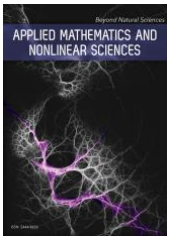
sciendo Applied Mathematics and Nonlinear Sciences, 9(1) (2024) 1-14



Applied Mathematics and Nonlinear Sciences

https://www.sciendo.com

A study of innovations in legal governance with respect to the safety of artificial intelligence

Yanggui Li[1,†]

1. Law School, Dongguan City College, Dongguan, Guangdong, 523419, China.

Submission Info

Communicated by Z. Sabir
Received January 18, 2023
Accepted June 9, 2023
Available online November 29, 2023

Abstract

This paper aims to promote the safe development of artificial intelligence and improve legal policies. Combined with the cluster analysis algorithm, it analyzes the safety risks as well as legal defects of artificial intelligence. The Laplace matrix is derived using the similarity matrix, and the feature vector space is constructed by analyzing the associated features of artificial intelligence safety. Combining the spectral clustering algorithm, legal assessment indexes for artificial intelligence safety were constructed. The modular metric value method is utilized to assess the clustering effect of laws on the safety of artificial intelligence. Analyzing the security risks of artificial intelligence, improved legal policies are proposed from the perspective of technology and privacy. The results show that the effect of improving privacy protection policy on privacy protection is 0.85, and the effect of clarifying subject rights is 0.9. The introduction of laws should consider social ethics, and the effect degree of ethical principles is 0.75. Clarifying subject rights can help avoid technological risks to a certain extent, and improving privacy protection policies can help protect users' privacy.

Keywords: Artificial Intelligence; Cluster Analysis; Spectral Clustering Algorithm; Modular Metrics; Legal Governance.
AMS 2010 codes: 97R40

†Corresponding author.
Email address: lyg2004523@126.com

ISSN 2444-8656
https://doi.org/10.2478/amns.2023.2.01300

1 Introduction

Humanity has entered into the 21st century at three key points in time. There have been three new eras that are interconnected and slightly different from each other, i.e., the era of network society, the era of big data, and the era of artificial intelligence, which together constitute a new social era. Accompanied by the development of the Internet and big data, the breakthrough of computing power and data capacity makes the development of artificial technology break the bottleneck and flourish [1-3]. Massive data resources, supercomputing power and core algorithms for thinking robots "deep learning" to provide favorable conditions so that artificial intelligence is finally out of the laboratory and into human life. Although the development of artificial intelligence is still far from the scene described in science fiction movies, it is undoubtedly the future development trend of science and technology, no matter whether worrying about it is the devil's call or happy that human beings become the "Creator", now artificial intelligence has been applied to many areas of people's lives [4-6]. Nowadays, AI is no longer the ideal of scientists but can penetrate our lives to bring us real surprises and touches, which can not only bring us a lot of auditory and visual enjoyment but also make our lives more efficient and convenient [7-8]. However, the security and ethical challenges brought by AI to human society are also real, and recognizing risks, predicting risks, preventing risks, and maximizing the benefits to human society are the themes of today's AI era.

In order to fully avoid risks, countries around the world have taken the formulation of AI ethical guidelines, improved laws and regulations and industry management to carry out AI safety governance. The AI safety technology system has a significant role in guiding AI safety governance. Specifically, the AI safety technology system is an important part of AI safety governance, an important support for the implementation of AI ethical norms and legal regulatory requirements, and an important guarantee for the healthy and orderly development of the AI industry [9-10].

Van Dijk, N et al. argue that artificial intelligence brings convenience with certain drawbacks, especially in terms of morality and ethics. By elucidating the points and drawbacks of legal governance in AI, the laws related to AI technology are improved [11]. Zhang, B et al. argue that researchers play an important role in the ethics and governance of AI. By collecting the views of employees in different research AI fields and comparing the findings with publicly available data information, a new approach to AI governance was proposed [12]. Janssen, M et al. argued that the rise and exploitation of big data are increasingly affecting individuals and society, which also means that the use of AI and big data should be subject to strict regulation and ethical constraints, proposing appropriate management approaches and governance measures [13]. Yee, D. H et al. argued that the emergence of artificial intelligence has brought great impact and change in various fields such as politics, economy, culture, etc., and there are inherent risks associated with this progress. Statistical methods are used to analyze the factors of risk, and relevant solutions are proposed [14]. Grassi, A et al. argue that most companies currently use artificial intelligence technology to process data for analyzing external factors of the company. A governance and management approach to the movement of AI technology is proposed to address the problems of AI in corporate data analysis [15]. Qichun, Yang et al. focuses on the impact of new technologies on the law by presenting the scope of application of legal interoperability, increasing the rules governing AI around the development and use of AI while also including the increase in the number of related products and their use [16].

In this paper, the clustering algorithm is first studied, focusing on hierarchical clustering using the classical clustering algorithm and the k-means clustering algorithm by constructing the affinity matrix describing the similarity of sample points, using the similarity matrix to derive the Laplace matrix and calculating the first k eigenvalues and eigenvectors of the Laplace matrix to derive the eigenvector space. Next, the cluster analysis algorithm is used to analyze the risk of cybersecurity governance in the context of artificial intelligence. Create an association map for AI safety's current

application scope using subject terms to extract the key features of AI safety risks. Establish the multidimensional features of artificial intelligence for legal security risk and implement classification to achieve subdivided risk types so as to construct indicators for artificial intelligence for legal security risks. Combine the modular metric values to construct an evaluation of the effect of artificial intelligence security and legal clustering. Finally, by analyzing the types of AI security risks, better legal principles are proposed for privacy risks and technology risks. By enhancing the privacy protection policy and integrating the human-centered principle, a new governance policy is constructed.

2 Cluster analysis-based security risk assessment method for artificial intelligence

2.1 Research on clustering algorithms

2.1.1 Classical clustering algorithms

k-means is the most classical unsupervised clustering algorithm. Its main purpose is to divide n sample points into k clusters. The similarity between the samples is measured using the distance between the samples so that similar samples are grouped into the same cluster as much as possible, that is, to make the distance between the samples within the cluster as small as possible, and the distance between the samples between the clusters as large as possible. The Euclidean distance is used to calculate the distance; the smaller the Euclidean distance between two samples, the more similar they are. When we use the k-means algorithm to cluster the sample data, in the first step, we need to specify the number k of clusters to be divided, which is the number of classes [17-18]. In the second step, the algorithm randomly selects k data objects as the initial cluster centers. k data objects cannot be sample points. In the third step, the distance of each of the remaining data objects to these k initial clustering centers is calculated, and the data object is assigned to the cluster class in which the center closest to it is located. In the fourth step, the algorithm adjusts the new class and recalculates the center of the new class. In the fifth step, loop steps three and four to see if the centers converge or remain the same, and stop the loop if it converges or reaches the number of iterations.

Assume that the sample set $D=\{x_1, x_2, \ldots, x_m\}$, the number of clusters is equal to k and the maximum number of iterations is equal to N. Assign the samples to their nearest center vectors according to Eq. (1) and decrease the value of the objective function. The new center of mass is recalculated according to Eq. (2) and the criterion function E is calculated according to Eq. (3) to minimize E.

$$d_{ij} = \left\| x_i - p_j \right\|^2 \tag{1}$$

where d_{ij} denotes the distance from the sample point to the initial clustering center p_j. The new center is recalculated according to Eq. 2 and the criterion function 3 is calculated according to Eq. E to minimize E.

$$\overline{x_i} = \frac{1}{|C_i|} \sum_{x \in C_i} x \tag{2}$$

$$E = \sum_{i=1}^{k} \sum_{x \in C_i} \left| x - \overline{x_i} \right|^2 \tag{3}$$

Where the division of clusters is denoted as C, $C=\{C_1,C_2,\ldots,C_k\}$, $\overline{x_i}$ is denoted as new clustering centers and E is used as an evaluation metric to evaluate whether the clustering effect is optimal or not.

Hierarchical clustering is one of the commonly used clustering methods. According to whether the order of hierarchical decomposition is bottom-up or top-down, hierarchical clustering algorithms can be divided into merged hierarchical clustering algorithms and split hierarchical clustering algorithms. In practice, most of the hierarchical clustering belongs to merged hierarchical clustering. The merging algorithm of hierarchical clustering calculates the distance between two types of data points, combines the two types of data points that are closest to each other, and iterates this process repeatedly until all the data points are combined into one class, and ultimately generates a series of nested clustering trees to complete the clustering. Single-point clustering is at the bottom of the tree, and there is a root node clustering at the item level of the tree. The root node clustering covers all the data points, and the final result is displayed in the clustering spectral graph [19-20].

In contrast to the k-means algorithm, hierarchical clustering does not require a predetermined number of clusters and allows the discovery of hierarchical relationships of the classes, which is very useful in some specific domains. The hierarchical clustering algorithm first considers each object as a class and calculates the minimum distance between two and two. Secondly, the two classes with the minimum distance are merged into a new class. Then, the distance between the new class and all the classes is recalculated; finally, steps two and three are repeated until all the classes are merged into one class.

In hierarchical clustering, a class consisting of one sample is the most basic class, and the distance between samples can be used as absolute value distance, Euclidean distance, and Minkowski distance, among others. If a class contains more than one sample, then the interclass distance is determined. The interclass distance is defined based on the distance between samples and is roughly calculated by the shortest distance method, the average connection between groups method, and the center of gravity method. Suppose G_1 and G_2 are two classes and $D(G_1,G_2)$ is the distance between these two classes. The shortest distance method involves taking the shortest distance between samples of two classes as the distance between classes.

$$D(G_1,G_2)=\min d\left(\overrightarrow{x_a},\overrightarrow{x_b}\right) \tag{4}$$

where $\overrightarrow{x_a}\in G_1,\overrightarrow{x_b}\in G_2$. $d\left(\overrightarrow{x_a},\overrightarrow{x_b}\right)$ is expressed as the distance between two samples. Mean connectivity between groups is the average of the distances between all the samples of the two classes, and d_1,d_2,d_3,d_4 is the distance between the samples.

$$D(G_1,G_2)=\frac{d_1+d_2+d_3+d_4}{4} \tag{5}$$

2.1.2 Spectral clustering algorithm

Spectral clustering is a popular clustering method that originated from the division of graphs. The spectral clustering algorithm is built on the theoretical basis of graph theory. Spectral clustering treats the sample dataset as points in space, which can be connected by edges, thus constituting an undirected graph, which divides the weighted undirected graph into two or more optimal subgraphs so that the similarity within the subgraphs is as high as possible, and that the similarity between the

subgraphs is as low as possible. Compared with the traditional k-means clustering algorithm and hierarchical clustering algorithm, spectral clustering is more adaptable to the distribution of the data and has the advantage of being able to cluster on an arbitrarily shaped sample space and converge to the global optimal solution. When performing spectral clustering, it is first necessary to construct the affinity matrix describing the similarity of the sample points and then use the similarity matrix to derive the Laplacian matrix and calculate the first k eigenvalues and eigenvectors of the Laplacian matrix to construct the eigenvector space. By the above method, the data in the high-dimensional space has been mapped to the low-dimensional, and finally, the feature vectors in the eigenvector space are clustered on the low-dimensional space using k-means or other clustering algorithms". The steps of the clustering spectral class algorithm are shown in Fig. 1. Firstly, the similarity matrix W between the points in the graph is constructed, the Laplace matrix L is calculated according to the similarity matrix, and the smallest k eigenvalues and the corresponding eigenvectors are calculated, so as to construct the feature matrix. Third, each row in the feature matrix is taken as a sample, and the new sample points are clustered using the traditional clustering algorithm.

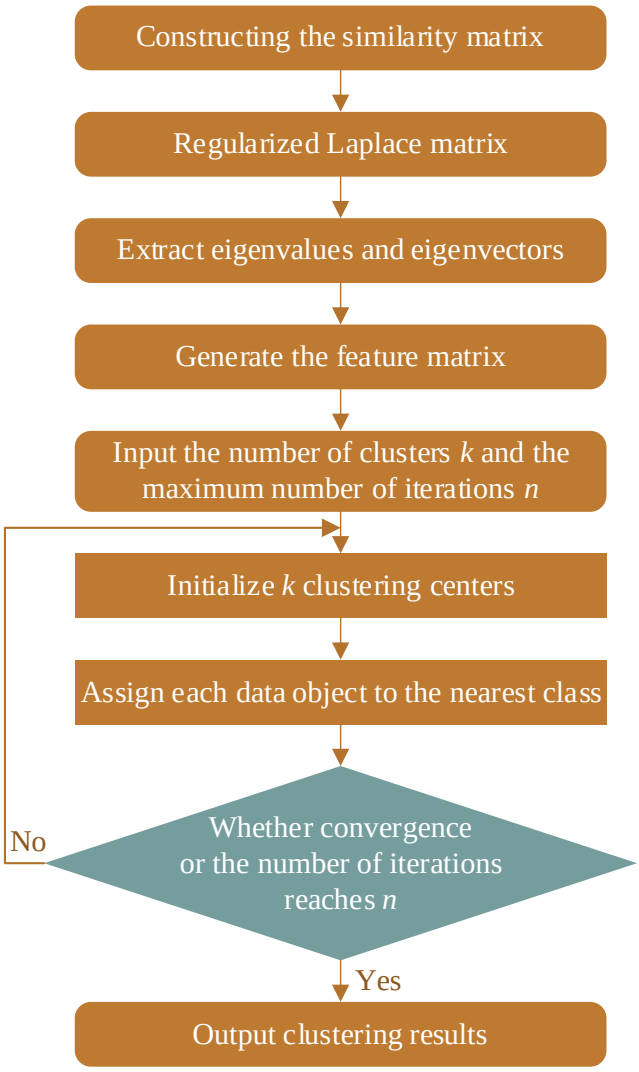


Figure 1. Cluster spectral class algorithm step

For a network graph G, generally denoted by $G(V,E)$, V is used to denote the set of nodes, E is used to denote the set of edges, and for any two nodes in V can be connected by edges or not. The measure of similarity between nodes is a very important part of the spectral clustering algorithm,

and it is generally considered that the similarity between two points that are far away from each other is low, and the similarity between two nodes that are close to each other is high. There are usually three methods for constructing the similarity matrix W, which are ò-nearest neighbor method, k-nearest neighbor method, and fully connected method. The commonly used sample similarity calculation methods are Gaussian similarity method with the following formula:

$$w_{ij} = \sum_{i=1, j=1}^{n} \exp \frac{-\left\| x_i - x_j \right\|^2}{2\sigma^2} \tag{6}$$

Where w_{ij} denotes the node to node similarity value and the matrix W consisting of w_{ij} is known as similarity matrix.

Cutting and dividing the network graph is also a very important part of spectral clustering algorithms. For the undirected graph $G(V, E)$, the final goal is to cut it into k subgraphs that are not connected to each other, and the set of points of each subgraph is $\{A_1, A_2, \ldots, A_k\}$. There are three commonly used cut methods, namely, MinCut, RatioCut, and Ncut cuts, and the one that has been most used by the scholars is the Ncut cut, whose goal is to minimize the Ncut function, which is computed by the following formula:

$$NCut(A_1, A_2, \ldots, A_k) = \frac{1}{2} \sum_{i=1}^{k} \frac{W(A_i \overline{A_i})}{vol(A_i)} \tag{7}$$

The results obtained from spectral clustering are often superior compared to traditional clustering algorithms, and therefore, it has been widely used in clustering.

2.2 Risk Clustering for Legal Security Governance under Artificial Intelligence

2.2.1 Artificial Intelligence Security Feature Correlation

Design the association map of the current application range of AI products in the form of topic words, extract the key features of the development of AI products, and complete the selection of clustering centers in the sample points, whose features discrete attributes and continuous attributes are defined in the following formula:

$$\rho_i = \chi \sum_{j \neq 1} \left(d_{ij} + d_c \right) \tag{8}$$

$$\rho_j = \sum_{j \neq 1} \exp\left[d_{ij} d_c \right] \tag{9}$$

where i denotes a sample point with discrete key features, j denotes a sample point with continuous key features, χ denotes the distribution pattern of the discrete distribution of the sample points, d_{ij} denotes the distance between sample points i to j, and d_c denotes the truncated distance between 2 sample points.

The first step in the application of cluster analysis is to use the thesis domain in that cluster analysis to create a maximum nearest neighbor rough set to obtain the characteristic covariates of regular and

abnormal factors. The rough data set utilizes the known influence conditions to describe the uncertain influence factors and discover the potential characteristics of the data. Assuming that the thesis domain is a non-empty set of relevant data such as influence factors, denoted by the letter W, the studied influence data are categorized according to this set, and data with similar characteristics are grouped into subsets of class clusters with the same or different objects, which can be denoted by $w_1, w_2, \cdots, w_i$.

Rough datasets on this thesis space, the factors in the set are divided according to the equivalence relation, where the data relations with the same class and small gaps are called indistinguishable relations.

Suppose that given a thesis as U, with γ_i denoting the equivalence relation in this thesis U, set x_i as the object in U, $u_1, u_2, \cdots, u_i$ as the subset of the thesis U, and judge the largest set $u_{\max}$ consisting of the data x_i belonging to u_i, which is the lower approximation of the set u_i with respect to the equivalence relation γ_i. And the non-empty equivalent concatenated set intersecting with u_i is the smallest set $u_{\min}$, which is called the lower approximation of set u_i with respect to equivalence relation γ_i. The feature extraction process is shown in Fig. 2, which firstly sets an argument space, collects the related data, and processes them to derive the feature class clusters.

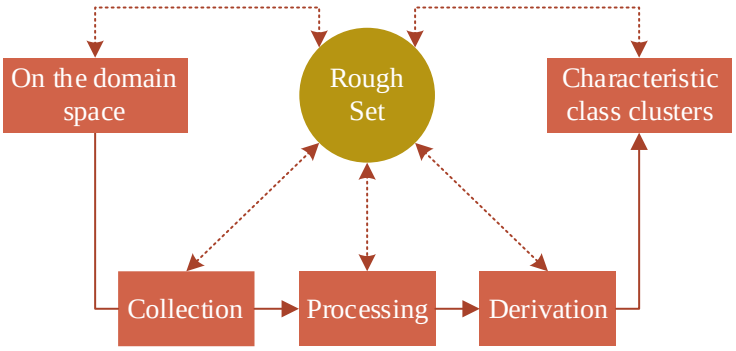


Figure 2. The rough-set feature extraction process

The extraction process described above results in a quantitative influencing factor characteristic covariate, which can be described using the following equation:

$$q_i(x_i) = \left[x_i \mid \Delta\left(x_i^a, x_i^b\right) < d(x_i), x_i \in u_i \right] \tag{10}$$

Where $q_i(x_i)$ denotes the rough set on the subset of the i nd thesis domain, the characteristic parameter under the constraint of equivalence relationship, x_i denotes the variable factor affecting the development of AI industry, a denotes the surface influence relationship of the factor, b denotes the deep influence relationship of the factor, and $\Delta\left(x_i^a, x_i^b\right)$ denotes the mining coefficient under different association depths. Influence covariates with similar characteristics are obtained through the above formula to provide precise data for defining similarity.

2.2.2 Indicators for legal assessment of security aspects of artificial intelligence

Every industrial development has specific objectives and corresponding industrial development tools. Therefore, when analyzing the development of the AI industry under the framework of "target tools", it is necessary to refine the industrial development goals and classify the industrial development tools. By analyzing the AI industrial environment in different regions, we have constructed an AI industrial environment perspective based on the industrial development goals, which includes basic theories, key technologies, support platforms, industrial development, integration and application, etc., aiming to optimize the AI industrial environment [21-22]. The types of risks are more complex due to the extensive characteristics of risks in the development process of each industry and the increased labeling information. By establishing multidimensional features and implementing the classification of AI legal security risks, risk types can be subdivided to determine the risk characteristics under different attributes. The indicators for the assessment of AI legal security risks are shown in Table 1. The first-level indicators mainly include technical risks, safety issues, and ethical risks. Legal loopholes and the qualified professional ability of the lawmaker are the main indicators of technical risks. The presence of an emergency handling plan is the main indicator of security issues. The ethical question is whether or not the ethical and moral boundaries have been violated.

Table 1. Artificial intelligence security legal risk assessment index

Level 1 indicators	Secondary indicators	
	Metric	Give an example
Technical risk	Whether there are loopholes in the law	Technical addiction risk
	Professional competence of the law-enamers	Risk of unemployment
safety problem	Whether there is an emergency handling plan	Privacy leakage risk
Ethical risk	Whether to follow the ethical bottom line	Risk of cyber crime

2.3 Evaluation of Artificial Intelligence Security Law Clustering Effectiveness

The quality of the clustering effect influences the analysis of the clustering results. Since clustering is an unsupervised learning algorithm, the evaluation of the quality of the clustering effect is an important task. Otherwise, the results of clustering will be difficult to be applied. The evaluation of clustering is generally categorized in two ways. The first is the external information evaluation way. The external information refers to the intuitive information embodied by the data, whether the clustering results are in line with reality, but in most cases, the huge amount of data and the use of textual clustering methods and so on will make it difficult to evaluate the external information efficiently, so the second type of evaluation is the evaluation of the internal information. Some parameters generated by some models after clustering are used as indicators to evaluate the clustering effect, according to which the relationship characteristics of the clustering structure itself and the dataset are often used as the measurement information for clustering evaluation. In this paper, we use a combination of external and internal information to evaluate the clustering effect, and the external metrics are based on the a priori knowledge of the data structure. The internal information evaluation mainly selects two representative metrics, which measure the complementary characteristics between classes, which are the modularity metric o, the error squared, and sse.

The modularity metric Q was proposed by Newman and Girvan et al. It is a commonly used method to measure the quality of network community segmentation as well as the strength of the network community structure, and the size of the Q value mainly depends on the community segmentation of the network, and the larger the Q value, the higher the quality of the network community segmentation. Therefore, many scholars use the modularity degree Q to obtain the optimal network

division. The range of Q value is in $[-0.5,1)$, and a large number of literatures show that when the Q value is between 0.3 and 0.7, it indicates that the clustering is very effective.

$$Q = \sum_{i=1}^{k} \left(\frac{e_i}{m} - \left(\frac{\varphi_i}{2m} \right)^2 \right) \tag{11}$$

where k denotes the number of clusters, e_i is defined as the number of edges in cluster i, φ_i is defined as the sum of node degrees in cluster i, and m denotes the total number of edges in the entire network. When $Q = 0$, it means that all nodes are within a cluster, and when $Q > 0$, it means that there is some inherent cluster structure in the network, and the modularity measure is the difference between the total number of edges in the cluster and the number of randomly placed edges.

The sum of squares of errors is used in many algorithms, where the parameter is calculated as the sum of the squares of the errors at the points corresponding to the fitted and original data. In clustering algorithms, k-means clustering is often used for the selection of the optimal k value using SSE, which measures the cohesion of the clusters, i.e., quantifies the closeness of the elements in the clusters, without taking into account the external information. SSE is suitable for comparing two clustered partitions, and given two different sets of clustering results from different clustering processes, the one with the smaller SSE is preferred because it means that the that the center of mass of such clusters is a better representation of the cluster center. In this paper, the formula for SSE is improved as follows:

$$SSE = \sum_{i}^{k} \sum_{j \in A_i} dist\left(c_i, j\right)^2 \tag{12}$$

Where k denotes the number of clusters, c_i denotes the center node of cluster i, j denotes the general node in cluster i, and $dist$ denotes the shortest path from node j to the center node c_i of the cluster in which it is located.

3 Study on the legal governance of artificial intelligence security

3.1 Artificial Intelligence Security Risk Clustering Analysis

3.1.1 Artificial Intelligence Privacy Risk Analysis

After more than 100 years of development, the traditional theory and system of privacy have been relatively mature, but with the advent of the era of artificial intelligence, the traditional theory and system of privacy are no longer sufficient to deal with the reality of various privacy protection problems. To a certain extent, human society can be said to have entered the “privacy-free era”. In the era of artificial energy, privacy risk presents new forms and characteristics. The characteristics of privacy infringement under artificial intelligence are shown in Table 2, which mainly include complexity, extensiveness and severity. The complexity is primarily due to the complexity of the infringing subject and the complexity of the infringement method. The seriousness of privacy leakage is mainly reflected in the seriousness of the consequences and the impact on parties. The highest risk of the three characteristics is the severity of the consequences of infringement, with a risk degree of 0.9, a risk degree of complexity is 0.75, and a risk degree of extensiveness is 0.8.

Table 2. Characteristics of privacy infringement under artificial intelligence

Privacy infringement characteristics	complexity	catholicity	severity
Reflect the level	The complexity of the subject of tort liability	The larger object is not the individual, but the whole society e	The seriousness of the consequences
	The complexity of the infringement methods		The seriousness of the consequences
degree of risk	0.75	0.8	0.9

In the "privacy-free era", privacy risks have increased dramatically. Although artificial intelligence based on networks and data is still in the stage of weak artificial intelligence, the privacy risk brought by it has shown different forms and characteristics from traditional privacy infringement. In the stage of artificial intelligence, the formation of privacy risk is still inseparable from human participation, and the main forms of privacy risk in the age of artificial intelligence are shown in Table 3, namely, the violation of physical space privacy, the violation of cyberspace privacy, and the violation of self-determination privacy by means of artificial intelligence. Physical privacy violations are mainly reflected in video surveillance and microcassette recordings. Cyberspace privacy mainly reflects data intrusion, virus invasion, and information theft. Self-determination privacy mainly includes algorithmic interference and big data recommendations. Physical space privacy is mainly characterized by external leakage, such as the body, etc. Cyber privacy invasion is characterized by information leakage, and self-determination privacy is characterized by a behavioral willingness to leak, and the discovery rates of the three are 0.6, 0.7, and 0.5, respectively.

Table 3. Major forms of privacy risk in the era of artificial intelligence

Main form of privacy risk	Physical space	cyberspace	Self-determination privacy
Specific embodiment	Video surveillance	Data into debt	Algorithmic interference
	camera	Network information leakage	Big data recommendation
feature	External privacy leaks	information disclosure	Disruption of willingness to act
discovery rate	0.6	0.7	0.5

3.1.2 Artificial Intelligence Technology Risk Analysis

There are risks in the application of artificial intelligence technology, which are the "inherent risks" of artificial intelligence technology. The three necessary elements for artificial intelligence technology have basically matured in recent years, leading to its explosive and rapid development in recent years. These three elements are algorithms, deep learning, and big data. The development of these three elements is driving the improvement of artificial intelligence technology.

Artificial intelligence technology, through certain algorithms for deep learning of big data, may eventually have an impact on the existing human life system. The existing system of human life is designed based on the basic capabilities of human beings, and if there is a "capability" that breaks through the limits of human beings, then the existing system of human life is bound to be broken. Artificial intelligence technology risks, as shown in Table 4, are mainly reflected in the breakthrough of the existing social order, the upper-level system, disruption of the industry market and so on. Among them, disrupting the market results in a large number of labor workers losing their jobs. The three have the highest degree of influence on people, including an employment rate of 0.8.

Table 4. AI technology risks

Artificial intelligence technology risk	Break the existing order	The upper system	Raid the market
Embody	It brings convenience to people and also disrupts the social order	The upper layer has formulated the corresponding system because of artificial intelligence	Artificial intelligence is gradually replacing labor
Impact degree	0.65	0.7	0.8
Bear fruit	Age of intelligence	Legal loophole	A large number of workers are unemployed

For example, the emergence of the artificial intelligence alphagozero, which defeated the world Go champion alphago after only three days of learning, proves that artificial intelligence products can break through the limits of human beings and that the laws and rules it masters can completely break through the experience accumulated by human beings over thousands of years. In this case, the pattern and order of human social life may be completely disrupted by AI technology. Taking the securities market as an example, if AI technology can completely realize the control of trend risk through arithmetic and calculate returns almost without error, then the most basic principle of "three publics" in the securities market has been completely dismantled, and it seems that the significance of the existence of the securities market as well as the rules of trading should be rethought and redefined.

3.2 Artificial Intelligence Security Risk Management Strategies

3.2.1 Legal Regulation of Artificial Intelligence Privacy Risks

In the face of the widespread application of AI technology, privacy leakage is also facing great risks, and the challenges to privacy protection are increasing, and the law as the most basic and final safeguard is an indispensable part. However, China does not have a specialized Data Protection Law or Privacy Protection Law, and the protection of privacy is scattered among different sectoral laws, which makes it difficult to deal with the privacy risks in the application of AI. The legislation on the protection of privacy should combine the development of the AI industry and the current protection status in China, and it should draw on extra-territorial legislative practices to standardize the institutional construction of privacy legislation in China. The legal direction of the privacy risk of artificial intelligence is shown in Table 5, and the relevant laws on privacy and security, the principle of notification should be sound, the privacy protection policy should be improved, especially for minors, and the subject of power should also be further clarified. The perfect degree of legal policy of all three is high, respectively 0.95, 0.85, 0.9. The user's right is mainly reflected in the data carrying, forgetting, and interpretation, and the perfect degree of all three is higher than 0.6.

Table 5. The legal direction of ai's privacy risks

Principles when introducing privacy laws	Improve the principle of notice	We will improve privacy protection policies	Clear subject rights
Perfect degree	0.95	0.85	0.9
User subject rights	Data carrying rights	Data is forgotten	The right to reject and interpret the data
embody	Users can exercise control over their own data	Users have the right to request the deletion of their own personal information records	Users have the right to reject automated AI decisions
Perfect degree	0.75	0.7	0.65

When introducing legislation on privacy protection, it is important, on the one hand, to improve the rules of notification so that data controllers disclose information to users in a timely manner, in a clear, detailed and easily understandable manner, and ensure that the notification effectively reaches the

user. Regardless of the manner in which the data controller or data processor processes the user's data, it must notify the data subject in addition to obtaining the user's express consent. In addition, it is necessary to improve privacy protection policies for specific groups, particularly minors. On the other hand, subject rights should be granted to users to enhance their ability to control their privacy data in an environment where privacy risks exist in AI applications. First, the right to data portability should be granted to users to incentivize data controllers to form a competitive model as a way to protect users' privacy to a higher standard. Second, the right to be forgotten should be granted to data, and data subjects have the right to request data controllers to completely delete the data information of individuals that can be collected by AI applications, such as search records, travel records, shopping information, medical records, and so on, and, third, the right of refusal and the right of interpretation should be granted to the data. In order to minimize the negative impact of automated decision-making by AI applications on users, users have the right to reject automated decision-making by AI applications and have the right to request the controller of the data to explain the results of such decision-making accordingly.

3.2.2 Legal Regulation of Artificial Intelligence Technology Risks

Nowadays, the rapid development of science and technology makes us also enter a brand-new era to do a good job in advance to prevent risks and improve the ability to deal with risk response. Rethinking the legal concept of technology in the era of artificial intelligence. After entering the 20th century, with the development of industry, environmental pollution, nuclear proliferation, gene editing and so on increased social risks, and artificial intelligence makes all kinds of risks to be integrated, and any loophole in any link will trigger global risks. The legal governance of AI technology risks, as shown in Table 6, should further strengthen the legitimacy of government regulation, follow the principle of human-centeredness, which should be focused on human beings under any AI technology, and any technology that harms human beings should be treated rigorously. Ethical principles should also be followed. Although some technologies may promote social progress, they are contrary to human ethics, such as cloning, and they should be curbed. The governance of AI technology risks is greatly impacted by the implementation of the three. The effectiveness of the three is 0.8, 0.85, and 0.75, respectively.

Table 6. Legal governance of artificial intelligence technology risks

The direction of perfecting the legal governance of technical risk	Strengthen the legitimacy of government supervision	The principle of putting people first	Ethical principles
Specific practices	We will improve the supervision and management system	Human-centered, the role of technology is open	The Tao obeys the bottom line of social morality
The governance effect of technical risk	0.8	0.85	0.75
feature	Regulatory	subjectivity	Bottom linear

Establishing a concept of a risk society and carrying out enhanced regulation is the necessary process of regulation by law. The first step is to strengthen the legitimacy of government regulation. The progress of science and technology is accomplished under the domination of capital power, realizing the elimination of old industries, while the theory of technological supremacy and technological neutrality has been reflected in the case of fast broadcasting ten years ago and today's artificial intelligence is also the same. Human safety can be guaranteed most effectively by strengthening government regulation. Secondly, the principle of risk control should be established, and the modesty of state power should be ensured without hindering technological progress so as to put people at the center and prevent the abuse of power.

4 Conclusion

The emergence of artificial intelligence brings convenience to people and also many security risks. With the prominence of the security risks of artificial intelligence, the law on the safety of artificial intelligence has gradually withdrawn. This paper constructs an artificial intelligence safety index based on the clustering algorithm and formulates legal principles that correspond to different risks. Artificial intelligence's security risks under the clustering score are primarily divided into privacy and technology risks. For the privacy risk problem, this paper puts forward the suggestion that the notification principle should be sound, the privacy protection policy should be improved, especially for minors, and the subject of power should also be further clarified. The degree of perfection of all three legal policies is high, respectively 0.95, 0.85 and 0.9. Improving the privacy protection policy and the rules of the subject's right can govern the privacy risk to a certain extent. In terms of technological risk, this paper proposes the ethical principle as well as the human-centered principle, in which the degree of effectiveness of the ethical principle is 0.75. The implementation of the three is highly effective in managing AI technological risk.

References

[1] Alic, D. (2021). The role of data protection and cybersecurity regulations in artificial intelligence global governance: a comparative analysis of the european union, the united states, and china regulatory framework.

[2] Shearer, E., Cho, M., & Magnus, D. (2021). Regulatory, social, ethical, and legal issues of artificial intelligence in medicine. Artificial Intelligence in Medicine.

[3] Caroline, J., James, T., & Wyatt, J. C. (2023). Artificial intelligence and clinical decision support: clinicians' perspectives on trust, trustworthiness, and liability. Medical Law Review.

[4] Fritz, Z. (2022). When the frameworks don't work: data protection, trust and artificial intelligence. Journal of medical ethics, 48(4), 213-214.

[5] Bilgic, E., Gorgy, A., Young, M., Abbasgholizadeh-Rahimi, S., & Harley, J. M. (2022). Artificial intelligence in surgical education: considerations for interdisciplinary collaborations:. Surgical Innovation, 29(2), 137-138.

[6] Afridi, Y. S., Ahmad, K., & Hassan, L. (2021). Artificial intelligence based prognostic maintenance of renewable energy systems: a review of techniques, challenges, and future research directions. International Journal of Energy Research(2).

[7] An, N., & Wang, X. (2021). Legal protection of artificial intelligence data and algorithms from the perspective of internet of things resource sharing. Wireless Communications and Mobile Computing, 2021(2), 1-10.

[8] Ronquillo, C. E., Peltonen, L. M., Pruinelli, L., Chu, C. H., Bakken, S., & Beduschi, A., et al. (2021). Artificial intelligence in nursing: priorities and opportunities from an international invitational think-tank of the nursing and artificial intelligence leadership collaborative. Journal of Advanced Nursing(9).

[9] Spanjol, J., & Noble, C. H. (2023). From the editors: engaging with generative artificial intelligence technologies in innovation management research—some answers and more questions. Journal of Product Innovation Management, 40(4), 383-390.

[10] Ho, J. H., Lee, G. G., & Lu, M. T. (2020). Exploring the implementation of a legal ai bot for sustainable development in legal advisory institutions. Sustainability, 12(15), 5991.

[11] Van Dijk, N., Casiraghi, S., & Gutwirth, S. (2021). The 'ethification' of ict governance. artificial intelligence and data protection in the european union. Computer Law & Security Review: the international journal of technology law and practice(Nov.), 43.

[12] Zhang, B., Anderljung, M., Kahn, L., Dreksler, N., & Dafoe, A. (2021). Ethics and governance of artificial intelligence: evidence from a survey of machine learning researchers. Journal of Artificial Intelligence Research, 71.

[13] Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: organizing data for trustworthy artificial intelligence. Government Information Quarterly, 101493.

[14] Yee, D. H., & You, Y. Y. (2020). The Impact of Awareness of New Artificial Intelligence Technologies on Policy Governance on Risk.

[15] Grassi, A., & Vallati, M. (2021). An exploratory study on the use of artificial intelligence to initiate legal understanding for business development. Journal of Applied Logic, 8(4), 1065-1082.

[16] Qichun, Yang, Xuesong, Zhang, James, & E., et al. (2019). Artificial intelligence and accountability: a multinational legal perspective. Environmental Pollution.

[17] Jia, Y., & Gu, H. (2019). Sample entropy combined with the k-means clustering algorithm reveals six functional networks of the brain. Entropy, 21(12), 1156.

[18] Qin, X., Li, J., Hu, W., & Yang, J. (2020). Machine learning k-means clustering algorithm for interpolative separable density fitting to accelerate hybrid functional calculations with numerical atomic orbitals. The Journal of Physical Chemistry A, 124(48), 10066-10074.

[19] Tal, G. (2015). Dendextend: an r package for visualizing, adjusting and comparing trees of hierarchical clustering. Bioinformatics(22), 3718-3720.

[20] Nunez-Iglesias, J., Kennedy, R., Parag, T., Shi, J., & Chklovskii, D. B. (2013). Machine learning of hierarchical clustering to segment 2d and 3d images. PLoS ONE, 8(8), e71715.

[21] Envelope, H. J. A. (2022). Impact of information security on continuance intention of artificial intelligence assistant. Procedia Computer Science, 204, 768-774.

[22] Liu, Q., Wang, G., Hu, J., & Wu, J. (2022). Preface of special issue on artificial intelligence: the security & privacy opportunities and challenges for emerging applications. Future Generation Computer Systems, 133, 169-170.