ISSN Print: 2707-1499  Online: 2707-1502
*Advance in Law* − 2025, 7(2)

sciscan
https://doi.org/10.35534/al.0702018

# A Study of the Expropriation of Data in Emergency Situations

Xuanxuan Zhou

Shanghai University of Political Science and Law, Shanghai

**Abstract:** With the rapid development of information technology, data has become an important resource in modern society. In emergency situations, such as natural disasters and public health events, the timely acquisition and utilisation of data is of great significance for effective response and loss mitigation. However, the expropriation of data in emergencies also involves a series of legal issues and social ethical problems. This article examines the issue of government expropriation of data in emergency situations. The article firstly analyses the necessity and legality of data expropriation, analyses the risks of data expropriation in emergency situations and puts forward corresponding suggestions, and finally puts forward an outlook on the development of the future data expropriation system, stressing that while ensuring data quality and improving the efficiency of expropriation, more attention should be paid to data security and privacy protection.

**Key words:** Emergency situations; Data expropriation; Legal issues; Social ethics; Legal regulation

## 1 Introduction

With the advent of the big data era, data has become a national foundational strategic resource. In emergency situations, the timely acquisition, analysis, and application of data play a crucial role in rapid response, scientific decision-making, and precise rescue operations. However, data requisition during emergencies faces multiple challenges, including the protection of data privacy rights, ensuring data security, and maintaining the legality of data usage. In the digital era, data has not only emerged as the fifth major factor of production following land, labor, capital, and technology, but also serves as a critical element in social governance, playing a significant role in digital government construction and scientific decision-making.

Article 5 of the “Opinions of the Central Committee of the Communist Party of China and the State Council on Building Data Infrastructure Systems to Better Leverage the Role of Data Elements” (commonly known as the “Data Twenty Articles”) clearly stipulates: “Government departments may obtain data from relevant enterprises and institutions according to laws and regulations when performing official duties, but must establish agreements and strictly comply with usage restrictions.” Data disclosure aims to require market entities and market operators

Author's Profile: Xuanxuan Zhou, Shanghai University of Political Science and Law, Master’s degree student.
Article Citation: Zhou, X. X. A study of the expropriation of data in emergency situations. *Advance in Law*, 7(2), 200-209.

to provide relevant data to each other, while also publishing and supplying necessary data to the public and data regulatory agencies. In practice, governments primarily obtain corporate data through voluntary enterprise sharing, mandatory data reporting, government procurement, and data requisition mechanisms. Current research on corporate data sharing with the government in China remains in its nascent stage. For instance, FENG Xiaoqing proposes that commercial data property rights may be subject to restrictions through data requisition based on national interests, thereby achieving necessary constraints on commercial data ownership. SHI Weidong also points out that under special circumstances, following strict procedures, the government may implement data requisition for specific purposes. This paper proposes establishing data requisition as a novel governmental pathway for data acquisition, which aligns with the proprietary attributes of data while addressing the distinctive needs of governments as special data users. With the rapid advancement of information technology, data has evolved into critical infrastructure underpinning modern societal operations, encompassing information collection, processing, analysis, and application across all sectors. During emergency states, governments and relevant institutions require swift decision-making capabilities where data serves as the foundational basis for such determinations. However, data requisition may encounter multifaceted challenges and constraints due to inherent issues surrounding data ownership, privacy rights, and security concerns. Consequently, investigating the legitimacy, rationality, and operational efficacy of data requisition under emergency circumstances holds imperative significance for safeguarding public interests and maintaining social order.

With the widespread application of technologies such as big data and artificial intelligence, the value and impact of data resources are becoming increasingly prominent. In emergency situations, by requisitioning data resources, these advanced technologies can be better utilized for prediction, early warning, and decision-making support to improve the efficiency and accuracy of crisis response. At the same time, this also puts forward higher requirements for data security and privacy protection in the process of data expropriation. Through in-depth research on data expropriation, data laws and regulations can be further improved, key issues such as data ownership, usage and supervision rights can be clarified, rational utilization and sharing of data resources can be promoted, and strong support can be provided for the construction of a more efficient, fair and secure data governance system.

To summarize, the problem of data expropriation in emergency situations mainly stems from the high dependence on data in modern society, the special demand for data resources in emergencies, and the need to improve the data governance system. The purpose of this paper is to discuss the problem of data expropriation in emergency situations, analyze its necessity, legality, and possible risks, and put forward corresponding legal regulations and ethical recommendations.

## 2 Analysis of the Need for Data Expropriation in Emergencies

### 2.1 Improving the Speed and Effectiveness of Emergency Response

Data expropriation has potential advantages in emergency situations, but needs to be regulated and safeguarded in legal, ethical, and technical terms. The positive role of data expropriation in emergency response can be fully realized only on the premise of ensuring that data are legal, accurate, and secure. In emergency situations, such as natural disasters and public health events, time is often of the essence.

Through data requisitioning, the Government or relevant organizations can quickly access a large amount of real-time and historical data to provide a scientific basis for emergency decision-making, thereby improving the speed and effectiveness of emergency response. Critical information related to emergencies, such as the distribution of personnel, resource reserves, traffic conditions, etc., can also be quickly accessed. This information is crucial for formulating emergency response strategies, deploying resources, and guiding rescue operations. Through the analysis of requisitioned data, real-time and accurate information support can be provided to decision makers to help them better understand the emergency situation, so as to make more scientific and reasonable decisions.

Data requisitioning can help to identify areas where resources are stretched and areas where there is a surplus of resources, leading to an optimal allocation of resources. This can ensure that in emergencies, resources can be used effectively to maximize relief needs. By analyzing historical and real-time data, it is possible to predict the development trend of emergencies and issue early warnings, providing a valuable window of time for emergency response. This helps to reduce disaster losses and protect people’s lives and property.

## 2.2 Reducing Disaster Losses

Data requisitioning helps to comprehensively understand and assess the scope and severity of the impact of disasters and provides strong support for the deployment of relief resources, thereby minimizing the losses caused by disasters. These aspects are of vital importance in protecting people’s lives and property, maintaining social stability, and promoting post-disaster recovery.

Data requisition can quickly gather and analyze information from various channels, provide decision makers with comprehensive, real-time disaster data, help decision makers grasp the dynamics of the disaster in a timely manner, and formulate correct response strategies. It can grasp the distribution and status of rescue personnel, materials, equipment, and other resources in real time, so as to optimize the allocation and dispatch of resources, ensure that rescue forces can reach the disaster area quickly and accurately, and improve rescue efficiency.

Data requisition not only supports decision makers but also provides timely and accurate disaster information to the public. By conveying information such as disaster warning and risk avoidance knowledge to the public, it can enhance the public’s awareness and ability of disaster prevention and mitigation, so that the public can be more proactive in participating in rescue and self-rescue and mutual aid in the event of a disaster, and reduce disaster losses. Meanwhile, in emergency situations, multiple departments and organizations are required to work together. Data elicitation can promote information sharing and collaborative work among departments, break down information silos, and improve the overall efficiency of disaster response. At the same time, data requisition can also provide data support and a decision-making basis for cross-sectoral collaboration, ensuring that various departments can form a synergy when responding to disasters.

## 2.3 Breaking up Data Monopolies and Promoting Data Sharing

In emergencies, data are often dispersed in the hands of various departments and enterprises, and there is a data silo effect and data monopoly. Through data requisitioning, it is possible to break this monopoly, promote data sharing and interconnection, and improve the efficiency of data utilization. For example, in the prevention and control of epidemics, by requisitioning data from medical, transportation, communications, and other departments, it is possible to realize the rapid transmission and sharing of information and provide strong support for the prevention and control of epidemics.

### 2.4 Responding to Network Emergencies

In the era of network informatization, unexpected network emergencies occur frequently, such as network security accidents and information leakage. Through data requisition, network data can be quickly accessed and analyzed to provide strong support for responding to network emergencies.

For example, in the emergency response to a network security incident, by requisitioning data from network monitoring, log analysis, etc., it is possible to quickly locate the source of the attack and the attack method, formulate effective countermeasures, and safeguard network security.

## 3 Analysis of the Legality of Data Expropriation in Emergency Situations

### 3.1 Legality of the Subject of Expropriation

According to relevant laws and regulations, the subject of emergency requisition is usually the people's government at or above the county level. In emergencies such as the new coronavirus epidemic, the people's government at or above the county level is authorized to carry out requisition of materials, including data, within its administrative area. Therefore, in an emergency, it is lawful for the people's government at or above the county level or an agency authorized by it to carry out data requisition.

According to relevant laws and regulations, the subject of emergency requisition is usually the people's government at or above the county level. Article 3 of the Emergency Response Law defines "emergencies" as natural disasters, accidents, calamities, public health incidents, and social security incidents that occur suddenly, cause or are likely to cause serious social hazards, and require emergency response measures. This provides a legal basis for judging the urgency of data requisition. Article 12 states, "The relevant people's governments and their departments may requisition the property of units and individuals in order to respond to emergencies." In emergencies such as the New Crown Epidemic, the people's governments at or above the county level are authorized to includes expropriating materials within their administrative areas, including intangible assets such as data.

### 3.2 Legality of Expropriation Procedures

Data expropriation procedures must be carried out in accordance with relevant laws and regulations. In China, laws such as the Constitution, the Emergency Response Law, and the Law on the Prevention and Control of Infectious Diseases provide a legal basis for the Government to expropriate private property, including data, in emergency situations. These laws provide the government with the right to expropriate private property in an emergency, but they also make clear that expropriation must follow legal procedures and the principle of reasonable compensation.

Although the law does not specify in detail the specific procedures for expropriation, the act of expropriation should comply with the basic principles of administrative law, in particular the principle of rational administration and the principle of consistency of power and responsibility. This means that administrative authorities should follow the principles of necessity and appropriateness in carrying out expropriation, avoiding damage to the legitimate rights and interests of the parties concerned, and ensuring the transparency and fairness of expropriation actions. The legality of data expropriation procedures in emergency situations is crucial, and it involves the balance between government power and individual privacy, corporate rights, and interests.

First, the government should publicize information on the purpose, scope, duration, and compensation standards of data expropriation to ensure that the public has a full understanding and oversight of data expropriation. Secondly, the government should follow due process in carrying out data expropriation, including steps such as prior notice, a hearing, and justification. The Government should give notice of expropriation to the expropriated party and give it the opportunity to present and defend itself. Finally, after the government expropriates data, it should give the expropriated party reasonable financial compensation to make up for the loss it has suffered as a result of the data expropriation.

### 3.3 Legality of Compensation for Expropriation

According to the law, the State has the right to carry out expropriation based on the needs of the public interest and to provide compensation. Therefore, after expropriating data in an emergency situation, the government should provide fair and reasonable compensation to the expropriated party in accordance with relevant regulations in order to protect the legitimate rights and interests of the expropriated party. In China, data expropriation and its compensation are usually carried out in accordance with relevant laws and regulations. For example, the Emergency Response Law and other relevant laws stipulate that in case of emergency, the government has the right to requisition required materials, including data resources, in accordance with the law, and clarify the principle that reasonable compensation should be given after requisition.

Data expropriation is usually carried out in unexpected events or emergencies, such as natural disasters and public health events, when rapid access to and analysis of data is crucial for responding to crises. In such cases, the government has the right to expropriate relevant data in accordance with the law to ensure public safety and social order.

After data expropriation, the government should provide financial compensation to the owner or provider of the expropriated data in accordance with the principle of reasonable compensation. The principle of reasonable compensation balances the interests of the state and private interests, embodies the state's right of expropriation in emergency situations, and protects the legitimate rights and interests of data owners. Data expropriation and its compensation follow due process, which includes procedures such as notification and hearings prior to expropriation to ensure the right to information and participation of data owners. At the same time, the compensation should follow the principles of openness and transparency to avoid backroom operations and injustice. Finally, a sound monitoring mechanism, including internal and external supervision, should be established for data expropriation and its compensation. In addition, effective legal remedies, such as administrative reconsideration and administrative litigation, should be provided to ensure that the legitimate rights and interests of data owners are promptly and effectively remedied in the event of infringement.

## 4 Risk Analysis of Data Expropriation in Emergencies

### 4.1 Data Breach Risk

In the complex and detailed process of data requisition, which involves the frequent transmission and in-depth processing of a huge amount of sensitive information, there is a great risk of data leakage if the relevant security measures are not properly implemented. Once the data is leaked, the consequences are unimaginable. This kind of security vulnerability may not only cause unscrupulous infringement of personal privacy, personal identity, property and even action track and other key information into the hands of criminals, but also may pose a serious threat to the business interests of enterprises, leaking the enterprise's core secrets, and jeopardize its market competitiveness. More seriously, if the leaked data involves sensitive areas such as national infrastructure, military, or politics, then the overall security of the country may also be affected.

Taking hacking activities as an example, these highly skilled cybercriminals with impure purposes often aim at the soft underbelly in the process of requisitioning data, such as storage or transmission links, and make use of possible system loopholes to carry out malicious attacks. They cunningly and relentlessly steal sensitive information, which may subsequently be used in illegal transactions, fraudulent activities, or other forms of cybercrime, bringing huge economic losses and mental stress to the victims. Therefore, in the process of data expropriation, the strict implementation and continuous upgrading of security measures are crucial, which is an indispensable part of the protection of personal privacy, corporate interests, and national security.

### 4.2 Risk of Data Tampering

In emergency situations, such as natural disasters, public health events, or major social crises, rapid and accurate access to and processing of data is critical. The authenticity and completeness of data are not only the cornerstone of information communication, but also the key for decision makers to make rational response strategies. Especially in the process of data requisition and transmission, as it involves numerous processing links, such as data collection, collation, validation, analysis, and transmission, any omission in these links may bring risks to the security and accuracy of data.

In occasions of multi-departmental collaboration and cross-regional information sharing, data may be unintentionally modified or intentionally destroyed due to a variety of factors, such as unstable network transmission, malicious human tampering, or simple misuse. Such data distortion not only leads to misleading information transmission, but more importantly, it may directly affect the decision makers' judgment of the emergency situation and the formulation of response strategies. If decision makers make decisions based on incorrect data, the consequences can be catastrophic, not only failing to respond effectively to the emergency, but also exacerbating the severity of the situation through incorrect response measures. Therefore, ensuring the authenticity and integrity of data in emergencies is of irreplaceable importance to crisis management and response.

### 4.3 Risk of Data Loss

In the complex series of processes of data requisition, transmission, and storage, a variety of factors can lead to the loss of data. Technical failures, such as hardware damage, software crashes, or network outages, can trigger the risk of data loss. In addition, human error is an issue that should not be ignored. Whether it is misuse, malicious damage, or poor security awareness, it may pose a threat to data security. Even more unpredictable are natural disasters, such as earthquakes, floods, or fires, which can destroy storage devices in an instant and, in turn, lead to the permanent loss of large amounts of data.

The consequences of such data loss can be extremely serious. In today's data-driven era, data is often the basis for important decisions made by organizations and individuals. Once critical data is lost, and this loss is permanent, decisions made on the basis of this data will lose their foundation, which may lead to wrong judgment, waste of resources, and may even lead to significant economic losses or legal liabilities. Therefore, the protection of data and backup work is particularly important; they are the last line of defense to prevent data disasters.

### 4.4 Technology Management Risk

The application of big data is not limited to a single subject area but involves the in-depth integration of technologies from multiple interdisciplinary fields. This integration requires an in-depth understanding and precise manipulation of various technologies, making the requirements for technology management exceptionally strict. In every aspect of data collection, storage, processing, and analysis, professional technicians are needed for precise operation and maintenance.

However, in emergency situations, such as natural disasters, emergencies, or public health crises, this highly technology-dependent system may face multiple challenges. First of all, technicians may be overstretched for various reasons and unable to respond to problems in a timely manner, which directly affects the efficiency and accuracy of data processing.

### 4.5 Legal and Compliance Risks

The expropriation of data in emergency situations may involve legal and regulatory constraints. If the requisition does not comply with the relevant legal requirements or the necessary authorization is not obtained, legal disputes and compliance issues may arise. In addition, data protection laws vary from country to country and region to region, making it all the more important to exercise caution when expropriating data across borders.

To mitigate these risks, a series of measures need to be taken, such as strengthening data encryption and access control to ensure data security; establishing strict data processing processes and audit mechanisms to prevent data tampering; implementing regular data backup and disaster recovery plans to cope with data loss; strengthening technical team building and technology updating to ensure efficient technology management; and strictly complying with relevant laws and regulations and obtaining necessary authorizations. Authorization, etc.

## 5 Recommendations for Data Requisition in Emergency Situations

### 5.1 Establishment of a Sound Data Requisition Mechanism

In the face of the growing demand for data, the government must act proactively and formulate a set of detailed and clear regulations on data expropriation. This will ensure that every act of data expropriation has a solid legal foundation and moral support, fully reflecting its legality and legitimacy.

In order to achieve this goal, the government needs to regulate data expropriation in all aspects at the legislative level. In the regulations, the prerequisites for data expropriation, the operational process, the rights and obligations of the relevant responsible persons, and the penalties for illegal behavior should be clearly defined. This will not only provide clear guidance for data expropriation but also effectively curb the abuse of the power of data expropriation.

In addition, the government should also establish a comprehensive data expropriation management system, which should cover the entire process of data expropriation, including application, approval, use, supervision, and destruction.

In the application process, it should be clearly stipulated which departments or organizations have the right to make applications, as well as what materials need to be submitted and what conditions need to be fulfilled in the application. During the approval process, a specialized approval body should be set up to conduct a rigorous review in accordance with established standards and procedures to ensure that only applications that meet the requirements of the legislation and the purpose of data expropriation are approved.

Finally, when data are no longer needed, clear processes and standards for data destruction should be established to ensure that data are thoroughly and securely destroyed and to prevent potential risks arising from data residuals. Through the implementation of these measures, the government can more effectively manage data expropriation and protect individual privacy and data security, while also providing a solid institutional guarantee for the rational use of data.

## 5.2 Enhancing Cross-sectoral Data Sharing and Collaboration

In emergencies, an efficient data-sharing mechanism should be established between departments to ensure the timely transmission and effective utilization of information. Comprehensive monitoring and rapid response to emergencies can be realized through cross-departmental collaboration.

Enhance the intelligence of data requisitioning technology: use big data, artificial intelligence, and other technical means to improve the efficiency and accuracy of data requisitioning. For example, intelligent algorithms can be used to screen, analyze, and predict data to provide decision makers with more valuable information.

## 5.3 Guaranteeing Data Quality and Reliability

When requisitioning various types of data, we must pay great attention to and ensure the authenticity and accuracy of the data obtained. This is because the reliability of the data has a critical impact on subsequent data analysis and decision-making. There are a number of measures we can take to achieve this goal.

The first priority is to establish a comprehensive data quality assessment system, which should cover multiple aspects such as data source verification, integrity assessment, and consistency checking. In addition, the active use of advanced data cleaning techniques can effectively eliminate duplicated, erroneous, or incomplete data and further improve the overall quality of the dataset. At the same time, data validation techniques are indispensable, as they can detect and correct outliers in the data in a timely manner, thereby greatly reducing the interference of erroneous information in data analysis and decision-making. Through these comprehensive measures, we can significantly improve the quality of the requisitioned data and lay a solid foundation for subsequent in-depth research.

## 5.4 Respect for and Protection of Personal Privacy

In expropriating personal data, we must always bear in mind that privacy is a fundamental right of every individual and should strictly comply with the privacy protection regulations set by the State. These regulations aim to ensure that the personal privacy of citizens is not unlawfully accessed, abused, or disclosed, thereby safeguarding the dignity and information security of every individual. In order to achieve this goal, we can take a variety of effective measures.

First of all, sensitive information in personal data can be replaced or blurred through desensitization technology, so that even if the data is leaked, it will be difficult for attackers to obtain real personal information from it. For example, key information such as identity card numbers and telephone numbers can be partially hidden or replaced by asterisks, thus reducing the risk of privacy leakage.

Secondly, encrypted storage is also a key measure to protect personal information security. By using advanced encryption algorithms, we can ensure that personal information stored in the database is difficult to decrypt and read even if it is illegally accessed. In this way, even when faced with the risk of data leakage, personal privacy can be protected from invasion to the greatest extent possible.

In summary, by strictly complying with privacy protection regulations and combining technical means such as desensitization processing and encrypted storage, we can effectively protect the security of personal information and ensure that everyone's right to privacy is fully respected and safeguarded. When requisitioning personal data, privacy protection regulations should be strictly observed to ensure that personal privacy is not compromised.

## 6 Concluding Remarks

This paper provides an in-depth discussion of data expropriation in emergencies, analyzing its necessity, legality, and challenges in implementation. Through this study, we recognize the importance of reasonable and legitimate data expropriation in emergencies to improve the efficiency of emergency response and protect public safety. However, there are still limitations in this study, such as the diversity of data sources and the generalizability of the research methodology that could be improved. In the future, we will continue to explore the balance between data expropriation and personal privacy protection, with a view to providing stronger support for relevant policy formulation and practical operation.

With the continuous progress of technology and the rapid development of society, we believe that the issue of data expropriation will receive more and more attention, and due to the continuous development of artificial intelligence technology, data expropriation will become more intelligent in the future. Natural language processing, image recognition, and other technical means can be used to realize automatic identification and extraction of various types of data and improve the efficiency and accuracy of data requisition. With the popularization of cloud computing, blockchain, and other technologies, data sharing will be more convenient and secure, and real-time data sharing and exchange can be realized between departments to improve the collaborative operation capability in emergency situations. With the rapid development of IoT, 5G, and other technologies, the type and scope of data that can be requisitioned will be more extensive in the future. For example, real-time data can be collected through smart sensors, drones, and other devices to provide more comprehensive information to support emergency situations. In the future, with the continuous progress of privacy protection technology, effective data expropriation can be realized while safeguarding individual privacy. For example, technical means such as differential privacy and federated learning can be adopted to ensure the privacy and security of personal data.

In the future, it is expected that measures will be taken to establish a sound data requisition mechanism, strengthen cross-departmental data sharing and collaboration, and enhance the level of intelligence in data requisition technology in order to improve the efficiency and accuracy of data requisition. At the same time, with the continuous development of technology, the requisitioning of data in emergencies will be more rationalized, programmed, intelligent, convenient, and safe.

# References

[1] Zeng, C.X. & Zhu, X. Z. (2022). Establishing a Data Compulsory Licensing System in the Context of the Digital Economy: Rationality,Basic Principles, and Regulatory Approaches— From the Perspective of Data as Essential Facilities. *E-Government*, (2).

[2] Feng, X. Q. (2022). Research on the Protection of Commercial Data from the Perspective of Intellectual Property. *Comparative Law Research*, (5).

[3] Shi, W. D. (2022). On the Legal Promotion of Digital Transformation in Municipal Social Governance. *Politics and Law*, (3).

[4] Jin, C. B. (2021). On the Construction of the Emergency Requisition System. *Henan Social Sciences*, (4).

[5] Liu, Q. (2019). On the Data Reporting Obligations of Online Platforms. *Contemporary Law Research*, (5).

[6] Zhang, L. (2020). The Emergency Requisition Authority and Its Legal Control in Operation: A Doctrinal Analysis Based on Article 12 of China's Emergency Response Law. *Politics and Law*, (11).

[7] Zhou, X. P. (2022). On the Protection of Corporate Data Rights in the Big Data Era. *Chinese Journal of Law*, (5).

[8] Yang, Y. C. (2021). Optimization of Governance Mechanisms for Sudden Public Crises under Big Data Thinking. *Socialist Research*, (6).