INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

ISSN: 2582-6433

November 2026

RESEARCH ARTICLE

From Algorithmic Match To Judicial Finding: A Comparative Study Of Facial-Recognition Evidence In India, The United States And The United Kingdom And A Proposed Indian Facial Recognition Evidence Reliability Framework (IFRERF)

Rishi M

Ramaiah school of law

www.ijlra.com

ABOUT THE JOURNAL

International Journal for Legal Research and Analysis (IJLRA)

ISSN: 2582-6433

IJLRA provides a platform for scholarly writing and discussion on law, legal research and interdisciplinary questions. Research articles explore legal principles, institutions, policy and contemporary developments.

Journal website: www.ijlra.com

PUBLICATION INFORMATION

International Journal for Legal Research and Analysis

ISSN: 2582-6433

Editorial note

The views and arguments expressed in this article are those of its author(s). Readers should consult the original legal authorities and sources cited in the manuscript.

Copyright and permissions are subject to the applicable publication agreement.

ARTICLE DETAILS

From Algorithmic Match To Judicial Finding: A Comparative Study Of Facial-Recognition Evidence In India, The United States And The United Kingdom And A Proposed Indian Facial Recognition Evidence Reliability Framework (IFRERF)

Author: Rishi M

Institution: Ramaiah school of law

Journal: International Journal for Legal Research and Analysis

ISSN: 2582-6433

From Algorithmic Match To Judicial Finding: A Comparative Study Of Facial-Recognition Evidence In India, The United States And The United Kingdom And A Proposed Indian Facial Recognition Evidence Reliability Framework (IFRERF)

Rishi M

Ramaiah school of law

Abstract:

The use of Artificial Intelligence (AI) is becoming more prominent in Facial Recognition. Issues therefore arise as to the reliability and acceptance of evidence gained using AI. Police have used facial recognition to analyse video and still images in order to identify potential offenders and match them against photographic databases. Although facial recognition can be a valuable investigative tool, it can also be unreliable. Issues regarding reliability can also relate to technology and databases, as well as human factors. A comparative analysis is made of the situation in the United States and the United Kingdom so as to assess the current evidential regime operating in India relating to AI facial recognition. India has legislation in place relating to 'Expert Opinion Evidence' and 'Electronic Evidence'. These are found in the Bharatiya Sakshya Adhiniyam, 2023. However, in India there is presently no legal guidance which addresses the reliability of technology related evidence. In the United States, Daubert and expert evidence criteria may be used to assess reliability. Similarly, the United Kingdom has a wealth of case law to draw upon to assess computerised facial recognition. Equally importantly, R (Bridges) v. Chief Constable of South Wales Police emphasises the need for a sound legal foundation on which to base technology based investigations. Furthermore, the UK is highly committed to analysing the effects of technology and to furthering equality. This is a mixed methodological research project, analysing relevant legal, case and academic material. This research asserts that Indian courts need to be able to distinguish between AI and reliable evidence. Therefore, an Indian Facial Recognition Evidence Reliability Framework (IFRERF) is suggested. The framework includes six key judicial aspects – (i) legality of acquisition; (ii) source verification; (iii) reliability; (iv) assessment of human factor involvement; (v) information sharing and (vi) right to a proper defence. Consideration is also given to the evidential value and further validation. Although Facial Recognition Technology can provide valuable assistance during criminal investigations, human judgment should not be removed. Even where an AI facial recognition system identifies a match for an individual, this should not necessarily be presumed reliable. Reliable evidence should be analysed by open, independently reviewed and appropriate judicial procedures prior to being used in respect of a defendant.

Keywords: Artificial Intelligence, Facial Recognition Technology, Criminal Evidence, Algorithmic Bias, Electronic Evidence, Expert Opinion, Fair Trial, Bharatiya Sakshya Adhiniyam, Comparative Legal Research.

Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 39, 61–63 (India) [hereinafter BSA].

.Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579, 589–95 (1993).

R(Bridges) v. Chief Constable of South Wales Police [2020] EWCA Civ 1058, [91], [124], [130]–[131], [151][154], [199]–[202] (Eng.) [hereinafter Bridges].

Hypothesis:

India recognises the value in electronic and scientific evidence, but is thought to not yet have suitable processes in place to effectively analyse and assess the science behind AI face recognition. Should this be the case, there is believed to be a risk that the Courts and investigating agencies will come to depend too heavily on face recognition technology. Using, and effectively merging, relevant components of U.S. and U.K. law it is proposed that India can further develop its analysis of face recognition. Within the U.S., there is much importance placed on the scientific assessment of evidence. Moreover, within the U.K. there is a strong focus on correct application of the law, transparency and independent analysis.

Thus, many areas of both U.S. and U.K. law can be used to further support India's evidence analysis. It is therefore proposed that:

1. Electronic and scientific analysis are separate areas of law.

2. A person's likeness score should not be taken as conclusive.

3. Defence lawyers need sufficient knowledge of, and analysis relating to, both the face recognition technology and process so that they can effectively counter the prosecuting party's evidence.

4. Furthermore, independent scientific analysis and associated evidence should be accessible to allow for an analysis of face recognition technology.

5. Structured judicial analysis of science can continue to further the concept of an individual's entitlement to a fair trial and at the same time allow for suitable application of AI in criminal investigations.

Research Problem:

CCTV and photographic images are regularly used by the police, and are then compared to a database. Thus technology can be utilised in the investigation process and the police can identify who they consider may have committed a crime. Concerns have been raised about how to scientifically determine the validity of facial recognition technology. Usually police will review CCTV footage and identify individuals that they believe may be linked to a crime. They can then input this into facial recognition programme. This programme will endeavour to identify a corresponding image and will return an estimated level of the likeness between these two images. In some situations, the police may conclude this is sufficiently similar and so identify an individual. This can be impacted by a variety of issues, ranging from the nature and standard of the original image, as well as external influencing factors such as illumination and the orientation of a persons face. Problems can also stem from both the database and programmes. Indian legislation permits electronic and expert evidence to be given. Expert evidence is dealt with in section 39 of the Bharatiya Sakshya Adhiniyam, 2023. **1** Electronic and digital evidence is regulated in sections 61-63. **2** Additionally, section 79A of the Information Technology Act, 2000 details a process for informing Examiners of Electronic Evidence. **3** Nevertheless, there is no

particular legislation that outlines how the scientific validity of facial recognition evidence can be evaluated.

Issues that can be analysed include: which guidelines should be adhered to by the judiciary for evaluating the scientific validity of facial recognition; whether police should disclose the operation and limitations of facial recognition programmes; and if facial recognition is privately operated, how can a defendant challenge the outcomes of such programmes? Moreover, if a person is mainly identified by means of facial recognition, what then transpires? Both the US and UK each manage these issues in different ways. Analysis of these countries' legislation and judiciaries can afford India useful learning so that it can then devise appropriate responses. It is crucial to evaluate the extent to which Indian evidential legislation currently shields defendants against potentially invalid facial recognition evidence. Subsequently, it must also be determined how fundamental values that underlie the US and UK judiciaries can be adapted so that a structured process can be established for evaluating the scientific validity of facial recognition evidence. Appropriate application of such a system can then be realised in Indian criminal courts.

Research Questions:

1.What is the acceptability of AI enhanced face recognition in the Indian court system?

2.How is technology aided expert and digital evidence acknowledged and controlled under Indian laws including the Bharatiya Sakshya Adhiniyam, 2023?

3.How do U.S. Courts analyse the scientific reliability of technology supported expert evidence?

4.How are UK Courts controlling automated face recognition technology, using privacy and procedural means?

1.BSA§39(1) (India), which corresponds to § 45 of the Indian Evidence Act, No. 1 of 1872 (repealed). Section 39(2) separately makes the opinion of an Examiner of Electronic Evidence a relevant fact. Id. § 39(2).

2.BSA §§ 61–63 (India). Sections 62 and 63 correspond to §§ 65A and 65B of the repealed Indian Evidence Act, and § 61 provides in substance that an electronic or digital record is not to be denied admissibility merely because of its form. On the earlier provisions, see Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India), and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C. 1 (India) (certificate requirement for electronic records).

3.Information Technology Act, No. 21 of 2000, § 79A (India); see also BSA § 39(2) (India).

5.What potential legal and technological issues could emerge from the use of face recognition technology to identify individuals that are part of criminal matters, in police and court settings?

6.What safeguards can India adopt from the United States and the United Kingdom to ensure AI enhanced face recognition evidence is reliable, transparent and free from bias?

7.How might the suggested Facial Recognition Evidence Reliability Framework (IFRERF) aid Indian Courts in analysing the reliability of AI generated face recognition evidence?

Research Aims To:

1. Explore the use of Artificial Intelligence powered facial recognition within criminal investigations.

2. Evaluate the existing laws concerning digital evidence and expert evidence in India.

3. Evaluate the laws in the United States regarding scientifically and technologically advanced evidence and their acceptance and reliability.

4. Examine the laws of the United Kingdom surrounding automated facial recognition, alongside data and judicial privacy.

5. Identify relevant legal concerns which arise from algorithms, erroneous identifications, lack of transparency and inadequate information sharing.

6. Compare the laws of India, the U.S. and the UK. From this, identify appropriate legal safeguards.

7. Develop an Indian Facial Recognition Evidence Reliability Framework (IFRERF) so that the judiciary can better assess AI-enhanced facial recognition evidence.

Research Method:

I am undertaking doctrinal research and have adopted an analytical method in order to evaluate and contrast statutory provisions, case law and academic work. Alongside my evaluation of Indian legislation I have researched both constitutional and criminal law. Comparisons have then enabled me to explore how India, the United States and the United Kingdom have responded to the issue of determining the credibility of technological evidence and in turn ensuring the rights of those who are investigated for alleged crimes. Within the US, I have analysed the Court's methodology for evaluating specialist and scientific evidence. In particular I explored Daubert v. Merrell Dow Pharmaceuticals, Inc. **4** My research has been especially interested in the UK's response to facial recognition. This was of particular relevance in assisting my understanding of R (Bridges) v. Chief Constable of South Wales Police. Further to this, academic work relating to data protection, proportionality and policing has been evaluated by me. **5** A range of journals has provided information for my research including the Indian Journal of Law and Technology, the University of Louisville Law Review, Legal Studies, the Cambridge Law Journal and the Northern Ireland Legal Quarterly. **6**

4.Daubert, 509 U.S. at 589–95

5.Bridges, [2020] EWCA Civ 1058, [209]–[210].

6. Full citations to these sources are given at their first substantive reference in Part 6 and in the Bibliography

No data is gathered. Neither are interviews held nor is there any external testing. Only legal research is carried out and a suitable court process is formulated. This research will therefore identify aspects of the law that need to be advanced and also propose a suitable court process for adoption in India.

6. CURRENT LEGAL POSITION:

6.1 Introduction:

Police are increasingly using artificial intelligence in order to analyse and process information and also to examine CCTV. Facial recognition is one area of interest as it allows technology to recognise faces and then cross reference these with information on record. Whilst there are benefits that can arise from the use of facial recognition to assist with police investigations, a 'match' does not necessarily always lead to clear knowledge regarding who was involved in a particular crime. Therefore, it is essential that we are able to distinguish between investigative information and evidence. Although artificial intelligence can be of value in police investigations, the court must independently evaluate what has been produced by such technology so as to decide if it can be classed as evidence. Jessica Gabel Cino and others examine the issues that arise from the employment of facial recognition technology as evidence in criminal courts in their article entitled The Oracle Testifies: Facial Recognition Technology as Evidence in Criminal Courtrooms. The article considers algorithmic, as well as confidentiality- and accuracy-based, discrimination and also a defendant's right to challenge facial recognition results**.7** Ameen Jauhar has also studied the application of computerised facial recognition within the Indian police. He has analysed the constitutional aspects of this, and in particular referred to Article 21 of the Constitution.**8** Thus, these sources highlight that alongside evaluating facial recognition technology, it is important to consider how it can act as evidence and how this interacts with constitutional rights within our criminal justice system.

6.2 Artificial intelligence and facial recognition:

Facial recognition is a process where the features of someone's face are analysed and then converted into data. Such data can then be compared with that held in a database. Images can be compared with each other in order to determine if they may be of the same person. Alternatively, an image can be compared with a collection of images on a database. A

7. Jessica Gabel Cino, Heather Kleider-Offutt, Beth Stevens, Kat Albrecht, Robert Evans & Emma Riedley, The Oracle Testifies: Facial Recognition Technology as Evidence in Criminal Courtrooms, 61 U. Louisville L. Rev. 137 (2022).
8.Ameen Jauhar, Facing Up to the Risks of Automated Facial-Recognition Technologies in Indian Law Enforcement, 16 Indian J.L. & Tech. 1 (2020).

selection of possible matches can then be produced. This type of facial recognition can be particularly useful in relation to criminal investigations. Police can analyse CCTV footage and apply facial recognition technology in an attempt to recognise an individual who may have committed a crime. Indeed, there are various factors which can affect the effectiveness of facial recognition.

6.2 Understanding AI-Assisted Facial Recognition:

Face recognition can be used and is commonly used. Two options exist – either a 1-1 comparison can be made between two images to decide if they could pertain to the same person. Or alternatively 1-n recognition is available where an image can be analysed and compared to numerous other images within a database. This can therefore establish whether or not there are any connections. Within the legal system this can prove to be extremely beneficial as the Police can view CCTV and possibly recognise people who may have committed crime. There are a

variety of aspects which can affect the accuracy of facial recognition. Often, the image which is being assessed is of poor quality especially when relating to CCTV. Furthermore, the lighting and angle of the image can also contribute to this. Algorithms too can suffer from some degree of bias. It has in fact been demonstrated that varying sections of society can be impacted upon to differing degrees by facial recognition and so may experience varying levels of mis-recognition. Problems can also occur with databases. As previously discussed, once more the quality of the images contained within them can be an issue as they may be old, low and/or inadequate. People furthermore have control over facial recognition. Officers can deliberately choose certain images, databases and/or recognitions in order to aid their enquiry. Thus it is crucial that both technological and human elements are analysed in order to appropriately assess facial recognition. Although a likeness value can give an indication of the likelyhood that the person in the video is in fact the defendant, this should not be analysed in a vacuum. Good analysis of quantitative data will also require adequate understanding of both facial recognition and statistics.

6.3 Indian Legislation:

A. Article 21 of the Constitution of India:

Article 21 of the Indian constitution provides a person with fundamental rights to life and liberty. Alongside these articles there is also an acknowledged fundamental right to privacy.14 Currently, individuals' facial data can be gathered, processed and compared and then stored. If a large level of monitoring takes place and/or if there are insufficient protections in place, then a person's right to privacy could be breached. Especially if facial data is being used for investigative reasons. Although the State may well want to reduce levels of crime and increase communal safety, it must attempt to achieve this in a manner which complies with the constitution.

B. Article 14 of the Constitution:

Article 14 guarantees that everyone is equal before and is subject to equal treatment under the law. There have been concerns that facial recognition can show prejudice towards certain demographics and misidentify them. Should this occur then this could affect both equality and the use of the discretionary powers which public authorities have. It is therefore important that the courts assess whether suitable consideration has been given to this issue and also whether facial recognition has been applied equally.

C. Bharatiya Sakshya Adhiniyam, 2023– Section 39:

Experts can give useful information. As facial recognition is technology led, experts are in an ideal position to inform the court about this technology and indeed demonstrate how results are produced. Although expert evidence can be very beneficial it must be ascertained that the expert is appropriately qualified and has used suitable techniques in order to produce and reach their findings. The expert should also be able to describe the analysis technique and assess its reliability for a specific use.

D. Sections 61–63 of the Bharatiya Sakshya Adhiniyam, 2023:

There are requirements which apply to digital evidence and indeed digital video and photographs will fall under such criteria. Just because an electronic piece of evidence (such as digital video footage) has been properly accepted as evidence, does not necessarily mean that an AI has interpreted it correctly. Likewise, despite data possibly being appropriate for computers to analyse,

this does not automatically confirm that the science behind a facial recognition tool is sound. Therefore, alongside assessing digital evidence, it is up to the courts to establish the reliability of facial recognition technology.

6.4 United States: Judicial Assessment of Scientific Reliability:

As a key jurisdiction, the United States has produced an extensive body of law concerning scientific and expert evidence. In particular, the decision in Daubert v. Merrell Dow Pharmaceuticals, Inc is of significance.

In this decision, the US Supreme Court described the role of trial judges as 'gate-keepers', responsible for examining scientific expert evidence to determine its reliability and relevance. Judges have since been given the additional function of 'gate-keeping' for non-scientific expert and technical evidence. 21, 22 Daubert identifies various aspects (although this is by no means a complete list) which can be considered by a judge in order to decide whether scientific expert evidence is reliable. This includes whether the scientific method is testable; whether it has been subjected to peer review and/or has been published; whether the error rate of the science can be identified; whether there are appropriate guidelines governing its application; and whether it is accepted within the relevant scientific community. These aspects can be utilised when analysing the reliability of AI facial recognition. For example, if police deploy some form of facial recognition evidence then the prosecution should be able to demonstrate whether or not the technology has been tested and what its error rate is. Moreover, they should be able to show that the technology has been appropriate for the particular image and database in question. Under Federal Rule of Evidence 702, expert evidence must be founded upon a reasonable volume of data and must be grounded in and apply in a trustworthy manner both sound principles and methods. Following changes to this rule which came into effect on 1 December 2023, it is now the responsibility of that wishing to present expert evidence to prove that it is more probably than not based upon sound data, sound principles and methods and that it has been reliably applied in the specific context. 24 Although Daubert relates to federal courts, certain US states continue to employ the previously existing 'general acceptance' test. 25 Cino and others emphasise that there are particular concerns in relation to facial recognition. As well as the possibility that this technology is private, there can also be insufficient clarity surrounding the metrics used to assess its accuracy. Thus, it can prove difficult for the defence to investigate and contest facial recognition. This is highly significant in relation to delivering justice. Those who face criminal charges should not find themselves in a position where the prosecution is able to present technological evidence, yet fails to supply the defence with essential details which could be used to challenge this evidence.

Lessons for India:

India could also learn from the American method. The court should investigate the scientific basis for an expert's methods. Further, information should be provided by the prosecution to the court concerning both the technology and methodology applied together with data on its error rate. There must also be a strong defence right of cross examination in respect of an expert's method. Rather than implementing a specific test such as Daubert, it is enough for the Indian law of evidence to base a structured method of enquiry upon the concept of reliability.

6.5 United Kingdom: Legality, Privacy and Judicial Supervision:

As well as those mentioned above, the UK has also encountered problems relating to live facial recognition. Members of the public brought a case against the South Wales Police in relation to their use of live facial recognition in the local community. It was alleged that this had infringed people's rights to privacy as well as data protection and equality. The Court of Appeal held that the police had indeed acted unlawfully in using live facial recognition. Poor processes had been followed in order to assess who should be added to a database and there had also been insufficient regulation regarding the areas in which live facial recognition can be used. Furthermore, poor quality was identified in relation to the data protection impact assessment. The court additionally held that the police had not sufficiently followed the public sector equality duty. This includes examining whether the use of live facial recognition may lead to discriminatory outcomes. Nevertheless, it was held that the way in which the police had used live facial recognition had not been disproportionate. Thus it is clear that appropriate legal regulation of live facial recognition is vital. Although the key aspect of the Bridges case related to the legal regulation of police use of live facial recognition and police surveillance, it is important to recognise that this case did not involve assessing whether live facial recognition could be used as evidence in a criminal trial. Joe Purshouse and Liz Campbell analyse the significance of the Bridges case in their article Automated Facial Recognition and Policing: A Bridge Too Far? Furthermore, they explore additional aspects relating to human rights and the regulation of live facial recognition. Resse Adimi Gikay recommends a phased method of regulating live facial recognition. He analyses a number of different areas such as databases, proportionality and legal regulation in his article in the Cambridge Law Journal. 30 Therefore it can be seen that appropriate legal analysis should be undertaken prior to the use of live facial recognition in an investigation.

Lessons for India:

There are many useful points which can be learnt from each country. India has laws and admissibility provisions covering privacy, expert evidence and digital information. However, it does not have specific guidelines about how to evaluate facial recognition evidence. The US provides excellent guidelines concerning scientific and expert evidence. The UK also has high quality guidelines around technology, proportionality and oversight. Points which can be transferred from the US are; scientific analysis, error assessment, scientific explanation and cross examination. Points which can be transferred from the UK are; statutoryisation, proportionality, controlled list availability, data logging and oversight. Points which can be transferred from India are; constitutional protection for human rights, privacy, equality and the right to a fair trial together with the present admissibility framework. Whilst international legal systems can provide valuable points for consideration, it is essential that an Indian specific approach is developed which appropriately incorporates international best practice and still complies with the Indian criminal justice system.

6.7 Proposed Indian Facial Recognition Evidence Reliability Framework (IFRERF):

A new methodology has been created for Indian judges in order that they can assess facial recognition evidence using artificial intelligence. Currently, this is not law. The methodology has been independently formulated and differs from other methodologies highlighted within the literature. This is because of both the judicial assessment and analysis of evidence which it involves. In addition, it enables the judge to recognise and segregate the legal, genuine, trustworthy and disputable aspects of evidence. There are six stages to this methodology.

Stage 1: Lawful Acquisition:

It should also consider how the original image was acquired as well as the legality of the process of both acquisition and examination. The motivation and source of the image and the database that was referenced should be explored. It should then examine whether and to what extent it was both essential and suitable to implement facial recognition. As mentioned, this is again relevant to the UK Bridges case.

Stage 2: Authenticity and Integrity:

In addition, consideration must be given to the authenticity and safe-keeping of digital and non-digital evidence. The prosecution must establish: The source of the CCTV footage; Whether the footage has been edited; Whether suitable source attribution was followed; Whether the facial recognition software conducted an accurate search; And whether relevant computer information has been recorded. This is where evaluation of digital evidence authenticity differs from that of correct identification.

Stage 3: Scientific Reliability:

Additionally, the Court should examine and review the technology that has been utilised for facial recognition. This will involve reviewing the software and its specific version together with the search methodology. Other areas to consider are if the technology has been independently assessed, the error rate and its performance when analysing people from different demographics. Additionally, image quality and appropriate sensitivity settings should be examined. Having undertaken such an assessment it will then be necessary to establish if the technology has been correctly implemented. This is done using the 'Daubert' test which is used in the USA.

Stage 4: Human Intervention and Bias:

Judicial review should also consider police and processes. As well as automatic facial recognition processes, decisions can also be made by a person as to which image is to be analysed, and which database and search is to be used. It is therefore essential that the court considers if there has been any influence of human decision making within the identification procedure. Judicial review should also consider confirmation bias. An independent review is especially important where the investigating officer already had preconceived ideas as to the identity of the person in question.

Stage 5: Disclosure and Defence Challenge:

An accused should be permitted to challenge an analysis of a facial recognition system. Information must also be provided by the prosecution including details of which specific software was used, the searching process and the database which was searched. Alongside this, information on likely matching results should also be included. Information may also need to be confidential for sound commercial reasons. Despite this, the defence should still be permitted to challenge the central matching process employed by the prosecution. This is of fundamental importance to ensure that an individual is able to receive a fair trial.

Stage 6: Evidentiary Weight and Independent Corroboration:

In addition to assessing other factors (as set out above), consideration must also be given to how reliable an AI facial recognition result can be. The court should further assess if there are alternative sources of evidence which can additionally confirm who the defendant is. These may include excellent eyewitness accounts and/or further forensic and/or circumstantial and/or

information based evidence. Ideally the court will be able to identify and differentiate between such alternative evidence and that which is obtained solely as part of the post-AI facial recognition result investigative process. Consequently, this guidance highlights that an AI facial recognition result alone, does not provide sufficient evidence to prove someone's guilt.

Application of IFRERF:

CCTV footage can be analysed and compared using police databases. There are 3 major aspects that must be investigated about this method – firstly, how the footage was obtained and secondly the footage's quality. Thirdly, the analysis process must also be investigated and checked for scientific accuracy. The court will then endeavour to provide the defendant with enough information so that they can dispute the analysis. It will then analyse how strong the evidence is that has been produced by the comparison and will combine this with additional evidence. If it cannot be proven that the analysis is robust then the court should not accept it as robust recognition evidence. Based upon suitable evidential rules and the type of error present, the evidence could either be wholly inadmissible or deemed to be of limited evidential strength. The remit of IFRERF is to guarantee that even though Artificial Intelligence can be used to advise, the judiciary will continue to maintain control over this.

7. FINDINGS AND RECOMMENDATIONS:

Although one may question the admissibility and science reliability of AI, a number of other factors can cause facial recognition to misidentify people. Low image and database quality and both algorithmic and human prejudices can all contribute to faulty facial recognition. Individuals being investigated must then have the ability to question the science that is applied. In the USA, good science reliability guidelines have been developed. As well as ensuring legal compliance, the UK places great value on proportionality. Moreover, India must also be able to differentiate between investigatory and scientifically reliable identification. I propose that:

Indian courts should establish guidelines for assessing science reliability of AI assisted facial recognition. Police should properly document and maintain information about facial recognition searches. Prosecutors must disclose pertinent information to the defence. If science reliability is in question, independent scientific analysis of facial recognition should occur. Investigative facial recognition also requires suitable validation and regular re-assessment to ensure its suitability. Investigative bodies must further implement procedures to limit confirmation bias and to provide adequate human oversight. Finally, facial recognition purely produced by AI must not be allowed to constitute conclusive evidence of an individual's identity and thus their guilt. These proposals aim to effectively reconcile innovative technology with constitutional rights and essential principles of criminal justice.

8. CONCLUSION:

Artificial intelligence can also be applied within policing and is therefore a valuable area of technology. Additionally, it can recognise people and so can be involved in criminal proceedings. However, outputs produced by artificial intelligence require appropriate evaluation. Despite the many advantages which technology can offer, at present there are concerns that outputs generated by algorithms can be accepted as evidence without sufficient scientific and legal evaluation. Expert and digital evidence are recognised in Indian law under the Bharatiya Sakshya Adhiniyam, 2023. The Constitution also plays key role in ensuring that neither executive nor criminal

procedures infringe upon people's rights. Relevant articles include Article 14 and 21. Nonetheless, Indian law currently lacks a structured mechanism whereby the reliability of AI evidence can be evaluated. An analysis of both the United States and United Kingdom's approach to evaluating scientific and expert evidence, and facilitating information exchange to support a defendant's defence, demonstrates that India can successfully adopt effective practices. Moreover, the UK has established protocols concerning appropriate usage, proportionality, data privacy and independent evaluation. By amalgamating best practice from the United States and the United Kingdom, the Indian Facial Recognition Evidence Reliability Framework aims to develop an effective mechanism for evaluating facial recognition evidence. Taking into account aspects including legal conformity, innovation, scientific reliability, human involvement and relevance, it aspires to enable just and open evaluation of facial recognition outputs. Rather than supplanting human evaluation, artificial intelligence should be employed within the criminal justice system to enhance processes. Nevertheless, a computer's facial recognition output alone is insufficient to determine someone's culpability. As emphasised above, it is still essential that the courts evaluate evidence, uphold the rights of the accused and produce just judgements. Effective science, legal conformity and independent evaluation are key to enabling appropriate use of technology as evidence in respect of an individual.

BIBLIOGRAPHY:

Authorities are cited in Bluebook style, consistent with the footnotes.

A. Constitutional and Statutory Materials

Bharatiya Sakshya Adhiniyam, No. 47 of 2023, 55 39, 61-63 (India).

Fed. R. Evid. 702

India Const. arts. 14,21.

Indian Evidence Act, No. 1 of 1872, 55 45, 65A-65B (repealed) (India).

Information Technology Act, No. 21 of 2000, 5 79A (India).

B. Cases:

Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C. 473 (India)

Arjun Panditrao Khorkar v. Kailash Kushanrao Goraneyal, (2020) 7 S.C.C. 1 (India).

Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 U.S. 579 (1993).

E.P. Royappa v. State of Tamil Nodu, (1974) 45 5.C.C. 3 (India)

Frye v. United States, 293 - 1013 (D.C. Cr 1923).

Justice K.S. Puttaswamy (Retd.) . Union of India, (2017) 10 S.C.C. 1 (India)

Kumho Tire Co. v. Carmichor, 526 UIS. 137 1994)

Maneka Gandhi v. Union of India. (1978) 1 S.C.C. 248 (India).

R (Bridges) v. Chief Constable of South Males Police (2019) EWHC 2341 (Admin) (Eng.),

https://caselaw.nationalarchives.gov.uk/ewhc/admin/2019/2341

R (Bridges) v. Chief Constable of South Wales Police (2020] EWCA Civ 1058 (Eng), https!

//caselaw.nationalarchives.gov.uk/ewca/ciw/2020/1058

C. Journal Articles and Conference Papers:

Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 81 Proc. Mach. Leaming Res. 77(2018), https:

//proceedings.mlr.press/v81/buolamwinil8a.html

Jessica Gabel Cino, Heather Kleider-Offutt, Beth Stevens, Kat Albrecht, Robert Evans & Emma Riedley, The Oracle Testifies: Facial Recognition Technology as Evidence in Criminal Courtrooms, 61 U. Louisville L. Rey 137(2022), https://openurl.ebsco.com/contenti tem/gcd%3A162888289

Asress Adimi Gikay, Regulating Use by Law Enforcement Authorities of Live Facial Recognition Technology in Public Spaces: An Incremental Approach, 82 Cambridge L.414(2023), https://doi.org/10.1017/S0008197323000454.

Ameen Jauhar, Facing Up to the Risks of Automated Facial-Recognition Technologies in Indian Law Enforcement, 16 Indian J.L. & Tech. 1(2020), https://repository.nls.ac.in/ijlt/vol16/is

SILA

S. Kalpana, Beyond the Match Score: Admissibiliy, Reliability and Fair-Trial Safeguards for Facial Recognition Evidence under the Bharatiya Sakshya Adhiniyam, 2023, 1(1) Imaginex Int. Interdisc. Res. & Revs. 30(2026), https://articles.lijirr.com/v1/11/05-facial-

recognition-evidence/

Te Li, Bridges v South Wales Police and Emerging Privacy Concerns, 75 N. Ir. Legal Q. 806

(2024), https://doi.org/10.53386/milq.v75i4.1127.

Joe Purshouse & Liz Campbell, Automated Facial Recognition and Policing: A Bridge Too

Far?, 42 Legal Stud. 209(2022), https://doi.org/10.1017/st. https://doi.org/10.1017/st.2021.22

D. Technical Reports:

Patrick Grother, Mei Ngan & Kayee Hanaoka, Face Recognition Vendor Test (FRVT) Part 3:

Demographic Effects, NISTIR 8280 (Nat'1 Inst. of Standards & Tech. Dec. 2019), https: //www.nist.gow/publications/face-recognition-vendor-test-part-3-demographic-effects.