Legal Risk Determination of Public Security Brain Building and its Prevention by FTA and FCE Methodisation

Mengfei Chen[1] and Yue He[2]

[1] International Institute, Zhejiang Police College, Hangzhou, China
[2]Law Faculty, Zhejiang Police College, Hangzhou, China
Email: cmfei1@163.com; heyue@zjjcxy.cn

Abstract. Legal risk assessment during constructing "Public Security Brain"is an essential part of building a scientifically intelligent police system. The legal risk factors affecting the construction of the "Public Security Brain"are summarised and extracted, realistic and feasible research and evaluation methods are provided, and the corresponding risk assessment system is established by adopting the Fault Tree Analysis Method and Fuzzy Comprehensive Evaluation Method to provide suggestions on risk prevention for the construction and operation of "Public Security Brain". Fault tree analysis and fuzzy comprehensive evaluation method are used to establish the corresponding risk assessment system, and to provide suggestions on risk prevention for constructing and operating "Public Security Brain".

Keywords: public security brain; risk assessment; quantitative analysis; indicator system

1. Introduction

In recent years, data technology has been widely used in policing, such as Zhejiang public security in the digital reform process has gradually explored the formation of the construction of the "Public Security Brain" as the traction of the development direction and path. In order to more effectively promote the construction of the "Public Security Brain" specific implementation programme, to ensure the standardization and orderly development of the work, and at the same time to enhance the public security reform and policy implementation of the degree of scientific and refined, this paper intends to "Public Security Brain" construction process may lead to the establishment of a preliminary legal risk measurement framework. This paper is intended to establish a preliminary measurement framework for legal risks that may be triggered during the construction of "Public Security Brain", combine the practical experience of policing in-depth, focus on building a set of scientific and reasonable legal risk assessment index system, and put forward feasible and effective risk prevention measures.

M. R. Mohyuddin and N. A. D. IDE (eds.), *Proceeding of the 2024 International Conference on Diversified Education and Social Development (DESD 2024)*, Advances in Social Science, Education and Humanities Research 899,
https://doi.org/10.2991/978-2-38476-346-7_21

2. Legal risks in the construction of the "Public Security Brain"

The current system of institutional provision for regulating the new form of intelligent policing work led by the "Public Security Brain" is insufficient, which further exacerbates the multiple risks public security authorities face in collecting, processing, using and sharing personal information. As the core legislation in private law, the Civil Code clearly defines the legal protection mechanism for citizens' personal information. This law plays an important role in regulating and balancing the relationship between the private and public sectors, and provides guidelines for administrative agencies in data processing. Based on the Civil Code's classification of personal information processing, and in conjunction with the current status of data application in the practice of smart governance, in-depth research is vital, and public security organs may have the following risks in the process of collecting and utilizing personal information [1], as shown in Table I.

TABLE I. CORRESPONDENCE TABLE FOR "RISK INDICATOR - LEGAL RISK"

Primary Indicators	Secondary Indicators	Counterpart of the Civil Code	Specific Risks
Information collection	Overcollection	Article 1032 Article 1035	The collection of personal information beyond the scope of the Smart Police Platform,occasionally occurs .
	Illegal collection	Article 1032 Article 1035	There may be intentional or unintentional breaches in collecting information by the Smart Police Platform.
	Data mutilation	Article 1038	The primary data source for adjudication predictions makes it challenging to encompass all the factors that significantly impact case disposition, and the residual data will cause some of the predictions to fall into small-sample thinking.
Information processing	Illegal classification labelling	Article 1035	Public security authorities may use classified labelling that lacks a legal basis, thereby biasing the data with illegal or incorrectly labelled information.
	Over-associative clustering	Article 1035	In practice, certain acts replace causal judgements with correlation and, accordingly, adopt undue restrictions on the subject of information with undesirable consequences.
Use of information	Misuse of information	Article 1035	The misuse of information has the potential to extend the responsibility of individuals for their actions.
	Algorithmic domination	/	Practices such as technology-assisted administrative decisions are bound to create a dual structure of administrative subjects, and the blurring of the boundaries of authority can make accountability a mere formality. It can lead to a state of affairs where algorithms dominate the administration.
	Constraints	Article 1038	Intelligent technology is unable to encompass the entire process and information of decision-making, and probabilistic modelling makes decision-making simpler and flatter under the operation of information technology and intelligence, limiting potential administrative elements.
	Data chimney	/	Enforcement behaviours resulting from the operation of the algorithmic model will further self-justify the

			need for increased enforcement, which may create a distortionary feedback loop that leads to unfairness.
Information sharing	Excessive delegation	Article 1032 Article 1035 Article 1039	Discretion is gradually being handed over from people to algorithms and systems, and enforcement errors may have the potential to be systematically amplified by imbalances in the internal transmission flow from different departments.
	Public exposure	Article 999 Article 1032 Article 1035 Article 1039	The imbalance in data sharing by public security authorities to other third-party subjects may lead to the leakage of personal and even private information.
Lack of supervision	Lagging legislation	/	The use of information data in the public domain, especially in smart governance scenarios, urgently needs of a system to regulate it.
	One-sided data	Article 1038	Training models on indirect data can lead to the escape of invisible features that can bias results; the "silo" effect also makes big data often underused.
	Algorithmic black box	Article 1035	The lack of interpretability creates doubts about legitimacy, the likelihood of impure or tampered data is significantly increased in the absence of an audit, calculations collapse, and bias and injustice ensue.

3. Construction of Legal Risk Assessment dictator System for "Public Security Brain"

3.1 Principles and Methods of Indicator System Construction: Based on Fault Tree Analysis (FTA) and Fuzzy Comprehensive Evaluation Method (FCE)

Fault Tree Analysis (FTA), as a systematic design analysis and assessment tool, is centred on the in-depth analysis of the multiple factors that lead to system failure and the construction of a reverse tree logic structure diagram, i.e. a fault tree[2].

If the system fails to accomplish legal and compliant digital policing operations, or if there is a risk potential, it is judged that the system has failed, and a risk warning must be issued. Combined with the description in Table 1, it can be determined that the most frequently occurring fault states of the system are as follows:

1. Information collection is at risk when the supervisory module fails.
2. Information processing is at risk due to a failure of the supervisory module.
3. A risk in the internal aspects of the information use phase due to a fault in the supervisory module.
4. Risk in the external flow of information in the information use phase with a fault in the supervisory module.

In the qualitative analysis phase, the core task focuses on identifying all the minimal cutsets in the fault tree. They represent a specific failure mode of the system, and the set of all minimum cutsets constitutes a comprehensive map of system failures, mapping out the potential risk scenarios of complex systems such as the "Public Security Brain". Based on the assumption that the primary failure events of each component are independent of each other, we adopt the downward method to systematically search for and list all the minimum cutsets to to grasp the micro-mechanisms of system failure comprehensively.

$x_1 \sim x_{13}$ denotes the 13 underlying events respectively. In fault tree analysis, a fault tree is classified as monotonically correlated if the events are only related to the set of

"and" and "or" relationships. The essence of monotonic association system analysis can be reduced to dedicating Boolean expressions. The Boolean expression of the fault tree of the "Public Security Brain" system is as follows.

$$\begin{aligned} T = {} & x_1x_3 + x_1x_4 + x_1x_5 + x_1x_6 + x_1x_7 + \\ & x_1x_8 + x_1x_9 + x_1x_{10} + x_1x_{11} + x_1x_{12} + \\ & x_1x_{13} + x_2x_3 + x_2x_4 + x_2x_5 + x_2x_6 + x_2x_7 + \\ & x_2x_8 + x_2x_9 + x_2x_{10} + x_2x_{11} + x_2x_{12} + x_2x_{13} \end{aligned} \tag{1}$$

According to the classical fault tree analysis process, a quantitative assessment phase should follow. However, given the challenge of the uncertainty of statistical data in the process of FTA, coupled with the non-absolute binary distribution of risk factors of the "Public Security Brain" system, the traditional method is not satisfactory. Therefore, we plan to introduce the Fuzzy Comprehensive Evaluation (FCE) method as a complementary tool to alleviate the uncertainty problem in the risk determination model.

3.2 Key Elements of the Indicator System

Synthesize the weight vector W with each evaluation object's fuzzy relationship matrix R, and each evaluation object's fuzzy comprehensive evaluation result vector S is finally output[3].

$$\begin{aligned} & S = W * R = \{w_1, w_2, ..., w_n\} \\ & * \begin{bmatrix} r_{11} & r_{12} & \cdots & r_{1m} \\ r_{21} & r_{22} & \cdots & r_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ r_{n1} & r_{n2} & \cdots & r_{nm} \end{bmatrix} = (s_1, \wedge, s_n) \end{aligned} \tag{2}$$

Among them, s_i reflects the overall affiliation of the evaluation object to the hierarchical fuzzy subset.

The fuzzy statistical method is used to determine the affiliation value of the risk factor-evaluation level of the "Public Security Brain" system. A questionnaire will be issued to the front-line police and technicians in close contact with the "Public Security Brain" and the relevant research experts to obtain the affiliation function that is relatively consistent with the objective reality. In order to obtain an affiliation function that is relatively in line with the objective reality, a definite element of the domain is used to determine the affiliation function of the system. That is, a definite element v_0 on the domain that belongs to a clear set A^* can be changed to make a clear judgment. Clear set A^* can have different boundaries for different investigators, but they all correspond to the same fuzzy set A. The calculation steps of the fuzzy statistics method are as follows: in each statistic, v_0 is fixed in the value is variable; for n investigations, its fuzzy statistics can be calculated according to the following formula.

$$\text{the affiliation value of } v_0 \text{ to } A = \frac{\text{number of times } v_0 \in A}{n} \tag{3}$$

As n increases, the affiliation frequency will tend to stabilize, and this stabilization value is the affiliation value of v_0 to A.

4. Empirical Analysis of Legal Risk Assessment or the Construction of the "Public Security Brain"

4.1 Targets and Data Sources

In this paper, based on collecting data from 15 civilian police officers and experts in the legal department of the public security organs through the issuance of the importance consultation form and using the hierarchical analysis method described above, the weights of 14 secondary indicators were obtained. The judgment matrix was tested to have consistency ($CI = 0.0196$), the distribution of the weights was reasonable, and the results were as follows.

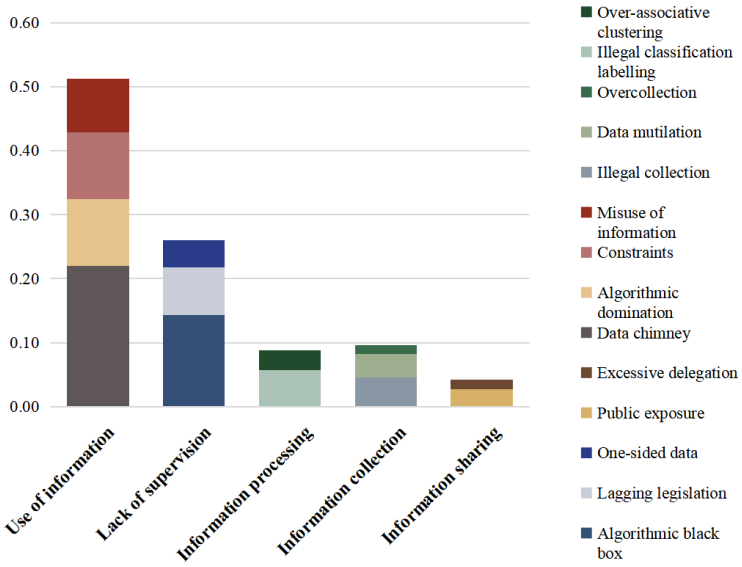

Figure 1. Importance of legal risk indicators for the construction of the "Public Security Brain"

It can be concluded that in the process of building the grassroots Public Security Brain in practice, the degree of influence of multidimensional risks varies, of which, the data chimney is a very high risk evaluation index, which is subordinate to the risk evaluation index of the use of information; algorithmic black box is a high-risk evaluation index, which is subordinate to the risk evaluation index of the lack of supervision; algorithmic domination, elements of the limit of shrinkage is a medium-risk, which is subordinate to the risk evaluation index of the use of information; information misuse is a low

The risk of information misuse is low, which belongs to the risk evaluation index of information use; legal lag, data one-sidedness, excessive disclosure, transfer of irregularities, illegal collection, data mutilation, excessive collection, illegal classification and labeling, and excessive correlation and clustering are the lower risk evaluation index, which belongs to the evaluation index of the risk of lack of regulation, information processing, information collection, and information sharing.

Compared with the multidimensional risk, the risk of information use is more focused. For the construction of the "Public Security Brain" system, the exclusion of the injustice formed by the self-reinforcement of the algorithmic bias should become the primary goal of necessity and urgency.

4.2 Evaluation Methodology and Process

In the previous section, the indicators at all levels of "Public Security Brain" legal risk evaluation have been determined, and the weight coefficients of the indicators at all levels have been obtained using AHP, forming a complete risk evaluation system. In this module, this paper will utilize the built "Public Security Brain" legal risk evaluation system, take the actual data of H city public security organs and T city public security organs as an example, and use the fuzzy comprehensive evaluation method to assess the evaluation value of specific intelligent policing legal risk factors.

This paper adopts a five-point system to classify the legal risk level, which is divided into "red, orange, yellow, blue, and green." The red indicates that the activities carried out by the public security organs in the region using the "Public Security Brain" have a high probability of violating the law. In contrast, the green color indicates that the probability of violating the law is extremely low, or even if it occurs at the initial stage, it can be detected and prevented in time and will not cause any harm.

From the above, the final result of the "Public Security Brain" legal risk assessment of the public security organs of City H is $V = 3.8456$ using weighted calculation. According to the criteria of the "Public Security Brain" legal risk level, the risk level of the public security organs of City H is orange, and the risk of the "Public Security Brain" legal risk of this organ is high. Similarly, the evaluation result of City T is $V = 1.9242$, with a risk level of blue.

4.3 Evaluation Results and Analysis

Based on the statistical data from the police information platforms of City H and City T public security organs, the actual number of cases related to the "Public Security Brain" was calculated and compared with its risk level, and the results are shown in the table below.

TABLE II. LEGAL RISKS OF THE "PUBLIC SECURITY BRAIN" IN THE TWO CITIES

City	***V***	**Fuzzy Composite Evaluation Rating**	**Number of violations /years**
City H	3.8456	Orange	5
City T	1.9242	Blue	1.3

From the above, after comparing with the actual situation, the results are relatively consistent: City T should control the risk at the current level and prevent the risk from deteriorating. At the same time, City H should pay attention to the relevant risk situation and take effective countermeasures and preventive measures in advance.

5. Evaluation of the Legal Risk Assessment Indicator System of the "Public Security Brain"

In digitalization and intelligence, "Public Security Brain", an essential carrier of public security innovation, aims to improve the decision-making efficiency, law enforcement accuracy and social governance capacity of public security organs through advanced technologies such as big data, cloud computing and artificial intelligence. However, with the in-depth application of technology, the accompanying legal risks should not be ignored. Therefore, it is of great significance to build a scientific and systematic legal risk assessment index system for the "Public Security Brain" to prevent legal risks and ensure the healthy and orderly development of the technology[4].

For the legal risks proposed in this paper, the following prevention strategies should be adopted:

5.1 Strengthen Data Protection and Enhance Technical Protection Capability

Establish a sound data security management system, clarify the standards and processes of data collection, storage, processing, and use, and ensure the legality and security of data use. At the same time, strengthen the application of data encryption, access control, and other technical means to prevent data leakage and illegal access.

Increased investment in the technical protection of the "Public Security Brain" system has been made to improve the system's ability to resist attacks and recover. Regularly conduct security vulnerability scanning and system risk assessment to discover and repair potential security risks promptly.

5.2 Strengthen the Standardization of Law Enforcement and Improve the System of Laws and Regulations.

Strengthen the legal training of law enforcement personnel. When using the "Public Security Brain" to conduct intelligent analysis and assist in decision-making, legal procedures should be followed to ensure the legality and fairness of decision-making. Establish a sound law enforcement supervision mechanism to provide comprehensive and effective supervision of law enforcement behavior.

Pay close attention to the development of technologies related to intelligent policing, and promptly study and formulate or revise relevant laws, regulations, and policy documents to clarify the legal boundaries and responsibilities for applying new technologies. Strengthen communication and coordination with the legislative authorities to promote the timely updating and improvement of laws and regulations.

5.3 Improve Risk Management and Emergency Response Mechanisms:

Establishing a legal risk monitoring platform to provide real-time monitoring and early warning of legal risks that may arise during the operation of the "Public Security Brain". Potential legal risks are discovered and assessed in advance through data analysis, model prediction, and other means.

The monitored legal risks are assessed and graded, and the risks' nature, degree, and scope of influence are clarified. Based on the assessment results, corresponding risk response measures and contingency plans are formulated[5].

In a legal risk incident, the contingency plan should be immediately activated, and forces should be quickly organized to deal with it. At the same time, communication and coordination with relevant departments are strengthened to form a joint effort to deal with risk challenges.

Conclusion

Security risk assessment is an integral part of the construction of an administrative security system through the analysis of the problems faced by the algorithmic administration in the process of operation, the use of security assessment methods to assess the current security status of the algorithmic system, and to focus on the defense of the parts and areas where the risk is likely to be more significant. Therefore, this study has substantial application value to provide a reference tool for the legal risk assessment of "Public Security Brain" construction across the country. In practice, local public security authorities can use the legal risk assessment index system to derive the specific legal risk level of intelligent policing, thus laying a data foundation and providing a direction for improvement in order to reduce the number of violations of the law and improve the level of law enforcement.

Acknowledgement

Supported by the National Innovation and Entrepreneurship Training Programme for Undergraduates 2023 (202311483001).

References

[1] Fang Zhiwei and Wang Jianwen, "Risks and Protection of Personal Information in Smart Governance: Centered on Personal Information Protection in the Civil Code," Jiangxi Social Science, vol. 5, 2021.

[2] Wu Jiachen and Yu Xiao, "A Review of Network Security Risk Assessment Methods," Electronic Science and Technology, vol. 3, 2024.

[3] Chen Xiaohong and Yang Zhihui, "Research on the Credit Evaluation System Based on Improved Fuzzy Comprehensive Evaluation Method: An Empirical Study of Small and Medium-sized Listed Companies in China," Chinese Journal of Management Sciences, vol. 1, 2015.

[4] Wang Jiawei, "Strategic Considerations for Ensuring Police Data Security in the Big Data Era," Network Security Technology and Application, vol. 12, 2022.

[5] M. Boban, Z. Pozgaj, and H. Sertic, "Strategies for Successful Software Development Risk Management," Management, vol. 32, no. 6, pp. 501‑508, 2017.