Application and Optimization of Algorithm Technology in the Criminal Governance of Telecom Network Fraud from the Perspective of Data Governance

Jiazhi Yu
Department of Public Security Management, Beijing Police College, Beijing, China

Abstract: As we witness the swift progression of information technology, the issue of telecom network fraud has become increasingly prevalent, posing a significant threat to the well-being of society. Consequently, the prevention of such fraudulent activities has become an urgent matter that requires immediate attention. In this contemporary era, the advancement of algorithm technology in managing telecom network fraud has opened up new avenues and methodologies, offering support to entities combating fraud by enhancing the efficiency of their operations and refining the precision of their preventative measures. However, during the implementation of algorithm technology, the issue of data governance has surfaced and become a topic of public concern. Hence, this paper delves into the analysis of algorithm application and optimization from the perspective of data governance, exploring the synergistic effects of these two elements in the fight against telecom network fraud crimes. The goal is to offer insights that can contribute to enhancing the overall effectiveness of fraud governance strategies.

Keywords: Data Governance Algorithm Technology Telecom; Network; Fraud; Fraud Governance; Governance Effect

1. Introduction

1.1 Research Background and Study Significance

1.1.1 Research Background

With the rapid development of communication network technology, telecom fraud cases occur frequently, and the means of fraud are constantly renovated, which poses a serious threat to the people' s property security and social stability. Traditional anti-fraud propaganda methods, such as posters and household propaganda, have played a preventive role to some extent, but limited to the breadth and depth of propaganda, it is difficult to fully cover all potential victims, and it is difficult to deal with the rapidly changing fraud methods. Therefore, how to use advanced algorithm technology to improve the accuracy and effectiveness of anti-fraud propaganda has become an urgent problem to be solved. As a key link of information management, data governance can realize the comprehensive management and efficient utilization of data through the collection, integration, analysis and application of data. In the anti-fraud propaganda, data governance can provide rich data sources and provide strong support for the application of algorithm technology. At the same time, through data governance, the real-time monitoring and evaluation of the anti-fraud propaganda effect can be realized, providing scientific basis for optimizing the publicity strategy. In addition, with the use of big data analysis, we can more accurately identify the patterns and trends of fraud behavior, so as to develop more targeted preventive measures. Through machine learning and artificial intelligence technology, an intelligent anti-fraud system can be built, which can automatically identify and intercept fraud information and reduce the occurrence of fraud events. In addition, data governance can also help to analyze the distribution of fraud cases and the characteristics of the victim group, so as to provide more accurate decision support for the public security organs to fight against fraud crimes.

1.1.2 Study Significance

One is the theoretical significance. The algorithm technology under the data governance has a higher value to the anti-fraud propaganda. It helps us to get a deeper

understanding of the complexity of combining data governance with algorithmic techniques. Through the in-depth discussion and analysis of the application of the algorithm technology in the anti-fraud propaganda, the research can reveal the key role of data governance in improving the efficiency and accuracy of the algorithm. In addition, this research can also promote academic progress in related fields, and provide new theoretical support and research perspective for the development of data governance and algorithm technology, thus bringing new enlightenment and thinking to the academic and practical circles.

Second, the practical significance. The application and optimization of algorithm technology in anti-fraud propaganda can significantly improve the efficiency and effect of anti-fraud work. Through accurate data analysis and algorithm prediction, potential fraud can be more effectively identified and timely warning information to the public, so as to reduce the incidence of fraud cases. In addition, the research can also promote the intelligence and individuation of anti-fraud propaganda strategies, develop more targeted propaganda programs according to the characteristics and needs of different audiences, and improve the public's awareness and ability to prevent fraud. At the same time, the optimization of algorithm technology can also reduce the cost of anti-fraud work, improve the efficiency of resource utilization, and provide strong support for the long-term sustainable development of anti-fraud work.

1.2 Research Status at Home and Abroad

1.2.1 Status of Domestic Research

At present, the domestic research on the challenges and responses brought about by algorithm technology mainly includes the following aspects:

From the application status of algorithm technology in the field of anti-fraud propaganda. In the article "The Influence of Artificial Intelligence on the Governance of Telecom and Network Fraud", Wei et al. systematically combed the application practice of artificial intelligence technology in the governance of telecom and network fraud, analyzed the risks and challenges brought by its improper use for the governance work, and put forward ideas and suggestions on the basis of summarizing the domestic and foreign governance measures [1]. Wu provides the idea of the governance of telecom network fraud crime to digital, promote the advancement of digital thinking; expand the development path with digital resources; with the support of digital technology; improve the governance ability of electric fraud crime; and further improve the cooperation framework of electric fraud crime governance with digital cooperation as the guarantee [2].

From the optimization level of algorithmic technology. Kou in the people-oriented perspective of artificial intelligence of police ethics in view of the current algorithm technology in the application of police, put forward for the future to establish a people-oriented artificial intelligence policing ethics, the correct use of police artificial intelligence relationship with police officers, to build a complete regulatory framework of artificial intelligence and risk control mechanism, promote police can only better function, safeguard national security [3]. In the article "Ethical Crisis and Legal Regulation of Artificial Intelligence Algorithm", Zheng raised the corresponding problems for the application and development of artificial intelligence from the moral and ethical level, and put forward the corresponding governance methods from the legal level [4].

Research from the level of data governance. In From Algorithmic Crisis to Algorithmic Trust: Multiple schemes and Localization Pways of Algorithmic Governance, Zhang Xin pointed out that the idea of connecting algorithm governance, data governance and platform governance was adopted when improving the algorithm governance scheme. In the article "Ethical Crisis and Legal Regulation of Artificial Intelligence Algorithm", Zheng Zhihang put forward the ternary structure governance of public power, social power and private power, so as to jointly improve the algorithmic data governance.

1.2.2 Status of Foreign Research

Kafhali et al. proposed an intelligent system that uses multiple deep learning architectures (including artificial neural networks, recurrent neural networks, and long and short-term memory networks) to detect fraudulent transactions, and uses Bayesian optimization algorithm for hyperparameter optimization. Through experiments on the credit card fraud transaction dataset, we prove that the recurrent

neural network architecture performs better in efficiency and results [5].

In The power of big data affordances to reshape anti-fraud strategies, Gianluca et al. in the era of big data, the explosion of data volume and the diversification of data types bring opportunities for anti-fraud work. Big data contains not only traditional structured data (such as transaction records, customer information), but also unstructured data (such as social media activities, web logs, etc.). This wealth of data provides the basis for building a more accurate anti-fraud model. Through the analysis of data integration and association, analysis and monitoring, and application, it points out the role of big data on anti-fraud strategy, and summarizes its significance to anti-fraud propaganda.[6]

In August 2024, the National Bank of Malaysia launched the national anti-fraud platform. When people encounter fraud, just by dialing the relevant number, the national anti-fraud platform will be launched to help victims track the flow of funds in time and transmit the relevant information to financial institutions so that they can take necessary measures. The platform uses technologies such as artificial intelligence to identify suspicious transactions faster and speed up execution. There are currently 16 financial institutions involved. The Belgian Network Security Center has created a "Safe Net" website to quickly access Internet security information and advice, including tips to install the latest software updates and how to strengthen personal information protection when selling or buying goods on the Internet.

2. Impact of Data Governance on the Application of Algorithm Technology

2.1 Impact of Data Quality on the Algorithm Application

2.1.1 Accuracy of the Data

The accuracy of data is the basis of telecom network fraud management. In the anti-fraud propaganda, the calculation technology relies on accurate data to identify fraud patterns, predict fraud behavior, and develop effective publicity strategies. If the data is inaccurate, such as the recording of fraud cases, then the model trained on these data may produce misleading results, causing the failure of anti-fraud propaganda strategies. For example, if data on scam phone numbers are incorrect, then call interception systems based on these data may be unable to correctly identify and intercept scam calls, thus reducing the effectiveness of governance. Therefore, ensuring data accuracy is crucial to improve governance effectiveness.

In addition, the accuracy of the data also directly affects the stability and reliability of the algorithm model. In the practice of anti-fraud propaganda, the algorithmic model needs to be constantly learned and updated to adapt to the new fraud means and trends. If the input data is not accurate, the algorithm model may learn the wrong information during the training process, leading to the bias of the model in predicting and identifying the fraud behavior. This deviation will not only reduce the effect of the anti-fraud propaganda, but also may mislead the public, making people doubt and distrust the anti-fraud propaganda.

2.1.2 Integrity of the Data

The integrity of data is also crucial to the effectiveness of telecom network fraud governance. A complete data set can provide a comprehensive perspective to help analyze the overall picture of fraud, so as to develop a more comprehensive anti-fraud strategy. If the data set is missing, such as some fraud cases are not recorded, then the computing technology may ignore these unrecorded fraud patterns, resulting in anti-fraud propaganda can not cover all potential types of fraud. For example, if data on a particular type of online fraud case is missing, promotional materials for this type of fraud may not be developed, raising the public's awareness of this kind of fraud. Therefore, maintaining data integrity is a key factor in improving governance effectiveness.

To achieve data integrity, a series of measures are needed to ensure data completeness and no omission. First, a strict data collection process should be established to ensure that all related fraud cases can be timely and accurately recorded. This includes strengthening the construction of data collection channels, improving the professionalism of data collectors, and the adoption of advanced data collection techniques. Second, the data should be reviewed and updated regularly to reflect the latest fraud methods and trends. This helps to ensure the timeliness and accuracy of the data set, thus enhancing the pertinence and

effectiveness of anti-fraud propaganda.

2.1.3 Reliability of the Data

The reliability of data is the guarantee of the successful implementation of telecom network fraud governance. Data with high reliability can ensure the accuracy of calculation techniques in prediction and decision making, thus improving the effectiveness of governance. In the management of telecom network fraud, the algorithm needs to obtain data from a variety of channels, such as the case records of the police, the transaction data of financial institutions, the communication records of telecom operators, and the reporting information of users on social media. The data quality of these different channels is uneven. For example, reports on social media can be exaggerated, misjudged, or incomplete. Users may be angry or panic, adding personal emotions and speculation when describing the fraud process, resulting in information distortion. Moreover, the data formats and standards from different channels are also inconsistent. Police records may be followed by strict legal procedures and professional jargon, while users' descriptions on social media may be colloquial and casual. This difference increases the difficulty of data integration and cleaning, and affects the data quality.

2.2 Influence of Data Security on the Algorithm Application

2.2.1 Data Privacy Protection

In the digital society, algorithm technology has become a key variable in the development of The Times. Through the database operation platform established by the technical mechanism of information content recommendation, production and collaborative filtering, it can comprehensively integrate the language and psychological analysis of algorithm technology, and carry out targeted transmission to users one by one. In the long run, algorithmic technology may replace the human subjectivity position, and even unlimited access to people's thinking. For example, the generative pre-trained transformation model (ChatGPT) is better than the search engine, which is changing the above risks from possible to reality. Chat GPT Through human-machine interaction with users, continuous data collection and self-training, for example, in the case of Internet users input business sensitive information or personal user information, the system will summarize the above data into the database, which will produce the risk of information leakage [7].

In the current anti-fraud propaganda, the application of algorithm technology has become an important means to improve data security and prevent fraud. In this work, a large number of data containing personal sensitive information (such as victim identity information, bank account number, contact information, etc.) and fraud details need to be stored. If the security measures of the storage system are not in place, such as the database does not have a proper encryption mechanism, and the access control permission setting is not reasonable, the hackers may obtain these data through network attacks. For example, the vulnerability of the database can be used to conduct SQL injection attacks to steal the user information stored in the database. Once these information is leaked, it will not only violate personal privacy, but also may be used by fraudsters, leading to more serious fraud incidents.

When analyzing the data, the algorithms may mine for more information by correlating different data points. In the scenario of telecom network fraud governance, this may over-dig personal privacy. For example, an algorithm may correlate a person's consumption habits, social relationships, and possible scams to produce a very detailed personal portrait. If the portrait is used improperly, such as used for commercial purposes or obtained by other unrelated agencies, it can violate personal privacy.

2.2.2 Data Security Awareness

Yuval Harari, author of A Brief History of Humanity, once said, " Data may become the ultimate weapon to dominate the human destiny." From the perspective of the process of crime implementation, telecom network fraud includes accurate information acquisition, fraud script design, communication guidance, fund payment and transfer of four key links. Fraud relies on fraud scripts, and the accurate acquisition of the victims' personal information is the premise of the design of fraud scripts, but also the root cause of telecom network fraud [8].

In the telecom network fraud management, a large number of personal sensitive information

(such as victim identity information, bank account number, contact information, etc.) and fraud details of the data need to be stored. If the security measures of the storage system are not in place, such as the database does not have a proper encryption mechanism, and the access control permission setting is not reasonable, the hackers may obtain these data through network attacks. For example, the vulnerability of the database can be used to conduct SQL injection attacks to steal the user information stored in the database. Once these information is leaked, it will not only violate personal privacy, but also may be used by fraudsters, leading to more serious fraud incidents.

Data is transmitted between different institutions (such as police, financial institutions, telecom operators, etc., etc.) to control telecom network fraud. If the data transmission does not use a secure encryption protocol (such as SSL / TLS), it may be intercepted during the transmission process. For example, through a man-in-the-middle attack, an attacker can steal the data being transmitted to obtain sensitive information in the data.

In addition, data is at risk of internal leakage during storage and transmission. Some criminals may use their positions or authority within the agency to illegally access, copy or leak such data. This behavior not only violates professional ethics and laws and regulations, but also poses a serious threat to personal privacy and data security. Therefore, strengthen the awareness of data security, to ensure the security of the data storage, transmission and processing process, for the entire data governance, power algorithm technology in the governance of telecom network fraud plays an important role.

2.3 Influence of Data Sharing on the Algorithm Application

2.3.1 Increase of Data Scale

At present, most public security departments are expanding the scope of their resources and improving the priority of their departments. Due to the different launching division of labor, the scope of the jurisdiction is not exchange, if the use of artificial intelligence to information monopoly, makes the police information cannot organization between various departments and harmony, in the definition of the problem, decision-making and execution process, because of artificial manipulation of a closed space, can not really achieve information sharing, it is easy to appear information asymmetry, form information barriers [9].

In order to solve this problem, it is necessary to establish an effective data sharing mechanism, break down the information barriers, and realize the information sharing among various police departments. This can not only improve the efficiency of data use, but also avoid decision-making errors and waste of resources caused by information islands.

At the same time, data sharing is not only limited to the public security organs, the sharing between the public security organs and enterprises and institutions is also very important, which is conducive to the elimination of data islands, and greatly expands the amount of data that can be used for the governance of telecom network fraud. Although the amount of data of a single institution may be small, many institutions share data and converge into a huge data resource database.

Extensive data is crucial for the training and optimization of algorithms. During the training process, the increase of the amount of data allows the algorithm to learn more diverse patterns and features, which helps to improve the generalization and accuracy of the algorithm. At the same time, a large amount of data helps the algorithm to better converge during training, reduce the risk of falling into the local optimal solution, and then obtain a better algorithm model.

The expansion of the data scale also provides more space for the algorithm optimization. By analyzing and mining large-scale data, researchers are able to identify shortcomings of the algorithms and propose improvements. For example, after analyzing a large amount of fraud case data, researchers may find that the algorithm is not very accurate in identifying new fraud methods. To address this problem, researchers can use large-scale data containing new fraud cases to improve the algorithm and enhance their ability to identify new fraud, so as to improve the overall effectiveness of the algorithm.

2.3.2 Fuzzred Data Standards

In the process of cross-institutional data

sharing, due to the lack of unified data sharing standards and norms, different institutions have significant differences in data formats, definitions, interfaces and transmission protocols, which brings great challenges to data sharing and integration, and thus affects the collaborative application of algorithms in cross-institutional scenarios.

Taking the data format as an example, different institutions may take different approaches to record and preserve the data. For example, some financial institutions may prefer to use relational databases to keep customers' transaction records, with data organized in tables, each containing specific fields and records. In contrast, some Internet companies may prefer to use non-relational databases (such as NoSQL databases) to save users' behavioral data, and the data exists in the form of documents, key values, etc., providing greater flexibility and scalability. The inconsistency of these data formats makes the complex data transformation and mapping work necessary for the data of different institutions when sharing and integration, thus increasing the difficulty and cost of data processing.

In terms of data definition, different institutions may have different definitions and understandings of the same data element. Taking the data element of "customer age" as an example, some organizations may be defined as the current actual age of the customer by a year; while others may be defined as the age at a specific point in time, or in different ways (e. g., the age by the lunar calendar). The inconsistency of data definition will lead to data misunderstanding and conflict in the process of data sharing and integration, and affect the accurate analysis and application of the algorithm.

3. Optimized Application of the Algorithm Technology

3.1 Application Scenarios of the Algorithm Technology

3.1.1 Fraud Telephone Detection

The algorithm technology can identify the abnormal behavior different from the normal call mode by analyzing the characteristics of the call time, call time and call frequency. For example, scam calls tend to be short for calls, but may be more frequent and will call multiple different numbers in a short time.

With the continuous development of artificial intelligence and deep learning technology, more and more algorithms are applied to the detection of fraudulent calls, such as deep neural network (DNN), which can train a large amount of historical data to learn the characteristic mode of fraudulent calls, and realize the real-time detection and classification of new calls. This method has high accuracy and adapts to different kinds of scam calls; the recurrent neural network (RNN) performs well in processing sequence data, suitable for analyzing voice content in phone calls. By combining speech recognition technology, RNN can extract key information, such as keywords, and intonation, to determine whether the call involves fraud. Support Vector Machine (SVM) is a machine learning method that is suitable for high-dimensional data and nonlinear problems. In scam call detection, SVM can distinguish normal and fraudulent calls from fraudulent calls by building classification models.

3.1.2 Malicious Website Interception

The algorithm technology can be based on the data sample library, using the machine learning algorithm and big data platform to carry out feature comparison and detection, page similarity analysis of massive websites, and find and intercept suspected fraudulent websites [10]. By analysis of url character combination, length, special character features, analyze the text of the website page, pictures, links, observe the site access behavior pattern, such as access frequency, access time distribution, associated with other sites access to determine whether the site involves gray industry, whether belong to malicious website, and after determining the user to timely remind, and intercept the visit.

The most widely used malicious site interception technology is the Web Application Firewall (WAF). WAF is the first line of defense between applications and Internet traffic, blocking undesirable traffic and malicious requests by monitoring and filtering Internet traffic. WAF uses a number of methods to prevent malicious attacks, including IP fences, geo-fencing, checking request content, analyzing HTTPS traffic, and checking HTTP request headers. WAF can also decode and analyze various data transfer formats, such as XML, JSON, etc., to detect

and prevent potential threats.

3.1.3 Fraud Information Monitoring

Through the use of natural language processing technology and related algorithms, the text content of the fraud information in-depth analysis, extract such as keywords, semantics, emotional tendency and other characteristics. For example, inducing keywords such as "winning", "tax refund" and "emergency transfer" often appear in fraudulent text messages. The algorithm determines the suspicious degree of information by identifying these keywords and their combination patterns.

In practical application, the algorithm technology has achieved remarkable results. For example, some banks use deep learning technology to explore anti-fraud, and significantly improve the accuracy and efficiency of fraud detection by building aggregation models with a variety of deep learning models, including CNN and LSTM. In addition, the intelligent public security bureau also uses algorithm technology to conduct real-time monitoring and multi-dimensional display of the police situation data, realizing the rapid positioning and crackdown on fraudsters.

3.1.4 Establishment and Update of Fraud Information Database

In order to establish a comprehensive fraud information database, it is necessary to collect data from a variety of channels. Web crawler algorithm can be used to collect public fraud cases, fraud warning information issued by government departments, and fraud experiences exposed by users on social media platforms. For example, by setting appropriate keywords (such as "fraud", "network fraud", "fraud", etc.), the web crawler can traverse the relevant web pages and extract the types of fraud, fraud means, victim characteristics and other information.

For a large amount of text information collected (such as fraudulent SMS content, fraudulent website speech, etc.), the text classification algorithm in natural language processing can be used for classification. For example, the fraud information is divided into investment and financial fraud, fake public security law fraud, part-time fraud and other different categories. First, the classification model is built by training the text of known fraud categories, and then the newly collected text information is input into the model for classification. For example, for a text message saying, "Congratulations on you for winning a huge lottery ticket, click on the link to get the prize money," the text classification algorithm can classify it as a winning fraud category.

After a series of processing, classification, marking of fraud information stored in the database, the formation of fraud information database, and continue to update the data source according to the promotion of fraud means, the diversification of fraud methods, expand the information of the information database, enhance the coverage of fraud information.

3.2 Optimization of the Algorithm Technique

3.2.1 Efficient Identification of Fraud Information

In the process of carrying out anti-fraud propaganda, the algorithm technology often makes mistakes in identifying fraud information. For example, if the fraudulent information is replaced by words, it may evade the identification of the detection system, resulting in the failure to classify it as fraudulent information, thus affecting the comprehensiveness of the anti-fraud work.

In the optimization of algorithm technology, we should continue to deepen the recognition ability of algorithm technology, so that the detection system can be more intelligent and efficient to identify all kinds of fraud information, such as deep learning algorithm, especially deep neural network, because of its powerful pattern recognition ability, can significantly improve the recognition accuracy of fraud information. By training the deep neural network model, it can learn the feature representation of the fraud information, so as to realize the rapid and accurate identification of the new fraud information. In addition, natural language processing technology can also be combined to conduct semantic understanding and emotional analysis of text content to further improve the recognition effect. For example, by analyzing the keywords, phrases and sentence structures in the text, as well as the emotional tendencies expressed in the text, the authenticity of information and fraud intentions can be more accurately judged.

At the same time should pay attention to the

comprehensive application of other technologies, such as NLP technology, it can be used to analyze the text content in the fraud information identification, identify keywords, sentence patterns, in the ability of semantic understanding, can help algorithm more accurately grasp the meaning of the text and context, reduce the misjudgment caused by context differences. In addition, the image recognition technology can also be introduced to identify and analyze the text, QR code and other key information in the picture, so as to identify the potential risk of fraud. Through the comprehensive use of a variety of technologies, a more comprehensive and efficient fraud information identification system can be built to improve the accuracy and efficiency of anti-fraud work.

3.2.2 Precise Implementation of Anti-fraud Push

The push of anti-fraud information plays an important role in the prevention of fraud propaganda work. However, in the process of push, due to the incomplete user information and the inconspicuous characteristics of fraud, the accuracy of anti-fraud push is often insufficient, resulting in the waste of human and material resources, affecting the efficiency and accuracy of anti-fraud work.

In terms of algorithm recommendation, the public security organs innovate and improve from the two aspects of anti-fraud message push and interactive learning. According to users' personal information and behavior habits, they use algorithm technology to push personalized anti-fraud knowledge. This helps to improve users' attention and acceptance of anti-fraud information, and enhance their anti-fraud awareness. At the same time, the algorithm can use the algorithm technology to push the personalized anti-fraud knowledge according to the user's personal information and behavior habits. This will help to improve users' attention to and acceptance of anti-fraud information, enhance their awareness of anti-fraud, develop intelligent anti-fraud learning and testing platform, and guide users to participate in learning and testing through gamification. This method not only increases the interest of learning, but also improves the learning effect and user participation.

In the current social security management, some local public security organs have begun to adopt an innovative technical means —— to introduce AI digital employees. These AI digital employees can automatically obtain anti-fraud warning lists and actively dial out warning calls by simulating the way humans interact with the business. This intelligent push method not only greatly improves the work efficiency, but also effectively reduces the risk of omission caused by human operation error or negligence.

3.2.3 Focus on Improving Risk Monitoring

Risk monitoring is the beginning link of anti-fraud work. Only by doing a good job in risk monitoring can we establish the leading direction for the follow-up work process and formulate the corresponding anti-fraud strategy. If the failure to more efficiently identify the current fraud risk, it may lead to the occurrence of fraud and unable to timely respond.

Algorithm technology can use big data analysis and machine learning algorithms to monitor and analyze a large amount of data in the network in real time, including user behavior data, transaction data, etc., so as to dig out potential fraud. For example, deep learning algorithms can quickly identify and process a large amount of data, analyze user behavior and historical cases for pattern recognition, so as to improve the accuracy of anti-fraud. At the same time, the machine learning model can also continuously learn the emerging fraud cases and optimize its recognition ability, so that the anti-fraud system can respond more quickly in the face of new fraud methods.

At the same time, it can also use algorithm technology to be used to build anti-fraud knowledge graph, and graph algorithm can be used to build multi-dimensional correlation between fraud behaviors, mine potential connections between behaviors, and realize cross-domain detection. This can not only summarize the characteristics of various kinds of fraud, reproduce the evolution process of various "routines", but also can reason, predict and identify new fraud means, helping to prevent and fight network fraud in advance.

In addition, the algorithm technology and the traditional risk control means are combined to form a complete set of risk monitoring system. For example, in the account opening process, the applicant can assess the risk through algorithm technology, and formulate differentiated account opening strategies and

restriction measures; in the transaction process, real-time risk monitoring rules can be deployed to conduct real-time monitoring and early warning of suspicious transactions; during the duration, construct the post-risk monitoring model to comprehensively check the risk of stock account, realize the risk monitoring without dead corners and avoid fraud to the greatest extent.

4. Synergy between Data Governance and Anti-Fraud Technology

4.1 Improve Data Wellbeing

4.1.1 Protect the Data Security

Data security in the whole telecom network fraud management work is a concern by most people, only to ensure the data security to ensure that the governance work is effectively implemented in place. In the collaboration of data governance and anti-fraud technology, differential privacy (Differential Privacy) technology can be used to protect data security.

First, differential privacy techniques protect personal privacy by introducing noise into the data. The noise mechanism can introduce subtle interference in the process of data release or retrieval to blur the identity of individual users, ensuring that even if the processed anonymous data is obtained, the real identity of personal information cannot be analyzed by any means. This can not only effectively avoid the potential risk of data leakage, but also effectively protect the privacy rights of each user.

Secondly, the differential privacy technology can provide users with more reliable and confidential data processing services in practice. For example, in anti-fraud propaganda efforts, user behavioral data can be collected and analyzed to identify potential fraud patterns. However, direct analysis of this data may compromise personal privacy. Through the application of differential privacy technology, the data can be effectively analyzed while protecting personal privacy, so as to identify the fraud behavior.

Finally, to fully leverage the advantages of differential privacy technologies, a balance between data privacy and data availability is needed. The size of the added noise can directly affect the privacy and availability of the data. Therefore, the size of the noise according to the specific situation to ensure that while protecting privacy, data is still available enough to support the governance of telecom network fraud.

4.1.2 Break through the Information Cocoon Room

Information cocoon room refers to the phenomenon that people's information field will be habitually guided by their own interests, thus shackling their own life in the "cocoon room" like a silkworm cocoon. In the anti-fraud propaganda work, the information cocoon room may lead to the public contact with the anti-fraud information is limited. As a technical means, the algorithm can play a role in reconstructing the public environment and regulating people's behavior. The accuracy of the algorithm not only facilitates the people to obtain information quickly, but also shapes the cognitive structure of individuals, so that people stick to their own information cocoon and gradually "domesticated" by the algorithm [11].

In the information cocoon, individuals or communities often only contact and consume information that is similar or consistent with their views, but ignore or reject information with different views. This behavioral pattern of selective exposure to information may lead to the limitation of public exposure to anti-fraud propaganda information, especially when the information is inconsistent with their existing views or interests. As a result, anti-fraud propaganda may be difficult to effectively reach those potential victims in the information cocoon.

The most basic point to break through the information cocoon is to strengthen the collection of data diversity. Through a variety of data collection, integration and analysis, we can more comprehensively understand users' needs and information preferences, so as to push more diversified information. Algorithm technology from the user behavior data, transaction data, social data, external data, biometric data, equipment data, biological crawler, data sources through different data sources of data integration, eventually form a real and complete information, build user portrait, for the algorithm of accurate fraud propaganda to provide the correct goal, indicate the way.

At the same time, in order to break through the information cocoon, it is necessary to promote

the optimization and upgrading of the algorithm to achieve the balance between personalization and diversity. On the one hand, the algorithm should be personalized according to the interests and preferences; on the other hand, the algorithm should also pay attention to the diversity and comprehensiveness of information to avoid users being bound by a single information source. In addition, the transparency and interpretability of the algorithm should be enhanced to ensure that users can understand the operation mechanism and recommendation logic of the algorithm, so as to more effectively grasp their own information consumption habits and ensure the actual implementation of anti-fraud work.

4.2 Innovative Algorithm Technology

4.2.1 Enhance the Technical Basis

Only when computers absorb a lot of data can algorithms run and learn and evolve. The algorithm can transform and control the data, so as to form a "quasi-public power", which is an important reason for the alienation of the algorithm [12]. The quality of the data is crucial for the optimization of the algorithm. As a means of management, the core goal of data governance is to provide accurate, comprehensive, consistent and updated data in real time, which is crucial to ensure that the algorithm can obtain more reliable information in the training and optimization stage. Through data governance, we can ensure the quality and consistency of the data, so as to provide a solid foundation for the algorithm, and thus improve the efficiency and accuracy of the algorithm. For example, when optimizing the natural language processing algorithm used to identify fraudulent information, data governance ensures that the training dataset contains accurate fraudulent text information under multiple types and multiple scenarios, as well as the corresponding normal text information as controls. These high-quality data enable the algorithm to learn the linguistic characteristics, patterns and rules of fraudulent information more deeply, thus improving the identification accuracy and recall rate of fraudulent information by the algorithm.

At the same time, with the continuous update and accumulation of data, data governance can timely incorporate new data into the training process of the algorithm, so that the algorithm can constantly adapt to the new fraud means and change trends, and continuously optimize the efficiency and effect of the algorithm. Therefore, data governance not only plays a key role in the early stage of algorithm optimization, but also plays an indispensable role in the whole life cycle of the algorithm, ensuring that the algorithm can continuously provide accurate and efficient services.

4.2.2 Optimization Algorithm Logic

Optimizing the logic of the algorithm from the technical level can effectively improve the identification accuracy of telecom network fraud, reduce the consumption of the algorithm resources, and enhance the overall adaptability of the algorithm. By optimizing the algorithm, more accurately identify and intercept fraudulent calls, text messages and emails, reduce false and underreporting. While ensuring the identification accuracy, it can also reduce the consumption of computing resources and storage resources, constantly adapt to the changing fraud techniques and modes, and maintain its long-term effectiveness.

In terms of optimization logic, we should first optimize from the most basic data collection, constantly collect multi-dimensional data, including users' age, gender, occupation, region, consumption habits, social network behavior and other information, and integrate these data to form a complete user portrait database. The algorithm logic is optimized based on a more complete database.

The optimization of algorithm logic should start from two aspects of propaganda subject and propaganda audience. The subject of publicity should make full use of and improve the feature selection technology, select the most representative features among the collected data as "data labels", and more accurately identify all kinds of fraud activities, so as to improve the identification ability of the algorithm and prevent the occurrence of omission, misjudgment and misjudgment. At the audience level, the government should fully grasp the content and time of personalized push, and formulate personalized sorting rules of content. In addition to considering the user's interests and risk factors, the timeliness and importance of the content can also be combined. For example, for the new fraud methods, such as the new AI face change fraud, no matter how the user's

previous preferences are, the relevant publicity content will be pushed in priority. At the same time, choose the right push time. Analyze the daily behavior and habits of users to determine the best push time. For example, for office workers, they can choose to push at 7-9 PM, because they may have time to check their mobile phone information; for students, they can push on weekends or holidays to improve the reception rate of promotional content.

4.3 Improve the Anti-Fraud Efficiency

4.3.1 Accurate Anti-fraud Propaganda

With the dual assistance of data governance and algorithm technology, the public security organs can perform the anti-fraud propaganda task more accurately and more efficiently. Through the comprehensive collection and analysis of multi-source data, the algorithm technology can accurately build user portraits. Data governance through the integration of the user's multidimensional information, including basic demographic information (such as age, gender, occupation, etc.), consumption behavior data (such as shopping preference, consumption amount, consumption frequency, etc.), network behavior data (such as browsing records, search keywords, social platform activities, etc.), communication behavior data (such as the duration, call object, SMS frequency, etc.), the use of data mining and machine learning algorithm for in-depth analysis of the data and processing, build an accurate user portrait. For example, by analyzing the shopping records of users on the e-commerce platform, grasp their product preferences and consumption ability, understand users 'social circle and interests by analyzing the social platform, and analyzing the communication behavior data, master users' communication habits and important contacts. The integration and analysis of these multi-dimensional information can build a comprehensive, detailed and accurate portrait for each user, clearly depicting the users' behavior patterns, interests and hobbies, consumption habits, risk preferences and other characteristics.

Based on the accurately constructed user portrait, the algorithm technology can select the most suitable personalized anti-fraud content for each user from the rich anti-fraud publicity resource database according to the specific needs, interests and risk status of the users, and accurately push these content to the users through appropriate channels. For example, for users who frequently conduct online shopping, the algorithm can recommend prevention knowledge about online shopping fraud, such as false website identification, payment security precautions, etc. For older users who have little financial knowledge, the algorithm can push some simple and understandable financial fraud prevention content, such as common means of illegal fund-raising, prevention points of pension fraud, etc. For users who prefer using social media, the algorithm can recommend some case analysis and prevention suggestions on social media fraud, such as posing as friends fraud, false winning information fraud, etc. At the same time, the algorithm can also continuously optimize the personalized push strategy according to the user's feedback and behavior data, improve the pertinacity and effectiveness of the push content, enhance the user's attention and acceptance of anti-fraud propaganda, so as to achieve personalized anti-fraud prevention, improve the user's own anti-fraud ability and prevention awareness.

4.3.2 Optimize Resource Allocation

The connection governance of data and algorithm not only conforms to the design law of algorithm, but also gives users the basis of choice and action in the process of operation [13]. Under the joint action of data governance and algorithm technology, the resource allocation in the telecom network fraud governance work has become more reasonable. On the one hand, the algorithm technology can use the data analysis to predict the resource allocation. Data management is responsible for collecting and sorting out all kinds of data related to anti-fraud work, including historical fraud case data, police resources allocation data, publicity resources input data, technical equipment use data, etc. Through the in-depth analysis of these data, the use of data mining, machine learning and other technical means, to build a resource demand prediction model. For example, on the basis of historical fraud cases time, place, type, scale, combined with the current social and economic situation, policy and regulations changes, technology development trend and other factors, predict the future for a period of time in different regions, different types of fraud cases probability and size, to infer the corresponding

police resources, propaganda resources, technical equipment against cheat resources demand quantity and types.

On the other hand, intelligent algorithms promote the optimal allocation of resources. Based on the resource demand prediction results, the algorithm technology using intelligent optimization algorithm, such as linear planning, integer planning, genetic algorithm, simulated annealing algorithm, etc., considering the goal of fraud work, tasks, resource constraints and different regions, different types of fraud cases risk and priority factors, develop the optimal fraud resource allocation scheme. For example, for areas with high incidence of fraud cases and high degree of risk, the algorithm can give priority to more police resources for patrol prevention and control and case investigation, increase the investment of publicity resources, carry out various forms and well-targeted anti-fraud publicity activities, improve the anti-fraud awareness and prevention ability of local residents; for fraud types of new fraud methods and high technical content, the algorithm can focus on allocating technical equipment resources and professional and technical personnel, strengthen the research and analysis of new fraud technologies, develop targeted anti-fraud technical tools and solutions, and improve the ability to identify and prevent the new fraud methods. Through intelligent algorithm to promote the optimization of resource allocation, can make the limited anti fraud resources more reasonable and efficient utilization, maximize the role of resources and efficiency, improve the overall efficiency of fraud, effectively combat and prevent all kinds of fraud crime, protect the people's property safety and the stability of social harmony.

5. Conclusion

With the increasingly rampant telecom network fraud, algorithm technology is playing a more and more important role in the management of telecom network fraud, and data governance plays a crucial role in the application and optimization of the whole algorithm technology. It provides the guarantee and support for the accuracy, integrity and reliability of the data, and through the role of data quality, security and sharing, constantly promote the algorithm technology to play a better role in the governance of telecom and network fraud. Data governance ensures the high quality of the data and provides accurate input to the algorithm, thus improving the output quality of the algorithm. At the same time, data governance also ensures the security of data, prevents data leakage and abuse, and provides a safe environment for the application of algorithm technology. In addition, data governance also promotes the sharing of data, making the algorithm technology can make better use of various data resources, and improve the efficiency and effect of the algorithm.

Algorithm technology has a wide application in telecom network fraud governance for fraud phone detection, fraud website interception, fraud information monitoring, fraud early warning and fraud information database establishment and update and other specific scenarios, and with the continuous improvement of data governance efficiency, its application form and efficiency are also constantly optimized. Through more perfect scientific data, establish a perfect mechanism and quote new technical methods to guide the development of anti-fraud work. For example, through machine learning and artificial intelligence technology, fraud calls and malicious websites can be identified and intercepted more accurately, through big data analysis technology, can more effectively monitor and warn fraud information, through data mining technology, fraud information database can be better established and updated. Through the collaborative operation of data governance and algorithm technology, data governance continues to provide support and guarantee for algorithm technology, optimizes the application of algorithm technology, algorithm technology also provides solutions for data governance, makes the direction of governance clearly, so that data can be better applied to anti-fraud activities. Under the interaction of the two, the anti-fraud work can realize accurate anti-fraud propaganda and optimize the allocation of resources, and improve the anti-fraud efficiency. For example, through data governance, the patterns and characteristics of fraud can be better identified and analyzed, providing more accurate training data for the algorithm technology, so as to improve the identification and prediction

ability of the algorithm. At the same time, the algorithm technology can also provide more effective data processing and analysis methods for data governance, and improve the efficiency and effect of data governance.

In short, from the perspective of data governance, the application basis of algorithm technology in telecom network fraud governance is constantly enhanced, the technology is constantly innovated, and the effect is constantly improved. Only by making the data governance and algorithm technology fully integrated, can we better play the technical efficiency, make the anti-fraud work constantly deepen, and better solve the current problem of rampant telecom network fraud. The integration of data governance and algorithm technology can not only improve the efficiency and effect of anti-fraud work, but also provide useful reference and inspiration for data governance and algorithm application in other fields.

Acknowledgement

The project name of this article is "Research on the Application and Impact of Algorithm Technology in Precise Anti-Fraud Publicity". This work was supported by the 2024 National Innovation and entrepreneurship training program for college students (02). The supervisor of this paper is Professor Li Danyang, an associate professor in the Department of Public Security Management of Beijing Police College. She has put forward a lot of guidance on the writing of this article.

References

[1] Wei Wei, Shang Tieli, Zhou Shuai. The influence of artificial intelligence on the management of telecom network fraud and its coping ideas. Information and communication Technology and Policy, 2020, (04): 80-84.

[2] Wu Dan. Under the background of artificial intelligence, telecom and network fraud crime pattern and digital governance. Public Security Research, 2024, (10): 87-97.

[3] Kou Jianbo. Artificial intelligence policing ethics from a people-oriented perspective. Journal of the People's Police University of China, 2023, 39 (04): 31-40.

[4] Zheng Zhihang. Ethical crisis and legal regulation of artificial intelligence algorithm. Social Science Digest, 2021, (04): 74-76.

[5] [Kafhali E S, Tayebi M, Sulimani H. An Optimized Deep Learning Approach for Detecting Fraudulent Transactions. Information, 2024, 15(4):227-.

[6] Gianluca Gabrielli, et al. "The power of big data affordances to reshape anti-fraud strategies." Technological Forecasting & Social Change 205. (2024):123507-.

[7] Thunderstorm Xin, Ai Zhiqiang. Control and governance: algorithmic technical risk and its response. Journal of Liaoning Polytechnic University (Social Science Edition), 2024, 26(03):5-7. DOI:10. 15916/j.issn1674-327x. 2024.03. 002.

[8] Yang Shengqin. The influence of AI on the criminal governance of telecom network fraud from ChatGPT. Research on Crime and Transformation, 2024, (05): 26-33.

[9] Yang Huan. Application of artificial intelligence technology and risk regulation in police work. Journal of Liaoning Police College, 2024, 26 (01): 83-88.

[10] Wei Wei, Shang Tieli, Zhou Shuai. The influence of artificial intelligence on the management of telecom network fraud and its coping ideas. Information and communication Technology and Policy, 2020, (04): 80-84.

[11] Zhang Aijun and Wang Hang, Algorithm: A New Form of Power, Research on Governance Modernization, no. 1, 2020

[12] Zhang Aijun, Li Feng, Algorithm Power in the Era of Artificial Intelligence: Logic, Risk and Regulation, Journal of Hohai University (Philosophy and Social Sciences Edition), no. 6, 2019

[13] Xin Zhang. From algorithmic crisis to algorithmic trust: multiple solutions and localization path of algorithmic governance. Journal of East China University of Political Science and Law, 2019, 22 (06): 17-30.

