Science of Law Journal (2025)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2025.040518
ISSN 2616-2296 Vol. 4 Num. 5

Research on the Determination of Damages Caused by Data Leaks

Zeng Yi

China Jiliang University, Hangzhou, China

Keywords: Data Leakage; New Type of Damage; Damage Determination; Rule Construction

Abstract: In the era of big data, people's lives have undergone rapid and continuous changes. Daily necessities such as food, clothing, housing, and transportation have become increasingly convenient and efficient. However, the resulting data leaks have also triggered a series of new problems. In this regard, the first step should be to consider the essence of data leaks, identify the subjects involved in the data leaks, and analyze the sensitivity and secrecy of the data. Data leaks should be regarded as a new type of damage. Secondly, the new types of damages caused by data leaks should be classified in terms of their types, and they should be divided into actual property losses and mental damages. We need to identify the flaws and shortcomings in the determination of the new types of damages caused by data breaches, eliminate the problem of overly long causal chains of indirect damages, optimize the quantification standards for actual property losses, incorporate necessary prevention costs into the determination system, expand the scope of damages in a restricted manner, re-evaluate the constituent elements of mental damages, draw on foreign experience, gradually weaken or even eliminate the severity standards for mental damages, and appropriately reduce the burden of proof for the victims. In addition, the subsequent risk and damage issues arising from the occurrence of new types of data leaks should also be considered as a damage determination rule.

1. Introduction

Big data is increasingly profoundly changing the existing world and even redefining human understanding of knowledge.[1]With the rapid development of information technology, the production, storage and exchange of data have become unprecedentedly convenient and rapid. The rapid development of information technology and digitization have brought huge convenience and benefits to human society. Whether it is the digital management of personal daily life, the intelligent confidential data of enterprise operations, or the digital economy construction at the national level, almost all important information is stored and transmitted in an electronic form. It can be said that data is everywhere in the real society and has an irreplaceable position and role. At the same time, the wide application of data has also brought unprecedented security challenges. One of the most prominent problems is data leakage. Data leakage has become a serious security issue worldwide. It not only causes the loss of personal privacy or property damage to the victims, but may also seriously affect the brand reputation, competitiveness of enterprises, and even pose a threat to national security.

2. The Presentation of the Problem

2.1 Nature of Data Leakage Damage

Data leakage generally refers to the situation where personal data, especially sensitive data, is lost, stolen, tampered with, damaged, or otherwise accessed or disclosed without authorization during the collection, storage, processing, and transmission of data, thereby endangering the confidentiality, integrity, and availability of these data. Such situations may involve sensitive personal information, business secrets, and even national secrets.[2]Regarding whether data leakage constitutes damage, there is considerable controversy both in theory and in judicial practice. Some scholars believe that data leakage is a new type of damage.[3]Some other scholars believe that data leakage is essentially a form of data infringement rather than a consequence of damage.[4]In judicial judgments, there is a middle-ground view that data leakage can also constitute damage in certain specific circumstances. However, it is necessary to consider whether the behavior has exceeded reasonable limits, the manner and scope of the leakage, as well as the privacy of the data.[5]Regarding the various viewpoints on data leakage mentioned above, this article is more inclined to and supports the first one, which is that data leakage can be regarded as a new type of damage and evaluated separately.

The primary characteristic of data leakage is its riskiness. The riskiness of data leakage refers to the negative consequences that may arise from unauthorized access, disclosure, or abuse of sensitive data within individuals, organizations, or systems. Data leakage can pose various risks to individuals, which not only involve financial losses but also may affect personal privacy and identity security.

The second characteristic of data leakage is its invisibility. After a data leakage incident occurs, there may be no direct physical loss or visible damage, but the consequences and impacts can be extensive and far-reaching, and are often difficult to be detected immediately. Since most data leakage incidents take place in a virtual environment, the leaked content is often intangible digital information that cannot be perceived directly with the naked eye. Moreover, the collection and analysis of data are usually carried out without the consumers' knowledge. Even if consumers suspect they have been infringed upon, they may not be able to determine the responsible party or lack sufficient evidence to prove the infringement and demand compensation. The intangibility of data leakage makes it difficult to immediately assess and reflect its impact, yet it may lead to long-term and severe consequences.

Data breaches usually have long-term effects that are difficult to detect. The invisible dissemination of data on the internet makes it almost impossible to control. Once leaked, the ownership of the information is almost lost, and the recovery process is extremely challenging.

2.2 Analysis of Data Leakage Actors

During the process of data processing, utilization and generating profits, it usually involves several parties. The first and foremost is the individual or enterprise that generates the data, which we can refer to as the data controller. The "data controller" is a role defined in the European General Data Protection Regulation (GDPR). It refers to the entity or individual responsible for determining the purpose and method of processing personal data. In other words, the data controller is the party that decides why and how data is collected and used.

The second entity involved is the data processor. From the perspective of the entities that bear the obligation for data security protection, a data processor refers to all entities that engage in data processing activities, namely, natural persons, legal persons or unincorporated organizations that undertake actions such as data collection, storage, use, processing, transmission, provision, and disclosure.[6]Data processors usually do not have the right to decide on the collection, purpose or processing method of the data. Their role is to process, store or manage the data as required by the data controller. Whether obtaining or exercising data ownership rights such as possession, usage or

operation rights, data processors must not harm the rights of the data source.[7]

2.3 Distinction of Data in Data Breaches

In the context of data leakage, it is crucial to have a differentiated understanding of the data. Based on its sensitivity, the data can be classified into two categories: the first is ordinary data, which refers to data without specific privacy protection requirements. These data usually do not cause serious harm to individuals or organizations after leakage. The second is sensitive data. Sensitive data are those that, after leakage, may cause significant damage to personal privacy, economic security, reputation, etc. At the same time, the leakage of sensitive data has its particularity. Even if it has not yet caused downstream damage, the victim can also demand compensation for the resulting mental distress and risk damage, including the expenses spent for preventing the damage. When determining whether the data collection and processing party is responsible for the damage, the data type and downstream damage are important bases for determining liability.[8]

2.4 Definition of Types of Data Leakage Damages

(1) Actual Direct Property Damage

For individuals, when payment information, bank accounts, credit card information, or other financial data are leaked, malicious users may use this information for fraud, resulting in direct financial losses. For instance, stealing a credit card for illegal consumption or transfers. In many countries and regions, there are laws regarding data protection. If the data leakage is proven to violate these laws, enterprises may face huge fines. At the same time, in cases where personal information or sensitive data is leaked, enterprises may also need to pay compensation to the affected users.

(2) Mental Damage

Data leakage not only causes victims to suffer economic losses, but also may lead to severe mental damage. With the continuous development of the cyber space, its searchability and permanence prevent things that people originally expected to fade away over time from disappearing, resulting in the long-term nature of mental and reputation damage, thereby exacerbating the consequences of the damage.[9] These mental damages include anxiety, fear, emotional trauma, damage to one's career and social reputation, as well as the resulting physical and mental health problems.

3. Defects and Limitations in the Determination of Data Leakage Damage

3.1 The extent of data leakage damage is unclear

In data leakage incidents, indirect damage refers to losses or adverse effects that result from the data leakage but are not directly caused by the leakage itself. Such damages are typically indirect and cumulative, and it is difficult to establish a clear causal relationship with the leakage event directly. Because apart from expressions such as "particularly" or "exceptional" damage amounts, the next step is that the damage consequences must be "exceptionally distant" or the damage must be "particularly distant". Usually, indirect damages do not occur immediately but gradually manifest over time. Due to the inconsistent legal frameworks in different regions, the determination of indirect damages after data leakage lacks universality and consistency. In legal and practical evaluations, how to define the scope of indirect damages depends on various factors, and the situations of each case may vary greatly, thus it is difficult to have a clear standard.

In the determination of data leakage damage, the necessary preventive costs refer to the expenses that must be paid to prevent or mitigate the potential damages caused by data leakage. After a data leakage occurs, there may be various types of damages, and it is necessary to apportion the

responsibilities and corresponding costs. However, if the contract terms are unclear or there is no specific provision in the contract on how to apportion the relevant costs after the leakage, it is prone to cause attribution issues. At this time, it may be necessary to resolve the issues of responsibility and cost allocation through legal means.

3.2 Difficulty in quantifying property losses

One major issue currently faced by our country in the determination of data leakage damage is that the damage caused by data leakage is difficult to be directly quantified. Traditional damage determination mostly relies on the standards of property loss or personal injury, but the damage caused by data leakage often not only manifests as direct economic losses, but may also involve damages to users' privacy rights, reputation rights, credit risks, etc. At this time, in the pure economic losses, the size of individual losses and social losses may be different, and it is very likely that the social losses are smaller than the individual losses.[10]On the other hand, the damage caused by data leakage has a high degree of uncertainty. The scope, degree and time span of the damage may not be immediately clear when the leakage event occurs.

3.3 There are disputes regarding the determination of risks and anxiety damage.

In the assessment of the damage caused by data leakage, there is a disagreement regarding the assessment of risks and anxieties. The reason is that the determination of anxiety and risks relies on the individual emotional experiences and expectations of the victim, making it difficult to provide objective and standardized measurement standards, resulting in a large number of disputes. Unlike actual property losses, mental damage and emotional damage usually lack unified and objective measurement tools. In many judicial decisions, the causal relationship between anxiety and psychological damage and data leakage incidents is difficult to directly prove. The degree of anxiety and risk often requires reliance on psychological assessment and subjective judgment, which leads to significant differences in the standards for assessing anxiety and risk damage by different courts. Although in some legal systems, the possibility of mental damage caused by data leakage events has begun to be gradually recognized, overall, many legal systems are still relatively conservative and reluctant to widely recognize risk and anxiety damage as part of compensation.

4. The improvement and establishment of the rules for determining the damage caused by data leakage

4.1 Restrictive Expansion of Damage Scope

In the determination of data leakage damage, the restrictive expansion is mainly aimed at reasonably defining the scope of damage, to prevent the losses caused by data leakage from being overestimated or abused. The restrictive expansion helps to clarify which damages are indeed directly or indirectly caused by data leakage. The "Personal Information Protection Law" and "Data Security Law" in China have made certain regulations on data protection to some extent, but they have not specified the scope of damage. Therefore, there is much discussion on the scope of damage in the academic community. Some scholars believe that the act of infringement itself constitutes damage.[11]Some scholars believe that the increased risk resulting from data infringement should be regarded as a form of damage.[12]Some scholars also advocate for presuming the existence of intangible damages, incorporating expected benefits into the category of economic damages, and expanding the scope of application of personal injury. Furthermore, there are also scholars who support a partial acceptance of the new types of damages.[13]When determining the extent of the

damage caused by data leakage, it is necessary to clearly define which types of damage can be regarded as legitimate and reasonable. In law, damages are often assessed based on the "predictability principle". In practice, a combination of quantitative and qualitative assessment methods is required.

4.2 Introduce risk damage as a determination criterion

Data breaches usually cause subsequent risks and damages. Adding "risk damage" as a criterion in the assessment of data breach damages is mainly to more comprehensively evaluate the potential impacts brought about by data breaches, especially when the actual damage has not yet fully manifested. At this point, it is necessary to entrust the determination of damage risks to judicial adjudicators in individual cases. The basic approach here should be scenario-based, and the judgment should be made by comprehensively considering factors such as the type and processing method of the data.[14]This requires clearly stipulating "risk damage" through relevant laws and regulations. The definition of risk damage can be added to the existing legal framework such as the "Cybersecurity Law" and the "Personal Information Protection Law", and the applicable scope of risk damage in data leakage incidents can be clearly defined.

4.3 Reconstruction of the Elements for Determining Mental Injury Compensation

In the assessment of the damage caused by data leakage, the type of indirect damage most directly related to the actual incurred property damage is the mental type of indirect damage. However, it is quite different from property damage. Although mental damage is relatively easy to identify and obtain compensation, in actual judicial decisions, the evidence submitted is often insufficient to prove that the victim has suffered sufficient mental torture. In comparative law, the requirement for the severity of mental damage has gradually weakened. The EU's "General Data Protection Regulation" and the new data protection legislation in Germany have not set a severity standard for data leakage damage. Therefore, the author believes that foreign experience should be referred to for application, and the mental damage should be reconstructed. The "severity" standard should be appropriately relaxed to fully protect the rights and interests of the victim while ensuring fairness and justice.

4.4 Introduce necessary rules for prevention costs

The necessary prevention costs refer to the expenses that victims incur to take appropriate preventive measures after experiencing events such as data breaches in order to prevent the damage from further expanding or reduce potential risks in the future. When introducing the prevention cost rule, it is necessary to clearly define what constitutes "necessary prevention costs". Such costs should be reasonable and directly related to the consequences of the data breach. These costs should be reasonable expenditures made to avoid greater damage caused by the data breach.

5. Conclusion

With the continuous development and popularization of information technology, data leakage incidents have become increasingly frequent and have far-reaching impacts. Data, as an important resource, its protection and management directly affect personal privacy, corporate reputation, and social trust. However, the issue of damage determination caused by data leakage often faces complex legal, economic, and social challenges. This thesis conducts research on the damage determination of data leakage, explores the multi-dimensional types of damage and their legal responsibilities, analyzes the deficiencies in the existing legal framework, and proposes a more scientific and reasonable damage determination model. It is hoped that this research can provide valuable references

for theoretical research and practice in related fields, and encourage more scholars and practitioners to pay attention to the issue of damage determination of data leakage, contributing to the construction of a safer and fairer information society.

References

[1] Danah boyd, Kate Crawford. Six Provocations for Big Data[C].A Decade in Internet Time: Symposium on the Dynamics of the Intemet and Society, 2011(09).

[2] Clara Kim. Granting Standing in Data Breach Cases: The Seventh Circuit Paves the Way towards a Solution to the Increasingly Pervasive Data Breach Problem[J]. Columbia Business Law Review, 2016: 544-546.

[3] Ye Mingyi. The Protection of Personal Information by Tort Law[J]. Legal Studies, 2018,(04):88.

[4] Wang Yiqiang. The Recognition of Data Infringement Damages from the Perspective of Judgments [J]. Journal of East China University of Political Science and Law, 2023,(5):78.

[5] See (2019) Beijing Internet Court No. 16142 Civil Judgment.

[6] Cheng Xiao. On the Obligations of Data Security Protection[J]. Comparative Law Studies, 2023,(2):64.

[7] Ruan Shenyu. On the Generalized Path of Data Ownership[J]. Wuhan University Journal (Philosophical and Social Sciences Edition),2024,(5):157.

[8] Xie Hongfei. The Liability of Information Processors for Downstream Damages Caused by Information Infringement[J]. Legal Application, 2022,(1):23.

[9] Xu Ming. The Privacy Crisis in the Era of Big Data and Its Legal Response in Infringement Law[J]. Chinese Law, 2017, (1):130-149.

[10] Wagner. Münchener Kommentar[M]. Munich: C.H.Beck, 2009:826.

[11] Maxwell E. Loos. Exposure as Distortion: Deciphering Substantial Injury for FTC Data Security Actions[J]. George Washington Law Review Arguendo, 2019,(87):42.

[12] Jennifer Wilt. Cancelled Credit Cards: Substantial Risk of Future Injury as a Basis for Standing in Data Breach Cases[J]. SMU Law Review, 2018,(71):615.

[13] Ye Mingyi. Infringement Protection of Personal Information[J]. Legal Studies,2018,(4):88.

[14] Tian Ye. Risk as Damages: The Innovation of the Concept of Infringement Damages in the Era of Big Data[J]. Politics and Law, 2021(10):25-39.