AI BASED FACIAL RECOGNITION TECHNOLOGY AND CRIMINAL JUSTICE: ISSUES AND CHALLENGES

Dr.Zubair Ahmed Khan [a] & Asma Rizvi [b]
[a] Assistant Professor, USLLS, GGSIPU, Dwarka.
[b]PhD Scholar, USLLS, GGSIPU,Dwarka.

Abstract
Law enforcement agencies in many countries have initiated the use of AFRS (Automated Facial Recognition System),it's an artificial intelligence system that compares face traits automatically, to identify unknown suspects using images and other social media platforms. Its capabilities are fast developing in conjunction with artificial intelligence, and it has a lot of potential for solving crimes. However, it also has a negative connotation. There are substantial privacy and ethical considerations that necessitate legislation and regulation. The Ministry of Home Affairs of India has released a new plan for AFRS aimed at upgrading law-enforcement agencies for the purpose of detection of criminals, proper data exchange among law enforcement agencies throughout the globe. It is indeed evident to say, India is third largest country in technological development and the citizens are coping up with these changes. The author proposes to examine the emergence of Automated Facial Recognition System, contemporary uses, and legislative developments in various countries like US, UK and Australia, as well as doing an ethical examination of the concerns that may arise during its implementation. The author will also implicate the authenticity of FIR registered against unknown person through the use of AFRS, and legislations related to it. Ethical considerations are used to mediate conflicting issues with reference to modern innovation vis-à-vis public safety mechanism, privacy and democratic responsibility.
Keywords: Privacy, Artificial Intelligence, Algorithms, Investigation.

Introduction

The origin of tern biometrics is from Greek language, where bio literally means life and metrics refer to measuring something. Biometrics comes from the Greek languages, Bio meaning "life," and Metrics, meaning "to measure." Biometric application usually helped in proper assessment and statistical analysis of the physical and physiological features of people.[1] This technology is frequently used by a safety company to identify, authenticate and regulate access purposes. It is useful in finding out suspect persons in criminal cases based upon their thumbprint, voice/face identification and medical necessity for a criminal investigation. There are two types of biometric methods which are generally prevalent among official practices. Physical biometrics is usually useful for the objective of verification. It facilitates in getting fingerprints, facial recognition and identification though eye/hand. The other category is Biometrics of Comportment which is also used to identify and verify processes. Our behavior is examined

with this approach. The keystroke recognition and speaker identification are an example of this approach.

There are different law-enforcement agencies established in western nations and corporate entities like Facebook, Apple,etc have employed the face recognition technology. It is used for several purposes, but not just to assist users to identify, check and search a person's face via a vast facial database. The technique of facial recognition is applicable through scanning of basic facial features and its measurement through which a mathematical formula in the form faceprint can be created. The image is then compared to the database image and the corresponding picture is shown in the system. In the year 2020, The National Crime Records Bureau (NCRB) put a public proposal to facilitate the technique of automated facial recognition system called as AFRS. The NCRB is targeting to update new database through which identification of criminals through pictures and videos can be possible. This application can be made compatible to identify unrecognized corpses and also detecting possible crime. Integration with different existing database of criminals and technology like CCTV footage may help further in analyzing accurate analysis and information exchange in the interest of criminal investigation.

Emergence of AI based Facial Identification Technique

For considerable period of time, AFRS is generally used by law enforcement agencies and different corporate firms across many western and South-Asian countries. Facial recognition technology based on AI technology is the rise of a new era which is going to revolutionize the whole criminal justice system. This system works on the entails of innovative capturing, digitalization and comparability of the dimensional facet of outward face so as to recognize a specific person. This technique may involve usage of a digital picture of a person, sharp mapping of facial components something can be changed to a computerized format, algorithm for comparing picture with that of existed in database. Pictures can be gathered from archives of different identification card details with photos or different number of pictures which can be found on social-media platforms. Biometric facial identification framework can be amalgamated with the enclosed-loop mechanism which earlier subsisted in societal or personal platform for the purpose of recognition of individual. The enhanced utilization of this innovation raises various socio-ethical issues in democratic society where privacy right is given sufficient significance.

Concerns with biometric facial recognition stem mostly from possible contradictions between ethical ideals and their use in diverse sectors. The whole discourse revolve about AFRS is about private rights, national safety , transparency, just accountableness. Such issues may raise in diverse sectors like criminal investigation, public security matters or any corporate regime.

There are various reasons for the emergence of this technology. Posing a threat to national security about a number of important changes were made in policies and rules of law enforcement agencies in many western & non-western democratic nations.[2] As a consequence of this, the government agencies now have a far larger ability to gather and monitor evidence, to detect and apprehend non-state threats, such as terrorist and international crimes, more

proactively through Facial Recognition Technology. The authoritarian governments gives more insight into the possible consequences of biometrical use. China uses biometric face recognition technologies to identify those who are accused of minor offenses, including jaywalking or humiliating people in "non-disclosed behavior," such as "wearing pajamas in public" in public areas using CCTV. According to BBC news, it is believed that ethnic minorities like as the Uighurs are subjected to extensive surveillance and discrimination through the use of face recognition and other biometrics.[3] The AI based Facial Recognition software is helping various democratic and authoritarian nations. The future holds much broader use of Biometric Facial Recognition system, which is going to change the dynamics of the world.

Recent Legislative Developments in Different Countries

Over the last decade, substantial modern applications and innovative strategies in the field of biometric facial identification continue to progress rapidly in various developed nations like USA, UK, etc. For more than a decade, they have been used in conjunction with passports at international airports, and it still have significant role in supervision and checking measures at border inspection fronts. The specific innovation has grown exponentially significant for facilitating law-enforcement agencies. Through these years various developments were made in legislation in various countries by facilitating the data and facial images from passport and driving license. A significant attempt has been made for integration of facial images from social media platform. The technology is subjected to judicial review in courts.[4] Identix®, a Minnesota-based business firm, is evolving innovator in the field of face identification process. FaceIt® application can recognize a person's face in a crowded place, and take specific picture of face from whole picture & thereby comparison can be made with existed photos in the database.[5]

This program must be able to distinguish & identify one face from the backdrop in order to function. It was reported that enforcement institutions in the US were scanning photos on the internet for suspects using a face identification algorithm created by the company Clearview AI[6]. The same company was deployed by law enforcement institutions in UK and other western nations. Clearview's facial recognition program has generated outrage throughout the world. Data protection advocates recently filed complaints against Clearview AI in five European nations. They claim that the software, a search engine for faces that sifts through billions of photographs breaches the rigorous privacy regulations of the United Kingdom and the European Union. The debate shows how, as artificial intelligence technology improves, it might lead to unprecedented levels of monitoring. Clearview AI is accused of violating the California Consumer Privacy Act of 2018 and the Illinois Biometric Information Privacy Act [7], according to the statement of claim. The plaintiff action claims that the persons didn't give their permission for utility or redeployment of pictures, biometric data & finders. It was alleged that the entity 'was able to scrap' images from social media platforms violating various terms of use of such platform. The entity disposed accessed pictures , biometrics and finders to 3rd parties

with trade. Clearview did not grant access or distribution of photographs, biometric information and Identifiers to third parties. It was further alleged that determining the worth of biometric and identifying information of people has led to damage, which puts people at risk of infringing on their privacy[8].

Algorithms for Face Recognition are highly accurate (over 90%), however these results are not universal. A rising number of researchers disclose differing mistake rates in different demographic categories, with lowest exactness in women, black and 18-30 years[9]. In the 2018 "Gender Shades"[10] landmark project, three gender algorithms, including those produced by Microsoft and IBM, were evaluated by an intersectional methodology. Those involved were divided into four categories: females with dark skins, males with dark skins, females with lighter skins and males with light skin. All three algorithms fared the worst for females with darker complexion with errors up to 34 per cent greater than for males with light skin. These latest discoveries add more intricacy to socio-ethical & legal problems related to biometric face recognition by corporations such as the banks and merchants of grave importance reportedly using the technology.

In case of Bing Guo v. Hangzhou Safari Park[11], decided by Chinese court, it was held that any kind of collection of personal data through usage facial biometric application without the consent of any person is totally illicit and prohibited for an organization. It was emphasized that such biometric application violates basic rights of privacy and endangers the rights of consumers in general.

Interestingly, in contrast to previous case, one of the leading case of R (Bridges) v. CCSWP & SSHD,[2019] EWHC 2341(Admin) decided by UK court where it was made quite explicit that usage of facial recognition application by law enforcement agency is legitimate in nature. It was observed that existing legal framework is sufficient enough to make sure proper usage of AFRS in the large interest of peace, law & order. In fact, it was also highlighted that the usage goes in contemporaneous to human right legislations ,privacy regulations and it rationally justify the objective of the application being treated as less intrusive method.[12] It argued that it violates the European Convention on Human Rights (ECHR), which is not justified in Article 8(2), as it does not for any purpose in this Article 'lawful compliance' or essential in democracy ,' which covers societal security and crime prevention, and that this infringement is a violation of privacy rights.

The court acknowledged that the AFR Locate was infringing on the rights to privacy of Mr. Bridges, but the police's authority to prevent and identify crime was outweighing this. The statutory independent commissioner, Commissioner for Biometric Material Retention and Use, has been established to deal with issues pertaining to the consent, retention and utilization of biometric information in the UK[13]. The Commissioner's role is to oversee the use and protection of biometric information against excessive law enforcement[14].

Legal Issues related to Facial Recognition from Indian Context

The AI based facial recognition application was used by Delhi Police for the first time in the year 2018 as per the direction of Delhi High Court where the technology was asked to used to trace missing children.[15] Interestingly, there is absence of any policy/regulation/ guideline in effective usage of this facial identification technology.[16] But enforcement agencies started using this technology to facilitate investigation procedure for different criminal cases. After the arrival of Facial Recognition Technology (FRT) in India, criminal investigations have become convenient for law enforcement agencies. Whatever its advantages, it is a threat to citizens' privacy and fundamental human rights. The abuse of power will result in abuse by the authorities and the consequent creep of function in the absence of any regulatory authority or law. FRT means a method by which a person's identity using his face can be identified or verified. Although there is little knowledge of what FRT's potential involves, in India the potential for improvement of national security is being examined.

The government is building a massive FRT network, known by the AFRS[17], aimed at easing the monitoring of CCTV by extracting face biometrics from recordings and comparing it with photos contained in a database. The National Crime Records Bureau (NCRB) issued a request for proposal for an Automated Facial Recognition System (AFRS) to be utilized by law enforcement officials across the country on June 28 2020.It was used by investigative agencies in many cases. It was used recently to track demonstrators during Anti CAA protests. Use of AFRS obviously infringes the exercise, as laid out by Article 21 of the Indian Constitution, of a person's right to privacy. When anyone protests, even peacefully, against the government, this technology will allow the government to record the details of all such people, which might lead to the individual protesters being targeted. This will affect the freedom of expression and speech, the right to demonstrate and the right to move in accordance with Article 19. It is important to deliberate as to whether the use of this technology really meet the standard of observation made in the case of K.S. Puttaswamy (Retd.) vs. Union of India[18]. The Supreme Court make it clear that privacy issue is one of the essential right In this case, even in the public area, the Supreme Court held that privacy is an essential right and it has to be respected by the state. But, there is no doubt that it can't be treated as absolute right. To violate this right, the Government must demonstrate that its actions are sanctioned by law, consistent with the necessity of such intervention and in pursuit of a legitimate purpose. With regard to AFRS' legality, the 2000 IT Act categorizes biometric data as sensible personal data and provides procedures for collecting, disclosing and sharing of such data. However, this applies exclusively to 'body companies' rather than the use of biometric facial data by government. This monitoring is also immoral as without its agreement, it necessitates the deployment of FRT among civilians. The lack of confidence among civil society also derives from the fact that without prior discussion or input the government is seeking to create this system. In the Aadhaar judgment[19], which rejected the reasoning for countering black money, for which Aadhaar (India's National Biometric ID) was forced to link up with bank accounts, the Supreme Court noticed that such a restriction would constitute a disproportionate

response for the entire population, without proof of their misconduct. The concern of the Court here plainly demonstrates how the government might misuse AFRS. Moreover, the precision of this technology is sometimes uncertain and might lead to adverse investigative repercussions. Deploying AFRS without any valid controls and balances may therefore lead to significant implications in India. In order to regulate and to achieve responsibility within the framework of governance, the government should create an effective legislative structure, an independent oversight commission.

Issues relating to the Usage of AFRS

Each individual recorded in pictures from CCTV footages & different derivation will be treated as a possible offender by the system, which will create mapping of face, complete with dimensions and biometrics & compare the characteristics to the CCTNS repository. If anyone walk by a CCTV camera, that person are all viewed as possible criminals, which flip the "innocent until proven guilty" assumption on its head.[20] There is apprehension that Face recognition algorithm accuracy rates might be less in the matter of vulnerable section/people of society as many researches across the world are trying to establish this fact. When such technology is used in a criminal justice delivery mechanism where disadvantaged people are overrepresented, misrepresentation become common and they considered as prime offender constitute a risk . Even in laboratory circumstances, image recognition is a difficult process that causes significant errors. Data protection is very difficult since facial recognition is based on the gathering and analysis of information available to the public. The technology can also activate a seamless mass monitoring system, depending on the combination of pictures and other data points. At a time when there is no data protection law in India, AFRS is being considered. For example, Indian tech firms joined hands with Russian tech companies for surveillance cameras on Railway stations.[21] Recently, projects have been started in Gujarat and Maharashtra in over 30 railway stations, as per technology of Ntech Lab of Russia. The law enforcement authorities will be very discretionary in the absence of guarantees. It can result in a cracking mission. The Personal Information Protection Bill 2018 is still in place, and although it is, there are very widespread exceptions for government entities.

There is a vital need to analyze the idea that advanced technology implies increased efficiency. Indian law enforcement will benefit from a deliberate approach, as police agencies worldwide are discovering now that the application is not really efficient from practical perspective as it would appear in principle. In UK, English police services are beleaguered to restrain in usage, following evidence of prejudice and lack of efficiency, of face recognition technology. A total prohibition on the police use of face recognition was just enacted in San Francisco. India is ideally placed to learn from its errors. Whenever , it is important to contemplate ethical considerations of AI based facial recognition, it doesn't limit to the right of privacy only as societal security will always be given priority over individual right. But, the public safety is always a strong argument for a better discourse in the interest of vibrant social democracy. It can

be argued that if putting CCTV camera is justified in vulnerable hotspot area where crime rate is relatively high, then modern technology like facial recognition must be accepted in facilitating crime investigation in sensitive crime. Where there is apprehension of inadequacy of substantive evidence.

Conclusion with Suggestions

Contemporary innovation & advancements in India, the USA, and the UK for the spread of biometric facial recognition for safety and security goals have been described and commented on. The current uses and legal developments of biometric facial identification for public safety purposes in India, the USA, and the UK were emphasized and remarked on. We discussed the basic ethical principles and identified numerous present or potential issues in respect to this type of rapidly growing information technology based on these applications and advancements. The broad demands on community safety nudged the expansion of the use of biometric face recognition databases and systems, which is explicitly and convincingly justified in terms of efficiency in fulfilling a specific security and safety purpose. The rising investment in face recognition technology is required to propel the business over the passage of time. Various companies like Megvii in China, are investing in this area for mass use of facial recognition technology[22]. Covid 19 has also given a boost to its growth. The ongoing trend of less contact life has also given rise to Facial Recognition technology powered by Artificial intelligence in many organizations.

Embracing modern technology and innovation is always encouraging and necessary in the social and national interest of the country. Considering the limited comprehension of AFRS on legal and ethical consideration, it has been widely used by law-enforcement agencies. This innovative mobile based & web based programs can be useful in preventing, detecting crimes and verification of documents in speedy mode. But, in the larger interest of fair and speedy investigation and justice, it is important to synchronize AFRS with Crime and Criminal Tracking Network & Systems (CCTNS) so that a comprehensive database of pictures of people could be arranged. It will interesting to understand how so far this mechanism will success in detection of crime patterns and how does it assist in dismantling of modus operandi of crime gangs. But ,it is essential to assess the limitation and challenges of AFRS as due to error of judgment will give inaccurate conclusion. It is important to maintain the accuracy standard of algorithm used in existing data for identification in the interest of criminal justice delivery system. There is no doubt that due diligence is required for law enforcement agencies and forensic cyber laboratories for which proper training and capacity building programmes should be encouraged in the field of application of artificial intelligence and machine learning. No doubt, it is also treated as vulnerable innovative application, mismatches in identification of faces can't be ignored as it can be misused and used as tainted evidence. Perhaps, that's why, critics raised their apprehension about its integration with different law- enforcement agencies. It is matter of contemplation how modern technology like facial recognition often face with conflicting discourse with advocates of privacy law and data protection despite the fact data protection bill is still pending and under

consideration. In fact, corporate entity like IBM also withdrew from there facial recognition business explaining concerns related to public vigil, ethnic profiling and actions adverse to basic fundamental rights.[23]

However, this mapping technology of facial recognition seems to be accepted by different institutions for their specific purpose. For example, this innovative AI based facial- recognition vigil assist prison administration in Gurugram last year to execute crowd management and appropriate compliance of social –distancing norms among prisoners. It also helps in preventing and detecting any kind of illegitimate practices occurred among prisoners.[24] Even, it can be quite useful in identification of crime professionals and victims in cases of human trafficking, missing persons and different kinds of organized crime where there is element of conspiracy and inadequacy of direct evidence or eye witness to specific crime. With the increasing technology, it is possible that this AFRS may come with more modern innovation, but the concerns related to prejudices and bias for vulnerable section of society will remain same. So, it is important that such kind of modern AI technique based facial recognition may have to pass through appropriate test of proportionality so that legal criticism can be addressed and it is possible to find a balanced approach whereby proper regulation could be made about its nature and effective implementation to fulfill the existing inadequacy in the legal regime.

References

[1] Mordini, Emilio & Petrini, Carlo. (2007). Ethical and social implications of biometric identification technology. Annali dell'Istituto superiore di sanità. 43. 5-11.

[2] Yaroslav Kuflinski, How Ethical is Facial Recognition Technology?, Towards data science, April,11, 2019, https://towardsdatascience.com/how-ethical-is-facial-recognition-technology-8104db2cb81b.

[3]Jane Wakefield, AI emotion-detection software tested on Uyghurs, 26th May 2021, *BBC News* https://www.bbc.com/news/technology-57101248.

[4] Marcus Smith · Seumas Miller, The ethical application of biometric facial recognition technology, AI & Society, https://doi.org/10.1007/s00146-021-01199-9 .

[5] Kevin Bonsor& Ryan Johnson, How Facial Recognition Systems Work, 28th Jan 2019, https://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm.

[6]Clearview AI, https://clearview.ai/.

[7]Statement of Claim, State of Vermont v Clearview AI, Vermont Superior Court, 10 March 2020, 8.

[8] Haeggquist & Eck, LLP, Sean Burke and James Pomerene, v. Clearview AI, Inc., a Delaware Corporation; Richard Schwartz, Case Number: 20CV0370 BAS MSB, 5–8.

[9]Alex Najibi, Racial Discrimination in Face Recognition Technology, 24th Oct 2020,*Havard University Blog,* https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

[10] Joy Buolamwini, TimnitGebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, Conference on Fairness, Accountability, and Transparency, p 12.

[11] Bing Guo v Hangzhou Safari Park (Hangzhou Fuyang District Court, Zhejiang 0111, Civil No. 6971, 20 November 2020).

[12] R (Bridges) v. CCSWP & SSHD,[2019] EWHC 2341(Admin).

[13] The UK Biometrics Commissioner was established under the Protection of Freedoms Act 2012 (UK) in response to the judgement in the S and Marper v United Kingdom [2008] ECHR 1581 case in the European Court of Human Rights in 2008.

[14]Protection of Freedoms Act 2012 (UK) c 9, s 20.

[15] Neetu Thru Rewati Ram v. State, W.P.(CRL) 869/1998 & CRL.M.A.5967/2018.

[16] Soibam Rocky Singh, Facial recognition technology: law yet to catch up, The Hindu, Dec. 31, 2020, https://www.thehindu.com/news/cities/Delhi/facial-recognition-technology-law-yet-to-catch-up/article33458380.ece.

[17]Karishma Malhotra, , Automated facial recognition: what NCRB proposes, what are the concerns, *Indian Express,* July 10 2019, https://indianexpress.com/article/explained/automated-facial-recognition-what-ncrb-proposes-what-are-the-concerns-5823110/ .

[18] Writ (Civil) No 494 of 2012, (207) 10 SCC 1, AIR 2017 SC 4161.

[19]K.S. Puttaswamy (Retd.) v Union of India Writ (Civil) No 494 of 2012, (207) 10 SCC 1, AIR 2017 SC 4161.

[20]VidushiMarda, Facial recognition is an invasive and inefficient tool,19th July 2019, *The Hindu* https://www.thehindu.com/opinion/op-ed/facial-recognition-is-an-invasive-and-inefficient-tool/article28629051.ece.

[21]*Dipanjan Roy Chaudhury, Indian, Russian tech firms join hands to implement landmark face recognition project*, Economic Times, Aug.26,2021, https://economictimes.indiatimes.com/news/india/indian-russian-tech-firms-join-hands-to-implement-landmark-face-recognitionproject/articleshow/85646014.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst .

[22]Megvii, the Chinese startup known for facial recognition, 19 Aug 2019, https://techcrunch.com/2019/08/26/megvii-the-chinese-startup-unicorn-known-for-facial-recognition-tech-files-to-go-public-in-hong-kong/ .

[23] Anu Thomas, As IBM exits facial recognition business, A look at how the tech has advanced in India, Analytics India Mag., 9th June,2020, https://analyticsindiamag.com/as-ibm-exits-facial-recognition-business-a-look-at-how-the-tech-has-advanced-in-india/.

[24] Anu Thomas, How AI can help manage prisons amid covid-19 pandemic, Analytics India Mag., 3rd May,2020, https://analyticsindiamag.com/how-ai-can-help-manage-prisons-amid-covid-19-pandemic/.