Research on the Application of Artificial Intelligence in Criminal Investigation and Its Legal Issues

Yun Pei
[1] EMILIO AGUINALDO COLLEGE, 006302, Manila, Philippines

Abstract—With the rapid development of artificial intelligence technology, its application in the field of criminal investigation has become an important direction of change in the investigation model of public security organs. The embedding of AI technologies such as face recognition, big data analysis, and behavior prediction has significantly improved the efficiency of investigation, but it is also accompanied by many legal risks such as privacy infringement, algorithm bias, and lack of procedural justice. Starting from the current status of technology application, this article systematically analyzes the main legal issues faced by artificial intelligence in criminal investigation, including the legal boundaries of personal information protection, the admissibility of AI evidence, and procedural control mechanisms. On this basis, drawing on the legal regulatory experience of the United States, the European Union, Japan, Germany and other countries, it is proposed that China should establish the boundaries of technology use, strengthen data protection mechanisms, and improve the evidence system and supervision mechanism through legislation to build a legal regulatory system for artificial intelligence criminal investigation that takes into account efficiency and rights protection. The article aims to provide theoretical support and institutional reference for the construction of relevant systems and legal responses in China.

Keywords: artificial intelligence; criminal investigation; privacy rights; algorithm regulation; legal supervision

1. INTRODUCTION

With the deepening of the new round of scientific and technological revolution and industrial transformation, artificial intelligence technology has gradually moved from the theoretical level to practical application, and has penetrated into many fields such as social governance, medical care, education, finance, and transportation. Among them, in the criminal justice system, especially in the field of criminal investigation, the intervention of artificial intelligence is unfolding at an unprecedented speed and depth. AI technologies represented by face recognition, big data analysis, behavior prediction, and natural language processing are being widely used in combating crime, maintaining social order, and improving case handling efficiency, promoting the gradual transformation of criminal investigation from the traditional "manpower + experience-driven" model to the "technology + data-driven" model. This trend not only improves the accuracy and efficiency of investigation work, but also significantly changes the operating logic of traditional criminal justice. Taking face recognition technology as an example, public security organs can quickly lock and locate suspects through a large number of cameras deployed in public spaces; with the help of big data analysis platforms, public security personnel can screen and correlate massive social information, thereby constructing a suspect's social relationship map and behavior trajectory; and with the help of AI algorithms, the system can even conduct "predictive policing" before a case occurs to assess potential high-risk individuals and high-risk areas. The application of these new technologies not only improves the efficiency of solving cases, but also effectively saves manpower and resource costs, demonstrating strong technological governance capabilities.

However, the rapid intervention of technology has inevitably raised many legal and ethical issues. First, in the case of technology abuse or lack of supervision, citizens' personal information and privacy rights are easily violated. For example, collecting personal biometric information without explicit authorization, conducting all-round monitoring of citizens' daily behavior, and arbitrarily calling private information in big data platforms may constitute a substantial violation of the relevant provisions of the "Personal Information Protection Law of the People's Republic of China" and the "Civil Code of the People's Republic of China". Secondly, there is a "black box operation" problem in the process of data screening and judgment by algorithms. Due to the lack of transparency and explainability of the operating mechanisms of many AI systems, when the results of algorithm judgments are used as criminal evidence, their legality and fairness are easily questioned, which in turn affects the procedural justice and substantive justice of the case. In addition, the data samples used by AI systems often carry historical biases. If they are not corrected, it is very likely that specific groups will be misidentified, discriminated against, or even "labeled", thereby objectively exacerbating judicial inequality. In the process of deep integration of artificial intelligence and criminal investigation, investigators may weaken their subjective analysis and comprehensive judgment of case facts due to their high dependence on technology, and show a tendency of "technological determinism". This is not only easy to lead to the occurrence of false and wrongful convictions, but also may shake the basic trust of the public in judicial justice.

In short, the reshaping of the criminal investigation model by artificial intelligence is an inevitable trend, and the legal challenges it brings cannot be ignored. Only on the basis of a comprehensive review of the application scenarios and potential risks of AI technology, combined with the actual construction of China's legal system, and building a scientific, reasonable and perfect legal regulatory framework, can we achieve the long-term goal of rule of law in China while ensuring judicial efficiency and social stability. Technology is neither good nor bad, the key lies in whether its application method and institutional regulation can be reasonably in place. Therefore, how to build a legal normative system that conforms to China's national conditions, is forward-looking and operational while promoting intelligent investigation has become an important topic that urgently needs to be explored in depth.

2. Research Methods

The application of artificial intelligence in criminal investigation is a comprehensive research topic with strong technicality, high degree of interdisciplinary integration, and increasingly prominent legal disputes. In order to ensure that this study is scientific and logical in theory and has practical guiding significance in practice, this paper adheres to the basic principles of "combining theory with practice" and "combining comparison with localization" in the selection of research methods, and comprehensively uses the following research methods:

2.1. Literature analysis method

The literature analysis method is one of the basic methods of this study. This paper systematically sorts out the relevant research results on artificial intelligence in the judicial field, especially criminal investigation, at home and abroad, including academic papers, judicial interpretations, legal texts, policy documents, international conventions and various technical reports, etc., and extracts the main views and controversial points of the current academic and practical circles on this issue, and builds a theoretical framework for the research based on this. Special attention is paid to the advanced experience of other countries developed countries (such as the United States, the United Kingdom, Germany, etc.) in privacy protection, data security, AI technical specifications, procedural justice protection, etc., as well as China's legislative and judicial progress in the legal regulation of artificial intelligence in recent years, in order to provide solid literature support and comparative perspectives for this study.

2.2. Comparative research method

Considering the significant differences in the operating mechanisms and regulatory models of AI criminal investigation technology in different countries and legal systems, this article widely uses comparative research methods to compare and analyze the similarities, differences, advantages and disadvantages of AI investigation technology deployment, legal regulatory framework, and procedural control mechanisms in China and other countries countries. Through in-depth research on the legal regulatory mechanisms of the US "predictive policing" system, the EU "Artificial Intelligence Act", and the British police face recognition system, we explore the reasonable factors in their institutional design and explore their inspiration and limitations for China's institutional construction, so as to provide theoretical support and practical reference for China to build a legal regulatory path with local characteristics.

2.3. Case analysis method

In order to enhance the pertinence and practicality of the research, this article selects several representative China and Other countries cases to analyze the application scenarios of artificial intelligence technology in specific criminal investigation practices, the legal issues arising, and their judicial responses. Through the restoration of the cases and legal analysis, we reveal the legal disputes, power abuse risks, procedural deviations and other issues that may arise in the process of AI intervention in investigation. For example, we analyze the privacy dispute cases caused by the public security organs in a certain place in China using facial recognition technology to arrest criminal suspects, as well as the constitutional review cases in the application of algorithm prediction systems in the United States, extract common legal issues from specific events, and further verify the realistic basis of theoretical analysis.

2.4. Normative analysis method

Normative analysis method is one of the core methods of this study. Starting from the perspective of jurisprudence and criminal procedure law, this paper focuses on analyzing the interactive relationship between artificial intelligence technology and current legal norms, including the adaptability and limitations of the current legal system in the context of AI application, such as the right of investigation, the right of privacy, the rules of evidence, and procedural justice. Through the interpretation of current legal provisions such as the Criminal Procedure Law, the Personal Information Protection Law, and the Data Security Law, combined with judicial interpretations and case handling rules, we analyze the legal obstacles that AI investigation technology may face in practice, and further propose specific directions and path suggestions for the improvement of the legal system.

2.5. Logical deduction and system construction method

On the basis of completing the in-depth analysis of existing legal provisions and practical problems, this paper will also use logical deduction and legal system construction methods to try to propose a set of operational and forward-looking legal regulation paths for AI criminal investigation. This method mainly summarizes existing problems, deduces legal relations, and extracts normative principles, and on this basis builds a logically self-consistent and structurally complete legal system recommendation system. This process not only attaches importance to theoretical consistency, but also takes into account practical feasibility, reflecting the institutional construction orientation of the research.

3. Review of China and Other countries research

3.1. Technological development perspective: the current status of AI deployment in the police system

Against the background of the rapid development of artificial intelligence, many countries have actively promoted the deployment and application of AI technology in the police system, especially in the field of criminal investigation, aiming to improve law enforcement efficiency, reduce crime rates and optimize the public security governance structure.

Internationally, as an important promoter of artificial intelligence technology, the United States introduced AI technology into the police system earlier. Police in New York, Los Angeles, Chicago and other places have deployed "predictive policing" systems based on AI algorithms. Through the mining and analysis of historical crime data, early warning intervention is carried out on potential high-incidence areas and key personnel. Among them, the "PredPol (predictive policing)" system is the most representative. It builds an algorithm model based on variables such as time, location and crime type to assist the police in the reasonable deployment of patrol forces. In addition, US law enforcement agencies widely use technologies such as face recognition, voice recognition, license plate recognition, and drone detection to locate, track and collect evidence of suspects. For example, the US Federal Bureau of Investigation (FBI) has established the "Next Generation Identification System", which integrates multiple biometric data such as fingerprints, faces, and irises to achieve cross-regional and cross-departmental information sharing and comparison, greatly improving the efficiency of investigation.

In Europe, the application of AI in the police system is also accelerating. The Metropolitan Police in the UK once piloted the use of the Live Facial Recognition system for street patrols, but at the same time, the technology triggered strong privacy disputes and legal challenges in the UK. The EU focuses more on the coordination between technology deployment and legal ethics. The draft of the "Artificial Intelligence Act" clearly stipulates that high-risk AI systems must be subject to strict review, and proposes that technology development must comply with the principles of explainability, fairness and controllability, reflecting the high attention paid to the "responsible use" of AI.

In China, the promotion of artificial intelligence technology in the public security system is particularly rapid, especially in the fields of face recognition, video surveillance, voice recognition, semantic analysis and big data combat platforms, which have achieved a high degree of integration. At present, most provincial and municipal public security organs in the country have built "synthetic combat centers" or "intelligence and command integration platforms", relying on artificial intelligence and big data analysis tools to conduct dynamic deployment, trajectory tracing, case-related relationship analysis and other combat commands. Among them, the "Skynet Project" and the "Xueliang Project" constitute the backbone system of the national video surveillance network. A large number of front-end camera equipment use AI algorithms to realize face recognition and behavior recognition, and connect with the public security back-end database, enhancing the technical prevention and control capabilities of criminal crimes.

However, it is worth noting that although the AI system has greatly improved the efficiency of police operations, the relevant technical deployment has problems such as generalized application, inconsistent standards, and opaque algorithms, which are prone to legal risks such as abuse of rights and privacy leakage. Especially in criminal investigations, there is still a lack of systematic institutional responses to issues such as the legal boundaries of technology, standardized collection of evidence, and secure storage of data. Therefore, more and more studies have begun to reflect deeply and build regulations on AI investigative behavior from a legal perspective.

3.2. Legal research perspective: Preliminary discussion on privacy rights, data protection, and procedural justice

The application of artificial intelligence technology in criminal investigation has aroused the academic community's attention to a series of legal issues such as privacy rights, data protection, algorithmic fairness and procedural justice, and gradually formed an interdisciplinary research trend with "law-technology integration" as the core.

In terms of privacy rights and data protection, Western scholars generally advocate that the "minimum necessary principle" should be used to limit the collection and processing of personal information by investigative agencies. Daniel Solove proposed that privacy is not only a "right to be forgotten", but also a "right to control information flow", emphasizing that individuals should have the right to decide how their information is collected, transmitted, analyzed and stored. Under the guidance of this theory, the European Union passed the General Data Protection Regulation (GDPR), established a complete set of personal information protection systems such as data minimization principles, transparency principles, consent principles and "right to be forgotten", and required enterprises and public agencies to review and explain "automated decision-making" behaviors. This legislation provides a normative reference for data governance in criminal investigation activities under the background of artificial intelligence.

The American academic community is more concerned with the "conflict between technology and constitutional rights." Scholars such as Laurence Tribe pointed out that technology cannot override the Constitution, and the use of AI in criminal investigations must strictly follow due process, especially under the premise that the citizens involved have not yet been convicted, the results of technology cannot be regarded as the basis for conviction. Many judicial cases (such as Carpenter v. United States) have emphasized that law enforcement agencies must obtain legal authorization to obtain electronic data, and cannot use technology to circumvent traditional search warrant procedures, which reflects the constitutional review path for the use of technology.

The Chinese legal community started research on this issue a little later, but in recent years, it has gradually formed relatively systematic academic results. On the one hand, some scholars focus on the risk of infringement of citizens' privacy rights and personal dignity by AI investigation activities, and advocate the establishment of bottom-line norms for the use of technology through basic laws such as the "Personal Information Protection Law" and the "Data Security Law"; on the other hand, some studies have proposed that AI's involvement in the investigation process may challenge traditional criminal prosecution principles such as "innocent until proven guilty" and "legality of evidence", and call for the establishment of special rules and certification mechanisms for the acceptance of AI evidence. In addition, some practitioners emphasize the need to introduce an "algorithm audit system" to ensure that the use of AI systems does not constitute a disguised means of depriving the defendant of his rights.

At the same time, some studies also focus on the systematic impact of "algorithmic discrimination" and "technical bias" on judicial justice. Since AI systems rely on large-scale historical data for training, these data may contain labeling of specific groups, regional bias, and even racial discrimination, which in turn leads to "selective law enforcement", "high-risk group locking", and "group accidental injury" in AI execution. For example, a study in the United States found that some predictive policing systems generally have a high risk assessment of black groups, which directly affects the deployment of police forces and law enforcement strategies, reflecting the problem of "structural injustice" in the application of technology.

In summary, although the current legal research on the application of artificial intelligence in criminal investigation at home and abroad has achieved certain results, it is still in the exploratory stage overall. Existing studies mostly focus on principled analysis and value conflict analysis, lack of in-depth discussion of specific technology usage scenarios, and have not yet formed a systematic and complete legal governance framework. Therefore, based on previous research, this article attempts to systematically analyze the current status of the use of AI technology in criminal investigation, legal conflicts, and regulatory paths from the perspective of technical practice, and strives to provide theoretical support and institutional reference for the construction of relevant systems in China.

4. Application of AI in Criminal Investigation and Legal Implications

4.1. Main Applications of Artificial Intelligence in Criminal Investigation

The rapid development of artificial intelligence technology and its deep integration in public security law enforcement are gradually reshaping the working mechanism of traditional criminal investigation. Different from the previous case-handling methods that rely on manual judgment and experience accumulation, artificial intelligence, with its powerful data processing capabilities, accurate identification capabilities and real-time response capabilities, makes criminal investigation more efficient and technically supported. The following will expand from four key technical dimensions to explain its core application scenarios and functional characteristics in criminal investigation.

4.1.1. Face recognition and behavior recognition technology

4.1.1.1. Public place monitoring and target locking

Face recognition technology is one of the most widely used AI investigation methods at present. It mainly collects, compares and recognizes facial features through high-resolution cameras and deep learning algorithms. This technology is widely deployed in public security monitoring systems such as the "Skynet Project" and the "Xueliang Project", realizing 24-hour video monitoring and key personnel control functions in public places such as stations, airports, shopping malls, and streets. By comparing the captured faces in the surveillance images with the fugitives, suspects involved in the case, and key targets in the public security database in real time, the identity can be confirmed and an early warning can be issued within a few seconds, greatly improving the efficiency of on-site crackdown and control.

In addition, behavior recognition technology has developed rapidly in recent years. It can identify possible violent behaviors, thefts, or suspicious wandering behaviors by analyzing human postures, movement patterns, and abnormal trajectories. For example, some cities have deployed AI systems to identify abnormal actions such as fighting, falling, and running. Once the preset threshold is triggered, the system will automatically issue an alarm and push the image to the command center to achieve the integration of active investigation and early warning response.

4.1.1.2. Recognition accuracy and risk of misidentification

Although face recognition and behavior analysis systems have greatly improved the efficiency of investigation, their recognition accuracy and risk of misidentification are still key issues that need to be urgently solved by current technology. For example, in scenes such as poor lighting, more occlusion, and fast-moving targets, the recognition accuracy rate drops significantly; when the face database data is not updated in time or the data collection quality is not high, "false alarms" and "missed reports" are also prone to occur, which in turn affects the fairness of law enforcement. In addition, for behavior recognition systems, complex human behavior patterns are highly ambiguous, and the boundaries between different actions are difficult to clearly define. If there are deviations in algorithm training, ordinary behaviors may be "labeled", increasing the frequency of unnecessary law enforcement intervention and causing misjudgment problems.

4.1.2. Big data and algorithm analysis

4.1.2.1. Automatic generation of case clues and predictive policing

Big data and algorithm analysis have shown strong case prediction and clue generation capabilities in criminal investigations. Public security organs use AI algorithms to conduct deep learning and statistical analysis of historical case data by accessing multi-dimensional data sources from network platforms, banking systems, communication operators, video surveillance systems, etc., to identify potential crime patterns, time nodes and high-incidence areas, and generate predictive reports such as "high-risk area maps" or "high-frequency crime time periods", thereby realizing "predictive policing".

This technology is particularly suitable for combating serial crimes, telecommunications fraud, cybercrime and other case types with obvious data characteristics. For example, by modeling the time, area, and content of historical fraud calls, the fraud-related communication number segments can be locked in advance; for serial theft cases, the possible next target area can be analyzed through the path trajectory and modus operandi to achieve pre-emptive prevention and control.

4.1.2.2. Social relationship map and suspect portrait

AI systems are also used to construct social relationship maps and behavioral portraits of criminal suspects to assist investigators in accurately analyzing their activity patterns and potential accomplices. By integrating data such as suspects' communication records, traffic trajectories, financial transactions, and social media activities, the system can automatically draw a "social network map" to reveal the degree of connection and frequency of interaction between suspects and other persons involved in the case. Such technologies play an important role in combating mafia organizations and cross-regional criminal gangs, helping to expand from the "point" of the case to the "surface" of the organization and achieve a three-dimensional crackdown.

However, big data analysis relies on algorithm parameter settings and data input quality when processing unstructured data. If there is a lack of accurate labeling and review mechanisms, it may lead to distorted association inferences and mistakenly lock innocent objects. Therefore, clear standards still need to be established in data collection, model training, and explainable algorithms to balance the relationship between technical efficiency and legal prudence.

4.1.3. Speech recognition and natural language processing technology

Auxiliary functions of communication monitoring, speech transcription, and intelligent interrogation systems

In criminal investigations, speech recognition and natural language processing (NLP) technologies are widely used in work scenarios such as communication monitoring, on-site speech recognition, conversation content transcription, and semantic analysis. For example, law enforcement agencies can monitor the phone calls of people involved in the case through authorization, and use AI speech recognition systems to automatically transcribe the recordings, thereby quickly locating key information, keywords, and suspicious behaviors, reducing the time cost of manual monitoring.

In addition, some local public security organs have begun to pilot the deployment of "intelligent interrogation systems", combining speech recognition with NLP technology to identify the confession content of suspects in real time, and compare semantic associations with case databases to assist interrogators in judging the authenticity, logical consistency, and even possible psychological state of the confession content. For example, if the suspect uses too much "ambiguous tone" or "evasive expression" or there is an abnormal pause in the voice waveform, the system will mark it as a "high-risk statement" and prompt the investigators to further question.

Although this technology helps improve interrogation efficiency, it still faces challenges such as dialect diversity, semantic ambiguity, and context jumps in language semantic recognition, which may lead to recognition bias. In addition, the extent of AI intervention and the scope of acceptance in intelligent interrogation also need to clarify the legal boundaries and evidence exclusion rules to prevent the abuse of technology.

4.1.4. Drones and intelligent patrol systems

Extension of non-contact investigation methods and enhancement of control capabilities

As an emerging aerial investigation tool, drone systems have demonstrated powerful functions in crime scene investigation, fugitive tracking, and key area control. AI-driven drones can not only take real-time photos from high altitudes, but also carry modules such as thermal imaging, infrared scanning, and face recognition to achieve target search and remote monitoring in complex terrains, especially in mountainous areas, woodlands, suburbs, and other areas that are difficult for conventional police forces to cover.

At the same time, ground intelligent patrol robots are also being piloted in some cities, which can automatically patrol routes, identify suspicious targets, broadcast warnings, and transmit real-time data to the command center during specific periods of time. This type of "intelligent sentinel" helps to release grassroots police forces and enhance night patrol coverage.

However, the large-scale deployment of drones and smart patrol equipment also brings a series of technical and legal issues: on the one hand, technical security needs to be strengthened, and there will be risks if the equipment is hacked or falls out of control; on the other hand, all-weather, all-round reconnaissance activities may constitute an infringement on the privacy boundaries of citizens, especially in the absence of clear legal authorization and procedural control, it is difficult to ensure the legality and appropriateness of the use of technology.

4.2. Main legal issues faced in the application of artificial intelligence

The rapid expansion of artificial intelligence technology in criminal investigation has shown unique advantages in improving the efficiency of solving cases, reducing the cost of investigation, and realizing dynamic supervision. However, at the same time, it has also caused many deep-seated legal issues. These problems are mainly manifested in the risk of infringement of individual rights, insufficient procedural legitimacy, potential distortion of substantive justice, and the lag of institutional gaps, which urgently need to be responded to from the legal, institutional and practical levels. The following will analyze four major legal issues:

4.2.1. Infringement of personal privacy and data protection issues

4.2.1.1. Unauthorized collection and abuse issues

The core of artificial intelligence technology relies on the collection and processing of large amounts of data. Especially in the field of criminal investigation, investigative agencies often use facial recognition, voice monitoring, big data comparison and other means to obtain personal sensitive information such as biometrics, life trajectories, and communication records of persons involved in the case and potential suspects. However, in practice, the data collection link often lacks a clear legal authorization basis and procedural control mechanism, and there is a phenomenon of "collection without notification" and "processing without authorization", which can easily cause substantial infringement of citizens' privacy rights.

For example, in some cases, the police automatically collected facial data through public camera systems and compared it with the national public security database, without clearly distinguishing whether the target population was involved in the case and whether it constituted a legitimate reason for the collection. At the same time, there was a lack of strict use restrictions and de-identification of the collected data, resulting in the "secondary use" of information outside of case investigation or even commercial circulation, exacerbating the risk of privacy leakage.

4.2.1.2. Protection and use boundaries of citizen information

The "Civil Code", "Personal Information Protection Law", "Data Security Law" and other laws and regulations have made basic provisions for the legal handling of personal information, but in criminal investigations, the use of citizen information is often in the tension between "national security" and "personal privacy", with unclear boundaries and insufficient supervision. For example, the restrictive provisions on the exercise of investigative power in the "Criminal Procedure Law" are relatively principled, and no targeted constraints are made on specific collection methods in AI technology (such as remote monitoring, algorithm profiling, and relationship map modeling), resulting in the "gray area" of technology use becoming a hotbed for power expansion.

At the same time, citizens' rights to know, object and remedy regarding the collection, processing and use of their information lack effective protection, and it is almost impossible to question the decision of AI system in criminal proceedings, which also weakens the procedural basis of privacy protection.

4.2.2. Algorithmic bias and discrimination

4.2.2.1. Imbalance of algorithm training data and discriminatory consequences

The application of AI system in criminal investigation relies heavily on massive training data and model learning process. However, these training data are often constructed based on historical cases, past law enforcement records and even social prejudices, which can easily lead to structural bias in the output of the algorithm. For example, the predictive policing algorithms used by the early US police (such as the COMPAS system) tend to over-judge the risk of African-American groups in their scoring, resulting in “algorithmic reinforcement” of racial discrimination.

In China, because the data resources involved in the case are concentrated in specific regions, specific populations or specific types of cases, the algorithm may form a “high-risk label” for low-income groups, specific occupations or migrant populations during training, resulting in a shift and misleading of the focus of law enforcement. For example, the big data system may use "frequent late return", "multiple cross-provincial movements" and "low-frequency financial activities" as suspicion indicators, and then automatically label a certain group as "suspicious objects". This labeling thinking not only infringes on personal dignity, but is also likely to cause erroneous investigations and even wrongful convictions.

4.2.2.2. Procedural injustice caused by group labeling

The bias of the AI system is not only reflected at the individual level, but also creates group injustice at the structural level. Driven by algorithms, law enforcement agencies are prone to implement "preconceived" investigative tendencies against specific groups, so that some people are "procedurally labeled" before entering the litigation process, and lose the right to equal treatment that they should enjoy as ordinary citizens. Such risks seriously challenge modern criminal rule of law principles such as "presumption of innocence" and "individualized justice".

In addition, due to the "black box" nature and technical monopoly of algorithms, suspects and defense lawyers often find it difficult to obtain the logical path and data basis of the algorithm reasoning process, and lack substantive defense opportunities. This undermines procedural oversight and risks transforming AI decision-making into an unchallengeable exercise of authority.

4.2.3. Issues of the legality and admissibility of evidence

4.2.3.1. Issues of the subject eligibility of AI-generated evidence

In traditional criminal proceedings, evidence must be obtained by investigators with legal subject qualifications within the scope of legal authority. However, AI systems often assume the function of "active testimony" in criminal investigations, such as automatically generating "location matching" evidence between a suspect and the crime scene through an intelligent recognition system, and extracting "suspicious speech" as the basis for investigation through a voice analysis system. The question that arises at this time is: Does the AI system have the status of a "qualified subject" in the sense of criminal procedure law?

In addition, there is still great controversy over whether the evidence generated by AI meets the evidence standards of "legal source, proper procedure, stable form, and true content". For example, do automatically generated image recognition results, behavior judgment reports, semantic analysis inferences, etc. belong to the type of evidence that is "verifiable and verifiable"? Is the algorithmic logic in the process of evidence formation open and verifiable? These are directly related to the admissibility and probative force of evidence in court trials.

4.2.3.2. Evaluation of the legality and rationality of AI intervention in the investigation process

The involvement of AI technology in investigation is becoming increasingly profound, and some links have even achieved "dehumanization" operations (such as intelligent comparison without human intervention, automatic triggering of arrest mechanisms, etc.). However, according to the Criminal Procedure Law, investigation activities should be completed in person by state agency personnel with investigative powers, and there must be room for accountability and supervision in the process. The participation of AI systems often lacks a clear authorization basis, and the necessary procedural control mechanism is not set up, which makes it easy to break the boundaries of power exercise.

In addition, some intelligent systems lack the ability to judge the specific circumstances of the case, and may make investigative decisions that do not conform to the legal principles or proportionality principles due to the rigid setting of algorithm parameters. Therefore, a legality evaluation mechanism for AI intervention procedures should be established to clearly define its scope of application, applicable procedures, technical boundaries and supervision paths to prevent it from undermining the fairness of the case due to technical abuse.

4.2.4. Challenges of criminal procedural justice

4.2.4.1. The legality risk of AI replacing human judgment

Criminal investigation is essentially a process of judging "the identity, behavior and illegal nature of the suspect", which has a strong value judgment attribute. In this process, AI systems replace humans to complete core tasks such as clue analysis, behavior judgment, and evidence selection, which can easily weaken the sense of responsibility and judgment of law enforcement personnel, resulting in the problem of "technology dependence" or "responsibility shifting". Once a wrong judgment occurs, the investigative agency may blame the system's "misjudgment" rather than its own dereliction of duty, which directly shakes the legal responsibility mechanism for law enforcement behavior.

More importantly, criminal investigations need to comprehensively consider non-data factors such as circumstances, motives, and social background, while AI systems can only perform quantitative analysis based on limited parameters, making it difficult to achieve the prudence and empathy that human justice should have. Relying solely on AI and making judicial judgments technical and procedural will inevitably weaken the balance between procedural justice and humane law enforcement.

4.2.4.2. Impact on "procedural justice" and "substantive justice"

The widespread embedding of AI technology has improved the efficiency of case investigation and the rate of evidence discovery to a certain extent, but it may also pose a substantial threat to "procedural justice". In the process of evidence collection, suspect identification, and evidence presentation, if the AI system lacks openness and questionability, the procedure will be meaningless, and even if the substantive conclusion is correct, it will not be able to obtain procedural legitimacy support.

In addition, the core of procedural justice lies in "visible justice", and AI systems often operate in an incomprehensible way. The "inexplicability" of their algorithms and decision paths makes it difficult for the public to believe their conclusions, which seriously affects the credibility of the judiciary.

Therefore, in the context of the continuous development of AI technology, it is necessary to re-examine the trade-off between technical efficiency and procedural justice, avoid sacrificing procedural guarantees in the name of efficiency, and ensure that the application of AI always serves the basic principles of criminal rule of law.

4.3. Overseas regulatory experience

Globally, the application of artificial intelligence technology in criminal investigation is gradually becoming institutionalized and standardized. Developed countries in Europe and the United States, as well as countries with relatively mature legal systems such as Japan and Germany, have established a certain degree of legal constraints and procedural guarantee mechanisms in AI investigation practices, striving to find a balance between efficiency and rights protection. The regulatory experience of these countries or regions not only reflects the legal response to technological development, but also provides important reference for China to build a legal regulatory system for artificial intelligence investigation.

4.3.1. The United States: Review mechanism and case practice for the use of technology

4.3.1.1. Clearview AI case: warning of abuse of facial recognition technology

The United States started early in the application of AI investigation, especially in facial recognition technology, big data policing, predictive algorithms, etc. However, the privacy infringement and legal disputes brought about by its rapid technological development are also particularly significant. Among them, the most representative is the Clearview AI company incident.

Clearview AI has developed a powerful facial recognition engine that provides investigative support for US law enforcement agencies by capturing billions of facial images on social media. Although this technology has been used to quickly identify suspects in some criminal cases, it has also triggered large-scale lawsuits on issues such as "unauthorized capture", "unnotified use", and "information abuse". Several states (such as California and Illinois) have filed lawsuits against it under the Biometric Information Privacy Act (BIPA). The courts generally believe that facial recognition technology constitutes sensitive use of personal information and must obtain explicit consent from users in advance.

This case reflects that: on the one hand, US law restricts the abuse of technology through ex post judicial relief mechanisms; on the other hand, state legislation under its decentralized system has pre-regulated the "technical boundaries". This has important implications for China - while introducing new technologies, we should simultaneously promote the construction of legislation and relief mechanisms to prevent the legal vacuum of "use first and then rule".

4.3.1.2. The institutional checks and balances function of the exclusionary rule

The "exclusionary rule" in US criminal proceedings provides a key procedural constraint for limiting AI's involvement in investigations. In classic cases such as Miranda v. Arizona, the Supreme Court emphasized that evidence obtained without procedural legitimacy cannot be used in court. This principle also applies to the field of AI investigation evidence.

For example, in some state cases, if the police obtain clues through an unauthorized automatic facial recognition system and further conduct a search, the court will consider whether the technology violates the "prohibition of unreasonable searches" principle in the Fourth Amendment. If it is determined to be an illegal search, the subsequent evidence obtained will also be excluded. This mechanism has established an important counter-logical logic for technical investigation power in practice, which helps prevent the unlimited expansion of AI means under the unsupervised power.

4.3.2. EU: Regulation of AI use under the background of GDPR

4.3.2.1. Institutional design of data protection and "right to be forgotten"

The EU is known for its strict legislation on personal information protection. The General Data Protection Regulation (GDPR), which officially came into effect in 2018, has set a high standard for the legal and compliant use of AI technology around the world. GDPR not only stipulates core rules such as "data minimization", "purpose limitation" and "legality principle", but also enhances individuals' control over their own information through systems such as "right to be forgotten" and "data portability".

In the field of AI investigation, this means that if law enforcement agencies use technologies such as facial recognition and voice analysis, they must ensure the legality of the collection process, the clarity of the data use, and accept the review of independent supervisory agencies (such as data protection commissioners). If the data subject raises an objection or finds that the data is misused, he or she has the right to request deletion, restriction of processing or lodge a complaint.

GDPR has set clear boundaries for AI technology through the institutionalized "informed consent-restriction-relief" process, and particularly emphasizes the priority of personal dignity and privacy rights. When building a regulatory mechanism for AI investigation technology, China should draw on the "rights-dominated" design concept in its data protection system and establish a multi-dimensional personal information rights protection system.

4.3.2.2. Draft of the European Union Artificial Intelligence Act

In 2021, the European Commission issued the "Draft Artificial Intelligence Act", marking the launch of the world's first special legislation to systematically regulate AI technology. The bill is centered on the principle of "risk orientation" and divides AI systems into four categories: "unacceptable risk", "high risk", "limited risk" and "minimum risk", and puts forward strict access and transparency requirements for high-risk AI systems (such as facial recognition and behavior prediction).

In the field of criminal investigation, the draft AI bill explicitly restricts the use of "real-time remote face recognition systems", allowing them to be implemented only under conditions such as "specific authorization", "public interest" and "court control", and requires all usage records to be subject to independent supervision. This practice reflects the institutional design of a balance mechanism between national security and human rights protection.

The draft also requires that all high-risk AI systems must have "explainability", "human controllability" and "data audit mechanism" to ensure that the system output has legal legitimacy and error correction mechanism. This provides a model for the design of China's future AI legal regulatory system: that is, not only to be based on data compliance, but also to achieve algorithm supervision, responsibility traceability and process auditability.

4.3.3. Japan and Germany: Institutional coordination between police technology and investigative procedures

4.3.3.1. Japan: Technology use relies on "prior permission" and "procedural review"

Japan is more cautious in the application of AI technology, especially in criminal investigations. Its legal system emphasizes the procedural legitimacy of police behavior and the judicial review mechanism. According to the relevant provisions of the Criminal Procedure Law and the Police Law, the police must obtain a warrant issued by the court and provide detailed descriptions of the collection behavior before using large-scale monitoring, listening equipment or biometric systems.

In addition, Japan's public security agencies have introduced an "expert review mechanism" to conduct ethical and legal feasibility assessments on the deployment of new technology systems, emphasizing that the technology system should ensure "minimum infringement of citizens' basic rights." This system effectively avoids the "regulatory lag" problem caused by the rapid application of technology and ensures that police technology behavior is always within the framework of the rule of law.

4.3.3.2. Germany: Emphasis on the clarity of legal authorization and power supervision mechanism

As a continental legal country, Germany attaches great importance to the boundary between police power and technology use. The German Federal Data Protection Act, the Criminal Investigation Procedure Code and other laws clearly stipulate that the use of technical means must have "specific statutory authorization" and be subject to the "principle of proportionality", "principle of necessity" and "principle of minimum infringement".

In practice, the German Constitutional Court has repeatedly reviewed the constitutionality of technical means. For example, in the famous "online monitoring case", the court ruled that the state may not conduct automated monitoring of citizens' online behavior without explicit authorization, emphasizing that the state's technical behavior must be subject to effective supervision by the judiciary. In addition, Germany has established mechanisms such as the "Federal Commissioner for Freedom of Information" and the "Data Protection Officer" to achieve external supervision and public accountability of police technical behavior, effectively ensuring that procedural fairness and basic rights are not eroded by technology.

5.Suggestion for Path to Building a Legal Regulatory System for Criminal Investigation of Artificial Intelligence

With the continuous deepening of the application of artificial intelligence in criminal investigation, its advantages in improving investigation efficiency and expanding investigation capabilities have become increasingly prominent. But at the same time, the lagging problem of the relevant legal system has become increasingly prominent. How to strike a balance between technological innovation and legal governance, both to ensure the effective exercise of the state's criminal judicial power and to protect the basic rights of citizens from being abused by technology, is an important issue that China urgently needs to solve. This chapter will propose a specific path to building a legal regulatory system for criminal investigation of artificial intelligence in China from four dimensions: setting legal boundaries, protecting personal data, improving evidence rules, and building a supervision mechanism.

5.1 Clarify the legal boundaries of technology application

5.1.1. Clearly stipulate the types of cases and procedural links to which AI can be applied in legislation

At present, China has not yet made a clear legal definition of the involvement of artificial intelligence in criminal investigation activities, resulting in the risk of generalization and expansion of the use of technology in practice. To this end, the scope of application, case types and procedural links of artificial intelligence technology in criminal investigations should be clarified through the formulation or revision of legal documents such as the Criminal Procedure Law, the People's Police Law, the Data Security Law, and the Artificial Intelligence Law (Draft), and the legal boundaries of "what can be done", "what cannot be done" and "what should be reviewed" should be defined.

For example, it can be clearly stipulated that highly sensitive AI methods such as facial recognition and predictive analysis can only be used in specific serious criminal cases, under court authorization or prosecutorial supervision. At the same time, the investigation link involving technology should be limited to auxiliary procedures such as "clue acquisition", "suspect portrait" and "intelligence analysis", rather than replacing substantive judgments or replacing the subjective judgments of investigators.

5.1.2. Establish the application standards of the "proportional principle" and the "minimum infringement principle"

Referring to other countries experience, China should incorporate the "proportional principle" and the "minimum infringement principle" into the legal application standards for artificial intelligence criminal investigations as the basic principles for measuring the legality and legitimacy of technology use.

Specifically, when deciding whether to use AI technology, the investigative agency should comprehensively consider factors such as the degree of infringement of personal rights by technical means, the nature and severity of the case, whether there are alternative less infringing means available, and whether legal authorization has been obtained. For highly sensitive means such as big data dynamic tracking and face recognition, more stringent start-up conditions and approval procedures should be set to ensure that the use of technology does not exceed its necessity and rationality.

5.2. Strengthen the protection mechanism for personal data

5.2.1. Introduce the principle of technical transparency and the mechanism of information use traceability

The essence of artificial intelligence criminal investigation technology is the extensive processing and in-depth mining of data, so a systematic data protection mechanism must be established. First of all, the "principle of technical transparency" should be established in legislation, requiring that any AI system used in criminal investigation must have a technical structure with verifiable data sources, explainable processing processes, and recordable operating behaviors. At the same time, the "information use traceability mechanism" should be introduced to achieve a full-chain record of each data call, analysis, storage and sharing, which is convenient for post-event review and responsibility tracing.

This move not only helps to protect citizens' right to know and right to object to the use of their own data, but also encourages law enforcement personnel to use technology in accordance with laws and regulations to reduce the risk of abuse.

5.2.2. Build a citizen-centered data use consent mechanism

In non-emergency situations, we should promote the establishment of a citizen-centered data authorization mechanism. In particular, for biometric information such as images, voiceprints, and locations of people not involved in the case, informed consent should be obtained in advance, and individuals should be allowed to object to the collection of information or request deletion. For data collected in public security video surveillance systems, their purpose of use, storage time, and access rights should also be clearly defined.

At the same time, industry supervision and judicial supervision of AI data collection should be strengthened, and an "information rights complaint channel" should be established to ensure that citizens have effective remedies when they find that their data is used illegally.

5.3. Improve evidence rules and procedural guarantees

5.3.1. Clarify the admissibility standards and certification process of AI-generated evidence

As AI technology is widely used in investigation links such as suspect positioning, scene restoration, and audio and video analysis, the information it generates will inevitably enter the judicial trial process and become the basis for the final decision. At this time, the admissibility of AI-generated evidence has become a core legal issue.

The current Criminal Procedure Law and Judicial Interpretation of the People's Court in China have not yet clarified the legal position of AI-generated data as criminal evidence. Therefore, it is urgent to clarify its nature of evidence, the standard for evaluating the probative force and the process of legality certification from the level of legislation and judicial interpretation.

Specifically, the following systems can be established:

Technical source review system: All AI-generated evidence must be accompanied by software source description, algorithm description and equipment registration information.

Verifiability mechanism: Ensure the originality, integrity and reproducibility of evidence, and avoid tampering and falsification in the middle.

Expert assisted evaluation mechanism: Third-party technical experts independently evaluate the reliability of AI evidence and issue professional reports.

5.3.2. Introduce the principles of "algorithmic explainability" and "human final decision-making responsibility"

The process of AI participating in investigation should not completely replace human judgment, otherwise it is very easy to lead to the lack of procedural justice. To this end, the "algorithmic explainability principle" should be established in the system, requiring all AI models used in criminal investigation to explain their logical paths and reasoning basis, so as to avoid "black box decision-making" from becoming a judicial reference.

At the same time, the "principle of human ultimate decision-making responsibility" should be clarified, that is, no matter how detailed the clues and judgments provided by AI technology are, the final legal judgment and procedural advancement responsibility should still be borne by investigators and judicial personnel. AI is only an auxiliary tool and cannot independently lead the case process. This principle not only helps to ensure the traceability of judicial responsibility, but also meets the fundamental requirements of procedural justice.

5.4. Establish an independent supervision and review mechanism

5.4.1. Set up a technical ethics committee and an expert review group

A special "artificial intelligence technology ethics review committee" or "AI technology legal risk assessment expert group" should be established in public security organs, procuratorates and national judicial institutions to conduct prior review and post-evaluation of AI systems to be put into the field of investigation.

The members of the committee should include a diverse group of legal experts, technical experts, ethicists, data protection officers, etc., to conduct a comprehensive review of the legality, rationality, data sources, potential biases and other aspects of AI technology, and put forward feasibility reports and regulatory recommendations.

5.4.2. Introduce a check and balance mechanism of multiple subjects (lawyers, technicians, judges)

The compliance operation of AI investigative means not only relies on technical supervision mechanisms, but also requires procedural supervision through checks and balances between legal professional groups. In the case, defense lawyers should have the right to question AI technology evidence and review algorithms; technicians should provide professional analysis as a neutral third party; and judges should be responsible for substantive review of the admissibility of AI evidence.

In addition, courts and procuratorates should be encouraged to set up "AI evidence special review teams" to train judicial personnel with technical backgrounds so that they can understand and judge the formation process and legal effect of AI evidence. Through the linkage of the three parties, closed-loop supervision of the legal use of AI technology can be achieved to prevent technical means from becoming a tool to cover up the abuse of power.

References

[1] Chen, X.L. (2021). Artificial intelligence and new challenges of criminal law. Journal of Legal Studies, 43(1), 3–20. https://doi.org/10.15994/j.cnki.1001-2397.2021.01.001.

[2] Zhou Guangquan. (2019). The legal boundary of artificial intelligence-assisted investigation. China Legal Science, (4), 39–57. https://doi.org/10.19387/j.cnki.1005-0221.2019.04.004.

[3] Ouyang Wu. (2022). Algorithmic bias and criminal justice: procedural rights protection in the era of artificial intelligence. Modern Jurisprudence, 44(3), 123–137. https://doi.org/10.16292/j.cnki.1003-8981.2022.03.009

[4] Yang Jianshun. (2021). Facial recognition technology and protection of personal rights. Legal Science (Journal of Northwest University of Political Science and Law), 39(1), 38–51. https://doi.org/10.13868/j.cnki.issn1008-6850.2021.01.004

[5] Wu Shenkuo. (2020). An analysis of China's legislative path for artificial intelligence. Tsinghua Law Review, 14(2), 118–134. https://doi.org/10.14138/j.1005-3126.2020.02.007

[6] Liu Pinxin. (2021). Legal regulation of face recognition from the perspective of the Personal Information Protection Law. Electronic Intellectual Property, (12), 16–24. https://doi.org/10.19331/j.cnki.epub.2021.12.003

[7] European Commission. (2021). Proposal for a Regulation laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206

[8] Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the General Data Protection Regulation. International Data Privacy Law, 7(2), 76–99. https://doi.org/10.1093/idpl/ipx005

[9] Ferguson, A. G. (2017). The rise of big data policing: Surveillance, race, and the future of law enforcement. NYU Press. https://doi.org/10.18574/nyu/9781479892822.001.0001

[10] Pasquale, F. (2015). The black box society: The secret algorithms that control money and information. Harvard University Press. https://doi.org/10.4159/harvard.9780674915665

[11] Zuboff, S. (2019). The age of surveillance capitalism. PublicAffairs. https://doi.org/10.1002/asi.24163

[12] Selbst, A. D., & Barocas, S. (2018). The intuitive appeal of explainable machines. Fordham Law Review, 87(3), 1085–1139. https://ir.lawnet.fordham.edu/flr/vol87/iss3/3

[13] Citron, D. K., & Pasquale, F. (2014). The scored society: Due process for automated predictions. Washington Law Review, 89(1), 1–33. https://digitalcommons.law.uw.edu/wlr/vol89/iss1/1

[14] Sunstein, C. R. (2020). Too much information: Understanding what you don’t want to know. MIT Press. https://doi.org/10.7551/mitpress/11617.001.0001

[15] Yeung, K. (2018). A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework. Council of Europe Expert Paper. https://rm.coe.int/algorithms-and-human-rights-en-rev/1680796d10

[16] National People's Congress of the People's Republic of China. (2021). "Personal Information Protection Law of the People's Republic of China".

https://www.npc.gov.cn/npc/c30834/202111/b1f8e316ccfb4ed1a4228f4c95fc01c1.shtml

[17] Cyberspace Administration of China. (2022). "Regulations on Algorithm Recommendation Management". https://www.cac.gov.cn/2022-01/04/c_1642894604767300.htm

[18] Wang Liming. (2021). The balance between technology regulation and rights protection - On the legal approach to algorithm governance. Law and Business Research, 38(6), 5–18. https://doi.org/10.19404/j.cnki.1000-4203.2021.06.001