EXPLORATION OF TECHNOLOGY GLOBALLY AND ITS LEGAL DIMENSIONS

Editor-in-Chief
Prof. (Dr.) Shefali Raizada

Editors
Ekta Gupta, Swati Kaushal

Foreword by
Vakul Sharma, Advocate, Supreme Court of India

THOMSON REUTERS

CHAPTER 3

LABYRINTH OF EVIDENCES IN THE WORLD OF TECHNOLOGY

MR. SAJU JAKOB,* MS. EKTA BHARATI** AND MS. NANCY SHAH***

ABSTRACT

As Justice Lord Denning rightly stated, "Law is an Ass", if not properly applied and proved its purpose. Another renowned lawyer of Indian Jurisprudence, Nani Palkhiwala said, "Law may or may not be an ass but in India, it is certainly a snail. It moves so slowly that it might be considered too slow in a community of snails." With the world being in lockdown during the times of COVID-19, most of the courts all over the world are partly paralysed. Court proceedings, except urgent cases are kept under suspension due to the lockdown, resulting in temporary abeyance. Though Supreme Court of India didn't close its doors even for a day during the lockdown thanks to technological assistance of video courts, it has become clear to everyone that the assistance of the technology is inevitable in the days ahead for the administration of justice. The purpose of the litigation will be defeated if there is no timely or effective solution. Even though criminality or wrong doings have reached its great heights with extensive use of technology, the judicial /investigation process still relies primarily on the oral testimonies of the witnesses. Resultantly, most cases are either resolved on a subjective assumption leading to wrong administration of justice due to defective assessment or investigation, or remain sometimes undecided resulting in high pendency of cases. Since ages, mankind has mainly relied on subjective opinions of various witnesses, at various stages of investigation or judicial examination. Examination of evidence is a difficult and complex process in today's world and hence is vulnerable to imperfection or incorrectness and is made subject to various levels of reviews by way of appeals. Technological exploration

* The author Saju Jakob [LL.B (IND), LL.M (GER), MBA (USA)], is the Advocate practising in the Supreme Court of India. He is the Member of Law Society, London; Member of Bar Council, Cologne, Germany; Life Member of Supreme Court Bar Association; Solicitor of U.K and Germany, and the Senior Counsel in the law firm Lily Thomas and Saju Jakob. His expertise lies in constitutional law, criminal law and international contracts.

** Assisted by the co-author is Ekta Bharati [LL.B], Advocate practising in the Supreme Court of India and is associated with the Law firm Lily Thomas and Saju Jakob. Her expertise lies in Criminal Law, Constitution Law and Arbitration Law.

*** The co-author is Nancy Shah [LL.B], Advocate practising in the Supreme Court of India and, is associated with the Law firm Lily Thomas and Saju Jakob. Her expertise lies in Criminal Law, Constitutional Law as well as Personal Laws.

will lead to greater clarity while uncovering the mystery of the case from the labyrinth of evidence. Collection, production, recovery, assessment and judicial review of various evidences/ witnesses are laborious task and time consuming too. The exploration of technology is naturally a part and parcel of today's world of Covid era, but becomes more inevitable especially to find out the veracity of truth in a given case in the world of forensic science or to prove the credibility of witnesses by supplying significant bits and pieces of other circumstantial evidences in the totality of examination.

INTRODUCTION

According to Edmond Locard's principle, also termed as 'Locard's Exchange Principle', "when something comes in contact with the other, it always leaves traces/marks behind."[1] Such traces can be visible or invisible to the naked eye. These traces form the basis of evidence. Various scientific methods are used to track the correct sources of those traces/marks.

The time of collection as well as production of evidence is of essence in determining the accuracy, in most of the cases. For instance, under the Insolvency and Bankruptcy Code in India, no forensic evidence is required at the pre-admission stage. In the recent ruling *Allahabad Bank* v. *Poonam Resorts*,[2] the National Company Law Appellate Tribunal (NCLAT) observed that the time limit of 14 days for the investigation cannot be relaxed even for forensic investigation. In a country like India, where forensic experts take months to supply the preliminary report, the Code does not envisage forensic or even technology-supported evidence in admitting a case for winding up the Company under Insolvency and Bankruptcy Code.

As we talk about the essence of time in using technology for collection and production of evidence, the current paper discusses about the collection and production of evidence, focussing on its authenticity at the pre-trial stage and its evidentiary value during trial stage. In this paper we attempt to find out how technology can be used to find out the truth of the matter from the labyrinth of evidences, which is hidden and invisible in various elements or factors.

As per a study report by the 'Institute of Law and Justice', titled '*The Role and Impact of Forensic Evidence in the Criminal Justice System, Final Report*'[3], forensic evidence has been categorised into Biological Evidence, Weapons Evidences, Fingerprint Evidence, Drug Evidence, Impression Evidence, Trace Evidence, Natural/Synthetic Material, Generic Object and electronic/printed data.

---

1. E.J. Wahner, 'The French Connection of Sherlock Holmes', available at: https://ejdissectingroom.wordpress.com/2011/02/25/the-french-connection-of-sherlock-holmes/, last accessed on 20 May 2020.
2. Company Appeal (AT) (Insolvency) No. 1304 of 2019, Judgment delivered on 22nd May 2020.
3. Tom Mc Ewen, 'The Role and Impact of Forensic Evidence in the Criminal Justice System, Final Report' as published in 2010, available at: https://www.ncjrs.gov/pdffiles1/nij/grants/236474.pdf, last accessed on 25 May 2020.

Forensic evidence in a criminal trial has several roles to play and is not just restricted to proving that a crime has been committed.[4] It can be employed for establishing the key element of a crime; placing the suspects in contact with the crime or the victim; establishing the identity of the suspects; corroborating with the witness and victim's testimony and further providing accuracy to establish the fact of what occurred.

One of the trends that have been seen in the past that, though forensic evidence can give conclusive evidence with respect to the crime, it is yet used only in cases when major or sensational crime occurs.[5] It was observed in the Report of Malimath Committee, formed for reforming the Criminal Justice System,[6] that the inadequacy of logistical and forensic back-up support is one of the major difficulties faced by the police officer in ensuring speedy, effective and fair investigation. It is pertinent to note that the effect of forensic evidence depends on the stage of the collection of evidence that is the time duration after the commission of crime.

In a research conducted in 1987, by the National Institute of Justice, US Department of Justice,[7] it was found that police on an average are three times more likely to clear cases when scientific evidence is gathered, and the sentences are more severe when forensic evidence is presented at trial. Further, the clearance rates of offences, with the evidence scientifically analysed, were found to be about three times greater than where no such evidence was used. Nearly two-thirds of workload in the crime laboratory was identified as that of drugs, narcotics and determination of alcohol content in the sample. The use of forensic science in crime investigation is even lesser in India, with only 5–6% of the registered crime cases being referred to the Forensic Science Laboratory and Finger Print Bureau.[8] Similarly, in a study conducted by Prof. S.L. Vaya, the former Director of Institute of Research and Development titled "*Fidelity of Forensic Evidence in Criminal Trial in India*"[9] it was found that though the mentioning of forensic science evidence has gone up considerably since 2000, these evidence are relied upon mostly in cases of murder and rape. Hence, though we have a presence of technology, which can be used in investigation, and such evidence is admissible in court of law, lack of technological availability still poses a problem for the proper investigation and judicial dispensation.

---

4. *Ibid.*
5. T.R. Baggi, 'Why is Forensic Science Stunted and Static in India?' *The Hindu* (11 September 2011).
6. Justice Malimath, *'Committee on Reforms of Criminal Justice System'*, I at 89 (2003).
7. Joseph L. Peterson, *'Use of Forensic Evidence by Police and Courts'*, US Department of Justice, National Institute of Justice, 1987, available at: https://www.ncjrs.gov/pdffiles1/pr/107206.pdf, last accessed at 12 June 2020.
8. *Supra* note 6.
9. Prof. S.L. Vaya, *Fidelity of Forensic Evidence in Criminal Trial in India* (Raksha Shakti University, 2017), 16, available at: http://hdl.handle.net/10603/211347, last accessed at 30 May 2020.

The benefits of forensic science would include assistance to the stakeholders to increase their efficiency in the criminal justice system and thereby reduction of chances of wrongful conviction. Collection of evidences such as firearms, fingerprints, hair strains, semen in rape cases, blood stains and getting it analysed with forensic laboratories would not only have impact in the investigation but would also remove the aspect of subjective judgment of the Investigating Officer. Besides, challenging forensic evidence is a hard task, as the attempt is made to challenge the credential of the forensic witness. The most important benefit of forensic evidence is that it is devoid of emotion as well as the subjective judgment of the examiner. It is a black and white report, that either links the crime to a particular person or don't. It leaves no place for any speculation. Even in the current times, due to the lack of timely reports on forensic testing, it becomes highly unfeasible for law enforcement agencies to rely completely on forensic evidence.

The few uses of technology in forensic evidence are enumerated in the following sections.

CAMERA-RELATED EVIDENCE

The first innovation in the technological field that necessitated the need for change in the provisions of the Indian Evidence Act and the Information Technology (IT) Act was the prevalent use of digital photographs, instead of traditional photographs.

The different methods of capturing and storing digital photographs have raised the questions about the authenticity of such photographs and videos, even though Section 3 of the Indian Evidence Act terms these photographs as 'documents'. The difference in checking the authenticity was based on whether these photographs or videos would be substantive evidence or demonstrative evidence. The level of identification is different in case of the photograph being the substantive evidence, as it will include Chain of Custody, Hash Value and Metadata Value, whereas the rules for demonstrative evidence are bit relaxed. Considering the evidentiary value of the digital photographs, Section 65B of the Indian Evidence Act considers such electronic evidence to be admissible as secondary evidence. However, if the electronic evidence is produced with its original medium in the court; such electronic evidence shall be brought as primary evidence under Section 62 of the Indian Evidence Act. Section 65B (4) further requires electronic evidence to be produced with the certificate from the witness. Section 45A of Evidence Act validates the electronic evidence through Expert Opinion.

Though there are concerns in India, with regard to video graphed tape being produced as evidence, and its admissibility, it is taken as a matter of violation of privacy and thus, even the judicial authorities require permission from the accused as well as the victim in many other developed democracies.

Crime Scene Photography and Videography

Numerous forensic science and technology professionals have been trained academically to conduct crime-scene photography. It involves the complete view and the cut-to-cut scenes of the crime scenes in order to give a clear picture of the crime scene to anyone who looks at the pictures. However, in practice, crime-scene photographs are not generally available in many cases, except the grave and serious offences and the only way left with the judges as well as the lawyers, to understand the crime spot is from the testimony of the Investigating Officer or witnesses. There is generally a crime scene report (mahazar)/location plan, but no videograph or photograph is attached. In the interim order, dated 12 October 2017, it was stated by the Hon'ble Supreme Court of India stated in *Shahfi Mohommad* v. *State of Himachal Pradesh*,[10] that *"A decision was taken to constitute a Committee of Experts (COE) to facilitate and prepare a report to formulate a road-map for use of videography in crime investigation and to propose a Standard Operating Procedure (SOP)."* Even though the concept received positive support by the States and the Central Investigation Agencies, reservations were expressed in its implementation.

Apart from production and admissibility of evidence, other issues such as funding, securing the data and storage needs to be addressed as well.[11]

In the Report of the Committee constituted on 22 November' 2017, by the Ministry of Home Affairs (MHA) of India, to analyse the use of videography in police investigation, the Committee observed that though the videography of the crime scene was a 'desirable and acceptable best practice', there are other major issues, which needs to be addressed to make crime scene videography mandatory. The aforesaid committee has stressed on the policy of 'Best Effort' on the part of authorities for conducting videography. The Committee in its Report even provided for various timelines in order to implement the use of videography and hence, suggested to form a committee of experts for the periodical review of guidelines and also a steering committee to monitor the same. On the basis of the report, in 2018, the MHA directed all central investigation agencies to form an action plan regarding the videography of the crime scene.

It was further observed in *Shahfiq Mohammad (Supra)* that *"the time is ripe that steps are taken to introduce videography in investigation, particularly for crime scenes, as desirable and acceptable best practice as suggested by the Committee of the MHA to strengthen the Rule of Law."* In this case, the Hon'ble Supreme Court has relaxed the

10. *Shafhi Mohammad* v. *The State of Himachal Pradesh*, SLP (C) 2302 of 2017.
11. *Ibid.*

necessity of the statutory certificate as required by section 65B (4) and stated that electronic evidence is admissible subject to the satisfaction of the court of its authenticity, though the Hon'ble Court has not overruled the settled legal position held in the case of ***Anvar P.V vs. P.K Basheer 2014(10) SCC 473*** , wherein the requirement of the statutory certificate was made mandatory. With a view to implement the plan of action prepared by the Committee, it was even directed by the Hon'ble Supreme Court that the MHA sets up a Central Oversight Body (COB).

In another case of *D.K. Basu* v. *State of West Bengal and Ors.*,[12] the Hon'ble Supreme Court of India directed installation of CCTV cameras in police stations and prisons to check human rights abuse.[13]

It is pertinent to mention that with the advancement of technology, the crime scene videography is the need of the hour to inspire confidence in the evidence collected, and to deviate the complete evidentiary reliance from testimonies of the witnesses and the investigating officers.

Post-mortem Photography

Usually, the opinion of a medical expert, conducting the post-mortem, is considered as relevant evidence depicting the cause of death, for the reason that it is conducted right after the body is found and can suggest the influence of any chemical within the body of the deceased. However, reliance is placed on the post-mortem report through the opinion of the concerned witness, who is the medical professional in this case. The chances of tampering with the witnesses are reduced if such a process is documented through videography.

In most of the underdeveloped countries, including Africa, the use of third-degree force by the investigative authorities is very much a common practise, despite being severely criticised and disparaged by the judiciary all over the world. The post-mortem report can be a valuable record in drawing a conclusion on the cause of death of a person in police lock-up or jail. The importance of videographing the post-mortem process in case of custodial deaths was emphasised by the National Human Rights Commission (NHRC) of India on 10 August' 1995, which was communicated to all States. The NHRC noted that *"though the process of video-recording of the post-mortem examination would involve extra cost, human life is more valuable than the cost of video-recording and in any case, occasions necessitating video recording should ideally be very limited."*[14]

---

12. *D.K. Basu* v. *State of West Bengal and Ors.* [(2015) 8 SCC 744].
13. *Supra* note 10.
14. *Re-Inhuman Conditions in 1382 Prisons*, WP(C) No. 406 of 2013.

Though it was further clarified by NHRC on 21 December' 2001 that the requirement of videographing a post-mortem examination in respect of custodial deaths would arise only where foul play by the concerned authority is alleged, or suspicion of such foul play is raised in the preliminary inquest report by the Magistrate or where there are reasons to suspect foul play.[15] Resultantly, the procedure laid down in the Code of Criminal Procedure (CrPC), 1973,[16] and the guidelines issued by the NHRC should be followed in the event of a custodial death.

Ultraviolet (UV) and Infrared (IR) Photography

Ultraviolet or Infrared photography helps the investigator to get photographs, by using wavelengths of light spectrum, that can be normally obscured from vision. It can even reveal bruises or scars not visible on the surface of the skin, sometimes even after they are healed.

This type of technological advancement in photography is highly valuable due to its usage even after a huge lapse of time as well as for the fact that it can also be subjected to re-examination. This method can also be used to detect the non-contact radiation, thus even heat traces left by humans and the objects can be investigated. These cameras eliminate the risk of contamination and also the potential loss of evidence. The UV and IR Technology can even be used during post mortems. In a study performed by Lin et al. in differentiation of blood stains,[17] blood stains diluted to a 1/8 ratio, were viable in 8 of 10 different cloth samples by IR photography." Other uses of UV and IR technology can be for examination of features of currency, passport, blood sample, palm prints, finger prints, old and new injuries, gunshot residues, invisible traces on clothes, blunt force injuries, bite and teeth marks, DNA analysis, tattoos, old documents and even burnt and charred documents.

Sting Operations and Tape Recordings

Sting operations can be a useful tool to expose long-going scandals; but raises certain questions, not only moral and ethical, but also legal. This includes whether the planted potential victim, who is otherwise innocent, can be called as a sting operator and be subjected to punishment for the commission of offence or the abetment of commission of the offence.[18]

---

15. *Ibid.*
16. Code of Criminal Procedure, 1973 (Act No. 2 of 1974).
17. Mahmut Asirdizer, Yavuz Hekimoglu and Orhan Gumus, '*Usage of Infrared-Based Technologies in Forensic Sciences*', Forensic Analysis – From Death to Justice, 7 September 2016; 10.5772/62773.
18. *Rajat Prasad* v. *CBI* (2014) 6 SCC 495.

The Hon'ble Supreme Court in *Rajat Prasad* v. *Central Bureau Investigation* claims in this regard that any journalist or private individual cannot be considered to be in conspiracy or abetting with the main offender in the main offences due to the absence of *mens rea*. However, it clearly stated that "a crime does not stand obliterated or extinguished merely because its commission is claimed to be in public interest."[19]

In *R* v. *Mack*,[20] the Canadian Supreme Court explained that the aforementioned entrapment occurs when,

> *(a) the authorities provide a person with an opportunity to commit an offence without acting on a reasonable suspicion that this person is already engaged in criminal activity or pursuant to a bona fide inquiry, and,*
> *(b) although having such a reasonable suspicion or acting in the course of a bona fide inquiry, they go beyond providing an opportunity and induce the commission of an offence.*

In *R* v. *Stevenson*,[21] while dealing with the admissibility of tape-recorded conversation in a criminal case, it was observed by the court that,

> *"Just as in the case of photographs in a criminal trial, the original un-retouched negatives have to be retained in strict custody so in my views should be original tape recordings. However one looks at it, whether, as counsel for the Crown argues, all the prosecution have to do on this issue is to establish a prima facie case, or whether, as counsel for the defendant Stevenson in particular, and counsel for the defendant Hulse joining with him, argues for the defence, the burden of establishing an original document is a criminal burden of proof beyond reasonable doubt, in the circumstances of this case it seems to me that the prosecution have failed to establish this particular type of evidence. Once the original is impugned and sufficient details as to certain peculiarities in the proffered evidence have been examined in court, and once the situation is reached that it is likely that the proffered evidence is not the original- is not the primary and the best evidence – that seems to me to create a situation in which, whether on reasonable doubt or whether on a prima facie basis, the judge is left with no alternative but to reject the evidence. In this case on the facts as I have heard them such doubt does arise. That means that no one can hear this evidence and it is inadmissible.*[22]

---

19. *Ibid.*
20. *R.* v. *Mack* (1988) 2 SCR 903.
21. *R.* v. *Stevenson* (2008) SKCA 149 (CanLII).
22. *R.K. Anand* v. *Registrar, Delhi High Court*, 2009 (10) SCALE 164.

Further, the Supreme Court of India in *Ziyauddin Burhanuddin Bukhari v. Brijmohan Ramdass Mehra & Ors.*[23]observed that a tape-recorded speech would be accepted as 'documents', defined under Section 3 of the Indian Evidence Act[24] on fulfilling the following conditions:

> *(a) The voice of the person alleged to be speaking must be duly identified by the maker of the record or by others who know 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.*

Body-Worn Cameras

The use of body-worn cameras by police and security personnel is fairly recent and their importance is starting to be recognised globally. According to a study by Cambridge University's Institute of Criminology which monitored 2,000 police personnel, who had started using body-worn cameras, across the United Kingdom and the United States for a period of time, it suggests that the complaints against those monitored personnel went down by 93%. When those police officers started wearing body cameras, only 113 complaints were registered against them as opposed to the 1,539 complaints registered against them the year before.[25] It has been widely argued by experts that wearing a body camera improves the behaviour of security personnel as well the general public because they know that their actions are being recorded. Studies have shown that body-worn cameras not only improves behaviour of security personnel but also reduces the number of complaints against security personnel as the camera acts as a witness and later the recording can be treated as an evidence. The footage from the cameras, also aids the judicial process more perfect and precise.

Moreover, in a study in the United Kingdom, it was found that the use of body-worn cameras resulted in reduction of citizen complaints as well as crime. It was also found that use of cameras led to increase in arrests, prosecution and guilty pleas.[26] In another study at the Arizona State University, it was found that an officer with body-worn cameras was more productive in making an arrest than an officer without cameras.[27]

---

23. *Ziyauddin Burhanuddin Bukhari* v. *Brijmohan Ramdass Mehra & Ors*, 1975 AIR 1778.
24. Indian Evidence Act, 1872 (Act No. 1 of 1872).
25. Chapman Brett, *'Body Worn Cameras: What the Evidence tells Us'*, November 14' 2018, National Institute of Justice.
26. *Ibid.*
27. Charles Katz, et al., *Evaluating the Impact of Officer Worn Body Cameras in the Phoenix Police Department* (Center For Violence & Community Safety, Arizona State University, 2015).

Body-worn cameras are an answer to reduction of police brutality and to infuse civility on behaviour of police officials towards people. As per a study conducted in 2017 in the United States, it was found that complaint about the use of force has been reduced after the use of body worn cameras.[28] Body-worn cameras are the constant check on the behaviour of the officials of the investigating agencies as well as the people coming in contact with those officials.

In India, body-worn cameras were first used by Hyderabad Traffic Police in 2015[29], with an aim to develop friendly policing and to increase transparency and accountability. Recently, Bengaluru Traffic Police officials and Railway Protection Force started using body-worn cameras to prevent crimes, reduce violence and complaints against police personnel. Traffic police of various States and Union Territories have started using body-worn cameras and have found significant results in reduction of crime such as chain snatching, petty theft, and so on. With the use of body-worn cameras in maintaining traffic and crime reduction, its use could be extended to investigation carried by police officials and investigating authorities of the crimes as well. Section 162 of the Civil Procedure Code' 1908[30] mandates a police official to maintain a police diary by the Investigating Officer, carrying the investigation, with the intention to assist the court in the trial. Wearing of cameras during investigation will not only result in better transparency and accountability, but also can be used as corroborative evidence. It has been found that the use of technology enables the officer to resolve criminal cases faster.[31] Hence, with the admissibility of such evidence being already recognised by the court under Evidence Act, it could not only provide corroborative evidence but would help in faster disposal of cases. Further, it reduces the possibility of raising false claims such as false evidence and framing of accused. With the knowledge of police officials, of being monitored while investigating a case, provisions of the law would be followed and mere technicality would not be a ground for acquittal of accused.

ELECTRONIC EVIDENCE

With the advent of technology and its influence on the day-to-day life of an individual, wherein reliance on electronic media for communication, entering into commercial

28. Anthony Braga, et al., *The Benefits of Body-Worn Cameras: New Findings from a Randomized Controlled Trial at the Las Vegas Metropolitan Police Department* (National Institute of Justice, U.S. Department of Justice, 2017).
29. PTI, 'In a first, Hyderabad Traffic Police Launches Body-worn Cameras', *Economic Times* (14 August 2015, 03:40 PM IST), available at: https://economictimes.indiatimes.com/news/politics-and-nation/in-a-first-hyderabad-traffic-police-launches-body-worn-cameras/articleshow/48481799.cms?from=mdr, last accessed on 09 January 2021.
30. *Ibid.*
31. *Ibid.*

agreements and exchange of information has been on increase, the Indian legislations were amended and enacted for these digital documents to be made as a piece of evidence and to provide a legislative framework for transaction in 'electronic' devices. These legislations include the IT Act, 2000 which is based on United Nations Commission on International Trade Law (UNCITRAL), the Indian Evidence Act, 1872, and the Indian Penal Code, 1860. Although with new enactment and amendments, electronic evidence has been made admissible; such evidences are prone to be altered and tampered, resulting in complete distortion of justice.[32] Though amendments were made recently, however, the Indian courts had already recognised the admissibility of such evidence as 'documents' within Section 3 of the Indian Evidence Act. In *Ziyauddin Burhanuddin Kukhari* v. *Brihmohan Ramdass Mehra and Others*[33] the Hon'ble Supreme Court of India observed that the tape-recorded speech would be a document as defined under Section 3 and stands in no different footing than a photograph. Hence with tape-recorded speech, photographs were also considered a piece of evidence, which is elaborated in the paragraph below.

Section 2(t) of IT Act, 2000,[34] defines "electronic record to mean data, records or data generated, image or sound stored, received or sent in an electronic form or micro-film or computer-generated microfiche."

Section 3 of the Evidence Act[35] defines 'Evidence' to mean and include oral evidence and documentary evidence, and documentary evidence includes electronic evidence within its ambit.

As per Section 79A of IT Act, 2000,[36] 'electronic form of evidence would mean "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 machine."

Moreover Section 4 of the Act, states that "requirement under any law for the information or any other matter to be writing or typewritten or printed form shall deemed to have satisfied such requirement of such information or matter if the same is rendered or made available in electronic form and is accessible so as to be used for a subsequent reference."

---

32. Kurian Joseph J. in *Anvar PK* v. *PK Basheer & Ors.* (2014) 10 SCC 473.
33. *Ziyauddin Burhanuddin Kukhari* v. *Brihmohan Ramdass Mehra and Others*, AIR 1975 SC 1788.
34. Information Technology Act, 2000 (Act No. 21 of 2000).
35. *Ibid.*
36. *Ibid.*

Body-worn cameras are an answer to reduction of police brutality and to infuse civility on behaviour of police officials towards people. As per a study conducted in 2017 in the United States, it was found that complaint about the use of force has been reduced after the use of body worn cameras.[28] Body-worn cameras are the constant check on the behaviour of the officials of the investigating agencies as well as the people coming in contact with those officials.

In India, body-worn cameras were first used by Hyderabad Traffic Police in 2015[29], with an aim to develop friendly policing and to increase transparency and accountability. Recently, Bengaluru Traffic Police officials and Railway Protection Force started using body-worn cameras to prevent crimes, reduce violence and complaints against police personnel. Traffic police of various States and Union Territories have started using body-worn cameras and have found significant results in reduction of crime such as chain snatching, petty theft, and so on. With the use of body-worn cameras in maintaining traffic and crime reduction, its use could be extended to investigation carried by police officials and investigating authorities of the crimes as well. Section 162 of the Civil Procedure Code' 1908[30] mandates a police official to maintain a police diary by the Investigating Officer, carrying the investigation, with the intention to assist the court in the trial. Wearing of cameras during investigation will not only result in better transparency and accountability, but also can be used as corroborative evidence. It has been found that the use of technology enables the officer to resolve criminal cases faster.[31] Hence, with the admissibility of such evidence being already recognised by the court under Evidence Act, it could not only provide corroborative evidence but would help in faster disposal of cases. Further, it reduces the possibility of raising false claims such as false evidence and framing of accused. With the knowledge of police officials, of being monitored while investigating a case, provisions of the law would be followed and mere technicality would not be a ground for acquittal of accused.

ELECTRONIC EVIDENCE

With the advent of technology and its influence on the day-to-day life of an individual, wherein reliance on electronic media for communication, entering into commercial

---

28. Anthony Braga, et al., *The Benefits of Body-Worn Cameras: New Findings from a Randomized Controlled Trial at the Las Vegas Metropolitan Police Department* (National Institute of Justice, U.S. Department of Justice, 2017).
29. PTI, 'In a first, Hyderabad Traffic Police Launches Body-worn Cameras', *Economic Times* (14 August 2015, 03:40 PM IST), available at: https://economictimes.indiatimes.com/news/politics-and-nation/in-a-first-hyderabad-traffic-police-launches-body-worn-cameras/articleshow/48481799.cms?from=mdr, last accessed on 09 January 2021.
30. *Ibid.*
31. *Ibid.*

agreements and exchange of information has been on increase, the Indian legislations were amended and enacted for these digital documents to be made as a piece of evidence and to provide a legislative framework for transaction in 'electronic' devices. These legislations include the IT Act, 2000 which is based on United Nations Commission on International Trade Law (UNCITRAL), the Indian Evidence Act, 1872, and the Indian Penal Code, 1860. Although with new enactment and amendments, electronic evidence has been made admissible; such evidences are prone to be altered and tampered, resulting in complete distortion of justice.[32] Though amendments were made recently, however, the Indian courts had already recognised the admissibility of such evidence as 'documents' within Section 3 of the Indian Evidence Act. In *Ziyauddin Burhanuddin Kukhari* v. *Brihmohan Ramdass Mehra and Others*[33] the Hon'ble Supreme Court of India observed that the tape-recorded speech would be a document as defined under Section 3 and stands in no different footing than a photograph. Hence with tape-recorded speech, photographs were also considered a piece of evidence, which is elaborated in the paragraph below.

Section 2(t) of IT Act, 2000,[34] defines "electronic record to mean data, records or data generated, image or sound stored, received or sent in an electronic form or micro-film or computer-generated microfiche."

Section 3 of the Evidence Act[35] defines 'Evidence' to mean and include oral evidence and documentary evidence, and documentary evidence includes electronic evidence within its ambit.

As per Section 79A of IT Act, 2000,[36] 'electronic form of evidence would mean "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 machine."

Moreover Section 4 of the Act, states that "requirement under any law for the information or any other matter to be writing or typewritten or printed form shall deemed to have satisfied such requirement of such information or matter if the same is rendered or made available in electronic form and is accessible so as to be used for a subsequent reference."

---

32. Kurian Joseph J. in *Anvar PK* v. *PK Basheer & Ors.* (2014) 10 SCC 473.
33. *Ziyauddin Burhanuddin Kukhari* v. *Brihmohan Ramdass Mehra and Others*, AIR 1975 SC 1788.
34. Information Technology Act, 2000 (Act No. 21 of 2000).
35. *Ibid.*
36. *Ibid.*

Section 62 defines documents as primary evidence if 'the same is produced for inspection of the court' and under Section 63[37] "secondary evidence would mean and include certified copies of documents, copies made from mechanical process and oral account of the contents of a document. These cases included the following:

i. *when the original documents are in possession or power of a person against whom it is sought to be proved;*

ii. *when the existence, condition or contents of the original have been proved to be admitted by person against whom it is proved;*

iii. *original is lost or destroyed;*

iv. *it cannot be moved easily;*

v. *document is in the nature of public document;*

vi. *when a certified copy of the document is permitted under Evidence Act or any other law in force and;*

vii. *when the document consists of numerous accounts.*

This section was turned for admission of electronic evidence as documents as per Section 63 of Evidence Act.

Further, Section 17 of the Indian Evidence Act[38] was amended to define admission as a "statement, oral; or documentary or contained in electronic form, which suggests any inference as to any fact in issue or relevant facts," and Section 22A was inserted to provide for oral admission as to the content of electronic record to be relevant if the genuineness of the electronic record produced is in question. The most important amendment was insertion of Sections 65A and 65B in the year 2000, wherein as per the former section the contents of electronic records could be proved in accordance with the provision of the latter section. Under Section 65B, "*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 also a documents*" and would be admissible without further proof or production of original file, if condition laid in relation to information and computer in question is satisfied. However, Section 65B(4) requires the production of a certificate of the authenticity of electronic evidence by the person responsible for its creation or storage.

In light of the aforesaid provision, electronic evidence is admissible in court of law as evidence. Though the Hon'ble Apex Court in *State NCT of Delhi* v. *Navjot*

37. *Ibid.*
38. *Ibid.*

Sandhu[39], while dealing with admissibility of telephone-recorded calls, has held that contents of electronic record in printout form and CDs are admissible as prima facie evidence without authentication. However, the said judgment has been overruled in *PV Anvar* v. *PK Basheer*[40] by the three judge-bench, wherein it was held that the certificate under Section 65(B) is the only possible way for authentication of an electronic evidence. It was further held that though Sections 61–65 of the Indian Evidence Act deal with admissibility of primary and secondary documentary evidence, Section 65B has a special component of electronic record, and thus the said evidence could only be dealt under Section 65B. Hence, it is only after the electronic evidence is produced as per aforesaid section that the question of its genuineness would arise and thereafter opinion of experts under Section 54A of the Evidence Act could be recorded. With the possibility of electronic evidence, being vulnerable, to be manipulated and to be abused, strict adherence to the required procedure is essential. Further, the Hon'ble Delhi High Court in *State of Delhi* v. *Mohd. Afzal and Others*[41], has held that 'electronic records are admissible as evidence'. However, in *Dharambir* v. *Central Bureau of Investigation*[42] it was held by the Delhi High Court that "While there can be no doubt that a hard disc is an electronic device used for storing information, once a blank hard disc is written upon it is subject to a change and to that extent it becomes an electronic record. Even if the hard disc is restored to its original position of a blank hard disc by erasing what was recorded on it, it would still retain information which indicates that some text or file in any form was recorded on it at one time and subsequently removed as by the use of software programs, it is possible to find out the precise time when such changes occurred in the hard disc. To that extent, even a blank hard disc which has once been used in any manner, for any purpose will contain some information and will therefore be an electronic record." Furthermore, in *Rakesh Kumar and Ors.* v. *State*,[43] the Hon'ble High Court of Delhi while making call records as admissible piece of evidence observed that any computer-generated electronic records would be evidence if the same is proved as per Section 65B of Indian Evidence Act.[44]

To facilitate the admissibility of electronic records, Section 92 of IT Act, 2000,[45] led to an amendment to the Indian Evidence Act, wherein certain presumptions with respect to electronic evidence were raised.

---

39. *State NCT of Delhi* v. *Navjot Sandhu* [(2005) 11 SCC 600].
40. *Supra* note 27.
41. *State of Delhi* v. *Mohd. Afzal and Others*, 107 (2003) DLT 385.
42. *Dharambir* v. *Central Bureau of Investigation*, 148 (2008) DLT 289.
43. *Rakesh Kumar and Ors.* v. *State*, Crl. Appeal No. 19/2007.
44. *Ibid.*
45. *Ibid.*

Under Section 81A of the said Act, there would be presumption as to the genuineness of every electronic record purporting to be the Official Gazette.

Section 85A raises a presumption as to "every electronic record purporting to be an agreement containing the digital signatures of the parties was so concluded by affixing the digital signatures of the parties."

Further Section 90A creates a presumption as to the authenticity of electronic records which are five years old and is produced from custody of a person.

Electronic Signature

Electronic signature has been defined under Section 2(ta) of IT Act, 2000,[46] as "authentication of any electronic record by a subscriber by means of the electronic technique specified in the second schedule and includes digital signature."

Section 5 of the Act of 2000 gives legal recognition to electronic signature.

With the provision for admissibility of electronic evidence, Section 67A deals with the proof of electronic signature wherein "except in cases of a secure electronic signature, if electronic signature of any subscriber is alleged to have been affixed to an electronic record, such electronic signature of the subscriber must be proved."

Now electronic signature can be of various types, that is, from typed name to digitised image of a signature, but such signatures are prone to tampering, hence only those electronic signatures are considered reliable if the technique employed could be linked to the creator of the message and is under the control of the maker of signature. Any change made to such a signature must be detectable.

Electronic Agreement

E-contract has been given validity by virtue of Section 10A of the IT (Amendment) Act, 2008, which states that "wherein a contract formation, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose." The agreements can be categorised into web-wrap agreements[47] and shrink-wrap agreements.[48] For any contract to be valid, it has to be signed by both the parties. Various sections of IT Act lays down

46. *Ibid.*
47. Agreements in which a party gives assent by way of clicking on 'I agree' or 'I accept' buttons.
48. These are agreements which are accepted by users when they install a software from CD ROM.

the provisions to deal with various aspects of determining as to when electronic record could be attributed to the originator (Section 11), what would be considered as acknowledgement of receipt (Section 12) and time and place of dispatch and receipt of electronic record (Section 13). Moreover, such contracts have been recognised by court of law as legally enforceable. In *Anver Nasheer* v. *PK Basheer*,[49] it has been observed by the Apex Court that "There may be revolution within the way that proof is produced earlier than the courtroom."

The Hon'ble Supreme Court of India, in the case of *FZE Limited Dubai* v. *Vendata Aluminium Ltd.*[50] held that a contract accepted unconditionally between two parties through email was a valid contract.

ADDITIONAL/SUGGESTIVE TECHNOLOGY USED IN INVESTIGATION

This section discusses the scientific procedures used by the Investigating and Law Enforcement Agencies globally and their legal backing.

Mobile Tracking

The GPS of the phone of the accused can be used to track the location in order to collect the evidence; however the tracking is not done in every case and is also subject to approval from the Central Government or the State Government, which means from the Home Secretary or Chief Secretary of the State, respectively. Also, mobile-phone-tracking devices can be used to detect the chain of people in the crime syndicate. In 2018, the US Supreme Court held that the police shall require a court-approved warrant in order to fetch the data of any individual through mobile tracking. The US Supreme Court held the practice of free mobile tracking in contradiction to the Fourth Amendment of the US Constitution.[51] Meanwhile, the Centre for Development of Telematics, under the Department of Telecom, in collaboration with Delhi Police and telecom service providers in India developed an online portal for mobile tracking of stolen phones in the cities of Delhi and Mumbai, where the citizens can file a request to track their phones along with the copy of the First Information Report.[52] Recently, amidst the coronavirus pandemic, the Central Government of India offered each State under Section 5(2) of Indian Telegraph Act to mass track the citizens in order to keep

49. *Anver Nasheer* v. *PK Basheer*, AIR 2014 SCW 5695.
50. *FZE Limited Dubai* v. *Vendata Aluminium Ltd.*, 2010 (1) SCALE 574.
51. Lawrence Hurley, 'Supreme Court Restricts Police on Cell Phone Location Data', *Thomas Reuters* (22 June 2018), available at:https://www.reuters.com/article/us-usa-court-mobilephone/supreme-court-restricts-police-on-cellphone-location-data-idUSKBN1JI1WT, last accessed on 11 May 2020.
52. ET Bureau, 'DoT Launches Portal to Track Lost/Stolen Phones', *Economic Times* (30 December 2019).

surveillance on those in quarantine as well as to inform the people in the containment zones.[53] According to Section 5(2) of the Act, legal interception of telecommunications is allowed in the case of public emergency or to prevent a crime, and thus it was invoked by the government in mass tracking stating that to evade the quarantine is a criminal offence and thus, mass tracking of mobile phones is justified.

Cell Tapping

In India, whereas telephone tapping is not allowed by private individuals, however under Section 5(2) of the Indian Telegraph Act, 1885, "on the occurrence of any public emergency, or in the interest of the public safety, the Central Government or a State Government or any officer specially authorised in this behalf by the Central Government or a State Government may, if satisfied that it is necessary or expedient so to do in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of an offence, for reasons to be recorded in writing, by order, direct that any message or class of messages to or from any person or class of persons, or relating to any particular subject, brought for transmission by or transmitted or received by any telegraph, shall not be transmitted, or shall be intercepted or detained, or shall be disclosed to the Government making the order or an officer thereof mentioned in the order: Provided that the press messages intended to be published in India of correspondents accredited to the Central Government or a State Government shall not be intercepted or detained, unless their transmission has been prohibited under this subsection."

However, the Supreme Court in the case of *People's Union of Civil Liberty* v. *Union of India*[54] observed that Section 5(2) does not confer unguided and unbridled power on investigating agencies to invade a person's privacy and the right to have telephonic conservation in the privacy of one's home or office is enshrined in Article 21 of the Indian Constitution, and "the said right cannot be curtailed except according to the procedure established by law."

DNA Profiling

DNA profiling is a forensic technique used in criminal investigations, wherein the profile, that is, the specific DNA pattern is obtained from a person's bodily tissue and is compared to the DNA in the evidence collected, so as to assess the likelihood of their involvement in the crime. Though the permission to take the DNA sample of

53. Madhukalya Amrita and Ramachandran Smriti Kak, 'Centre Tells State to Use Mobile Tracking Method for Quarantine Enforcement', *Hindustan Times* (18 April 2020).
54. *People's Union for Civil Liberties (PUCL)* v. *Union of India* [(1997) 1 SCC 301].

the accused has to be obtained from the concerned judicial authority as well as the accused, the results of the tests shall not fall under the statements 'pertaining to self-incrimination by the accused' under Section 23 of Indian Evidence Act.[55]

Chromatography

The process of Chromatography means the segregation of various components of a mixture into its components or stationary phase (normally solid or solid quoted with liquid) under the influence of mobile phase (liquid or gas).

This scientific technique is used in gathering evidence. For example, in a case of murder, the first thing done to search for the cause of death is the process of extraction, which is segregating the compounds in isolation. They are then made in liquid solutions, which are dissolved in various solvents to make it a soluble form. Then they are tested primarily by the Color Test, either at the laboratory or at the crime scene. Further, the results are tested through thin-layer chromatography. The final confirmation is conducted through the use of an instrument called UV Spectrophotometer.

Artificial Intelligence

Artificial Intelligence is the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions. On 30 January' 2020, the State of Kerala identified its first COVID-19 patient. Within a span of one week, they introduced robots to sanitise passengers coming out of the airport. Automated cars, autopilot in the planes, and so on come under the periphery of Artificial Intelligence. Moreover, biometrics, fingerprints as well as retina scan can be put under the ambit as well.

In early times, fingerprint scanning was used to search for children who ran away from their homes. After the introduction of Aadhar Cards, problems relating to biometrics have been reported by a huge number of citizens. This is because of privacy concerns as Aadhar consists of biometric data which can be misused against any individual by the authorities who are not allowed to. With regards to iris scanning and facial recognition in India, only competent authorities are allowed to access the data. This technology may help security agencies to identify and catch criminals with a criminal history. It will also be time saving and energy saving too. This aids the police to track the criminals, because facial recognition is software which uses all kinds of data present on social media and police databases. Social media is another platform through which a person can easily be tracked with the help of facial recognition. Nowadays everyone

55. *Ibid.*

is using social media like Facebook, Instagram and Twitter; all these platforms have privacy policy but applicable terms and conditions. Technology is improving day by day and the government is taking everything to the digital arena with a thought of easy availability of data and information for all. Face recognition, fingerprints and retina are scanned during the process of passport application. This is done so that when the person goes to a foreign country, and should an emergency situation arise he can be easily identified based on the data stored with the agency. Using all these data, a person's record can be maintained at every level.

It was found by the National Crime Records Bureau that, "In the year 2018, FP staff from SFPBx visited 36,627 crime scenes and found 40,111 chance prints fit for comparison. SFPBx has forwarded details of 144 important cases solved through finger prints in the calendar year 2018 to CFPB for inclusion in the annual report, out of which 63 were shortlisted for publishing in 'FPI 2018' under murder, theft, dacoity, robbery, Arms Act and NDPS Act."[56]

Facial recognition and fingerprint scanning are nowadays a trend and are available in smartphones and iPhone. This is also alarming from the point of the privacy of the user; however everyone is using it on the basis of trust. The use of technology thus must be limited and specific.

In India, National Institution for Transforming India (NITI) Aayog considered the importance of AI in different sectors in a policy paper, 'National Strategy for Artificial Intelligence'[57], in June 2018. Further, it was proposed in the Budget Report of 2019 that a national program on AI be launched. Now "while all these developments are taking place on the technological front, no comprehensive legislation to regulate this growing industry has been formulated in the country till date."[58]

Three-Dimensional Printer

3D Printer has been considered as a 'new industrial revolution' signalling a new era of manufacturing. The industry has been growing at a rapid pace and its use is not restricted, rather its application is diverse and still has scope of evolving with technology. Technology transforms Computer Aided Design (CAD) files into physical articles using different types of 3DPs, however with slightly different material. The CAD files are the blueprint of the article to be printed and are created manually using dedicated

56. A Report by National Crime Records Bureau on Finger Print in India, 2018, available at: https://ncrb.gov.in/finger-print-india, last accessed on 11 June 2020.
57. Available at: https://niti.gov.in/national-strategy-artificial-intelligence, last accessed on 09 January 2021.
58. G.S. Bajpai and Mohsina Irshad, 'Artificial Intelligence, the Law and the Future', *The Hindu* (11 June 2019).

software or 3D-scanning devices. This file is then uploaded to a 3DP which, through a layering process, creates the physical object by continuous deposit of relevant material.

The 3D-printing technology can be used for varied purposes, ranging from manufacturing automotive parts to using it in a criminal trial. Scientists have been able to reconstruct and solve 4,30,000-year-old murder mystery wherein through reconstruction, scientists could conclude on the cause of death and also state that the assailant and victim were standing face to face.[59] It has been used by investigators and forensic experts to reconstruct accident scenes and even facial reconstruction from unidentified skeletal remains. It can be used during trial to create replica of evidence and crime scene, however such use would not be new as in England at London's Old Bailey courthouse, 3D-printed skull was presented as evidence in a murder trial of Ben Butler for murdering his daughter Ellie Butler[60]. He was charged with having beaten his daughter in a fit of rage. To illustrate the extent of injuries suffered by the victim, 3D-printing was used. Yet in another case[61] 3D-printed bones were used to convict the perpetrator in a gruesome murder case by recreating the bones and showing them to be exact fit, when the body was dissected into pieces and some were burned. Further, the legal system of the United Kingdom took an extra effort to look into technology when it recreated a beer bottle, which was responsible for the brutal death of a minor who was attacked by a 42-year-old. The accused put forth the plea of self-defense which was not believable, and the replica of the murder weapon was recreated for the accused to demonstrate how the bottle was held.

3D technology can be used in forensic examination to recover latent prints and DNA from 3D printers and printed objects, and with greater understanding of the technology it would have evidentiary value. It is an excellent example of incorporation of technology in court facilities without major change in existing law. As stated above, such technology is being used in foreign countries to assist the courts; however use of such technology in trials in India seems like a distant dream. The definition of evidence under the Indian Evidence Act, 1872, brings within its ambit oral and documentary evidence, however Section 136 of the Act, 1872, gives discretion to a judge to decide on the admissibility and relevance of evidence in court. It can be decided by the presiding judge to allow or disallow evidence; however the evidence must be relevant to the

59. Thimmesch Debra, 'Materialise's Mimics 3D Modeling Software Helps Solve 430,000-Year-Old Murder Mystery', *Xometry* (28 September 2015), available at: https://3dprint.com/97717/mimics-430k-year-old-murder/, last accessed on 09 January 2021.

60. 'How 3d printing helped solve the murder case of Ellie butler', *Goprint 3D* (17 October 2019), available at: https://www.goprint3d.co.uk/blog/how-3d-printing-helped-solve-the-murder-case-of-ellie-butler/, last accessed on 09 January 2020.

61. Chris Parr, 'WMG's 3D printed bones help to solve murder case', *Times Higher Education*, (14 May 2015) available at: https://www.timeshighereducation.com/news/wmgs-3d-printed-bones-help-to-solve-murder-case/2020169.article, last accessed on 08 January 2021.

matter in dispute. Hence, though there is no explicit provision governing and bringing technological advancement within the ambit of evidence, the same is neither made inadmissible nor can be made admissible unless hit by constitutionally protected rights. Therefore, as much as technology can be used in the justice system, the potential of it being misused by criminals is higher. For them, admissibility and legality would not be an issue to use 3D-printing technology to produce guns and ammunition; hence such technology must be employed by law-enforcing agencies in investigation as well as be made admissible in court of law as evidence.

MABMAT/Virtual Reality

Inspired by NASA's Curiosity Mars Rover, Mehjeb Chowdhury of Durham University created a technology called MABMAT, which could be used in criminal trials to offer an accurate, panoramic view of the crime scene. It is a robotic system which would take comprehensive 360-degree video as well as photographs that would offer a snapshot of the crime scene. This technology, if developed, can be used via Bluetooth or a remote smart phone application. The technology does not require any 3D rendering but can run on any computer or smart phone. Further, a group of researchers at Staffordshire University created a system that would take the viewer through the crime scene.

Although with the development of technology, it could be seen that creating a crime scene is possible, the question lies in its admissibility in court of law. Though there is no legislation on admissibility of such evidence in Indian courts, the views on virtual reality were described by the Hon'ble Supreme Court of India in *Prafull B. Desai* v. *State of Maharashtra*,[62] wherein the Hon'ble Apex Court distinguished video-conferencing from the concept of virtual reality and held that video-conferencing is different from virtual reality wherein, in the latter a person is made to feel things which does not actually exist, however in video-conferencing, it is not a creation rather it is the use of technology wherein one is able to see and hear events taking place far away as they actually take place. Hence, drawing an analogy from the abovementioned judgment, evidence by way of virtual reality may not be admissible with the current legislation and would call for an amendment of existing legislation or enacting of legislation for the same.

Throwbot 2 (TB2)

One could never imagine a throwable micro-robot platform which would enable the operator to obtain video and audio view within indoor and outdoor environments. This robot can be dropped from up to 30 feet onto concrete and can crawl over a variety of

62. *Prafull B. Desai* v. *State of Maharashtra* (2003) 4 SCC 601.

terrain clearing obstacles upto 5 cm tall, however its efficiency could be increased with the use of a conversion kit. This is being used by law-enforcing agencies to reach and explore crime scenes which are dangerous or which are not easily accessible. In the first six months of 2016, around 201 robots were transferred from the US military force to the police force,[63] however most of these robots are used to gather intel or bomb disposal. Robots were used by the US police department to kill a suspect who was believed to have shot five police officers. The explosive for the same was carried by a robot.[64]

ShotSpotter

Gunshot detection systems are being used to "identify, discriminate, and report gunshots by the use of acoustic sensing technology. It detects the sound of gunshot and the transmitter sends a message to the police dispatch centre and a computer to receive and display that message." A criminal was apprehended in Fresno California in 2017 when ShotSpotter enabled the police to trace the killer's movement and was able to apprehend him in 4 minutes 13 seconds.[65] However, use of ShotSpotter was questioned when it could record conversation between two individuals.

Thermal Imaging

It is a technology which is helpful in dark conditions wherein thermal image cameras utilise infrared imaging to detect heat emission by human and animal body and deliver a heat picture or heat map. It can be used to trace the movement of a person in a dark building. Now as much as it can be used to detect a person, it can be used in search and seize and thereby collecting evidence. With the use of thermal screen processes well within the constitutional framework, it could be an added aid to police to carry investigation.

PSYCHOANALYTIC TESTING/DECEPTION-DETECTION TESTS

"Neuroscience is concerned with the structure, function, development, chemistry, pharmacology and pathology of the human nervous system."[66] "It is the study of function of the brain as well as the effects of stimuli on parts of brain and cerebral performance." Deception-detection test includes within its swipe polygraph, narco-analysis and brain mapping, which

63. Kann Drew, 'Why Your Local Police Force Loves Robots', *CNN US* (18 April 2017), available at: https://edition.cnn.com/2016/11/10/us/police-officers-future-technology-lisa-ling/index.html, last accessed on 10 May 2020.
64. McFarland Matt, 'Robot's Role in Killing Dallad Shooter Is a First', *CNN Business* (1 July 2016).
65. MacBride Elizabeth, 'The Scientist, The Investor and the CEO: How "Shots Fired!" Technology Turned a Profit' (30 October 2018), available at: https://www.forbes.com/sites/elizabethmacbride/2018/10/30/the-scientist-the-investor-and-the-ceo-how-shotspotter-turned-a-profit-after-22-years/#5066a18d468c, last accessed on 10 May 2020.
66. *Stedman's Medical Dictionary*, 24th Ed. (1982), 949.

can be used to extract concealed information related to a crime from a person. These tests are often used during investigation as well as during trial to collect vital information.

Polygraph Tests

In polygraph tests, different bodily responses are used to determine the veracity of a statement made by a person. It includes measuring blood pressure and change in a person's breathing pattern. It mainly involves asking controlled questions and then the responses are compared to the key questions. Though the choice of the technique involved is slightly different, the technology involved remains largely the same.[67] It is to be noted that this technology does not measure deception or lying, rather it only shows the possibility of a person deceiving the interviewer.[68]

Narco-analysis Tests

"Narco-Analysis is a method of administering intravenous hypnotic medication called the truth drugs to procure vital information."[69] "It involves monitoring of a person's blood pressure, pulse or EGC after injection of Sodium pentothal which is administered intravenously along with dextrose over a period of three hours."[70] Though the use of the aforesaid chemical sedates a person and puts him to sleep, it is an absolute mandate that the level of consciousness be kept and the patient be kept in a drowsy state.[71]

Brain Mapping

"It is a technology which measures the change in the electrical field produced by neuronal activity in the brain by means of electrodes placed on the surface of the skin covering head and face."[72] The subject is exposed to various stimuli, and it works on the underlying theory that if the accused is guilty, it would lead to emission of a wave compound which is recorded by the instrument. However, it only tests the memory of a person with the consent of the person, and the possibility of a person who has witnessed the crime to be implicated as an accused cannot be completely ruled out.[73]

---

67. Gareth Evans, 'How Credible Are Lie Detector Tests?', *BBC News* (4 October 2018)
68. *Ibid.*
69. Anonymous, "What Is Narco-Analysis, Polygraph Test And Brain-Mapping?" *Deccan Herald*, May 5' 2010, New Delhi, vailable at: https://www.deccanherald.com/content/67647/what-narco-analysis-polygraph-test.html, last accessed on 10 May 2020.
70. 'What Is the Narco Analysis Test That the Kathua Rape Case Accused Are Asking For', *India Today* (17 April 2018).
71. *Ibid.*
72. C.D. Lefebvre, et al., 'Use of Event-Related Brain Potentials (ERPs) to Assess Eyewitness Accuracy and Deception', *International Journal of Psychophysiology*, 73 (2009): 218–225.
73. Gautam Bhatia, 'Privacy and the Criminal Process: Selvi v. State of Karnataka', *SSRN* (22 April 2018).

It brings within its ambit the right of a person against self-incrimination. It was held in *Gobind Singh* v. *State of Madhya Pradesh*[74] that the mental state of a person comes within the ambit of 'Right to privacy', which later was brought under the ambit of Article 21 as a fundamental right. The admissibility of narco test, lie-detecting test and brain-mapping test was brought to rest by the Hon'ble Supreme Court in *Selvi* v. *State of Karnataka*.[75] The concern before the court was not only with respect to violation of fundamental right under Articles 20(3) and Article 21, rather it also concerned medical ethics while administering this technique and violation of human rights of an individual. The three-bench judge[76] observed that

> *"we hold that no individual should be forcibly subjected to any of the techniques in question, whether in the context of investigation in criminal cases or otherwise. Doing so would amount to an unwarranted intrusion into personal liberty. However, we do leave room for the voluntary administration of the impugned techniques in the context of criminal justice, provided that certain safeguards are in place. Even when the subject has given consent to undergo any of these tests, the test results by themselves cannot be admitted as evidence because the subject does not exercise conscious control over the responses during the administration of the test."*

Emphasising on the protection of fundamental right,

> *"The Court observed that This Court has recognized that the protective scope of Article 20(3) extends to the investigative stage in criminal cases and when read with Section 161(2) of the CrPC, 1973, it protects accused persons, suspects as well as witnesses who are examined during an investigation."*

The test results cannot be admitted in evidence if they have been obtained through the use of compulsion. Article 20(3) protects an individual's choice between speaking and remaining silent, irrespective of whether the subsequent testimony proves to be inculpatory or exculpatory. Further, a Bench comprising the then Chief Justice of India, Dipak Mishra, and Justice DY Chandrachud of the Hon'ble Supreme Court of India has held in a case filed by Sidhu Yadav, who volunteered to undergo narco-analysis to prove his innocence in case under Protection of Children from Sexual Offences (POCSO) in 2017,[77] that *"no accused in the criminal case can volunteer to undergo such a test to prove*

---

74. *Govind Singh* v. *State of Madhya Pradesh*, 1975 AIR 1378.
75. *Selvi* v. *State of Karnataka* (2010 (7) SCC 263).
76. *Ibid.*
77. Mahapatra Dhananjay, 'Accused Can't Seek Narco Test to Prove Innocence', *The Times of India* (9 September 2017), available at: https://timesofindia.indiatimes.com/india/accused-cant-seek-narco-test-to-prove-innocence-sc/articleshow/60432928.cms, last accessed on 09 May 2020.

innocence." Hence, any statement made during a narco-analysis test is not a piece of evidence and hence not admissible.

CYBERCRIMES

The internet has been in use by almost every person worldwide. However, there is also a vertical aspect to the internet. What we see and surf can only be called as the tip of the iceberg. There are three layers of internet, which includes Surface Web, Deep Web and Dark Web.

The Surface Web is the most used web, wherein every day-to-day surfing is done by an individual. It is used by an individual for searching on Google or any search engine – from sending an email, to posting on any networking sites such as Facebook, Instagram, Twitter or resorting to online shopping sites or watching any video on Youtube – it is used for all. It includes very few percentage of the web.

The Deep Web content includes private content including email and chat messages, other content on social media sites, electronic bank statements, electronic health records (EHRs) and other content accessible over the internet but not indexed by search engines like Google, Yahoo, Bing, etc. This area of web cannot be accessed by anyone, but only through a portal site by individuals who have been granted access privileges or using Virtual Private Network (VPNs).

Lastly, it is the Dark Web with the least or NIL security and safety. This space of the web can be used for the trafficking of guns, ammunition, drugs and other illegal items and has become a platform for various criminal activities. It is out of the purview of usual search engines to lead to the Dark Web.

The use of technology in committing crimes is done to the maximum extent in the case of cybercrimes, in which the committal as well as investigation is conducted through computers. Recently, Cyble, the online intelligence firm, released that information such as email, phone number, work experience and home address of around 2.9 crore Indians seeking jobs have been posted on the Dark Web for free on a hacking forum.[78]

Cybercrimes, like cyberspace, is not finite and brings within its ambit a plethora of acts committed in cyberspace; however few rampantly committed cybercrimes are hacking, cyber pornography, bullying, stalking, email bombing, email scams, online banking frauds, phishing, hacking and the list goes on. Hacking is made punishable

78. Anonymous, 'Cyber Criminals leak Personal Data of 2.9 Cr. Indians on Dark Web for Free', *Economic Times* (23 May 2020).

under Sections 43 and 66 of the IT Act, 2000,[79] wherein a person who accesses a computer source, computer system or computer network without permission of the owner or downloads, copies and extracts any data or cause disruption of any system; would be liable for damages, and if any of the aforesaid act is committed fraudulently or dishonestly, under Section 66 such act is punishable for a term up to 3 years or with fine of up to five lakhs. Further, though phishing was punishable, after the 2008 Amendment to IT Act, the offence was made more defined and expansive under Sections 66D, 74 and 66C of the Act. The Hon'ble High Court of Delhi [80] has defined phishing as a form of internet fraud wherein a person pretends to be a legitimate associate of a bank or an insurance company and extracts personal data from the user, which in turn are used by him for his advantage. Under Section 66C of IT Act, identity theft or identity fraud is a punishable offence that is fraudulent, or dishonest use of electronic signature, password or any other unique identification feature of any other person is punishable. Further, Section 419 of the Indian Penal Code'1860 punishes the offence of "cheating by impersonation" which is complimented by Section 66D of IT Act as the said section makes cheating by impersonation using a computer resource a punishable offence. The IT Act is the only legislation which covers cybercrimes, however it has been criticised for its soft-hearted approach on criminals where the majority of the crimes are bailable offences and has less quantum of punishment.

The admissibility of evidence before the court of law is not an issue subsequent to the amendment to IT Act, however collection of evidence is one of the major concerns in cybercrimes as there can be no marking of a crime scene or network and be kept as an exhibit before the court. The traditional methods of production, storing of information and records cannot be used and hence procurement and preserving of evidence is another issue in cybercrimes. This hindrance makes the process of trial and proving of charges beyond reasonable doubt, very difficult. Another stumbling block is the anonymity which the internet provides to a user, and the ease with which evidence could be erased once crime is committed. Usually in cybercrimes, evidence includes data, network, gadgets and log files with trails of events which emanate as crime. Most of the cybercrimes committed are made punishable under the Indian Penal Code along with various sections of IT Act. Though the National Cyber Security Policy 2013 and 2020 (yet to be passed by government) aims to facilitate creation of a secure cyberspace and strengthen the existing regulatory framework, we lack competent authority to investigate such cases.

---

79. *Ibid.*
80. *National Association of Software and Service Companies* v. *Ajay Sood*, 119 (2005) DLT 596.

Though the nature, tool, methods or even the space in which cybercrime is committed is different from usual crimes, however in India, there is no special body or investigating agency which is designated to investigate such crime. It has been provided under the Act, 2000 that the investigating officer for offences under IT Act 'shall not be below the rank of Deputy Superintendent of Police'.[81] Although most of the States in India have cybercrime cells which are specialised units that handle cybercrimes, they mostly rely on private firms and consultants to solve cybercrime cases.[82] Further, along with police personnel being trained by internet firms, assistance are sought from ethical hackers and hackathons are conducted. Even though such consultants are not barred under the law, with the increasing number of cybercrimes, there is a need for a framework on training experts and engaging them to solve such crimes.

Technology Misuse in Election Matters

In a case arising from election trial, the admissibility of tape-recorded conversations under the relevant provisions of the Indian Evidence Act was examined by the court in *Ram Singh* v. *Col Ram Singh.*[83] The court held that a tape-recorded statement would be an admissible piece of evidence, subject to the following conditions:

> *(1) The voice of the speaker must be duly identified by the maker of the record or by others who recognize his voice. In other words, it manifestly follows as a logical corollary that in the first condition for the admissibility of such a statement is to identify the voice of the speaker. Where the voice has been denied by the maker it will require very strict proof to determine whether it was really the voice of the speaker.*
> *(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.*[84]

---

81. Section 78 of Information Technology Act, 2000.
82. Chandrashekhar and Mohanty, "Police in State across India Are Relying on Private Firms and Consultants to Solve Cyber Crime', *The Economic Times* (13 December 2019).
83. *Ram Singh* v. *Col. Ram Singh* (1985 Suppl SCC 611).
84. *Ibid.*

The use of Electronic Voting Machines (EVMs), on the pretext of its possibility of being hacked, has been banned in countries including Germany, Netherlands and the United States of America. Besides, countries like England and France never used EVMs in the first place. The German Constitutional Court ruled in 2009 that voting through EVMs was unconstitutional, holding that transparency is a constitutional right but efficiency is not a constitutionally protected value.[85] "Further, the Court observed that EVMs fail the test of legitimacy of any polling method, which includes:[86]

1) *the voter can visually confirm that his/her selection has been registered;*

2) *the voting happens in secret;*

3) *and the counting happens in front of his/her representative's eyes."*

Meanwhile, there is an ongoing debate in India regarding the likelihood of tampering with Electronic Voting Machines.

Misuse of Technology in Banking Sector

With the growing aspect of e-commerce and e-transactions, India too has been experiencing a rapid surge in digital crimes being committed in the Banking Sector. The banks possess vital information of its customers, which are kept as confidential information. However, with the use of technology, bank insiders as well as people who can gain access to this information through software hacking are susceptible to commit various crimes which includes, but are not limited to, offences related to the funds of the customers and their personal information.

Cybercrimes which are committed using online technologies to illegally remove or transfer money to different accounts are tagged as banking frauds.[87] Other than banking frauds, the offences may include credit card fraud, spamming, spoofing, phishing, e-money laundering, identity theft, ATM fraud, denial of service, and so on. As the use of technology is wide under these head of offences, the electronic evidence produced must be subjected to strict cross-examination, verification, Expert Opinion and strict adherence to legal checks as enumerated in the case of *Anvar PK* v. *PK Basheer & Ors.*[88]

---

85. Anonymous, 'England, Italy, Germany Have Banned Their EVMs: What Were Their Reasons?', *The Quint* (09 May 2017), available at: https://www.thequint.com/news/politics/reasons-for-evm-bans-aap-expose, last accessed on 09 May 2020.
86. G. Sampath, 'Why EVMs Must Go', *The Hindu* (24 January 2019).
87. A.R. Raghavan and Latha Parthiban, 'The Effect of Cybercrimes on a Bank's Finances', *International Journal of Current Research and Academic Review*, 2(2) (February 2014): 173–178, ISSN: 2347–3215.
88. *Supra* note 27.

LEGAL IMPEDIMENTS RELATED TO FORENSIC EVIDENCE

Authenticity of the Evidence

In *Ram Singh and Others* v. *Col. Ram Singh*,[89] relying upon the judgments of *R.* v. *Maqsud Ali*,[90] *R.* v. *Robson*[91] and American Law[92] it was approved to the effect that

> *"it will be wrong to deny the law of evidence advantages to be gained by new techniques and new devices, provided the accuracy of the recording can be proved. Such evidence should always be regarded with some caution and assessed in the light of all the* circumstances of each case. *Electronic evidence was held to be admissible subject to safeguards adopted by the Court about the authenticity of the same. In the case of tape-recording it was observed that the voice of the speaker must be duly identified, accuracy of the statement was required to be proved by the maker of the record, possibility of tampering was required to be ruled out. Reliability of the piece of evidence is certainly a matter to be determined in the facts and circumstances of a fact situation. However, threshold admissibility of electronic evidence cannot be ruled out on any technicality if the same was relevant."*

In *Tukaram S. Dighole* v. *Manikrao Shivaji Kokate*,[93] the above principle was reiterated. The court observed that

> *"new techniques and devices are order of the day. Though such devices are susceptible to tampering, no exhaustive rule could be laid down by which the admission of such evidence may be judged."* Hence, the court observed only one rule to be followed, that is **"Standard of proof of its authenticity and accuracy has to be more stringent than other documentary evidence."**

The necessity for authenticity and certification by the witness arises from the high chances of tampering during recovery; time elapsed, fake witnesses as well as third party influence. Moreover, the admissibility of electronic as well as evidence obtained through technology has already been discussed in the above paragraphs, which essentially sum out to be 'Best Evidence Rule'.

Recording of the Witness Statement

The statement of the witness made before the police official under Section 161 of the CrPC or before the Magistrate under Section 164 of CrPC, is considered as an important

89. *Ram Singh and Others* v. *Col. Ram Singh* [1985 (Supp) SCC 61].
90. *R.* v. *Maqsud Ali* [(1965) 2 All ER 464].
91. *R.* v. *Robson* [(1972) 2 ALL ER 699].
92. American Jurisprudence 2d (Vol. 29), 494.
93. *Tukaram S. Dighole* v. *Manikrao Shivaji Kokate* (2010) 4 SCC 329.

piece of evidence in criminal trial, though the importance attached to each of the statements made is different. When we lack the aid of technology during the investigation stage due to lack of laboratories or proper training, technology can be used during the trial stage in recording the evidence made by the witness. This audio–video recording of the statement could be further extended to dying declaration and confession by the accused. Change or contradiction of the statement of the witness during the trial, which extends for even decades, frequently leads to miscarriage of justice and hence, also suggested by Malimath Committee, the recording of statement made by the witness can be done through video–audio recording. Though with the Criminal Procedure (Amendment) Act, 2008, statements can be recorded by audio–video electronic means under Section 161 CrPC, such provision is yet not mandatory rather the discretion has been left to the police officer as the same would place undue and heavy burden on the officer recording the statement.[94] However, the effectiveness and accuracy which the use of technology can add to the criminal justice system could not be more emphasised. It is not that the use of technology has not been contemplated by the legislature. Section 32 of the Prevention of Terrorism Act, 2002, provides for the recording of confessional statement of accused either by writing or by use of electronic devices from which sound and image can be reproduced. Further, such recorded confessional statements have been made admissible under Section 18 of Maharashtra Control of Organized Crime Act, 1999.

Moreover, the Hon'ble High Court of Delhi[95] has observed that recording witness statements would lend immense credibility to witness. It was further observed by the Bench of Justice Vipin Sanghi and Justice IS Mehta that storage of digital media by whichever way, would be less space-consuming than the space required for conservation of manually recorded proceeding or statement on paper. Furthermore, the Division Bench of Justice S. Vaidyanathan and N. Anand Venkatesh, High Court of Madras, directed the State Government to ensure that the audio–video recording facility must be provided in Magistrate, Session and Mahila Courts and arrangement must be made for storage and keeping of electronic data.[96] Hence, though we have legislation for audio–video recording of statements of witnesses and it being admissible in court of law, we lack in implementation of the same.

With the use of audio–visual recording of statement of witness and accused, it does not only create a long-lasting record, rather a statement once made by a witness cannot be retracted stating that the same was not said by him/her. Moreover, with the

94. 41st Law Commission Report.
95. Singh Soibam, 'HC for Digital Recording of Witness Statement', *The Hindu* (28 August 2018).
96. Chandar B. Tilak, 'Implement Audio/Video Recording of Witness Statements', *The Hindu* (29 November 2019).

audio–video recording of the statement the demeanour of the witness could also be recorded and would be easier to prove a statement in court of law. It will reduce the burden upon the police official to transfer the statement orally made into writing. Further, the audio–video recording of confession made by the accused to the police, though extra judicial and is inadmissible, the non-incriminating part of the confession can be made admissible without there being any question on fabrication. It further reduces the possibility of custodial torture or forceful recording of any statement. It also reduces to nullity the possibility of inconsistency, confusion and changing of statement during the trial. Now though the use of a system of audio–video would add to the expenses and would require improvement of infrastructure facilities and training of police officials in use of such technology, nevertheless the use of such technology would ensure a robust mechanism to realise a fair and speedy trial.

Thin Line between Right to Privacy and Collection of Evidence

The development of technology is paving new ways in the world of surveillance and monitoring criminal activities in countries across the world. The police in Scotland have developed an application named Pronto which would replace traditional paper notebook and other documentation, and officers can directly fill in a report on their mobile devices for any crime incident, record statements of witnesses and automatically submit them without going to the station. Moreover, the application would give them access to national as well as local police databases, hence saving time and making police personnel more efficient.[97] Pronto application is one example which would aid police to carry out its duty, however bypassing the right of an individual is a matter of concern.

The use of face recognition is yet another technological advancement in the Scottish Police, however it has its concerns and reservations attached. It is a method of identifying or verifying the identity of an individual using their face image and can be used to identify people in photos, video or live in a surrounding. This technology is employed in many technologically advanced countries to identify a person for any reason, let it be a criminal act, an eyewitness or a missing person. Face-recognition system picks up specific and distinctive details about an individual's face, such as distance between the eyes or shape of the chin, uses computer algorithms and then converts them into a mathematical representation that is algorithms and compares them to data on other faces collected in a face-recognition database. In San Diego, Tactical Identification System (TACIDS) is being used by law enforcement officers to take photographs and run the image against the country's mug shot database.

97. Anonymous, 'Police Scotland to Deploy Motorola Solutions Pronto, a Leading Digital Policing Application Development in Scotland', available at: https://newsroom.motorolasolutions.com, last accessed on 09 May 2020.

In Scotland, the police and security agencies are using a retrospective face-recognition system in crime investigation and are used with full authority by the Scotland Government to handle the ruckus on the street and maintain peace in the country. The cameras used for this purpose are fully equipped with sufficient data of the criminal record and criminals who had been arrested under some charges. The installed cameras with Artificial Intelligence would record live, meaning thereby the person in the crowd or street if caught doing any criminal act will be automatically identified and the police will get an update for the same, along with the location of the individual. However, the software is being criticised for its discrimination against females, and those from blacks, Asian and ethnic minority communities and is a breach of privacy for the individuals,[98] and hence is being opposed by the sub-committee of Scotland.

It is given that development and use of technology is a much-appreciated step, however such use must not be used as a tool to encroach upon people's rights and be misused. Although it has been clarified by security agencies that this technology of facial recognition would be used only for criminals and monitoring activities of the protesters on the street and would in no way interfere with the privacy of an individual, there is lack of regulation to balance between use of this technology and privacy. Moreover, the speculation of it being used against welfare of citizens cannot be overruled.

Another technological advancement which has brought Scotland police in the news is the use of cyber kiosks, which allows a police officer to gather data from mobile phones or tablets without feeding password; however none of the data can be stored, but would be deleted after examination. Though it is reported that the examination of a device would be done only when there is a legal support for such usage and when it is 'necessary, justified and proportionate' to the crime to be investigated,[99] it has been said that the technology has been used in light of the increase in involvement of digital devices in investigation which would mean increasing demand on digital forensic examination, hence with the current limitation, it would take months for investigating the devices of victims, witnesses and suspects. However, use of such technology is a breach of people's privacy and there is no legal basis or are deficient on which use of such technology is based.[100]

---

98. 'Facial Recognition: How Policing in Scotland makes use of this Technology', *Justice Sub-Committee on Policing*, 11 February 2020 (Session 5), available at: https://sp-bpr-en-prod-cdnep.azureedge.net/published/JSP/2020/2/11/Facial-recognition--how-policing-in-Scotland-makes-use-of-this-technology/JSPS0520R01.pdf, last accessed on 09 April 2020.
99. 'Police to Use Technology That Helps Search Mobile Phones', 14 January 2020, available at: https://news.stv.tv/scotland/police-to-use-technology-that-helps-search-mobile-phones?top, last accessed on 02 April 2020.
100. 'Old Law, New Tech and Continue Opacity: Police Scotland's use of Mobile Phone Extraction', 12 September 2019, available at: https://privacyinternational.org/report/3202/old-law-new-tech-and-continue-opacity-police-scotlands-use-mobile-phone-extraction, last accessed on 31 May 2020.

ShotSpotter was designed to detect gunshot. However, the use of ShotSpotter has come under criticism when it discovered and picked up a portion of a street argument between two individuals, which raised concerns about privacy of an individual and the extent of the reach of a police official.[101] While it has been reported that ShotSpotter has resulted in 60% to 90% reduction in gunfire in areas where it is located,[102] concern over civil liberty and rights is at stake. Concerns have been raised by citizens for the unknown capabilities of ShotSpotter. Right to privacy is protected under the Fourth Amendment of the US Constitution, except upon a warrant which is obtained after probable cause is established and the place of search, person or thing is specified. It protects the right of a person when there is a reasonable expectation of privacy. It has been observed by the US Supreme Court in *Berger* v. *State of New York*[103] that

> "[t]he security of one's privacy against arbitrary intrusion by the police------which is at the core of the Fourth Amendment------is basic to a free society."

The use of electronic listening devices such as ShotSpotter, which can evidently listen to a conversation, are seeking more than what it has been designed for without the mandate of the Fourth Amendment being followed. Hence, for any evidence obtained by the use of ShotSpotter to be used against an individual, it will have to pass the test of the Fourth Amendment and only when a warrant as per the process laid in the said amendment is produced; such evidence must be made admissible. Strict compliance to the mandate required must be observed by the court to keep a check upon the arbitrary use of such technology. There needs to be a balance in use of technology and protecting the rights of a person, else the world would turn into the State of Oceania, the dystopian society, as depicted in the novel *1984* by George Orwell, where every move and every word would be monitored.

Thermal screen is yet another advanced technology which can be used to invade a person's personal liberty and which was dealt by the US Supreme Court in *Kyllo* v. *United States*,[104] wherein it held that use of the thermal screen method by the police officers to look inside the house of Kyllo to indicate thermal lamps which is necessary for the production of marijuana, would amount to 'search' within the meaning of the Fourth Amendment. It was further held that if any evidence is obtained using technology which could have been obtained with 'physical intrusion' such search would fall

---

101. S. Gecas Alexandra, '*Gunfire Game Changer or Big Brother's Hidden Ears?: Fourth Amendment and Admissibility Quandaries Relating to Shotspotter Technology*', *University of Illinois Law Review* (2016): 1073–1121, available at: https://illinoislawreview.org/wp-content/uploads/2016/07/Gecas.pdf, last accessed on 02 April 2020.
102. *Ibid.*
103. *Berger* v. *State of New York*, 388 US 41 (1967).
104. *Kyllo* v. *United States*, 533 US 27 (2001).

within the ambit of the Fourth Amendment. Hence, though technology can be used to obtain evidence and make police efficient, the same has been placed below the protected right of an individual. Expectation of privacy within one's home premise cannot and should not be compromised at any cost.

GPS-tracking systems can be used to prevent crimes by its installation in a public vehicle with a panic button, however the use of the same technology when used in an individual, would amount to violation of the Fourth Amendment Right. In a landmark ruling by the US Supreme Court in *United State* v. *Jones*,[105] a GPS was installed in the vehicle of Jone's wife, and the movement of the vehicle was monitored for 28 days to establish drug-trafficking charges. It was held by the Apex Court that installation of GPS devices in vehicles constitute search within the meaning of the Fourth Amendment and any evidence obtained by warrantless use of GPS would be hit by the U.S Constitution.

With the pace at which the society and law-enforcing agencies have been using technology, even though it is considered a boon to society, there are growing concerns regarding the point where we draw the line. The court, though, has acted as a guardian for individual rights, yet with growing reliance on technology, at the same time, seems to be detrimental against the rights such as liberty and freedom. There is a need for technology to be used for crime control, or delivery of justice, but it must be handled with due care and be guided with proper regulations and guidelines for protection of individual rights.

Lack of Testing Equipment

To render 'high quality and credible forensic services' to the justice delivery system in India, on 31 December' 2002, the MHA created the Directorate of Forensic Science Services (DFSS), bifurcating it from Bureau of Police Research and Development (BPR&D). It has six Central Forensic Science Laboratories under its control, which are located at Chandigarh, Kolkata, Hyderabad, Pune, Guwahati and Bhopal,[106] approximately 30 'State Forensic Science Laboratories' and few other regional laboratories in the country.[107]

Even though the importance and the dire need of the increase in use of forensic science and technology has been emphasised in this chapter, the number of forensic science laboratories clearly do not fulfil the nation's requirement corresponding to the rate of pending litigations and increasing number of crimes. The lack of testing equipment

105. *United State* v. *Jones*, 200 US 321 (2012).
106. Information as available at: http://dfs.nic.in/, last accessed on 02 April 2020.
107. *Ibid.*

and the non-adherence to the timely testing of the evidence, often leads to delayed justice or unsolved mysteries. There has been a constant struggle in India to increase the infrastructure and manpower of these laboratories, to be able to adhere to the current lab-to-population ratio. Even though rule of law is established in Indian courts, the absence of a proper policy framework in the country, lack of scientific methods in investigations and lack of modernisation of police continue to hamper justice in India.

CONCLUSION

In the early Roman period, there existed only the hard and fast rule of 'direct evidence' in the world of judicial review. With the advancement of technology, legal systems of all the developed countries rest on the precinct of 'best evidence rule', amidst all other theories of evidences, which means that even in the absence of direct evidences, the original of a secondary document, writing or a photograph or any other electronic evidence shall be produced before the court and shall be made subject to cross-examination by the opposite party apart from a third party, who is an independent witness in the case, at the best, an expert. In other words, if there exists direct evidence of the original document, use of secondary evidence is not mandatory. This is what is accepted by the courts all over the world, especially Indian courts, which is synonymised in the doctrine of *profert incuria*. The original document rule was at first enunciated in the famous case of *Ford* v. *Hopkins*[108] in 1700, and later in *Omychund* v. *Barker* in 1745.[109] With technological support, investigation or search of truth can be made easily and quickly, but the output of a technological exploration shall be made subject to strict principles of legal scrutiny and evidentiary rules, especially when it comes to the life of a human being. But in many cases, especially in civil or quasi-criminal cases like cheque dishonour cases, falling under the negotiable instrument act, secondary evidences are also taken into consideration for admissibility of evidence, since there is no primary evidence always available and also for the purpose of easing the commercial transactions. Say for example, though there is no written agreement between the drawer and payee of the cheque, the court is mandated to presume as per law that there exists a legal obligation between them if there is a signed cheque. The Negotiable Instruments Act validates the cheque as primary evidence and rules out the necessity of all other evidence. In a fast-growing nation like India, every economic transaction occurs on the basis of such negotiable instruments like cheque, which is considered as a promissory note. Though it is not free from fallacies, which is very much criticised by many legal and forensic experts with respect to the originality of signature or existence of debt, the technological advancement of the 20th century would extend its support in eliciting

108. *Ford* v. *Hopkins* [(1700) 91 Eng Rep 250 (K.B.)].
109. *Omychund* v. *Barker* [(1745) 26 ER 15].

the veracity of originality of the signature or age of the cheque which will lead to the exploration of truth. Whenever primary evidence is available, which has tested its evidentiary corroboration, secondary evidence will be dissipated in its value. The birth and growth of technological explosion worldwide has also led various governments to formulate new laws like IT Act, 2000, or amend the Evidence Act to incorporate such evidence. Various agencies of crime investigation or detective agencies employ such laws to explore the truth beneath the surface and to produce before the courts, which started relying on electronic/digital evidence, if it is vital. Evidence means anything and everything relating to the relevance of a truth, which is in dispute, and is not only limited to computers but may also include all technological evidence. Digital evidence, though voluminous, is easy to store, but easily manipulative, modified and potentially duplicated as well. Hence, the Hon'ble Supreme Court of India, overruling the case of *State (NCT of Delhi)* v. *Navjot Sandhu alias Afsan Guru*,[110] also known as 'The Parliament Attack Case', re-interpreted the application of Sections 63, 65 and 65B of the Indian Evidence Act, 1872[111] and promulgated a new rule in the famous case, *Anwar* v. *Basheer*,[112] which has become the binding law and popularly called as the 'law of electronic evidence' in which the Hon'ble Supreme Court said,

> *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).*
>
> *It is further clarified that the person needs only to state in the certificate that the same is to the best of his knowledge and belief. Most importantly, such a certificate must accompany the electronic record like computer printout, Compact Disc (CD), Video Compact Disc (VCD), pen drive, etc., pertaining to which a statement is sought to be given in evidence, when the same is produced in evidence. All these safeguards are taken to ensure the source and authenticity, which are the two hallmarks*

110. *State (NCT of Delhi)* v. *Navjot Sandhu alias Afsan Guru* (2005) 11 SCC 600.
111. *Ibid.*
112. *Anwar P.V.* v. *P.K. Bashir & Ors.* [(2014) 10 SCC 473].

pertaining to electronic record sought to be used as evidence. Electronic records being more susceptible to tampering, alteration, transposition, excision, etc. without such safeguards, the whole trial based on proof of electronic records can lead to travesty of justice.

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.[113]

The Hon'ble Supreme Court of India further held in the case that

"The evidence relating to electronic record, as noted hereinbefore, being a special provision, the general law on secondary evidence under Section 63 read with Section 65 of the Evidence Act shall yield to the same due to Generalia specialibus non derogant, which means special law will always prevail over the general law. It appears the court omitted to take note of Sections 59 and 65-A, dealing with the admissibility of electronic record. Sections 63 and 65 have no application in the case of secondary evidence by way of electronic record; the same is wholly governed by Sections 65-A and 65-B. An electronic record by way of secondary evidence shall not be admitted in evidence unless the requirements under Section 65-B are satisfied. Thus, in the case of CD, VCD, chip, etc., the same shall be accompanied by the certificate in terms of Section 65-B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible".[114]

In another noted case of *Shafhi Mohammad* v. *State of Himachal Pradesh*,[115] in 2018, the Supreme Court ruled that,

"mandatory requirement of certificate under Section 65 B (4) is not always essential by observing that, *"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 Evidence Act cannot be held to be excluded. In such a case, procedure under the said Sections can certainly be invoked. If this is not so permitted, it will be denial of justice to the person who is in possession of authentic evidence/witness 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. Thus, the requirement of a certificate under Section 65B (4) is not always mandatory."*

113. *Ibid.*
114. *Ibid.*
115. *Shafhi Mohammad* v. *State of Himachal Pradesh* [(2018) 5 SCC 311].

Most recently, in *Arjun Panditrao Khotkar* v. *Kailash Kushanrao Gorantyal*,[116] division Bench comprising of Justice Ashok Bhushan and Justice Navin Sinha in the Hon'ble Supreme Court of India have referred the matter to the larger bench to clear the conflict between *Anvar P.V case* and *Shafhi Mohammad* case.

Resultantly, the Supreme Court has formed a three-judge Bench comprising Justice R.F. Nariman, Justice S. Ravindra Bhat and Justice V. Ramasubramanian, and embarked on the hearing, in view of conflict in the law laid down between the cases of *Shafhi Mohammad* v. *State of Himachal Pradesh* and *Anvar PV* v. *PK Basheer,* on the question

> "is the requirement of certificate under Section 65B(4) of Indian Evidence Act mandatory for production of electronic evidence?"

On July 14'2020, the three judge bench upholding *P.V Anvar* case and overruling *Shahfi Mohommad* case, had confirmed the certificate under Section 65B as a major requirement unless the document is a primary evidence under Section 62 of the Evidence Act.

The 3-judge bench, holding the ***Shahfi Mohommad*** case to be incorrect said,

> ***"the major premise of Shafhi Mohammad (supra) that such certificate cannot be secured by persons who are not in possession of an electronic device is wholly incorrect. An application can always be made to a Judge for production of such a certificate from the requisite person under Section 65B(4) in cases in which such person refuses to give it."***

Justice V. RAMASUBRAMANIAN, in the current judgment, has attempted to explain the structure of this warren, with reference to the digital images, in simple and plain words.

> *"Herein lies the interesting point: when three droplets of water fuse and then separate into three droplets, it is to be questioned whether the three droplets that merge from the bigger droplet were the identical droplets that existed before they merged. In the same way, consider a digital object that has been manipulated and added to, and the process is then reversed. The original object that was used remains (unless it was never saved independently, and the changes made to the image were saved in the original file), but another object, with the identical image (or near identical, depending on the system software and application software) now exists. Conceptually, it is possible to argue that the two digital images are different: one is the original, the other a copy of the original that was manipulated and returned to its original state (whatever "original" means). But both images are identical, apart from some additional meta*

116. *Arjun Panditrao Khotkar* v. *Kailash Kushanrao Gorantyal* (Civil Appeal no(s). 20825–20826 of 2017).

data that might, or might not be conclusive. However, it is apparent that the images, if viewed together, are identical – will be identical, and the viewer will not be able to determine which is the original, and which image was manipulated. In this respect, the digital images are no different from the droplets of rain that fall, merge, then divide: there is no telling whether the droplets that split are identical to the droplets that came together to form the larger droplet."