The Application of Artificial Intelligence in the Process of Intelligent Criminal Justice: From the Perspective of Cross-Border Data Governance

Xiqiao Tong
Law and Politics Department, North China Electric Power University, Baoding, Hebei, China

Keywords: Artificial Intelligence, Cross Border Data Governance, Criminal Justice, Algorithmic Ethics, International Rules.

Abstract: In the context of global digital transformation, artificial intelligence technology is gradually being widely applied by criminal justice institutions in various countries. While facilitating the law enforcement process of domestic and international criminal justice, it also reconstructs the practical paradigm of transnational crime investigation. However, its application in criminal investigation still faces certain institutional imperfections, as well as numerous legal and ethical issues. This article aims to explore how artificial intelligence can be correctly applied to the investigation of criminal cases from the perspective of cross-border data governance, ensuring its legality, fairness, and effectiveness. Research has found that there is a certain lag in the current WTO rules; Fragmentation of regional agreements increases the cost of judicial cooperation; Algorithm bias poses a certain risk of misjudgement. Propose innovative paths such as establishing a data classification system and creating an international AI investigation compliance committee.

1 INTRODUCTION

With the rapid development of artificial intelligence technology, it is increasingly widely used in criminal case investigation, especially in data analysis, evidence collection, and suspect identification. Artificial intelligence is changing the traditional mode of criminal investigation. However, this technological innovation has also brought new challenges, and the application of artificial intelligence in criminal investigation faces many legal and ethical issues(Li,2020; Zhang,2021；Joseph,2024).

At the same time, the rules for cross-border data flow affect the sharing and cooperation of transnational criminal data, and the limitations, biases, and privacy protection principles of algorithms pose higher requirements for the design and application of artificial intelligence algorithms (Dai,2023; Re, & Solow-Niederman,2019).

In addition, the principle of fair trade also requires countries to maintain fair competition in the research and application of artificial intelligence technology, avoiding technological monopolies and unfair competition.

This article adopts case analysis, comparative research, and literature research methods to explore how artificial intelligence can be correctly applied to the investigation of criminal cases from the perspective of cross-border data governance, ensuring its legality, fairness, and effectiveness. Firstly, by analyzing the main application scenarios of artificial intelligence in criminal investigation, we explore the efficiency improvement and potential risks it brings; Secondly, study the regulatory blind spots of laws in cross-border data flow, privacy protection, algorithmic fairness, and the dynamic balance of diverse value objectives; Finally, explore how to promote the healthy development of artificial intelligence in the field of criminal investigation while ensuring security and privacy.

Tong, X.
The Application of Artificial Intelligence in the Process of Intelligent Criminal Justice: From the Perspective of Cross-Border Data Governance.
DOI: 10.5220/0014384300004859

In *Proceedings of the 1st International Conference on Politics, Law, and Social Science (ICPLSS 2025)*, pages 448-453
ISBN: 978-989-758-785-6

2 THE CURRENT APPLICATION STATUS OF AI IN CRIMINAL INVESTIGATION

2.1 Typical Application Scenarios

2.1.1 Cross Border Crime Warning

With the development of technology, police work has gradually shifted from combating crime to focusing on crime prevention. Therefore, determining which type of person is a potential criminal before a crime occurs is called crime warning (Blount, 2024). AI integrates global data sources such as international flights, hotel stays, and financial transactions, combined with technologies such as facial recognition and voiceprint comparison, to track the biometric trajectory of suspects in real time. For example, the Deep Seek platform covers a data network of over 200 countries and can predict the hiding preferences of fugitives, such as in Chinese communities or remote areas. Machine learning models can also analyze historical cases, construct behavioral profiles of fugitives, and provide early warning of potential criminal pathways.

Meanwhile, by utilizing blockchain analysis and cross-border payment network monitoring, AI can track the hidden asset paths of virtual currencies, offshore companies, and other entities. For example, using on-chain transaction graph analysis tools to trace the money laundering behavior of privacy coins such as Monero, and even crack anonymous identities on the dark web.

In addition, AI can also perform sentiment analysis and topic mining on social media content to identify criminal threats. For example, extracting geographical location clues from the dialect accent or street view information in the background of short videos to assist in locating suspects.

2.1.2 Collection of Electronic Evidence

AI can process large amounts of text, images, audio and video data, extract key information, and classify them (Barbir & Stankovic,2024). For example, natural language processing (NLP) technology analyzes chat records and email content, while image recognition technology restores crime scenes or identifies malware features. Multimodal models can also mine hidden evidence from unstructured data, such as encrypted files and deleted records.

At the same time, AI can construct personnel relationship graphs, transaction networks, or time-series logs through association analysis to discover criminal patterns. For example, analyzing variables such as customer education level and debt ratio in loan fraud cases to identify risk points. Blockchain technology ensures the integrity and immutability of electronic evidence.

In addition, AI models such as Deep Seeker R1 can automatically generate case summaries, extract elements such as involved personnel and fund flows, and support parallel analysis of similar cases.

2.1.3 Judicial Cooperation

Intelligent systems (such as the artificial intelligence-assisted trial system launched by Shenzhen Court) unify the judgment scale, provide case recommendations and sentencing recommendations, and reduce the deviation of discretionary power. For example, by analyzing key case data comprehensively and generating judicial recommendations to assist in social governance.

China and the "Belt and Road" countries have combined satellite maps and other intelligent means to solve the problem of monitoring blind areas. At the same time, we will promote multilateral data security cooperation mechanisms and promote the unification of international judicial standards.

2.2 Focus on Legal Disputes

2.2.1 Data Sovereignty Conflict Issues

In cross-border criminal investigation, AI relies on multi-source data such as biometric features, financial transaction chains, and communication records, which often involve data sovereignty disputes in different jurisdictions. For example, the localization requirement of the EU GDPR, which requires that member states' data should not be transferred across borders to countries that have not passed the adequacy determination, has led to the need for Chinese AI systems to establish localized data centers in EU law enforcement cooperation, but may be questioned for data sovereignty transfer. In addition, the United States unilaterally requires companies to provide overseas storage data through the Cloud Act, which directly conflicts with the European Union's Data Governance Act and forces cross-border criminal investigation cooperation into a trade-off between sovereignty first and technical efficiency.

There is a clear divergence in the positions of China, the United States, and Europe regarding the flow of cross-border data. China advocates data sovereignty priority, that is, cross-border data flow needs to be approved by the source country, and the

localized AI governance template should be promoted through the Belt and Road countries. The EU, on the other hand, emphasizes compliance barriers, which require AI system design stages to embed data protection mechanisms (such as Article 35 of GDPR), leading non-EU technology suppliers to restructure their algorithm architectures to comply with European Standards. In addition, the United States places greater emphasis on the technology neutrality strategy, which involves restricting technology exports to China through the Chip and Science Act, while promoting the formation of a data flow alliance among allies.

The conflict between Article 8 of the European Convention on human rights (Privacy Issues) and AI criminal investigation technology is prominent. AI can invade cloud data through dark network cracking, blockchain traceability and other technologies. The traditional physical privacy boundary is invalid. The European Court of human rights requires judicial authorization in advance, but the real-time requirements of cross-border forensics make it difficult to guarantee procedural compliance, which leads to the fuzziness of digital residences. At the same time, there are also difficulties in the review of the legitimacy of evidence. For example, when the U.S. police use AI to generate a crime report, if the data comes from a third country server, the defendant often questions the validity of evidence by violating the data sovereignty law, causing a crisis of mutual trust in international justice.

2.2.2 Algorithm Discrimination Risk

Taking the controversy of predictive policing in the United States as an example, the algorithm of historical arrest data training (such as predpol) marks the black community as a high-risk area, resulting in excessive deployment of police force and screening discrimination. Research conducted by the Massachusetts Institute of Technology and the National Institute of Standards and Technology (NIST) shows that many face recognition technologies in the United States have poor recognition accuracy for people of color. At the same time, many black people have encountered algorithmic discrimination.

First, the application of AI in criminal investigation will lead to the failure of transparency mechanism. In some cases, the AI supplier will refuse to disclose the algorithm logic on the grounds of trade secret, which makes the defendant unable to effectively cross-examine; The EU AI Act requires algorithm interpretability, but technology companies use zero knowledge proof and other tools to avoid it, which essentially forms pseudo transparency.

In addition, there is a vacuum in the attribution of responsibility. When AI decisions lead to false arrest (such as the case of Robert Williams, a black man in Detroit), the police will blame the algorithm defect, while the developer invokes the user agreement exemption clause, which forms a double responsibility escape.

Regional governance attempts, such as the new artificial intelligence act of the European Union, which prohibits high-risk algorithms, but the legislation of various states in the United States is uneven (for example, California prohibits police face recognition, while Texas encourages the use), leading to the problem of compliance puzzle for multinational enterprises.

At the same time, developing countries are still dependent on technology. Due to backward technology and insufficient innovation, some countries' data services are difficult to have a foothold in the market. In the long run, developed countries almost take over the data services of some countries, and the local bias of their algorithms is questioned, which has the risk of penetrating into the data of other countries, thus triggering the controversy of digital colonization.

3 RULE DILEMMA OF CROSS BORDER DATA GOVERNANCE

3.1 Defects in the Current Rule System

3.1.1 Lag of WTO Rules

The cross-border data governance rules under the WTO framework still adhere to the traditional consensus decision-making mechanism, which cannot adapt to the rapid development of the digital economy. This mechanism is inefficient in updating rules and cannot meet the real-time needs of cross-border data flow.

In addition, the existing WTO rules (such as the general agreement on trade in services) do not explicitly cover the specific standards of data cross-border flow, and the dispute settlement body (DSB) lacks the legal basis for handling digital trade disputes. For example, the conflict between data privacy protection and trade liberalization between the United States and the European Union is difficult to be resolved through WTO judicial channels due to the lack of uniform substantive rules. The WTO dispute settlement mechanism focuses more on

traditional trade disputes in goods and lacks explanatory power on new issues such as data sovereignty and algorithm transparency.

3.1.2 Extraterritorial Expansion of Domestic Laws

The United States has implemented extraterritorial jurisdiction through the cloud act and the chip and Science Act, requiring enterprises to provide overseas storage data, and even including Chinese technology enterprises in the entity list to restrict technology exports. Such unilateral measures lead to direct conflicts with other countries' data sovereignty. For example, after the European Court overturned the safe harbor agreement, the EU built data flow barriers through the general data protection regulations (GDPR), forming a rule hedge.

In addition, countries have expanded data cross-border regulation on the grounds of national security, such as India's ban on Chinese applications and the United States' exclusion of Huawei's equipment with the clean network plan. Such measures are often questioned as digital protectionism. For example, the adequacy determination mechanism of the EU GDPR has been criticized as a disguised data flow barrier, leading to a surge in compliance costs for enterprises.

The extraterritorial expansion of domestic laws will also trigger transnational legal confrontation. Typical cases include the United States' request to Canada to arrest Meng Wanzhou, a Huawei executive, and so on. Such conflicts are difficult to resolve due to the lack of international coordination mechanisms. For example, the multiple criteria for determining the connection points such as the place of data storage and the nationality of the processing subject exacerbate the jurisdictional disputes.

3.2 Core Contradiction Analysis

3.2.1 Contradiction Between Efficiency and Safety

There are contradictions between the free flow of data and localized storage. Cross-border data flow is the core driving force for the development of digital economy, but its natural boundlessness has fundamental conflicts with national security and personal privacy protection. For example, the European Union has established strict rules for cross-border transmission through the general data protection regulations (GDPR), requiring data receiving countries to pass adequacy identification to prove that their protection level is equivalent to that of the European Union (Voss, 2019). Although this mechanism strengthens the protection of privacy, it leads to high compliance costs for multinational enterprises (such as the establishment of local data centers), which hinders the efficiency of data flow. The United States adopted the cloud act to implement the data controller principle, allowing the government to access enterprise data across borders to improve law enforcement efficiency, but was criticized by the European Union as sacrificing the sovereignty of other countries with efficiency.

In addition, there is a symbiotic relationship between technological empowerment and security vulnerabilities. Although new technologies such as blockchain and privacy computing can enhance the credibility of cross-border data flow (such as "zero knowledge proof" to make data available and invisible), they may also be used to avoid sovereign regulations. For example, the anonymity of the dark net and cryptocurrency provides a channel for transnational crime, forcing countries to make a difficult trade-off between improving data tracking ability and protecting citizens' privacy. At the same time, the global layout of cloud computing services weakens the relevance between the physical storage place of data and jurisdiction, and the traditional territorial principle faces the risk of failure.

3.2.2 Conflict Between Technology and Sovereignty

At present, the core contradiction of cross-border data governance has evolved from a simple legal conflict to the competition between technical standards and rule systems. The United States has passed the chip and science act to restrict technology exports to China. At the same time, the United States has established a data flow alliance with its allies to turn technological advantages into the right to speak on rules; The construction of EU compliance barriers requires that the privacy protection mechanism be embedded in the AI system design stage, forcing non-EU enterprises to restructure their technical architecture to meet European standards; China's promotion of localized data governance templates through the belt and road initiative has been questioned as digital rule output (Ozalp et al.,2022；Luo& Van Assche,2023).

In addition, developed countries rely on their technological advantages to form a data gravity effect, leading to the passivity of developing countries. At the same time, the output of algorithm bias is also a serious problem, which is easy to cause the controversy of digital colonization.

4 IMPROVEMENT PATH OF CROSS BORDER DATA GOVERNANCE

4.1 Rule Innovation

4.1.1 Establish Investigation Data Classification System

In cross-border data governance, it is necessary to implement classified and hierarchical management according to data sensitivity. For example, DNA, Biometrics and other core data related to personal privacy or national security should be strictly prohibited from cross-border flow, while low-risk data such as IP addresses and public transaction records can be conditionally shared through the negotiation mechanism. China's data security law has put forward a hierarchical framework of core data - important data - General data, which can be further refined to specific scenarios, such as distinguishing terrorism related and classified data from ordinary case clue data in investigation data and clarifying cross-border transmission rules at different levels.

4.1.2 Developing International Standards for AI Investigation

For the application of AI in criminal investigation, it is necessary to promote the unification of international technical standards. For example, the EU AI Act requires that high-risk algorithms need to be embedded with interpretability and privacy protection mechanisms, while China can work with BRICs countries to develop AI Investigation Technical specifications that take into account efficiency and security, covering data desensitization, algorithm transparency, evidence chain traceability and other dimensions. The principle of human rights centrism proposed by UNESCO can also provide an ethical framework for global AI investigation standards.

4.2 Mechanism Construction

4.2.1 Establishment of International Ai Investigation Compliance Committee

Establish a multilateral institution composed of sovereign states and technical legal scholars to review the compliance of the AI investigation system. For example, the risk of racial discrimination in predictive policing algorithms and the legitimacy of cross-border data call procedures are dynamically evaluated, and innovative technology applications are piloted through the regulatory sandbox mechanism.

4.2.2 Pilot Cross-Border Counter-Terrorism Intelligence Exchange

The Sino Russian "border defense cooperation-2024" joint anti-terrorism exercise has practiced the cross-border intelligence sharing mechanism and realized real-time data collaboration through technical means such as air reconnaissance and water interception. In the future, such models can be promoted, and Regional Anti-Terrorism data exchange platforms can be established under the frameworks of ASEAN and the Shanghai Cooperation Organization to clarify the scope of shared data (such as encrypted communication metadata), authority (such as judicial authorization) and dispute resolution rules.

4.3 China's Coping Strategies

4.3.1 Actively Participate in the Formulation of International Rules

China needs to promote the concept of safe and orderly flow of data into international agreements such as CPTPP and DEPA on the basis of the global cross border data flow Cooperation Initiative. For example, the "negative list+security assessment system" was piloted by RCEP to allow the free flow of data that does not involve national security. At the same time, the provisions on personal information protection were improved against the EU GDPR to enhance the compatibility of rules.

4.3.2 Improving Domestic Support Systems

China has refined the enforcement rules of the data security law and the personal information protection law for domestic demand, such as establishing a "dynamic database for data exit security assessment" and relying on blockchain technology to achieve the full life cycle of cross-border data storage. At the same time, we should cultivate professional cross-border data service institutions, provide one-stop support for enterprises such as compliance consulting and risk assessment, and reduce the cost of going to sea compliance. At the technical level, we will increase investment in research and development of technologies such as privacy computing and homomorphic encryption and build an independent and controllable infrastructure for cross-border data flow.

5 CONCLUSION

AI investigation has become an inevitable choice to improve the efficiency of criminal justice through crime prediction, evidence correlation, risk early warning and other technical means. However, the cross-border data flows it relies on (such as biometrics and communication records) fundamentally conflict with the existing international rules: the localization requirements of the EU GDPR, the extraterritorial jurisdiction of the US cloud act and the data sovereignty demands of developing countries form a structural contradiction. Data shows that 80% of the world's data is stored on servers in the United States and Europe, and developing countries are in a passive position in the data value chain, highlighting the urgency of rule reconstruction.

In the future, rules need to be innovated, such as establishing the classification system of investigation data (such as the prohibition of cross-border DNA data and conditional sharing of IP addresses) and the international standard of AI investigation, promoting the mutual recognition of algorithm transparency (such as the interpretability requirements of the EU AI act) and data desensitization technology, and reducing technical barriers.

Carry out relevant mechanism construction, such as the establishment of the International Ai investigation compliance committee, relying on the UN framework to review the risk of algorithm discrimination, and pilot the regulatory sandbox to verify the technical compliance.

REFERENCES

Barbir, M. & Stankovic, B. 2024. Collecting and using electronic evidence in criminal proceedings. In Collection Papers from Conference Organized on Occasion Day Faculty of Law 326.

Blount, K. 2024. Using artificial intelligence to prevent crime: Implications for due process and criminal justice. AI & Society 39(1): 359-368.

Cohen, J.N. 2024. Adapting to AI: How will generative AI affect work? How should we respond? SocArXiv.

Dai, Y. 2023. Artificial intelligence regulation from the perspective of international trade law: From the perspective of WTO rules. Journal of Shanghai University of Finance and Economics 25(2): 122-136+152.

Li, H. 2020. The reform of criminal investigation work mode in the era of artificial intelligence. China Criminal Police (3): 9-12.

Luo, Y. & Van Assche, A. 2023. The rise of techno-geopolitical uncertainty: Implications of the United States CHIPS and Science Act. Journal of International Business Studies.

Ozalp, H. et al. 2022. “Digital colonization” of highly regulated industries: An analysis of big tech platforms’ entry into health care and education. California Management Review 64(4): 78-107.

Re, R.M. & Solow-Niederman, A. 2019. Developing artificially intelligent justice. Stanford Technology Law Review 22: 242.

Voss, W.G. 2019. Cross-border data flows, the GDPR, and data governance. Washington International Law Journal 29: 485.

Zhang, Z., Zhang, J. & Tan, T. 2021. Current situation analysis and countermeasures of artificial intelligence ethics. Journal of the Chinese Academy of Sciences 36(11): 1270-1277.