AI'S TRANSFORMATIVE ROLE IN CRIMINAL INVESTIGATION AND THE QUEST FOR ETHICAL BALANCE

Prabhakara Rao Karlapalem, Research Scholar, Noida International University, Noida

ABSTRACT

The integration of Artificial Intelligence (AI) in criminal investigation represents a paradigmatic shift in law enforcement methodology, offering unprecedented capabilities in data analysis, predictive policing and criminal investigations. This paper examines the multifaceted role of AI technologies across the criminal justice jurisdiction, from initial crime registration till forensic analysis. Contemporary AI applications include facial recognition systems like Clearview AI, predictive policing tools such as PredPol, risk assessment instruments like COMPAS and HART, and digital forensic platforms including Magnet AXIOM AI for comprehensive data extraction and analysis.

The study reveals AI's transformative potential in processing voluminous datasets, reconstructing crime scenes, identifying suspects through biometric analysis, and optimizing resource allocation for law enforcement agencies. Countries including the USA, UK, Germany, and India have increasingly deployed AI systems, demonstrating enhanced investigative efficiency, reduced human error, and improved decision-making support.

This paper notes significant ethical concerns emerge regarding output bias, data privacy violations, accountability issues, and threats to fundamental rights including presumption of innocence and fair trial guarantees. The "black box" nature of advanced AI systems raises questions about transparency and judicial acceptance of AI-generated evidence. Critical issues include biased data feeding leading to discriminatory outcomes, particularly affecting minority communities, and the insufficient legislative regulatory frameworks.

The paper concludes that while AI offers revolutionary investigative capabilities, realizing its full potential requires striking a delicate balance between technological advancement and ethical safeguards through comprehensive legislation, international cooperation, and robust

accountability mechanisms to protect fundamental human rights while enhancing criminal justice efficiency.

Keywords: Artificial Intelligence, Criminal Investigation, Forensic Investigation, Bias, Ethics

INTRODUCTION

The rapid development of Artificial Intelligence across the disciplines touched all the facets of human life creating a paradigm shift in our thinking. In the middle of 20th Century, Alan Turing conceptualized it and in 1955 John McCarthy coined the term Artificial Intelligence. Defining Artificial Intelligence in a single universally acceptable statement proves difficult due to its rapid growth in every human activity and multifarious functionality. The High Level Expert group on AI technically defined - "Systems designed by that, given a complex goal, act in the physical or digital world by perceiving their environment, interpreting the collected structured or unstructured data, reasoning on the knowledge derived from this data, and deciding the best action(s) to take".[1] Simply defined Artificial Intelligence is a subdiscipline of computer science that aims at the design of systems able to perform tasks that normally require human intelligence.

Based on their functionality AIs can be categorized into three types: The first category is Reactive AI like Deep Blue or IBM's chess-playing computer, which cannot form memories or past experiences to determine present decisions. Second category AIs carry large stored memory to provide solutions to future problems. Third category is 'Theory of Mind AIs' mimicking human mind in decision making while possessing some quantum of emotions and having conversations. In future, self-awareness AIs may come into existence that behave just like human brains in thinking and emotions.[2]

Based on the capability or level of intelligence, AI can be classified as Narrow/weak AI (ANI), General / strong AI (AGI) and Super AI (ASI). Presently available Weak or narrow AIs perform special tasks with intelligence in specific area, particularly in professional fields like speech and image recognition or self-driven automobiles etc. displaying highly specialized,

[1] Maria do Céu Cunha Carrão, Artificial Intelligence in Criminal Proceedings The Admissibility of AI-Generated Evidence (2022) (Master's Thesis dissertation, Universidade NOVA de Lisboa (Portugal)), https://search.proquest.com/openview/2db3a1fd2e98d844a73157712b3a3dba/1?pq-origsite=gscholar&cbl=2026366&diss=y.

[2] David Ekanem, Artificial Intelligence as a Mechanism for Crime Control in Nigeria: A Critical Appraisal (2020), https://www.academia.edu/download/62394027/Artificial_Intelligence20200317-42980-yle5e5.pdf.

and purpose-built characteristics. Strong AIs supposedly able to think at the level of nearly like humans with self-awareness and it is still in offing and may be future AI. Super AIs surpass human intelligence in all dimensions and can solve humanely impossible all problems and tasks and it is still a hypothetical wish of mankind.[3]

Based on their implementation AIs can be divided as software-based AIs like voice assistants, image analysis software, search engines, speech, image and face recognition systems or hardware-based AI such as advanced robots, driverless cars, drones and Internet of Things etc.[4]

Artificial Intelligence touched all walks of life and impacted every facet of human activity through its application and exploding transforming potential. Be it in Cybersecurity or combating cybercrime, Healthcare or Medicine, Transportation, finance, daily life automation or criminal justice or law enforcement, everywhere AI displayed unique, ubiquitous, and indispensable nature. Several experts forecast that total dependence on AI invites adverse consequences for future generations in social, economic and political life and sane advices pour to strike a balance between human activity and AI's role in day-to-day life.

ROLE OF AI IN CRIMINAL INVESTIGATIONS

AI role in criminal investigations is no exception. Criminal jurisdiction can be traditionally divided into three stages. It starts with law enforcement or crime detection agencies initiate criminal investigation after taking cognizance of crime committed. Next, courts conduct inquiry during judicial proceedings and later on trial commences and concludes by acquittal or conviction. The appellate courts and revisional courts deal with revisions and appeals, if they are called for. Besides, courts during the trial, deal with bail matters and post-conviction, deal with the matters related to parole and furlough. Courts consider the issue of recidivism or repetition of offence, while deciding quantum of punishment to the convicts. Rapid growth of AI found its way in all the stages of criminal justice system, but, at present, it plays the vital role in the first stage, criminal and forensic investigation. The courts yet to initiate to deploy AI in judicial inquiries, trials, revisions and appeals, even though Court administration use AI

[3]Yingjie Du et al., *A Review of the Application of Artificial Intelligence in Criminal Investigation*, *in* 2022 3rd International Conference on Artificial Intelligence and Education (IC-ICAIE 2022) 1544 (2022), https://www.atlantis-press.com/proceedings/ic-icaie-22/125981187.

[4] Srishti Agarwal, *Use of Artificial Intelligence in Criminal Cases*, 2 International Review of Law and Technology (2023), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4609135.

applications in case management system, preparation of cause lists, data analysis, translation of documents and judgements, which do not require high level of intelligence.

Deployment of AI in the first phase, i.e., criminal investigation by enforcement agencies emerged as imminent feature in the current criminal investigations. USA uses PredPol to predict the place of a crime and allocate the police resources to prevent crime. The USA courts use AI tool HART (Harm Assessment Risk Tool) while deciding the bail applications of under-trials and, also parole applications of convicts to assess the risk of letting him go from confinement and his potential to repeat the offence. US courts deploy COMPAS (Correction Offender Management Profiling for Alternative Sanctions) that provides 137 questions to the court to put to the accused or convict and elicit answers to assess his propensity to repeat the offence within two years of its first occurrence, to take informed decision about his bail or quantum of punishment to be imposed on him. In forensic investigations and analysis, Canada developed Magnet AXIOM AI for digital investigation to discover and check the relevant information from smart phones and computers for thorough digital analysis. It analyses semantic and conversational content recovered from the smartphones and computers of the suspects and aids in crime detection.[5] The reliance on AIs like Clearview AI for facial recognition or the skeleton ID[6] programme to identify the deceased, during pre-trial investigation, became norm.

The facial recognition technology (FCT) analyzes human facial features, creating mathematical representation of them, and comparing this representation with known faces from databases.[7] This technology is used in surveillance, airports, border crossings, unlawful assemblies, rallies and demonstrations, identifying the suspects and criminals from vast databases available with the authorities. USA uses Clearview AI FCT, Facebook uses Deepface and I-phone uses Mobile Offender Recognition and Information System (MORIS). Indian Government deploys Automatic Facial Recognition System (AFRS) developed by it, Punjab police use FRT-PAIS, Rajasthan police use ABHED, U.P. police use Trinetra, Delhi Police use CMAPS and A.P. Police use e-Pragati. Besides, in India, for data processing, inter-agency coordination, and

[5]N. A. Wickramarathna & EATA Edirisuriya, *Artificial Intelligence in the Criminal Justice System: A Literature Review and a Survey* (2021), http://192.248.104.6/handle/345/5244.
[6] Valery Shepitko et al., *Artificial Intelligence in Crime Counteraction: From Legal Regulation to Implementation*, 1 Social and Legal Studios 135 (2024), https://sls-journal.com.ua/en/journals/tom-7-1-2024/shtuchny-intelekt-v-protidiyi-zlochinnosti-vid-pravovogo-regulyuvannya-do-realiy-zastosuvannya.
[7]Omar Alakayleh, *The Use of Artificial Intelligence Systems in Crime Detection and Prevention: Applications and Challenges*, Available at SSRN 5132225 (2025), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5132225.

crime data analysis CCTNS (Crime and Criminal Tracking Network System), E-prisons and e-forensics are used for integration and connection of data related to crimes across the states. Government of India launched AI driven e-Courts Project ad E-SCR portals for legal research, case management and translating court judgements and AI driven legal chatbots to answer the queries of citizens relating legal matters.

When complaint is received through telephone, Speech to text software is used to register FIRs in real time. Voice analysis AIs assist to identify speakers matching with the voice samples procured by the investigative authorities from suspects or comparing it with already available vast audio database or extract important information in a text format from audio recordings.

The indispensability of AI springs from its capability to learn and adopt from data and experiences provided to it, incessive reasoning, precise problem solving, perfect decision making while providing alternative decisions to choose from and creating innovative ingenious thoughts provoking future actions, perceiving enormous visual and auditory sensory data locating, pinpointing, and identifying the requisitioned images or voices. In processing vast amounts of data and identifying patterns, AI displays unparallel triple qualities of enhanced efficiency, accuracy and capability.

AI demonstrates its usefulness in several spheres of criminal investigation. Firstly, it segregates crime-related specific data from massive generic data, i.e., communication data, network data, audio, video data and other sorts of data and examines and analyses crime data and give the requisitioned output. Secondly, mining the vast data including social media data, it recognizes patterns and predict vulnerable crime spots and potential suspects and advice the police department to deploy sufficient police force to prevent crimes and also catch criminals in the event of crime takes place. It optimises police force and also saves human and financial resources. Thirdly, AI scans the crime scene photographs and images, analysing them and produce animated videos of crime scene by reconstructing crime scene. Then it identifies and recognize individuals and objects in the photographs and images by comparing with the stored data by facial, image and voice recognition technologies. In forensic investigations, AI identifies the dead bodies of unknown persons, estimate age, injuries that caused death, weapon used, ballistic reports, analyse DNA samples and generate reports that could be used as corroborative evidence in courts.

AI provides improved investigative tools, decision making support, reduction of human error and bias and enhanced predictive policing and resource allocation resulting to cost and resource efficiency, speedy investigation and criminal trial.

In wide range of areas within criminal investigation, several countries like USA, UK, Fance, Germany, Netherlands, Greece, Estonia, Portugal, Lithuania, Singapore, Argentina, United Arab Emirates actively deployed AI and in India it is still in nascent stage. In India, AI activities are restricted within the boundaries of criminal and forensic investigations and courts are still hesitant to introduce AIs in judicial proceedings, recording evidences and decision makings.

RISKS RELATED TO AI USE

Indubitably increased AI deployment in criminal and forensic investigations would be unavoidable on account of its ability to deal with voluminous data speedily and accurately generating spectacular analytical output, but several quarters raised concerns of ethical considerations surrounding bias, data privacy, human rights violations and trust issues. AI works on the massive data including sensitive personal data fed in the system for analysing and perceiving and if the data provided to the system intentionally or unintentionally laced with bias, the output result would obviously reflect the correspondinng bias creating the issue of trustworthiness of the AI in the minds of stakeholders. After all, only human agencies collect and feed data to AI. If human agents suffering from racial, linguistic, colour, religious, caste, gender, geographical or any other variety of bias, collect and feed data, the result delivered by AI would indubitably be unreliable biased data. Meticulous precaution required to be taken while feeding unbiased data into AI to obviate all types of adverse consequences in criminal investigations and allay the apprehensions about trustworthiness of AI in Criminal and forensic investigations. In India it becomes more so, because the significant section of criminal law critics perceive that members of religious minority communities face criminal proceedings and convictions at disproportionately high rates compared to their share of the general population and their overrepresentation in jail populations reflects the biased attitudes of law enforcement and investigative agencies. The police department of Pennsylvania, USA has been phasing out PredPol technology as its outcomes displayed bias against black communities. Similarly, some courts in USA raised credibility questions about COMPAS (Correction Offender Management

Profiling for Alternative Sanctions) technology that assists courts to determine parole or alternative sentencing apprehending its skewedness against black people.

The advanced AIs operate on deep learning, called 'Black Boxes', and they deliver the result based on opaque and indecipherable reasoning process and that creates ethical concerns. The courts would be reluctant to consider the results derived from the opaque Black Box logarithms.

In democratic Societies, in criminal investigations, some human agent or agency is accountable for every wrong doing. In AI stimulated outcomes, machines cannot be accountable for the pitfalls, however grave they may be and whatever evil consequences they bring in. While relying AI outcomes in criminal jurisdiction, absence of accountability creates great ethical concern.

DATA PRIVACY AND HUMAN RIGHTS VIOLATIONS

Once investigative agency brings the suspect to the police station, it collects his personal data during detention before producing him into the court within 24 hours of his detention. The data consists of his photograph, signature, blood sample, voice sample, medical examination etc. and other personal data which becomes raw material for Facial, image, speech, gait, finger print recognitions, identification of person, voice analysis, and other biometrics and this data subsumed permanently in the data bank violating fundamental right of data privacy of the suspect. This sensitive data, in the absence of data security environment, becomes target for breaches and misuse.

The basic principle of criminal law all over the modern criminal jurisprudence recognizes the innocence of accused till proven guilty and also provides fair trail and these dual fundamental rights protect the sanctity of criminal justice system. Predictive policing undermines presumption of innocence. The rampant use of AI without safeguards to the data from where it draws its power poses great threat to the suspect's fundamental rights of presumption of innocence, no-discrimination, fair trial, privacy and due process. This major concern demands enough legislative and accountability measures before engaging AI in full pledged manner in criminal investigation.

LEGISLATION TO REGULATE AI FUNCTIONS

The balance has to be struck between the benefits AI brings in criminal and forensic investigations and the ethical concerns, it generates. A comprehensive legislation that addresses these concerns may be the answer.

European Union, in the forefront, enacted a comprehensive EU AI Act[8] balancing benefits and risks aiming to ensure the AI systems are lawful, ethical and technically robust. As all the nation-states widely use AI in criminal investigations, a unified international approach can plug the problem. Disorganized, inadequate or totally absent legal frameworks across the countries create roadblocks for effective utilization of AI in criminal justice system. Lack of technical expertise in law enforcement agencies pose problems for optimum utilization of AI. Legislative provisions in Evidence Acts across the jurisdictions prohibit or restrict the admissibility of AI generated evidence nullifying the benefits of AI utility in criminal investigations.

Indian Parliament has not passed any specific Act, rules or regulations regulating the use of AI generally and in criminal investigations, particularly. AI threats like deepfakes came into light repeatedly and even then, the parliament has not taken remedial legislative measures to curb such nefarious activities and misuse of AI in public domain.

The Parliament of India passed the Digital Personal Data Protection Act, 2023 (DPDP) on 31st August, 2023[9] indicating its purpose as "to protect digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes and for matters connected therewith or incidental thereto". Critics of this Act attributed it only a foundational law that addresses the limited area of data privacy aspects of AI, and needs a more comprehensive regulatory framework specifically dealing with AI technology itself targeting variety of AI threats like deepfake pornographic content against women, accountability etc. AI systems work on massive amounts of data that includes personal data of large population, its application in any field and more particularly in criminal justice field raises significant concerns about privacy and security of

[8] https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

[9] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

personal data. The provisions of DPDP Act, 2023 addresses those concerns to a certain extent, as the Act seeks free, clear and informed consent of the data Principal, (the individual to whom the digital personal data relates), notice to the data Principal before processing his data indicating the grounds for processing data, appointment of data protection officer, constitution of Data Protection Board, creation of Data trusts for restraining misuse of data. The predecessor Acts like Information Technology Act, 2000, RTI Act, 2005 and Aadhar Act, 2016 covered other aspects of data but not protected privacy and security of personal data of individuals available in public domain. When IT Act, 2000 focuses on electronic records, RTI Act, 2005 limits access to information held only by Public Authorities and Aadhar Act, 2016 regulates Aadhar number and biometric information for identity purposes. Despite its limitations, DPDP Act, 2023 provides consented, lawful and transparent use of personal data, as well as purpose limitations, data minimisation, data accuracy, storage limitations, reasonable security safeguards and accountability. The Parliament of India must consider in their future legislations about specifically dealing with the deepfake pornographic content against women and provide explicit regulations for all AI related harms while dealing with data as the usage of AI in criminal and forensic investigations is ever increasing and may soon extend to criminal courts.