NFSU JOURNAL OF FORENSIC JUSTICE

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

REGULATION OF FRT THROUGH INDIA'S FACIAL RECOGNITION TECHNOLOGY BILL, 2023 AND ITS ADMISSIBILITY UNDER BSA

Amanpriya Singh, Parveen Kumar

Abstract: *The integration of facial recognition technology (FRT) into law enforcement practices is rapidly transforming modern policing, offering tools for faster identification of criminals and aiding in tasks such as locating missing persons. India, has increasingly adopted FRT for public surveillance, often justifying its use under the guise of ensuring public safety. This rapid expansion has thus raised grave apprehensions regarding privacy protections, data protection, and potential misuse of surveillance powers.*

While research is evolving highlighting the effectiveness of FRT in crime detection, equally compelling arguments question its impact on individual privacy and the absence of robust regulatory safeguards. The researchers have even called for a moratorium or outright ban on its use by law enforcement agencies until appropriate legal frameworks are established.

This paper seeks to critically examine whether evidence derived from FRT can be admitted in a court of law as electronic evidence under the Bharatiya Sakshya Adhiniyam (BSA), 2023. It will also explore the regulatory mechanisms proposed under the Facial Recognition Technology (Regulation of Police Powers) Bill, 2023 (FRT Bill 2023), and assess their alignment with the principles of justice, privacy, and procedural fairness. Furthermore, the paper will evaluate the interplay between this Bill and the adoption of FRT as a method for surveillance and the Digital Personal Data Protection (DPDP) Act, 2023, offering a nuanced perspective on how such technologies can be deployed responsibly and lawfully within India's evolving legal framework.

Keywords: *Admissibility, electronic evidence, facial recognition, police, technology, privacy.*

I. INTRODUCTION

The extensive and open use of facial recognition technologies (FRTs) is visible and undeniably an evitable part of the law enforcement agencies and police officers to smoothly conduct the criminal investigations without use of human powered force and labour. This concept of facial recognition origins dates back to the 1964, where American Researchers, W. Bledsoe, Helen Chan Wolf and Charles Bisson studied facial recognition using computer . It was in 1991, that Alex Pentland and Matthew Turk of the Massachusetts Institute of Technology (MIT) succeeded in the creating the FRT in and by 2011 and onwards, the accelerated use of digital modes and with Facebook, FRTs gained precision coupled with needed attention .

While artificial intelligence (AI) and digital advancements go hand in hand, yet there persists a significant difference between both, allowing one to easily understand this difference through the application of closed-circuit television surveillance (CCTV) becoming obsolete since the FRTs has operationally taken over the attention of the law enforcers . The FRTs shows a sophisticated interface between artificial intelligence and digital developments. It creates mathematical representations in form of biometric templates of facial characters and features and compares the same with the reference data bases having a collection of facial images . In India, similar kind of databases exists since the implementation of Aadhar, a unique identification number for every Indian resident in year 2009. The constitutionality of Aadhar Act was challenged before the Supreme Court in the year 2019 through Justice K.S.Puttaswamy (Retd.) v. Union of India, wherein it was laid down that the Act per se is not unconstitutional, except few of its provisions . Notably, it was also contended by the Court that the Aadhar does not create a surveillance state. It is only a 'minimal biometric data" collected with due security and safety measures of the sensitive personal data of its citizens. The Court also mandated that the data stored shall not be exceeding six months as opposed to what was a legislated mandate of five years suggesting that the authentication records need to be protected . It is pertinent to note that since the Aadhar has come forth, the linking of Aadhaar to avail basic services by the citizens like banking services, ration, direct benefit and social security schemes have become a government's mandate, thus further questioning the aspect of data sharing and privacy. In addition, in 2025, the new Aadhaar

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

app shall be redesigned and launched by the Unique Identification Authority of India (UIDAI) as against the old mAadhaar app . The new revamped design is the facial recognition feature to secure the Aadhaar data with hotels and other requesting agencies without the need to extend a hard copy . Although it marks as a great deal of relaxation for the users to avoid carrying the physical Aadhaar cards to airports, hotels or other places to use as an ID proof but to simply scan the QR Code and it's their own mobile gadgets to can their face to verify the identity. This feature was used by banking agents during the Know-Your Customer (KYC) procedures through an app called AadharFaceRD . This further underscores the concerns surrounding over-reliance on the digitalization methods without proper legal framework to regulate the adoption of FRT systems. The fact that facial recognition is a concept slowly taking over from mobile face scans to unlock the gadgets to the live surveillance of public involved in protests or election rallies raises very intricate questions about its legal framework vis-à-vis the privacy rights and data protection laws. Recently, DPDP, 2023 was brought forth to protect the data of the individuals and to ensure its privacy from being misused by external entities. The FRT Bill, 2023, is still under discussion in Rajya Sabha since December 2023 .

This paper demonstrates that even though FRTs adoption in the criminal justice administration is a pivotal step in the order of digitalization and the extensive use of artificial intelligence in various field of law, the emphasis is laid on the regulation of these technologies against the backdrop of the DPDP, 2023 and the FRT Bill 2023. Admissibility of FRTs in the judicial courts needs to be understood within the paradigm of the new criminal law reforms namely the BSA, 2023 which introduces to admit electronic evidences as primary evidences. The critical analysis in this paper follows in two aspects, firstly whether the DPDP, 2023 is sufficient to regulate the data collected from the FRTs and its usage by the law enforcement agencies and moreover, whether the new Bill, 2023 is in itself conclusive enough to regulate and protect the privacy of individuals as a standalone legislation, if not within the provisions of DPDP, 2023.

II. FRTS AND ITS USE BY LAW ENFORCEMENT AGENCIES: INDIAN AND GLOBAL PERSPECTIVE

FRT has been considered as a most powerful advancement in the subject matter of artificial intelligence and digital progression for police personnel and enforcement bodies to enable automated identification, verification and establish proofs of individuals pertaining to their unique facial characteristics . The analysis is through images and video footage of the individuals under surveillance. The question of the legality of FRTs has been raised and answered by many researchers, for instance under the EU laws and regulations and with the advent of the AI Act, it has been contended to forbid the utilization of FRTs in criminal investigation process as the AI Act is not specifically regulating the use of FRTs and that such use violates the individual's privacy on large scale. The application of FRT in the EU for policing and surveillance purposes is thus prohibited . Furthermore, the General Data Protection Regulation governs the privacy data of the individuals, which also fails to safeguard the FRT related data . Moreover, in Dutch Law, the Code of Criminal Procedure (Wetboek van Strafvordering) is silent upon the use of FRTs and who has the powers to use and deploy the same, the European Court of Human Rights (ECtHR) has out rightly that a proper legal mechanism is needed which lays down appropriate procedures for using and deploying of such technologies . In March 2023, the Dutch police published 'Police Deployment Framework for Facial Recognition Technology', which was developed by the police, to be used by the police to experiment with the FRT . In UK, there is an extensive use of FRTs by legal enforcement agencies subjected to the application of the data protection and human rights laws through Criminal Justice Bills and Data Protection Laws while also allocating budget to spending in such investments . In USA, the adoption of FRT is largely discrete in usage by the police officials. There exist separate privacy laws amongst the states which raises the complexity of the issue . Thus, the absence of uniform standards across the nation could result in strict regulations in utilization of FRTs by law enforcers in some states as compared to other. Like in Europe, the use of biometric data requires explicit consent; such a requirement is not absent in the United States legal mandate .

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

Currently, with absence of legislation on the oversight of deployment of the FRT by law enforcements within India the application of digital methods has been employed by the police officers in furtherance of the criminal investigations since long ago. The new criminal law reforms in 2023 have made us of forensic methods to make the process of criminal investigation efficient and time bound the adoption of electronic evidences, mandate of audio video conferencing in search and seizure proceedings, mandatory videography of police statements for victims of certain category and similar changes which harness the modernization in the criminal justice system . There was earlier the Criminal Procedure (identification) Act, 2022 which authorizes the law enforcement agents to take measurements of convicted or other persons for the identifying and investigating the criminal matters while also preserving such data . Thus, it is clear that the utilization of technological methods to facilitate the criminal investigation isn't a novel concept within the criminal justice system.

Notably in India, the use of FRTs was accelerated during the Covid-19 lockdown when the government mandated the use of masks in public spaces . The Technology Development Board of Department of Science and Technology, Government of India allowed for surveillance of the public who are wearing masks through advanced FRTs which could scan and identify an individual even behind a mask . The NCRB has also requested for tenders from bidding companies including foreign entities, thus raising the question of data privacy and data sovereignty through such FRTs equipment. The tender also does not provide in detail as to what all databases shall be linked to this system . The Board has argued that the deployment of the FRTs is exclusive of installation of CCTVs or its connection to any other camera in the vicinity and will be purely for identification of criminals and missing children in broad range which is humanly not possible . Concerns have been raised though within these requests for tenders explicitly harming the individual's privacy as the tenders call for N: N development of FRT as opposed to 1: N or 1:1 system which will further be connected with crime analytics centers or private entities raising alarms for data sharing . It is significant to understand the implications of the use of 1: N and 1:1 technology in facial recognition aspects, since these further broaden the aspect for establishing a regulatory framework as a necessity . FRTs in general can be used for security or non-security uses, wherein the former is where the use is by law enforcement agents and surveillance entities can be understood, while in the latter the use of FRTs can be explained through Digi yatra apps for airport security checks, mobile phone unlocking scans etc. . Furthermore, there are two kinds of FRTs i.e. 1:1 and 1: N, wherein in the former system, the FRT is authenticating and verifying a particular individual by matching their facial characters to a facial image within a dataset, and the latter pertains to the identifying and authentication thereafter of the individual between two faces when compared to a given dataset . The latter system is also where there are live FRTs used majorly by the law enforcement agents to monitor the individuals. The consent is not provided in 1: N as compared to 1:1 systems, making the 1: N systems more susceptible to violation of privacy of individuals . In continuation to these discussions, another fundamental aspect of FRTs is that they can be controlled and managed by human interceptor or they can be completely managed by the machine/ computer . The pertinent question to consider is that when solely giving all the controls and powers to one individual to manage and scrutinize the technology becomes questionable on the ethical use without any form of discrimination and partiality on the part of the human, while the same argument can follow for the fully automatic machine learning systems as well, that the algorithms can also cause bias in their assessment and scans thus highlighting the dilemma of how this technology must be used with utmost care and precaution without any form of discrimination or bias being followed from either the human intervention or by the machine itself.

In India, FRT has been deployed to be used in Maha Kumbh Mela in Uttar Pradesh to aid crowd management and find missing children or women . Moreover, through Sadha Haldar v. The State of NCT of Delhi , Delhi Police was authorized to use FRT to find missing children. Due to this approval, the police officials in Delhi had been successful in locating and finding approximately 3000 missing children . In 2024, during the Independence Day, 700 AI cameras were deployed for close scrutiny in the event upon the prospective threat or any terrorist attack . While a regulated and a limited use of this technology certainly yields extraordinary results and enhances protection, safety and security of the individuals only, the harm of these technologies is wider if not regulated and

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

are used arbitrarily without any just and reasonable cause.

III. REGULATION OF FRT IN INDIA THROUGH FRT BILL 2023: CRITICAL ANALYSIS

While understanding various socio-legal nuances of the artificial intelligence, particularly FRTs being used by the law enforcement agencies and police officials to facilitate criminal investigation process, there is a need to understand this usage within the given legal framework and, if any, the existing regulations pertaining to the subject matters allied to such usage of artificial intelligence.

Currently, there is no legislation governing and regulating the use of FRTs by the police officials or the monitoring authorities. The use of technology in general has been governed by the Information Technology Act, 2002 (IT Act, 2002), the associated rules, the new criminal laws namely the Bharatiya Nagarik Suraksha Sanhita (BNSS), Bharatiya Suraksha Adhiniyam (BSA), Bharatiya Nagarik Sanhita (BNS) 2023 and Criminal Procedure (Identification) Act, 2022 (CPIA, 2022) when dealing with criminal matters. Notably, the IT Act does not apply on the governmental agencies that use facial/ biometric data, thus raising alarming concerns . In other words, the IT Act is applicable on private entities. Furthermore, the Act is silent upon regulating the FRTs as well . Under section 54 of the BNSS, 2023, there is also an identification of the accused/suspected so arrested by the police for the investigation purposes by the witnesses or such person considered necessary, this is also called the Identification Parade Test. This process of conducting the TIPs by the police officials required Court's order and could be dealt in like manner as the court may direct. Thus, by literal interpretation of the said provision, the authors suggest that there exists the potential for employment of digital ways to identify the accused by the witnesses without any need for physical appearance of the accused and the witnesses. When the person arrested is mentally or physically disabled, and then the process takes place through audio-video conferencing. Thus, concluding that the use of digital methods is not novel but rather embedded in the procedure of investigation itself.

While the CPIA, 2022 carries with its own criticism of being violative of privacy besides the equality of the accused, the law stipulates to take such measurements of convicts or any other person for the purpose of carrying criminal investigation . Section 2(b) of the said Act defines clearly what these measurements like the fingerprints are, palm prints, foot prints, biological samples etc. the Act gave wide powers to Magistrate to order for collection of samples from any person who is not even arrested to give samples . Moreover, the data so collected is kept with the NCRB database for 75 years which shall be deleted only upon the final acquittal of the accused or upon the discharge of the arrested person for the offence . FRT is used by police officials to identify criminals through their facial verification from the database that is there with the NCRB . The CPIA does not apply on FRTs; rather it is the initial stage of finding the individual who might be the suspect of the offence or the accused per se. The FRT Bill 2023 was introduced in the Parliament and still awaits the approval from Rajya Sabha . This legislation is brought given the criticism and reported instances where the FRT has been deployed by police authorities for the purpose to track the individuals within the protests involved against the government, which thus needs a serious introspection . It is crucial to lay down a benchmark for what offences, when and by whom such systems can be deployed and used within the bounds of the constitutional principles. Upon the plain reading of the Preamble to the Bill, it states that, 'to provide for a framework to regulate, control and define powers of the police agencies and central investigative agencies to use facial recognition technologies for the purposes of identification, investigation and inquiries of criminal offences and for matters connected therewith and incidental thereto' . The Bill entails nine sections in total of which Section 2 provides for definition of terms like "facial recognition technology', 'face surveillance', 'other remote biometric recognition'. These terms are imperative to understand the regulation being set forth owing to the use of FRTs. FRT means an automated or semi-automated algorithm which is deployed to identify, verify and match the facial characters of an individual including both 1:1 and 1: N systems to find the emotions and activities of the individual . This definition itself is broad and exclusive to include all types of FRTs which can be used for investigative purposes or for any other related matter. Face surveillance means the use of FRT to track and observe, analyze the behavior or the actions of individuals or groups . While section 2(d) states that other means of biometric data shall include

voice recognition or other surveil information relating to the individuals, but shall exclude the finger prints and palm prints. Section 3 states that the use of FRT shall be in certain offences which affect or endanger the national security of India or integrity of the country while excluding the police officials and other investigative agencies to employ such methods in any other form for investigation purposes . This section however seems clear, but the critical understanding is the Bill or the section is still not particular about what kind of offences would be classified as those being committed against or affecting or threatening the national security of India or its integrity. Moreover, the police officer who is the officer in charge of the police station or the investigating officer is required to obtain the order from the Magistrate who is a Metropolitan or a Judicial Magistrate of first class, as the case maybe for using such technology. The employment of such technology is not considered as 'measurements' as under the CPIA. A very significant provision regarding the utilization of FRT without any form of bias or discrimination on the basis of race, caste, religion, gender, political ideology, sexual orientation etc. will not be employed to identify a person, thus removing and eliminating the risk of techno-discrimination of any form . The explicit mention in the provision makes it a legal mandate it literal and strict sense and thus making it a very strong provision to employ FRT being used by the law enforcement agents. The NCRB has the authority to collect, store and destroy such data at national level and process or disclose such records to any enforcement agency in the manner prescribed . The authors assert that this makes the provision ambiguous insofar as the data within the reach of the NCRB which is being kept for 75 years can be shared amongst the enforcement agencies whenever needed . Even though it reduces the risk of multiplicity of data from every law enforcement agency, this rule can be interpreted liberally by the NCRB. Moreover, so far, the FRT Bill is silent upon the privacy concerns, or the law-abiding individuals who are not guilty but still by the default understanding of algorithms and machine learning being subjected to such scrutiny, therefore becoming the victims of the criminal administration system by being mandatorily subjected to police surveillance. This goes against the basis of criminal justice system i.e. presumption of innocence until proven guilty. The Bill should have catered to these aspects as well. While section 5(2) of the Bill allows for audi alteram partem before employing the FRT, the power of the Magistrate to direct any person to give face surveillance or other biometric records, seems broad and arbitrary and which is purely based on the level of his satisfaction. The law cannot function properly when such arbitrary options are left upon the officials regarding the utilization of AI and subjecting personal satisfaction to legitimize the procurement of personal data to be scrutinized at national level. In addition, section 6 puts a bar on the proceedings or suits against such official who acts in good faith. This again stands as a discretionary provision, unable to define what acts shall constitute as 'good faith for the acts to be done within this Act'. Section 8 further gives an overriding effect to the laws in force for provisions being inconsistent to this Act. This raises a concern of whether the DPDP, 2023 shall also stand in this category, since section 38 of the DPDP, 2023 also gives an overriding effect to its provisions in so far as found inconsistent to the Act . The two laws are crucial in their own concerning subject matters and probably the use of harmonious construction and golden rule of interpretation may be applied for removing any ambiguities in the said laws, however the fact that right to privacy also comes with reasonable restriction and whether such constraints are legitimate and reasonable for using FRT is another disconcerting issue. The understanding of giving overriding effect to the provision of the said Act raises doubts for the future regulatory laws on artificial intelligence or any other laws that might take effect like the Witness Protection Bill, 2023 . The Bill also entails a repealing section thus repealing certain clauses of the CPIA in respect to the use of FRTs and other biometric techniques . It is undeniably a very intricate use of technology administered by the government by putting the personal data and privacy rights of its citizens at stake.

Arguably, the question that needs deliberation is how the data obtained from the use of FRTs are to be utilized by the police officials and law enforcement agencies to their benefit. In 2009, NCRB under the aegis of Ministry of Home Affairs (MoHA) was entrusted with project of coordinating, monitoring and implementing the Crime and Criminal Tracking Network & Systems (CCTNS) . This project connects 15,000 plus police stations and 6000 high ranking offices of the police. The police officials have access to this data to search for a suspect or a criminal through Digital Police Portal . CCTNS National Database has now records grown up to 28 crores . This CCTNS in Phase II is subjected to link the FRTs and thereby linking this

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

database to other central databases like the Passport & Immigration, Visa and Foreigners Registration & Tracking (IVFRT), Arms Licenses and many more . FRT is a progressive shift in modern policing to easily identify, verify and map the suspects to arrest them within time bound manner, however certain questions still need to be answered before fully utilizing this technology to its best possible manner.

While the enhanced interoperability between law enforcement agencies strengthens the Criminal Justice System, it also poses significant concerns for both justice administration and the protection of citizens' rights in India. The authors argue that the use of live FRTs must be exclusively shut down and prohibited by the law enforcement agents i.e. 1: N FRT systems as compared to the 1:1 systems, if there exists no current legal mechanism to regulate the same. Since, this usage gives arbitrary power and often misuse of power entrusted to the executive agents. Further, the generalization of the use of FRTs under the Bill of 2023 raises various concerns regarding the protection of personal data of individuals, which needs serious deliberation by the legislators.

IV. FRT BILL, 2023 VERSUS DIGITAL PERSONAL DATA PROTECTION (DPDP) ACT, 2023

In furtherance of the ongoing discussion the real time question which brings this matter to highly debatable stance lies in the fact that the current privacy and data protection laws in India and the legal stipulations in the Bill of 2023 providing a legal framework for the use of FRT are not compatible on various aspects like there is lack of checks and balances of the use of FRTs and lack of supervision, the difference in proportionality to the extraction of maximum versus minimum data and lastly, the principle of legality, necessity and proportionality to use FRTs .

The Apex Court through the Aadhar Case (2017) held that the right to privacy is guaranteed, though subject to reasonable legal constraints and these restrictions imbibe a threshold of legality, necessity and proportionality . Any intrusion which affects the privacy of individuals must anchor such powers from a legislation clearly subjecting such data to be collected for some reasonable purpose. The use of FRTs in present lacks regulatory framework and the Bill of 2023 is also still pending in the Parliament for discussion. Thus, currently the use of FRTs by either private or public entities is not fulfilling these criteria of legality as a lawful restriction upon the privacy rights of individuals. In continuation of the said discussion, there holds no justification of necessity, since the use of FRT is to facilitate the criminal justice administration and assist the police officials in easy identification and verification of the criminals or the suspects to the cases . Moreover, it has been argued invariably that the accuracy of the FRTs is not 100% such that there are chances of errors or false positives which further raise questions on the use of FRTs for identification of innocent individuals as criminals . Additionally, the third threshold is also not met currently where the data collected by use of FRTs has no direct nexus to the images/ photos taken at the scene of crime to showcase any wrongdoing on their part or just on their mere presence at the crime scenes . The Apex Court clearly held in the Aadhar case that the broad set of individuals ought not to be taken as suspicious persons for the prevention of money laundering acts in the garb of mandatory linking of the Aadhaar of the individuals to their banking services .

Within the provisions of the DPDP, 2023, the Act stipulates through the Preamble that the processing of digital personal data must balance the recognition of individual rights with the lawful use of such data . Accordingly, it is evident that the Act does not exclusively pertains to the biometric data collected through the use of FRTs in any of its provisions, however impliedly one can understand that the collected personal biometric facial data constitutes as 'digital personal data' under section 2(n) of the said Act. Section 4 (1) states that the data which is personal maybe used at the consent of the data principal or the one whose personal data is needed to be extracted or where there exists no consent but the procurement of the same is needed for legitimate purposes. In addition, the term lawful purposes have been framed broadly as what is not forbidden by the law. The authors argue that currently the use of FRT is not forbidden by law, and the procurement of private data is mostly without consensus of the individuals at large and thus raising concerns of privacy infringement at large scale when such data is distributed amongst central law enforcement agencies. This argument is further strengthened through Section 11(2) and 17 (c) of the DPDP, 2023. While section 8 and 16 of the said Act lays down certain exemptions upon data fiduciary to explicitly use the personal data of the data principal, section 17 enlists where

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

such exemptions shall not be implemented. In simple words, where the data fiduciary is duty bound to protect the personal data of the individual from getting disbursed within and outside country or from any misuse, through S. 17, the data fiduciary may process such data in view of prevention of crime or detection. Thus, raising the very basis of these provisions to protect the personal data but within the aspect of "lawful purposes" the data may be processed and even transferred to another country or territory outside India. Under the said Act, there is an establishment of an independent Board, Data Protection Board of India , functioning as the digital office while also managing with the complaints and making decisions. Moreover, the Board takes assistance from the police officials of the Central or the Government of different states for complying with the legal clauses of the Act, this makes the concern of checks and balance negligible and rather also pin points to the issue to separation of function as opposed to separation of power of the law enforcing agents who are using FRTs to procure the personal data of the data principal . On one hand, the independence of the Board is attributed, while on the contrary they use police force to forward the goals of DPDP, 2023, in addition to the members of this Board being as notified by the Central Government. Even under the FRT Bill, 2023, no such independent authority exists, which should be a mandate within the law itself which can supervise the employment of FRTs by police officials in a rightful manner and to entertain complaints on any misuse of such technology.

The authors have critically assessed these two legislations upon their personal assessment and intellect, thus, the argument that the DPDP, 2023 may provide answers to the issue of data privacy and protection of personal data procured by the use of FRTs by the law enforcement agents and police officials remains at a dead-end. Since, the DPDP, 2023 gives way with reference to personal data processed by the data fiduciary in the garb of 'legitimate purposes', however staying silent on the what 'lawful' methods are to be employed to obtain such personal data.

V. ADMISSIBILITY OF FRT AS EVIDENCE IN INDIAN COURTS: CRITICAL ASSESSMENT

While the world is progressing in utilizing the use of AI and various digital means to make their lives easier and faster, the judicial proceedings are also developing ways to make such electronic and digital based evidences admissible in the legal proceedings from E-mails, WhatsApp messages, social media updates, CCTVs and other surveillance footage . With the use of AI come the complexities associated with it. Some examples of AI generated evidences are the biometric methods to identify criminals or transcript written models, use of Alexa or Siri as Internet of Things (IoTs) . Recently, in US based judge in New Hampshire ordered Amazon to provide with the recordings of their Echo Device that could have evidences of murder of two women in January 2017 . However, care must be taken while assessing these AI based models as they can be inaccurate and can lead to bias or lack the reliability, thus providing false or mis-information at large scale . Moreover, the issue of opacity in the algorithms of these AI models is where the intervention from human intellect is needed. Notably, there exists no general guideline on how to verify the AI models and their algorithms which further complicates the judicial decision making. Therefore, final call to evaluate the admissibility of these AI generated models as evidences is upon the judges. It is significant to know that the understanding of the algorithms with proper training is needed in this aspect.

UNESCO in collaboration with the Inter-American Human Rights Court and National Judicial College, USA, and the Center for Communication Governance, National Law University (India), recently through a webinar deliberated upon the 'The Admissibility Challenge: AI-Generated Evidence in the Courtroom' while discussing the complexities around the admissibility of the AI based evidences . While largely discussing upon the model of self-driving car having a self-automatic system to detect drowsiness of the driver, what happens when there is an accident caused and upon the initiation of the judicial proceedings, it was found that the AI based model installed in the car was biased on the aspect that it only recognized 'white guy' to be the perfect driver while questioning the programming of the algorithm that it did not recognize brown female drives or drivers having natural drowsy eyes were also errored to be understood as under intoxication . In such scenarios, the proof of AI based evidence can only be projected by the one who developed, manufactured and programmed such model, while judges making sure that the state in which the evidence was presented before the court shall remain in the safe hands and must be kept from any ways of tampering .

AI based evidences basically means such information or generation of data which can be processed and analyzed by the AI systems to support claims, statements or decisions in legal context . The admissibility of these evidences is based upon authenticity, compliance with the procedural laws and rules, relevance and reliability . The court having the discretionary powers may assess whether given evidence in the light of said material facts and circumstances around the case, that the evidence is admissible or not . In India, the legal framework of evidences is under the BSA, 2023. It does not comprehensively deal with the AI based evidences and their admissibility. The application of FRT to determine the identification and verification of the suspect and further arresting the individual and projecting them to criminal administration, raises a pertinent question on whether the FRTs based evidences can be admissible in the Indian criminal courts. FRTs can be rendered as AI generated based evidences since it is based on certain algorithm and mathematical programming to relate such data to the general database. In addition, these must be accurate and relevant evidences . Now, whether FRTs are advancing accurate data or otherwise, remains a matter of practical question which needs employing of the FRTs to practical usage. In Delhi, the police officials through an RTI have confirmed 80% matches to be positive identities . Notably, it isn't 100% accurate; hence the discussion on the utilization of FRTs as being accurate is still a valid question to be answered. In the matter of Regina v. Maqsud Ali, court contended that the technological evidences maybe admissible like tape recordings if they are accurate and relevant.

While deeply examining the Indian Justice System through the lens of evidences advanced in the cases to establish a claim or defend a party. With technological advancement, there is a fine line of difference between electronic and digital evidences. While electronic evidences as per the IT Act are evidences having information with values which can be stored or transmitted electronically like the computer data, audio-videos, cell phones etc. . The digital evidences may be in various forms like messages, pictures, videos, digital signatures, use of social media applications, digital documents like presentations or notes, internet log histories, geolocation like GPS on mobile phones, online purchases, IP addresses, Google drive, crypto currencies, block chains etc. . There is no requirement of hand print or finger print like forensic evidences to investigate the matter . The storage of the digital evidences is in electronic form . In 2023, with the major legal reform in the criminal administration, BSA replaced the old Indian Evidence Act, (IEA), 1872 . Section 57 and 58 of the BSA explicitly define what are primary and what secondary evidences are. Thus, from the plain reading of these provisions it is apparent that the digital evidences are considered as primary evidences while under the old law the digital evidences were considered as secondary evidences. The importance of being primary evidence over secondary evidence is that former can be produced in the court directly . What is critical to note is that though the terms electronic and digital evidences are mentioned, such terms are not defined either in the BSA or BNSS . Nonetheless, their usage in the given context of provisions is understood that the digital evidence is the electronic form evidence as given under the IT Act .

Within the new legal framework, the electronic evidences are treated as primary evidences and are thus admissible unlike the old evidence laws . Within section 63 (2) (a), one can say that FRTs are the electronic evidences such that the facial recognition and identification done through computer programmed algorithm, thus creating a data of the individual to store or process such given information by a person who controls the device or the system. This action has likewise been carried out for a substantial amount of time and was performed using computer systems or networks are electronic evidence. Thus, the digitally produced scans by the FRT systems and thus storing and processing such data for further mapping and verification within the electronic means of devices are a electronic evidence. However, the need for certificate to be provided to advance en electronic certificate to be admissible in the court is done away with the electronic evidences under the new laws, but the certification by an expert was well intended towards ensuring that the evidence is authentic and holds its integrity . BSA is silent upon when the electronic evidences as primary evidences be supported by a certificate . Additionally, maintaining data integrity is well established under the BSA stating that where any electronic or digital evidence is advances from an appropriate custody, it shall be regarded as primary evidence unless it is disputed . However, the Supreme Court contended that there is absence of proper guidelines on search and seizure measures of

JFJ
Volume: 4, Issue: 1
January-June 2025
E-ISSN: 2584 - 0924

keeping the electronic evidences in the matter of Amazon Seller Services Pvt. Ltd. & Anr. v. Directorate of Enforcement & Ors .

While addressing the admissibility question of the FRTs, another intriguing paradigm needs attention and that is whether the digital evidences in form of electronic evidences by the use of FRTs may also be utilized for forensic investigations . Forensic investigation basically involves the analysis of fingerprints, DNA, blood stains, post mortem reports etc. The facial attributes obtained through the use of FRTs to identify criminals can be attributed as digital forensic evidences which can be used in forensic evidences apart from the physical evidences as mentioned above . While the digital forensics investigations are still growing in their field, the experts have suggested strengthening the cyber security mechanism and protecting the information transmission through strict application of the IT Act to avoid future harms.

In conclusion, thought the admissibility question of FRTs is a substantial question which demands thorough deliberation, according to the authors, the FRTs can be understood as digitally procured electronic evidences which can be admissible in the court provided that the record produced is relevant and accurate, it cannot harm the accused rights in any manner . The judges need to be careful and vigilant to be sure and satisfied beyond reasonable doubts that the AI based evidence is admissible as primary or secondary evidence. This shall require some guidelines from the judicial intervention or through some legislation which inculcates the FRTs as a form of evidence as well in furtherance of criminal investigations or in any case.

VI. CONCLUSION & RECOMMENDATIONS

The outcome is only a matter of time before there is use of FRTs by the private companies for scanning their employee's entry and exit or to identify and verify the individuals thus gaining a worldwide recognition across globe. However, what remains to be seen is whether this technology will be accepted to be used in regulated and restricted manner or will it be completely banned. FRTs are bound to evolve with time and advancements in technology which makes it crucial for us to understand its implications in various social, economic, legal and ethical levels. While there isn't any denying in the fact that adoption of use of FRT can bring positive changes for India's crime rate, however there needs to be a regulation which limits and defines the contours within which this technology can function. The authors hold the opinion that certain recommendations can be considered in completely adopting the use of FRTs in justice system. Firstly, with use of FRT by the law enforcement comes various legal and ethical issues of its usage, it is suggested that there is limited use 1: N form of FRTs and rather 1:1 FRTs are much feasible and viable option. Moreover, there needs to be a specific mention of offences within the FRT Bill 2023 to use FRT systems without hampering the general public and rather creating a police surveillance state. Thirdly, there is a need to cater to the large-scale distribution of the data by interoperability of these technologies to other law enforcing agencies thus widening the scope of cybercriminals and putting the personal data of the general public at such a risk, hence limited transmission and sharing of this data is needed with much stricter legal compliances being needed to regulate cybercrimes and ensure cyber security. In addition, there is a need to ensure that the databases maintained are not keeping the records for indefinite period of time that is even when the person has died, rather there the data must be kept for some years and then updated for some years depending upon the biological, physical and mental changes in the individual. There is a need to maintain data sovereignty and the police officials must keep a record of the Impact Assessment of procuring such personal data from individuals at large. There is a need for sensitization amongst the police personnel's and law enforcement agencies to cater to the privacy rights of individuals and protect their innocence while also putting the criminals behind the bars with extensive use of technology and to foster the criminal justice administration in an efficient manner. There is a need to establish an independent body which shall supervise the use of FRT by law enforcement agencies and enforce penalties for violations if any and ensure transparency and accountability.