a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of -

(A) the safeguards adopted by the system to ensure that data is entered or any other operation performed

the printout taken under section 2(8) of the Act. It provides that a printout of entry or a copy of printout referred to in sub-section (8) of section 2 shall be accompanied by (a) a certificate to the effect that it is a printout of such entry or a copy of such printout by the principal accountant or branch manager; and (b) a certificate by a person in-charge of computer system containing a brief description of the computer system and the particulars of the safeguards adopted by the system to ensure the integrity of the data, identification of such data storage devices, the safeguards to prevent and detect any tampering with the system; and any other factor, which will vouch for the integrity and accuracy of the system.

There is no clarity in the Bankers Book Evidence Act as to whether section 2A is exclusive of section 65B of the Indian Evidence Act. It may be argued that since the Bankers Book Evidence Act is a special law it shall have precedence upon the general law of evidence and hence a certificate simplicitor under section 2A will suffice. However one cannot be oblivious to the fact that section 65B begins with a non-obstante clause. This being the case it may also be argued that for a printout of any electronic record to be admissible in evidence, the production of a certificate under section 65B is imperative.

It was held in the case of ***Om Prakash v. Central Bureau of Investigation***[279] that Section 65B of the Indian Evidence Act is pari materia to Section 2A of the Bankers' Books Evidence Act and therefore they should be construed together. However the court was dealing with an issue were there was no certificate was produced under section 2A

---

only by authorized persons;
(B)the safeguards adopted to prevent and detect unauthorized change of data;
(C) the safeguards available to retrieve data that is lost due to systemic failure or any other reasons;
(D)the manner in which data is transferred from the system to removable media like floppies, discs, tapes or other electromagnetic data storage devices;
(E)the mode of verification in order to ensure that data has been accurately transferred to such removable media;
(F) the mode of identification of such data storage devices;
(G)the arrangements for the storage and custody of such storage devices;
(H) the safeguards to prevent and detect any tampering with the system; and
(I)any other factor, which will vouch for the integrity and accuracy of the system.

[279] Om Prakash v. Central Bureau of Investigation 1999 (48) DRJ 686

of the Bankers Book Evidence Act. The court followed the maxim of 'generalia specialibus' and held that Section 2A of the Bankers Book Evidence Act will be preferred over Section 65B of the Indian Evidence Act in dealing with banking records in electronic form.

What would happen if the reverse situation exists. Can the court exempt a party from filing a certificate under section 65B of the Indian Evidence Act and rely only on the certificates filed under section 2A Bankers Book Evidence Act. The researcher was unable to find any judgment which has set this issue to rest.

If the principle laid by the Delhi High court in ***Om Prakash (supra***) is considered, it may appear that a certificate under section 2A will suffice. However with utmost respect to the findings of the learned judge the researcher finds that although section 2A of the Bankers Book Evidence Act is pari materia to section 65B it is not identical in the sense one can replace the other. Section 65B is boarder on certain aspects that have not been covered by section 2A and specifically begins with a no obstante clause. The researcher is therefore of the view that for a electronic bank statement to be admissible it is necessary to produce all certificates namely a certificate under section 2A of the Bankers Book Evidence Act and Section 65B of the Indian Evidence Act. In other words no certified copy from an electronically maintained bankers book will be admissible in evidence until all the above certificates are produced.

### 4.4.8 Self Authenticating Documents:

A self-authenticating document is generally a document that can be admitted into evidence at a trial without any proof being produced to support the claim that the document is what it appears to be.

The Indian Evidence Act does not contain any provision that permits self authentication of electronic records unlike the US Federal Rules of Evidence[280].Basic computer operations relied in ordinary course of business are admitted without an elaborate emphasis on accuracy. The accuracy of the individual computer will not be scrutinized unless specifically challenged and even perceived errors in the output are not significant enough to challenge its admissibility.

The courts however come across documents that contain a line " that this document is self authenticated and does not require signature" like in case of E- Tickets or e-challan or E- Tax Invoice.

Although these computer generated records can be admitted in evidence when accompanied by a certificate under section 65B. The certificate only ensures the correctness of its contents from vis a vis the receiver.

The difficulty arises when the document is an invoice say taken from a grocery store. There are no signatures affixed on such documents. The person to whom the invoices are issued cannot be expected to produce a certificate under section 65B. There is no clarity under the Indian Law as regards self authentication of third party electronic records.

[280] The Federal Rules of Evidence were amended effective December 1, 2017 to make it easier to authenticate data from electronic sources. The new rules describe a process for authenticating records "generated by an electronic process or system," such as a printout from a webpage, or a document retrieved from files stored in a personal computer. They also provide for using a "process of digital identification" such as hash values to authenticate that electronic data is what it purports to be. Rule 902 lists "items of evidence that are self-authenticating" and "require no extrinsic evidence of authenticity in order to be admitted." Amendments effective December 1, 2017 added two new items of evidence to this list. Rule 902(13) provides for the self-authentication of: "A record generated by an electronic process or system that produces an accurate result, as shown by a certification of a qualified person that complies with the certification requirements of Rule 902(11) or (12). The proponent must also meet the notice requirements of Rule 902(11)."

## 4.5 General Principles Of Appreciation Of Evidence That May Be Specifically Applied In Appreciation Of Electronic Evidence.

The researcher interviewed a sample size of judicial officers, prosecutors and advocates who echoed the sentiment that is generally expressed by all that electronic evidence is a new breed of evidence that requires a specialized law. This however would not deter the courts from relying on electronic evidence and appreciating the same in the context of the existing laws. Therefore the stakeholders are found to apply the following general principles in appreciating electronic records.

1. Most courts do not recognize the objection as to fabrication and insist on expert evidence, unless there is plausible ground to contend that the electronic record has been altered or is fabricated. Pure speculation or unsupported conjectures are generally discouraged.

2. Minor irregularities in the evidence do make the electronic evidence inadmissible unless the irregularity goes to the root of the matter and is incurable. Here the principle of procedures being a handmaid of justice is generally applied.

3. Principle of Conditional relevance: Most judges relate the issue of authentication of electronic record to the fact that the record seeks to prove. For example in case of an audio recording the question whether the voice in the recording is of the accused or not may be fact that requires intervention of an expert. But the question whether the mobile that was used for recording belonged to a particular person or not, the number to which call was made belonged to the accused etc. can be proved by regular mode.

4. In case of self authenticating documents no further proof is insisted upon and ordinarily the authenticity of such documents is not disputed.

5. Circumstantial evidence cannot be a substitute to prove the integrity of an electronic record when the same has been questioned, however where a fact is sought to be proved by other modes as well as electronic evidence, circumstantial evidence is

found to play major role for the court to accept or reject the objections on fabrication of electronic record.

6. The intertwined authentication/relevance issues: At times the integrity of data contained in the electronic record may not be a fact in issue, the only disputed fact may be its authorship. In such cases evidence is not rejected on the ground that the integrity of the data has not been proved. An opportunity is given to the party relying upon the electronic record to prove the relevant fact by adducing any other form of evidence.

7. Best evidence Rule: In deciding whether an electronic record is sufficiently authenticated, the court generally apply the best evidence rule. It is determined whether a party has exhausted all the modes available to him to authenticate the electronic record.

8. Rule against heresay: When admitting and authenticating electronic records there is complete bar in proving the same through a third person who has no role in

**4.6 Precautions To Be Taken In Production Of Any Kind Of Electronic Record.**

1. Preservation of the original: The most important rule in respect of this form of electronic record is preservation of the original image, audio or video. Computer forensic scientists also propose using image security software, however the same is not feasible for private parties. Secondly, such record should be preserved in their original file formats. Compressing of files must be avoided as substantial data may be lost in this process. If images are stored on a computer that is accessed by several individuals it is advisable to make these files password protected or read only.

2. Documenting the process of copying: When any form of electronic record is produced the endeavour is to clear all doubts in the mind of the judge regarding preservation of integrity of the data. Therefore there must be a clear record particularly stating the chain of custody. This can be best achieved in criminal cases by preparing a

detailed panchanama and in Civil cases by incorporating relevant facts in the certificate under section 65B of the Indian Evidence Act.

3. Evidence of the person recording the image or video: Strictly speaking, as section 65B contains a non obstante clause it is not permissible to prove or admit an electronic record by oral evidence. However if the fact in issue is as to who created, generated or transmitted the electronic record(when the record is generated, created or transmitted by a human agency) , then the evidence of the person who did so would be relevant. Visual and audio evidence, is usually created by a human agency therefore the evidence of the person creating that evidence would be most relevant.

**4.7 Case Studies:**

In this part of the Chapter the researcher has randomly studied pending cases in Courts of Goa involving some king of electronic evidence. Although the researcher went through a number of files nonetheless has selected 20 of them which were found to have greater significance to the research. The researcher has also referred to three civil cases as the issue involved therein is of universal importance.

**Case No.1**

**State v. Alister Fernandes;** ***SCORS 2.2020;*** **District and Sessions Court Panaji**

This is a case where accused was charged under section 67A, 67B, of the Information Technology Act and Section 82 of the Goa Children's Act and Section 4 of the Protection of Children from Sexual Offences Act, 2012. The case is that the accused created a fake face book profile of the victim. The police have attached the mobile of the accused and sent it for CFSL Examination. However no correspondence was made from facebook to show details about who opened the account and when it was opened etc. Also no CDR was attached or obtained and the police have merely relied on the call

history on the mobile.

**Case No.2**

**State v. Dinesh Kumar ; *SCORS 6.2021* ; District and Sessions Court Margao**

This is a murder case where the accused was charged under section 302 of IPC, where the police have photographed the scene of offence and disclosure Panchanama. In addition to examining the panchas the police have also examined police photographer who has produced a certificate under section 65B of the Indian Evidence Act and has produced a CD containing photographs. Here it is pertinent to note that the original electronic record which is contained in the memory card of the camera has not been produced. What are produced are printouts of the photographs and a CD. I have perused the certificate given under section 65B of the Indian Evidence Act however it is noted that the certificate is not as per the requirement of section 65B and it does not contain details of section 65B(2) which has to certify the integrity of the process that was used to generate the computer output.

**Case No.3**

**State v. Eppliel Dhanwar; *Sessions case 1/2018*; District and Sessions Court Margao**

This is a case under section 302 of the Indian Penal Code. The police had produced photograph showing the place of offence. The prosecution has examined police photographer as PW7. PW 7 has deposed that he has clicked the photos and downloaded them on a CD. He has produced the CD which is exhibited by the witness and he has also identified the hard copy of the photographs produced through panch witnesses. The issue in this case is that there is no noting in the file stating that the CD is viewed in the court as the certificate produced by the witness under section 65 B is only confined to the fact that the photos were transferred from the memory card of the phone of the

witness to the CD produced in Court. There is no certificate under section 65B certifying that the photographs which are printed on the photographic paper and produced through the panch witnesses have been printed either through the original contained in the mobile phone of PW7 or from the CD which is generated by PW7 from the original electronic record contained in his mobile phone. In other words there is no document linking the original photos on the memory card with the photos that a printed on the photographic paper. Secondly, the certificate under section 65B does not state the requirements of section 65B(2).

**Case No. 4**

**State v/s Mohammad Zameer; *Sessions case 45 of 2019* ; District and Sessions Court Margao**

This is a case under section 307 of Indian Penal Code. The electronic evidence produced herein are photographs of section 27 of the Indian Evidence Act. No certificate under section 65B is produced or taken on record. Neither the accused or is advocate has objected to the production of photographs or its marking without a certificate under section 65B. Person who has clicked photographs has not be cited as a witness nor any certificate under section 65B is produced subsequent to the filing of the chart sheet in order to support that the photographs that have been produced along with the panchanama. Here this exercise relevant on account of the fact that the photographs would not be admissible until and unless a certificate under section 65B is produced. And since the issue pertains to admissibility of the document any amount of no objection from the opponent cannot rectify the defect.

**Case No.5**

**State v/s Saroj Surendra Betkikar; *Sessions case 34 of 2019*; District and Sessions Court Margao**

This is a case under section 307(2) of Indian Penal Code and section 4 and 5 of Immortal Traffic Prevention Act of 1956. The police have attached electronic record namely one mobile phone found with the accused and one mobile phone found with the victim. As per the complaint the police have received information that the accused will be coming to a certain spot to deliver victim girls to prospective customers for prostitution. Accordingly the police conducted raid and attached the belongings of the accused and the victim. These mobile phones are a part of the said belongings. The issue here is that the attachment of the mobile phones without showing how the electronic record is relevant to the fact in issue is unnecessary. Such recovery only burdens the record of the court and serves no purpose. Researcher has checked the entire charge sheet and noted that there was nothing from the said mobile that was investigated including call records if any therefore the recovery and attachment of the said mobiles from the accused and the victim is an exercise in vain.

**Case No.6**

**VPK Credit Society v. Anthony Joao Fernandes; *Case No. 419/OA/2019*; District and Sessions Court Margao**

This is a complaint under section 138 of Negotiable Instruments Act. The electronic record that is produced in this case is a loan account statement generated by the finance society which is maintained in a computer package in electronic form. There is a certificate produced under section 65B of the Indian Evidence Act. It is noted that this certificate is not at all in compliance with section 65B or section 2A of the Bankers Book Evidence Act. In fact the certificate does not bear any endorsement that it is under section 2A of the Bankers Book Evidence Act. The person who has produced the certificate is not the signatory of the said certificate.

**Case No. 7**

**Mrs. Maria Sylvia Cardozo e V. . Mrs. Savita Tina Cardozo e Caiado; *Regular Civil Suit No. 598/2010/D* (CJJD D Court Margao)**

In this case when the defence witness was in the witness box she was confronted with a voice recording which was not relied upon at by the plaintiff at the first instance along with the plaint. The witness denied her voice and the CD was marked X for identification, subject to production of certificate under 65B. Thereafter an application was made in the court to send the CD for expert analysis under section 45A of the Evidence Act which was also allowed. However eventually the CD was not sent, as the plaintiffs failed to take steps. Questions that arose in this case is whether a witness could be confronted for the first time with a copy of an electronic record without it being produced in evidence or without it being accompanied by any certificate under section 65B? And when the authenticity of an electronic record is in dispute how should the court deal with it? In this case court permitted the defendants to subsequently produce certificate under section 65B and allowed the application for referring the electronic record to expert.

**Case No.8**

**Maria Beatriz De Souza v. Agnelo John Bosco Savio Fernandes; *Civil Misc. Application no.80/2009/A* (CJSD A Court Panaji)**

In this case the respondent relied upon receipts of travel itinerary issued to the respondent by Jet Airways, some tax credit documents issued by the ministry of Revenue and Customs, U.K., some documents issued by a hospital in UK all of which were copies of original electronic record belonging to a third party which is not connected with this litigation. It was contended that the respondent, therefore, is not in a position to produce the certificate u/s 65B of the Indian Evidence Act and view of the judgement in the case of Shafi Mohammad (supra)leave may be granted to produce

these documents. The court allowed the application holding that leave can be granted to produce these documents in view of Shafi mohd ( which case is now overruled) issue of admissibility was set to rest, however if the other side objects the documents were ordered to be marked subject to proof. Moot questions arising in this case is after the judgement of Shafi Mohd (supra) being overruled how third party electronic records which are formal in nature such as travel itnenery, tax invoices or receipts, even provision store bills which are auto generated can be proved. Eventually till the point of final arguments the documents were not proved as per law.

**Case No.9**

**The Indian Performing Right Society v. The CEO, Entertainment Society of Goa (ESG); *Civil Suit No. 4.2011*( District Judge 3 Panaji)**

In this case a plaintiff filed a suit under section 62 of the Copyright Act 1957 and had relied upon 5 CDs containing the recording of the music played at a music festival in violation of the Copy Right Act. When the matter came up for a trial, the plaintiff contended that he had lost the compact discs and applied to the registry for copying from the CDs that were filed along with the suit. The trial Court dismissed the plaintiff's application. It held that the CDs lying with the Court is secondary evidence and that the plaintiff cannot have the secondary evidence of that secondary evidence. Again a similar application was filed explaining that about seven years ago its people recorded the event on a mobile phone and, later, transferred the digital data on to five compact discs. Now the video recording on that mobile phone was erased and was lost. It could not be retrieved. Second application was also dismissed by the trial court. In a writ petition, the Hon'ble High court allowed the application keeping the issue of admissibility and mode of proof open[281].

[281] The Hon'ble High court observed that *" I reckon the validity of the video recording available either on the CDs lying with the Court or on any other device to be produced by the plaintiff is a matter of*

**Case No. 10**

**Cyber Crime Police Station versus Anita Marissa D Cruz *Criminal Case (IPC) 425 of 2018* Court of JMFC H court Margao** .

This is a chargesheet filed under section 66C and 66D of the Information Technology Act. The case of the prosecution is that the accused committed identity theft of the complainant and further used the fake profile of the complainant on facebook to cheat Goan boys who are working abroad and make them send money and thereby committed offence of cheating by a impersonation by using computer resource. Prosecution has examined the complainant and she has produced screenshots of the print outs in respect of the Facebook profile having her profile name along with certificate under section 65B, however it is noted that she has not given the details of the computer from which the print out was taken. It is further noted that the Investigating Officer had made a request letter under section 91 of CRPC seeking relevant details of the person who has created the Facebook profile. Prosecution has produced and email from the enforcement response team of Facebook giving details of the IP address from which the profile was created. Since the matter is undertrial the main point is how the prosecution will admit and prove the email sent from Facebook which is the most crucial evidence to connect the accused to the offence.

---

*adjudication under, say, Section 65 of the Indian Evidence Act. It is the plaintiff's case that he has lost the material evidence in his possession, but he wanted to take advantage of the material lying with the registry. In fact, the plaintiff itself produced that material before the trial Court. Once the plaintiff secures the copies of the compact discs lying with the Court, it is entirely open for the defendant to object to its validity or admissibility when that evidence is sought to be tendered, during the trial. Only then can the trial Court rule on that aspect: the admissibility of secondary evidence. Instead, here, the trial Court has prematurely ruled on an issue which has not yet arisen. 8. Under these circumstances, I set aside the impugned order, dated 19.01.2019, and direct the trial Court to allow the plaintiff to have copies of the five compact discs already available on the Court's record. I also clarify that it is entirely upon the defendant, or the Court on its own accord, to object to the validity and admissibility of the evidence the plaintiff wants to rely on during the trial.* WRIT PETITION NO.273 OF 2019 para 6

**Case No. 11**

**Margao Town Police Station versus Glenn D Souza*; IPC 466 of 2018*; JMFC H Court Margao**

This is a chargesheet filed under section 295 and 427 of IPC. The case of the prosecution is that the accused damaged the structure of golden cross at Margao thereby hurting the religious feelings of the complainant and Christian community. The prosecution has relied upon a CCTV footage. Footage is produced in form of a CD. The owner of the CCTV camera Mr Wilson Fernandes has deposed that the police came to his house and requested to have access to the CCTV footage and after viewing the footage asked for a copy. He accordingly contacted the CCTV operator and give them the CCTV footage on a compact disc. List of witnesses show that the said CCTV operator Santosh is listed as witness number 5. It is noted that in the list of documents filed along with the chargesheet Section 65B certificate is produced. This section 65B certificate is signed by Santosh. However the same is extremely cryptic and does not contain the requisite ingredients of section 65B. The prosecution has not made any attempt to play the CCTV footage in the presence of Wilson or other witnesses who claim to have seen the CCTV footage. There are no details in the panchanama where the IO has showed CCTV footage to the panchas before the recovery. It is also not stated anywhere in the chargesheet as to on which time stamp the accused is seen committing the act in the CCTV footage and no details are given to the court about the time stamp connecting the accused to the CCTV footage. An issue may arise in this case. Suppose if the accused disputes the authenticity of the CCTV footage whether the original footage recorded in the DVR will be available at the relevant time for forensic examination ?

**Case No. 12**

**Kshatratej Urban Co-operative Credit Society Ltd. versus Shaber Desur: *Case Number 181/OA/2020* : JMFC H Court Margao.**

In this case the complainant has produced statement of loan account generated by a computer application along with the certificate under section 65B however the certificate under section 65B is does not contain the requisite details as required by law. Further there is no certificate produced under section 2A of Bankers Book Evidence Act. The section 65B certificate is signed by one Desai who identifies himself as the Chief Executive Officer of the society.

**Case No. 13**

**State v. Abdul Azziz Batwani; *174/S/2014*; Court of Chief Judicial Magistrate Panaji**.

Accused was charged under section 457 and section 380 of IPC. Electronic Evidence involved in this case was a CCTV footage which was produced on a CD with section 65B certificate. The CCTV footage was attached under the scene of offence panchanama and the CD was produced through PW1 Rajesh Redkar. The CCTV footage was shown to all witnesses examined in the court who were from the office where the theft was committed. The court at the time of passing that judgement however did not consider the CCTV footage as relevant evidence as the accused was masked.

**Case No. 14**

**State v. Guri Shankar Gajre *: SCORS 24/2018*: Court of Additional Sessions Judge FTC-1 Panaji**

In this case the accused was charged for committing theft in an ATM. There was CCTV

footage available in the said ATM. CCTV footage was produced on a CD which was attachéd under the panchanama. This CCTV footage was shown to the complainant/injured. The court viewed the CCTV footage and noted that the CCTV footage depicted in clip 3. Here it is pertinent to note that the court had to view all clips in the CCTV footage to single out that clip 3 as relevant. There were no such details provided in the panchanama.

**Case No. 15**

**State v. Ismail Mulla @Chutto; *SC 8/2020;* District and Sessions Court Margao**

This is a murder case filed under section 302 of IPC. The case of the prosecution is that after the murder the accused called his friend on his mobile and the friend recorded the call. The police attached the said mobile from the friend under a panchanama where the recording was played to the pancha and the contents of the conversation were stated in the panchamama. The mobile was sent to GFSL with a request letter to the GFSL Verna to record the voice sample of the accused. The GFSL recorded the voice sample using some forensic software. The comparison report is awaited from GFSL. The charge sheet is filed. Trial is in progress.

**Case No. 16.**

**State of Goa v. Om Prakash Chand; *SC 7.2019;* DJI and Addl Sessions Judge Margao.**

This is a murder case filed under section 302 of IPC. The case of the prosecution is that the entire incident of murder was captured on a CCTV where the witnesses have identified the accused. The CCTV was first encountered by the Investigating Officer when he visited the scene of offence for the first time. Thereafter he viewed the CCTV footage and found that the incident of murder was recorded on it. Eyewitness at the scene identified the assailant accused by name hence the police could easily trace him.

The IO thereafter conducted a scene of offence panchanama and attached the original electronic record namely the DVR and hard disk which was forwarded to the FSL Verna Goa along with two blank Hard disks and 2 pen drives. The GFSL copied the data on the hard disk as well as on the pen drive and forwarded the exhibits to the court along with certificate under section 65B. It is pertinent to note that original DVR and the hard disk has not been opened and played in the court. What was played and shown to the relevant witnesses was the footage on the pen drive.

**Case No 17.**

**State v. Vijendra @Chetan Arondekar *SC 3.2017* DJI and Addl Sessions Judge Margao**

The accused was charged for murder of his girlfriend. There were no eye witnesses to the said offence. As per the case of the prosecution the accused sent a message (SMS) to the sister of the deceased where he confessed that he is going to kill the deceased and he too will commit suicide. The Police attached the mobile of the accused and sent it for forensic examination. The sim card from which the sms was sent belonged to the deceased. The Police also obtained the CDR of the mobile from which the SMS was sent and the mobile on which it was received. The only issue was how the prosecution would prove that the SMS was sent by the accused. The learned court looked into the fact that the deceased and the accused has a love affair. The phone number that was saved as being of the accused in the call records of many eye witnesses. The IMEI No. of the sim card found in the mobile that was attached from the accused corresponds with the imei no. on the SIM card found on that mobile. Hence the court found that the fact that the mobile belongs to the accused stands proved.

**Case No. 18.**

**State v. Jerry Feranandes; *SPCC 2.2021* Court of Additional Sessions Judge Margao.**

The accused has been charged under section 7, 13(1)(d) r/w 13(2) of the Prevention of Corruption Act. As per the chargesheet the complainant has recorded a conversation between the accused and him where the accused has made a demand of bribe. The complainant further has stated that he has recorded the conversation on a CD and the CD was played at the police station in the presence of Panch witnesses and attached under the panchanama. Thereafter the Police have conducted a trap and arrested the accused. Thereafter the Investigating officer has taken voice sample of the accused and sent it to CFSL for comparison with the voice recorded on the CD. And the CFSL has opined that it is the probable voice of the same speaker. The matter is at preliminary stage and evidence is yet to be recorded however it is noted that the original mobile on which the call/conversation was recorded was not sent to CSFL. And neither has it been produced along with the chargesheet. What is produced is a CD which is a copy of the original electronic record. Secondly there is no certificate under section 65B given by the complainant in support of the CD.

**Case No. 19.**

**Suchilinga Dash v. Tapam Kumar Dash *31/PWDV/2020* JMFC G court Margao.**

This is a case under section 12 of the PWDV Act. The case of the applicant is that she was subjected to domestic violence and she has prayed for protection orders to be passed. In reply the respondent husband has alleged that a false case is filed against him and that the applicant is having an extra marital affair. He has relied upon photographs of the mobile screen containing whatsapp chats. And printout of some whatassp chats. It is seen that the printouts are taken from the mobile screen of the applicant. Admittedly the Mobile Phone is not in custody of that respondent. All the electronic record produced is in form of printouts but no certificate under section 65B is produced. The matter is at preliminary stage. Although a defence was raised about the extra marital affair at the stage of arguments on interim relief but no orders have been passed.

**Case No. 20**

**State v. Vivek Govekar *IPC/337/2015* JMFC B court Panaji.**

The accused has been charged under section Section 354 C of IPC. The accusation against the accused was that accused fitting his mobile with its camera on in the toilet of Architecture College and recorded videos of women using toilet thus outraging their modesty. The police attached the original electronic record which is the mobile phone and without sending it for forensic examination the same was produced in the court. At the time of attachment the offending videos were played in the presence of panchas at the police station and what was viewed by the panchas was succinctly stated in the panchanama. When the matter came up for trial the mobile phone was shown to the pancha of the attachment panchanama and he identified the mobile. Thereafter an attempt was made to switch on the mobile but the mobile could not be switched on. The prosecution thereafter filed an application to view the CD with the help of Memory card reader. Accordingly the CD has been viewed with the help of a memory card reader and minutes have been drawn about its contents by the court. In the meanwhile accused filed an application requesting the court to issue directions to furnish the copy of the video clips available in the memory card of MO No. 1 which is pending for adjudication.

Thus the case studies above reveal there is no uniform process that is followed to produce and prove electronic evidence in the courts in Goa. There is still confusion among lawyers, prosecutors and investigating officers about the relevancy of the evidence sought to be produced. Even if that hurdle is crossed there appears to be laxity in concentrating on making the copy of electronic record admissible.

In the next Chapter the researcher has assessed the empirical data obtained from the stakeholders and has drawn inferences there from to test the hypothesis.

# Chapter 5

# Data Analysis And Findings: Comparison Of Idealism With Practical Reality

## 5.1 Introduction

Having elucidated in the foregoing chapter No. 4 the modes employed by the Police for seizure of electronic record and the modes used by the courts to admit and authenticate electronic records, this chapter shall examine the sufficiency of the existing laws and regulations to in admitting and proving a fact through electronic evidence.

Strictly speaking no form of evidence can guarantee full proof of authenticity of facts in issue. That is why the law prescribes standards of beyond reasonable doubt or balance of probabilities in ascertaining the truth of the fact in issue. However electronic evidence is a new breed of evidence that was not anticipated at a time when the Indian Evidence Act was enacted. No doubt the same has been amended to cater to this form of evidence, this chapter shall examine on various parameters whether these amendments or any other statutory enactments are sufficient to cover all aspects of electronic records. The hypothesis broadly generated for this research is that there exist impediments in the existing law and legal systems that hinders the proper seizure, preservation, admissibility and mode of proof of electronic evidence. As stated in Chapter 1 these impediments can broadly be divided into two categories:

1. Impediments at procedural level of legislation.
2. Impediments at substantive level of legislation.

The entire hypothesis rallies around these two factors. At the outset it is pertinent to note that use of the word procedural level here implies the stage where the electronic evidence is seized, procured, presented and preserved as evidence. Broadly speaking these impediments would mean and include the impediments that are faced on field at the time when electronic evidence is procured, seized, preserved, copied and produced

in the court. In this part of the chapter the researcher has examined the real challenges that the stake holders face in this process. Anticipating the impediments at procedural level the researcher had observed in her hypothesis that there is limited use of methods of investigation using electronic evidence due of lack of information, knowledge and training. Further that the present rules of procedure is obsolete and do not contain a full proof mechanism for making optimum use of electronic evidence. There is inadequate infrastructure available in the State of Goa that would assist the law enforcing agencies in proper preservation, production and authentication of electronic evidence in court.

The term substantive level employed here is intended to simply mean the law and legislations. The researcher in chapter 1 had hypothesised as to how the existing legislations are found wanting in providing a complete framework, which is conscious of the fallible nature of electronic records. The researcher had hypothesised that the amendments are essentially general in nature enacted without anticipating the variety of the forms in which electronic records are produced as evidence.

## 5.2 The Mode Of Empirical Research

To test these hypothesis against real time data the researcher has taken the views of relevant stake holders namely judicial officers, police, prosecutors and advocates. The first interaction with electronic records is of the Police. The responsibility of presenting it in admissible form and proving it as per law is upon the learned advocates and the learned public prosecutors. But the most important task is vested in judicial officers who appreciate the evidence produced and hold that either the evidence has sufficiently proved a fact, or has failed to prove the same.

These stake holders where asked questions about the issues relevant to the hypothesis raised. Based on their responses the researcher has tested the hypothesis.

**5.2.1 Identification of the Universe**:

The universe for the purpose of this study is the State of Goa. As per 2001 census, the population of the State is 13,43,998. Judicially, the State is organised into two districts, North Goa comprising of six talukas and South Goa comprising of 5 talukas. In all there are 383 villages of which 233 are in North Goa District and 150 in South Goa District. As per the 2001 census, there are 44 towns of which 14 are Municipalities and remaining are Census towns.

The State of Goa consists of two judicial districts namely the North Goa and South Goa districts. The details of number of courts and their strength and overall vacancy position is described in tables 3 to 6 below:

**Table 3**

*Taluka wise number of Courts in North Goa District.*

| **NORTH GOA DISTRICT** | | | |
|---|---|---|---|
| **Taluka** | **District Courts** | **Trial Courts** | **Total** |
| Tiswadi Taluka | **5** | **6** | 11 Courts |
| Bardez Taluka | **3** | **7** | 10 Courts |
| Ponda Taluka | **1** | **3** | 04 Courts |
| Bicholim Taluka | - | **3** | 03 Courts |
| Sattari Taluka | - | **1** | 01 Court |
| Pernem Taluka | - | **1** | 01 Court |

*Source: District and Sessions Court North Goa*

**Table 4**

*Details of strength and Place of sitting of Court: North Goa District*

| **Sr. No.** | **Name of the Court** | **Sanctioned Strength** | **Place of sitting** | **Remarks** |
|---|---|---|---|---|
| 1 | Principal District & Sessions Court | 1 at Panaji | At Panaji | ---- |

| | | | | |
|---|---|---|---|---|
| 2 | Regular District and Addl. Sessions Court | 6 | 3 at Panaji<br>2 at Mapusa<br>1 at Ponda | |
| 3 | Adhoc District and Addl/Assist Sessions Court | 3 | 2 at Panaji<br>1 at Mapusa | All are Fast Track Courts, initially appointed as Assistant sessions judge and additional sessions powers have been conferred to the Judicial Officers after completion of one year) |
| 5 | Chief Judicial Magistrate & Senior Civil Judge | 1 at Panaji | At Panaji | ---- |
| 6 | Addl Senior Civil Judge and JMFC | **6** | 1 at Panaji<br>3 at Mapusa<br>1 at Bicholim<br>1 at Ponda | Some judicial officers officiate as (Adhoc) Senior Civil Judge & JMFC |
| 8 | Civil Judge Junior Division and JMFC | **15** | 4 Mapusa<br>4 Panaji<br>2 Ponda<br>2 Bicholim<br>1 Pernem<br>1 Valpoi | 1 post vacant at Valpoi (Gram Nyayalaya) |

*Source: District and Sessions Court North Goa*

**Table 5**

*Taluka wise number of Courts in South Goa District.*

| **SOUTH GOA DISTRICT** | | | |
|---|---|---|---|
| **Taluka** | **District Courts** | **Trial Courts** | **Total** |
| Salcette Taluka | **6** | **10** | 16 Courts |
| Mormugao Taluka | - | **4** | 04 Courts |
| QuepemTaluka | - | **2** | 02 Courts |
| Sanguem Taluka | - | **1** | 01 Courts |
| Canacona Taluka | - | **1** | 01 Court |

*Source: District and Sessions Court South Goa*

**Table 6**

*Details of strength and Place of sitting of Court:South Goa District*

| **Sr. No.** | **Name of the Court** | **Sanctioned Strength** | **Place of sitting** | **Remarks** |
|---|---|---|---|---|
| 1 | Principal District & Sessions Court | 1 at Margao | At Margao | ---- |
| 2 | Regular District and Addl. Sessions Court | 4 | All at Margao | |
| 3 | Adhoc District and Addl/Assist Sessions Court | 2 | All at Margao | All are Fast Track Courts, initially appointed as Assistant Sessions Judge and additional sessions powers have been conferred to the Judicial Officers after completion of one year) |

| | | | | |
|---|---|---|---|---|
| 5 | Chief Judicial Magistrate & Senior Civil Judge | 1 at Margao | At Margao | ---- |
| 6 | Addl Senior Civil Judge and JMFC | **6** | 3 at Margao<br>2 at Vasco<br>1 at Quepem | Some judicial officers officiate as (Adhoc) Senior Civil Judge & JMFC |
| 8 | Civil Judge Junior Division and JMFC | **11** | 6 Margao<br>2 Vasco<br>1 Quepem<br>1 Sanguem<br>1 Canacona | 1 post vacant at Canacona (Gram Nyayalaya) |

*Source: District and Sessions Court South Goa*

Like wise as per *https://citizen.goapolice.gov.in/web/guest* there are 12 police stations in North Goa District and 16 police stations in South Goa district. In addition to this there are 16 other police stations such as crime Branch, Cyber crime Police station etc. The list of police stations in the State of Goa are provided in **Annexure 2**.

### 5.2.2 Methods of Data Collection

The accessible portion of the universe, are the stake holders. For the purpose of this study the term population shall be considered vis a vis 4 categories of stake holders namely (1) Judicial Officers, (2) Prosecutors, (3) Lawyers, (4) Police.

The researcher is conscious that the process of sampling is based on the principle of generalization. The sample frame for this research is extremely broad as the total number of the stake holders are large in number therefore sampling frame size is selected 50 Judicial officers, 150 lawyers, 150 Police personnel, and 50 prosecutors.

The samples representing an independent unit are reliable and a valid source of data as they have all characteristics of the cluster/Strata of population that they represent. At the time of selection of sample, the researcher has earnestly attempted to make the sample feasible, practical and empirical to the study. The researcher adopted the survey method, interview method, case study method and observation technique and use of Empirical Data from Custodian Primary Sources for the research.

Then the entire population, of stake holders was divided into four categories the researcher used the random stratified sampling method so as to indentify the smaller homogenous group existing within the population. These fourfold stake holders are judges, prosecutors, police, lawyers as stated above. For conducting survey into this homogenous group the researcher employed the random sampling techniques.

For the interview and case study method the researcher used the non probability sampling technique and purposive and convenience sampling sub technique. The person selected for interview were persons who had essentially dealt with cases relating to electronic evidence and had first hand experience in handling cases with electronic evidence. Based on these interviews the researcher has conducted case studies of 20 cases pending in the court of North and South Goa district to study the manner in which different form of electronic evidence is handled in the court of law.

### 5.2.3 Tools Of Data Collection

The researcher followed 4 tools of data collection namely, Personal Observation, Interview with stakeholders, Questionnaire, Empirical Data from Custodian Primary Sources

To employ the personal observation technique the researcher was in an advantageous position being a judicial officer, having 15 years experience, first as a trial court judge and presently as a Sessions Court Judge. The researcher therefore could purposefully and carefully watch the process of use, admission and proof of electronic evidence to draw out factual statements with adequate evidence. The observation therefore was essentially participant and non structured.

Using the Interview Technique the researcher interviewed a select few from amongst the stakeholders including bank representatives and computer forensic experts who were not a part of the survey population. From amongst the survey population employing partly the convenience sampling method and partly the purposive sampling method the researcher has interviewed some vital persons from amongst the survey population, consisting of Police, Judges, Forensic scientists, Lawyers, Prosecutors and even Litigants. These persons may or may not have constituted the sample used in the survey method for administration of the questionnaire. Considering that this research is not purely emphirical the researcher conducted an unstructured interview as it provided a high degree of flexibility to both the interviewer and the interviewee in questioning and responding.

Next the researcher took aid of questionnaires. The stratified random samples of the four stake holders were administered four different questionnaires. Although substantively the questionnaires had common questions however to some extent they were customised keeping in mind the role that each stake holder played in the matter of production/seizure, admission and appreciation of electronic evidence. The questionnaire was a combination of closed as well open ended responses. However as the data which was to be obtained from the questionnaire was to be analysed there were higher number of closed questions. Some questions in the questionnaire were used in form of rating scale so as to ascertain the extent of comfort and interaction of the respondents with electronic records.

The research needed foundational data essentially, empirical in nature, from various stakeholders and Government Departments. Here the researcher with the aid of Right to Information Act and request letters has obtained the same from the various legal

custodians of that data.

### 5.3 Data Analysis

The researcher interviewed sample size of judges to ascertain from them as to what are the anticipated objections when an electronic record is not properly produced. The most common answers were that 1. Seizure was not properly done, 2. Electronic evidence was not properly preserved, 3. The electronic record was not properly admitted, 4. The electronic record was not properly proved, 5. The electronic record is not properly appreciated in evidence.

The first two objections pertain to the **investigation stage**, the third and fourth pertain to objections raised at **trial stage** and the fifth pertains to objections raised at **appreciation of evidence stage**. When an electronic record is produced as evidence care must be taken to ensure that the original electronic record is properly *procured, preserved and extracted.* The first part of the chapter examines whether there are any procedural safeguards prescribed by the legislature in matters of seizure, procurement and preservation of electronic evidence, the knowledge of the police of this process and the infrastructure available. The first part therefore examines the challenges that are faced at the investigation stage. The second part examines the knowledge of the other three stake holders namely the prosecution, judiciary and advocates of the subject of electronic evidence, challenges in the process of production and availability of infrastructure. This therefore encapsulates the challenges that are faced at trial stage. The first two parts of the chapter is backed by empirical data. Third part of the chapter is essentially critical study of the law based on doctrinal research.

#### 5.3.1 Practical Challenges at Investigation Stage:

The stakeholder that has first contact with relevant electronic evidence is the Police. The Police are enjoined with the responsibility of seizure, preservation and production of electronic record in the court. The researcher using the mode of questionnaires examined the challenges faced by them in this process.

First the researcher has examined the comparable case load of cases involving electronic evidence vis a vis cases involving conventional form of evidence. In the light of this data the researcher has then taken a bird's eye view of the comfort level of investigating agencies on the subject of electronic evidence.

**A. Case Load Of Cases Involving Electronic Evidence At The Stage Of Investigation.**

At the outset it would be proper to look into the aspect comparable case load of cases involving electronic records and cases involving other forms of evidence at the stage of investigation. This shall underscore the importance of laying emphasis on streamlining the process of evidence collection in matters pertaining to electronic evidence. The Police Personnel were asked as to how often they have handled cases containing some form of electronic evidence and further what is the nature of cases where electronic evidence is commonly found. Their response is noted as under:

**Table 7**

*Caseload Of Cases Involving Electronic Evidence At Investigation Stage*

| Sr No. | Percentage | Response | Percentage |
|---|---|---|---|
| 1 | Less then 20% of the total number of cases | 44 | 29% |
| 2 | About 50% of the total number of cases | 87 | 58% |
| 3 | More than 50% of the total number of cases. | 19 | 13% |
| 4 | Never | 0 | 0 |

*Source Primary data*

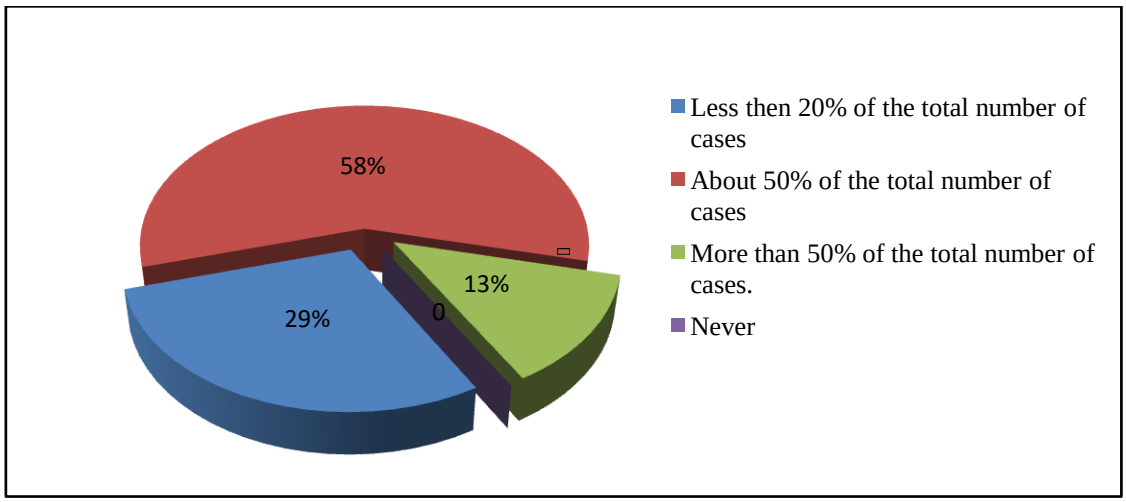



**Figure 1** *Caseload Of Cases Involving Electronic Evidence At Investigation Stage*

Table 7 and Figure 1 represents the views of Police officers about the caseload of cases involving electronic evidence. The researcher had given options of four distinct categories to choose from indicating the percentage of cases involving electronic evidence. 10 percent of the respondents have chosen the first category of electronic evidence constituting less then 20% of the case load. 59% of respondents have chosen the second category of cases being about 50%. 31% of respondents have chosen the third category of cases being more then 50%. 1% of respondents stated that they have never handled any case involving electronic evidence. The pie chart showing the trend in the case load of cases involving electronic evidence therefore indicates that about 50 to more than 50 cases that come for investigation have some kind of electronic evidence involved in it. This electronic evidence may be in most simple form such as photographs or complicated forms like Meta data etc.

B. **Knowledge And Understanding Of The Subject Of Electronic Evidence amongst Police Personnel:**

The most important factor that determines the quality of search and seizure is the comfort level of the Investigating Officer with the subject of electronic evidence. The greater the comfort level, higher will be his knowledge and understanding of the subject

of electronic evidence. Hence the researcher assessed the familiarity of the police with the subject of electronic evidence and evidences other then electronic evidence on a rating scale. At the outset on the scale of 1 to 10, 150 investigating officers were asked to rate their familiarity with the subject of electronic evidence, Where 1 stands for low and 10 for high. Their response has been as under:

**Table 8**

*Rating Scale Showing Familiarity Of The Police With Electronic Evidence*

| Scale | Response |
|---|---|
| 1 | 0 |
| 2 | 0 |
| 3 | 0 |
| 4 | 0 |
| 5 | 15 |
| 6 | 35 |
| 7 | 75 |
| 8 | 12 |
| 9 | 13 |
| 10 | 0 |

*Source: Primary data*

*NOTE: Rank 1 stands for lowest and rank 10 stands for highest.*

Further on the scale of 1 to 10, 150 Investigating Officers were asked to rate their familiarity with subject of evidence other then electronic evidence, Where 1 stands for low and 10 for high. Their response has been as under:

**Table 9**

*Rating Scale Showing Familiarity Of The Police with Evidence other then Electronic Evidence*

| Scale | Response |
|---|---|
| 1 | 0 |
| 2 | 0 |
| 3 | 0 |
| 4 | 0 |
| 5 | 7 |
| 6 | 35 |
| 7 | 12 |
| 8 | 83 |
| 9 | 13 |
| 10 | 0 |

*Source: Primary data*

*NOTE: Rank 1 stands for lowest and rank 10 stands for highest.*

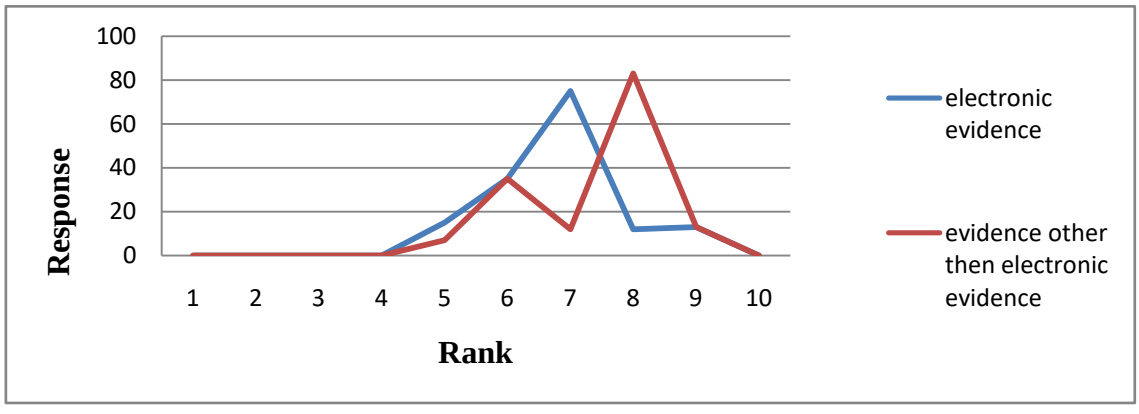



**Figure 2**: *Trends in familiarity of Police on the subject of electronic evidence vis a vis evidence other then electronic evidence*

Upon analysis the Table 8 and Table 9 and Figure 3 it is seen that in the category of electronic evidence, the highest ranking was given as 7 by as many as 75 respondents from a total 150. Whereas for other regular forms of evidence the highest ranking of 8 was given by 83 respondents. This therefore goes to show that Police are more familiar with regular form of evidence then electronic evidence. Consequently there is greater comfort level in handling and seizure of conventional form of evidence in contrast with electronic evidence.

**C. Knowledge of rules and procedure in handling electronic record.**

The functionary/ stake holder that has the first interaction with an electronic record is the Police. As noted in chapter 4 above there is a certain protocol that needs to be followed at the time of seizure of electronic records. There are however no such rules, regulations or SOP prescribed by the legislature for that purpose. The question that needs to be addressed is the extent of knowledge of the Police about the Standard operating procedures or rules if any prescribed by the Legislature for seizure and handling of electronic evidence at the time of investigation or trial.

The case studies reveal that there is no uniform procedure followed by the investigating officers in seizure of electronic record. Whereas some investigating officers seize the original electronic record and produce it in the court, others taken a printout and produce them and whereas some seize the original electronic record and send it to forensic science laboratory for extraction of data therefrom.

Police respondents were asked whether they are aware of any Standard operating procedures or rules prescribed by the Government of Goa for seizure and handling of electronic evidence at the time of investigation or trial. The question was a closed question with option of affirmative and negative as answers.

The respondents have answered as under:

**Table 10**

*Knowledge of Police about rules or procedure of seizure and preservation of electronic record.*

| Response | Number | Percentage |
|---|---|---|
| YES | 48 | 32% |
| No | 102 | 68% |

*Source: Primary data*

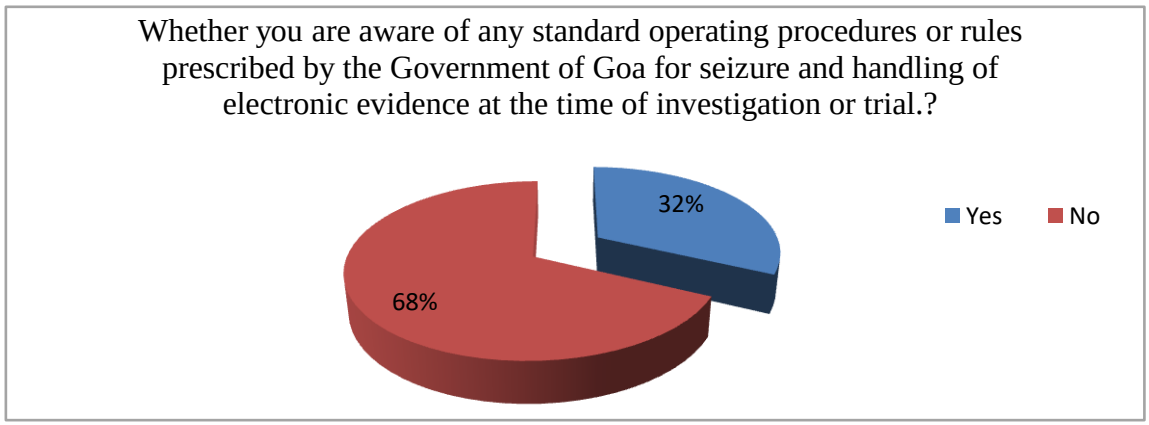



**Figure 3:** *Knowledge of Police about rules or procedure of seizure and preservation of electronic record*

Table 10 and Figure 3 represents the data about the knowledge of the police about rules or procedure of seizure and preservation of electronic record. 102 respondents out of 150 were not aware of any SOP or rules made by the Legislature for seizure and handling of electronic record. Only 48 answered in the affirmative. To avoid a false claim of knowledge the respondents who answered in the affirmative were asked to give details of such SOP or rules. Out of the police personnel who have answered in the affirmative only 4 have answered the next question and given details. Three have stated that they refer to the rules given to them by training academies in the course of trainings. One respondent has given a vague answer. This exercise only fortifies that

there are no standardized rules of procedure in seizure, preservation and production of electronic record and even if judicial and police training academies have prepared handbooks and training manuals, majority of the police personnel are not aware of them.

The analysis of the data above suggests that electronic evidence being a new form of evidence has not been as rooted and streamlined as the traditional forms of evidence. Even if there are no statutory rules or SOP for handling electronic evidence majority of the Investigating Officers are not aware of any guidelines issued by the Ministry of Home affairs or the Cyber Crime investigation manual.

Further concerned Department were asked a question as to whether any directions are issued to the Police Officers or staff as SOP (Standard Operating Procedure), rules or notification for handling electronic records in the court produced in civil and criminal cases. All the departments have answered as under:

**Table 11**

*Details of existence of SOP (Standard Operating Procedure), rules or notification for handling electronic records*

| Name of the department | Response | Remarks |
|---|---|---|
| Police Department | Negative | On oral inquiry with the cyber crime PS. It was informed that the Police follow Cyber Crimes Investigation Manual[282] |
| North Goa District Court | Negative | |

[282] The Cyber Crimes Investigation Manual is an outcome of a partnership between NASSCOM and DSCI representing Indian IT industry, and the law enforcement agencies across India. This publication contributes to the development of standardized methodologies for cyber crime investigations.To standardize the operating procedures for cybercrime investigation, DSCI has prepared Cyber Crime Investigation Manual which is based on its experience of operating the Cyber Labs and working with the police in handling many of the cybercrimes over the last few years. The manual aims to bring a uniform and scientific approach in investigating these crimes and bringing them to the court of law. The manual covers a comprehensive list of Cybercrime topics including procedures for pre-investigation, evidence collection, and handling evidence.

| | | |
|---|---|---|
| South Goa District Court | Negative | |
| Directorate of Information and Technology | Negative | No reply received till date. |

Source: *Data obtained from Concerned Head of Departments.*

As enunciated in Chapter 4 above in 2018 the Ministry of Home Affairs (MHA) with the help of central training institutes, stakeholder Ministries, States, academia and professional bodies conducted a course on Cybercrime Investigation and released a Handbook For Police Officers And State Law Enforcement Agencies. This book which is created, compiled and edited by CCPWC - PMU team MHA. Annexure 1 gives general draft certificate under section 65. Annexure 2 gives a sample certificate u/s. 65B to be issued by service providers for authenticating Call Data Records (CDR). Annexure 3 gives List of Nodal officers of Service Providers along with their emails and area of operation. As per the Advisory released by MHA on 2/2/18 (F.No 22006/2/2017-CIS-II), a recommended training schedule is given under Annexure 4 of the handbook[283].

These rules can at the most be comparable to Drug Law Enforcement, Field Officers' Handbook" prepared by the Narcotics Control Bureau, Ministry of Home Affairs, Government of India. In the case of ***Manas Krishna T K v. State***[284] Bombay High Court has held that the Drug Law Enforcement Field Officers' Handbook issued by the NCB had no legal efficacy, or any statutory flavor nor is the handbook a set of executive instructions issued by the Central Government. Therefore with the proposition at hand that there are no rules or statutory procedure laying down the manner in which data or electronic record has to be seized procured preserved and extracted the researcher has proceed to examine how the absence of universal techniques affect the efficacy of electronic records as evidence to prove a fact.

[283] *https://ssb.gov.in/WriteReadData/LINKS/5%20days36c9f227-7ceb-4b60-bada-f52beeb7e196.pdf on 12.11.2021 at 10.00 pm.*

[284] Criminal Misc Application 88.2021

**D. Availability Of Adequate Infrastructure For Investigating Agencies.**

This part of the chapter examines the availability of proper infrastructure at the stage of investigation. It looks into the aspect of creating digital images or availability of forensic assistance. At pre-trial stage the first exercise that has to be undertaken by the investigating officer is seizure of an electronic record either from the crime scene or the suspect or a witness. Sometimes it is convenient to seize the original record, like in case of a mobile phone, but sometimes there may be complicated processes that may have to be undertaken at crime scene. Sometimes the holder of the original electronic record may be reluctant to part with the same as in case of a DVR containing CCTV footage or a mobile belonging to a third party where there may be an accidental recording. In such cases it is necessary that the Investigating Officer is equipped with some technical assistance that would help him in immediately making cloned copies(images) of the original.

Hence the researcher in this part of the chapter examined whether investigating officers are aware of the concept of cloning or image creation, whether there is equipment available at the police station to conduct such processes and if not whether there is any emergency computer forensic response accessible.Thus at the outset a sample size of the respondents were asked whether they were aware of a process called cloning in the context of electronic evidence. The Police respondents have answered as under:

**Table 12**

*Awareness about cloning process among Police*

| Response | Number | Percentage |
|---|---|---|
| YES | 39 | 26% |
| No | 111 | 74% |

*Source: Primary data*

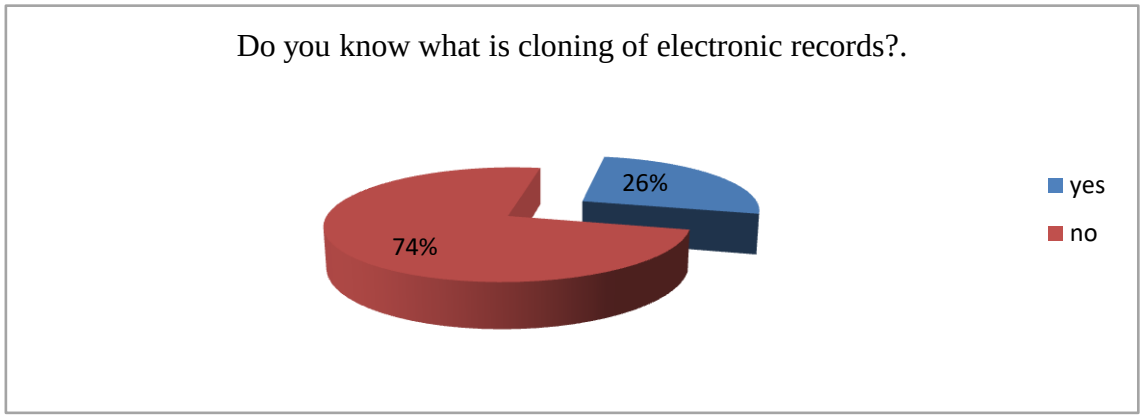



**Figure 4 :** *Awareness about cloning process among Police*

Table 12 and figure 4 indicates the knowledge police personnel of the concept of cloning. To the question whether they are aware of the concept of cloning of electronic records 26% police respondents have answered in the affirmative and 74% have answered in the negative. Resultantly majority of the police respondents are not aware that when an electronic record is seized they are supposed to make an image or a cloned copy of the same.

The next question asked was whether the police station equipped with a device that assists the police in making cloned copies of electronic records at the time of investigation to which the respondents have answered as under:

**Table 13**

*Existence of device for making images or cloned copies at Police Station*

| Response | Number | Percentage |
|---|---|---|
| YES | 10 | 7% |
| No | 140 | 93% |

*Source: Primary data*

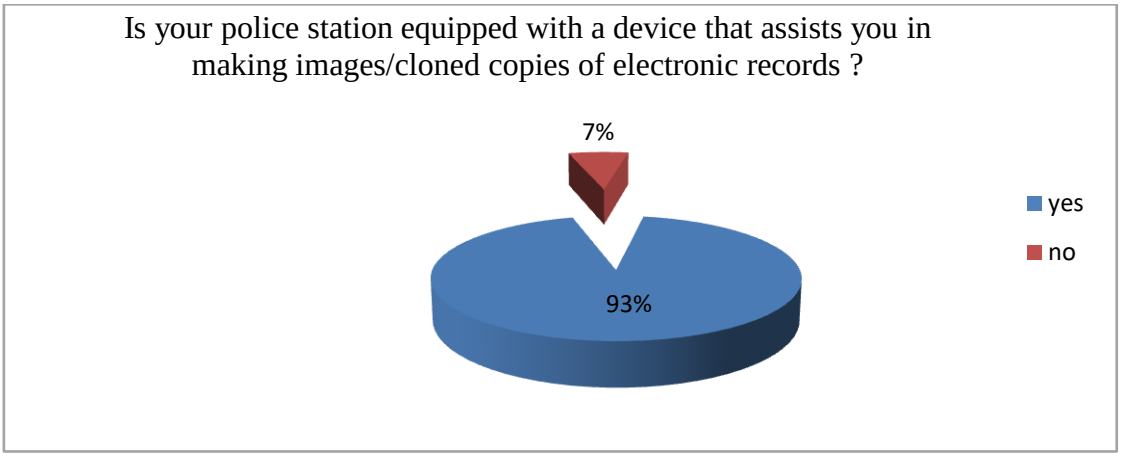



**Figure 5:** *Existence of device for making images or cloned copies*

Table 13 and figure 5 indicates whether police stations are equipped with a device that assists investigating officers in making cloned copies of electronic records. 93% of the respondents have answered in the affirmative and 7% have answered in the negative.

However to get better clarity on this point information was sought from the police department on the point whether they is any such equipment provided at the police station and they have stated that the only police station that has been provided with equipment to prepare images or cloned copies is the cyber crime Police Station.

When the researcher interviewed some senior Investigating officers on this aspect, they were of the view that it is not desirable and necessary that every police station is equipped with write blockers and other forensic tools. This is because firstly such tools are expensive and secondly not every police station will have personnel to use the tools properly. Hence in these circumstances it would be proper that the forensic science laboratories are equipped with proper man power and a networking system such as a mobile van or an Emergency response team that can either visit the site with necessary equipment or can provide quick services of creating an image of the electronic record for investigation or giving of copies to the accused.

Thus in continuity of this thought Police personnel were asked whether there is any emergency computer forensic response team that would assist the Investigating Officer in seizure of electronic record? and they have replied as under:

**Table 14**

*Existence of forensic emergency response team.*

| Response | Number | Percentage |
|---|---|---|
| YES | 21 | 14% |
| NO | 129 | 86% |

*Source: Primary data*

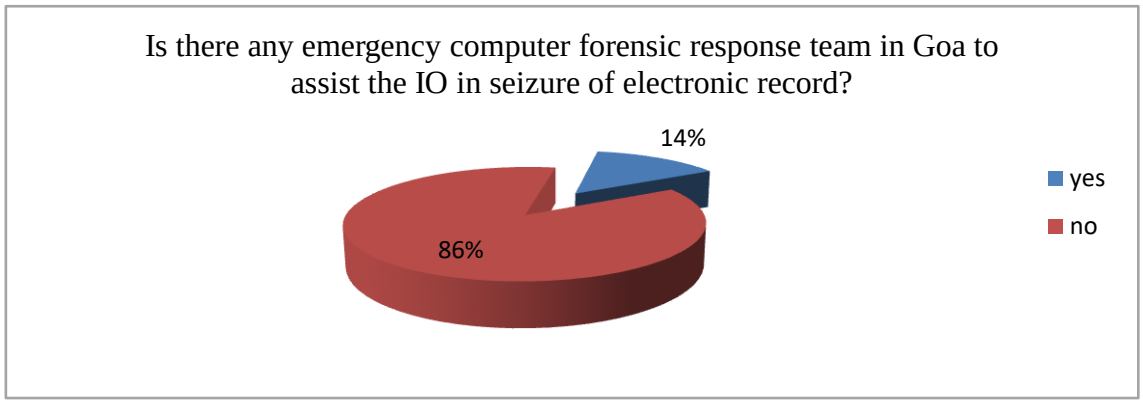



**Figure 6:** *Response on Existence of Cyber Forensic Emergency Response Team*

Table 14 and figure 6 shows that 86% of the respondent police have stated that there is no emergency computer forensic response team in Goa to assist the Investigating Officer in seizure of electronic record. 14 % have answered in the affirmative. In reply to a similar query the Goa State Forensic Science Laboratory Goa, Verna, Goa have responded that there is no emergency response team that would assist the investigating officer on site to seize or copy electronic evidence.

Thus at the first stage of investigation which involves procurement and seizure of electronic records there are significant hurdles in terms of lesser comfort level with electronic evidence of the functionaries, absence of standardised rules, lack of infrastructure, equipment and technical assistance.

With this understanding of the issues at investigation stage, the researcher in the second

part of this chapter has examined the issues that arise at the stage of trial. In the second part of the chapter although the empirical data is predominantly collected from prosecutors, judicial officers and lawyers, nonetheless on certain aspects such as knowledge of procedural law and training which is of common relevance, the data obtained from police respondents is examined alongside.

### 5.3.2 Practical Challenges at Trial Stage.

This part of the thesis looks at only the procedural hurdles in production of electronic evidence in the court. Here the research is not doctrinal in the sense that the researcher will not attempt to examine whether there is any lacuna in the law, the researcher has against the dictum of the existing law examined what are the actual difficulties in compliance of the same.

There are three functionaries who play a combined role in matters relating to production of evidence in courts. They are the lawyers and prosecutors who tender the evidence in electronic form and the judges who decide the issues of admissibility, mode of proof and appreciate that evidence.

On this point the researcher has framed three hypotheses namely, *there is lack of knowledge and sufficient training of all stakeholders in matters relating to electronic evidence and usage of electronic evidence is infrequent as formal nature of proof requisitioned in the court a major discouraging factor. There is lack of infrastructure to process, validate and preserve electronic data in the courts.*

In the foregoing paras the want of proper infrastructure at the procurement stage has been discussed. In this part of the chapter the practical hurdles faced in processing, and validating the electronic records in the courts will be examined.

**A. Knowledge and familiarity of Judicial Officers, Prosecutors and Lawyers with electronic evidence:**

First the researcher has gauged whether the three stakeholders who are responsible for processing the electronic evidence in court find electronic evidence different and new

and thus are fairly less comfortable with this form of evidence. In a rating scale all the three stake holders were asked to rate their knowledge of electronic evidence vis a vis other forms of evidence.

From amongst the stakeholders, judicial officers were asked to rate on the scale of 1 to 10 their familiarity with electronic evidence where 1 stands for lowest and 10 stands for the highest.Their response has been as under:

**Table 15**

*Rating Scale Showing Familiarity of the Judicial Officers with Electronic Evidence*

| Scale | Response |
|---|---|
| 1 | 0 |
| 2 | 1 |
| 3 | 0 |
| 4 | 1 |
| 5 | 13 |
| 6 | 14 |
| 7 | 10 |
| 8 | 06 |
| 9 | 04 |
| 10 | 01 |

*Source: Primary data*

*NOTE: Rank 1 stands for lowest and rank 10 stands for highest.*

Further on the scale of 1 to 10 the judicial officers were asked to rate their familiarity with subject of evidence other then electronic evidence, Where 1 stands for low and 10 for high. Their response has been as under:

**Table 1**6

*Rating Scale Showing Familiarity Of The Judicial Officers with Evidence other then Electronic Evidence*

| Scale | Response |
|---|---|
| 1 | 0 |
| 2 | 0 |
| 3 | 1 |
| 4 | 0 |
| 5 | 2 |
| 6 | 8 |
| 7 | 12 |
| 8 | 15 |
| 9 | 08 |
| 10 | 04 |

*Source: Primary data*

*NOTE: Rank 1 stands for lowest and rank 10 stands for highest.*

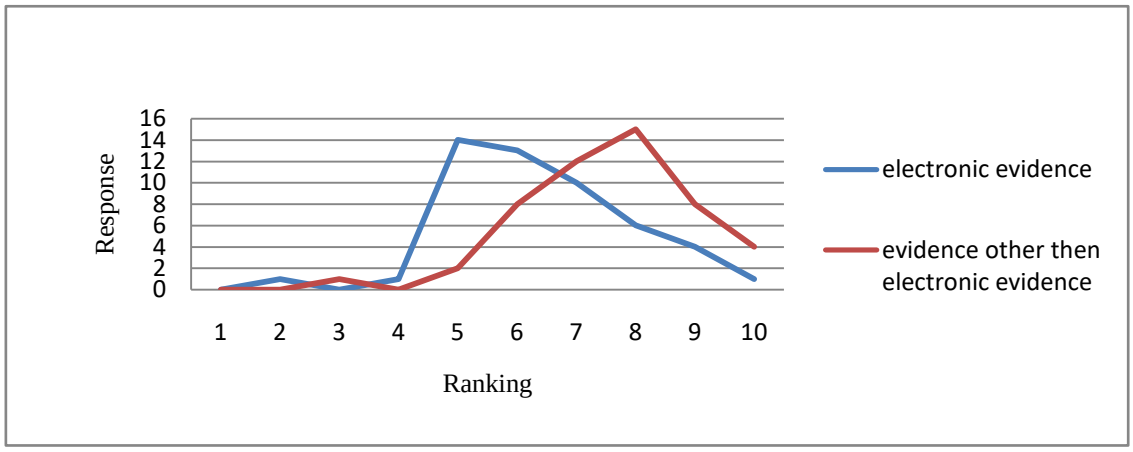



**Figure 7***: Trends in familiarity of judicial officers on the subject of electronic evidence vis a vis evidence other then electronic evidence.*

Upon analysis of the table15,16 and the figure 7 it is seen that in the category of electronic evidence, the highest ranking of 6 was given by as many as 14 respondents from a total 50. Whereas for other regular forms of evidence, the highest ranking of 8 was given by 15 respondents. This therefore goes to show that judicial officers are more familiar with regular form of evidence then electronic evidence. Consequently there is greater comfort level in handling and seizure of this form of electronic evidence then the conventional form.

Next from amongst the stakeholders, Prosecutors were asked to rate on the scale of 1 to 10 their familiarity with electronic evidence where 1 stands for lowest and 10 stands for the highest.Their response has been as under:

**Table 17**

*Rating Scale Showing Familiarity Of The Prosecutors With Electronic Evidence*

| Scale | Response |
|---|---|
| 1 | 0 |
| 2 | 0 |
| 3 | 0 |
| 4 | 0 |
| 5 | 11 |
| 6 | 12 |
| 7 | 13 |
| 8 | 11 |
| 9 | 1 |
| 10 | 2 |

*Source: Primary data*

*NOTE: Rank 1 stands for lowest and rank 10 stands for highest.*

Next on the scale of 1 to 10 the Prosecutors were asked to rate their familiarity with subject of evidence other then electronic evidence, Where 1 stands for low and 10 for high. Their response has been as under:

**Table 18**

*Rating Scale Showing Familiarity Of The Prosecutors with Evidence other then Electronic Evidence*

| Scale | Response |
|---|---|
| 1 | 0 |
| 2 | 0 |
| 3 | 0 |
| 4 | 0 |
| 5 | 3 |
| 6 | 5 |
| 7 | 11 |
| 8 | 13 |
| 9 | 15 |
| 10 | 3 |

*Source: Primary data*

*NOTE: Rank 1 stands for lowest and rank 10 stands for highest.*

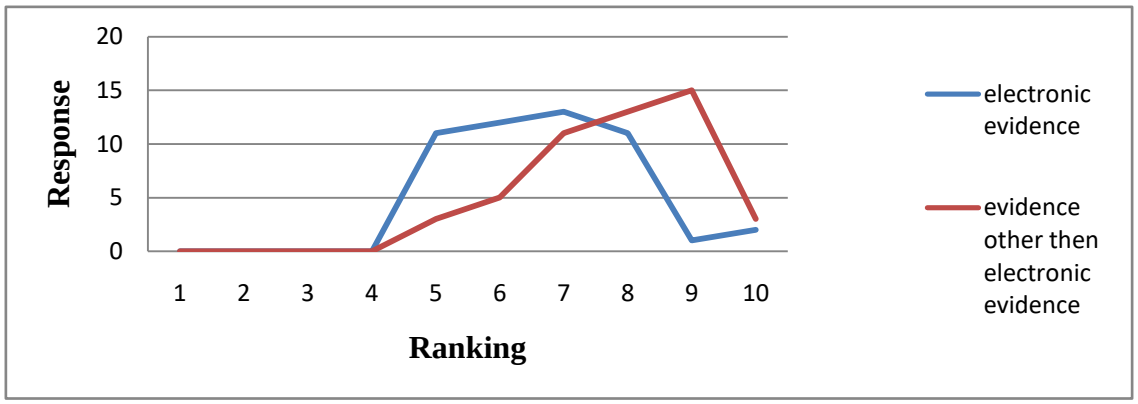



**Figure 8** : *Trends in familiarity of Prosecutors on the subject of electronic evidence vis a vis evidence other then electronic evidence*

Upon analysis the table No. 17, 18 and the Figure No. 8 it is seen that in the category of electronic evidence the highest ranking was given as 7 by as many as 13 respondents from a total 50. Whereas for other regular form of evidence the highest ranking of 9 was given by 15 respondents. The chart clearly shows the gap between higher ranks for both forms of evidence. This therefore goes to show that prosecutors are more familiar with

regular form of evidence in contrast with electronic evidence. Consequently there is greater comfort level in handling conventional form of evidence in courts rather then electronic evidence.

Thereafter from amongst the stakeholders, lawyers were asked to rate on the scale of 1 to 10 their familiarity with electronic evidence where 1 stands for lowest and 10 stands for the highest.Their response has been as under:

**Table 19**

*Rating Scale Showing Familiarity Of Lawyers With Electronic Evidence*

| Scale | Response |
|---|---|
| 1 | 3 |
| 2 | 1 |
| 3 | 2 |
| 4 | 8 |
| 5 | 31 |
| 6 | 36 |
| 7 | 23 |
| 8 | 25 |
| 9 | 11 |
| 10 | 10 |

*Source: Primary data*

*NOTE: Rank 1 stands for lowest and rank 10 stands for highest.*

Further on the scale of 1 to 10 rate lawyers were asked to rate their familiarity with subject of evidence other then electronic evidence, Where 1 stands for low and 10 for high. Their response has been as under:

**Table 20**

*Rating Scale Showing Familiarity of Lawyers with Evidence other then Electronic Evidence*

| Scale | Response |
|---|---|
| 1 | 0 |
| 2 | 0 |
| 3 | 0 |
| 4 | 3 |
| 5 | 8 |
| 6 | 14 |
| 7 | 29 |
| 8 | 47 |
| 9 | 32 |
| 10 | 17 |

*Source: Primary data*

*NOTE: Rank 1 stands for lowest and rank 10 stands for highest*

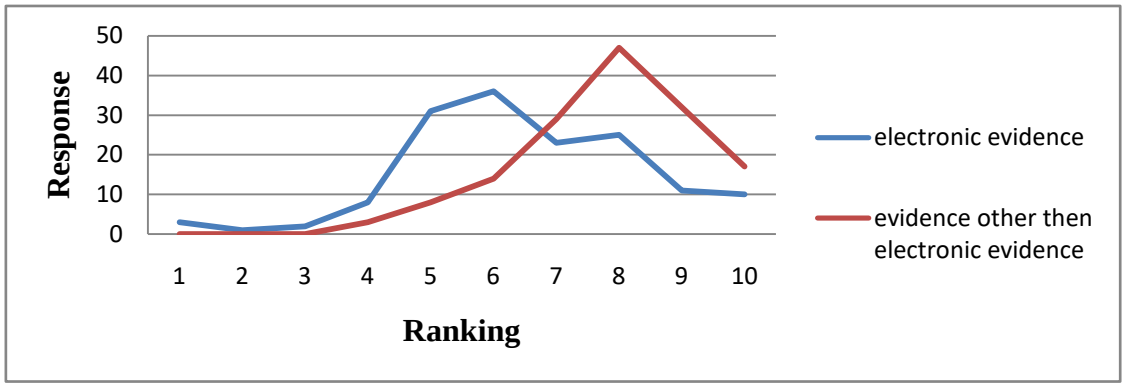



**Figure 9** *Trends in familiarity of lawyers on the subject of electronic evidence vis a vis evidence other then electronic evidence.*

Upon analysis the table No19, 20 and figure No. 9, it is seen that in the category of electronic evidence the highest ranking was given as 6 by as many as 36 respondents from a total 150. Whereas for other regular form of evidence, the highest ranking of 8 was given by 47 respondents. This therefore goes to show that Lawyers are more familiar with regular form of evidence then electronic evidence. Consequently there is greater comfort level in tendering and proving conventional form of evidence in court rather than electronic evidence.

The researcher has conducted a comparative study of the responses given by all three stakeholders by taking a contrast of the highest ranking given by them in each of the categories. This comparative study has assisted the researcher in determining whether there is any gap between the familiarity with electronic evidence and other form of electronic evidence interse between all stakeholders and what is the extent of this gap. For this comparison Police as a category of stakeholders has also been added by considering the data enlisted above. The comparison of responses is made in a tabular form as under:

**Table 21**

*Comparison of Highest Ranking given by the stakeholders*

| Sr. No. | Stakeholder | Highest rank for familiarity with Electronic Evidence | Highest rank for familiarity with evidence other then Electronic Evidence |
|---|---|---|---|
| 1 | Lawyers | 6 | 8 |
| 2 | Prosecutors | 7 | 9 |
| 3 | Judicial Officers | 6 | 8 |
| 4 | Police | 7 | 8 |

*Source: Primary data*

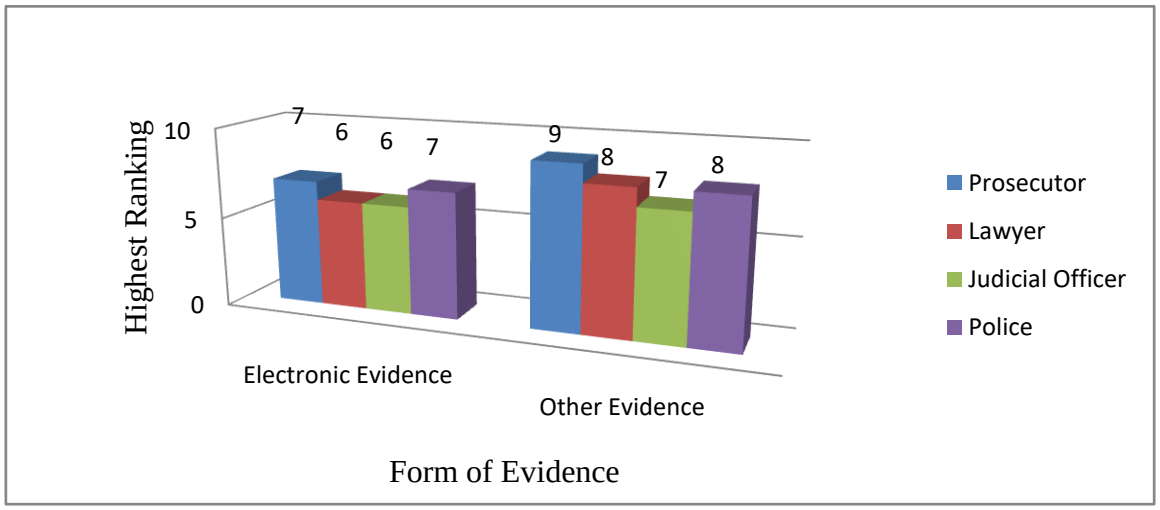



**Figure 10:** *Comparison of Highest Ranking given by the stakeholders*

If a comparison is done of the cumulative data as indicated in table 21 and figure 10 obtained from judicial officers, prosecutors, lawyers and Police it is seen that amongst the judicial officers the knowledge of electronic evidence was ranked to the highest point of 6. Whereas knowledge of evidence other then electronic evidence was ranked at the highest rank of 8. Amongst the prosecutors the knowledge of electronic evidence was ranked to the highest point of 7 whereas knowledge of evidence other then electronic evidence was ranked 9. Amongst the Lawyers the knowledge of electronic evidence was ranked to the highest point of 6. Whereas knowledge of evidence other then electronic evidence was ranked 8.

The analysis of the response of all the three stake holders on the familiarity with the law indicates that all the three stake holders have a lesser comfort level with the subject of electronic evidence as compared to the traditional form of evidence, as a result the law that pertains to electronic evidence needs to be examined assessed and implemented in a improvised manner ensuring that all the stake holders achieve the same comfort level to this form of evidence as compared to the conventional form.

It is seen that prosecutors have a better familiarity with electronic evidence as compared to lawyers and judges. The researcher is of the humble view that this may be because the exposure of prosecutors to different forms of electronic record is greater as they get myriad opportunities to produce the same in variety of cases. Also at the first

instance it is the person producing evidence who has to determine its relevancy. As a result the scrutiny and the study of this subject is greater for a person who produces it then the person who merely assesses its fitness to prove a fact.

The figure also reflects that the trend is more or less same amongst all the stakeholders and there is no serious gap or disparity.

**B. Caseload of cases involving Electronic Evidence in Courts.**

In order to ascertain the exposure of the stakeholders to the subject of electronic evidence it is necessary to find out the share of cases involving electronic evidence amongst the total number of cases. The researcher therefore asked all the three stakeholders as to how often they have handled cases containing some form of electronic evidence? Their response has been as under:

**Table 22**

*Comparative case load of Electronic Evidence with Prosecutors*

| Sr No. | Percentage | Response | Percentage |
|---|---|---|---|
| 1 | Less then 20% of the total number of cases | 29 | 58% |
| 2 | About 50% of the total number of cases | 18 | 36% |
| 3 | More than 50% of the total number of cases. | 3 | 6% |
| 4 | Never | 0 | 0% |

*Source: Primary data*

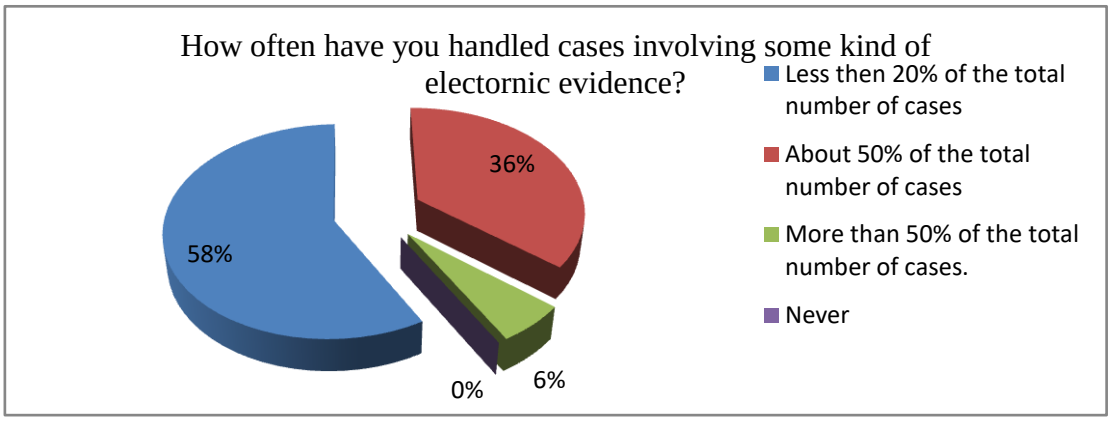



**Figure 11:** *Comparative case load of Electronic Evidence with Prosecutors*

Table 22 and figure 11 indicates the response of prosecutors about the caseload of cases involving electronic evidence. The researcher had given options of four distinct categories to choose from indicating the percentage of cases involving electronic evidence. 58 percent of the prosecutors have chosen the first category of electronic evidence constituting less then 20% of the case load. 36 percent of prosecutors have chosen the second category of cases being about 50%. 6% of prosecutors have chosen the third category of cases being more then 50%. There is no one from amongst the prosecutors who have never handled any case involving electronic evidence.

Next a similar question was put to the lawyers and they too were given the same options. Their response is as under:

**Table 23**

*Comparative case load of Electronic Evidence :Lawyers*

| Sr No. | Percentage | Response | Percentage |
|---|---|---|---|
| 1 | Less then 20% of the total number of cases | 91 | 61% |
| 2 | About 50% of the total number of cases | 35 | 23% |
| 3 | More than 50% of the total number of cases. | 24 | 16% |
| 4 | Never | 0 | 0 |

*Source: Primary data*

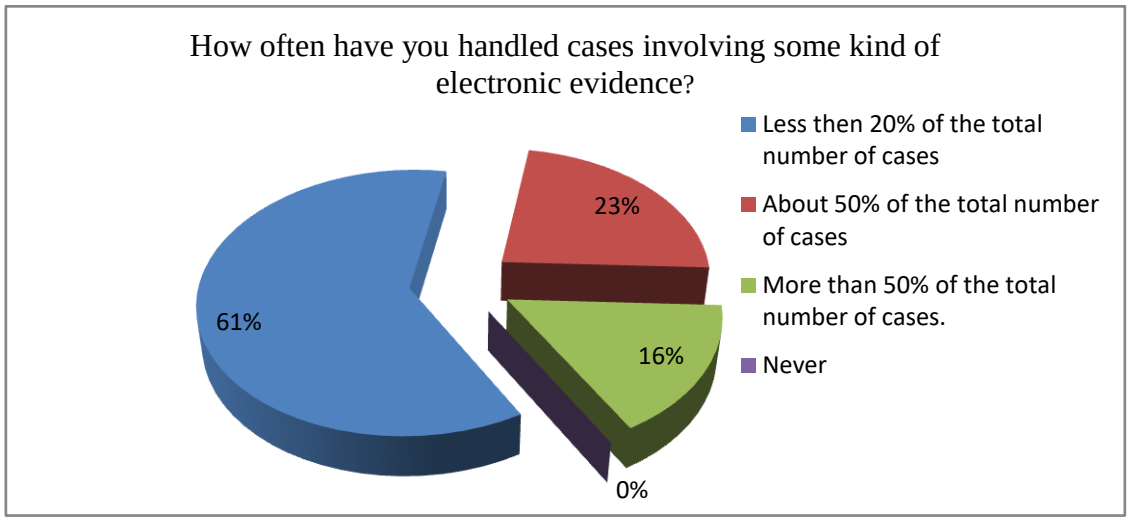



**Figure 12:** *Comparative case load of Electronic Evidence :Lawyers*

Table 23 and figure 12 indicates the response of lawyers. The researcher had given options of four distinct categories to choose from indicating the percentage of cases involving electronic evidence. 61% of lawyers have chosen the first category of electronic evidence constituting less then 20% of the case load. 23% of lawyers have chosen the second category of cases being about 50%. 16% of lawyers have chosen the third category of cases being more then 50%. There is no one from amongst the lawyers who have never handled any case involving electronic evidence.

Lastly, Judicial officers were asked the same question and were given the same four options. Their response is as under:

**Table 24**

*Comparative case load of Electronic Evidence: Judicial Officers*

| Sr No. | Percentage | Response | Percentage |
|---|---|---|---|
| 1 | Less then 20% of the total number of cases | 27 | 54 |
| 2 | About 50% of the total number of cases | 19 | 38 |
| 3 | More than 50% of the total number of cases. | 4 | 8 |
| 4 | Never | 0 | 0 |

*Source: Primary data*

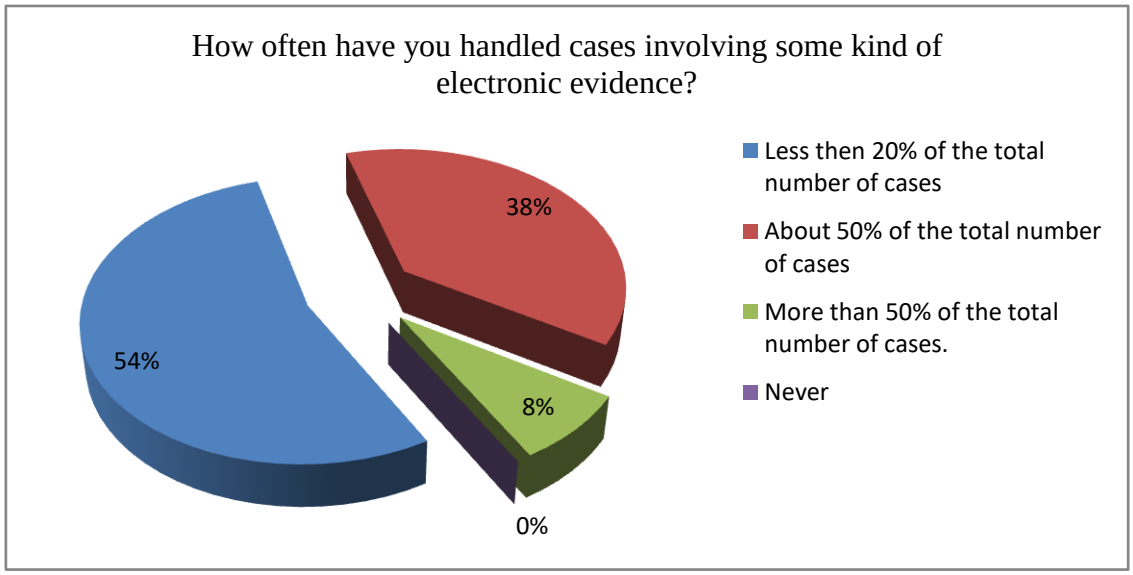



**Figure 13:** *Comparative case load of Electronic Evidence: Judicial Officers*

Table 24 and figure13 indicates the response of judicial Officers. The researcher had given options of four distinct categories to choose from indicating the percentage of cases involving electronic evidence. 54% of judicial officers have chosen the first category of electronic evidence constituting less then 20% of the case load. 38 percent of judicial Officers have chosen the second category of cases being about 50%. 8 percent of judicial officers have chosen the third category of cases being more then 50%. There is no one from amongst the judicial officers who have never handled any case involving electronic evidence.

Next the researcher has compared the responses of all the three stakeholders. This comparison was imperative because in the hypothesis framed it had to be ascertained whether there is frugal use of electronic evidence in courts. Hence this data has to be examined in contrast with the position of case load of cases involving electronic evidence before the Police at the stage of Investigation.

**Table 25**

*Comparison of response of all three stake holders*

| Scale | Response in Percentage | | | |
|---|---|---|---|---|
| | PROSECUTORS | LAWYERS | JUDGES | AVERAGE |
| Less then 20% of the total number of cases | 58 | 61 | 54 | 57.6 |
| About 50% of the total number of cases | 36 | 23 | 38 | 32.3 |
| More than 50% of the total number of cases | 6 | 16 | 8 | 10 |
| Never | 0 | 0 | 0 | 0 |

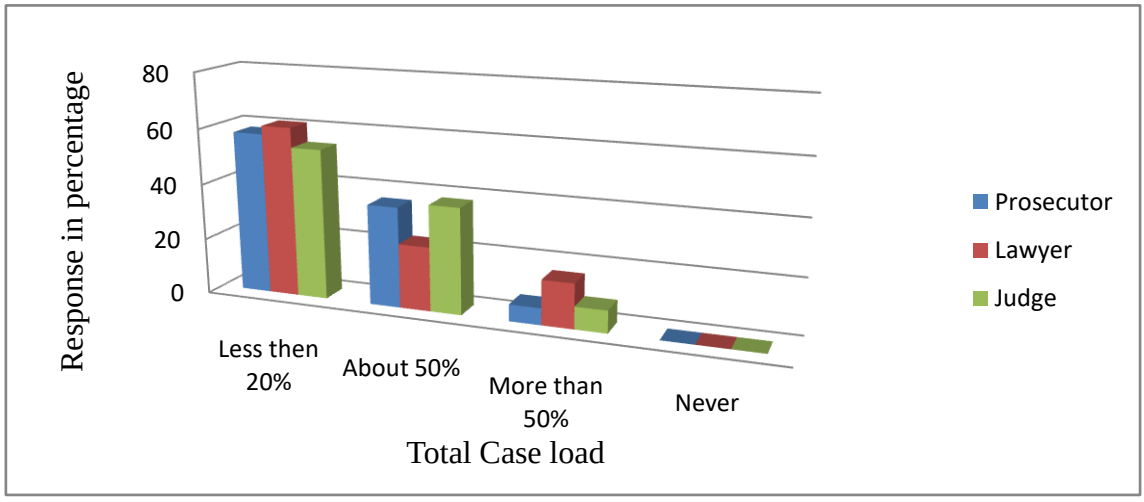



*Figure 14 Comparative case load of electronic evidence in Court*

Table 25 and figure 14 shows the trend in the case load of cases involving electronic evidence. It indicates that majority of the stakeholders from amongst the Judicial

officers, Prosecutors and Lawyers find that there are less then 20% of cases before them for trial that have some kind of electronic evidence involved in it.

**C. Compliance Of Section 65B**

As noted in the foregoing chapters that law exempts production of the original electronic record if a copy thereof has been prepared by resorting to section 65B of the Indian Evidence Act and a certificate to that effect is annexed to the copy. Despite this simple requirement of law, upon interviewing the stake holders the researcher found that there were cases that failed due to non production of certificate or production of a defective certificate under section 65B of the Indian Evidence Act. When prosecutors and lawyers were randomly interviewed they were of the view that parties and IO's must refrain from production of original electronic record as it may not be possible to access the same at the time when the matter finally is posted for trial.

The unanimous view is that depending upon the nature of the electronic record, a physical copy printed on paper is the best alternative because in future if it is shown that the original record is destroyed due to passage of time, a copy that is properly prepared by resorting to section 65B will suffice in admitting the electronic record. Secondly, there is no mechanism to properly preserve electronic records in court therefore a copy either as backup or otherwise is most desirable.

Thus resort to section 65B plays a crucial role in determining the extent to which electronic records will be conveniently relied upon by the courts to prove a fact. The respondents were asked certain questions about certificate under section 65B of the Indian Evidence Act. Police respondents are persons who have no formal training in law in contrast with the other three stakeholders. Thus the researcher did a preliminary exercise of broadly finding out the extent of knowledge police officers have about section 65B. Police respondents were asked whether they are aware of section 65B, of the Indian Evidence Act and their response has been as under:

**Table26**

*Knowledge of Police about section 65B.*

| Response | Number | Percentage |
|---|---|---|
| YES | 131 | 87% |
| No | 19 | 13% |

*Source: Primary data*

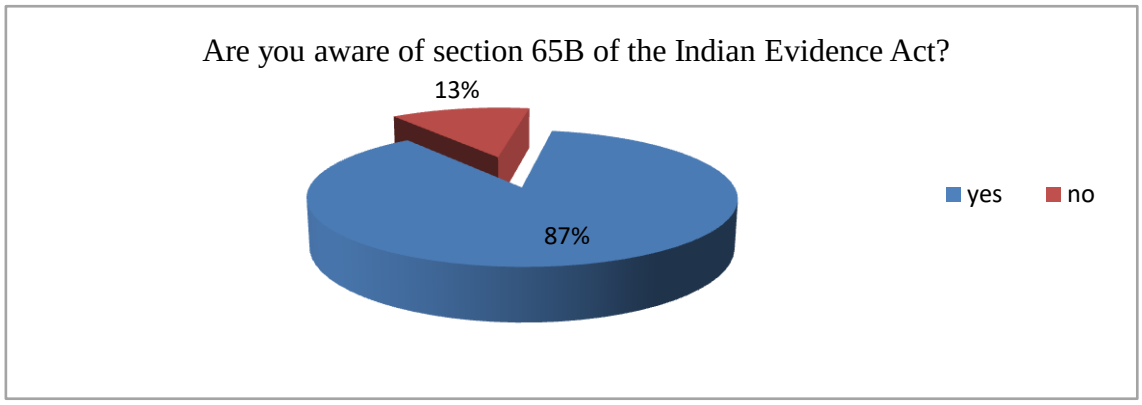



**Figure 15:** *Knowledge of Police about section 65B*

Table 26 and figure 15 shows that 87% of the Police respondents are aware of section 65B of the Indian Evidence Act, whereas 13% are not aware of the same.

In the light of these answers the researcher examined the procedure followed by the other stakeholders in producing and admitting copy of electronic record. First and foremost judicial officers were asked whether they have admitted electronic evidence without the witness producing certificate under section 65 B of the Indian Evidence Act. They were given four options to choose from namely, “yes always” “yes when the other side has not objected” “yes in cases before the judgement of Anwar Bhasir was passed’ “no never”. Their response is recorded as under:

**Table 27**

*Admission of copy of electronic evidence without certificate under section 65 B of the Indian Evidence Act by Judicial Officers*

| Category | response | Percentage | Remarks |
|---|---|---|---|
| yes, always | 1 | 2% | |
| yes when the other side has not objected | 10 | 20% | |
| yes in cases before the judgement of Anwar Bhasir was passed | 7 | 14% | After the Judgement of Anwar Bhasir it was clarified that section 65B certificate is mandatory. |
| no never | 32 | 64% | |

*Source: Primary data*

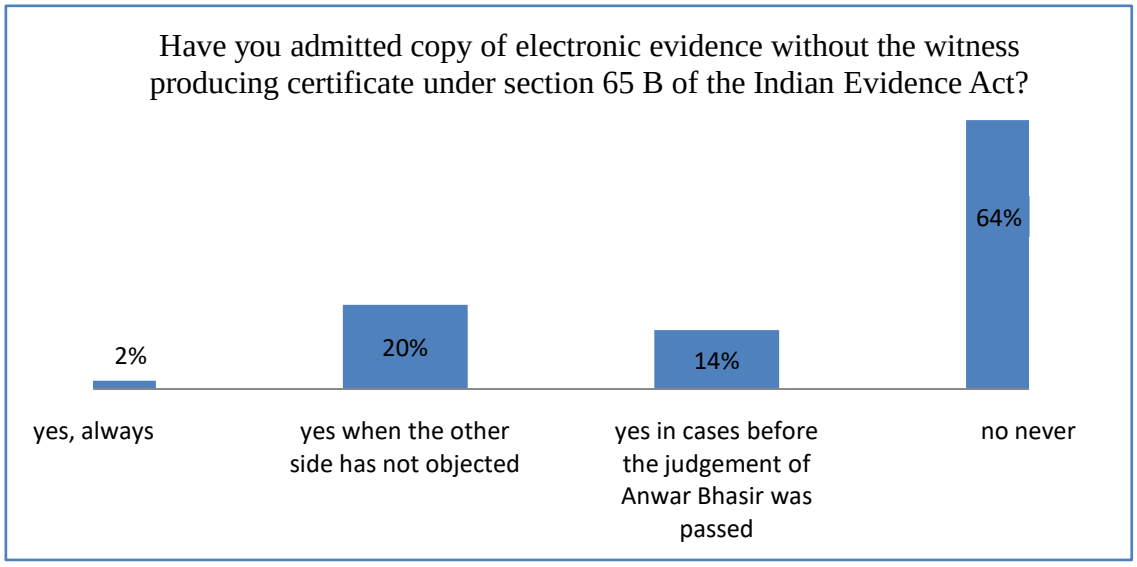



***Figure 16:*** *Bar chart on admission Of copy of electronic evidence without Certificate under section 65 B of the Indian Evidence Act*

Table 27 and figure 16 shows that 64% of the of judicial officers have never admitted copy of electronic record without certificate under section 65B. 20% have stated that they have admitted copy of electronic evidence without certificate under section 65B, when the other side has not objected. 14% have admitted copy of electronic evidence without certificate under section 65B, before the passing of the judgement in the case of Anwar Bashir (supra) and one of the judge has always admitted copies of electronic record without a certificate under section 65B.

Lawyers and prosecutors could not be asked the same question. As they are the persons who produce electronic evidence and are not enjoined with the responsibility of admitting the same. The researcher has also undertaken the exercise of ascertaining from them their knowledge about the importance of section 65B of the Indian Evidence Act.

The question therefore was slightly customised to as to find out whether these stakeholders have produced electronic evidence without the witness producing certificate under section 65 B? They were given two options namely "yes" or "no". The staekholders who answered in the affirmative were asked to state the circumstances under which the electronic record was produced without producing a certificate under section 65B. The response was as under:

**Table 28**

*Admission of copy of electronic evidence without certificate under section 65 B by Lawyers*

| Response | Number | Percentage |
|---|---|---|
| YES | 22 | 15% |
| No | 128 | 85% |

*Source: Primary data*

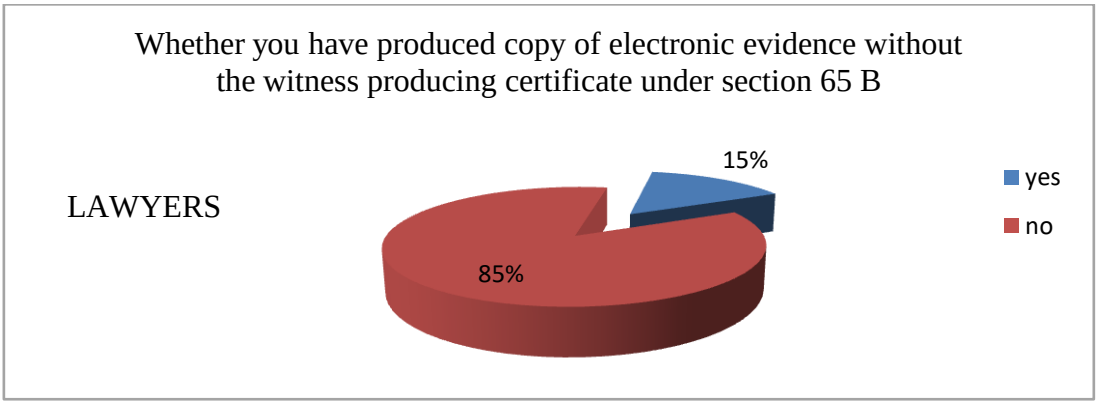



**Figure 17:** *Pie chart on admission of copy of electronic evidence without Certificate under section 65 B of the Indian Evidence Act.*

As per table 28 and figure 17, 85% of lawyers have never produced copy of electronic record without certificate under section 65B. 15% have stated that they have produced copy of electronic record without certificate under section 65B. Thus majority realise the significance of certificate under section 65B. As regards the circumstances under which the electronic records were produced without certificate under section 65B, some respondents have stated that it was produced when not objected by other side or that when the certificate was not available.

The next category of stakeholder is the prosecutors. They too were asked the same question with similar options. Their response is as under:

**Table 29**

*Admission of copy of electronic evidence without certificate under section 65 B of the Indian Evidence Act by Prosecutors*

| Response | Number | Percentage |
|---|---|---|
| YES | 14 | 28% |
| No | 36 | 72% |

*Source: Primary data*

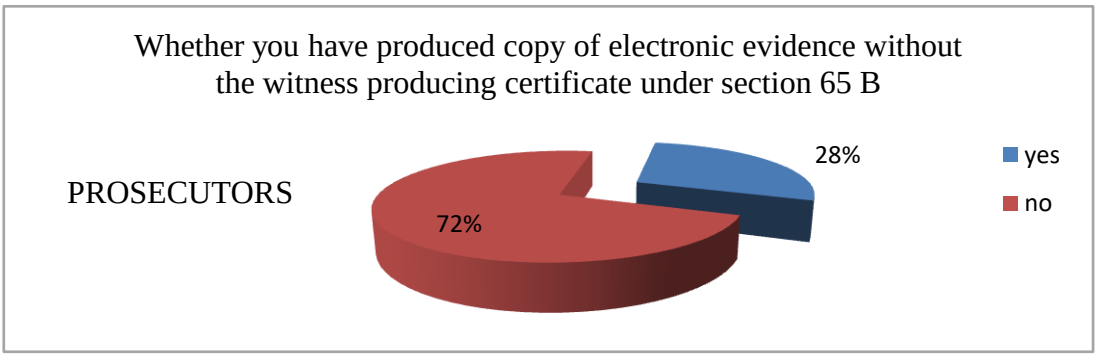



**Figure 18:** *Admission of copy of electronic evidence without certificate under section 65 B by Prosecutors.*

Table 29 and figure 18 shows that 72% of prosecutors have never produced copy of electronic record without certificate under section 65B. 28% have stated that they have produced copy of electronic record without certificate under section 65B.

As regards the circumstances under which the electronic records were produced without certificate under section 65B some prosecutors have stated that it was produced when not objected by other side or that when the certificate was lost or when the certificate was not relied upon by the IO in the charge sheet. The percentage of responses as above therefore indicates that majority of the prosecutors have always produced electronic evidence along with certificate under section 65B.

Next the researcher has compared the responses of both stakeholders:

**Table 30**

*Comparison of response of two stake holders*

| Scale | Response in Percentage | | |
|---|---|---|---|
| | PROSECUTORS | LAWYERS | AVERAGE |
| YES | 28 | 15 | 21.5 |
| NO | 72 | 85 | 78.5 |

*Source: Primary data*

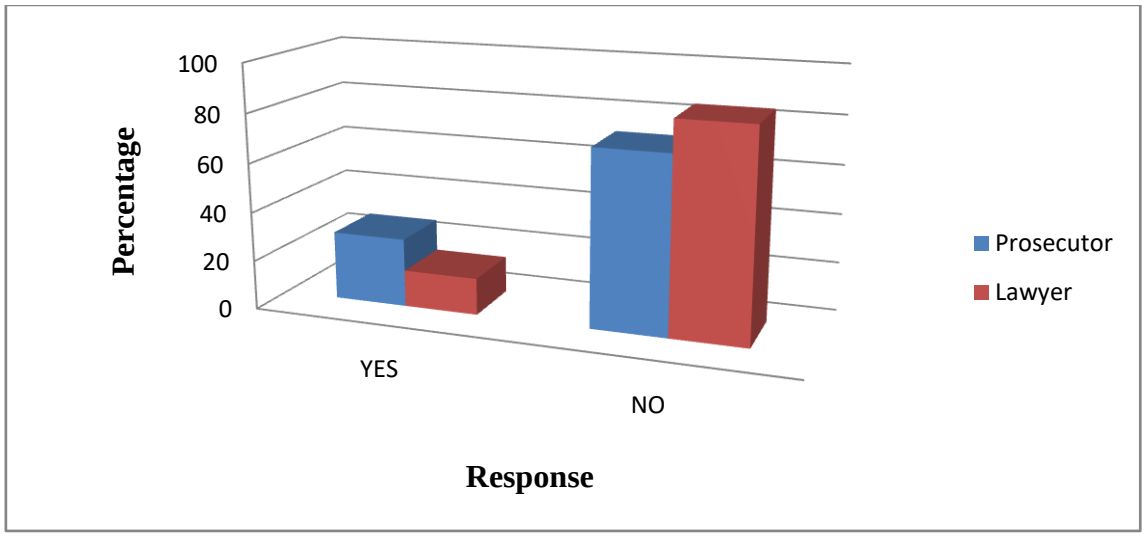



**Figure 19**: *Comparison of response of two stake holders on production of copy of electronic record without certificate under section 65B.*

Analysis of Table 30 and figure 19 indicates that majority of the stakeholders from amongst lawyers and prosecutors have not produced copy of electronic evidence without certificate under section 65 B of the Indian Evidence Act. Although the norm is that no copy of electronic record is admitted without certificate under section 65 B however, exceptions that are followed by the stakeholders are when a party against whom record is produced does not object to the same. The other circumstance that is mostly cited is non availability of certificate under section 65B. The researcher shall refrain from commenting upon the correctness of this practice as that aspect shall be considered at the time when the hypothesis is analysed.

The striking aspect of the responses given to this question is that most number of stake holders are aware that in order to make copy of electronic record admissible in evidence it is imperative to produce certificate under section 65B.

A pertinent question in this regard may arise as to whether a copy of an electronic record can be produced without certificate under section 65B if the other side does not object. The Judgement in the case of ***Anwar(supra)*** has shed some light on this by

referring to certain provisions of the Indian Evidence Act and the Information Technology Act. The court noted that as per section 22A[285] of the Indian Evidence Act Oral admissions of contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question. In other words a party can be absolved from proving the contents of an electronic record if the opponent orally admits the genuineness of same. Therefore there is no need to resort to any other proof or even section 45A in such a case.

The court also considered Section 59 under Part II of the Evidence Act and read it along with section 65B and held that there is no scope to admit a copy of electronic record without following section 65A and 65B. These provisions began with a non obstante clause and are not governed or guided by any other proving of the Indian Evidence Act[286]. Therefore if a copy of an electronic record is not properly admitted, the next step of proof does not arise. Admission therefore can at the most be of genuineness and not of the mode of proof.

**D. Use Of Expert Assistance:**

Section 65B of the Indian Evidence Act only relates to admissibility of evidence. In the sense that if the original electronic record is produced for perusal of the court there is no need to produce a certificate under section 65B. However if the authenticity of the

---

[285] Section 22A of the Evidence Act reads as follows:"22A. When oral admission as to contents of electronic records are relevant.-Oral admissions as to the contents of electronic records are not relevant, unless the genuineness of the electronic record produced is in question."

[286] In that case it was held that "*14. Any documentary evidence by way of an electronic record under the Evidence Act, in view of Sections 59 and 65A, can be proved only in accordance with the procedure prescribed under Section 65B. Section 65B deals with the admissibility of the electronic record. The purpose of these provisions is to sanctify secondary evidence in electronic form, generated by a computer. It may be noted that the Section starts with a non obstante clause. Thus, notwithstanding anything contained in the Evidence Act, any information contained in an electronic record which is printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be deemed to be a document only if the conditions mentioned under sub- Section (2) are satisfied, without further proof or production of the original. The very admissibility of such a document, i.e., electronic record which is called as computer output, depends on the satisfaction of the four conditions under Section 65B(2). 17. Only if the electronic record is duly produced in terms of Section 65B of the Evidence Act, the question would arise as to the genuineness thereof and in that situation, resort can be made to Section 45A - opinion of examiner of electronic evidence.18. The Evidence Act does not contemplate or permit the proof of an electronic record by oral evidence if requirements under Section 65B of the Evidence Act are not complied with, as the law now stands in India.*"

record is disputed an expert in terms of section 45A of the Indian Evidence Act will have to be examined. The question as to who has to examine the expert will depend upon whom the burden of proof lies in terms of section 101[287] and section 102[288] of the Indian Evidence Act. In this part of the chapter the researcher has examined the prevalance of the use of section 45A of the Indian Evidence Act.

The term expert is not defined under the Indian Evidence Act in the definitions clause . However it occurs in the heading of section 45 of the Indian Evidence Act " opinion of experts". Section 45[289] enumerates who are experts in the context of the Act and makes their opinion relevant 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, foreign law, science or art. **In *State of Himachal Pradesh v. Jai Lal and Ors***[290]it was held by the Hon'ble Supreme Court, that before relying upon the evidence of an expert the court has to be satisfied about his expertise. It was further held that evidence is only corroborative.

Section 45A[291] of the Indian Evidence Act makes Opinion of Examiner of Electronic Evidence relevant for a court that has to form an opinion on "any matter relating to any information transmitted or stored in any computer resource or any other electronic or

[287] Section 101 reads thus Whoever desires any Court to give judgment as to any legal right or liability dependent on the existence of facts which he asserts, must prove that those facts exist. When a person is bound to prove the existence of any fact, it is said that the burden of proof lies on that person.

[288] Section102 reads thus The burden of proof in a suit or proceeding lies on that person who would fail if no evidence at all were given on either side.

[289] Section 45 of Indian Evidence Act reads as under:. 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.

[290] (1999) 7 SCC 280.In this case it was held that "*An expert is not a witness of fact. His evidence is really of an advisory character. The duty of an expert witness is to furnish the Judge with the necessary scientific criteria for testing the accuracy of the conclusions so as to enable the judge to form his independent judgment by the application of this criteria to the facts proved by the evidence of the case. The scientific opinion evidence, if intelligible, convincing and tested becomes a factor and often an important factor for consideration along with the other evidence of the case. The credibility of such a witness depends on the reasons stated in support of his conclusions and the data and materials furnished which form the basis of his conclusions".*

[291] Section 45A of Indian Evidence Act provides that 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. Explanation .—For the purposes of this section, an Examiner of Electronic Evidence shall be an expert;

digital form". However the expert has to be a person who is empanelled under section 79A of the Information Technology Act.

Section 79A of the Information Technology Act, 2000 requires the Central Government to 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[292]. For that purpose the Government has enacted a detailed scheme called "the Scheme for Notifying Examiner of Electronic Evidence Under section 79A of the Information Technology Act 2000"[293].

A detailed scheme document is provided and all the eligible people can apply for the same through filling the form and after the selection and notifying process, an expert will be provided to the court. As per the scope of the scheme any Department, body or agency of the Central Government or a State Government can apply as per annexure given in the scheme to be notified as expert under section 79A of the Information Technology Act[294].

The applicant has to file an application form which is published on Ministry of Electronics and Information Technology, Government of India website along with annexures listed. The application thereafter is processed in three stages. After successfully completing these three stages the laboratory would be notified as

[292] 79A of the Information Technology Act: 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 purposes 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.]

[293] https://www.meity.gov.in/writereaddata/files/annexure-i-pilot-scheme-for-notifying-examiner-of-electronic-evidence-under-section-79a-of-the-information-technology-act-2000.pdf on 15.12.2022 at 6.00 pm.

[294] The scope of approval will be one or more of disciplines/ areas of activity in the applicant Forensic Science Laboratories: 1. Computer (Media) Forensics 2. Network (Cyber) Forensics 3. Mobile Devices Forensics 4. Digital Video / Image & CCTV Forensics 5. Digital Audio Forensics 6. Device Specific Forensics 7. Digital Equipment / Machines (having embedded firmware) 8. Any other Accreditation in additional disciplines may be offered in future as per requirement as per para 2 of the Scheme. The Lab has to follow general requirements for the competence of testing and calibration laboratories as per ISO/ IEC 17025:2005. It is also expected that the Lab follows the best practices as stated in ISO/IEC 27037:2012: Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence or any other National / International Standard (s) as per para 3 of the scheme

"Examiner of Electronic Evidence". Such a notification will continue to remain until the same is suspended or withdrawn.

**E. Evidentiary value of expert opinion under section 45A.**

It is a settled principle of law that the opinion of an expert is advisory in character, in the sense that a court is not bound by this opinion. However it does have a persuasive value and in the absence of proof to the contrary generally expert opinion can be relied upon in proof of a fact. It is however clarified that an expert opinion cannot be sole basis of a decision. It would be unsafe to convict someone merely on the basis of an expert opinion[295].

In ***Anvar P.V.***[296] has held that only if an electronic record is admitted in terms of section 65B of the Indian Evidence Act a question would arise of examining it in terms of section 45A of the Indian Evidence Act.

In ***Sanjaysingh Ramrao Chavan***[297]it was held that source and authenticity are the two important factors to prove electronic evidence. In this case the court held to prove the allegation of demand the prosecution had relied upon a conversation recorded on a voice recorder. The Forensic Science Laboratories, Maharashtra reported that the conversation was not in audible condition and thus the same was not considered for spectrographic analysis.. As the voice recorder was not subjected to analysis, the court could not have relied upon the translated version. As the authenticity of translated version was in doubt, the accused could not be convicted on the strength of the electronic record.

Whether the precedent in respect of opinion of experts generally could be applicable to opinion of experts in respect of electronic records is a point to ponder upon. Electronic records are not comparable to conventional documents particularly when a copy thereof

[295] In Murari Lal v. State of Madhya Pradesh, (1980) 1 SCC 704 it was held that "The more developed and the more perfect a science, the less the chance of an incorrect opinion and the converse if the science is less developed and imperfect. The science of identification of finger-prints has attained near perfection and the risk of an incorrect opinion is practically non-existent. On the other hand, the science of identification of handwriting is not nearly so perfect and the risk is, therefore, higher."

[296]Anvar P.V. vs P.K.Basheer (2014) 10 SCC 473

[297] Sanjaysingh Ramrao Chavan Vs. dattatray Gulabrao Phalke and Others, reported in 2015(3) SCC, 123

is produced as they can be easily tempered and the tempering cannot be detected by normal examination. This is because in substance of electronic records does not lie in what is seen with the naked eye but in its electronic form. However as the document exists in electronic form, tampering of that record can also be easily detected and proved with complete certainty. That is why computer forensic experts believe that electronic records are much safer then paper. It is often said that papers are vulnerable in myriad ways firstly, inappropriate access to papers cannot be easily averted secondly, data tampering like erasures or removal of pages cannot be easily detected and thirdly upon loss of a document it may not be possible to retrieve it.

This being the case it may be safer to consider a fact proved through an electronic record if the same is authenticated by a expert under section 45A of the Indian Evidence Act.

Thus in the light of this position of law at the first instance judicial officers were asked whether they have in cases involving electronic evidence ordered that electronic record be authenticated by examining an expert u/s 45A of Evidence Act?. If they answered in the affirmative they were asked to state in how many cases. Their response is noted as under:

**Table 31**

*Authentication Of Electronic Evidence By Examining An Expert U/S 45A Of Evidence Act by Judicial Officers*

| Response | Number | Percentage |
|---|---|---|
| YES | 8 | 16% |
| No | 42 | 84% |

*Source: Primary data*

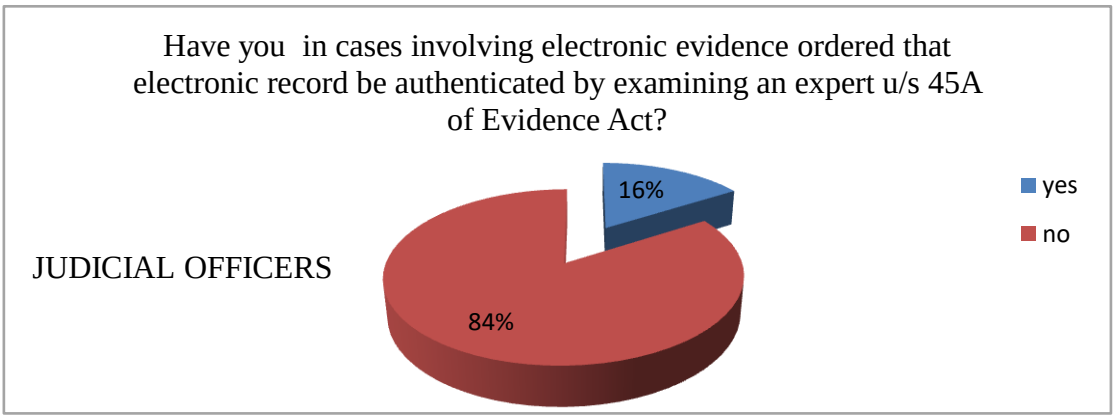



**Figure 20:** *Authentication Of Electronic Evidence By Examining An Expert u/s 45A Of Evidence Act by Judicial Officers*

Table 31 and figure 20 indicates the response of judicial officers to the question whether whether they have, in cases involving electronic evidence ordered that electronic record be authenticated by examining an expert u/s 45A of Evidence Act. 16% of judicial officers have answered in the affirmative. Whereas 84% of judicial officers have answered in the negative.

Likewise a similar question was asked to prosecutors and they have answered as under:

**Table 32**

*Authentication of electronic Evidence by examining an expert u/s 45A of Evidence Act by Prosecutors*

| Response | Number | Percentage |
|---|---|---|
| YES | 16 | 32% |
| No | 34 | 68% |

*Source: Primary data*

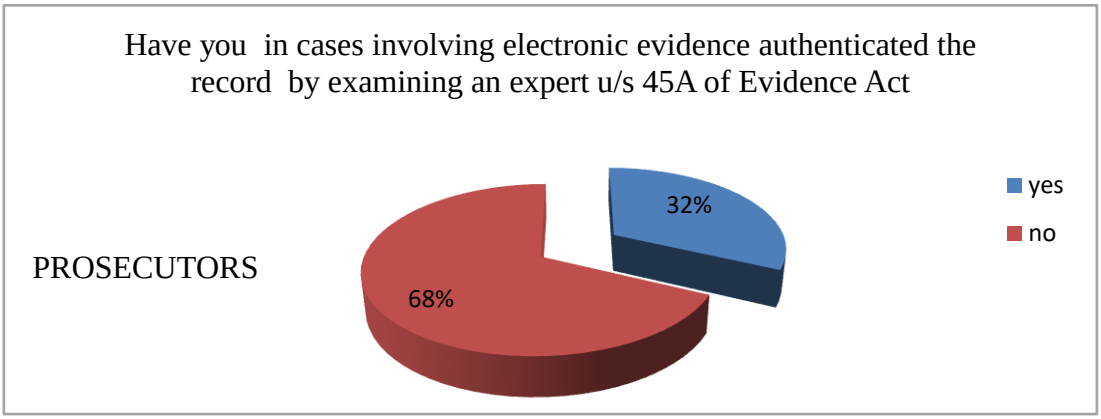



**Figure 21** *Authentication of electronic Evidence by examining an expert u/s 45A of Evidence Act by Prosecutors*

Table 32 and figure 21 indicates the response of prosecutors to the question whether they have in cases in cases involving electronic evidence ordered that electronic record be authenticated by examining an expert u/s 45A of Evidence Act. 32% of prosecutors have answered in the affirmative whereas 68% of prosecutors have answered in the negative. This shows that the majority of Prosecutors have not authenticated electronic evidence by taking assistance of an expert.

Next the lawyers too were asked whether they have examined an expert to prove any electronic record under section 45A of the Indian Evidence Act. Their response is recorded as under:

**Table 33**

*Authentication of electronic Evidence by examining an expert u/s 45A of Evidence Act by Lawyers*

| Response | Number | Percentage |
|---|---|---|
| YES | 41 | 27% |
| No | 109 | 73% |

*Source: Primary data*

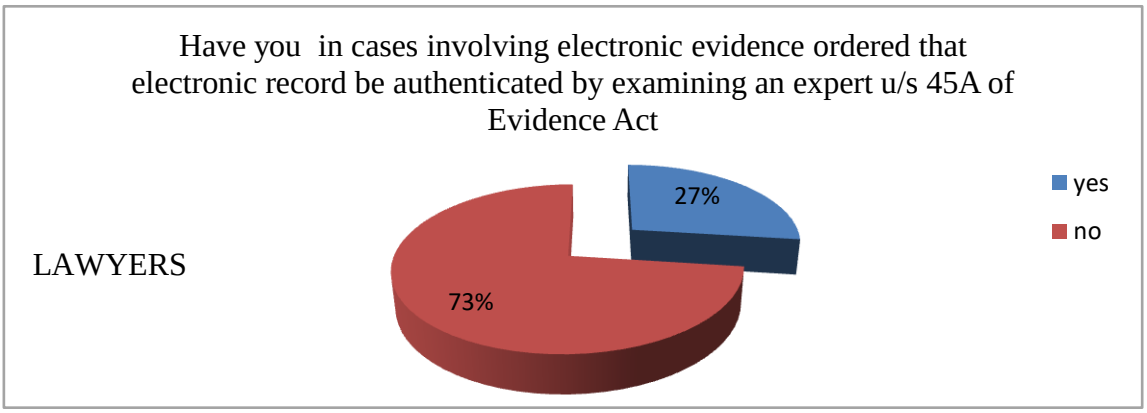



**Figure 22:** *Authentication of electronic Evidence by examining an expert u/s 45A of Evidence Act by Lawyers*

Table 33 and figure 22 indicates the response of lawyers to the question whether they have in cases involving electronic evidence ordered that electronic record be authenticated by examining an expert u/s 45A of Evidence Act. 27% of lawyers have answered in the affirmative whereas 73% of lawyers have answered that they have not sought assistance of expert under section 45A at any point of time.

The trend in the response given by the judicial officers as well as the prosecutors and lawyers show that there is frugal use of section 45A of the Indian Evidence Act. Section 45 A was inserted at a time when electronic records made a headway in the Indian Evidence Act. It was placed after the provision relating to relevancy of expert opinion. However the less use of section 45 A suggests that there are few cases in which the integrity or authenticity of an electronic record is questioned. Most of the criminal cases in this category were cases under the Prevention of Corruption Act or Cyber crimes.

### F. Furnishing Copy Of Electronic Record In The Chargesheet

The next relevant issue that often is not complied is giving copies of electronic records to the accused of the documents that the prosecution relies along with the chargesheet. As per section 207 of CrPC, the accused is entitled to copies of all documents relied upon in the chargesheet. The section makes it mandatory to supply copies of police report and other documents that are sought to be relied upon along with the police

report, to the accused free of cost.

When Judicial Officers were asked to enlist the difficulties faced by them in dealing with electronic evidence they have stated that one of the difficulties is that the investigating officers do not give a copy of the electronic records to the accused. In other words no spare copy of the electronic record when produced in electronic form is kept for the accused. Thus judicial officers were asked whether copies (to be given to the accused) of electronic records (CD, Pendrive etc) other then hard copies of photographs, produced along with the chargesheet?. Their response was as under:

**Table 34**

*Copies of electronic record for accused produced along with chargesheet;*

| Category | Response | Percentage |
|---|---|---|
| yes, in most cases | 27 | 53 |
| No, Very Rarely | 23 | 47 |

*Source: Primary data*

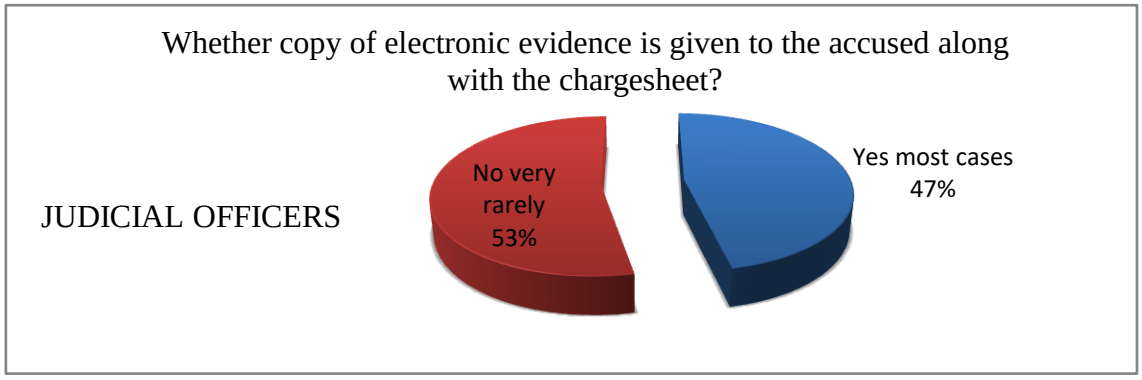



**Figure 23***: Pie Chart showing whether Copies of electronic record for accused produced along with chargesheet.*

Table 34 and figure 23 shows that 53% of the judges believe that copies (to be given to the accused) of electronic records (CD, Pendrive etc) other then hard copies of photographs, produced along with the chargesheet are very rarely appended to the chargesheet. Whereas 47% of the judicial officers believe that it has been done in most cases.

The relevance of this question stems front the fact that majority of the judges have responded to the question asked to them by stating that there is no copy of the electronic record relied upon by the prosecution given to the accused. The researcher went into the quest of as to why this happens. The answer to this question lies in the response given by the prosecutors about the form in which copy of electronic record is given by the party producing it to its opponent. Most of the times no copies are given, and copies which are given mostly in the cases where the electronic record can be reproduced on paper that is in case of photographs, sms, chats or webpages. In case of audio or video records it is often seen that no copies are given to the accused alongwith the chargesheet.

Upon interviewing some investigating officers it was revealed that this is because there is are no sufficient storage devices such as CDs, pendrives or spare hard disks provided at the police station. There are cases where the prosecution relies upon Hard disks, in such a case the accused is also entitled to copies of the hard disk, as there are no hardisks provided at every police station the process of procuring the same becomes tedious. It may however be added that cases where the audio video evidence contains material that is sexually explicit, no copies can be given to the accused and the accused is only entitled to view the material in the court.

Upon random examination of files by the researcher it was seen that copies of electronic record which are printed on paper are ordinarily furnished but where the record is copied in electronic form, either on a pen drive or a CD no copies are ordinarily provided. This is most common when the electronic record is an audio or video clip. There is thus violation of section 207 of CrPC.

Out of the case studies conducted some of which have been described above, indicate that sometimes the investigating officer seizes the device containing the original electronic record. This device is sent to the Forensic Science Laboratory to extract the data forensically for the preparation of its copies to be handled over to the accused. This process takes a significant time. If the accused is in custody the chargesheet is filed without this electronic document. As a result is it often seen that section 207 remains non complied.

Therefore wherever the copies of an electronic record can be printed on a paper it is seen that the dictum of section 207 is adhered to, whereas in all other case the attitude is lackadaisical.

G. **Storage Of Electronic Records:**

The issue of storage of electronic records intrigues both, the stakeholder who seizes the record and the stakeholder who appreciates it when produced before it. These two key stake holders are the Police and judges.

Preservation of an electronic record is the most essential at the stage investigation, as the ultimate aim of seizure is to produce the record as evidence in court. The record thus is to be preserved properly at the Police Station and thereafter in the courts. In the foregoing chapters the researcher had discussed how electronic record has to be seized and stored. On being interviewed in this regard the Investigating Officers submitted that there is no material or infrastructure provided for preserving the electronic record in the most optimal conditions so as to avoid any loss of data or damage to electronic record.

The researcher also inspected the Malkhanas of some police stations and found that except for the Cyber Crime Police station no other Malkhanas were properly equipped. Accordingly the researcher had formulated a question to the investigating officers to determine whether there were adequate storage facilities for electronic records at the Police station. The response to the question was as under:

**Table 35**

*Existence of Special Malkhana /Muddemal room/ to preserve Electronic record at Police Station*

| Response | Number | Percentage |
|---|---|---|
| YES | 38 | 25% |
| No | 112 | 75% |

*Source: Primary data*

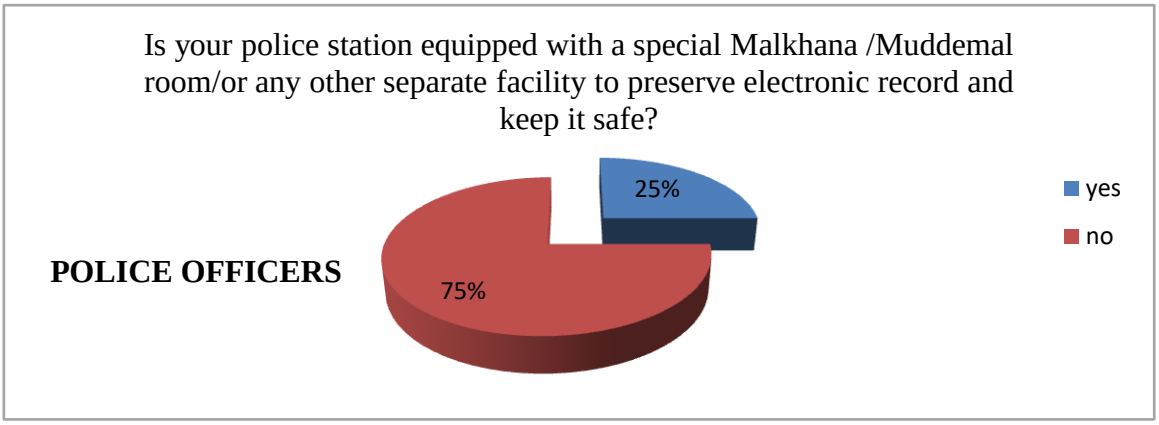



**Figure 24:** *Special Malkhana to preserve electronic record at Police Station*

Table 35 and figure 24 indicates that 75% of the Police respondents have stated that their Police station is not equipped with a special Malkhana /Muddemal room/or any other separate facility to preserve electronic record and keep it safe, whereas 25% are of the contrary view. The researcher upon random survey found out that except cyber crime Police station no other police station has a special muddemal room or facility to preserve electronic record and keep it safe. Further it is the experience of the researcher as a judge that most police stations in Goa do not have adequate space to store regular muddemal, sometimes articles are even kept at outposts which are often understaffed, in these circumstances a proper action plan needs to be prepared to ensure that muddemal containing electronic record is properly stored. In the course of research the researcher also noted that ordinarily the electronic record that is seized as muddemal are either hard disks or mobiles, very rarely are computers desktops or allied bulky equipment is seized. The space therefore required to keep such record will be minimal and can be carved out easily in the existing setup of police stations.

After filing of chargesheet the electronic record is produced in court as muddemal. Sometimes CDs or Pendrives are produced as documents in the court along with the charge sheet, the question arises as to why there is a need to have a separate muddemal room for electronic records. Electronic records are more susceptible to the vagaries of its environment as compared to the inanimate objects. They thus have to be preserved in a cool and dry place and have to be handled carefully.

This requirement is notwithstanding the fact the device containing the electronic record may not be in working condition at the time when the same is produced in the court at the time of trial. For example mobile phones what may contain an incriminating video or audio may not be in a working condition at the time of trial. Anticipating these eventualities the Investigating Officer has to take necessary steps to ensure that the copy that is prepared as per law is made available for the perusal of the court.

Similar information was sought from North Goa and South Goa District Courts and these courts as well have answered in the negative stating that there is no separate malkhana or Muddemal room to keep electronic records that may be produced as muddemal in the courts.

On a similar point Judicial officers were asked if the electronic record (other than muddemal) contained in an optical or magnetic device is produced before them, what steps do they take to preserve it separately. They were asked to choose from 2 options namely that(1) they are preserved/kept separately and not tagged along with the main file or (2) the electronic record is tagged together to the main file. The stakeholders have answered as under:

**Table 36**

*Steps taken to preserve electronic record (other then muddemal) contained in an optical or magnetic device by judicial Officers*

| Response | Number | Percentage |
|---|---|---|
| Yes; they are preserved/kept separately and not tagged along with the main file | 17 | 34% |
| No; the electronic record is tagged together to the main file | 33 | 66% |

*Source: Primary data*

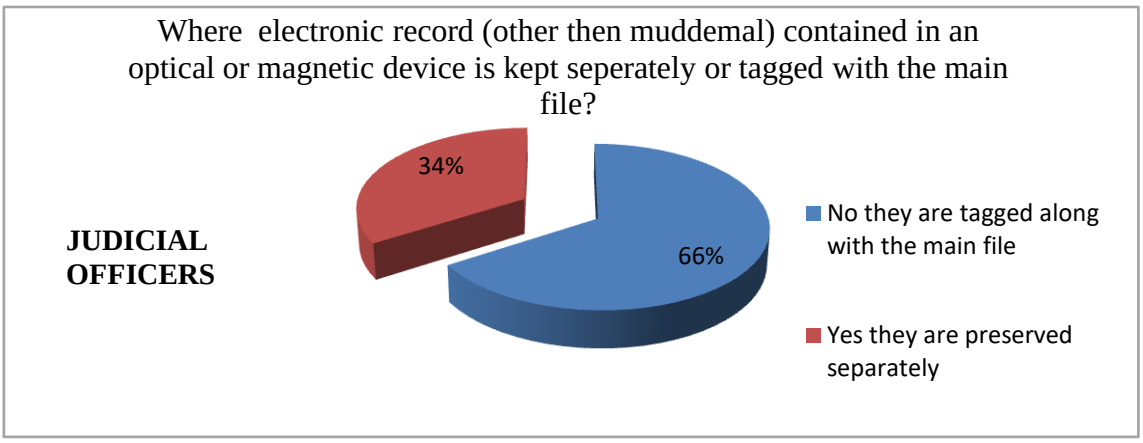



**Figure 25** *Steps taken to preserve electronic record (other then muddemal) contained in an optical or magnetic device by judicial Officers*

Table 36 and figure 25 suggests that 34% of the respondent judges have stated that the muddemal is preserved and kept separately and not tagged along with the main file. The rest namely 66% have candidly admitted that the electronic record is tagged together with the main file. The researcher has noted that the process in which documents are to be filed in the court files is contained in the civil and criminal manual but till date there has been no amendment to incorporate the process for filing of electronic records. On being interviewed in this regard a number of judicial officers narrated their experiences where the peon of the court has damaged electronic records such as a CD, by pricking it with a poker whilst stitching the papers in the rest of the file.

However in recent times it is seen that this issue has been discussed at workshops and judicial officers have been taking sufficient precautions to preserve electronic records such as CDs or pendrives from accidental damage. This is done by putting a caption or noting on the docket of the file that there is a CD inside. Or by putting the CD or pendrive in an envelope and securing it in a manner that there is sufficient margin on the side for the poker to pierce so that the CD is protected.

However despite this precaution it has been the experience of the researcher as a judicial officer that the CD produced on record is often damaged and has cracked into pieces if not protected well with the help of foam packaging.

At this juncture it would also be pertinent to point out that there is no SOP or guidelines issued to the courts on the aspect of handling of electronic records. It would have been desirable if some amendment is made to the Civil and Criminal Manual prescribing the mode in which electronic records which are now classified as documentary evidence be stored and preserved in the court. It has come in the experience of the researcher as a judicial officer that documents containing CDs are stitched along with paper documents without taking care that the CD is pierced with a poker whilst stitching. Hence the issue of preservation and storage needs to be properly addressed by providing proper infrastructure and guidelines for preservation of electronic records.

**H. Adequacy Of Infrastructure To Produce And Preserve Electronic Record.**

The two stake holders that play the most crucial role in production of electronic evidence in courts are police and prosecutors. The question whether there is adequate infrastructure available in the State of Goa that would assist the law enforcing agencies in proper preservation, production and authentication of electronic evidence in court, could only be answered by them.

The use of the term infrastructure herein refers to two aspects, one where proper infrastructure needs to be provided for seizure and preservation of electronic evidence and second where proper technical infrastructure is needed for its examination, authentication and generation of copies. A question may arise as to why the issue of infrastructure is so essential particularly when all the investigation machinery is already in place to collect evidence to prove facts. Special or different infrastructure is needed in view of the fact that electronic evidence cannot be equated to regular form of documentary evidence. As discussed in chapter 4 above the mode of its procurement, preservation and production is distinct thus the quest of understanding whether there is adequate infrastructure to handle electronic evidence.

In this context the police and prosecutors were asked whether they think there is adequate infrastructure available in the State of Goa that would assist the law enforcing agencies in proper preservation, production and authentication of electronic evidence in court. Their response is recorded as under:

**Table 37**

*Adequacy of infrastructure in the State of Goa response by Police:.*

| Response | Number | Percentage |
|---|---|---|
| YES | 47 | 30% |
| No | 103 | 70% |

*Source: Primary data*

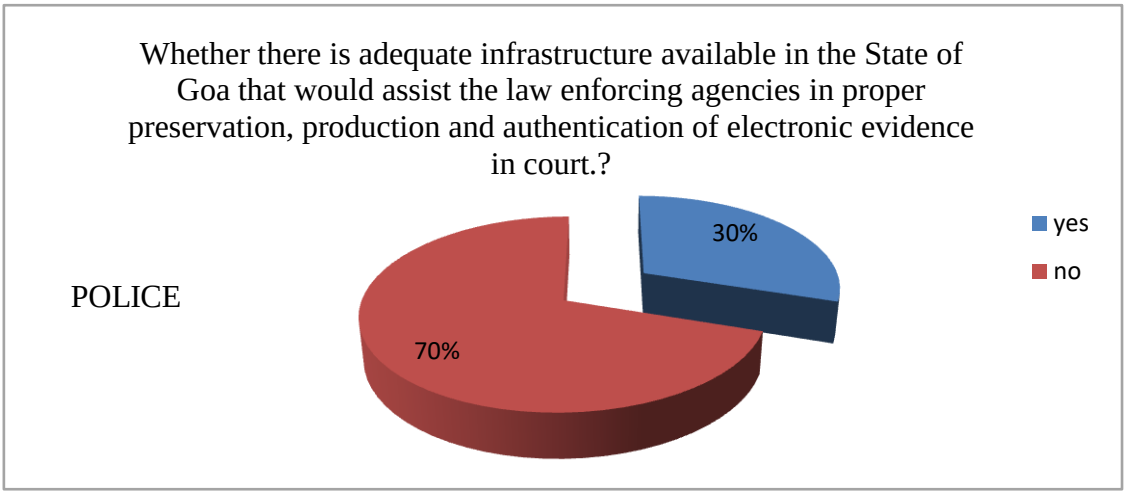



**Figure 26:** *Adequacy of infrastructure in the State of Goa response by Police:*

Table 37 and figure 26 indicates that 70% of the Police respondents are of the view that there is no adequate infrastructure available in the State of Goa that would assist the law enforcing agencies in proper preservation, production and authentication of electronic evidence in court, whereas 30% are of the contrary view.

On a similar question prosecutors have answered in the same manner underscoring that there is no adequate infrastructure available in the State of Goa that would assist the law enforcing agencies in proper preservation, production and authentication of electronic evidence in court.

**Table 38**

*Adequacy of infrastructure in the State of Goa response by Prosecutors*

| Response | Number | Percentage |
|---|---|---|
| YES | 10 | 20% |
| No | 40 | 80% |

*Source: Primary data*

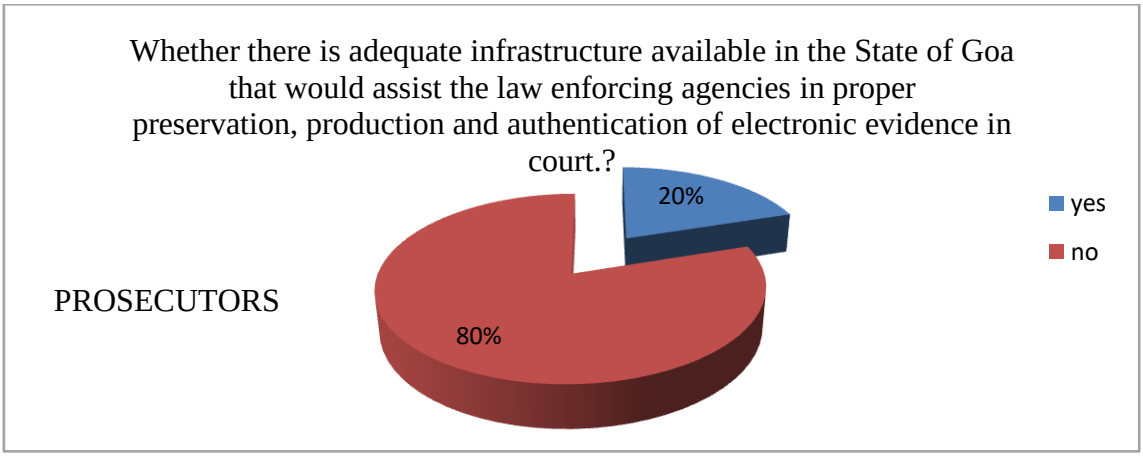



***Figure 27*: *Adequacy of infrastructure in the State of Goa response by Prosecutors:***

Table 38 and figure 27 indicates that 80% of the prosecutors in Goa are of the view that there is no adequate infrastructure available in the State of Goa that would assist the law enforcing agencies in proper preservation, production and authentication of electronic evidence in court, whereas 20% believe that there is sufficient infrastructure.

Next the researcher has compared the responses of both stakeholders:

**Table 39**
*Comparison of response of two stake holders*

| Scale | Response in Percentage | | |
|---|---|---|---|
| | PROSECUTORS | POLICE | AVERAGE |
| YES | 20 | 30 | 25 |
| NO | 80 | 70 | 75 |

*Source: Primary data*

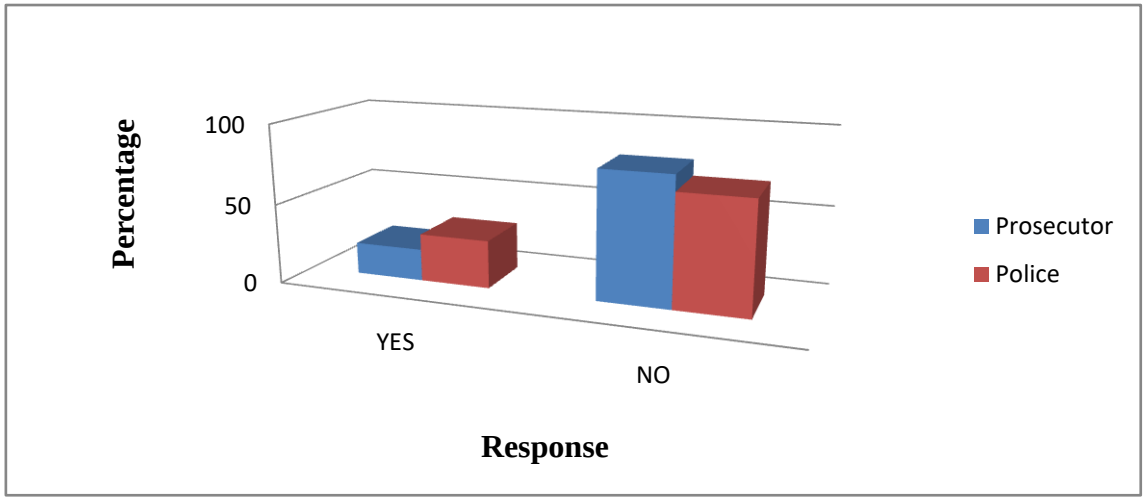



**Figure 28** *Comparison of response of two stake holders on adequacy of infrastructure.*

From the analysis of the table 39 and figure 28 above it is conclusive that there is no adequate infrastructure available in the State of Goa that would assist the law enforcing agencies in proper preservation, production and authentication of electronic evidence in court.

**I. Copy Of Electronic Records:**

The Indian Evidence act permits issuance of certified copies of documents. As electronic records are documentary evidence, certified copies thereof will also be applied for. The question arises as to whether certified copies of electronic records can be issued in the same manner as conventional paper documents, second whether the court has expertise to issue certified copies of electronic records and thirdly and most

importantly in the absence of any legislative guidance in this regard what procedure is generally followed by courts of law. For the purpose of discussion the word certified copies can be broadened to include plain copies. Stake holders were therefore asked some pertinent questions in that regard.

When the researcher interviewed the principal district judges, administrative judges and the concerned clerks who handle such matters it was learnt that application for certified copies of electronic records was an absolute rarity and most of the respondents had not handled this issue.

In CS 4.2011(Panaji District Court) in the case of *The Indian Performing Right Society v. The CEO, Entertainment Society of Goa (ESG)*[298] had encountered a similar issue however the applicant wanted mere photocopies of the CDs that were produced on record. The applicant who was in possession of the original electronic record claimed that it was contained in a memory card which was lost. The trial court dismissed this application. This order was challenged before Hon'ble High Court in the Writ Petition No.273 of 2019. The Hon'ble High Court observed that there was no bar in issuing copies of electronic records to the plaintiff as the records contained in the registry themselves are copies. All the issues of admissibility and mode of proof was kept open.

Upon thorough research on this subject the researcher is unable to find any legal precedent on the aspect of issuance of certified copy of an electronic record. There is thus a need to examine the existing law and ascertain as to how can a certified copy of an electronic record be issued when applied for in electronic form.

Here a reference needs to be made to the provisions of the criminal manual and the Indian Evidence Act. Chapter XXI of the Criminal Manual provides that a party to any proceeding can apply to the Court having the custody of the record, for certified copies of any judgment, order, deposition, memorandum of evidence, or any other documents filed in any proceedings. And the copy so applied shall be prepared and given to him as per section 76 of the Indian Evidence Act[299].

[298] This Case has been studied as a part of case studies in chapter 4 above
[299] Chapter XXI of Criminal Manual reads as: Copies and translations Certified copies

Section 76 of the Indian Evidence Act empowers a public officer having the custody of a public document, to issue a copy of it along with a certificate written at the bottom that it is a true copy of such document[300]. Public documents are defined under section 74[301] of the Indian Evidence Act.

---

1. Parties to any proceeding may, on application with the prescribed court fee made to the Court having the custody of the record, obtain certified copies of any judgment, order, deposition, memorandum of evidence, or any other documents filed in the said proceeding. The application may be made by the party himself or by his recognized agent or by his Pleader or Advocate and may also be sent by post. The application shall state whether the copy applied for is required for private use or otherwise. Where a party applies for a certified copy by post other than registered post, the date of its receipt by the office of the Court would be the date of the presentation of the application. Whenever such application is made by registered post, the same shall be prepaid for acknowledgment and the date of posting of the letter would be the date of presentation of the application to the Court.
2. Applications for copies by parties other than parties to the proceeding shall be supported by an affidavit stating the purpose for which the copies are sought.
3. On receipt of an application, the Office shall immediately scrutinize the application with a view to ascertaining the correct number of the proceeding, names of the parties, description of the document, copy of which is applied for, and whether the document is available for copying
.4. The Office shall estimate the costs of the copies before the copying work is undertaken. The estimate should, as far as possible, cover all probable costs of the copies including the postage, if the copies are required to be sent through the agency of post.
5. The applicant shall be called upon to deposit the estimated costs of the copies applied for, and make up other deficiencies then and there only, if his presence is available in the office. In other cases, the orders of the Presiding Officer shall be obtained requiring the applicant to comply with the necessary requirements before the copying work is taken in hand.
6. when the description of the document given in the application is incorrect or deficient, and it is, in consequence, necessary for the record Keeper to search his records in order to find it, a fee at the rate of one rupee for each year of which the records are searched, shall be payable by the applicant for such search, whether the document be found or not, and whether the copy of which he applies , on examination of the said document, be granted or not.
7. As soon as the Office find that the application is complete in all respects, it shall be placed before the Presiding Officer who may either grant the application, or refuse it for reasons to be recorded thereon, or pass such other orders as he may deem just.
8. Copies shall be furnished within 10 days of the application, if the application is complete, on the day on which it is presented, unless further delay is unavoidable, in which case the cause of delay shall be endorsed on the copy.
9. All copies shall be dated, subscribed and sealed in the manner prescribed by section 76 of the Evidence Act.
10. All copies should be correct and typed or written in a clear hand, with good ink, on substantial paper and on the outer three quarters margin only of sheets of foolscap papers, the inner one-quarter margin of every sheet being left blank

[300] Every public officer having the custody of a public document, which any person has a right to inspect, shall give that person on demand a copy of it on payment of the legal fees thereof together with a certificate written at the foot of such copy that it is a true copy of such document or part thereof, as the case may be, and such certificate shall be dated and subscribed by such officers with his name and his official title, and shall be sealed whenever such officer is authorized by law to make use of a seal, and such copies so certified shall be called certified copies. Explanation; Any officer who, by the ordinary course of official duty, is authorized to deliver such copies, shall be deemed to have the custody of such documents within the meaning of this section.

[301] Section 74 of the Indian Evidence Act: The following documents are public documents:
(1)documents forming the acts or records of the acts —

Like wise para 15 of Chapter XXI of the Manual provides that a Simple copies( implying plain photo copies) of any documents on the record of a proceedings can be certified as true copies.

If all these provisions are read together one interpretation can be that the terms electronic record has not been incorporated in the definition of the word "document" contained in section 2 of the Indian Evidence Act although it may have been classified as documentary evidence. Section 76 or chapter XXI supra refers to "documents". Thus strictly speaking they exclude electronic records that may have been filed as evidence. Thus a certified copy an electronic record under Chapter XXI r/w section 76 of the Indian Evidence Act can be refused. This will be either in electronic form or on paper.

This interpretation can however cause a paradox and it will completely incapacitate a person from obtaining copies of documents. In such a case a liberal interpretation needs to be given to the phrase "*obtain certified copies of any judgment, order, deposition, memorandum of evidence, or any other documents filed in the said proceeding*" used on chapter XXI para 1 of the criminal manual and hold that electronic records that may be produced as evidence in court can be copied and issued to the party applying for copies of the same.

The next pertinent question arises is whether such a process of copying can destroy the integrity of the electronic record so produced. The answer to the question is that given with the assistance of technical input, it may or may not. Everything depends upon the process used for copying. The experts in the field however caution that the original electronic record as far as possible should not be meddled with as it may be called into question for forensic examination at point of time by the court.

---

(i) of the sovereign authority,
(ii) of official bodies and tribunals, and
(iii) of public officers, legislative, judicial and executive, [1] of any part of India or of the Commonwealth, or of a foreign country;
(2) public records kept [2] in any State of private documents.

The researcher therefore is of the humble view copies of electronic records in electronic forms can be issued by following a mechanical process that will ensure the accuracy of the data copied. Only that person (preferably the computer administrator of the court) who can ensure its accuracy and who has adequate knowledge of the copying software must be entrusted with this job. And after issuing the copies the nodal officer must certify that the copy has been prepared by a mechanical process ensuring the accuracy of the data copied. In so far as obtaining copies from original records is concerned, that process will require intervention of a computer forensic expert and appropriate equipment and the legislature must also provide for it by laying down rules and regulations.

The researcher is also of the view that the legislature must make adequate provisions in the law to tackle this issue and provide for a certificate similar to a certificate under section 65B to the issued by the officer who carries out the copying process.

**J. Competence Of Investigating Officers In Contemporary Times In Handling Electronic Evidence.**

The two stake holders that play a primary role in assessing the competence of investigating officers in handling electronic evidence are judicial officers and prosecutors. As the defence counsel endeavours to prove how the investigating officer has failed in his duty to prove the case the researcher was of the view that lawyers could not have objectively opined on the aspect of competence of Investigating Officers in Handling electronic evidence.

As noted earlier the stakeholder that has first contact with an electronic record is the Police. If the Investigating officer ensures that he properly seizes and produces electronic evidence in court, the subsequent process of admissibility and mode of proof becomes even more simpler.

Thus only two stakeholders namely the judicial officers and the prosecutors were asked whether investigating officers are equipped to handle issues relating to electronic

evidence. Their response is noted as under:

**Table 40**

*Competency of investigating officers to handle Electronic evidence; Response by Judicial Officers*

| Category | Response | Percentage |
|---|---|---|
| Yes | 9 | 18 |
| No | 41 | 82 |

*Source: Primary data*

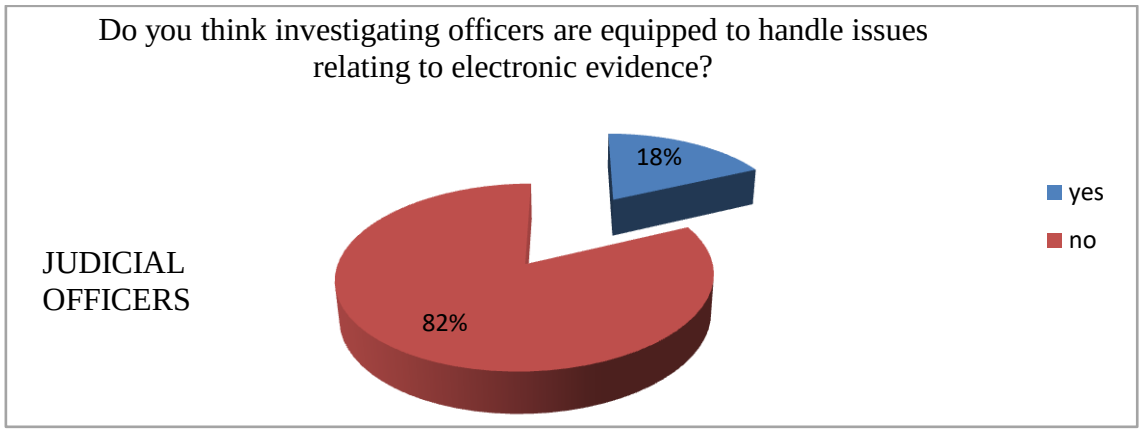



**Figure 29:** *Competency of investigating officers to handle electronic evidence; Response by Judicial Officers*

Table 40 and figure 29 shows that 82% of the Judicial Officers in Goa are of the view that investigating officers are equipped to handle issues relating to electronic evidence, whereas 18% think that that the position is contrary. Thus majority of the judicial officers are of the view that in contemporary times investigating officers are not competent to handle electronic evidence.

On a similar question majority of the prosecutors have expressed their view as under:

**Table 41**

*Competency of investigating officers to handle electronic evidence; Response by Prosecutors*

| Category | Response | Percentage |
|---|---|---|
| Yes | 43 | 86 |
| No | 7 | 14 |

*Source: Primary data*

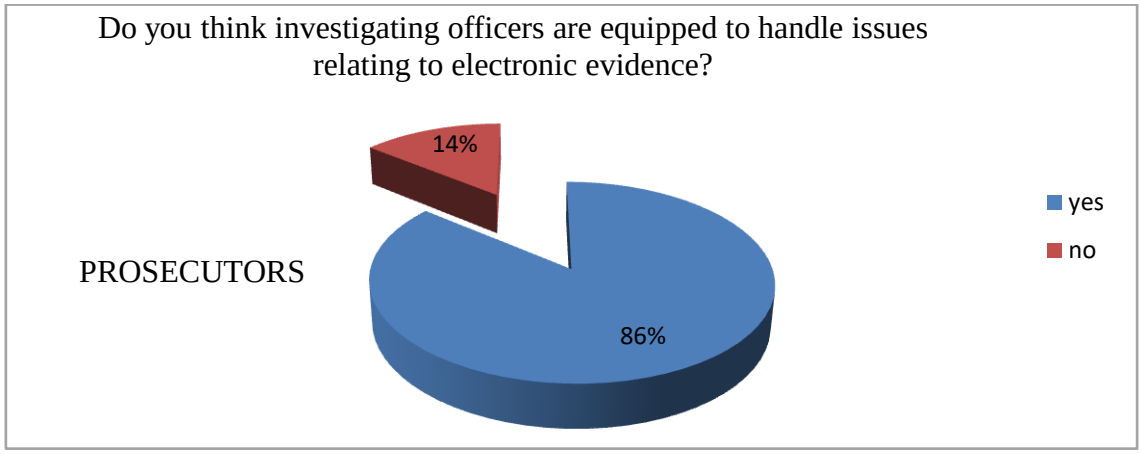



**Figure 30:** *Competency of investigating officers to handle electronic evidence; Response by Prosecutors*

Table 41 and figure 30 indicates that 86% of prosecutors in Goa consider that investigating officers are equipped to handle issues relating to electronic evidence, whereas 14% believe that they are not so equipped. It is evident from the data above that majority of the stake holders were of the view that investigating officers are well equipped to handle issues relating to electronic evidence

The prosecutors were additionally asked whether the IOs properly seize and preserve an electronic record so as to ensure its authenticity and integrity. They have responded as under:

**Table 42**

*Proper procedure in seizure and preservation of electronic record: Response by Prosecutors*

| Response | Number | Percentage |
|---|---|---|
| YES | 13 | 26% |
| No | 37 | 74% |

*Source: Primary data*

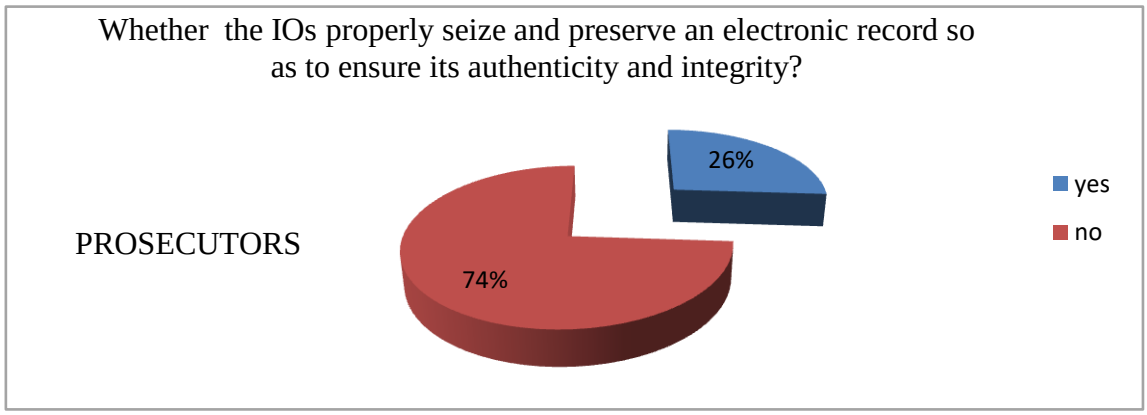



**Figure 31:** *Proper procedure in seizure and preservation of electronic record: Response by Prosecutors*

Table 42 and figure 31 shows that 74% of prosecutors in Goa are of the view that the investigating officers do not properly seize and preserve an electronic record so as to ensure its authenticity and integrity, whereas 14% believe that they do. Hence majority of the respondents are of the view this aspect requires improvement.

What then should be the solution for the problem. The answer is that we need to equip investigating officers who otherwise are found to be competent to handle electronic evidence. Until the procedure for seizure and preservation is streamlined by providing rules and regulations, technical assistance must be provided at every step. Secondly, there must be training imparted to all stake holders to ensure that there is optimum use of electronic records as a means of proof of a fact. The issue of training shall be considered in the next part of the chapter.

**K. Training:**

The issue of training is actually relevant for all stake holders, however proper emphirical data could be obtained from the judiciary, police and the prosecution. In so far as the bar is concerned, lawyers although are affiliated to various bar associations there is no obligation on those associations to train them. Upon been interviewed, the concerned heads of the association quiet rightly opined that being an association of professionals, they can only endeavour to organise informative seminars and workshops. As attendance cannot be made compulsory it cannot be classified as training in the strict sense of the term. The researcher therefore avoided asking lawyers whether they had undergone any training in the subject of electronic evidence. The three stake holders namely judicial officers, Police and prosecutors were asked whether undergone any special training in cyber crime, cyber forensics and electronic evidence. A sample size of  Police respondent were asked whether they have undergone any training cyber crime or cyber forensics and they has responded as under:

**Table 43**

*Response on aspect of Training by Police Respondents.*

| Response | Number | Percentage |
|---|---|---|
| YES | 87 | 58% |
| No | 63 | 42% |

*Source: Primary data*

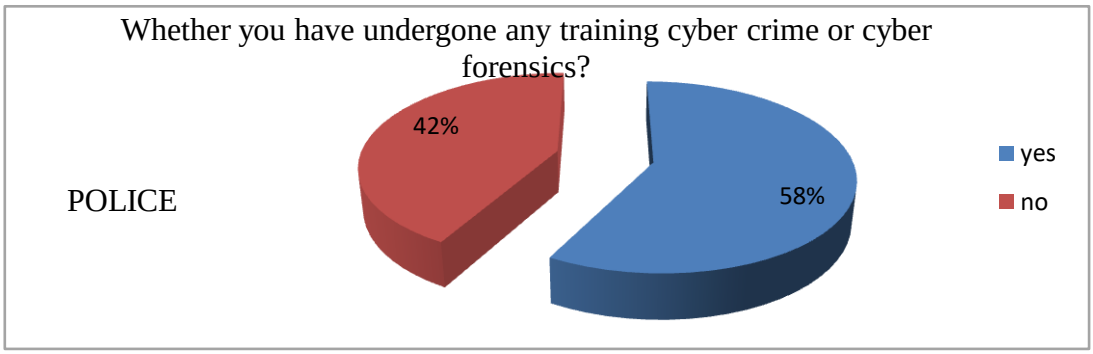



**Figure 32:** *Pie chart showing proportion of officers who have undergone training*

Table 43 and figure 32 represents the answers given by police personnel on the question of whether they have undergone training on the subject of cyber crime or cyber forensics? 42% of the respondents answered in the affirmative whereas 58% have answered in the negative.

It is pertinent to clarify here that the researcher deliberately used the word cyber crimes and cyber forensics instead of just electronic evidence simplicitor as preliminary research conducted before the preparation of questionnaire revealed that training programmes on this subject are designed broadly to cover aspects of cyber crimes where collection of electronic evidence is only a subject in addition to other subjects.

The researcher elicited information from the Superintendent of Police Training as regards training imparted to Police officers since 2016 to 2021 and they have replied as under:

**Table 44**

*Training of Police Personnel in Electronic Evidence and Cyber crime*

| Number of officers who have undergone training since the last 6 years* | | |
|---|---|---|
| Year | Training conducted in the state of Goa | Training conducted by national academy or other state academies |
| 2016 | - | 07 |
| 2017 | - | |
| 2018 | | |
| 2019 | 05 | 05 |
| 2020 | 07 | 03 |
| 2021 | 11 | 01 |
| Total | 23 | 16 |

*Source: Superintendent of Police; Training and GRP Camp.*

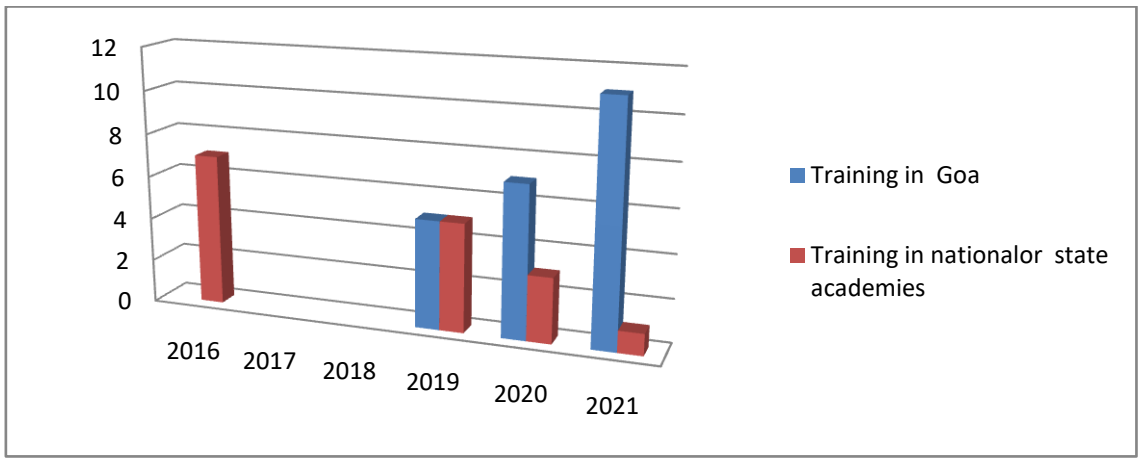



**Figure 33:** *No of Police Officers who have undergone training*

From table No. 44 and figure No. 33 it is seen that only since the year 2019 the Goa Police have been conducting trainings of Police officers in the subject of Electronic Evidence and cyber crime in the State of Goa. Whereas the officers appear to have been sent for training on this subject to National and State Judicial academies in the year 2016 and thereafter there seems to have been a break of 2 years. The positive aspect is that since the year 2019 there has been a upward trend in conducting trainings in the State of Goa, however the downward trend in sending officers to other states and national academies may be attributed to the Covid pandemic in the year 2020. In all there are only 23 training Programmes conducted in Goa for the last 6 years. The training programmes conducted in Goa are on the subject of "Cyber Crime Awareness Program; Cyber Forensic Tools; CDR Analysis.

As per the tabular information furnished by the office of Superintendent of Police it is seen that officers across all cadres are being sent for training on the subject of electronic evidence and the training is not restricted to officers of a particular rank. The researcher had asked a query as to whether all police officers in Goa given training on the subject of seizure of electronic evidence or cyber crimes (100% of the total strength)? This question has been answered in the negative . It is reported that only 56% of the Police personnel of Cyber Crime PS have undergone training on the above subject. This revelation is alarming as electronic records are handled by all police officers and not necessarily the Cyber Crime PS. It is therefore imperative that all police officers in Goa

are given training on the subject of electronic evidence.

There is no independent Police Training Academy in Goa. There is a training centre known as the Valpoi Police training centre[302]. The Centre imparts physical training to Police officers as well as conducts training on theory on subject of public importance.

After the original record is seized or a copy thereof is properly prepared, it may be required to be subjected to forensic examination based on the information that the investigating officers seeks to derive from that electronic record. Here the formulation of a proper question is quintessential. The Director of Goa Forensic Science Laboratory informed the researcher that a lot of investigating officers do not formulate the questions correctly therefore they are unable to get proper answers that would facilitate them to solve their case. In such a scenario it is advisable that the Investigating officers discuss the matter with the forensic scientist and accordingly formulate their questions and thereafter send the sample for forensic analysis. It was also informed to the researcher that investigating officers sometimes merely forward the exhibit for extraction of data without specifying what data is needed or found relevant. This data that is extracted from the original is directly produced in the court without the Investigating officer even viewing the extracted data and separating the relevant evidence that is intended to be produced for proof of facts. One such case study conducted by the researcher revealed this fact.

Next the aspect of training imparted to judicial officers was examined. The researcher obtained emphirical data from North Goa and South Goa District Judiciary about the training undergone by judicial officers from the year 2016 to 2021. The information is tabulated as under:

[302] Police Training School (PTS) was established in the year 1962 in Valpoi in North Goa to impart physical training to police personnel and also train the recruits in Indian laws and procedures. The PTS has come a long way since then and now also trains excise and forest personnel as well as jail guards. It is headed by a police officer of the rank of SP. The school as of now trains constabulary while the higher ranked officials are sent to other states, so that they can get specialized training. As per *https://citizen.goapolice.gov.in/web/guest/police-training-school on 25.12.2021 at 2.30 pm*

**Table 45**
*Training of Judicial Officers in electronic evidence and Cyber crime: North Goa District*

| Number of Judicial officers who have undergone training since the last 6 years*<br>NORTH GOA DISTRICT | | |
|---|---|---|
| Year | Training conducted in the state of Goa | Training conducted by national academy or other state academies |
| 2016 | - | 04 |
| 2017 | - | 03 |
| 2018 | 18(WORKSHOP) | |
| 2019 | | |
| 2020 | | |
| 2021 | 23(WORKSHOP) | 01 |

*Source: North Goa District Court*

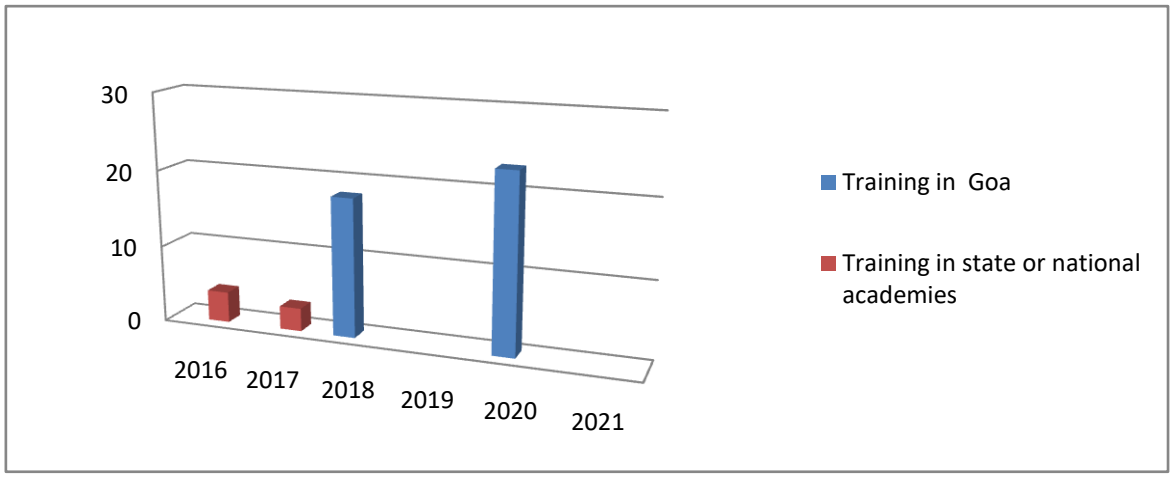



**Figure 34:** *Training of Judicial Officers North Goa*

Table 45 and figure 34 indicates the number of judicial officers who have been trained on the subject of Cyber crimes and Cyber Forensics. In respect of the North Goa district it is seen that in the year 2016, 04 judicial officers were sent for training conducted by

National/State judicial academies and in the year 2017, 03 judicial officers were sent for training in National/State judicial academies. In 2018 there was a workshop on the subject of Electronic Evidence and cyber crime a special Joint workshop for all judicial officers in the State of Goa. From 2019 to 2020 no judicial officer has been sent for training on this subject in national or state judicial academies.

Only in the year 2021 one judicial officer was sent. In 2021 there was a workshop for judicial officers of South Goa on this subject. This data has been collected in respect of trainings from 2016 to 2021.

**Table 46**

*Training of Judicial Officers in electronic evidence and Cyber crime: South Goa District*

| Number of Judicial officers who have undergone training since the last 6 years* SOUTH GOA DISTRICT | | |
|---|---|---|
| Year | Training conducted in the state of Goa | Training conducted by national academy or other state academies |
| 2016 | 17 | 03 |
| 2017 | - | 04 |
| 2018 | 18 | 01 |
| 2019 | - | - |
| 2020 | - | - |
| 2021 | - | - |

*Source: South Goa District Court*

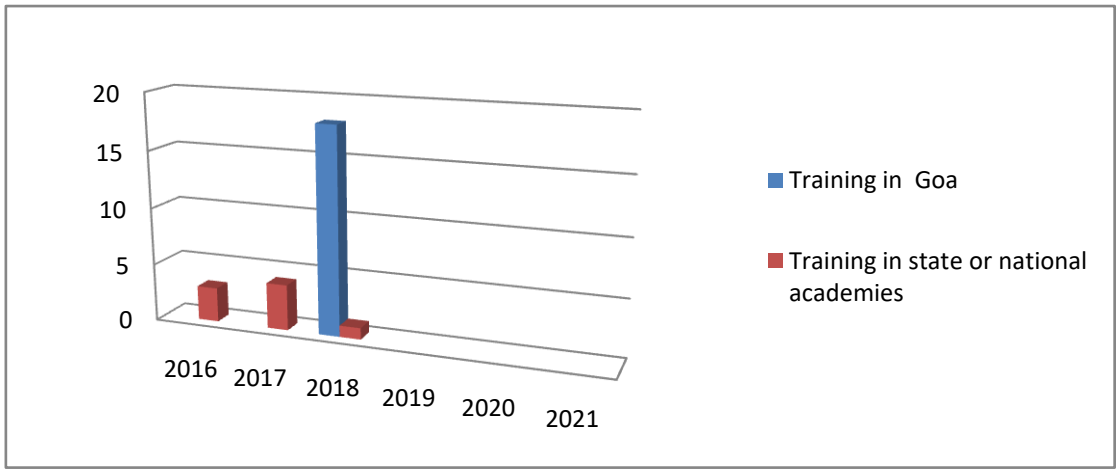



**Figure 35:** *Training of Judicial Officers South Goa District*

In respect of the South Goa District it is seen in Table 46 and figure 35 that in the year 2016, 03 judicial officers were sent for training conducted by National/State judicial academies and in the year 2017, 04 judicial officers were sent for training in National/State judicial academies. In 2018, 1 judicial officer was sent for training in National/State Judicial Academies.

In so far as training in the State of Goa are concerned, in 2018 there was a workshop on the subject of Electronic Evidence and cyber crime a special Joint workshop for all judicial officers in the State of Goa. From 2019 to 2021 no judicial officer has been sent for training on this subject in national or state judicial academies.. This data has been collected in respect of trainings from 2016 to 2021.

It was informed to the researcher that in addition to specific training programmes, the judicial officers also had periodic workshops on the subject of electronic evidence and cyber crimes. There are three to four yearly workshops held on myriad subjects of law of day to day importance. It was informed to the researcher that on October 2019 a day long workshop was held on the subject of Electronic evidence that included talks by master Trainer judicial officers and Resource persons on the subject of electronic evidence.

It was from the statistics given above it appears that almost all judicial officers have undergone some kind of training either through workshops or through trainings in

academies on the subject of electronic evidence.

The researcher has obtained empirical data from the Directorate of Prosecution about the training undergone by prosecutors from the year 2016 to 2021 and their response has been recorded as under:

**Table 47**

*Training of Prosecutors in electronic evidence and Cyber crime*

| Number of Prosecutors who have undergone training since the last 6 years* | | |
|---|---|---|
| Year | Training conducted in the state of Goa | Training conducted by national academy or other state academies |
| 2016 | - | - |
| 2017 | - | - |
| 2018 | - | - |
| 2019 | - | - |
| 2020 | - | - |
| 2021 | 0 | 02 |
| Total | 0 | 02 |

*Source: Directorate of Prosecution Goa*

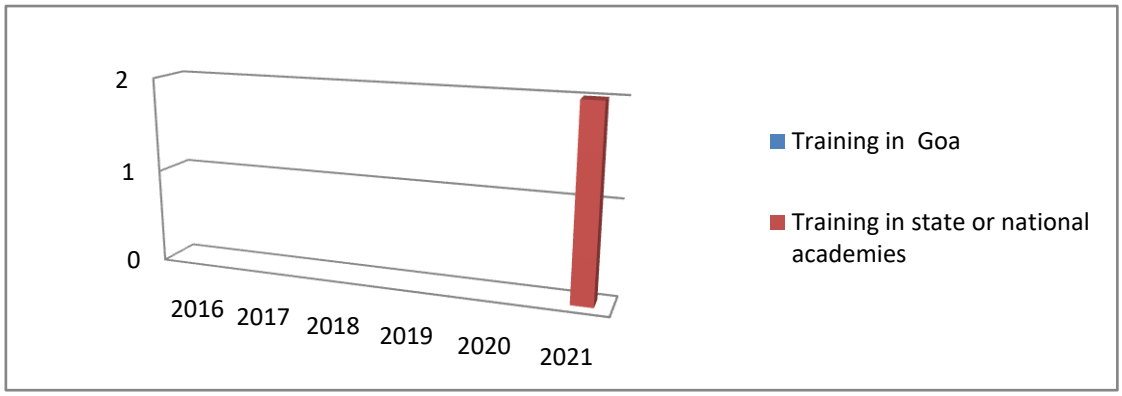



**Figure 36** *Training of Prosecutors in Goa*

Table 47 and 36 indicates the number of Prosecutors who have been trained on the subject of Cyber crimes and Cyber Forensics. In so far as the prosecution is concerned, it is seen that there are no periodic training in form of workshops held for prosecutors. Therefore the training on the subject of electronic evidence is confined to workshops, seminar and training programmes attended by individual prosecutors at different times, in different academies. In this regard it is seen that only two officers have been trained by National and State Judicial Academies that to only in the year 2021.

While the researcher officiated as the chairperson of the Taluka Legal Services Tiswadi Panaji, as a part of the programme calendar the researcher has conducted a workshop for investigating officers on the subject of production of electronic evidence in courts. This workshop was attended by about 50 investigating officers of the rank of Police inspector and Police sub inspector. The resource persons were Mr. Mallikarjun Male, Cyber Forensics expert, Cyber crime cell Ribandar, Mr. Darshan Gawas Assistant Public Prosecutor Valpoi and the researcher herself who presented the perspective of a judicial officer.

## L. Adequacy Of Law On Electronic Evidence

In the foregoing part of the Chapter the police and the prosecutors were asked whether there is adequate infrastructure available for proper authentication of electronic evidence. The lawyers and the judicial officers were excluded from this question as this aspect of the matter does not directly concern them. They were however along with

prosecutors and police asked a more generic question as to whether the present Indian Law is fully equipped to deal with all issues relating presentation, authentication and admissibility of electronic evidence in Court?.

Here the researcher has tried to combine the substantive as well as the procedural aspect. In the sense that the researcher seeks to gather from the stake holders whether the existing law or rules of procedure are sufficient to offset the difficulty or handle any issue relating to use, admissibility and proof of electronic evidence in the courts. The respondents have replied as under:

**Table 48**
*Suitability of present Indian Law on Electronic Evidence: Response of Judicial Officers*

| Category | Response | Percentage |
|---|---|---|
| Yes | 15 | 30% |
| No | 35 | 70% |

*Source: Primary data*

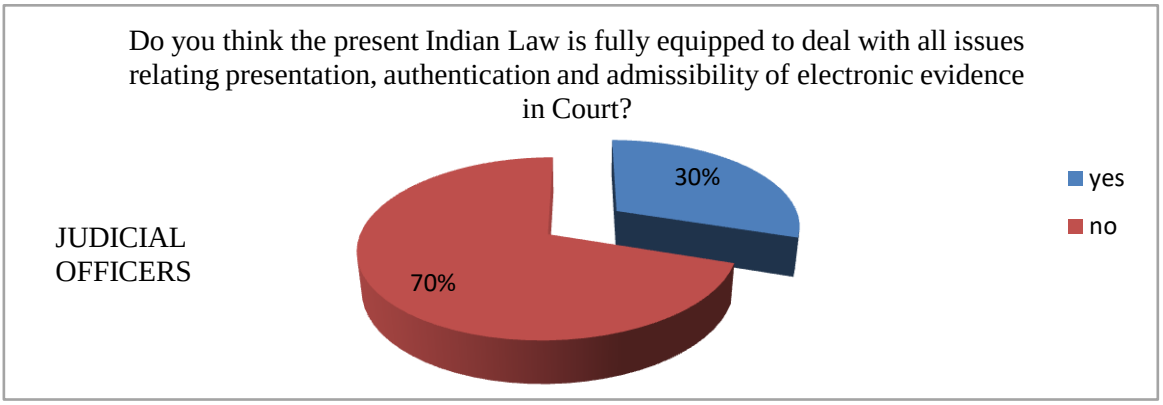



**Figure 37** *Suitability of present Indian Law to deal with all issues relating to electronic evidence: Judicial Officers*

Table 48 and figure 37 indicates that 30% of Judicial Officers in Goa are of the view that the present Indian Law is fully equipped to deal with all issues relating

presentation, authentication and admissibility of electronic evidence in Court, whereas 70% have a contrary view.

**Table 49**

*Suitability of present Indian Law on Electronic Evidence: Response of Prosecutors*

| Category | Response | Percentage |
|---|---|---|
| Yes | 20 | 40% |
| No | 30 | 60% |

*Source: Primary data*

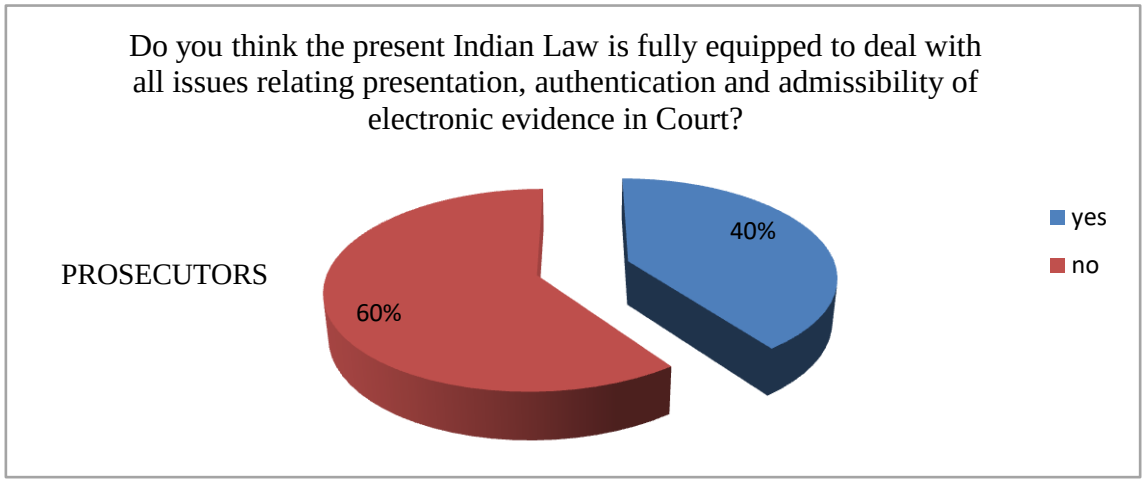



**Figure 38:** *Suitability of present Indian Law to deal with all issues relating to electronic evidence: Prosecutors*

Table 49 and figure 38 indicates that 40% of prosecutors in Goa are of the think that the present Indian Law is fully equipped to deal with all issues relating presentation, authentication and admissibility of electronic evidence in Court, whereas 60% hold that the law is not fully equipped.

**Table 50**

*Suitability of present Indian Law on Electronic Evidence: Response of Lawyers*

| Category | Response | Percentage |
|---|---|---|
| Yes | 20 | 13% |
| No | 130 | 87% |

*Source: Primary data*

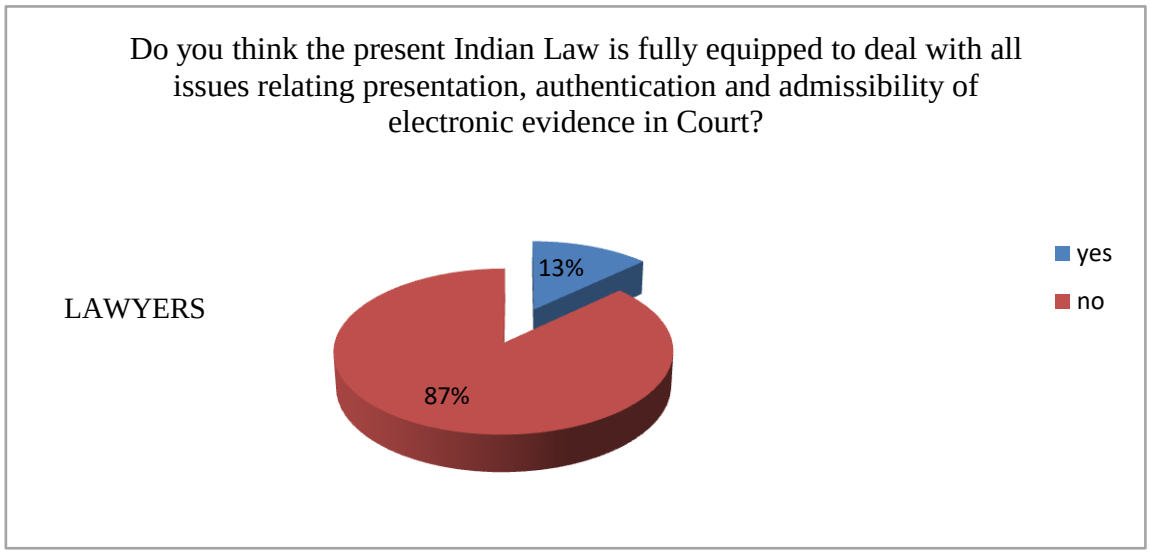



**Figure 39** *Suitability of Indian Law on Electronic Evidence: Response of Lawyers*

As per Table 50 and figure 39 only 13% of lawyers in Goa think that the present Indian Law is fully equipped to deal with all issues relating presentation, authentication and admissibility of electronic evidence in Court, and a majority of 87% opine that is not so. Below is a comparative chart showing the trends.

**Table 51**

*Comparative chart on Suitability of present Indian Law on Electronic Evidence: Response of all stake holders*

| Category | RESPONSE OF PROSECUTORS IN PERCENTAGE | RESPONSE OF LAWYERS IN PERCENTAGE | RESPONSE OF JUDICIAL OFFICERS IN PERCENTAGE |
|---|---|---|---|
| YES | 40 | 13 | 30% |
| No | 60 | 87 | 70% |

*Source: Primary data*

AVERAGE

YES- 21%

NO.- 79%

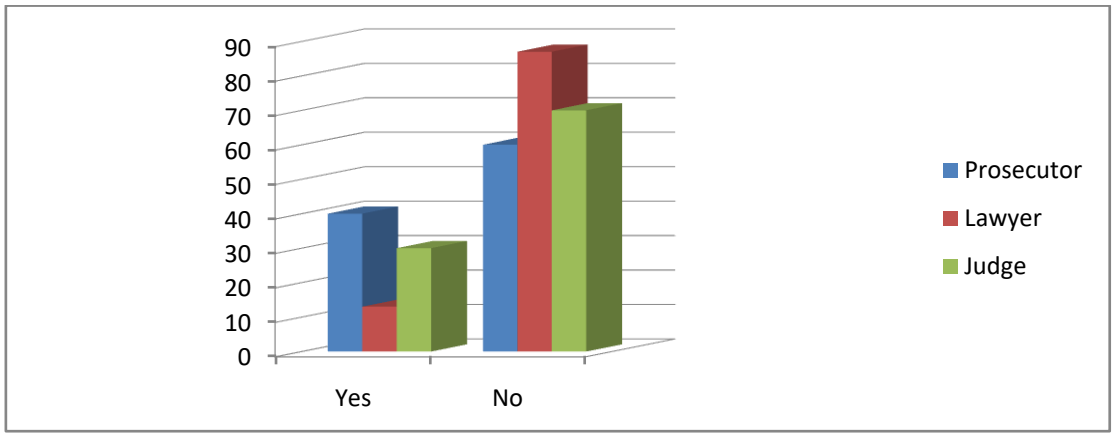



**Figure 40:** *Comparative chart on Suitability of present Indian Law on Electronic Evidence: Response of all stake holders*

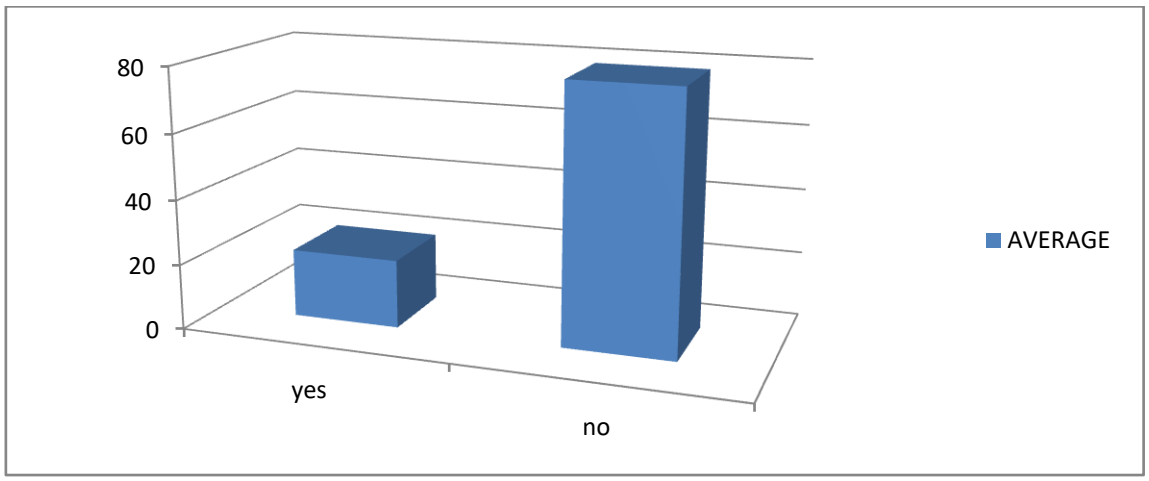



***Figure 41:*** *Average of responses of all stake holders on suitability of Indian Law on electronic evidence.*

Figure 41 indicates the average taken by adding all the responses at table 51 and figure 40. The average taken indicates that 79% of the stakeholders are of the view that Indian Law is still not fully equipped to deal with all issues relating presentation, authentication and admissibility of electronic evidence in Court. Whereas 21% consider the contrary. Thus of the take majority of the stake holders are of the view that the present Indian Law is not fully equipped to deal with all issues relating presentation, authentication and admissibility of electronic evidence in Court.

**M . Difficulties faced by stakeholders in dealing with Electronic Evidence**

From the overall field research the researcher found that there are issues and difficulties faced in use, admissibility and authentication of electronic evidence in court. The researcher therefore put two forms of questions to respondent stakeholders, namely an open ended question and a closed question with multiple choices.

The first closed question with multiple choices was what according to the stake holders are the reasons for difficulty in authentication and admissibility of electronic evidence in Court. There were a definite set of choices given. Judicial officers were excluded from this set as they sit in adjudicatory position and they were only administered an open ended question.

For the open ended questions the respondents were asked to state briefly the difficulties that they face in handling cases involving electronic evidence. The responses are analysed separately as the circumstances under which each category of the stake holder functions are unique to that stake holder.

At the outset lawyers were asked as to what they think are the reasons for difficulty in authentication and admissibility of electronic evidence in Court. They were asked to choose from 4 options, namely(1) Limited knowledge of judges and advocates in the field of electronic evidence (2) Want of empanelled experts u/s 45A to prove electronic record (3) Failure of litigant to preserve the original electronic record (4) All the above and (5) Others. Their response is recorded as under:

***Table 52***

*Reasons for difficulty in authentication and admissibility of electronic evidence in Court: Response of Lawyers*

| Reasons | Response | Percentage |
|---|---|---|
| Limited knowledge of judges and advocates in the field of electronic evidence | 40 | 27% |
| Want of empanelled experts u/s 45A to prove electronic record | 28 | 19% |
| Failure of litigant to preserve the original electronic record | 15 | 10% |
| All the above | 66 | 44% |
| Others | 01 | 1% |

*Source: Primary data*

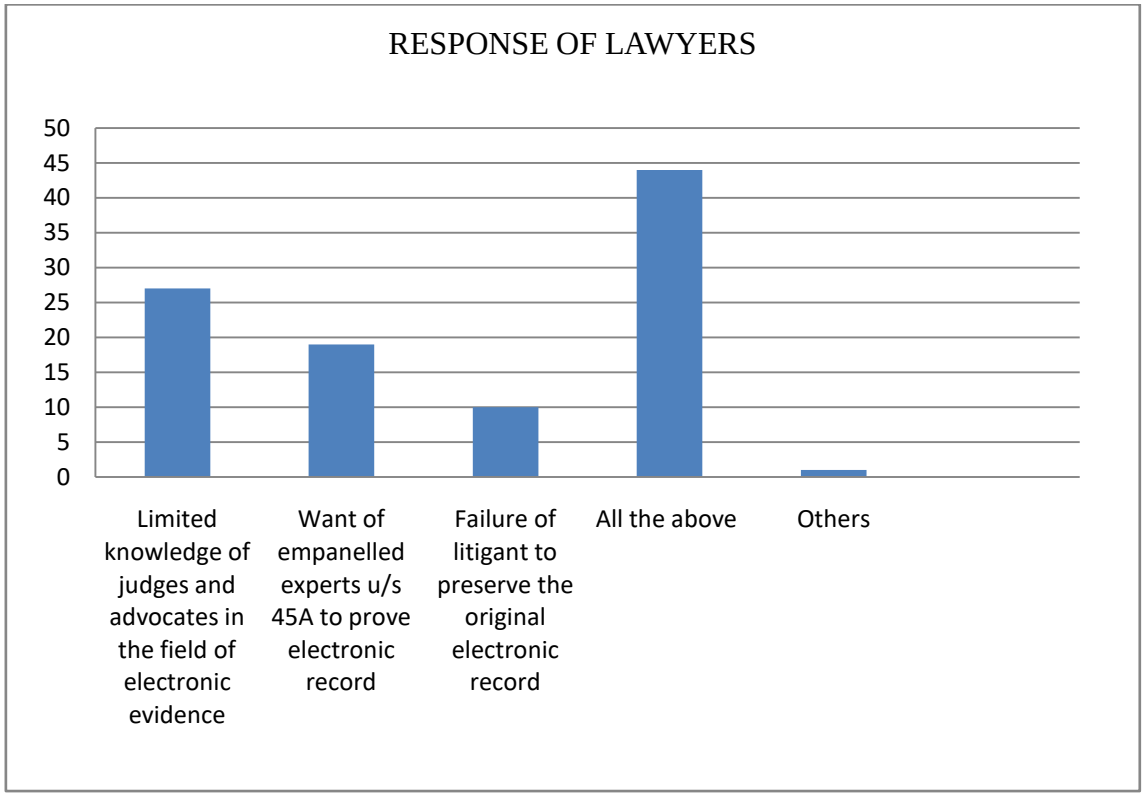



**Figure 42:** *Response of lawyers on the difficulty faced in authentication and admission of electronic evidence.*

Table 52 and figure 42 reveals that 27% of lawyers are of the view that Limited knowledge of judges and advocates in the field of electronic evidence is the reason for difficulty in authentication and admissibility of electronic evidence in Court. 19% and 10% respectively consider that want of empanelled experts u/s 45A to prove electronic record and the failure of litigant to preserve the original electronic record are the reasons. but majority of the lawyers namely a percentage of 44% feel that all the above factors cause difficulty. Only one lawyer has chosen the option others by stating that new technology versus old laws are the reason for difficulty in authentication and admissibility of electronic evidence in Court.

The open ended question that was put to the lawyers was to state what difficulties they faced in production of electronic evidence in Court. Some lawyers have answered this question some have left a blank. Some answers given are repetitive for brevity sake all

the answers given are complied as under:

1. Connectivity issues
2. No Uniformity in format of certificate under section 65B.
3. Person in control of the original record may not be available at the time of recording evidence.
4. No procedure to actually verify the contents of the certificate.
5. Mere production of certificate does not ensure genuineness as electronic evidence can be edited easily.
6. Difficulty in preserving electronic record till the trial is over
7. Unnecessary objections on authenticity
8. Failure to preserve original
9. Difficulty to obtain CDR in all cases.
10. Want of experts
11. No clarity whether section 65B certificate is required for electronically generated public records such as survey plans.
12. Law cannot cope up with rapid change in technology .
13. Lack of proper guidelines
14. Lack of knowledge of procedure in admitting copy of electronic record.
15. Professional photographers do not want to come to the court to give 65B certificate.
16. No guidelines for collection of data and use of anti forensic techniques.
17. Limited knowledge of litigants about electronic record.
18. Law not fully evolved causing doubts, vagaries and confusion.
19. No adequate infrastructure.
20. Difficult to prove Electronic evidence through ISP.
21. No proper equipments in courts to view electronic evidence.

22. Senior advocates who have never dealt with computers find difficult to cope up with electronic evidence
23. Litigant does not preserve the original.
24. Difficulty when original is with third party.
25. Difficulty to prove deleted emails.
26. Face book and twitter evidence cannot be proved in private criminal cases where the party denies the existence of an account.

Next Prosecutors were asked as to what they think are the reasons for difficulty in authentication and admissibility of electronic evidence in Court. They were asked to choose from the same 4 options as above. Their response is recorded as under:

***Table 53***

*Reasons for difficulty in authentication and admissibility of electronic evidence in Court: PROSECUTORS*

| Reasons | Response | Percentage |
|---|---|---|
| Limited knowledge of judges and advocates in the field of electronic evidence | 03 | 6% |
| Want of empanelled experts u/s 45A to prove electronic record | 01 | 2% |
| Failure of litigant to preserve the original electronic record | 18 | 36% |
| All the above | 26 | 52% |
| Others | 02 | 4% |

*Source: Primary data*

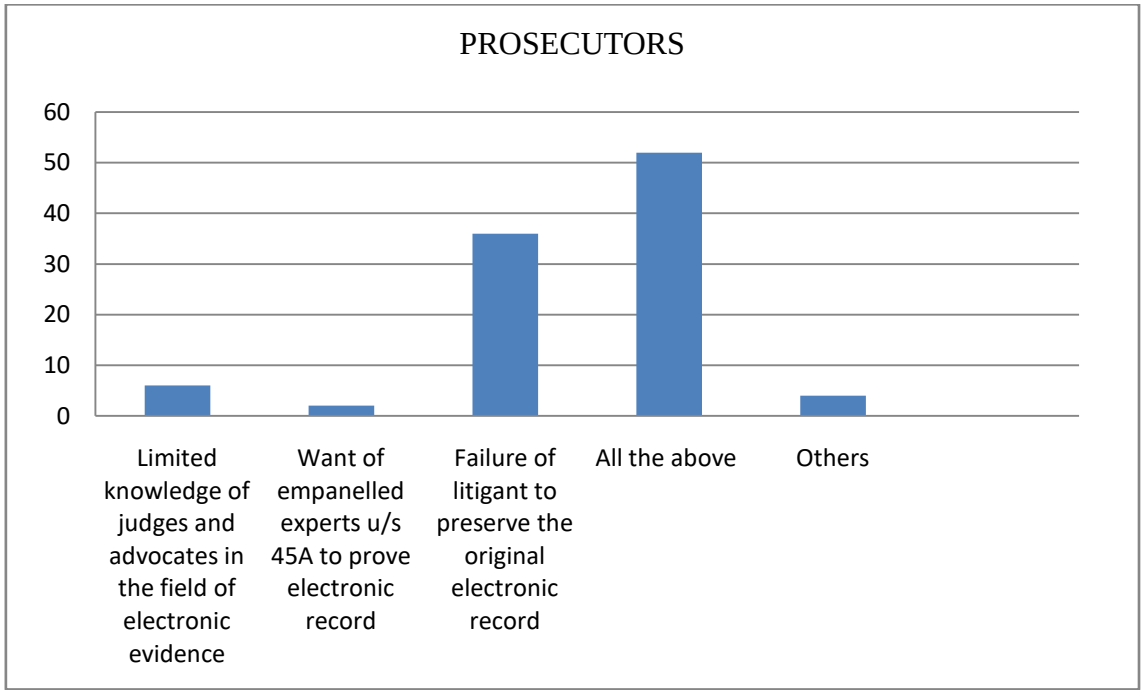



**Figure 43** *Reasons for difficulty in authentication and admissibility of electronic evidence in Court: Response of Prosecutors*

Table 53 and figure 43 reveals that 6% of prosecutors are of the view that Limited knowledge of judges and advocates in the field of electronic evidence is the reason for difficulty in authentication and admissibility of electronic evidence in Court. 2% and 36% respectively consider that want of empanelled experts u/s 45A to prove electronic record and the failure of litigant to preserve the original electronic record are the reasons. But majority of the prosecutors namely a percentage of 52% feel that all the above factors cause difficulty. 2% of the prosecutors have chosen the option others.

As regards the open ended questions as to the difficulty faced by them in admitting evidence the prosecutors have answered as under:

1. CD gets damaged during trial
2. Data is not properly copied on the CD
3. Section 65B certificate is not given along with chargesheet that contains Electronic Evidence.

4. Difficulty in identification of CCTV footage
5. Memory card is not produced by IO
6. IO does not collect proper electronic evidence
7. Original not seized at all or copy not prepared properly
8. Delay in seizure causes destruction of electronic record
9. Electronic Evidence is not preserved properly in court
10. Cloned copies of hard disks or CCTV footage are not given by experts.
11. Memory card is not preserved by IO
12. Section 65B certificates not properly preserved.
13. Photos of accused are not sent to CFSL experts to compare with images seen in CCTV footage
14. CDs misplaced by IO.
15. Lack of awareness among IO on how to collect electronic evidence
16. Device on which original is stored becomes corrupt.
17. Incase where evidence is contained in a mobile phone due to passage of time till trial witness changes the device.
18. Lack of knowledge and training amongst stakeholders.
19. No training in collection of evidence to the IO.
20. IO does not properly formulate questions to be asked to the Forensic Expert.
21. IO sometimes does not even view the relevant electronic record and unnecessarily attaches the entire storage device like mobile phones, tablets, computers etc.
22. Lack of interest in seizing electronic evidence in Older Police Officers.
23. Difficulty in producing viral videos and audio.
24. No clarity about production of electronic record at the time of bail or arguments before charge.

Next the Police stakeholders were asked a similar question. Unlike the other stake holders an additional category namely Lack of proper SOPS or Rules for investigation of electronic records was added in the options.

Thus Police Personnel were asked to choose from 6 options, namely (1) Limited knowledge of judges and advocates in the field of electronic evidence (2) Want of empanelled experts u/s 45A to prove electronic record (3) Failure of litigant to preserve the original electronic record (4) Lack of proper SOPS or Rules for investigation of electronic records (5) All the above and (5) Others. Their response is recorded as under:

***Table 54***

*Reasons for difficulty in authentication and admissibility of electronic evidence in Court: POLICE*

| Reasons | Response | Percentage |
|---|---|---|
| Limited knowledge of judges and advocates in the field of electronic evidence | 26 | 17 |
| Want of empanelled experts u/s 45A to prove electronic record | 17 | 11 |
| Failure of litigant to preserve the original electronic record | 23 | 15 |
| Lack of proper SOPS or Rules for investigation of electronic records | 78 | 53 |
| All the above | 06 | 4 |
| Others | - | |

*Source: Primary data*

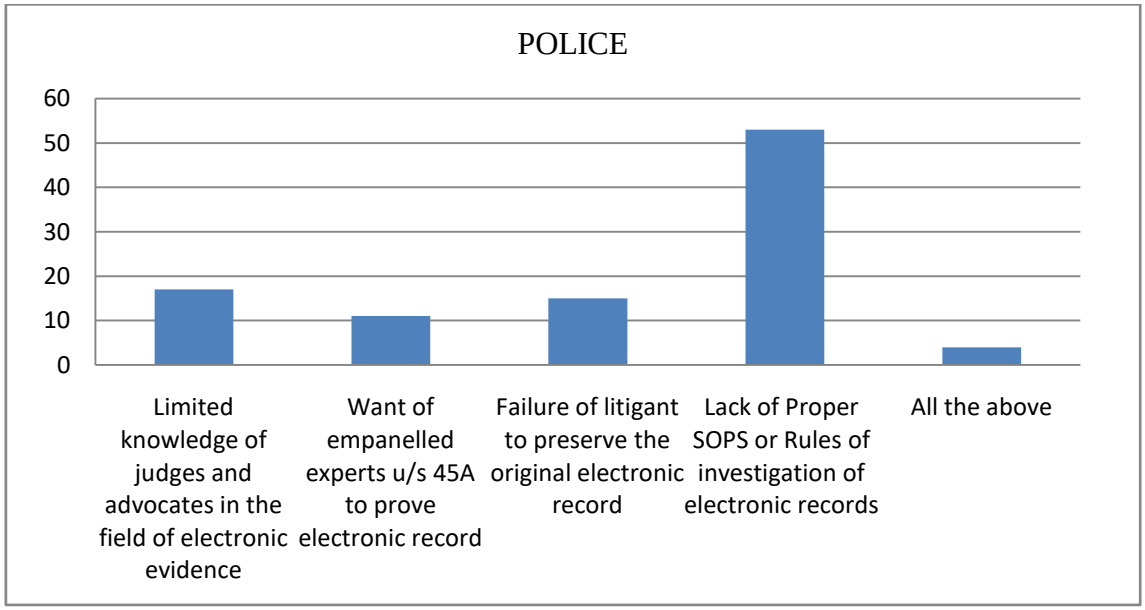



***Figure 44*** *Reasons for difficulty in authentication and admissibility of electronic evidence in Court: POLICE*

Table 54 and Figure 44 reveals that 17% of the Police are of the view that Limited knowledge of judges and advocates in the field of electronic evidence is the reason for difficulty in authentication and admissibility of electronic evidence in Court.11% and 15% respectively consider that want of empanelled experts u/s 45A to prove electronic record and the failure of litigant to preserve the original electronic record are the reasons. 53% of the Police respondents which is a majority believe that Lack of Proper SOPS or rules of investigation of electronic records is the reason. Whereas only 4% are of the view that all the above are the reasons for difficulty in admissibility of electronic evidence. As regards the open ended questions as to the difficulty faced by them in admitting evidence the Police officials have answered as under:

1. Difficulty in obtaining section 65B certificate as third parties do not wish to come to the court.
2. Scarcity of trained staff to assist investigating officer in investigation relating to electronic evidence.
3. Lack of infrastructure facilities for handling cases involving electronic evidence.

4. Some investigating officers are aged and do not have basic computer knowledge and therefore it becomes difficult for them to take up investigation of cases involving electronic evidence.
5. Procedure for production of electronic evidence is complicated which ultimately leads to the court rejecting electronic evidence.
6. Delay in the process of arranging for equipments/Storage devices to retrieve data from the original source.
7. Excessive dependence on computer forensic expert to extract and search for clues from electronic evidence available .
8. No trained officials at the police station.
9. Risk of data breach, tampering and cyber attack.
10. Difficulty in retrieving backup data in the absence of adequate equipment at the police station.
11. All police stations should be provided adequate funds for procuring DVR, spare drives and storage devices which have to be given by the IO to forensic science laboratories to prepare copy of the original electronic record that may be contained in a mobile or a hard disk.
12. Difficulty in obtaining details from internet service providers where the internet service provider has its server located beyond the jurisdiction of the police station or beyond the waters of the country.
13. Police photographers do not give section 65B certificate in time and hence it cannot be produced at the time of filing of charge sheet.
14. When electronic evidence is contained in a mobile or CCTV footage of a private party who is not connected to the matter, the private party is extremely reluctant to hand over the original electronic record.
15. Original electronic record is handed over to a party after extracting a copy there of the party does not take the responsibility of preserving the original as a result it becomes imperative to attach the original.
16. Offences involving molestation and stalking where the complainant is a lady ,the lady is mostly reluctant to hand over her mobile for the purpose of investigation.
17. There are no sufficient computer forensic science laboratories and equipment in Goa and many times the electronic record that is seized has to be sent out of State

**N. Comparative Study on Use Of Electronic Technology And Its Utility:**

One of the hypothesis formulated in this research is that the use of electornic evidence will add clarity to the process of adjudication. In order to test this proposition empirically, the researcher randomly selected 5 sessions cases filed prior to 2019 in the courts of Adhoc District and Session Judge FTC2 Panaji and Adhoc District and Session Judge FTC 1 Margao and assessed the panchanamas produced therein.

It has been the personal experience of the researcher as a judicial officer that with passage of time there is better use of electronic evidence in the process of investigation. On analysis of the files it was noted in majority of the cases filed after 2019 there were photographs clicked at the time of preparing the panchanama as a result there was greater certainty attributed to the panchanama. The empirical research made in this regard is as under:

***Table No. 55***

*Assessment Of Panchanama Produced In Sessions Cases In The Court Of Additional Sessions Judge Margao: Cases Prior To 2019*

| Sr. No. | Case No. | Names of the Parties | Whether the process of conducting panchanama was photographed? |
|---|---|---|---|
| 1. | SC 2.2016 | State v. Pedro Xavier Andrade | NO |
| 2. | SCORS 28.2019 | State v. Gulshan Bi@Resham Khan | NO |
| 3. | SC. 1.2018 | State v. Vinod Prabhu Velgekar | NO |
| 4. | SCORS 5.2017 | State v. Jyoti Dhoble | NO |
| 5. | SCORS 18.2016 | State v. Joaquim Peixeto | NO |

*Source: Primary data*

***Table No. 56***

*Assessment Of Panchanama Produced In Sessions Cases In The Court Of Additional Sessions Judge Margao: Cases after 2019*

| **Sr. No.** | **Case No.** | **Names of the Parties** | **Whether the process of conducting panchanama was photographed?** |
|---|---|---|---|
| 1. | SC 11.2022 | State v. Kishan Kalangutkar | Yes |
| 2. | SCORS | State v. Deepak Kumar | Yes |
| 3. | SC 3.2020 | State v. Nagraj Naikar | Yes |
| 4. | SC 2.2021 | State v. State v. Samuel Jhonson | Yes |
| 5. | SC 10.2020 | State v. Omkar Patil | Yes |

*Source: Primary data*

***Table No. 57***

*Assessment Of Panchanama Produced In Sessions Cases In The Court Of Additional Sessions Judge Panaji: Cases Prior To 2019*

| **Sr. No.** | **Case No.** | **Names of the Parties** | **Whether the process of conducting panchanama was photographed?** |
|---|---|---|---|
| 1. | SC 2.2016 | State v. Sameer Sarkar | NO |
| 2. | SC 15.2013 | State v. Sebastaio Fernandes | NO |
| 3. | SC. 21.2012 | State v. Guruprasad Kurtikar and ors | NO |
| 4. | Sessions Case No. 52/2018 | State v. Shital Subba | NO |
| 5. | SC 11.2011 | State v. Rajendra Harmalkar | NO |

*Source: Primary data*

***Table No. 58***

*Assessment Of Panchanama Produced In Sessions Cases In The Court Of Additional Sessions Judge Panaji: Cases after 2019*

| **Sr. No.** | **Case No.** | **Names of the Parties** | **Whether the process of conducting panchanama was photographed?** |
|---|---|---|---|
| 1. | SCORS 47.2021 | State v. Pooja Kharde | Yes |
| 2. | NDPS 21.2021 | State v. Prakeet Pillai | Yes |
| 3. | NDPS 8.2021 | State v. Azrudeen Achi | Yes |
| 4. | NDPS 10.2021 | State v. Vinod Kumar Sharma | Yes |
| 5. | NDPS 39.2021 | State v. Mikel Okoro | Yes |

*Source: Primary data*

A scene of offence panchanama depicts the position or state of affairs at the scene of an offence. The CrPC does not contain any provision that necessitates a panchanama or depicts the manner in which it is to be conducted. A panchanama is ordinarily conducted n the presence of two respectable persons called panchas who narrate what they saw at the scene. Ideally if this narration is accompanied by photographs of the scence of offence there will be greater clarity about the facts relevant to the case. Table 55,56, 57 and 58 indicate that in contemporary times panchanamas are accompanied by photographs as a result it is easier for the court to appreciate evidence and unnecessary cross examination that is conducted to prove that the pancha witness was never present at the scene is avoided.

Thus in this chapter the researcher attempted to ascertain answers to questions that would serve as the basis of proving or disproving the hypothesis. In analysing whether the hypothesis is proved the researcher has to conduct comparative study of some responses given by various stake holders. The analysis of the responses have given a edifice for construction of a theory based on the hypothesis coined in this research.

In the second part of this chapter, the researcher has analysed the substantive issues that the court is confronted with in dealing with electronic evidence. As stated earlier section 65B forms the bedrock of the law relating to electronic evidence. However section 65B is found to pose challenges in its interpretation. As a result the evolution on law on its applicability has a chequered history. At the outset in this part of the chapter the researcher looks at the impediments in the application of substantive law on electronic evidence.

### 5.3.3 Practical Challenges at Appreciation of Evidence Stage

In this part of the chapter the researcher with the help of doctrinal research has critically analysed the challenges in appreciation of electronic evidence and what in the humble view of the researcher is the lacuna in the existing laws. This part of the research is conducted using inputs obtained from various stake holders, judicial precedents and the personal experience of the researcher as a judicial officer.

As is noted above, in order to admit a copy of an electronic record, procedure prescribed under section 65B has to be followed. Section 65B however has some shortcomings which in the humble view of the researcher need to be properly addressed. These short comings are elucidated as under:

A. **Challenges in admission of copy of electronic records namely.**

**1. Lack of accountability:**

The stakeholders with whom the researcher interacted were of the view that law does not require that a certificate under section 65B has to be on an affidavit as a result there is not accountability to what the maker of the certificate certifies. Even if it is shown that a false statement is made in the certificate there is no mechanism by which the person making the statement can be held liable.

The counter argument to this is also that most cases the certificate is tendered in evidence by a witness who takes an oath. Likewise the law makes production of false

document as evidence in court an offence. Therefore in case it is found that a statement in the certificate is incorrect the court can resort to any of these provisions and penalize the author of the certificate.

The researchers agrees with the later however it is also correct that has the legislature added that the certificate under section 65B had to be made on an affidavit there would have been greater sanctity and a sense of responsibility upon the maker. Most of times the persons giving the certificates are lay persons and they are not aware consequences as aforesaid. Had the legislature made the issuance of certificate under oath mandatory the persons giving the certificate would have ensured that it is properly given.

**2. No clarity as to who has to give the certificate**

Section 65B does not contain any clarity as to who has to give certificate. In order to understand this paradox section 65B(4) becomes crucial. Section 65B (4) gives a checklist of things that the certificate must contain.

Clause a) provides that the electronic record has t be identified and the manner in which it was produced has to be described.

Clause b) provides that the particulars of any device involved producing the electronic record have to be given

Clause c) of Section 65B provides that the certificate can be given by a person who occupies a responsible official position in relation to

(a) the operation of the relevant device OR
(b) the management of the relevant activities

Here the word "relevant device" and relevant activities becomes crucial. The term device occurs in sub clause (4) earlier and is used to mean the device that was *"involved in the production of that electronic record"*. Thus the brief description of the process by which the original electronic record was produced and the details of the device used for its production will have to be given by the person who produced the original and who has the lawful custody of the original. The sub clause further requires that the certificate

must contain details of the conditions mentioned in sub-section (2) of section 65B.

The section further uses the term “whichever applicable”. This would mean that the certificate can be given by a person who is in possession of the relevant device or relevant activities. This person may not be the same.

If the process of producing the original electronic record and generating a computer output is done by one and the same person there will not no difficulty. What happens when the process is done by two different persons. The person who generated the electronic record is different from the person who printed it?

For example A clicks photographs of the site and takes the memory card of the camera and gets the photos printed from B at his photo studio. In this case the details of the manner in which the electronic record is produced, and the particulars of the device will be to the knowledge of A, the conditions pertaining to the computer generating the computer output will be to the knowledge of B. The question is whether two certificates are required to be given in such a case.

The researcher asked majority of Judicial Officers and they have responded by stating that they have never come across a case where two certificates have been given by a party relying upon such copies of electronic records which have been generated by one person and the computer output is produced by another.

Apart from the response given by the respondents, it is noted that section 65B(4)(c) uses the conjunction “OR” and not “AND” which would mean that in the illustration above either the person producing the original electronic record or the person producing the computer output can give a certificate. This is the paradox as the latter cannot certify the process and the device used for generating the original and the former cannot certificate about the condition of the computer that was used to generate the computer output. The researcher is of the view that the conjuction “OR” must be omitted and there must a a clear provision to deal with the eventuality where the person generating the original and the computer output are two different persons.

3. **Law does not insist on lawful possession of the original record.**

When a electronic record is generated by an electronic process this record is the original electronic record. This record will have its distinct characteristics and a unique hash value. This original electronic record may thereafter be (a) printed on a paper or (b) stored, recorded or copied in optical or magnetic media. Section 65B deals with the later. However it nowhere requires the person giving a certificate under section 65B to certify that the computer output is of the original electronic record. It may be argued that section 65B(4)(a) makes identification of the electronic record and description of the manner in which it was produced mandatory nonetheless the provision further says that the certificate is to be " best of knowledge" in other words section 65B does not impose any liability or responsibility on the maker to certify that he is aware that the electronic record is original.

**4. Section 65B uses the phrase computer output instead of copy.**

Section 65B of the Indian Evidence Act uses the phrase computer output instead of copy. These are two different phrases having two separate meanings. There is no clarity as to why the legislature uses this phrase "computer output".

**5. The section does not prescribe the stage at which certificate is to be produced.**

Section 65B of the Indian Evidence Act makes it imperative to produce a certificate in case secondary electronic evidence is intended to be produced. However the section does not prescribe the stage at which the certificate is to be produced. It may be argued that there are precedents that have held that a certificate under section 65B of the Indian Evidence Act can be produced at any stage even at the time when the computer output is tendered in evidence. Respectfully stated some stakeholders are of the view that delay in production of certificate may sometimes cause the court to rely on inadmissible evidence earlier on in the trial which causes grave prejudice to the accused. The best way out therefore would have been to provide a stage for production of the certificate in law.

**6. Section 65B may be a redundant provision**

Section 65B of the Indian Evidence Act was introduced after the enactment of the Information Technology Act. The Indian Evidence Act classified documents as primary and secondary. Secondary documentary evidence are essentially in the nature of copies and if section 63 of the Indian Evidence Act is read, it makes copies of the original produced by a mechanical process that ensures the integrity of the original to be intact as admissible.

Here we were now confronted with electronic records which were now classified as documentary evidence. The legislature thought it fit to create a new category of rules of evidence that would make secondary documentary evidence of electronic records admissible. This led to the enactment of section 65B of the Evidence Act. This section requires that when a copy ( which the section calls a "computer output") is produced it must be accompanied by a certificate under section 65B. However if section 65B is read it is seen that the section only requires details of the device by which the electronic record is produced and the details of computer and its working by which the computer output was generated. Both these aspects do not throw any light or cast any responsibility on the integrity of the computer output vis a vis the original record. It may be argued that section 65B only pertains to the aspect of admissibility and not mode of proof. However when section 65 simplicitor can make copies of paper documents produced by a mechanical process admissible in evidence, could the legislature not use the same phrase "mechanical process" and make the copy of an electronic record admissible in evidence. The difficulty in admitting a copy of electronic record arises from the inability of a human mind to discern whether the copy has been tampered with. The researcher is of the opinion that section 65B does not in anyway aid in ruling out any tampering.

Some stakeholders have argued that Section 65B describes that "mechanical process" rather then using a vague term and fixes responsibility on the person who carries out that process. The researcher respectfully differs from this argument. The reason being, the person who certifies the conditions under section 65B(2) is not required to know or state whether the electronic record whose copy(computer output) he has prepared is the

original record. This observation is made in the light of the fact that section 65B does not require that the person generating the original electronic record and the computer output has to be one and the same person.

Therefore in view of the researcher since section 65B only relates to admissibility and nothing else description of the process by which the computer output is prepared is a redundant exercise and section 65B needs to be omitted. It is pertinent to note that section 65B was borrowed from the English law. However the original English statute has abrogated that section as being redundant.

B.**Existing Law Does Not Emphasize On Authentication And Integrity Rather Law Uses Conventional Phrases Like "Admissibility" And Mode Of Proof.**

Section 65B of the Indian Evidence Act deals with admissibility of electronic records. It is well settled that admissibility is distinct from mode of proof in as much as it pertains to the ease of producing a copy rather than the original. The reluctance to admit an electronic record, whether a original or a copy stems from the belief that electronic records can easily be tampered and the tampering of records may be such that they cannot be discernable to human eye. Unlike paper documents it is very difficult to distinguish between a original and a copy of an electronic record. Section 65B nowhere assists the court in overcoming this hurdle. This is because the person certifying the conditions under section 65B(3) need not have the knowledge that the copy (computer output) he is generating is actually of an original record. This particularly comes into play where the person producing the original record and the person producing the computer output is not the same.

Whereas to affirm the integrity of the original electronic record the only full proof mechanism is the one that is prescribed under section 45A of the Indian Evidence Act. Section 45 A of the Indian Evidence Act like its preceding section only pertains to opinions. And as is observed by the researcher in the foregoing chapters the opinion is a weak form of evidence. Interestingly section 45A does not use the word integrity or authentication it uses a omnibus phrase " form an opinion on any matter relating to any

information".

The researcher is of the view that the legislature has to enact a mechanism whereby there is a clear mechanism prescribed for authentication and certification of integrity of the electronic record produced, whether or not the record is original or a copy. There need not be unnecessary emphasis on admissibility.

The second aspect is mode of proof. When we talk about mode of proof we mean to the proof of the fact that the document was executed. And thus a question arises as to who has executed that document. Once the authorship of the document is fixed the document is said to have been proved by law.

Unlike conventional documents, an electronic record may have to pass the hurdle of authentication before its authorship is fixed. Therefore a person may admit of sending an electronic record but not of the kind as is produced in the court. He may allege that the electronic record is tampered. Illustratively stated a person may admit that he has sent an email but would deny that it is the same email that is produced in court.

By the time the objections are assessed and raised before the court the original may be lost. To offset such eventualities there must be emphasis on authentication and integrity.

C. **Does Not Tackle The Issue Of Issuance Of Certified Copies to The Accused.**

It is now well settled that electronic records are documentary evidence. Necessarily therefore a party is entitled to apply for copies of the same. There is no mechanism to certify the correctness of the copy that is issued. In other words there are no SOPs or rules enacted in this regard. Section 207 of the CrPC directs the police to furnish copies of the chargesheet to the accused, it is well settled that the accused may even apply for a cloned copy. However, the court does not have any mechanism to issue certified copies of any original electronic record if produced in court.

**D .No Emphasis On Preservation Of Original**.

Electronic evidence is classified as that kind of evidence which cannot be easily movable to the court. Therefore the emphasis is on producing it on a more readable format. This is possible for that electronic record which can be printed on paper. For example any form of written text and still images. Other forms of electronic records such as voice recordings and videos cannot be printed on paper. In such a case this evidence is produced either on a memory card or on a CD.

If computer output (copy) stored, recorded or copied in optical or magnetic media it is essentially done in electronic form and meta data of the information so copied can be available for future purposes. However no sooner the information is printed on paper it is of no use for any future analysis. Computer forensic experts have opined that original is a must for giving any opinion as to tampering of records. Ordinarily the stage at which section 45A is invoked may come many years after the production of the original. In such a case original may be either lost or may not be functional or accessible on account of non usage or improper storage.

No responsibility could be fixed on any person as the law does not make preservation of the original mandatory. Likewise in a civil suit before a district court in Panaji the plaintiff has relied upon CDs containing recording of an event that was alleged to have been conducted in violation of the copyright law. The original memory card on which the event was recorded was lost. Objections were raised to the production and authenticity of the copies that were produced in the court. Since the original memory cards were not produced it would not be possible to send the CDs on which copies were made for forensic analysis.

Thus there needs to be law that would emphasise on preservation of original electronic record.

**E. Electronic Record Cannot Be Classified As Documentary Evidence but may also be a material object.**

One of the hypothesis raised in this research is that electronic evidence is a new breed of evidence that requires a specialized law. In the year 2000 electronic records came to be classified as documentary evidence; however the legislature continued to maintain the distinction between electronic records and document. Section 2(e)[303] of the Indian Evidence Act defines a document as any matter that is expressed or described upon any substance. This expression can be by means of letters, figures or marks and which is intended to be used for the purpose of recording that matter .Whereas electronic records are defined as **data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche**. The word documentary evidence is defined as a part of the term "Evidence"[304] under section 3 of the Indian Evidence Act so as to mean and include all documents including electronic records produced for the inspection of the Court literally speaking "Documentary evidence" as a phrase presupposes that the evidence in essence has to be in the nature of a document that is why the legislature has added there phrase "including electronic record" and not and "electronic records". This is where the anomaly lies as one fails to understand the reason of using the word including as a prefix rather then "and". The use of the word including suggests that the intent was to convey a thought that " document" is a genus and electronic records are species.

There is no dispute about the fact that "electronic records" and "documents" are conceptually and fundamentally different. Cynics may argue that they are both used to record or used as record of a matter and hence can be placed in the same genre. The researcher disagrees with this proposition as mere one form of similarity cannot equate electronic records as a form of documents.

---

[303] Section 2(e) "Document". —"Document" means any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter. Illustrations A writing [5] is a document; Words printed, lithographed or photographed are documents; A map or plan is a document; An inscription on a metal plate or stone is a document; A caricature is a document.

[304] Section 3 "Evidence" – "Evidence" means and includes – (1) Oral Evidence – all statements which the Court permits or requires to be made before it by witnesses, in relation to matters of fact under inquiry; such statements are called oral evidence; (2) Documentary Evidence- all documents including electronic records produced for the inspection of the Court; such documents are called documentary evidence.

The fundamental difference lies in the fact that an electronic record is created in one form and made presentable (readable or discernable by human beings) in another form. Whereas a document can be viewed or read or discerned in the same form in which it was created. In the foregoing chapters the researcher has stated in detail the differences between the two and these differences are over whelming.

Likewise electronic records also possess some trappings of oral evidence. Section 59 of Indian Evidence Act requires that oral evidence has to be direct. Section 60[305] provides elucidation as to in what way that evidence has to be direct. It can record facts that can be seen, heard or felt using artificial intelligence(AI) and its accuracy and reliability is much greater if the record is properly produced and proved as per law.

The researcher is therefore of the view that electronic records ought to have been classified as a separate category or a third category of evidence namely and preferably as "electronic evidence". If this is done all the other provisions relating to its production and proof can be streamlined. Also there shall not be any unwanted issues of overlapping.

### 5.4 Findings on Hypothesis

The theoretical data and the empirical data discussed herein above have, in conjunction with each other, made myriad revelations. The researcher had formulated the hypothesis based on her exposure to the subject essentially as a judicial officer. However upon interaction with stakeholders and a thorough study of judicial precedents revealed that there are deep and pervasive intricacies to this issue then what meets the eye. Most of the results were as anticipated, however some revelations were startling and conflicting.

---

[305] Section 60. Oral evidence must be direct – Oral evidence must, in all cases whatever, be direct; that is to say –
if it refers to a fact which could be seen**,** it must be the evidence of a witness who says he saw it; if it refers to a fact which could be heard, it must be the evidence of a witness who says he heard it;
*if it refers to a fact which could be* perceived by any other sense or in any other manner, it must be the evidence of a witness who says he perceived it by that sense or in that manner;
*if it refers to an* opinion or to the grounds on which that opinion is held, it must be the evidence of the person who holds that opinion on those grounds:

The researcher also found that on the substantive legal side there is a conflict of opinion especially in the areas which are yet not resolved by any judicial precedents. In the light of the analysis made,the researcher in this chapter has tested the validity of the hypothesis formulated.

**HYPOTHESIS 1**

**There is limited use of methods of investigation using electronic evidence due of lack of information, knowledge and Training.**

In the course of research, as well as drawing snippets from personal experience as a judicial officer the researcher found that there was limited use of electronic evidence in investigation and eventually in the course of trial. Illustratively stated, when any seizure of an object is done from a scene or where the state of affairs in a scene of offence is recorded, the police resort to an archaic practice of drawing a panchanama. A panchanama is a document that describes the process of seizure or the state of affairs at the scene of offence through the narration of persons who are called panchas. These are two random respectable persons having no connection with the offence. After this process is done, the panchanama is proved by examining these persons in court. There is thus complete dependence on their memory, making their testimony subject to thorough scrutiny.

The use of videography or say atleast photography to make such a record instead of a panchanama will give greater precision and certainty to the entire process. The researcher randomly inspected about 100 files 50 in North Goa District and 50 in South Goa District and found that in none of the cases the investigating officer had resorted to videography. However in some files it was seen that the police did click photos of the scene of offence, overall however there was no much enthusiasm to conduct investigation using electronic evidence. Likewise it was also seen that where a fact could be proved by electronic evidence such as CCTV footage, the investigating officers did not show much enthusiasm and interest in attaching the same

Empirically the factum of limited use is indicated by the response of the police that about 50 to more than 50 cases that come for investigation have some kind of electronic evidence involved in it. ( See Table 7 and figure 1). In contrast the response of Judicial Officers, Lawyers and prosecutors in Table 25 and figure 14 *supra* shows that majority of the stakeholders from amongst the Judicial officers, Prosecutors and Lawyers find that there are less then 20% of cases before them that come for trial that have some kind of electronic evidence involved in it. This shows that though there is electronic evidence available or investigation techniques using electronic evidence possible at the stage of investigation, there is no much enthusiasm in the Police to use them, as a result when the cases are finally charge sheeted there is comparatively lesser electronic evidence found in it.

As per the hypothesis formulated the researcher was of the view that this has been happening because of lack of information, knowledge and Training.

The lack of information is revealed from the fact that majority of the stakeholders were less comfortable with electronic evidence in contrast with the conventional form of evidence as is revealed by table No 8 and 9 and figure No.2 and comparative table 21 and figure No.10.

From the empirical data collected in the context of section 65B of the Indian Evidence Act and Section 45 A Indian Evidence Act, it is seen that there still exists a sizeable number of population from each category of stakeholders that did not have proper knowledge of the meaning and import of section 65B of the Indian Evidence Act. Table 26 and figure 15 indicates that 13% percent of Police respondents are not aware of section 65B. Table 27 and figure 16 showed that there are justifiable circumstances under which Judicial Officers have admitted electronic record without certificate under section 65B. Likewise Table 28 and figure 17 and table 29 and figure 18 are indicative of the fact that15% lawyers and 28% prosecutors respectively have produced copy of electronic record without certificate under section 65B.

The law is that no copy of an electronic record can be produced without certificate under section 65B. Section 65 B forms a bedrock of the entire superstructure of electronic evidence. For electronic evidence to achieve the same level familiarity as

conventional forms of evidence it is imperative that every stake holder who deals with this form of evidence has proper clarity about the meaning and import of the same. The data analysis above therefore confirms that there is lack of sufficient information and knowledge amongst stakeholders as regards the importance of section 65B. .

Thirdly, training plays the most crucial role in the process of admissibility and proof of electronic evidence. For there to be proper use admissibility and proof of electronic records every stakeholder has to be given basic training in the subject of technology. This training may be basic or elementary but it is imperative that 100% of the stakeholders have to be trained. Table 43, 44 and figures 32 and 33 revealed that there is no much emphasis on this aspect in respect of Police Personnel. Comparatively the judiciary have fared better in contrast with the police as is indicated table 45 and 46 and figures 34 and 35.

However it seems from the data shown in table 47 and figure 36 that there is no emphasis laid in training prosecutors on the subject of electronic evidence and cyber crimes. For electronic evidence is to be used more frequently and rampantly in investigation it is necessary that the horizons of knowledge of the stakeholders are broadened with the help of training.

Thus the empirical data above justifies the hypothesis drawn and hence hypothesis No.1 stands proved and validated.

**HYPOTHESIS 2**

**The present rules of procedure are obsolete and do not contain a full proof mechanism for making optimum use of electronic evidence.**

The rules of procedure referred to in these hypothesis above refer to rules of procedure relating to seizure, preservation and authentication of electronic records before they are tendered in evidence. Electronic evidence being more vulnerable to tampering and being difficult to discern without the assistance of technology there needs to be specialised rules of procedure that can guide the investigating officers in the process of search and

seizure. Experts have stated that the process or seizure and copying of the data is very crucial to determine its integrity. There is thus a pressing need to have a common legislation, standardised protocols or rules of procedure in this regard.

As noted in chapter 5 the investigating agencies have revealed that there are no such rules or regulations enacted by the Government that would govern the process of search and seizure. This is indicated in table 10 and figure 3 and Table No. 11 the investigating agencies rely on a handbook that does not have the force of law. Likewise the obsolete CrPC which was enacted much before the invention of a computer also does not assist the law enforcement agencies in the matters of search, seizure and preservation of electronic records.

Research further revealed that the criminal and civil manual also does not prescribe any guidelines for handling of electronic records. As a result there is no harmony between the requirement of conventional ways and the challenges of technology. In Table 34 and Figure 23 reveals that about 53% of judicial officers have stated that copies of electronic record are not annexed to the chargesheet as mandated under section 207 CrPC. The investigating officers cite expense of providing storage devices to the Forensic Science Laboratory as one of the reasons.

Table 51 and figures 40 and 41 reveal that majority of the stake holders were of the view that the present law is not equipped to deal with all issues relating to presentation, authentication and admissibility of electronic evidence in court.

Thus the present rules of procedure being obsolete and enacted in an era that did not have computer technology, thus they do not contain a full proof mechanism for making optimum and convenient use of electronic evidence. Hence the second hypothesis stands proved and validated.

**HYPOTHESIS 3**

**There is inadequate infrastructure available in the State of Goa that would assist the law enforcing agencies in proper preservation, production and authentication**

**of electronic evidence in court**

The term “Infrastructure” used in the hypothesis refers to availability of proper material and devices needed for seizure and preservation of electronic records as well as expert availability at the time of seizure and authentication of that evidence. The term also broadly refers to availability of rooms or storage spaces that would assist in ensuring longevity of the data contained in the electronic record.

Majority of the stake holders in unison have agreed that there is no proper infrastructure in the State of Goa that would facilitate optimum use of electronic evidence. Table 37, 38 and 39 and figure 26, 27 and 28 validate this claim.

There is no separate malkhana or mudemmal room for storage of electronic records and the records are kept with other articles and objects at the Police station. Table 35 Figure 24 confirm this proposition. There are no guidelines for filing, preservation and destruction of electronic records either in the Civil or criminal manual. Table 36 and figure 26 shows that if the electronic record other then muddemal is produced it is tagged along with the main file and not kept separately, as a result it is susceptible to damage.

The data obtained from the Goa Forensic Science Laboratory Verna and the Goa Cyber Forensic Science Laboratory reveals that these laboratories are seriously understaffed and there is no scientist who can exclusively deal with matters of cyber forensics.

The case studies taken up by the researcher indicates that due to improper seizure and storage of electronic records a relevant fact has been missed by the court and/ or the trial suffers. In chapter 5 when asked about the difficulties faced, all stake holders have responded to the open ended question by stating that there is no proper Infrastructure in the State of Goa. Hence in order to ensure that an electronic record sufficiently performs its role in proving a fact there must be adequate infrastructure made available for its preservation, production and authentication. There is thus empirical data to support the hypothesis that there is inadequate infrastructure available in the State of Goa that would assist the law enforcing agencies in proper preservation, production and authentication of electronic evidence in court. Hence the third hypothesis stands proved

and validated

**HYPOTHESIS 4**

**Electronic evidence being new breed of evidence require a specialised law of procedure governing and regulating the same and the Amendments to the Indian Evidence Act are cryptic and unfit to cover all cases involving proof of electronic records.**

This part of the research was non empirical and based on critical analysis of the law and the precedents on the subject of electronic evidence. The critical analysis was made based on the researchers own experiences as a judicial officer and the views and opinions of lawyers and other judicial officers. It may be noted that the edifice of criminal law in India is the Criminal Procedure Code, Indian Evidence Act and the Indian Penal Code. All these laws were enacted at a time when the computer was not even invented. When amendments were made to these laws in view of the enactment of the Information Technology Act 2000, these amendments were more in the nature of an SOS. They were essentially borrowed and copied from foreign legislations and needed to stand the test of time and practical use for them to sufficiently deal with all aspects of admissibility and mode of proof of electronic records. These amendments although have substantially provided for a mechanism for admitting and proving electronic records however as the perspective still continues to be of the conventional form of documents, serious problems do arise in this process.

In the of ***Arjun kotkar (supra)*** Hon'ble Justice Fali Nariman has noted the lack of proper legislation on the aspect of admissibility of third party electronic records. This notwithstanding in the course of research the researcher found certain more intriguing issues pertaining to the applicability of the existing law on admissibility and mode of proof of electronic records. These substantive impediments have been discussed in detail in the last part of this chapter where, the researcher has examined the redundancy of section 65B of the Indian Evidence Act at the same time the ambiguities in the same. The researcher has looked at the practical difficulties in enforcing the letter of law and

particular the paradox in matters of third party electronic records. The reluctance to treat data in electronic form as a proof of a fact emanates from the attributes of the electronic record of being vulnerable to tampering. The escalating point here is also that the tampering cannot be detected easily, a law therefore is needed to resolve this issue in the most simplified form, instead it has laid greater emphasis on documenting the process of copying without fixing any liability on the person generating copies to ascertain the authenticity of the record. In other words there is a longwinded provision that is dedicated to admissibility rather than simplifying the process of proof. In so far as the proof of contents is concerned the Indian Evidence Act relies upon regular modes and as a bonus only adds section 45A which is on a similar footing as the existing section 45 which deals with relevancy of an "opinion". It is a matter of common experience that an opinion is not binding. Even here the law requires empanelment of experts under section 45A read with section 79A of The Information Technology Act 2000. Very few agencies have been empanelled as on date thus causing hardship and delay. The law as it stands today does not conveniently and sufficiently address the issue of reliability of electronic record. Case study has revealed that no doubt that most of the electronic record produced in the court as corroborative evidence goes unchallenged after it has passed the test of admissibility, nonetheless there are cases where when the record forms star evidence and it is challenged.

However the hypothesis that the amendments to the Indian Evidence Act are cryptic and unfit to cover all cases involving proof of electronic records is a farfetched proposition. Because if they were cryptic, they would not have been used for the last 20 years in the process of admitting and proving electronic record. Also, the evolution of law relating to electronic evidence which was studied by the researcher with the help of judicial precedents indicates that the courts in India have beautifully expounded the law. Thus electronic evidence being new breed of evidence does require a specialised law or procedure governing and regulating the same and the amendments to the Indian Evidence Act although are extremely useful do not cover all cases involving proof of electronic records. However they cannot be termed as cryptic and hence the fourth hypothesis stands partly proved and validated.

HYPOTHESIS 5

**Proper use and authentication of electronic records will lead to complete demystification of the adjudicatory process ensuring transparency, clarity better accessibility and certainty in evidence.**

For the purpose of analysis the researcher selected two courts to determine how use of electronic records has provided certainty to evidence. The researcher randomly selected 5 sessions cases filed prior to 2019 in the courts of Additional Sessions Judge-2 (FTC-2) Panaji and the court of Additional Sessions Judge-2 (FTC-2) Margao and noted in majority of the cases filed after 2019 there were photographs clicked at the time of preparing the panchanama as a result there was greater certainty attributed to the panchanama.

Electronic evidence despite of being a new intriguing breed of evidence the development of which is at nascent stage, holds the potential of revolutionising the manner in which regular investigations are carried out and facts are produced and proved in courts. This is because when any act is in question is photographed or videographed, it creates a record that is available for posterity. The uniqueness of technology lies in the fact that it records and replicates what has actually occurred. Therefore electronic technology is untouched by the fallibilities of the human mind. As a result it has greater accuracy and trustworthiness as compared to the convention oral evidence tendered through the human agency.

Thus if an electronic record which is classified as documentary evidence is properly tendered and proved in the court it will suffice better in proving a fact in contrast with the traditional modes. Needless to say the human civilization is consumed by technology and effectively every human is prone to technical surveillance in oblivion. Unknowingly we all are leaving electronic footprint that can assist in investigation of crimes and proof of facts related thereto in a simpler, swifter and accurate manner. Proper use and authentication of electronic records will lead to complete demystification of the adjudicatory process ensuring transparency, clarity better accessibility and certainty in evidence.

To assimilate electronic technology seamlessly into the Indian adjudicatory system it is however important to prepare the existing rules of procedure to challenges that technology may pose to the adjudicatory process. Hence the fifth hypothesis stands proved and validated.

In the next chapter which constitutes the finale of the research, the researcher attempts to use the inferences drawn to create ways and means of making optimum use of resources to ensure proper production and proof of electronic record. At the same time a humble attempt is made to recommend legislative changes.

# Chapter 6

# Conclusion and Suggestions

## 6.1 Introduction

The purpose of any research is to operate as a catalyst of change. A researcher only identifies an existing problem and dwells into the root of it to ascertain possible solutions. As a judicial officer, the researcher found that the field of use, admissibility and mode of proof of electronic records is fast growing and a lot of issues have arisen in application of the law in this regard that require a thorough scrutiny and assessment. This assessment was needed to be done with the aid and assistance of the stakeholders who are actively involved in the process of use, admissibility and mode of proof of electronic evidence. Against this empirical data, the doctrinal data through laws, legislations and precedents had to be compared and analysed. That is precisely how the research was designed and has progressed.

## 6.2 Overview of all Chapters

The research was divided into 6 distinct chapters having its distinct and unique flavour.

Chapter 1 of the research served as both a prologue as well as a road map of the entire process of research. The study of the existing literature on the subject of research aided the researcher in assessing the gaps and voids and thus the research ended up being more concise and specific to the production and appreciation of evidence in Goa without unnecessary straying into aspects of cyber laws or the technical and non legal aspect of electronic evidence. It was thus clarified from the very beginning that this research is conducted with the perspective and understanding of the subject of electronic evidence, by a Law student with limitations on knowledge of technology. Thus a conscious effort is made to refrain as far as possible from any technology references.

Chapter 2 commenced with elucidation of the concept of relevancy, admissibility and

mode of proof contained in the Indian Evidence Act and eventually dwelled into the subject of electronic evidence introduced in form of an amendment to the Act. The researcher noted that the amended Indian Evidence Act acknowledged the difficulty in production of electronic evidence in Courts and thus introduced a mode in form of section 65B, to make secondary evidence, as a computer output of electronic record, admissible. The researcher has discussed the nuances of section 65B and its area of operation. It was noted that section 65B has nothing to do with authenticity of the electronic record that is produced and the same is covered by section 45A of the Act. In the latter part of the Chapter the evolution of law on electronic evidence was traced with the help of judicial precedents. It has been noted that although the amendment of the Indian Evidence Act by the Information Technology Act led to issues of interpretations of provisions and practical applications, the judiciary rose up to the occasion and elucidated the manner in which different forms of electronic records could be admitted and presented in the course of trial.

Chapter 3 gave a bird's eye view of the International Conventions and Model laws on electronic evidence and its utility in creating a hustle in the international community, leading to enactments of local legislations. One of such indigenous local legislation was the Information Technology Act 2000 that led to amendments in various Indian statutes that incorporated the word "electronic record" following the word "documents". As the now amended Indian Evidence Act classified electronic record as documentary evidence, the mode of admitting that evidence in secondary form and the procedure for proving it to some extent, was also incorporated into it. As this precisely forms the fountainhead of this research, reference to the Information Technology Act 2000 and its precursor conventions was imperative.

In Chapter 4 the researcher has discussed the evidentiary aspects of electronic evidence by understanding the law or rules of procedures pertaining to its seizure, preservation and production in courts of law. The researcher noted that there are no enacted rules or standard operating procedures in the State of Goa that would assist the law enforcing agencies to properly seize and preserve electronic record. As a result the case studies revealed that there were lapses in the process of production of electronic record in court. The researcher also noted that though admissibility of copy (denoted as computer output

in section 65B) of electronic record was covered by section 65B, for proving the same, members of the bar and judiciary relied on the conventional principles of proof as are enunciated in the Indian Evidence Act. Using participant observation and interview technique the researcher has enlisted the modes in which different kinds of electronic records are admitted and proved. Using valuable experiences of stakeholders elicited by interview technique, the researcher has summarised the general principles of appreciation of evidence that may be specifically applied in appreciation of electronic evidence and precautions to be taken in production of any kind of electronic record.

Chapter 5 is the heart of this research and consists of the empirical study conducted to test the hypothesis formulated. This chapter has been a revelation of trends and views on issues of vital significance. Empirical research revealed some important facts. Firstly, that all the three stake holders have a lesser comfort level with the subject of electronic evidence as compared to the traditional form of evidence, as a result the law pertaining to electronic evidence needs to be examined assessed and implemented in a improvised manner ensuring that all the stake holders achieve the same comfort level to this form of evidence as compared to the conventional form.

In contemporary times more than 50% of the cases have some form of electronic evidence involved in it however by the time chargesheets are filed the quantum reduces to 20%. This shows that despite of electronic record being potentially available at the time of investigation there is reluctance amongst the Police to use it in court at the time of filing of chargesheet. Although the norm is that no copy of electronic record is admitted without certificate under section 65B however, exceptions are when a party against whom record is produced does not object to the same. Whereas a copy of electronic record cannot be produced without 65B certificate on the ground of non availability of certificate under section 65B, most number of stake holders are aware that in order to make copy of electronic record admissible in evidence it is imperative to produce certificate under section 65B. Majority of the judges have stated that there is no copy of the electronic record relied upon by the prosecution given to the accused. Prosecutors responded by stating that the investigating officers don’t give copies. Investigating officers revealed that this is because there is are no sufficient storage devices such as CD or spare hard disks provided at the police station which are

requisitioned by the Forensic Laboratories.

Further it was noted that there is frugal use of section 45A of the Indian Evidence Act. Most police stations in Goa do not have adequate space to store regular muddemal, sometimes the articles are even kept at outposts which are often understaffed, in these circumstances a proper action plan needs to be prepared to ensure that muddemal containing electronic record is properly stored. Minority of respondent judges have stated that the muddemal is preserved kept separately and not tagged along with the main file. The rest have candidly admitted that the electronic record is tagged together with the main file. Majority of the stakeholders have stated that there is no adequate infrastructure available in the State of Goa that would assist the law enforcing agencies in proper preservation, production and authentication of electronic evidence in court. Empirical data on training prosecutors, Police and Judicial Officers obtained shows that there is periodic training conducted for Judicial Officers and Police by their departments, but the Prosecution department comparatively lags behind. In so far as lawyers are concerned there is no systematic training sessions organised for them on this subject. There are seminars and conferences conducted, the participation in which is optional.

In the last chapter No. 6 the researcher has summarised the pith and substance of each chapter above to commence with, based on which the researcher has reached to certain conclusions on the subject of Use, Admissibility and Proof of Electronic Evidence. The Chapter ends with suggestions and recommendations.

## 6.3 Conclusion.

Although the law relating to electronic evidence has been enacted so as to provide mode for its production and authentication, research shows that it has failed to create a water tight full proof mechanism that would ensure seamless process of its production and authentication.

The judiciary in the country has played a heroic role in elucidating the concept of electronic evidence and its applicability to day to day issue. Challenges such as anomalies in section 65 B of the Indian Evidence Act or admissibility of third party electronic records or providing copies of electronic records or preservation of electronic records are concepts that have not been dealt by the existing law and hands the law relating to electronic evidence as it is contain in the Indian evidence act needs to be relocked and reconsidered.

Inferences drawn from critical analysis of the law indicates that the letter of law on the aspect of electronic evidence is flawed in some respects. Section 65B, which attempted to create an element of ease in production of electronic record, by admitting its computer output instead of the original, poses serious challenges of interpretation. The provision does not fix accountability on the person giving the certificate. If the section is literally taken then there may be a requirement of two certificates instead of one. The section does not prescribe the stage at which the certificate is to be given. It does not insist on lawful possession of the original record. Section 65B uses the phrase computer output instead of copy. Existing law does not emphasize on authentication and integrity rather law uses conventional phrases like “admissibility” and mode of proof. The law does not emphasise on preservation of original when infact the original may be needed at the time of trial in case any objections are raised about the authenticity of the electronic record.

The inferences drawn from the empirical research indicate that that the following factors essentially affect the optimum use of electronic records namely, (1) Lack of comfort level, sufficient Knowledge and awareness of electronic evidence (2) Improper understanding and production of certificate under section 65B, (3) Absence of equipment and infrastructure for preservation of electronic evidence.(4) Non Production of copies of electronic record along with chargesheet.(5)Absence of periodical training for lawyers. (6) Absence of SOP for destruction and issuance of certified copies of electronic record by court. (7) Ambiguity and paradoxes in section 65B. (8)Absence of empanelled expert under section 79A of the Information Technology Act in Goa. (9) Absence of SOP or Rules for seizure and preservation of electronic record.

## 6.4 Suggestions and Recommendations

The last chapter is the chapter that culminates the entire researcher and attempts to provide suggestions so as to make optimum use of available resources. In this chapter the researcher has segregated the suggestions and recommendations for each category of stake holders.

In the light of legislative idealism, practical reality has been tested. Chapter 4 and 5 form the heart of this research where the facts and flaws have been revealed and understood. These facts have helped the researcher to test the hypothesis and attain results.

However, stating a problem and verifying its correctness can never be the goal of a research. The larger purpose is always to find a solution. In this chapter the researcher has made an honest and humble attempt to enlist a few suggestions which in the humble opinion of the researcher may facilitate optimum use of electronic evidence with lesser challenges and snags. The recommendations have been divided into three categories namely (1) Recommendations to the Executive. ,(2) Recommendation to the legislature,(3)Suggestions to the Stakeholders,

### 6.4.1 Recommendations to The Executive

The executive wing of the Government has the responsibility of enforcing the law. This can be done through its various departments and instrumentalities. The researcher has identified certain vital areas and has recommended modes in which the executive can aid in optimum and seamless use of electronic evidence.

**A. Standardization of Rules Of Procedure In Handling Electronic Records:**

As is revealed in chapter 5, the investigating officers continue to rely upon training manuals provided to them by training institutes in matters of seizure and preservation of electronic record. These manuals have no authority of law and differ from State to State. Until the legislature legislates and enacts rules in the manner in which investigation

pertaining to electronic records can be done, there is a need to standardize procedures, processes and methods by which electronic evidence is handled at the level of investigation. At the same time there needs to be standardization of the format in which reports are prepared and statements are recorded in matters involving seizure of electronic records. This will go a long way in improving the quality of documentation and production of electronic evidence in courts.

When we talk about standards, experts suggest that the standards should be such that they should not intend to encroach into the discretion of the investigating officer to gather evidence as may be needed against the facts and circumstances of the case. The standards should not be over prescriptive. They should prescribe the bare minimum requirement that is needed in collection of electronic record and its scrutiny and analysis for the purpose of investigation and for the electronic record to be admissible and capable of being proved in the court of law. The intent is to reduce over dependence on cyber forensic experts for the most rudimentary and mundane processes of investigation. These rules may be the kind of standard rules that are found in statutes like the NDPS Act or the Food Adulteration Act. The researcher therefore suggests that these rules should be in line with those prescribed by the above statutes or in the nature of Standard Operating Procedures applicable to all police stations in the State of Goa.

**B. Training of Stakeholders**

The empirical data collected revealed that the stakeholders have been given periodical training on the subject. However considering the special attributes of duties of the stakeholders and their nature of work the researcher has made the following recommendations on the training module.

**i. Segregation of groups of participants based on knowledge of technology**

The stakeholders are from different age groups. They also consists of a population that may have never used a computer in their entire life and the same time a population that was born in the computer era and were introduced to technology at a very young age.

Upon considering the data on training programmes and interviewing the stake holders at the training institutes it seems that the training modules on the subject of cyber laws and electronic evidence does not recognise this segregation rather the emphasis is on training a lott based on their vocation. When the researcher interacted with senior officers nearing the age of retirement, very reluctantly they revealed that they heavily relied on their younger colleagues or even family members to assist them whilst dealing with issues relating to electronic evidence. Training module therefore must be properly prepared so as to bridge this gap between persons having limited knowledge of computers and electronic devices and persons who are fairly proficient. Senior Officers must be first given basic computer training.

**ii. Segregation of groups based on vocation and occupation**

Secondly, it is essential to address the culture of complacency and unwillingness of the stakeholders to acknowledge the rampant use of electronic records and its utility in day to day investigation of cases. The training that is proposed to be administered has to be customized as per the requirement of each stake holder and there cannot be a general template training programs organized for all stake holders as a cluster. In other words when training judicial officers, prosecutors or lawyers emphasis must be on the legal aspect and in training the Police personnel the emphasis must be in the practical aspect of search seizure and production. The researcher has noted from her own experience that the training programs organized for the police rally essentially around the practical aspect, however when trainings are held in National or State Judicial Academies for prosecutors as well as judges the training still continues to lay less emphasis on the evidentiary aspect of electronic evidence and appears to be more technical in nature.

**iii. Organization of experience sharing conclaves and joint sessions**

An antithesis to the above suggestion of segregation is this suggestion for organizing conclaves and joint sessions. Persons who have fair bit of expertise in the field of

electronic evidence or cyber laws need to come together by forming a conclave and conference and discuss the difficulties that are faced in handling electronic evidence. It is from these discussions and conclaves that the creases can be ironed out and the challenges that every technology advancement poses can be effectively handled. Such kind of joint sessions must be restricted only to experience sharing and must not be training sessions presided over by resource persons. They must be jointly attended by all stake holders who shall circulate their issues, problems and questions well in advance. There may be experts to chair such sessions and help resolve issues raised.

**iv. Training in formulating relevant questions for cyber forensic investigation.**

It is seen that when investigation officers seek assistance of cyber forensic experts they do not have proper knowledge about the manner in which questions are to be formulated and referred to the forensic science experts. These stake holders have to be given specific training in this field with the help of field training by forensic science experts. This will assist the court in considering only relevant forensic evidence that is needed to prove the fact in issue and discard unnecessary irrelevant evidence.

**C. Constitution Of Cyber Emergency Response Team.**

A team of computer forensics experts can be constituted who go to the scene of offence and/or may assist investigating officer in matters of seizure and investigation of electronic records. This team will be distinct from the computer forensic experts who operate from forensic science laboratories and examine exhibits which are forwarded to them for the purpose of their opinion..

**D. Involvement Of Forensic Experts From The Very Inception**.

No doubt all stakeholders need to be thoroughly trained on the subject of electronic evidence, nonetheless the limitation of technological knowhow may hamper the process

of introducing the element of impeccability and seamlessness in matters of admissibility and proof of electronic record. For that the researcher suggests that investigations relating to electronic records must necessarily require intervention of three distinct categories of persons at various stages, namely the (i) Digital Investigators (ii) Digital Crime scene technicians and (iii) Digital forensic experts. The researcher has formulated this concept seeking inspiration from the book of Stephen Mason. Stephen Mason[306] in her book electronic evidence at page 54 recognizes three distinct roles that a cyber forensic expert may perform.

(i)Digital Investigators

The first person to have contact with any form of electronic evidence is the investigating officer. Therefore the first category that the researcher proposes is the individual who is responsible for overall investigation of the case who may not have any qualification or degree in computer science. However these should be individuals who have thorough training in matters of search and seizure of electronic records. These persons with the assistance of Crime scene technicians should be able to securely seize electronic records from the scene of offence prepare its copies as is required for the purpose of forensic examination and copies to be given to the court and the opposite party at the time of trial, at the same time prepare proper documentation of seizure and equip themselves to answer all questions that may be asked in the course of cross examination.

The researcher recommends that all police personnel above the rank of ASI should be given basic training in matters of seizure and handling of electronic records and that there is no point giving them extensive training as the technical aspect of investigation can be handled by the second category of persons as suggested below.

(ii) Digital Crime scene technicians

Digital Crime scene technicians are individuals who are responsible for assisting the investigating officer in gathering electronic evidence from the crime scene or otherwise. These persons must have proper training in handling electronic records,

[306] Stephan Mason "Electronic Evidence" Butterworths Law; 2nd edition (26 April 2010)

having a degree in computer science and technology. These persons shall assist the investigating officer in preparing documentation after seizure. These persons should be in a position to answer questions raised by the Investigating Officer that may be connected to the process in which the electronic evidence is extracted or seized. These persons shall be equipped with all instruments that may be needed to extract electronic record and to prepare its cloned copies either for forensic examination or for its production in court. Here it is important to note that these persons may not be computer forensic experts. They can assist the investigating officer in formulating proper questions to be put to the forensic expert. These persons will also insure that they will not be any data loss at the scene of offence or any tampering of electronic record in the process of preparing its copies.

(iii) Digital Forensic Experts.

The third category of persons are forensic digital forensic experts. These persons are experts recognized under section 45A of the Indian Evidence Act and empanelled under section 67A of the Information and Technology Act.The role of these persons will be to forensically examine the exhibits that may be sent to them for analysis.

It may be argued that there is no need of creating two different categories of experts to assist the investigating officer in search in seizure of electronic evidence and those digital forensic experts can go to the crime scene and assist the IO in all matters in which digital crimes scene technicians are proposed to be doing. In this regard the researcher is of the view that not in every case were electronic record is produced, intervention of a digital forensic expert is needed. Such intervention is seen in matters where some latent data has to be extracted from a computer or where there is a doubt as regards authenticity and integrity of an electronic record which may be produced as evidence.

Ordinarily electronic record is produced in evidence without it being subjected to any forensic analysis. The manner in which the electronic record is handled destroys the very purpose for which it is produced. The idea of having a digital crime scene technician is to assist the investigating officer in every case where there is an electronic record used as evidence so that the investigating officer can concentrate on other aspects

of investigation without making mistakes in handling evidence that may require basic knowledge of technology.

**E. Empanelment Of Forensic Science Laboratory In Goa.**

Fortunately there is a forensic science laboratory in Goa however the same has not been empanelled to belong to the category of experts[307] as required under section 79A of the Information Technology Act. It is therefore incumbent upon the Central Government to forthwith recognize at least one forensic science laboratory in every State of India to function as an expert under section 79A of the Information Technology Act and section 45A of the Indian Evidence Act.

**F. Signing Of Mutual Cooperation Treaties With Other Countries So That They Cooperate In Investigation.**

On interviewing investigation officers, the researcher found that the servers of Internet Service Provides or Social Networking platforms are sometimes located in a foreign country. And untill and unless there is something akin to a Mutual Cooperation treaties the countries do not assist in investigation. Signatories to such bilateral treaties are duty bound to provide mutual legal assistance in collecting electronic evidence. No doubt there are other methods like letter rogatories, however existence of a mutual cooperation treaty makes the entire process much faster, simpler and affords greater sanctity to the information provided.

### 6.4.2 Recommendations to the Legislature

**A. Streamlining Production of Electronic Evidence in Civil Jurisdictions in Par with Criminal Jurisdictions**

[307] Section 45A of the Indian Evidence Act.

Electronic evidence maybe relied upon and proved in both civil and criminal cases. As the entire prosecution and investigation in criminal cases is funded by the State, the electronic evidence management process does not impose any financial burden on the parties relying upon electronic record as evidence. However if the authenticity of an electronic record admitted in evidence is challenged in a civil proceedings an issue may arise of financing the entire electronic evidence management process.

Secondly in a number of cases seizure of electronic records is preceded by discovery of the same. In criminal proceedings an investigating officer is equipped with forensic tools that may assist him in discovery of the relevant electronic record or copying the same in a manner which is acceptable by all. Whereas in civil cases it is seen that the party often relies on open source tools to discover or extract an electronic record when the same may not be apparently or evidently found.

Illustratively stated in matrimonial cases it is found that one spouse may restore deleted WhatsApp chats or other social media messages from the mobile phone of his spouse. Since this process is neither legal nor can be documented in a legally acceptable (like panchanama in criminal cases) manner it becomes difficult to prove these WhatsApp chats in the court.

In the research the researcher found one case which was pending in a magistrate court in Panaji whereby in a domestic violence case, the husband of the victim, claimed that the wife had illicit relations with her paramour and he relied upon deleted WhatsApp chats that he had extracted from her mobile using some free to download open source software. The case had not come up for trial as such the researcher could not examine as to how the court dealt with the issue of proof of this electronic record. However upon discussing the matter with the counsel of the party producing the same and the learned judge who handled the matter it appears to the researcher that the process of proof would involve expense and understanding of a much unexplored area. Eventually upon follow up it was learnt that the matter was later transferred to a Mumbai Court

Ordinarily in such cases it was incumbent upon the respondent husband to seek an order from the court directing the applicant wife to surrender her mobile soon after the case was filed. This would have assisted the court to preserve the original electronic record

in the same form as was contained in her mobile. The existence of the original electronic record is a must for determination of the authenticity of the copy if the same is alleged to be fabricated.

Hence it would be safe to conclude that in criminal jurisdictions it is much easier to produce and prove electronic records as compared to civil jurisdictions. Thus making the need of a standardized legal protocol common to both civil and criminal cases much more pressing than ever.

**B. Preservation Strategies and Time Factor.**

Ordinarily a trial in India takes a very long time to conclude. In this process any evidence which is perishable may not be available at a time when it is produced and tendered through a witness. Electronic evidence is no different. It is often noted that the time gap between electronic discovery and legal process becomes so long drawn that if the investigating officer has seized the original electronic record and he purports to produce the same through a witness in the course of a trial, then it is often seen that by the time the witness enters the witness box the original electronic record deteriorates and is rendered unusable. It is therefore essential to devise a strategy that assists in preservation of the original record or certifies the authenticity of the electronic record before the same is tendered in evidence by the witness.

This can be done by making necessary amendments in the law that requires relevant functionaries to build a clean and separate malkhana or mudemal room with proper cooling facilities to store electronic records. These rooms shall be periodically manned and checked by forensic technicians who shall time to time verify the health of the original electronic records. Secondly, the Criminal Manual and Civil Manual prescribes the manner in which the record has to be filed in A B C category. The researcher recommends that the civil and criminal manual should be suitably modified to provide for segregation electronic record in magnetic form when produced in the file and its safe handling. This may include directions to the judicial officer that such record may be kept separately instead of being stitched along with paper documents in the file.

Thirdly, it is recommended that the Civil and Criminal Procedure Code be suitably amended to contain directions to complete recording of evidence containing evidence in form of electronic records expediously.

**C. Setting Up Of Digital Notary System**

A digital notary system is a concept that may have to be tested with availability of relevant technology and legal restrictions. This is only a concept that is suggested by the researcher to facilitate preservation of electronic record and offset the difficulty that may arise due to its destruction. A digital notary who is a computer expert certifies the authenticity of the electronic record by comparing its copy with the original as a result if the original is destroyed anytime subsequently the copy of the same is available through the digital notary who can certify its authenticity. Through cloud storage such an authority can also be a repository of the authenticated record like regular notaries. Needless to say they will have to be empanelled by enacting a law for that purpose or amending the existing laws.

**D. Enactment of Law Permitting Creation Of Back Up By Court**

The next option in contemporary times is that at a complete basic level the court before which a charge sheet is filed should be legally authorised to create its backup by following a due process of law at the time of committal and the process of creating backup should serve as proof of authenticity of that electronic record. There must be legal recognition given to this process by making necessary amendments to the relevant procedure Codes and Manuals. The presiding officers of the court can take assistance of computer nodal officers who have been appointed in every court as a part of the e-courts project. A backup however can only be created of a copy and not the original record.

**E. Notice to Accused To Admit Contents of Electronic Records**

When the prosecution relies upon an electronic record as a vital piece of evidence which is contained in an article that may be kept and preserved at the malkhana, the accused upon his appearance must be asked to state at the outset whether he disputes authenticity of the same and if he does so before starting the trial the court should have necessary recourse to forensic assistance and start the process of determining the authenticity of the electronic record. Similar process mutatis mutandi can be followed in Civil cases where the defendant appears on the first summons. It is recommended that the CrPC and CPC should be accordingly amended to incorporate this change.

**F. Use of Appropriate Technology by Courts to Preserve Original.**

The law relating to preservation of electronic records as it stands in India today does not distinguish between paper documents and electronic records. Electronic records are therefore tendered, exhibited and preserved in the same manner as paper documents. Due to volatile nature of electronic records it is impossible, at the same time highly risky, to preserve the same, as paper documents in the court. It is therefore suggested that electronic records could be preserved using suitable technology that can protect the documents from being modified or overwritten. Such technology includes creation of mirror images or cloned copies or devising protocols that no longer requires preservation of original and provides a copy to be sufficient evidence of the contents of the original electronic record. For this purpose appropriate amendment needs to be made in the civil and criminal manual. However before that through R&D such technology has to be devised and made readily available. This process is not very difficult as the judicial system has migrated from the typewriter era to computer storage and now to the usage of cloud technology.

**G. Upkeep and Destruction.**

Likewise there is absence of any provision in the civil and criminal Manual laying down the protocol for destruction of electronic records such a CD or pen drives that maybe tagged in the court file. In the absence of such protocol such electronic evidence is destroyed in the same manner as physical documents when the case is disposed off.

CDs, Pendrives and other magnetic devices if not destroyed properly can cause environmental hazard. There are norms set up for destruction of e-waste. Some of it can also be recycled. Hence the researcher recommends that suitable amendments may be made in the Civil And Criminal Manual to effectively cater to the issue of destruction of electronic records.

Secondly, some court records have to be preserved for more then 10 years as per the Civil and Criminal Manual. If such record is in form of evidence in a CD it is technically impossible for the CD to be functional for 10 years. When the researcher discussed this aspect with judicial officers who have functioned as administrative judges having powers to order destruction of records it was a opined that, wherever is permissible the court should be permitted to take a printout of the contents of electronic records in a disposed file before the destruction of electronic records. It is therefore recommended that there should be suitable amendment in law that would permit the court to take printouts from the storage device and preserve the print outs as a record of its contents, along with necessary certificate under section 65 B of the Indian Evidence Act.

## H. Obligation to Certify Under Section 65 B

In the case of ***Arjun Pandit Rao Kotkar(supra)*** the Honorable Supreme Court of India has devised a mechanism has to how third party electronic records can be proved when the party intending to produce the record is not in possession of the original. The Honorable Supreme Court of India has discussed various provisions of the Civil Procedure Code, Criminal Procedure Code and The Indian Evidence Act to hold that the court can resort to various provisions of law and direct the holder of original to produce a certificate under section 65B.However the existing provisions empowers the court to direct a party only to produce an existing document and cannot be stretched to direct a party to create a document in this case a certificate. It is therefore suggested that in case the legislature enacts a provision making it mandatory to the holder of any electronic record to issue copy along with the certificate under section 65B so that the difficulties like the ones encountered in the case of ***Arjun Pandit Rao Kotkar(supra)*** will be offset.

**I. Relooking At Section 65B**

Section 65B was based on the English law enacted in this regard. This provision under the English law stands repealed. In the course of research the stakeholders were of the view that section 65B is a redundant provision as it does not impose any responsibility on the person preparing a copy to check whether the original is tampered or not. Since the copy anyways is prepared by a mechanical process there seems to be no reason why the mechanical process has to be documented in form of a certificate. The only difficulty with electronic evidence is the possibility of it being tampered. Section 65B has nothing to do with tampering of electronic record. Hence certain provisions of section 65B have to be amended or section 65B has to be deleted.

**J. Enactment Of Provision Providing Penalty On Raising False Plea Of Tampering.**

The fact whether an electronic record that it is intended to be proved against a person is tampered or not is a fact within the knowledge of the person who claims that he is not the author of that fact that is sought to be proved by that record and that the record has been tampered with. Tampering of electronic record can be more accurately ascertained as compared to paper documents. However the process also requires as lot of time, expense and expertise. Most importantly it requires the preservation original. Enactment of provision for imposition of penalty when a false plea of tampering is raised and proved in trial will ensure that the instances of such pleas being raised is fairly less and will offer greater reliability on electronic records

**6.4.3 Suggestions to the Stakeholders:**

The stakeholders in the present case include the Judicial Officers; Advocates; Prosecutors and the Police. In the course of the research, the researcher had a threefold encounter with the process followed by these stakeholders in the use admissibility and mode of proof of electronic record. First was a direct interaction either through answers

in form of close ended questionnaires or inform of open ended interviews. Second was an indirect interaction as an observant to the entire judicial process and the third has been a scrutiny of sample size of cases using the case study method.

Based on this threefold interaction the researcher has enlisted her humble and earnest recommendations to the stake holders. This chapter is preceded with a disclaimer that the views expressed herein are from an academician's perspective and shall not be construed as demeaning, disrespecting or criticising any authority, their expertise and wisdom of any of the stakeholders. Being a judicial officer the researcher is mindful of the fact that the actual field work is very different from the theoretical dictates of law and no authority or person can claim to impeccably argue or apply the law. In the light of this the researcher has divided the recommendations and suggestions to the stakeholders into two categories namely (1) Common Recommendations to all stakeholder (2) Individual Suggestions to (a) Judicial Officers and Prosecutors (b) Police (c) Advocates.

## A. Common Suggestions

### i. Proactive and open minded approach.

In the course of the research the empirical data revealed that all stakeholders found greater comfort in dealing with conventional form of evidence then in dealing with electronic evidence. Majority stakeholders also agreed that electronic evidence is a new breed of evidence that requires a specialised law and that the amendments in the law are not adequate in dealing with the challenges. It was also found that the law relating to admissibility and mode of proof of electronic evidence was expounded to a greater extent by judicial precedents then by the existing legislations. Further that the constitutional courts have noted that there are a lot of grey areas which require immediate resolution and intervention by the legislature. This being the case with the existing law rules and regulations on one side and the infrastructure available for its enforcement, the stakeholders are expected to have an open-minded and board approach in handing issues pertaining to electronic evidence as opposed to a pedantic one.

It was until a few years ago that lawyers were found to advise their clients to click photos on old photographic films because the process of its production and admissibility was much easier. This has been the personal experience of the researcher when the researcher was posted on 2010-2013 as a judicial officer in Ponda Taluka of North Goa District.

Further it is seen that the police avoid seizing and producing electronic record presumably because of the tedious process involved in authenticating and preserving it. It is also seen that stakeholders tend to overlook perhaps due to pressure of work the safeguards that need to be followed in producing and admitting electronic record.

The researcher therefore suggests that all stakeholders have to be open minded in reception of technology, make efforts to understand and adopt it as a part of their daily judicial routine. There is the need of accepting that technology is the future and without relying upon support staff, individual stakeholders will have to manoeuvre through it. A pedantic and abhorrent approach will cause more and more errors leaving greater scope for challenge and interpretation.

Secondly, when handling electronic records, whether at the stage of seizure, production or interpretation, all stakeholders must be proactive in ensuring that they make efforts to see that requirement of law is thoroughly complied. Lawyers must advise their clients in matters which require preservation of originals, Judges must take proper precaution to preserve electronic record in court and police must see whether there is any chance electronic evidence available at the site which they can use in investigation rather than keeping away from such forms of evidence.

**ii. Keeping updates about latest development.**

Law relating to electronic evidence has been developed more through precedents and usage. It all started with the courts holding that the certificate under section 65B is not mandatory to prove secondary evidence of electronic record and that it can be proved through the other legal means. Now as the law stands, it is well settled that section 65B

starts with a non obstante clause and therefore the principle of substantial compliance is not applicable to this section. Further the law relating to proof of third party electronic record has also under gone a sea of change. There are a number of precedents where the courts have elucidated the manner in which different kind of electronic records can be produced and proved. Hence the researcher found that law relating to electronic evidence is in a constant flux. It is therefore imperative for all stakeholders to keep themselves updated about the latest developments in the law and particularly the latest precedents on various points.

The duty is primarily on the lawyers and the prosecutors to guide the court about the precedents on the relevant point of law despite the precedent going against the cause of the party. The Police as well need to thoroughly look at the requirement of law as it was found at the time of case study that invariably there are mistakes in preparing section 65B certificate.

Hence if the stakeholders keep themselves updated and aware of the latest precedents, rules and laws there will be less errors and scope for rejection of electronic evidence.

**iii. Making optimum use of available resources.**

It must be understood that despite of best intent of the executive, legislature and the judiciary, in enactment and elucidation of the law as well as preparation of the infrastructure, there are bound to be gaps as the field of electronic evidence is ever developing. Therefore the endeavour must be to make optimum use of available resources. This is possible by directing the Police to document the process by which seizure is made or to make use of forensic facilities to create back up. The judiciary can also ensure that muddemal containing electronic records is treated in par with valuable muddemal and is properly preserved. The Prosecutors and the lawyers can guide the witness so that proper certificate under section 65B is filed. Best use of provisions relating to admission, notice to admit, interrogatories contained in the Civil Procedure Code and Criminal procedure Code can be made in issues relating to proof of electronic records.

**iv. Active participation in training.**

From the data that has been collected from the various departments it is revealed that there are periodic trainings conducted for all stakeholders. This training is either separate for each category or are combined trainings.

The researcher has been both a participant as well as a resource person in these training sessions and has noted that not many participants take initiative in resolving the difficulties that they face in their day to day work relating to electronic evidence. It is recommended that when any stakeholder gets the advantage of attending a training session on the subject of electronic evidence the stakeholder must make best use of it to resolve any practical difficulties that they may have in day to day handling of electronic records.

Furthermore the combined training sessions can also serve as a experience sharing platform whereby one stakeholder can guide or mentor the other so that due to effective communication, some commonly encountered errors are offset. The best possible result from these training sessions can be achieved only upon the active participation of all stakeholders in the course of training.

**B. Suggestions to Judicial Officers and Prosecutors**

**i. Vigilant approach in producing/admitting electronic evidence.**

The prosecutor gets first interaction with any kind of electronic evidence filed in the chargesheet at the time when the chargesheet is filed in the court. Where electronic record is not produced as a material object but has been produced in some secondary form such as CD, Memory card or a printout. The prosecutor must immediately verify whether the electronic record is properly produced and adequate steps have been taken by the investigating officer to admit and prove it before the court. The prosecutor must personally check whether the text of the section 65B certificate is in consonance with

the record produced and whether the correct secondary evidence is produced. In one of the files referred above it was seen that section 65B pertains to a CD and what has been identified by the witness are printed photographs. There was no record of the CD being viewed in the court or the fact that the photographs were printed from that CD.

Also the prosecutor has to see whether the original has been properly preserved and pre plan the manner in which it will be produced in court. Being a judicial officer, the researcher is of the view that this is the primary exercise that has to be done by the prosecutor and it is not the job of the court to go through the file and point out shortcomings at the time of hearing arguments before charge or at any later point of time.

Likewise judicial officers must not blindly accept certificate under section 65B without checking its contents and authorship. The aspect of vigilant approach also includes proper application of law distinguishing between mode of proof and admissibility. An understanding that section 65B only relates to admissibility and not mode proof is imperative infact, to all stake holders.

**ii. Training and sensitisation of staff handling electronic records**

Training has been comprehensively dealt with in the foregoing part of the chapter, where the researcher has suggested modes by which the executive can adopt a training methodology so as to ensure that there is proper dissemination of relevant aspects of handling production and appreciation of electronic evidence. Nonetheless a judicial officer and prosecutors can ensure that they at their level train the staff and investigating officers respectively, on the matters relating to handling of electronic records. The prosecutors particularly at pretrial stage can guide investigating officers on how to extract the best electronic evidence in a form that can be easily admitted and proved in the court of law.

**iii. Directing proper handling of electronic records:**

Judicial officers must ensure that where electronic evidence is produced as a material object it is properly preserved and kept as far as possible safe from contamination. Where electronic records such as CDs are produced, care must be taken to stitch them properly in the file and instructions to that effect have to be given to the concerned staff. Endeavour must be made to record all evidence pertaining to electronic records as expeditiously as possible and necessary instructions to that effect have to be given to the prosecution and the defence. Similar directions must be given by the prosecutors to investigating officers particularly when the records are in the malkhana of the police of the original continues to be in the custody of the police and a copy is produced in the court. The prosecutors must ascertain whether any forensic analysis of the electronic record is needed especially when the case comes to them at the stage of bail and instruct the Investigating officers to do the needful.

**iv. Efforts to improve longevity of electronic record.**

In other to ensure that the original electronic record is available for examination at the time of trial the judicial officers must take effective steps to preserve it properly. In case the electronic record is not a material object (therefore is not sealed and produced as muddemal) the judicial officer can direct its backup to be created by following all safeguards of law. Such an exercise is now approved by the court of law. If CDs in form of secondary evidence have been produced particularly of an audio or video recording the court must insist on a transcript or view the CD at the first available opportunity and make a record of its contents. Where electronic records are produced as material objects the prosecutor must intimate about the same to the court on the day of filing of chargesheet so that proper steps are taken to preserve the record safely.

**C.. Suggestions To The Police**

**i. Thorough knowledge of process of handling electronic record.**

Every police officer who handles an electronic record either in a cyber crime or in a regular crime as electronic evidence. Whatever may be the nature of the crime, it is the duty of the police officer to ensure that the record is handled seized, transported and packed as per some standardised guidelines. The researcher found that in a number of cases valuable electronic evidence was lost or could not be considered on account of improper seizure or proof.

**ii. Documenting the process of seizure or handling of electronic record.**

As noted above electronic evidence is vulnerable to deterioration and corruption. As a result the clues obtained from any audio/video recording may be useful for investigation but the electronic record containing that audio/video recording may have been destroyed due to passage of time and not available for viewing in the court. Or it may so happen that the original record which may form the sole basis for charge sheeting the accused may be pending for forensic analysis and the matter may have to be argued for bail. In such cases a detailed panchanama of what forms the crux of the audio/video recording as seen or heard by the panch witnesses can play a very crucial role in appreciation of evidence.

When the researcher was presiding over the Juvenile Justice Board as the Principle Magistrate, the researcher dismissed the bail application of the juvenile accused by relying upon a detailed panchanama conducted by the Mapusa police whereby the contents of the CCTV footage clearly showing the juvenile chopping off the head of the deceased as described. The original footage was sent for forensic examination.

The second aspect of documenting the process includes making all such notes as may be required of the scene of offence and the equipment containing the electronic record including the time stamps as per practice guidelines described above.

**iii. Making full use of chance electronic evidence**.

The world today is taken over by technology to the extent that every active or passive user of technology has consented to what may be called a unknown technological surveillance. There are CCTVs installed at places which may record happening of a fact. Or the happening may simply be recorded by any witness or passerby armed with a smart phone. The location of a person can be traced from his phone usage using the IPDR, TDR and CDR. Internet of things(IOT) can help ascertain his activities and behaviour. Interaction of a person with technology can provide abundant clues, that may assist the police in determining facts in issue. What is needed is an investigative hunger to make optimum use of these clues. This is what the researcher prefers to call as chance electronic evidence. The researcher started this research in the year 2015 and has noted from her own personal experience the standard of investigation has been raised since the time the investigating officers have resorted to follow the e- trails left by the accused by use of technology.

**iv. Preservation of original.**

The law at its stands today keeps the option open to the party who disputes the authenticity of an electronic record to get the same examined by an expert. Till date there is no stage prescribed for the same and in criminal cases the accused can take the plea much later when the trial commences. Therefore it is the duty of the investigating officer to preserve the electronic record or direct the concerned to do so in case the device containing the original electronic record is released to its custodian.

**v. Exercise of proper discretion in seizure of electronic record.**

In the course of the research the researcher noted irrelevant electronic record is relied by the investigating officer in the chargesheet. Where only a message or a forward must be

attached and produced the mobile has been seized or where a hard disc could be seized the whole computer system is attached. It is therefore recommended that the Investigating officer exercise proper discretion in seizure of electronic record, by first determining its relevancy and thereafter proceed with the process of seizure.

**vi. Preparation of correct 65B certificate.**

The researcher randomly examined about 30 charge sheets where certificate under section 65B was produced and found that in more than 70% of the charge sheets there was a mistake in the certificate given by the police photographer under section 65B. It is recommended that the head of the training wing of the Police Department in consultation with the prosecution can prepare a template for issuing certificate under section 65B and circulate the same to call police stations.

**vii. Training and sensitisation of technologically challenged staff.**

It is seen that there is still a generation of officers in the police department who are technologically challenged. Whereas the newly appointed police sub inspectors have a greater comfort level with technology. Lastly and most importantly it recommended that these younger officers can give bare minimum training or guidance to other officers who are not adequately trained.

**viii. Avoiding unnecessary seizure of device containing electronic record when data can be obtained by other modes.**

In the course of case study the researcher noted that the police seize devices containing electronic record when data can be obtained by other modes. For example to ascertain call records there is no need to attaching a mobile phone. The investigating officers are therefore expected to show prudence and skill in attaching only relevant electronic record.

**D. Suggestions to Lawyers**

**i. Discernment of electronic evidence on the touchstone of relevancy.**

Selection of electronic evidence on the touchstone of relevancy and avoidance of unnecessary electronic record in evidence is most vital. The most important aspect in production of any form of evidence is the quest for determination of its relevancy. The person proving a fact has to prove it with evidence that is relevant on the touchstone of section 5 to 55 of the Indian Evidence Act. For that purpose the fact in issue has to be first determined and only that evidence that is needed to prove the fact in issue has to be produced. Admissibility and proof of electronic evidence is much more tedious as compared to conventional form of evidence. As a result the burden lies on lawyers appearing for the party to discern whether in the facts and circumstances of a given case is it really imperative to produce electronic evidence. It is therefore recommended that every lawyer must check the relevancy of electronic evidence to the matter before it is produced.

**ii. Make efforts to preserve and prove the original.**

It is the right of the party against whom an electronic record is produced to dispute its authenticity. Notwithstanding the issue of burden of proof, the original record may be required to be subjected to analysis by expert under section 45A of the Indian Evidence Act. In such a case it is recommended that the lawyer appearing for the party must instruct the part to take all possible efforts to preserve the original electronic record so that as and when required the same can be produced in the court.

**iii. Sensitize the party/witness on the basic principle of law relating to production of electronic record.**

It is further recommended that lawyers must sensitize the party/witness on the basic

principle of law relating to production of electronic record as the process of production is principally different from conventional form of evidence. It is often found that a party is under an impression that when they produce printed photographs or audio video recording on a CD the electronic record on the original hard disk or the memory card can be deleted. It therefore becomes the duty of an advocate appearing for the party to give basic information about both admissibility ( section 65B) and mode of Proof.

# Bibliography

## BOOKS


1. Stephan Mason, *Electronic Evidence, Second Edition*, (Asian reprint), LexisNexis,2010.

2. Sarkar's, *Law of Evidence*, Lexis Nexis Butterworths, 2014.

3. Biswas Chaterjee, *Electronic Evidence*, Asia Law House 2nd Edition 2015.

4. C R Khotari & Gaurav Garg, *Research Methodology Methods and Techniques*, New Age International Publishers, 3rd Edition, 2014.

5. Anirudh Rastogi, *Cyber Law and Law of Information and Technology and Internet*, Lexis Nexis, September 2014.

6. Ratanlal Dhirajlal, *Law of Evidence*, Lexis Nexis, 23rd Edition, March 2014.

7. Batuklal, *Law of Evidence*, Orient Publications, 7th Edition, January 2015.

8. Nayan Joshi, *Electronic Evidence*, Kamal Publishers; 2017 Edition.

9. Pavan Duggal, *Judicial And Practical Approaches To Electronic Evidence Law In India*, Kindle E-Book .

10. Anthony Reyes, *Cyber Crime Investigations: Bridging the Gaps between Security Professionals, Law Enforcement and Prosecutors* Syngress Publishing Inc. 2007.

11. N S Nappinai, *Technology Laws Decoded*, Lexis Nexis, 2017 Edition.

12. Vikram Singh Jaiswal and Shweta Jaiswal, *Cyber Crime and Information Technology Act 2000*, Regal Publications; 1st edition ( May 2014)

13. V Rajaram, *Introduction to Information Technology Act* , PHI Learning Pvt. Ltd. 2013.

14. Prashant Mali, *Cyber Law and Cyber Crimes*, Second Edition, Snowhite Publications, 2016.

15. Dr. Gupta and Agrawal, *Electronic Evidence,* Premier Publishing Company 1st Edition 2018.

16. Ram Jethmalani & D S Chopra, " The Law of Evidence, Commentary on Evidence Act 187 West Thomson Reuters, 2016 edition.

**ARTICLES**

1. Hasit B. Seth, *Impossibility Exception to the Section 65-B(4) Electronic EvidenceCertificate*,(https://www.scconline.com/blog/post/2021/06/05/impossibility-exception-to-the-section-65-b4-electronic-evidence-certificate/)

2. Ajay Bhargava , Aseem Chaturvedi , Karan Gupta and Shivank Diddi, *India: Use Of Electronic Evidence In Judicial Proceedings*, (https://www.mondaq.com/home/redirect/1487178?mode=author&article_id=944810&location=articleauthorbyline)

3. Pragnya Vashista, *Admissibility of electronic evidence in India*, (https://independent.academia.edu/PragnyaVasishtha?swp=tc-au-19223450)

4. Adv Prashant Mali, *Digital or Electronic Evidence in Indian Law or in Indian Courts*, (http://www.slideshare.net/cyberlawconsulting/electronic-evidence-digital-evidence-in-india)

5. Tejas D. Karia, *Paper on Digital Evidence an Indian Perspective*, (http://sas-space.sas.ac.uk/5368/1/1872-2608-1-PB.pdf)

6. Justice Raja Vijaya Raghavan, *Collection, Preservation & Appreciation Of Electronic Evidence*,(https://nja.gov.in/Concluded_Programmes/2021-

22/P1284_PPTs/3.Collection,%20Preservation%20&%20Appreciation%20of%20Electronic%20Evidence.pdf)

7. Tejas Kharia, Akhil Anand, Bhahar Dhawan, *The Supreme Court of India re-defines admissibility of electronic evidence in India*, (https://www.researchgate.net/journal/Digital-Evidence-and-Electronic-Signature-Law-Review-2054-8508)

8. Priyansh Raghu, *Admissibility Of Electronic Evidence With Special Reference To Instagram Chat* (https://www.legalserviceindia.com/legal/author-48246-priyansh-raghu.html)

9. Gokul Sundar K Ravi, *Relevancy of Electronic Records and its Admissibility in Criminal Proceedings*, (https://tndalu.academia.edu/GokulSundar?swp=tc-au-14343081)

10. Prem Pratap Singh Chauhan, *Recent trends in admissibility of electronic evidence: challenges for legal fraternity* (https://ujala.uk.gov.in/files/15.pdf)

11. Naman Jain, *Admissibility of E-evidence in India: An Overview* (https://papers.ssrn.com/sol3/cf_dev/AbsByAuth.cfm?per_id=4595799)

12. Sakshi Shairwal, *Judicial Interpretation Of Section 65B Over The Years* (https://www.lexology.com/1267187/author/Sakshi_Shairwal/)

13. Ranjan, Prabhat, *Resolving the Conundrum of Requirement of Certificate Under Section 65B of Indian Evidence Act, 1872*. (http://dx.doi.org/10.2139/ssrn.3735354)

14. Bhavyakirti Singh and Aditya Bamb, *The Dichotomy of the 65B Certificate* (https://doi.org/10.12728/culj.18.4)

## STATUTES, CONVENTIONS, MANUALS AND SCHEMES


1. Criminal Procedure Code, 1973
2. Indian Evidence Act, 1872
3. Indian Penal Code, 1860
4. Information Technology Act 2000
5. Bankers Book Evidence Act 1891
6. Criminal Manual
7. Civil Manual
8. UNCITRAL Model Law On Electronic Commerce 1996
9. UNCITRAL Model Law on Electronic Signature 200
10. United Nations Convention on the Use of Electronic Communications In International Contracts
11. The UNCITRAL Model Law on Electronic Transferable Records, 2017
12. ISO/IEC 27037:2012; Information Technology — Security Techniques — Guidelines For Identification, Collection, Acquisition And Preservation Of Digital Evidence
13. The ACPO Good Practice Guide for Computer Based Evidence
14. Electronic Crime Scene Investigation: A Guide For First Responders: The U.S. Department Of Justice (USDOJ, 2001)
15. CBI (Crime) Manual, 2005
16. Cyber Crime Investigation Manual (DSCI-NASSCOM)


## WEBLIOGRAPHY


1. www.academia.edu
2. www. scconline.com
3. www.indiankanoon.com
4. www.livelaw.com
5. https://districts.ecourts.gov.in
6. www.mondaq.com
7. www.slideshare.net

8. www.nja.gov.in
9. www.researchgate.net
10. www.legalserviceindia.com
11. www.ssrn.com
12. www.lexology.com
13. www.researchgate.net
14. www.main.sci.gov.in
15. https://www.meity.gov.in
16. www.indiacode.in.in
17. www.uncitral.un.org
18. www.manupatra.com

# Annexure 1.

## Notification of Forensic Laboratories as Examiner of Electronic Evidence under Section 79A of Information Technology Act 2000

| Sr No. | Name | Address | Scope |
|---|---|---|---|
| 1 | Forensic Science Laboratory, New Delhi | Sector 14, Rohini, New Delhi under Government of National Capital Territory of Delhi, | (a) Computer (Media) Forensics excluding Floppy Disk Drive; (b) Mobile Devices Forensics. |
| 2. | Computer Forensic and Data Mining Laboratory, New Delhi | New Delhi, under Serious Fraud Investigation Office, Ministry of Corporate Affairs,. | Computer (Media) Forensics excluding Floppy Disk Drive. |
| 3. | Directorate of Forensic Science, Gandhi Nagar | Gandhinagar Gujarat | (a) Computer (Media) Forensics; (b) Mobile Devices Forensics. |
| 4. | Central Forensic Science Laboratory, Hyderabad | Hyderabad, under Directorate of Forensic Science Services, Ministry of Home Affairs | (a) Computer (Media) Forensics excluding Floppy Disk Drive; (b) Mobile Devices Forensics. |
| 5. | State Forensic Science Laboratory, Bangaluru, | Madiwala, Bangaluru, | (a) Computer (Media) Forensics |

| | | | |
|---|---|---|---|
| | | Karnataka under Directorate of Forensic Sciences, Karnataka, Police Department | excluding Floppy Disk Drive; (b) Mobile Devices Forensics. |
| 6. | Cyber Forensic Laboratory, under Army Cyber Group, New Delhi | Signals Enclave, Rao Tula Ram Marg, New Delhi under Directorate General of Military Operations | (a) Computer (Media) Forensics excluding Floppy Disk Drive; (b) Mobile Devices Forensics. |
| 7. | Regional Forensic Science Laboratory, Northern Range | Dharamshala, District- Kangra (Himanchal Pradesh | (a) Computer (Media) Forensics excluding Floppy Disk Drive; (b) Mobile Devices Forensics. |
| 8. | Cyber Forensic Laboratory, Indian Computer Emergency Response Team (CERT-In), New Delhi | Electronics Niketan, 6 CGO Complex, Lodhi Road, New Delhi | (a) Computer (Media) Forensics excluding Floppy Disk Drive; (b) Mobile Devices Forensics. |
| 9. | Cyber Forensic Laboratory, Air Force Cyber Group, New Delhi. | New Delhi | (a) Computer (Media) Forensics excluding Floppy Disk Drive; (b) Mobile Devices Forensics |

| | | | |
|---|---|---|---|
| 10. | Cyber Forensic Division, State Forensics Science Laboratory, Kerala | Vellayambalam, Thiruvananthapuram Kerala, | (a) Computer (Media) Forensics excluding Floppy Disk Drive; (b) Mobile Devices Forensics. |
| 11. | Cyber Forensics Laboratory, Navy Cyber Group, New Delhi | Talkatora Annex, New Delh | (a) Computer (Media) Forensics excluding Floppy Disk Drive; (b) Mobile Devices Forensics. |
| 12. | Forensic Wing Lab, Defence Cyber Agency (DCyA) New Delhi | Rajaji Marg, New Delhi, | (a) Computer (Media) Forensics excluding Floppy Disk Drive; (b) Mobile Devices Forensics. |

# Annexure 2

## List Of Police Stations in the State Of Goa

### NORTH GOA:

1. Panaji Police Station
2. Old Goa Police Station
3. Agacaim Police Station
4. Mapusa Police Station
5. Anjuna Police Station
6. Pernem Police Station
7. Colvale Police Station
8. Porvorim Police Station
9. Calangute Police Station
10. Saligao Police Station
11. Bicholim Police Station
12. Valpoi Police Station

### SOUTH GOA:

1. Margao Town Police Station
2. Maina Curtorim Police Station
3. Fatorda Police Station
4. Colva Police Station
5. Cuncolim Police Station
6. Quepem Police Station
7. Curchorem Police Station
8. Sanguem Police Station
9. Canacona Police Station
10. Vasco Police Station
11. Verna Police Station
12. Vasco Railway Police Station
13. Dabolim Airport Police Station
14. Murmagao Police Station
15. Ponda Police Station
16. Collem

### OTHER POLICE STATIONS

1. Crime Branch Police Station
2. Cyber Crime Police Station
3. Anti Narcotic Cell Police Station
4. ATS Police Station
5. Womens Police Station
6. Anti human Trafficking Unit Panaji
7. Anti human Trafficking Unit Margao
8. Konkan Railway Police Station
9. EOC Police station
10. Harbour Coastal Police Station
11. Siolim Coastal Police Station
12. Betul Coastal Police Station
13. Panaji Coastal Police Station
14. Chapora Coastal Police Station
15. Tiracol Coastal Police Station
16. Talpona Coastal Police Station

# Annexure 3

## Questionnaires

### Questionnaires for Lawyers

NAME(OPTIONAL): AGE:

DESIGNATION YEARS IN SERVICE:

1.On the scale of 1 to 10 rate your familiarity with the subject of electronic evidence?(Where 1 stands for low and 10 for high)

_____

2.On the scale of 1 to 10 rate your familiarity with the subject of evidence other then electronic evidence?(Where 1 stands for low and 10 for high)

_____

3.On the scale of 1 to 10 rate your familiarity with the Information Technology Act?(Where 1 stands for low and 10 for high)

_____

4.How often have you handled cases(civil and criminal) containing some form of electronic evidence?

- Less then 20% of the total number of cases
- About 50% of the total number of cases
- More than 50% of the total number of cases.
- Never

5. What are the nature of civil cases in which electronic evidence is most commonly found? RANK IN THE ORDER OF PRIORITY on the scale of 1-5 (1 for most common)

- matrimonial cases
- Property matters
- contract matters
- company matters
- money decree

6. What are the nature of criminal cases in which electronic evidence is most commonly

found? RANK IN THE ORDER OF PRIORITY on the scale of 1-7 (1 for most common)

- offences affecting human body( assault, murder, rape etc)
- economic offences( misappropriation, cheating, forgery,)
- offences affecting property( trespass, theft etc)
- offences against state( sedition, rioting)
- domestic violence
- negotiable instruments
- others

7. Have you proved an electronic record been by examining an expert u/s 45A of the Indian Evidence Act in court?

- Yes
- No

8. If yes in how many cases have you proved electronic evidence by examining an expert u/s 45A of Evidence Act?

_____

9.What is the most common form of electronic evidence you encounter whilst presenting cases in the court? ? RANK IN ORDER OF PRIORITY

- Call records
- Photographs
- Electronic messages
- Videos
- Emails
- Text published on websites
- Statement of accounts
- others(PLEASE SPECIFY)_____

10. Have you produced electronic evidence without the witness producing certificate under section 65 B?

- yes, always
- No never

11. If yes under what circumstances have you produced electronic evidence without the witness producing certificate under section 65 B?

_____

12. Ordinarily in what form are the copies of electronic record produced along with the case of your opponent, generally given to you?

- Electronic form( in CDs or pendrives)
- hard copies
- both
- No copies given

13.Do you produce the memory card on which digital photographs have been clicked along with the hard copy of the photographs?

- yes in all cases
- no
- only when the opposite side objects to the production of hard copy simpiciter

14. Do you think the present Indian Law is fully equipped to deal with all issues relating presentation, authentication and admissibility of electronic evidence in Court?

- yes
- no

15.What do you think are the reasons for difficulty in authentication and admissibility of electronic evidence in Court?

- limited knowledge of judges and advocates in the field of electronic evidence
- want of empanelled experts u/s 45A to prove electronic record
- failure of litigant to preserve the original electronic record
- all the above
- other reasons_____

16.Please state briefly the difficulties you face in handling cases involving electronic evidence?

_____

**Questionnaire for Judges**

NAME(OPTIONAL): AGE: QUALIFICATION:

DESINATION: YEARS IN SERVICE:

1.On the scale of 1 to 10 rate your familiarity with the subject of electronic evidence?(Where 1 stands for low and 10 for high)

Ans:

2.On the scale of 1 to 10 rate your familiarity with evidence other then electronic evidence?(Where 1 stands for low and 10 for high)

Ans:

3.How often do u encounter cases containing some form of electronic evidence?

- Less then 20% of the total number of cases
- About 50% of the total number of cases
- More than 50% of the total number of cases.
- Never

4.What is the most common form of electronic evidence you encounter whilst presenting cases in the court? ? RANK IN ORDER OF PRIORITY

- phone conversations
- digital Photographs
- Electronic messages
- Videos
- others(PLEASE SPECIFY)_____

5. What are the nature of criminal cases in which electronic evidence is most commonly found? RANK IN THE ORDER OF PRIORITY on the scale of 1-7 (1 for most common)

- offences affecting human body( assault, murder, rape etc)
- economic offences( misappropriation, cheating, forgery,)
- offences affecting property( trespass, theft etc)
- offences against state( sedition, rioting)
- others

6. Have you in cases involving electronic evidence ordered that the evidence be authenticated by examining an expert u/s 45A of the Indian Evidence Act in court?

- Yes
- No

If yes in approximately how many cases?

_____

7. Have you admitted electronic evidence without the witness producing certificate under section 65 B of the Indian Evidence Act?

- yes, always
- yes when the other side has not objected
- yes in cases before the judgement of Anwar Bhasir was passed
- no never

8. Are copies (to be given to the accused) of electronic records (CD, Pendrive etc) other then hard copies of photographs, produced along with the chargesheet?

- Yes in most cases
- No rarely
- not at all. IO has to be summoned to give copies.

9. Do you think investigating officers are equipped to handle issues relating to electronic evidence?

- Yes
- No

10. Have u undergone any special training in cyber crime and cyber forensics?

- Yes
- No

11. Approximately how many cases involving electronic evidence have you handled since the year 2000?

_____

12. If any electronic record(other then muddemal) is contained in a magnetic or optical device (eg cd, pendrive, memory card)is produced before you do you take steps to keep it separately?

- yes they are preserved separately and not tagged along with the main file
- No they are tagged together with the main file.

13. If electronic record is produced as muddemal what do you do when the accused applies for copies of the same?

_____

14. Do you think the present law on electronic evidence is equipped to handle all issues relating to electronic evidence?

- Yes
- No

15.Please state briefly the difficulties you face in handling cases involving electronic evidence?

_____

**Questionnaire for Prosecutors**

NAME(OPTIONAL): AGE:

DESIGNATION YEARS IN SERVICE:

1.On the scale of 1 to 10 rate your familiarity with the subject of electronic evidence?(Where 1 stands for low and 10 for high)

_____

2.On the scale of 1 to 10 rate your familiarity with the subject of evidence other then electronic evidence?(Where 1 stands for low and 10 for high)

_____

3.On the scale of 1 to 10 rate your familiarity with the Information Technology Act?(Where 1 stands for low and 10 for high)

_____

4.How often have you handled cases containing some form of electronic evidence?

- Less then 20% of the total number of cases
- About 50% of the total number of cases
- More than 50% of the total number of cases.
- Never

5. What are the nature of criminal cases in which electronic evidence is most commonly found? RANK IN THE ORDER OF PRIORITY on the scale of 1-7 (1 for most common)

- offences affecting human body( assault, murder, rape etc)
- economic offences( misappropriation, cheating, forgery,)
- offences affecting property( trespass, theft etc)
- offences against state( sedition, rioting)
- domestic violence
- negotiable instruments
- others

6. Have you proved an electronic record been by examining an expert u/s 45A of the Indian Evidence Act in court?

- yes
- no

7. If yes in how many cases have you proved electronic evidence by examining an expert u/s 45A of Evidence Act?

_____

8.What is the most common form of electronic evidence you encounter whilst presenting cases in the court? ? RANK IN ORDER OF PRIORITY

- Call records
- Photographs
- Electronic messages
- Videos
- Emails
- Text published on websites
- Statement of accounts
- others(PLEASE SPECIFY)_____

9. Have you produced electronic evidence without the witness producing certificate under section 65 B?

- yes, always
- No never

10. If yes under what circumstances have you produced electronic evidence without the witness producing certificate under section 65 B?

_____

11. Ordinarily in what form are the copies of electronic record produced along with the charge sheet given to the accused?

- Electronic form( in CDs or pendrives)
- hard copies
- both
- No copies attached by IO

12.Do you produce the memory card on which digital photographs have been clicked along with the hard copy of the photographs?

- yes in all cases
- no
- only when the opposite side objects to the production of hard copy simpiciter

13. Do you think the present Indian Law is fully equipped to deal with all issues relating presentation, authentication and admissibility of electronic evidence in Court?

- yes
- no

14.What do you think are the reasons for difficulty in authentication and admissibility of electronic evidence in Court?

- limited knowledge of judges and advocates in the field of electronic evidence
- want of empanelled experts u/s 45A to prove electronic record
- failure of litigant to preserve the original electronic record
- all the above
- other reasons

15. Do you think the IOs properly seize and preserve an electronic record so as to ensure its authenticity and integrity?

- yes
- no

16. Do you think investigating officers are equipped to handle issues relating to electronic evidence?

- yes
- no

17. Have you undergone any special training in cyber crime or cyber forensics?

- yes
- no

18.Do you think there is adequate infrastructure available in the State of Goa that would assist the law enforcing agencies in proper preservation, production and authentication of electronic evidence in court?

- yes
- no

19. Do you think proper use and authentication of electronic technology in evidence will lead to complete demystification of the adjudicatory process ensuring transparency, clarity and certainty?

- yes
- no

20.Please state briefly the difficulties you face in handling cases involving electronic evidence?

**Questionnaire For Police**

NAME(OPTIONAL): AGE:

YEARS IN SERVICE: RANK

1.On the scale of 1 to 10 rate your familiarity with the subject of electronic evidence?(Where 1 stands for low and 10 for high)

_____

2.On the scale of 1 to 10 rate your familiarity with the subject of evidence other then electronic evidence?(Where 1 stands for low and 10 for high)

_____

3.On the scale of 1 to 10 rate your familiarity with the Information Technology Act?(Where 1 stands for low and 10 for high)

_____

4.How often have you handled cases(civil and criminal) containing some form of electronic evidence?

- Less then 20% of the total number of cases
- About 50% of the total number of cases
- More than 50% of the total number of cases.
- Never

5. What are the nature of criminal cases in which electronic evidence is most commonly found? RANK IN THE ORDER OF PRIORITY on the scale of 1-7 (1 for most common)

- offences affecting human body( assault, murder, rape etc)
- economic offences( misappropriation, cheating, forgery,)
- offences affecting property( trespass, theft etc)
- offences against state( sedition, rioting)
- domestic violence
- negotiable instruments
- others

6.What is the most common form of electronic evidence you encounter whilst presenting cases in the court? ? RANK IN ORDER OF PRIORITY

- Call records
- Photographs
- Electronic messages
- Videos
- Emails
- Text published on websites
- Statement of accounts
- others(PLEASE SPECIFY)_____

7. Are you aware of section 65B of the Indian Evidence Act?

- yes
- no

8. Have you produced electronic evidence without the witness producing certificate under section 65 B?

- yes, always
- No never
- Sometimes when the accused has not objected.

9. Do you think the present Indian Law is fully equipped to deal with all issues relating presentation, authentication and admissibility of electronic evidence in Court?

- yes
- no

10.What do you think are the reasons for difficulty in authentication and admissibility of electronic evidence in Court?

- limited knowledge of judges and advocates in the field of electronic evidence
- want of empanelled experts u/s 45A to prove electronic record
- failure of litigant to preserve the original electronic record
- lack of proper SOPS or Rules for investigation of electronic records
- all the above
- other reasons_____

11.Do you call for services of the cyber forensic team of Goa Police at the time of investigation where electronic evidence is involved?

- YES at all times
- NO
- YES SOMETIMES IN SPECIAL CASES

12.If you have selected the third option. Please state briefly what are those special cases.

_____

13.Is your police station equipped with a special Malkhana /Muddemal room/or any other separate room/ space to preserve electronic record and keep it safe?

- yes
- no

14. Are you aware of any Standard operating procedures or rules prescribed by the Government of Goa for seizure and handling of electronic evidence at the time of investigation or trial?

- yes
- no

15. If yes please give details

_____

16.Are you aware of the concept of cloned copies of electronic records?

- yes
- no

17. If yes please state the number of times you have resorted to cloning of electronic records as a part of your investigation.

_____

18. Is your police station equipped with a device that assists you in making cloned copies of electronic records at the time of investigation?

- yes
- no

19. Have you undergone training in the field of electronic evidence or cyber crimes?

- yes
- no

20.If yes please give details

_____

21. Is there any emergency Computer Forensics Response team in Goa to assist the IO in seizure of electronic record?

- yes
- no

22. Do you think there is adequate infrastructure available in the State of Goa that would assist the law enforcing agencies in proper preservation, production and authentication of electronic evidence in court?

- yes
- no

23. Do you think proper use and authentication of electronic will lead to complete demystification of the adjudicatory process ensuring transparency, clarity and certainty.

- yes
- no

24.Please state briefly the difficulties you face in handling cases involving electronic evidence?

_____