International Journal of Communication Networks and Information Security

ISSN: 2073-607X, 2076-0930

Volume 15 Issue 03 Year 2023

Analysis of the Role of Compliance Plan in AI Criminal Risk Prevention-Take AI Criminal Risk in Network Communication as Example

Bo Mou

Ph.D. Candidate, Faculty of Law, Krirk University, 10220, Thailand

mouboy1010@gmail.com

Xiaopei Yang*

Professor, Nanchang Vocational University, 330007, China

yangxiaopei13@gmail.com

Article History

Received: 1 November 2023
Revised: 15 November 2023
Accepted: 6 December 2023

Abstract

To address the criminal risks associated with artificial intelligence (AI) in network communications, such as privacy invasion, information leakage and abuse, prejudice and discrimination, and intelligent crime, it's crucial to implement robust compliance plans. These plans should ensure legal compliance by adhering to relevant laws and regulations, thus safeguarding against unlawful use of AI. Strengthening data privacy and protection is vital to prevent unauthorized access and misuse of sensitive information. Ensuring fairness and eliminating discrimination are essential to maintaining ethical AI practices and preventing biases in AI decision-making processes. Improving system transparency and interpretability is also critical; it involves making AI systems more understandable and accountable for their actions and decisions. Additionally, reinforcing security measures is necessary to defend against cyber threats and vulnerabilities, thereby reducing the probability of AI-enabled criminal activities. These comprehensive strategies are pivotal in mitigating the criminal risks of AI in network communication and promoting the responsible and ethical development of AI technology.

Keywords: Compliance Plan, Artificial Intelligence, Criminal Risk, Network Communication

1. Introduction

With the continuous progress of AI technology, there are more and more potential risks and challenges in the criminal fields [1,2], Such as the training of artificial intelligence system data may cause bias and imbalance, resulting in the decision results of the system being discriminatory. AI technology may be used to illegally monitor, manipulate, or attack, leading to criminal incidents. To reduce these risks, compliance plans are needed to address these issues.

Through the implementation of compliance plans in the AI criminal fields, AI systems can be required to provide interpretability of decisions, thus ensuring the fairness and rationality of decisions, and developers and operators can also be required to review and revise the training data to reduce the impact of bias and discrimination [3]. Criminal compliance can improve the credibility of enterprises, win the trust of customers, partners, and regulatory authorities, and thus enhance the advantages of enterprises in the market competition. It can protect the legitimate rights and interests of the enterprise, and the enterprise can follow criminal compliance, effectively prevent the illegal behavior of internal employees, and protect the legitimate rights and interests of the enterprise from being infringed. It can also promote corporate internal governance, improve employees' awareness of the rule of law, and form an excellent corporate culture. Corporate criminal compliance is conducive to safeguarding the social and public interests, reducing corruption and crime, promoting social fairness and justice, ensuring the legitimacy, fairness, and security of the artificial intelligence system, and then promoting the regular operation and development of the criminal justice system.

By digging deeper into the types of criminal risk in AI and the role of compliance plans, the types of AI criminal risk Analyze the compliance plan in terms of ensuring legal compliance, strengthening data privacy and protection, ensuring fairness and discrimination prevention, improving the transparency and interpretability of the system, and strengthening security and protection measures, To further reduce the occurrence probability of an AI criminal risk in network communication, Promote the sustainable development of AI technology in the fields of network communication, Ensure that AI systems are developed, deployed and used by legal, ethical and industry standards, Including but not limited to data privacy, fairness, transparency and responsibility.

2. Related Works

2.1 Risk of Data Bias and Discrimination

Data deviation refers to the unfair and uneven situation in data collection, collation, annotation, etc.[4], so that the data set only partially represents the diversity of the real world. For example, in AI criminal risk assessment, data bias occurs if training data datasets contain only group-specific personal information and criminal records while ignoring other groups. Such data bias may lead to errors in the judgment and prediction of some groups, which may further affect the lives and rights of individuals. Common types of bias are shown in Table 1 [5,6].

Table 1. Common Types of Data Bias

Deviation type	Description	Scale
Sampling deviation	The training dataset may not adequately represent samples of different ethnicities, genders, ages, and other groups	10%
Label deviation	Subjective factors may influence the labels in the training data	30%
Data collection bias	There may be preferences or limitations regarding sampling for data collection	60%

And the risk of discrimination. More emphasis should be placed on the discrimination and unfairness of some groups caused by data bias. In the criminal risk assessment [7], if a person's race, gender, age, and other factors are wrongly included in the algorithm, and the person's judgment result is high or low, it will bring unfair treatment and influence to the person. In this case, the judgment results of the AI system are not only inaccurate but also have the risk of discrimination against some groups [8,9].

2.2 Privacy and Data Security Risks

Privacy and data security risks refer to the threat to individuals, organizations, or society in a digital environment that may lead to privacy leakage, abuse of personal information, or data damage [10]. These risks may come from various sources. Data security risks mainly involve the integrity, availability, and confidentiality of the data. This includes data corruption, tampering, loss, and unauthorized access during data storage and transmission. Data security risks include network attacks, malware, ransomware, and other threats to the system and the network, which may lead to service interruption, data loss or tampering, system paralysis, and other serious consequences.

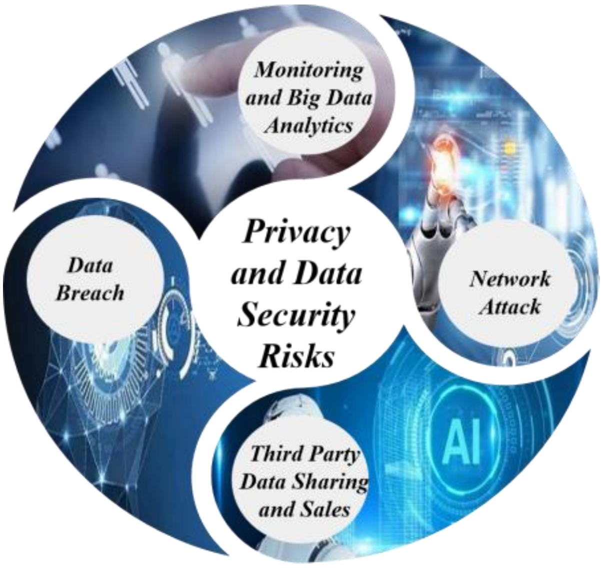
Monitoring and Big Data Analytics
Privacy and Data Security Risks
Data Breach
Network Attack
Third Party Data Sharing and Sales
AI

Figure 1. Privacy and Data Security Risk Types

Common types of privacy and data security risks are shown in Figure 1[11,12]. Among them, data leakage refers to disclosing sensitive information under unauthorized or unexpected circumstances. This can result in personal privacy invasion, financial loss, and damage to reputation of individuals or organizations. Identity theft involves someone impersonating another by obtaining personal information, leading to property damage, credit record issues, and various forms of fraud.

2.3 Explanative and Transparency Risks

Explaining Risk refers to the risk of lack of transparency and interpretability in the decision process or results of models in the application of machine learning and artificial intelligence algorithms[13]. This risk may cause users to understand why and how to make decisions, weakening their trust in the system and increasing the likelihood of misunderstanding, unfairness, or discrimination.

Transparency Risk involves the transparency of data collection and use [14]. Interpretative and transparency risks are partly associated with privacy and data security risks. On an algorithmic decision basis, users may question the way the data is used and the fairness of the algorithm. Lack of transparency and interpretability may cause problems such as racial and gender discrimination and lead to the risk of misuse or improper handling of personal information. Common types of explanatory and transparency risks are shown in Table 2 [15,16]. These risks may lead to user distrust and dissatisfaction with the system and may trigger social and ethical problems. Therefore, it is essential to ensure that the AI systems are explanatory, interpretable and transparent.

Table 2. Interpretive and Transparency Risk Types

Risk type	Description	Proportion
Black box decision	The decision-making process of some artificial intelligence systems is challenging to explain and understand, and users cannot know the basis of the decision and verify the rationality of the decision.	30%
Data deviation	The training data of the system may be biased, leading to misjudgments of specific groups or situations	15%
Lack of reliable explanatory and interpretability mechanism	In some cases, AI systems cannot provide a reliable explanation of the decision process, possibly due to technical limitations such as algorithm complexity and the large amount of data	30%
Mobility	The decision results of AI systems may produce inconsistent changes in different contexts, making users unable to predict the	25%

Risk type	Description	Proportion
	System's behavior and increasing the sense of uncertainty and distrust.	

3. Methodology

3.1 Compliance Plan Definition

A compliance plan refers to a series of norms and policies developed in AI applications to ensure legitimacy, fairness, transparency, and security. It aims to regulate the design, development, deployment, operation, and maintenance process of AI systems to ensure compliance with legal, regulatory, and ethical requirements while avoiding potential risks and challenges. Compliance plans can be applied to almost all areas and industries involved in AI technology, including data privacy protection, finance, healthcare, urban transportation, education, and more. By developing compliance plans, we can ensure the legitimacy, fairness, transparency, and security of AI systems, thus improving the credibility and social acceptance of the technology.

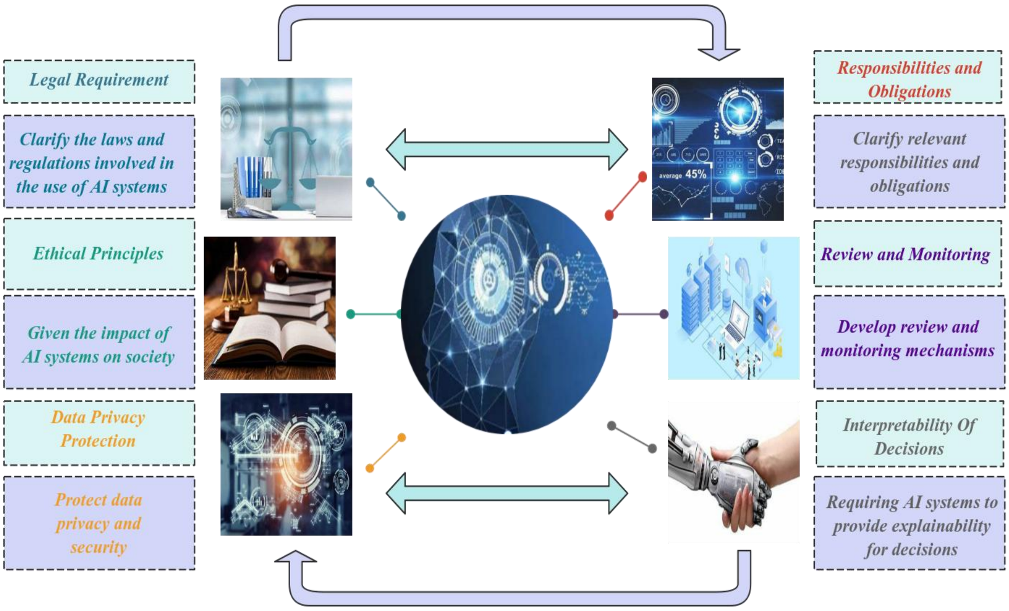
Legal Requirement
Clarify the laws and regulations involved in the use of AI systems
Ethical Principles
Given the impact of AI systems on society
Data Privacy Protection
Protect data privacy and security
Responsibilities and Obligations
Clarify relevant responsibilities and obligations
Review and Monitoring
Develop review and monitoring mechanisms
Interpretability Of Decisions
Requiring AI systems to provide explainability for decisions
average 45%

Figure 2. Compliance Plan Elements

However, the requirements should be met when developing the compliance plan, as shown in Figure 2 [17]-[19]. A compliance plan usually meets the six elements of legal requirements, ethical principles, data privacy protection, decision interpretability, review and monitoring, responsibilities and responsibilities and obligations.

Regarding legal requirements, the compliance plan should clarify the laws and regulations involved in using AI systems, such as data privacy Protection Law, Personal Information Protection Law, anti-discrimination Law, etc. In terms of ethical principles, compliance plans should take into account the impact of AI systems on society and follow moral and ethical principles, such as justice, equality, transparency, interpretability, etc. The compliance plan should specify how to collect, store, use, and share data and how to protect the privacy and security of the data. Regarding decision interpretability, the Compliance plan should require the AI system to provide the interpretability of decisions so that its results can be understood and evaluated, thus improving its fairness and rationality. The review and monitoring compliance plan should include review and monitoring mechanisms to ensure that AI systems comply with specified policies and requirements. Regarding responsibilities and obligations, the compliance plan shall specify relevant responsibilities and obligations, such as data management, data security, correctness of decision results, etc.

In addition, the content of the compliance plan can be adjusted and supplemented depending on the specific situation and the application area. It is essential to ensure that the compliance plan fully covers the design, development, deployment, operation, and maintenance process of the AI system, as well as to ensure the legitimacy, fairness, transparency, and security of the system.

3.2 Necessity to Introduce Compliance Plans into AI Criminal Risk

The academic circle has gradually recognized the problem of artificial intelligence crime and its serious harm. However, the single governance mode of traditional criminal law has lagged behind the prevention and control of artificial intelligence crime. As one of the means of corporate internal governance, the core goal of a criminal compliance plan is to avoid AI criminal risk by strengthening corporate internal governance and objectively realize the effect of preventing corporate crime through the formulation and implementation of a criminal compliance plan as the reduction of guilt, or even the basis of crime. In detail, professional compliance plans aimed at crime prevention are composed of a series of measures outside the law developed by the companies involved in crime prevention. The scope of these measures includes technical self-protection, the elimination of induced criminal systems, and the prevention of the system of internal corporate sanctions. From this level, the criminal compliance plan has the same crime prevention function as the criminal law.

3.2.1 Iterative Dissimilation of AI Crime Risk

With the network alienation of traditional crime and the rationalization of network crime, the crime alienation brought by artificial intelligence is more challenging to the traditional criminal law theory and criminal law rules. In artificial intelligence crime, the separation between human behavior and artificial intelligence decision-making makes the determination and assumption of criminal responsibility produce the fuzzy zone. As shown in Figure 3, on the whole, the alienation of AI crime risk is mainly reflected in the alienation of harmful behavior, the alienation of causality, the alienation of criminal responsibility, and the alienation of subjective crime [20,21].

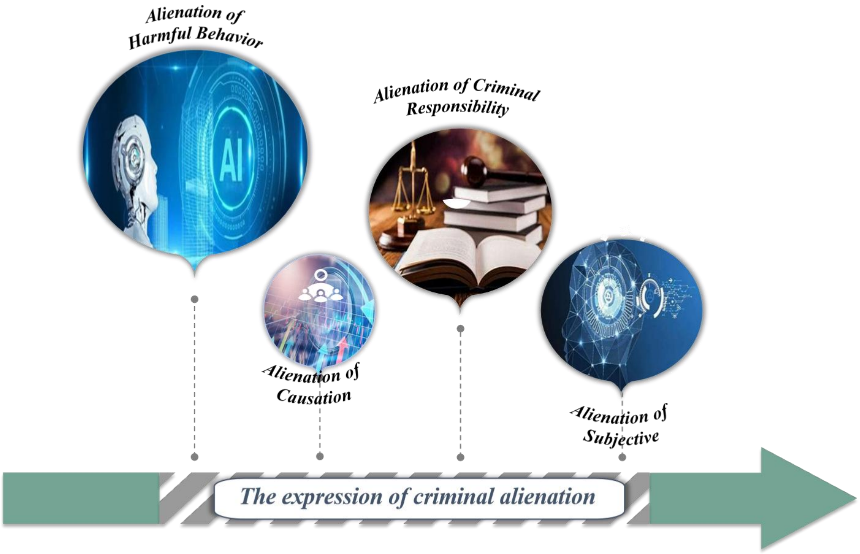
Alienation of Harmful Behavior
Alienation of Criminal Responsibility
Alienation of Causation
Alienation of Subjective
The expression of criminal alienation

Figure 3. The Alienation of Artificial Intelligence Crime is mainly reflected

Harmful behavior, as the cornerstone concept of criminology, becomes the basis and premise to determine the existence of a crime. However, with the enhancement of deep learning and autonomous decision-making ability of AI, "instrumental" AI gradually evolves to "ontology" AI, transforming the implementation of "harmful behavior" from human to artificial intelligence, resulting in the separation of "harmful behavior" and human.

Artificial intelligence harms causality between results and behavior and presents a very complex situation, even if the actor violated the corresponding duty of care or as a duty, caused the harm, but the duty of care or as a duty of obligation, whether a causal relationship between the harm results is still difficult to determine.

Artificial intelligence crime with traditional crime, other network crime, harmful consequences often have uncontrollable, and harmful consequences beyond the algorithm of human meaning consciousness, criminal law traditional evaluation and modesty evaluation, neither objectively practical evaluation of artificial intelligence crime multiplication, the harm of uncontrollable results, and cannot subjectively solve the problem of guilt of artificial intelligence.

Like the determination of causality, the guilt of the perpetrator is also the basic premise for the criminal responsibility of artificial intelligence. However, due to the separation of "harmful behavior" and people, the fault identification of people is more complicated than network crime, and it needs to be judged based on the violation of the duty of care or duty of duty.

Therefore, evaluating the criminal law of artificial intelligence crime should actively respond to the objective laws of artificial intelligence and related crimes and enhance the prevention and risk prevention of artificial intelligence crime. In this context, the criminal compliance plan, as an internal control system for enterprises to prevent crime risks and strengthen internal management, can effectively solve the criminal law challenges brought by the alienation of artificial intelligence crime. As some scholars say, "The norms formulated by the state sometimes do not conform to the specific situation of the company, and compared with these national norms, corporate autonomy can be a much more effective method. For controlling corporate crime, additional increases in efficiency are possible within a homemade framework." The alienation of artificial intelligence crime brings many challenges to traditional criminal law. Common challenges as shown in Table 3, artificial intelligence criminal compliance plan as artificial intelligence research and development, deployment, operation fields related to industry internal system, combined with its unique business scope, operation process, product characteristic design of targeted crime risk identification, determination, and prevention mechanism, and its fact is practical to perform the compliance plan, can be used as an essential basis to determine the crime.

Table 3. The Challenge of Artificial Intelligence Crime Alienation to the Traditional Criminal Law

Type	Description
Anonymity and concealment	Artificial intelligence systems can be used in cyber attacks, data theft, and other criminal activities, and it is often difficult to track the real identity and behavior of criminals.
Transnational sex	AI crime risk can be conducted across national borders, creating difficulties for law enforcement agencies; the national criminal law system, based on domestic laws and jurisdiction, limits combating transnational AI crime risk.
Technical complexity	Artificial intelligence crimes use advanced technologies and algorithms, such as malicious software, hacker tools, automated attacks, etc., which makes it difficult to deal effectively with traditional criminal law and requires training professionals and legal experts to deal with cases.
Conditional doctrine	Transnational AI crime risk may involve multiple national legal provisions and precedents, and the same behavior may be classified into different crime types/subject to different criminal sanctions, leading to complex difficulties in characterization and sentencing.
Law lag	The rapid development of artificial intelligence technology, while the legal system usually takes longer to keep up with technological changes, leads to the law lagging behind the new forms and new means of artificial intelligence crime and the lack of effective means between law enforcement agencies and the judicial system.

Therefore, through the introduction of the AI criminal compliance plan, the compliance obligations of the AI industry should be clarified, and the scope and boundary of the obligations of the relevant subjects should be clarified, which objectively provides a basis for determining the subjective guilt and causality of the relevant subjects. However, the premise of the criminal compliance plan lies in the implementation of the plan. Given the large degree of uncontrollability of ARTIFICIAL intelligence, it no longer belongs to the uncontrollable scope beyond the requirements of algorithm transparency and interpretability and the requirements of data security control.

3.2.2 Single Criminal Law Regulation Model Lags Behind

In the context of artificial intelligence, the prevention and control of cyber crimes is faced with the severe challenge of "refusing the tiger at the front door and entering the Wolf at the back door." That is, traditional cyber crimes have yet to be solved entirely, and artificial intelligence crimes are coming one after another. The AI crime risk patterns are ever-changing, and the common types and proportions of AI criminal risks are shown in Table 4 [22,23].In the traditional criminal law, "fire fighting" passive solution of network crime, it is still difficult to deal with the governance effect of the artificial intelligence crime after algorithm alienation is limited. The idea of network crime, especially artificial intelligence crime, and relying solely on the criminal law's single means of sanctions has been obviously insufficient. At the same time, compared with the traditional Internet, artificial intelligence has more powerful technical support, and the prevention and control of artificial intelligence crimes are more dependent on the professional knowledge level and technical level, especially the mastery of artificial intelligence algorithms and the screening and management of data capture.

Table 4. Types and Proportion of AI Crime Risk

Classification of crimes	Specific case	Percentage
Fraud and false information	False advertising	30%
	Phishing	25%
	Identity theft	20%
	Wash sale	15%
Malware and attacks	Ransomware	40%
	A Distributed Denial of Service (DDoS) attack	30%
	Steal data	20%
	Destruction of critical infrastructure	10%
Artificial intelligence assists in crime	Deep forgery	40%
	Intelligent fraud	30%
	Algorithmic discrimination	20%
	Data privacy leakage	10%

The traditional means of government supervision and crime prevention and control need to be revised in the face of artificial intelligence crime. Therefore, it is necessary to strengthen the concept of AI crime risk prevention and introduce a criminal compliance plan for the prevention and control of AI crime risk. Criminal compliance reduces the risk of crime by strengthening the internal management of enterprises, which is, in essence, the inclusion of enterprises into the crime prevention system. In contrast, "the traditional concept of criminal justice focuses solely on criminal law and criminal justice itself, which is too narrow to capture meaningful behavior." Artificial intelligence, therefore, criminal compliance is in the framework of criminal law and criminal justice, plays a positive role of the artificial intelligence industry in crime prevention through the combination of criminal law and internal criminal compliance system, giving the artificial intelligence industry reasonable and practical as a duty, reversed transmission artificial intelligence industry actively as obligations, prevent artificial intelligence in the development of crime and its potential risks. Therefore, through the criminal compliance of artificial intelligence, relevant laws and regulations can be effectively specific and operable, and legal responsibilities and legal obligations can be specifically refined and implemented into the daily work of AI research and development, deployment, application, and related management. In essence, criminal compliance is a valuable supplement to the current single-penalty punishment model.

4. Results and Discussion

4.1 Ensure Legal Compliance

Legal compliance is one of the most important aspects of compliance planning [24]. AI systems must be designed, developed, and used following applicable laws and regulations to ensure that organizations are not criminally liable for law violations. As shown in Table 5, it is the specific role of the compliance plan to ensure that AI systems comply with legal requirements.

Table 5. Role of the Compliance Plan in the Legal Requirements

Type of action	Description
Legal risk assessment	Identify applicable legal requirements and compliance risks by assessing and analyzing potential legal risks to AI systems.
The compliance framework is established	Establish a clear compliance framework, including determining compliance responsibilities, formulating compliance policies, and establishing internal compliance processes.
Privacy protection	Protect the compliance of the collection, storage, processing, and transmission of personal data.
Data security	Protect the data from unauthorized access, disclosure, tampering, or destruction.
IPR	Ensure that AI systems are designed, developed, and used do not infringe the intellectual property rights of others.
Anti-monopoly compliance	Abide by market competition rules, do not engage in unfair competition activities, and comply with the dominant market position.
Regulatory compliance	Work closely with regulators to ensure AI systems meet regulatory standards and requirements.

4.2 Strengthen Data Privacy and Protection

Compliance plans are essential to enhance data privacy and protection in AI systems. It can ensure that data collection, processing, and use follow applicable regulations, establish clear data protection policies and processes, and take necessary technical and organizational measures to protect data security and privacy while protecting the data subject's right to know and choose [25]. Figure 4 shows the role of compliance plans in data privacy and protection, mainly including ensuring compliance, establishing data protection policies, strengthening technical measures, transparency of data use, and compliance with data processing regulations.

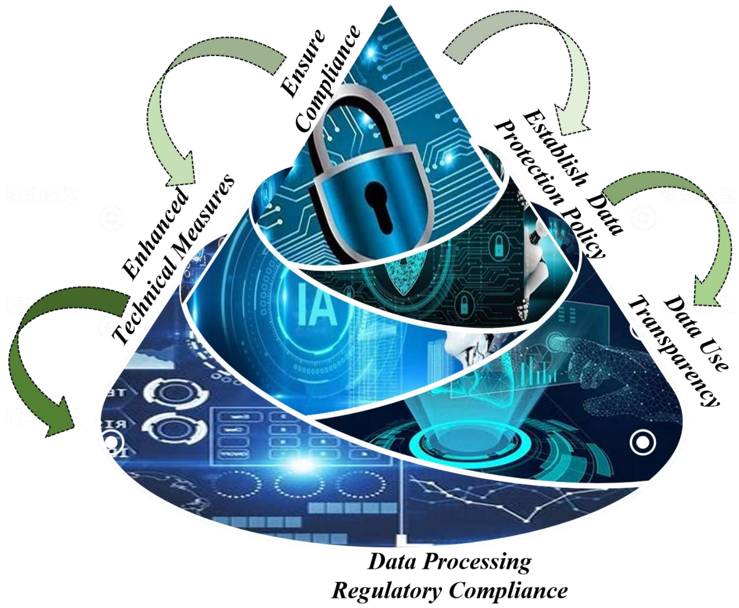
Ensure Compliance
Establish Data Protection Policy
Data Use Transparency
Data Processing Regulatory Compliance
Enhanced Technical Measures

Figure 4. Role of the Compliance Plans in Data Privacy and Protection

Through the compliance plan, the organization can ensure that its AI systems comply with applicable data privacy regulations and regulations, such as the Personal Information Protection Act, the Communications Secrecy Act, etc. The compliance team needs to identify and analyze potential data privacy risks and take steps to ensure that data collection, processing, and storage comply with legal and regulatory requirements. Compliance plans help establish clear policies and processes, including data collection, use, storage, and transmission. These policies need to consider data privacy requirements within and outside the organization and ensure that access and use of data comply with applicable regulations.

A compliance plan requires AI systems to take the necessary technical and organizational measures to protect data privacy and security. For example, using encryption technology to protect data, limit data access and scope of use, and ensure the confidentiality and integrity of data. Compliance plan requires the data use process of the AI system to ensure that the data subject's right to know and choose is respected. For example, provide sufficient notification and choice in data collection and use and disclose the specific purpose and method of transparent data use. Compliance Plan helps organizations ensure that applicable regulatory requirements are met during data processing; for example, personal information must be authorized or agreed to be collected, processed, and stored. In addition, the compliance team needs to establish internal processes to respond to data subject requests and protect their data privacy and rights.

4.3 Ensure Fairness and Prevention of Discrimination

Compliance plans play a crucial role in ensuring the fairness of AI systems and preventing discrimination [26]. It can establish clear equity policies and processes, take necessary measures to identify and eliminate potential risks of discrimination, review the decision-making process of AI systems, and strengthen regulatory compliance and other aspects. As shown in Figure 5, it mainly plays a vital role in establishing fairness policies, identifying discrimination risks, reviewing the decision-making process, and strengthening supervision and compliance.

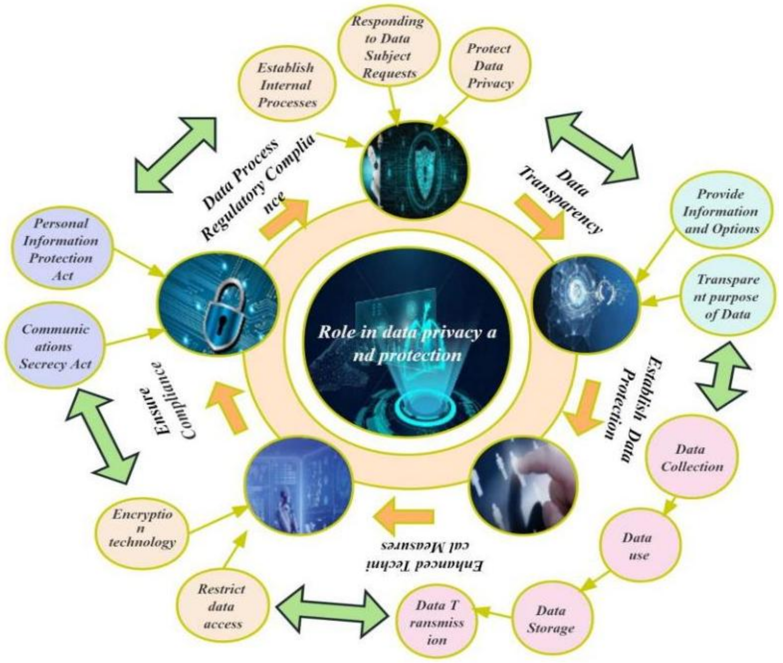
Responding to Data Subject Requests
Protect Data Privacy
Establish Internal Processes
Data Process Regulatory Complia nce
Data Transparency
Provide Information and Options
Transpare nt purpose of Data
Personal Information Protection Act
Communic ations Secrecy Act
Role in data privacy a nd protection
Ensure Compliance
Establish Data Protection
Data Collection
Data use
Encryptio n technology
Enhanced Techni cal Measures
Restrict data access
Data T ransmiss ion
Data Storage

Figure 5. Process of the Role of Compliance Plans in Fairness and Discrimination Prevention

Compliance plans can help organizations establish clear equity policies and processes to ensure that AI systems are designed, developed, and used by the principles of justice, transparency, and interpretability. These policies must consider potential discrimination and take the necessary measures to ensure that AI systems do not negatively affect certain groups.Compliance planning requires a review of datasets and algorithms for AI systems to identify and analyze possible risks of discrimination, such as race, gender, age, etc. Compliance teams need to take the steps necessary to eliminate or reduce these risks, for example, redesign the algorithm, improve the representativeness of the data sample, or incorporate additional data to enrich the diversity of the models. Compliance planning requires a review of the decision process of the AI system to ensure compliance with the principles of fairness, transparency, and interpretability. For example, it is necessary to ensure that the decisions of AI systems are not biased and discriminated by personal attributes and that the system can explain the reasons and logic behind the decisions.

Compliance plans must work closely with regulators, understand and comply with relevant regulatory requirements, and ensure that AI systems meet applicable regulatory standards and requirements. In addition, the compliance team needs to report to regulators on the fairness and anti-discrimination of the AI system to demonstrate compliance. These measures help to ensure the fairness, transparency, and interpretability of AI systems, promoting public trust and application development of AI systems while avoiding adverse effects on particular groups.

4.4 Improve the System Transparency and Interpretability

Compliance plans play an important role in improving the transparency and interpretability of AI systems [27,28]. It requires transparency in data collection and use, transparency in algorithms and models, interpretability assessment and validation, explanatory interface design, and compliance with review and regulatory requirements. Figure 6 shows the five specific roles of the compliance program in the transparency and interpretability of AI systems, including transparency in data collection and use, algorithm and model transparency, interpretability assessment and validation, design of the explanatory interface, and review and regulatory requirements.

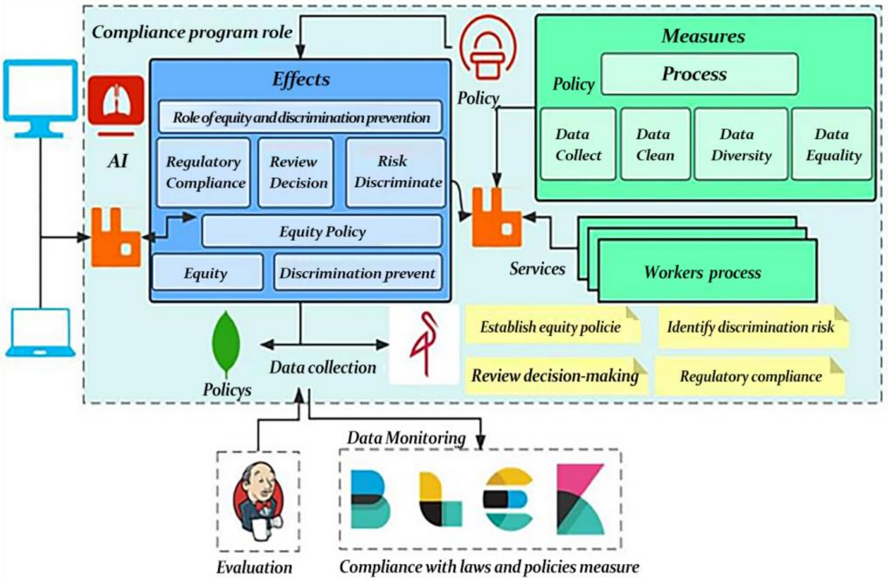

Figure 6. Role of Compliance Plans in Transparency and Interpretability

Regarding data collection and use transparency, the compliance plan requires the AI system to provide transparency in data collection and use and inform the data subject of the collection purpose, use method, and storage period of data collection. This helps build trust and lets the data subject understand how their data is used and processed.

In terms of algorithm and model transparency, the compliance plan encourages the transparency of the algorithms and models of AI systems, and even non-professionals can understand how the system works. This can be achieved by disclosing the key features of the algorithm, the structure of the model, and the input and output to let users and relevant stakeholders understand the logic behind the system decision.

In terms of interpretability assessment and validation, the compliance plan requires an interpretability assessment and validation of AI systems to ensure that their decision-making process meets understandable standards. This may involve reviewing and testing the algorithm to verify whether its responses and decisions across inputs and scenarios are consistent and reasonable.

In terms of explanatory interface design, the Compliance Plan encourages AI systems to adopt a user-friendly interface design to provide interpretation and understanding of system decisions. This can be achieved by visualizing the results, providing background information and interpretation of decisions, and displaying credibility and confidence, helping users and related parties to understand the behavior of the system better.

Regarding review and regulatory requirements, compliance plans need to work with regulators to understand and comply with relevant review and regulatory requirements and ensure that the transparency and interpretability of AI systems comply with legal and regulatory requirements. Compliance teams must regularly review the system operation and report system transparency and interpretability measures to regulators. These measures can enhance the trust of users and related parties in the AI systems, provide an interpretation and understanding of the decision-making process, and promote the sustainable development and widespread application of AI.

4.5 Strengthen the Safety and Protective Measures

Compliance plans play an essential role in strengthening the security and protective measures of AI systems [29,30]. It requires AI systems to establish sound data security strategies, conduct security review and testing, comply with relevant laws, regulations, and ethical standards, establish automated safety inspection and monitoring mechanisms, and conduct safety training and education for relevant personnel. These measures can effectively reduce the risk of artificial intelligence systems being attacked or abused, ensure their safe and stable operation, and promote their sustainable development and broad application.

Table 6 shows the specific role of the compliance plan in the security and protective measures of AI systems. These measures can regulate users' operations, improve the security of artificial systems, enhance users' trust in AI systems, and promote the sustainable development and broad application of artificial intelligence.

Table 6. Role of the Compliance Plan in System Security

Type	Description
Data security	Encrypt data transmission, storage, and access standardize data use permissions, monitor data leakage risk, etc.
Algorithms and model security	Review the algorithm safely to test for stability and find potential vulnerabilities to prevent malicious attacks and abuse.
Prevent abuse	Abide with relevant laws, regulations, and ethical standards, and prevent abuse through review and supervision.
Automation security	Establish automated security inspection and monitoring mechanisms to quickly respond to security events, such as automated vulnerability scanning and event response.
Training and Education	Provide safety training and education to raise awareness and awareness of system safety and protective measures.

5. Conclusion

With the promotion of the "artificial intelligence +" technology wave in recent years, the criminal fields face unprecedented changes. All kinds of innovative means and tools have also emerged. In this process, AI technology can play an essential role in helping companies better control risks and meet regulatory compliance requirements. As a management and normative means in AI, compliance planning can help ensure the legitimacy, security, and ethics of AI systems and promote the sustainable development of technology and the sustainable interests of society.

To reduce AI criminal risk, This paper provides an in-depth study of the types of AI criminal risk and the role of compliance plans in AI criminal risk. First, we summarize the common types of criminal risk. Then, for these risk types, analyze how compliance plans work in terms of ensuring legal compliance, enhancing data privacy and protection, ensuring fairness and discrimination prevention, improving system transparency and interpretability, and strengthening security and protection measures to reduce the probability of a criminal risk in network communication, promote the sustainable development of AI technology in the fields of network communication.

References

[1] P. Dai, Y. Chen and Y. Feng, “Big data analysis of applying artificial intelligence to criminal justice and their prevention,” *in Proc. 2022 Int. Conf. Comput, Big-Data Eng. 2022*, pp. 58-63, 2022.

[2] Z. Zhang, H. A. Hamadi, E. Damiani, C. Y. Yeun, and F. Taher, “Explainable artificial intelligence applications in cyber security: State-of-the-art in research,” *IEEE Access*, vol. 10, pp. 93104-93139, 2022.

[3] Z. Zefeng and X. Fang, “Motion planning and compliance control method for direct drive vacuum manipulator,” *in Proc. 2021 Int. Conf. Inf. Technol. Biomed.* Eng. *(ICITBE)*, pp. 120-125.2021.

[4] T. Xie et al., “Coordinate conversions and deviation analysis in multi-source data fusion,” *in Proc. 2021 2nd China Int. SAR Symp*, pp. 1-3.2021.

[5] G. Sui et al., “Data analysis of elevation standard deviation classifying geomorphological types,” *in Proc. 2010 Int. Conf. Comput. Appl. Syst. Model.* 2010.

[6] P. Wang et al., “Prediction of axis attitude deviation and deviation correction method based on data driven during shield tunneling,” *IEEE Access*, vol. 7, pp. 163487-163501, 2019.

[7] Z. Tang, "The empirical study on the credit risk discrimination of listed SMEs based on the distance to default," *in Proc. 2009 6th Int. Conf. Serv. Syst. Serv. Manag*, pp. 799-803, 2009.

[8] J. L. Gastwirth, "Case comment: Statistical tests for the analysis of data on peremptory challenges: Clarifying the standard of proof needed to establish a prima facie case of discrimination in Johnson v. California," *Law, Probab. Risk,* vol. 4, no. 3, pp. 179-185, 2005.

[9] Q. Pan and J. L. Gastwirth, "The appropriateness of survival analysis for determining lost pay in discrimination cases: Application of the ' Lost Chance ' doctrine to Alexander v. Milwaukee," *Law, Probab. Risk,* vol. 12, no. 1, pp. 13-35, 2013.

[10] X. Wang et al., "Research on big data security and privacy risk governance," *in Proc. 2021 Int. Conf. Big Data, Artif. Intell. Risk Manag*, pp. 15-18, 2021.

[11] L. Sion et al., "Privacy risk assessment for data subject-aware threat modeling," *in Proc. 2019 IEEE Secur. Privacy Workshops*, pp. 64-71, 2019.

[12] J. Sun et al., "Research on the characteristics and security risks of the internet of vehicles data," *in Proc. 2022 7th IEEE Int. Conf. Data Sci. Cyberspace*, pp. 299-305, 2022.

[13] R. Sharma, C. Schommer and N. Vivarelli, "Building up explainability in multi-layer perceptrons for credit risk modeling," *in Proc. 2020 IEEE 7th Int. Conf. Data Sci. Adv. Anal*, pp. 761-762, 2020.

[14] C. Champod, "Fingerprint examination: Towards more transparency," *Law, Probab. Risk,* vol. 7, no. 2, pp. 111-118, 2008.

[15] T. Zhang, C. Wagner and J. M. Garibaldi, "Counterfactual rule generation for fuzzy rule-based classification systems," *in Proc. 2022 IEEE Int. Conf. Fuzzy Syst*, pp. 1-8, 2022.

[16] R. S. A. Faqir, "Digital criminal investigations in the era of artificial intelligence: A comprehensive overview," *Int. J. Cyber Criminol*, vol. 17, no. 2, pp. 77-94, 2023.

[17] S. Sen et al., "Bootstrapping privacy compliance in big data systems," *in Proc. 2014 IEEE Symp. Secur*, pp. 327-342, 2014.

[18] A. S. Ferreira, J. B. Filho and M. N. Souza, "Comparison of segmental arterial compliance determined with three and four element Windkessel models," *in Proc. 25th Annu. Int. Conf. IEEE Eng*, pp. 3161-3164, 2003.

[19] M. Acer and A. Sabanovic, "Comparison of circular flexure hinge compliance modeling methods," *in Proc. 2011 IEEE Int*, pp. 271-276, 2011.

[20] K. Singh et al., "Bibliometric analysis of white-collar crimes- Concept and development using artificial intelligence," *in Proc. 2023 Int. Conf. Device Intell., Comput. Commun. Technol*, pp. 317-320, 2023.

[21] D. Jeong, "Artificial intelligence security threat, crime, and forensics: Taxonomy and open issues," *IEEE Access,* vol. 8, pp. 184560-184574, 2020.

[22] S. Singh et al., "Technological intervention: Prevention of crime using AI and IoT," *in Proc. 2023 IEEE World Conf. Appl. Intell. Comput*, pp. 778-782, 2023.

[23] B. S. Rawat et al., "The empirical analysis of artificial intelligence approaches for enhancing the cyber security for better quality," *in Proc. 2022 5th Int. Conf. Contemp. Comput. Inform*, pp. 247-250, 2022

[24] T. D. Breaux and C. Powers, "Early studies in acquiring evidentiary, reusable business process models for legal compliance," *in Proc. 2009 Sixth Int. Conf. Inf. Technol.: New Generations*, pp. 272-277, 2009.

[25] J. Huang and X. Kong, "Research on data privacy security comprehensive protection program based on computer data protection algorithm," *in Proc. 2023 IEEE Int. Conf. Image Process. Comput. Appl*, pp. 325-329, 2023.

[26] F. Mendoza and H. W. Behrens, "Arbiter: Improved smart city operations through decentralized autonomous organization," *in Proc. 2020 IEEE Int. Symp. Technol. Soc*, pp. 407-412, 2020.

[27] L. Da Silva Barboza, G. A. d. A. Cysneiros Filho and R. A. C. De Souza, "Towards legal compliance in IT procurement planning in Brazil's federal public administration," *in Proc. 2016 IEEE 24th Int. Requir. Eng. Conf. Workshops*, pp. 229-238, 2016.

[28] A. Sheth et al., "Process knowledge-infused AI: Toward user-level explainability, interpretability, and safety," *IEEE Internet Comput*, vol. 26, no. 5, pp. 76-84, 2022.

[29]T. Miyakawa, S. Umezaki and R. Mihira, “Study for return on investment by safety protection measures,” *in Proc. TENCON 2010 - 2010 IEEE Region 10 Conf* , pp. 631-635, 2010.

[30]L. Lu et al., “Safety risk analysis and safety protection measures of power distribution internet of things,” *in Proc. 2021 China Int. Conf. Electr. Distrib*, pp. 633-637, 2021.