Privacy Protection and Bias Challenges of Algorithmic Technology in Police Anti-Fraud Propaganda

Linhetian Zhong*
Beijing Police Academy, Beijing, China
**Corresponding Author.*

Abstract: This study examines the privacy protection and bias challenges of algorithmic technology in public security anti-fraud propaganda. Through literature review and case study, it reveals the issues of data privacy and algorithmic bias, and proposes research methods. The application value of algorithms in data collection, model construction, content optimization, and platform construction is described. In view of the problems of privacy security, bias, information cocoon and transparency, the improvement paths of perfecting specification, constructing fair model, promoting information diversity and strengthening supervision are proposed to provide reference for future anti-fraud propaganda.

Keywords: Anti-Fraud Propaganda; Algorithmic Technology; Privacy Protection; Bias

1. Introduction

1.1 Research Background and Significance

With the rapid development of the Internet and artificial intelligence technology, public security organs have begun to widely apply algorithmic technology in anti-fraud propaganda to improve the accuracy and effect of propaganda. Algorithmic technology, through the analysis of big data, can identify high-risk groups and realize accurate propaganda, thus effectively reducing the occurrence of fraud cases. However, with the in-depth application of algorithmic technology, the issues of privacy protection and algorithmic bias have gradually come to the fore. On the one hand, the application of algorithms relies on the collection and analysis of a large amount of personal data, which may violate the privacy of users; on the other hand, algorithmic models trained on the basis of historical data may produce bias, affecting the impartiality of propaganda. Therefore, studying the privacy protection and algorithmic bias of algorithmic technology in anti-fraud propaganda is not only of great significance for safeguarding citizens' privacy rights and promoting cyberspace clarity, but also provides theoretical support for enhancing the scientificity and effectiveness of anti-fraud propaganda. This study aims to analyze the current situation of the application of algorithmic technology, explore the challenges of privacy protection and algorithmic bias, and put forward suggestions for improvement, so as to provide theoretical guidance and practical references for public security organs, and to promote the integration and development of anti-fraud work and informationization construction.

Currently, scholars at home and abroad have conducted extensive research on the application of algorithmic technology in anti-fraud propaganda. Foreign research mainly focuses on the optimization of algorithmic models and the development of privacy protection technology, such as the application of differential privacy and federated learning, aiming to improve the accuracy of the algorithm while protecting user privacy. Domestic research pays more attention to the practical application effect of algorithms in anti-fraud propaganda, especially how to identify high-risk groups through algorithms and carry out accurate propaganda in the context of big data. However, there are still some shortcomings in the existing studies: first, the combination of privacy protection and algorithmic bias is less studied and lacks systematicity; second, the specific solutions for algorithmic bias mostly stay at the theoretical level, and the effect of the practical application is yet to be verified; and lastly, the study on how to balance privacy protection and propaganda effect in algorithmic application is

not yet sufficient.

The innovations of this study are: first, systematically combining the problems of privacy protection and algorithmic bias, and proposing a comprehensive solution for the application of algorithmic technology in anti-fraud propaganda; second, verifying the effect of the improved algorithmic model in practical application through empirical analysis, and providing actionable practical guidance for public security organs; third, exploring how to balance privacy protection and propaganda effect in the application of algorithmic technology, and proposing a technical path that takes into account Third, to explore how to balance privacy protection and publicity effect in the application of algorithmic technology, and to propose a technical path to balance efficiency and fairness. The significance of this study is: on the one hand, to provide scientific and reasonable algorithmic application solutions for public security organs, and to enhance the accuracy and fairness of anti-fraud propaganda; on the other hand, to promote the standardized application of algorithmic technology in the field of public service, and to provide theoretical support and practical reference for building a harmonious and safe digital society. Through this study, it is expected to provide a reliable theoretical basis for public security anti-fraud propaganda work, help improve the efficiency and quality of anti-fraud propaganda, and better protect the people's property security and legitimate rights and interests.

1.2 Domestic and Foreign Research Status and Evaluation

In recent years, with the rapid development of information technology, the application of algorithms in the field of public security anti-fraud has gradually become a research hot spot. Foreign scholars have extensively explored the privacy protection and algorithmic bias of algorithmic technology in anti-fraud propaganda.

For example, Smith et al. (2020) successfully identified potential fraudulent behaviors and proposed targeted preventive measures by constructing a machine learning-based predictive model, providing an important reference for the application of algorithms in the anti-fraud field. In terms of privacy protection, the implementation of the EU General Data Protection Regulation (GDPR) provides a clear legal framework for data processing, emphasizing that data processing activities must ensure the security and privacy of personal data (Jones & Brown, 2019). In addition, to address the problem of algorithmic bias, Johnson et al. (2021) proposed to reduce bias by improving algorithmic models and increasing the diversity of datasets, an approach that has been validated in several international studies (Lee et al., 2022; Zhang & Wang, 2021).

Domestic scholars have also conducted in-depth research on the application of algorithmic techniques in anti-fraud propaganda. For example, Li Ming (2020) pointed out that algorithmic technology can accurately identify high-risk groups through big data analysis, thus improving the targeting of anti-fraud propaganda. However, Wang Qiang (2021) emphasized that the privacy leakage problem in algorithmic applications should not be ignored, especially in the process of data collection and processing, how to balance the efficiency and privacy protection is a difficult problem that needs to be solved. In addition, Zhang Hua (2022) found through empirical research that algorithmic models may be biased in anti-fraud propaganda, leading to some groups being overly concerned or ignored, thus affecting the fairness of propaganda.

Although domestic and international research has made some progress, there are still some shortcomings. First, the combined research on privacy protection and algorithmic bias problem is less and lacks systematic (Chen et al., 2021). Second, specific solutions for algorithmic bias mostly stay at the theoretical level, and the effect of practical application is yet to be verified (Liu & Zhang, 2020). Finally, research on how to balance privacy protection and publicity effects in algorithmic applications is insufficient (Wang et al., 2022). Therefore, this study aims to propose a comprehensive solution that balances privacy protection and algorithmic fairness by systematically analyzing domestic and international research results and combining empirical studies, so as to provide theoretical support and practical guidance for public security anti-fraud propaganda work.

1.3 Main Innovative Points of the Thesis

This thesis focuses on the challenge of privacy protection and algorithmic bias of algorithmic technology in public security anti-fraud accurate propaganda, and puts forward several key innovative points:

(1). For the issue of data privacy and security, this study proposes a complete framework of data privacy protection mechanism from the three dimensions of compliance, security and user privacy protection. The framework not only examines in detail the legal and regulatory requirements for data collection and use, but also designs corresponding protective measures for the risks that may arise during data storage and transmission. In addition, this paper also explores methods to enhance users' awareness of privacy protection, aiming to build an all-round data privacy protection system.

(2). In terms of algorithmic bias, this study identifies the phenomenon of algorithmic discrimination and analyzes its causes, especially in the precise recommendation algorithm based on user profiles. By comparatively analyzing different anti-fraud propaganda strategies, it reveals the potential negative impact of algorithmic bias on a wide range of audiences, especially vulnerable groups. To solve this problem, this paper proposes effective ways to eliminate algorithmic bias, including strategies such as adopting diversified data sources and improving algorithmic transparency.

(3). For the study of information cocoon and group polarization, this paper describes the mechanism of information cocoon formation and analyzes its impact on the public's ability to receive anti-fraud information. The paper further explores the manifestations of group polarization and preventive measures, especially proposes innovative ways to break the information cocoon and group polarization, such as cross-platform cooperation and diversified content pushing, in order to enhance the effect of anti-fraud propaganda [1].

(4). On the issue of algorithmic interpretability and transparency, this study discusses the algorithmic black box problem in detail and emphasizes the importance of algorithmic interpretability in enhancing public trust and promoting decision-making transparency. In response, this paper proposes a series of measures to enhance algorithmic transparency, including the establishment of an algorithmic transparency reporting system and the increase of public supervision and participation, in order to ensure the openness and fairness of the algorithmic decision-making process.

(5). Finally, in terms of constructing a fair and impartial algorithmic model, this paper proposes methods based on the application of multi-source anti-fraud data, improving the interpretability of the model, and preventing algorithmic bias. These innovative points not only help to improve the effect of anti-fraud propaganda, but also provide new ideas and directions for the improvement path of algorithmic technology.

Through the in-depth discussion of the above innovations, this thesis provides strong theoretical support and practical guidance for the application of algorithmic technology in public security anti-fraud accurate propaganda, which is of great significance for improving the effect of anti-fraud propaganda and safeguarding the public's right to privacy.

2.The Practical Application of Algorithmic Technology in the Anti-Fraud Precision Propaganda

2.1 Algorithmic Recommendation Mechanism

2.1.1 Accurate recommendation based on user profile

In the public security anti-fraud propaganda, the accurate recommendation technology based on user profiles is an important strategy. Through in-depth analysis of the user's behavioral data, social network, historical feedback and other information, a detailed user profile is constructed, thus realizing the accurate identification of the user and personalized content push. The core of this technology lies in understanding user needs, predicting the anti-fraud propaganda content that users may be interested in, and optimizing it through algorithms to improve the propaganda effect.

The construction of user profiles usually includes the following key steps: data collection, data processing, feature extraction, model training and content recommendation. Data collection involves obtaining user information from multiple channels, such as social media and online behavior records. Data processing involves cleaning and organizing this data for subsequent analysis. Feature

extraction is the extraction of key information from the processed data that contributes to the construction of user profiles, such as age, gender, geographic location, interests and preferences. Model training, on the other hand, uses machine learning algorithms, such as decision trees and neural networks, to predict user behavior and preferences based on the extracted features. Finally, content recommendation is performed based on the model output.

Precision recommendation technology based on user profiles can effectively improve the targeting and effectiveness of anti-fraud propaganda. Through in-depth analysis of user data, the construction of detailed user profiles, the realization of accurate identification of users and personalized content push can not only improve user participation and satisfaction, but also effectively enhance the overall effect of anti-fraud propaganda [2].

2.1.2 Scene-specific anti-fraud information push

With the development of Internet technology, fraudulent means are becoming more and more complex, and the anti-fraud information push in specific scenarios has become an important means of public security anti-fraud propaganda. The use of algorithmic technology to accurately analyze user behavior data, identify high-risk groups, and achieve targeted information push.

On social media, e-commerce platforms, travel booking and financial service platforms, anti-fraud knowledge is accurately pushed through data on user behavior, shopping habits and transaction behavior. For example, high-value goods buyers are reminded to guard against phishing websites, and new users are popularized with basic fraud identification skills; travel users are provided with fraud warnings for tourist destinations; and anti-money laundering and anti-fraud information is pushed in real time to financial transaction users.

For the elderly group, the development of specialized applications, combined with voice and graphic methods, to simplify the delivery of information and improve acceptance. During holidays and other high-risk periods, relevant anti-fraud information is pushed in advance based on historical data and trend forecasts. Utilizing geographic location-based information services (LBS) to provide specific preventive tips, such as identifying fake online stores and avoiding leakage of personal information, for the types of fraud that occur frequently in specific regions.

Through these technologies and applications, effectively enhance the relevance and effectiveness of anti-fraud propaganda, and effectively protect public property security. Through the anti-fraud information push strategy in all the above specific scenarios, it can not only enhance the public's anti-fraud awareness and ability, but also promote the efficiency of the public security organs in combating and preventing fraud crimes, and ultimately realize the stability of social security and the protection of people's property safety [3].

2.1.3 Dynamic content optimization based on behavioral data

In the public security anti-fraud precision propaganda, dynamic content optimization based on behavioral data is an important technical means. By analyzing the user's behavioral data, real-time adjustment and optimization of the anti-fraud propaganda content can be achieved, thus improving the effect of propaganda and user participation. This method mainly relies on big data analysis and machine learning technology to achieve personalized recommendation and dynamic update of content through in-depth understanding of user behavior.

(1). Data collection and processing: first, user behavioral data needs to be collected from various channels, including but not limited to user browsing history, clicking behavior, dwell time, etc. These data are cleaned and pre-processed for training machine learning models.

(2). feature engineering: useful features are extracted from the processed data, such as user activity, distribution of points of interest, etc., which will be used as inputs to the machine learning model.

(3). model training: train the features using machine learning algorithms (e.g., decision trees, random forests, neural networks, etc.) to build a predictive model. The model is capable of predicting the anti-fraud propaganda content that a user may be interested in based on his or her behavioral data.

(4). Content Generation and Optimization: Dynamically generate or optimize anti-fraud propaganda content based on the prediction

results of the model. This step may involve content creation, editing, and the application of personalized recommendation algorithms.

(5). Feedback loop: user feedback on the publicized content (e.g., click-through rate, conversion rate, etc.) will be collected and used for model retraining to continuously optimize the effect of content recommendation.

2.2 Algorithm Technology Platform

2.2.1 Application of big data analysis in anti-fraud propaganda

In the digital era, big data technology has become an important tool for public security organs to combat and prevent online fraud. Through deep mining and analysis of massive data, it can effectively identify, predict and prevent fraud, and improve the targeting and effect of anti-fraud propaganda. Its application is mainly reflected in the following aspects: user behavior pattern analysis: by analyzing the user's behavioral data on the network platform (such as login frequency, browsing history, etc.), a personalized portrait is established to accurately identify potential fraud targets.

For example, analysis of the abnormal behavior of high-risk users can lead to early identification of user groups that may be victimized or involved in fraud, and targeted publicity and education.

Early warning model construction: Combined with big data technology, a dynamic fraud early warning model is constructed, integrating user information, behavioral characteristics and market dynamics, seasonal changes and other factors. Through real-time monitoring, it predicts the possibility of fraudulent behavior, deploys anti-fraud propaganda resources in advance, and realizes timely prevention and intervention.

Feedback Mechanism Optimization: Using big data to assess the effect of anti-fraud propaganda, collect user feedback, click rate, forwarding rate and other data to understand the acceptance of the propaganda content and user demand, timely adjustment and optimization of propaganda strategies to improve targeting.

Social Network Analysis: By analyzing the interpersonal relationships and information flow in social networks, we reveal the dissemination path and scope of influence of fraudulent information, identify and combat fraudulent activities using social networks, and block the chain of fraudulent information dissemination.

Intelligence Sharing and Collaboration: Big data technology promotes information sharing and collaboration among different public security agencies, builds a nationwide anti-fraud intelligence database, accelerates the speed of handling fraud incidents, and enhances the awareness and ability of society to prevent fraud.

The application of big data analysis improves the scientific and accuracy of anti-fraud work and enhances the relevance and effectiveness of publicity. With the continuous development of technology, its application in the field of anti-fraud propaganda will be more extensive and in-depth

2.2.2 Construction and application of artificial intelligence algorithm platform

In the public security anti-fraud accurate propaganda, the construction and application of artificial intelligence algorithm platform is one of the key technologies to realize efficient and accurate anti-fraud propaganda. The platform mainly relies on big data analysis and machine learning technology, through the analysis of a large number of user data, identifies high-risk user groups, and pushes customized anti-fraud propaganda content for these users.

Building an artificial intelligence algorithm platform first requires collecting and organizing a large amount of user behavioral data, including but not limited to user browsing history, transaction records, social network activities, etc. This data is preprocessed and used to train machine learning models to identify potential patterns of fraudulent behavior. The platform will use deep learning techniques such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) to analyze user behavioral data, extract features, and predict whether a user is likely to be a target of fraud. This predictive modeling can help platforms more accurately identify high-risk users for accurate campaigns.

2.2.3 Design and implementation of the intelligent push platform

The intelligent push platform is a key link in the public security anti-fraud propaganda, aiming to accurately reach the target audience through an efficient information push

mechanism. The platform integrates technologies such as big data analysis, artificial intelligence algorithms and user behavior analysis to realize the intelligent management of anti-fraud information push. In the design stage, the platform collects basic user information, historical behavioral data and online habits, and uses machine learning algorithms to build a user profile library, covering multi-dimensional data such as age, gender, occupation, social networks, consumption habits, etc., to predict the acceptance and preference of users' anti-fraud propaganda, and to customize personalized content recommendations.

During the implementation process, the platform adopts a dynamic optimization mechanism to adjust the push strategy based on user feedback and monitoring results. For example, when the click rate or conversion rate of a certain type of anti-fraud content is lower than the preset standard, the system automatically analyzes the reasons and adjusts the content form or push time. Meanwhile, the platform monitors the publicity effect in real time, assesses the effectiveness of push content through data analysis, and optimizes algorithms and strategies.

In addition, the platform focuses on user experience and privacy protection. It adopts anonymization and encryption technology to ensure user data security and avoid privacy leakage. The platform also provides a user feedback portal, allowing users to evaluate the push content, which is used to optimize the push strategy and improve the content quality and user satisfaction.

Overall, the design and implementation of the intelligent push platform is a comprehensive project, and through continuous optimization and iteration, the platform can effectively improve the accuracy and influence of anti-fraud propaganda and provide strong support for the fight against telecommunications network fraud.

2.3 Algorithm Technology Application Cases

2.3.1 Network platform anti-fraud propaganda strategy

Because of its high coverage and convenience, the network platform has become an important position for anti-fraud propaganda. In order to cope with the diverse means of fraud, the anti-fraud propaganda strategy needs to be adapted to the characteristics of the network, and customized communication methods are adopted for different user groups [4]. First, the content should be diversified, combining graphics, video, audio and other forms, such as case stories, explanatory videos or expert interviews, in order to enhance the attractiveness and comprehensibility. Second, anti-fraud information needs to be updated in real time, and a rapid response mechanism should be established to release the latest fraudulent techniques in a timely manner to help users identify new types of fraud. In addition, big data and algorithmic technology are used to make personalized recommendations and push relevant anti-fraud content to users to increase acceptance and participation. Interactive participation is also crucial, through online quizzes, prize surveys, virtual reality experiences and other forms, to enhance user participation and prevention capabilities. At the same time, cooperation with e-commerce platforms, social media, online games, etc., to broaden the publicity channels and form a synergy. In terms of technological empowerment, artificial intelligence is used to optimize content recommendation, and blockchain is used to verify the authenticity of information and enhance the intelligence and credibility of publicity. Educational guidance is also indispensable, enhancing users' legal awareness and sense of social responsibility through legal literacy lectures and thematic educational activities. Finally, cross-border cooperation with government departments, financial institutions, telecommunication companies and other anti-fraud publicity alliance, integration of resources, and the construction of the whole society to participate in the anti-fraud pattern. Through the implementation of the above strategies, the anti-fraud propaganda on the network platform can be It reaches the target users more effectively, enhances the public's anti-fraud awareness and ability, and contributes to the construction of a safe network environment. At the same time, these strategies also provide the future network platform anti-fraud propaganda with experience and direction that can be drawn from [5].

2.3.2 Case study of anti-fraud propaganda on short video platforms

With the rapid development of Internet technology, the short video platform has become one of the important channels for anti-fraud propaganda because of its rich content, fast dissemination speed, wide coverage and other characteristics. Anti-fraud propaganda through the short video platform can effectively improve the public's understanding of various fraudulent means and preventive awareness, and reduce the incidence of fraud [6].

On the short video platform, there are many cases of anti-fraud propaganda and the effect is remarkable. The following are a few typical cases:

Case 1: A well-known short video platform launched a series of short videos on anti-fraud propaganda, based on real fraud cases, using a first-person perspective to show the details of the fraud, and exposing common practices such as fake official websites, fictitious emergencies, and online loans. The video educates viewers to recognize and prevent fraud through real cases, and has gained a high number of viewers and a wide range of social reactions since its release.

Case 2: Another platform uses animation to show the process of fraud through exaggeration, adding interactive links, allowing viewers to choose whether they will be deceived or not, and enhancing the sense of fun and participation. The animation explains in-depth cell phone fraud, online shopping fraud and other types, successfully attracting the attention of a large number of users.

Case 3: A platform launched the “Anti-Fraud Challenge” to encourage users to create anti-fraud-themed short videos and set up a reward mechanism. The activity inspired users to participate in the enthusiasm, enriched the form of publicity, broadened the scope of dissemination, so that the anti-fraud message to reach a wider audience, and achieved good results.

The success of these cases is due to the rapid dissemination and high interactivity of the short video platform. Through the vivid and interesting form, the anti-fraud information is more easily accepted and understood, and the case analysis and interactive design also enhance the audience's memory and cognition of anti-fraud knowledge, which is of great significance in enhancing the public's ability to prevent fraud.

However, short video platforms also face some challenges in anti-fraud propaganda, such as how to ensure the accuracy and authority of the content, how to improve user participation, and how to measure the actual effect of anti-fraud propaganda. Therefore, future anti-fraud publicity work needs to continuously explore innovative methods to improve the quality and effect of publicity and better serve the public's anti-fraud needs.

2.3.3 Effectiveness assessment of anti-fraud publicity in mobile applications

The implementation of anti-fraud propaganda strategies in mobile applications aims to improve the efficiency and effectiveness of anti-fraud message reception through accurate user profiling and behavioral analysis [7]. In order to comprehensively evaluate the actual effects of these strategies, we used a variety of data analysis methods, including key indicators such as user feedback, click-through rate, and conversion rate.

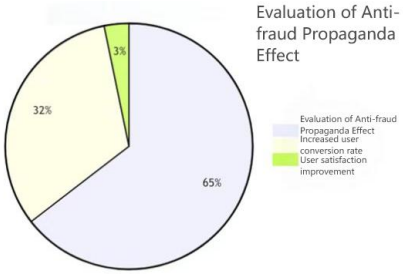

Figure 1. Anti-Fraud Publicity Audience User Pie Chart

From the Figure 1, it can be intuitively seen that the user conversion rate has increased the most, which indicates that the anti-fraud propaganda content optimized by algorithmic techniques is more capable of arousing users' interest and participation [8]. In addition, the increase in user satisfaction reflects the enhanced quality and relevance of the anti-fraud propaganda content.

During the evaluation process, we also noted some challenges and issues. For example, despite the significant overall effect, the response was not consistent across different user groups. Some users may not be interested in certain types of anti-fraud promotional content due to personal preference or specific needs. This requires us to analyze user data more carefully in future strategies and further optimize the algorithmic model to achieve more accurate personalized recommendations.

In addition, privacy protection is also an issue that cannot be ignored. When analyzing user

data and optimizing algorithms, we must ensure that all operations comply with relevant laws and regulations to protect users' privacy and security. This requires us to make corresponding adjustments and optimizations in both technical implementation and policy formulation.

In conclusion, the evaluation of the effectiveness of anti-fraud propaganda in mobile applications shows that the application of algorithmic technology can significantly improve the effectiveness of anti-fraud propaganda, but at the same time, it also brings a series of challenges, such as user variability, privacy protection and other issues. Future research and practice need to pay more attention to user experience and privacy protection while improving the propaganda effect to ensure the sustainable development and application of the technology.

3. Challenges of Algorithmic Technology in Anti-Fraud Propaganda

3.1 Data Privacy and Security Issues

In the context of the wide application of algorithmic technology in public security anti-fraud precision propaganda, data privacy and security issues have become the core challenge. The compliance of data collection and use is directly related to the respect of user privacy, the protection of data security and the establishment of social trust. Data collection needs to strictly follow the Cybersecurity Law and the Personal Information Protection Law to ensure legality, legitimacy and necessity, and to obtain the consent of the data subject. However, in practice, data collection may face the problem of unauthorized or excessive collection, leading to an increased risk of privacy leakage.

Data security involves the integrity, confidentiality and availability of data. In the context of anti-fraud propaganda, data tampering or falsification will seriously affect public trust. In addition, the handling of sensitive data (e.g., personally identifiable information, communication records) carries a risk of leakage, especially during data transmission and storage, which may lead to illegal access or misuse of data due to technical loopholes or mismanagement.

The issue of privacy protection is particularly prominent. With the application of big data and artificial intelligence technologies, the collection and processing of personal information has become more convenient, but it has also exacerbated the risk of privacy infringement. How to find a balance between data utilization and privacy protection has become an urgent challenge. Once user privacy is violated, it not only violates laws and regulations, but also weakens public trust in anti-fraud propaganda and affects social stability.

In conclusion, data privacy and security issues are focused on the compliance of data collection, the vulnerability of data security, and the high risk of privacy protection. These issues, if not properly addressed, will directly affect the effectiveness and social credibility of anti-fraud propaganda.

3.2 Algorithmic Bias and Discrimination Issues

In public security anti-fraud precision propaganda, the extensive application of algorithmic technology aims to achieve targeted prevention and education through in-depth analysis of big data. However, this data-driven precision propaganda strategy also raises concerns about the phenomenon of algorithmic discrimination, i.e., algorithms may unconsciously bias and discriminate against certain groups of people due to data bias, algorithm design flaws and other factors. Algorithmic bias refers to the deviation of algorithmic outputs from the actual situation due to imbalance, bias, or mislabeling of the dataset itself in the data processing and decision-making process. In public security anti-fraud precision campaigns, algorithmic bias may lead to specific groups being overly labeled or ignored, thus affecting the effectiveness and fairness of anti-fraud campaigns. Incomplete data collection, if there is insufficient or missing data on certain groups in the anti-fraud dataset, the algorithm may introduce bias based on the available data, resulting in these groups being incorrectly labeled as high risk in anti-fraud outreach. Algorithm design flaws, where the algorithm designer may have inadvertently introduced bias, such as using biased features or failing to adequately account for all relevant factors. Data labeling issues, where subjective judgments during the data labeling process may lead to biased labeling results, which in

turn affects the algorithm's learning and prediction results. These biases not only affect the accuracy of anti-fraud propaganda, but may also exacerbate social inequity and harm the interests of specific groups.

3.3 Information Cocoon and Group Polarization Problem

Information cocoon refers to the phenomenon in which individuals receive information that is highly similar to their previous views, interests and behavioral patterns and dissimilar information is ignored due to information screening and preference selection in Internet information dissemination. This phenomenon exacerbates information segregation and makes individuals' worldviews and behavioral patterns more closed. The formation of information cocoon is mainly influenced by recommendation algorithms, personalization, user-initiated screening, psychosocial factors, and selectivity of communication media. Recommendation algorithms based on users' historical behavior constantly push similar content, resulting in a narrower range of information exposure; personalized customization services of social media and news platforms make users see only content that matches their preferences, ignoring other important information; information overload causes users to pay attention to only the information that is consistent with their own stance, further limiting information exposure; people tend to choose information that confirms their self-identity and sense of belonging to a group and Rejection of contradictory information; Users choose specific media sources according to their needs, exacerbating the information cocoon.

Group polarization refers to the interaction of individuals in a particular group, which leads to the polarization of views. It is mainly manifested in information selection bias, dominance of extreme views and social network homogeneity. Individuals tend to select information that conforms to existing views and ignore contradictory information, which is reinforced by the algorithmic recommendation mechanism; group discussion focuses on extreme views and ignores intermediate positions, leading to further viewpoints away from the center; and tightly-knit group members have a high degree of homogeneity, which makes it easy for them to form the identity of extreme views.

In the context of information cocooning and group polarization, data privacy and security issues are becoming increasingly prominent. Personalized recommendations and algorithms rely on a large amount of user data, which may lead to privacy leakage; platforms may misuse user behavioral data, further exacerbating the information cocoon and group polarization; pushing specific information through algorithms may manipulate users' views and behaviors and influence public opinion. These problems not only threaten user privacy, but also exacerbate the closure and polarization of the information environment, and require urgent attention and solutions.

3.4 Algorithm Interpretability and Transparency Problems

The algorithm black box problem refers to the internal working mechanism of the algorithm is not visible or difficult to understand for external users, which is especially prominent in anti-fraud propaganda. Algorithms process large amounts of data to achieve accurate information pushing, but their opacity may lead to a lack of trust, regulatory difficulties, and fairness issues. Users are unable to understand how algorithms screen anti-fraud information, making it difficult to judge whether their decisions are fair and effective; the internal logic of algorithms is not open to the public, making it difficult for regulators to supervise and assess them, and increasing the risk of bias or discrimination; opacity also makes users skeptical of the recommended content, affecting the platform's trustworthiness, and potentially damaging the brand image and user base in the long term. Algorithmic interpretability is crucial in anti-fraud propaganda, especially after the widespread use of complex algorithms such as deep learning, which has increased public interest in the decision-making process. Transparent decision-making logic enhances user trust, improves publicity, and ensures the legitimacy and effectiveness of information dissemination. Users who understand how algorithms recommend information based on their behavioral data will be more actively involved in anti-fraud education; transparency helps prevent algorithmic bias and discrimination and protects the public's rights and interests; explaining how algorithms

identify fraudulent information and adjust publicity strategies improves the accuracy and relevance of the content; transparency also eases users' concerns about privacy protection, promotes data sharing, and facilitates the conduct of anti-fraud publicity; clear algorithmic logic helps the Clear algorithmic logic helps the public recognize false information, reduces fraud cases, and promotes the improvement of laws.

In anti-fraud propaganda, algorithms handle a large amount of user data, and privacy and security issues are particularly prominent. Users are concerned about the misuse or leakage of personal information, especially when the algorithms are not transparent, and this concern is further exacerbated. Data privacy issues not only affect user trust, but can also lead to legal risks and damage the platform's reputation. By solving the algorithmic black box, enhancing interpretability and safeguarding data privacy, the transparency and user trust of anti-fraud propaganda will be significantly improved, promoting the construction of a fairer and more equitable online environment.

4. The Study of the Improvement Path of Algorithmic Technology in Anti-Fraud Propaganda

4.1 Improve the Data Collection and Use of Norms

Data collection and use in the anti-fraud propaganda should strictly follow the standards and privacy protection measures to ensure the legitimacy and user trust. The purpose of collection should be clear, limited to anti-fraud needs, avoiding the collection of sensitive information, such as identity card numbers, bank accounts and so on. The process should be transparent to protect the user's right to know, requiring the user's consent and compliance with regulations such as the Cybersecurity Law and the Personal Information Protection Law, and anonymization techniques should be used to reduce privacy violations.

Data security management includes encrypted storage, access control, backup and disaster recovery to ensure full life cycle security. Setting time limits for storage and use, and timely handling of expired data to reduce the risk of leakage. Provide data usage reports to enhance credibility. Set up regulatory groups to rectify violations, promote secure data sharing, and optimize standards.

In the data security management system, categorize and manage sensitive data, implement encryption and the principle of least privilege, record access logs, make regular backups, adopt firewalls and intrusion detection systems, desensitize public data, and conduct regular assessments and tests to improve stress resistance.

Privacy protection measures include the principle of least necessary, informed consent mechanisms, open processes, data desensitization and anonymization, clear responsibility for violations, and ensuring traceability and remediation. Combined, these measures standardize data collection, use and privacy protection to provide safe and reliable technical support for anti-fraud propaganda.

4.2 Fair Algorithm Modeling

In anti-fraud propaganda, the application of multi-source anti-fraud data and algorithm optimization is the key to improving accuracy and fairness. First, information is extracted from heterogeneous data such as network transactions, user behavior, social media, etc., cleaned and standardized to ensure data unity. Data cleaning technology is utilized to deal with missing and noisy data, and the data set is continuously updated to improve the model's ability to identify emerging frauds. Utilize machine learning and deep learning, such as feature engineering and neural networks, to automatically identify patterns and improve efficiency. To enhance model interpretability, display input, processing and output details, analyze feature weights using SHAP values, graphically display impacts, and establish a user feedback mechanism for continuous optimization. LIME technology is used to build local interpretable models and provide intuitive explanations.

On algorithm bias prevention, introduce multi-dimensional crowd data to ensure universality and fairness. Establish an evaluation system to regularly test algorithmic effects and utilize explanatory AI to enhance transparency. Set up a review team to optimize models based on data and feedback. Strictly comply with data protection regulations to ensure legal compliance. Through these measures, the accuracy, fairness and user trust of anti-fraud

propaganda are effectively enhanced [9].

4.3 Breaking the Information Cocoon

In the digital era, anti-fraud propaganda needs to integrate multimedia technology, through video, animation, audio and other forms, with the help of short-video platforms and other channels, to vividly display anti-fraud knowledge, close to the habits of the public. At the same time, user data is analyzed and personalized content is customized to improve information relevance and engagement. Cooperate with education, Internet, and entertainment industries to develop courses and programs to broaden channels. Enhance interactivity, such as knowledge contests and case solicitation, to improve participation and memorization. Utilize VR and AR technologies to provide immersive experiences to help identify fraud. Popularize legal knowledge, focus on specific groups, and design intuitive content to ensure broad coverage.

Cross-platform cooperation is key, joining forces with online, social, and educational organizations to establish a collaborative mechanism, share data, and accurately publicize. Combine platform characteristics and design interesting content, such as short videos, live broadcasts, and H5 games, to enhance educational significance. Enhance the sense of experience through interactive links. Establish a monitoring and feedback mechanism to evaluate the effect and optimize the strategy.

Break the singularity of information, multi-channel release, innovative forms, such as short videos, games, VR, to enhance interest. Encourage exposure to diversified information, carry out media literacy education, and enhance discernment. Cooperate with technology and education across borders, develop diversified programs, and use AI to customize content [10].

In summary, breaking the monolithic nature of information requires the comprehensive use of a variety of strategies, including, but not limited to, diversification of information sources, innovation of content forms, elimination of information filtering barriers, enhancement of media literacy education, strengthening of cross-border cooperation, and the use of advanced technology for information analysis and customization. Through these measures, the effectiveness of anti-fraud propaganda can be effectively enhanced, and the public's comprehensive knowledge and understanding of anti-fraud can be promoted, so as to achieve better prevention and reduction of fraud incidents [11].

4.4 Enhancement of Algorithm Transparency

In anti-fraud propaganda, the application of algorithms improves accuracy, but also poses data security and privacy protection challenges. To this end, it is crucial to establish a regulatory mechanism. First, data collection and processing should be standardized to ensure legality, security, and transparency. The first step is to standardize data collection and processing to ensure legality, security and transparency. Subsequently, a review team is set up to regularly audit the algorithms, focusing on goal consistency, bias identification and privacy protection, and correcting deviations in a timely manner. Introduce third-party evaluation to comprehensively assess algorithms from technical and ethical perspectives. Encourage public participation by setting up complaint channels and reporting platforms to allow the public to participate in regulation and improvement. Require platforms to publish regular transparency reports and publicize algorithm design and data sources. Enact laws and regulations governing the use of algorithms, including design principles and data protection. Establish cross-sectoral cooperation to promote comprehensive regulation. In addition, public supervision and participation are indispensable; an open algorithm review platform should be established, the public should be invited to participate in testing and evaluation, algorithm education should be popularized, incentives should be provided for reporting bias cases, and a feedback mechanism should be created. Through these measures, anti-fraud propaganda algorithms are scientifically and systematically regulated, data privacy and security are safeguarded, anti-fraud efforts are optimized, and technical support and legal safeguards are provided to combat online fraud [12].

5. Conclusion and Prospect

The application of algorithmic technology in

the public security anti-fraud precision propaganda has significantly improved the propaganda effect, and the precise identification of the target group is realized through the user portrait technology to improve the pertinence and effectiveness of the propaganda. Big data analysis and artificial intelligence technology have enhanced the timeliness and real-time nature of information, and multi-platform linkage has expanded the scope of publicity coverage, while enhancing the public's anti-fraud awareness and ability and reducing the occurrence of fraud cases. However, the issues of data privacy protection and algorithmic bias still need attention to promote the improvement of relevant laws and regulations and technical standards.

In terms of strategy optimization, algorithmic technology quickly identifies high-risk areas or groups through data analysis, realizes precise publicity resource allocation, personalized push to improve the acceptance and conversion rate of information, and user interactive feedback to further optimize publicity strategies. Despite the technical challenges, ethical and moral considerations, social acceptance and regulatory restrictions and other application barriers, improving algorithm transparency, optimizing algorithm design, strengthening user privacy protection and improving relevant laws and regulations are the keys to overcoming these barriers.

In the future, the application of algorithmic technology in the field of anti-fraud will be more intelligent and adaptive, privacy protection technology will be a breakthrough, and the algorithmic model will be more diversified and integrated. Interactive and personalized anti-fraud propaganda, cross-platform and multi-channel fusion application, and international and localized algorithm design will become the development trend. In order to build a sustainable anti-fraud propaganda algorithmic technology application path, it is necessary to strengthen data governance and privacy protection, improve algorithm transparency and interpretability, build a fair and impartial algorithmic model, promote information diversification and break the information cocoon, strengthen algorithmic supervision and public participation, and promote anti-fraud propaganda and education and public awareness.

Acknowledgement

The project name of this article is "Research the Application and Impact of Algorithm Technology in Precise Anti-Fraud Publicity" This paperls supported by 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] Zou Wenshan. Research on online telecommunication network fraud crime prevention and publicity in the field of online media communication. Network Security Technology and Application, 2023, (03):141-143.

[2] Niu Shuo, Deng Jie, Chen Jiayu, Lin Yuchen, Li Haohai. Research on building an early warning information platform for telecommunication network fraud prevention. Cyberspace Security, 2020, (05):18-27.

[3] Zhang Yaowen, Luo Wenhua. Research on the Characteristics of Telecommunication Network Fraud Victims--Based on Comparative Analysis of Data from Different Regions. Journal of Shanxi Police Academy, 2023, (01):80-87.

[4] Pi Zixin, Luo Zhenlei. The psychological induction mechanism and prevention strategy of the brush single rebate network fraud. Journal of Guangxi Police College, 2023, (04):82-89.

[5] Li Ke, Zheng Yiming, Zhang Yuxuan. Exploring the Path of “Breaking the Circle” of Positive Propaganda in the Age of All-Media--Taking Anti-Fraud Propaganda as an Example. News Outpost, 2022, (17):22-23.

[6] Lu Jingyan, Liao Genwei. Research on contextual prevention strategy of fraud crime using short video platform. Crime Research, 2020, (02):55-63.

[7] Zhang Wenhao, Chen Qi, Hu Renbin, Qi Wanyi. Empirical Analysis of the Effect of Anti-fraud Publicity of Public Security Organs--A Survey Study Based on Residents' Awareness of Telecommunication Network Fraud Prevention. Cyberspace Security, 2022,

(03):94-100.

[8] Zhang Jieze, Liu Yunxiao, Qi Chenhang. Study on the Characteristics of Victimization and Countermeasures for Prevention and Control of Brush Order Rebate Class Fraud--Analysis Based on 211 Victims' Reported Materials in District J. Journal of Jiangxi Police College, 2022, (04):31-38.

[9] Wang Yuanyuan. Research on the third-person effect of anti-fraud propaganda--Taking college students' group as an example. News World, 2024, (01):60-63.

[10] Wan Qiao. Research on prevention and control countermeasures of telecommunication network fraud for middle-aged and elderly groups under the background of big data. Network Security Technology and Application, 2022, (03):156-158.

[11] Zhang Zhi, Chen Feng. Research on Countermeasures for Prevention and Publicity of Telecommunication Network Fraud--Empirical Analysis Based on Victim Characteristics. Journal of Guangxi Police College, 2021, (02):41-49.

[12] Ouyang Guoliang, Qi Weichao. The analysis of the cryptic language of marketing crime. Journal of Beijing Police Academy, 2023, (04):74-79.

