Justification of Risky Damage from Personal Information Infringement and Improvement of Recognition Pathways

Zhenyingzi Jin
Law School, China Jiliang University, Hangzhou, Zhejiang, China

Abstract: As the core element of personal information tort liability, damage is also the premise of the application of damage compensation. As the infringement of personal information presents new characteristics and damage forms in the era of digital economy, the consequences of the infringement of personal information are often reflected in the risk of damage suffered by the victim in the future, and the traditional relief of infringement damage has great limitations in dealing with it, so it is necessary to recognize the concept of risk damage. The revision of the concept of damage, the theory of risk allocation under the risk society, and the international practice of the expansion of the concept of damage provide a legitimate basis for the recognition of risk damage. Through the dynamic system of evaluation criteria, the identification dilemma of risk damage can be eliminated by integrating factors such as the type of personal information, the purpose, mode, consequences, and scope of influence of behavior. To achieve better protection of personal information rights and interests.

Keywords: Infringement of Personal Information; Risky Damage; Future Risks; Damage Determination; The Improvement of the Path

1. Introduction

In today's society, the rapid development of internet technology has promoted the prosperity of the data industry, making personal information increasingly valuable in the social and economic aspects of the big data era. However, as people's production and lifestyle become more informatized and intelligent, the collection and utilization of personal information have become easy, thus posing unprecedented challenges to personal information security. Ubiquitous information processing behaviors make it easy for the legitimate rights and interests of information subjects to be infringed, and illegal invasions of personal information occur frequently, in various forms and in large numbers.

Besides the conventional property damage and mental harm, there are new types of damage that are different from traditional ones, more manifested as potential risks, with concealment, uncertainty, and irreversibility. As a private law remedy, infringement damage compensation provides information subjects with the opportunity to claim rights and demand compensation from infringers under the current framework of the Personal Information Protection Law (hereinafter referred to as the "PIPL"). When personal information rights are damaged, information subjects often rely on the infringement damage compensation route to seek relief. Damage is a core element of infringement liability, and its recognition is the first step to obtain compensation. However, in the current situation where new forms are emerging in large numbers, the traditional "difference theory" is at a loss in recognizing such new types of damage—mainstream views require that damage must be actually incurred, which conflicts with the characteristics of risk-based damage. Given that risk-based damage has not yet been substantially converted into quantifiable actual losses and is accompanied by significant "uncertainty," these damages are often difficult to be included and recognized under the traditional definition of damage in infringement law.

In judicial practice, personal data breach cases where "damage" is difficult to be recognized and thus fail to obtain adequate and timely judicial relief are not uncommon. Therefore, acknowledging risk-based damage and establishing a unified recognition rule is crucial for safeguarding the rights of information subjects. Next, we will delve into the judicial status quo and challenges in the

recognition of risk-based damage in the field of personal information, as well as the necessity, justification, and establishment of recognition rules for introducing risk-based damage.

2. Personal Information Infringement Damage Recognition Status and Challenges

2.1 Judicial Status

With the advent of the big data era, the collection and utilization of personal information have become increasingly convenient. However, this has also led to a frequent occurrence of personal information infringement cases. The risks associated with personal information infringement have already attracted attention from all sectors, but in judicial practice, courts tend to adopt a cautious or conservative attitude when dealing with claims for risk-based damages due to multiple reasons.

When delving into the issue of compensation for damages caused by the leakage of personal information, case searches reveal a phenomenon: courts generally recognize that there is an infringement of personal information rights or privacy rights in personal information infringement cases. However, for victims' claims of compensation based on potential risks, the mainstream approach of courts is to reject the claims of the information subjects regarding damages, or to limit it to stopping the infringement, restoring reputation, eliminating the impact, and apologizing. For example, in the case of Sun Mou mou and Mobile Company Privacy and Personal Information Protection Dispute Case [(2021) Lu1602 Min Chao 83, Bin zhou City, Bin cheng District, Shandong Province People's Court], the court held that the defendant's marketing methods directly infringed on the data subject's right to know and the right to choose not to be processed. However, in this case, the data subject's claim for compensation based on potential future damage risks was not supported by the court. Similarly, in the case of Wang Mou and Shenzhen Tencent Computer System Co., Ltd. Personal Information Protection Dispute Case [Guangdong Shenzhen Intermediate People's Court Civil Judgment (2021) Yu03 Min Zhong 9583], the court held that the appellant Wang Mou did not provide evidence proving the "damage" required by the Personal Information Protection Law. Therefore, without evidence proving that the use of WeChat publicly available personal information by the WeChat app caused serious consequences or damage, the court did not support the appellant Wang Mou's claim for compensation for personal rights damage caused by the respondent Tencent Company.

Risk, an intangible concept, often poses significant challenges for legal recognition due to its association with uncertainty. This is particularly true in cases of personal information infringement, where the potential harm caused by risk is often difficult for judges to acknowledge. This can be seen in the aforementioned cases. In China, courts have not yet formed a unified view or approach to the recognition of such harm caused by risk. This inconsistency and ambiguity in legal recognition undoubtedly increase the difficulty for parties in the process of rights protection [1].

2.2 Existing Challenges

"No remedy without harm," damage being a core element of tort liability, its recognition is the first step to obtaining compensation. The Personal Information Protection Law (referred to as the 'Personal Information Law') was enacted to effectively regulate personal information infringement behaviors, and Article 69 provides strong legal support for the claim of information subjects. However, "damage" as a core element of tort liability adds numerous obstacles to the claim of information subjects. In traditional tort law, "damage" usually requires objective reality and certainty. However, the damage caused by the infringement of personal information often has potential, uncertain characteristics, making it difficult for information subjects to prove the existence of "damage" in specific cases, thus they are long-term threatened by various potential risks without compensation.

The main principle of traditional tort law generally requires that harm must be clearly and actually occurred, which is significantly incompatible with the characteristics of harm that may result from the infringement of personal information. As a renowned legal scholar has pointed out, harm not only needs to have objective reality but also, in practical operations, it is only in extreme cases, when a

real threat to individuals or society actually exists, that such danger will be recognized by law and considered as harm [2]. This viewpoint is reflected in many cases of personal information disputes. In the aforementioned case two, the court explicitly stated, "Harm is an essential element of all liability for damages. Without harm, there is no compensation. In personal information infringement tort disputes, the plaintiff must prove the harm they have suffered as a result of the defendant's infringement to demand compensation." However, traditional methods of harm recognition are inadequate when it comes to identifying potential, unknown, and uncertain future harms in cases of personal information infringement.

3. Risk-Based Damage

3.1 Overview of Risk-Based Damage

Some new forms of harm that have gradually emerged in cases of personal information infringement are risk-based harms, which refer to potential harms that have not yet occurred but have the possibility of occurring at any time. Risk-based harms differ from actual harms, focusing on the potential risks that may bring disadvantages to the subject.

The risk-based harms that personal information infringement subjects face have attracted the attention of many scholars, and many scholars have expressed their views on this issue. Regarding whether the risk-based harms caused by personal information infringement can be recognized as "harm," there are various scholarly perspectives, mainly including the affirmative view, the negative view, and the compromise view.

Most scholars agree that the current standards for identifying damage in traditional tort law are not suitable for the forms of infringement in the field of personal information in the era of big data. It is necessary to revise and adjust the concept of "damage" in personal information. If the existing legal framework is not promptly revised and transformed, it will severely hinder the thriving development of the data industry and the protection of individual personal information rights. Therefore, it is necessary to recognize and accept the concept of "risk-based damage" as a new form of damage. However, some scholars hold a negative view, arguing that the premise for damage compensation must be actual, substantial damage. These scholars adhere to the view of actual damage, believing that damage can only be recognized when it can be clearly proven that there is property damage or mental damage. They emphasize "certainty" as a prerequisite for damage recognition, arguing that compensation can only be demanded from the infringer when the damage has actually occurred and can be clearly quantified [3]. Among scholars, there is also a compromise view, which acknowledges that risk itself does not directly equate to damage, but the existence of risk cannot be ignored. It is a latent threat that may trigger a series of potential negative impacts at any time. These impacts not only include potential property loss, but may also lead to severe mental damage for individuals in specific situations. Therefore, even if the concept of "risk-based damage" is not fully recognized in legal terms, it is important to deeply understand that in the context of illegal infringement of personal information, even if no explicit actual damage has occurred, the anxiety, concerns, and additional expenses incurred to prevent potential risks that the information subject bears are real economic and mental burdens, which should be taken into account in the scope of compensation[4]. Currently, in judicial practice, in a few cases in China, the concept of risk-based damage caused by infringement of personal information is supported, but the mainstream view still denies or ignores risk-based damage. The following section will discuss the necessity of the existence of risk-based damage in the field of personal information.

3.2 The Traditional "Difference Theory" Has Limitations

Damage is the cornerstone for the victim to claim infringement damages, and it is an indispensable core element in the entire system of infringement law. In the current legal framework of China, traditional tort law primarily uses the difference theory to determine the existence of damage. The difference theory originates from Mommsen's advocacy of the interest theory, which defines damage as the difference in the hypothetical property status before and after the occurrence of the damaging event [5]. However, using the difference as the method to determine the

existence of damage has certain limitations in recognizing the special forms of damage in new types of personal information infringement.

First of all, personal information infringement damage has a latent characteristic. The act of information leakage is merely a prerequisite for subsequent other infringement behaviors. The stolen personal information will not be immediately used for subsequent infringement; instead, it will go through a series of deletion, selection, and other processes by the infringer before being used for subsequent crimes. After the leakage incident occurs, the damage consequences are gradually derived, and the damage facts may not be fully revealed for a period of time or even several years, rather than immediately. In today's highly developed information age, the collection, exchange, circulation, and utilization of information often take place in a covert manner, and many times, the information subject is unaware of it. This highly covert data flow method often causes the illegal collection and utilization of personal information without the information subject's knowledge. What is even more concerning is that many people do not realize that their personal information security has been threatened before they discover that their information is being misused. Traditionally, it is usually determined whether there is "damage" based on the "difference theory." This means that damage is only recognized when the property of the information subject suffers actual losses, i.e., there is a clear "difference." However, in the field of personal information protection, this standard of judgment is not entirely applicable. When facing the potential risks brought about by personal information infringement, it cannot be limited to whether there is a clear "difference" in property losses. In fact, even if the property of the information subject has not suffered obvious economic losses, the intrinsic value of their personal information may have already suffered a significant reduction. Although these damages may not be immediately apparent, they have a profound impact on the information subject. Therefore, it cannot be solely dependent on the traditional "difference theory" to determine whether there is damage.

Secondly, personal information infringement damage often has uncertainty. Compared to actual damage, the greatest difference of risk damage is its uncertainty [6]. Risk damage caused by personal information infringement is uncertain in many aspects. First, whether the risk damage after infringement will be converted into actual damage is uncertain; second, the purpose and use of the infringing personal information before the actual damage occurs are uncertain and cannot be accurately predicted; third, the target of risk damage is uncertain, which is different from traditional infringement behavior [7]. Due to the rapid spread of information brought about by big data technology, the number of information subjects who can be identified will continue to increase over a period of time, and the number of information subjects who suffer from risk damage is also changing [8].

Finally, personal information infringement damage also has irreversibility. Once personal information is leaked, the risk damage caused by it is irreversible, and it is difficult to completely eliminate such damage through subsequent remedial measures. Although processors can take various measures to prevent further damage, such as enhancing security systems, identifying and fixing potential vulnerabilities to prevent future attacks and leaks, the risk damage caused by leaked personal information cannot be compensated or reversed. In other words, subsequent repair and remedial measures cannot restore the risk damage caused by the leakage of personal information.

Based on the above characteristics, if the law ignores the risk of risk damage and adheres to the difference theory, waiting for actual damage to occur before providing relief, it cannot achieve the function of protecting the legitimate rights and interests of data subjects, and will also highlight the lag in rights relief [9].

3.3 Current Rules Are Difficult to Effectively Remedy Risk Damage

If we adhere to the boundaries of traditional definitions of harm, and wait until actual risk-based damages occur due to personal information infringement, the path to compensation for the victim will be much more difficult. First, proving causality will be an extremely challenging task. Personal information leaks can have various causes, and once the information is leaked, it is unknown

where it will go, making it difficult for the victim to determine a direct link between the loss and the leak of personal information. Additionally, given the possible long period between the occurrence of risk-based damages and the infringement event, this also means that the data subject may still face the issue of the statute of limitations expiring. The potential risks triggered by personal information leaks do not have a fixed time point and may persist for a long time, leading to the data subject being continuously exposed to the risk of damage over a long period. Traditional damage compensation systems require that the damage be tangible or imminent. Sometimes, data breaches or misuse may not immediately result in tangible economic losses or rights violations, but the potential threats and hazards may quietly grow. These potential damages may not occur immediately and may be difficult to confirm whether they will indeed occur. They may erupt like a dormant virus at some point in the future, causing unforeseen losses to the victim. Moreover, due to the relative lag in technological development and legal frameworks, the time of damage occurrence may even exceed the statute of limitations period for data infringement lawsuits.

Even if a data platform's fault or negligence leads to personal information infringement or data leaks, the victim still cannot obtain corresponding infringement damage compensation if it cannot be proven that there is actual and ascertainable property loss. Clearly, this standard is too strict and does not help protect the rights of the victim. Whether or not it meets the conditions of being "truly imminent," "serious," or "obvious," the literal interpretation will prevent almost everyone from seeking compensation based on concerns about future infringements, thereby significantly reducing their chances of filing a lawsuit or obtaining compensation [10].

4. Acknowledge the Justification and Feasibility of Risk-Based Damages

4.1 Modify the Concept of Harm to Provide Recognition Space

Under the consideration of pragmatism, traditional tort law tends to focus on actual damages that have already occurred, such as personal injuries and property losses. However, this does not mean that potential damages that subjects facing risks might suffer can be ignored. For example, French courts have recognized that, in certain circumstances, even if the damage has not yet occurred, if there is sufficient and convincing evidence indicating that the damage is highly likely to occur, such future damage should also be considered as meeting the certainty condition [11]. This view breaks the traditional limitations of tort law in damage recognition, providing a more comprehensive consideration of the actual and potential risks that victims may face. Additionally, American courts have also acknowledged risk-based damages in traffic accident cases. For instance, in one traffic accident case, the victim suffered a severe concussion due to a violent impact, which led to a risk of epilepsy attacks that could occur throughout their life. After the second-instance court's review, the court determined that the victim's risk of seizures was directly related to the collision and was a direct result of the increased risk of harm caused by the defendant's actions. Therefore, the court ruled that the victim would have to bear long-term medical expenses, potential income losses, and the mental suffering caused by these. Based on these considerations, the court ultimately ruled that the defendant must bear the corresponding compensation liability. In the above-mentioned scenario, if the difference theory is applied, it can be observed that the information subject has not experienced a significant change in property, which leads to difficulties in damage recognition and thus prevents compensation, which is clearly not conducive to the protection of current personal rights. It is evident that the difference is not equivalent to damage, and in specific cases in judicial practice, it is constantly being revised and innovated, and the concept of damage is not static.

4.2 Allocation and Equitable Distribution of Risk

In the context of risk allocation theory, it must be acknowledged that failing to make amendments to traditional damages would lead to an imbalance in risk distribution, making it difficult for personal information rights to be adequately protected. The recognition of risk-based damages is somewhat justified.

With the advent of the big data era, modern society has gradually evolved into a risk society. Many scholars in China have expressed their agreement and support for the concept of a risk society. In today's highly informatized society, high risks are inevitable, and the high level of informatization brings unprecedented new harms to individuals and society. These harms are characterized by their severe impact and large scale, and their occurrence is often unpredictable, making it difficult to prevent in advance and complicating the issue of responsibility attribution. Therefore, risk control and risk allocation are particularly important in the information age. In the digital economy era, a large amount of data and information is collected, exchanged, bought and sold, and leaked, highlighting that the risk of personal information infringement is no longer a small probability issue for an individual, but a systemic risk faced by the entire society.

In the internet big data era where information is easily collected and utilized, the positions of information subjects and information processors have become increasingly imbalanced. Information processors, with their vast amount of personal information and the ability to collect and process information, gain economic benefits, while information subjects are in a disadvantaged position, often unable to control and prevent risks in advance. Given this situation, it is reasonable for information processors to bear more risks, and treating risks as compensable damages is a way to achieve risk allocation [12]. They are the source of risks and the creators of risks, and they also have the responsibility and capability to control and manage these risks. They gain from information, and should therefore bear corresponding responsibilities; information processors have multiple ways to avoid or mitigate risks; more importantly, making information processors bear more risks can encourage them to place greater emphasis on risk prevention, thereby more effectively protecting the rights of information subjects. Therefore, treating specific risks as compensable damages and incorporating them into the controllable range before they occur is a concrete manifestation of risk allocation. This will effectively regulate the information collection and utilization behavior of information processors and compel them to enhance their risk avoidance capabilities, thereby better protecting the allocation and status of personal information rights.

4.3 Existing Practices and Trends of Risk-Based Damages Internationally

In the digital economy era, the recognition of risk-based damages has become a major challenge both domestically and internationally, and foreign judicial practices continue to explore the definition and revision of the "damage" concept. In domestic and international judicial practices, the recognition of infringement behaviors faces numerous difficulties, mainly due to the mismatch between new forms of damage and traditional damage concepts. To address this challenge, it is particularly crucial to make necessary revisions and innovations to the "damage" concept. Internationally, many countries support the expansion of the concept of damage compensation. The European Union has already recognized the identification of risk-based damages in its legislation, incorporating it into the scope of legal regulation. Its legislators have explicitly stated in the General Data Protection Regulation: "Damage should be given a broad interpretation according to the case law of the European Court of Justice and fully reflect the purpose of this Regulation." This important provision essentially establishes a clear legal principle: in the field of personal information protection, as long as the type of damage is recognized by the European Court of Justice, whether it is identity theft or property loss caused by the leakage of personal information, or various risks arising from the misuse of personal information, these damages will fall within the scope of legal protection and receive comprehensive legal safeguards. Personal information subjects will have the right to seek legal remedies and hold responsible parties accountable according to the law. The implementation of this provision not only demonstrates the EU's firm determination to protect personal information but also provides stronger legal safeguards for personal information subjects. By incorporating risk-based damages into the legal framework for comprehensive protection, it also plays a regulatory role in the behavior of information processors.

For example, in the typical field where risks

are recognized as damages for compensation—medical malpractice liability—in the case of Petriello v. Kalman, the victim suffered intestinal injury due to the doctor's negligence, and there was a certain probability that this accident would lead to intestinal obstruction in the future. The court ultimately ruled that this risk constituted a damage and should compensate for the loss [13]. In the case of "Re mi j as" [See Re mi j as v. Neiman Marcus Grp., 794 F.3d 688, 2015.], the credit card was hacked, leaked, and used for fraudulent activities, but the damage was caused several months after the cy b er attack, preventing the victim from receiving the best protection at the earliest opportunity. The U.S. federal court held that, given the precedent of the credit card being used for fraud, the remaining cards that had not been used for fraud were also at risk of damage, based on the "objective reasonable possibility." Therefore, the court believed that the plaintiff suffered "actual damage" because these cards would eventually be used for illegal activities. If the plaintiff had waited until the infringement occurred to file a lawsuit, it would have been very disadvantageous for their claims. The longer the time between the infringement and the information leak, the harder it would be to prove the causal relationship between the two.

In summary, this article supports the recognition of risk-based damages and believes that in the process of recognizing such damages, we should follow the trends of existing international theories and practices, break through the traditional "difference theory" limitations, and through the revision and innovation of the concept of damage, include the state and rights of legal protection in the scope of damage recognition, thus more comprehensively protecting the interests of information subjects. In current legal practice, it is difficult to accurately recognize the damage caused by the infringement of personal information, leading to insufficient protection of the rights and interests of information subjects. Therefore, acknowledging the existence of risk-based damages has sufficient justification and reasonableness. However, while recognizing risk-based damages, it is also necessary to balance the protection of the rights and interests of information subjects and public interests, ensuring the fairness and effectiveness of the legal system. By comprehensively considering the interests of all parties, a legal framework can be established that both protects the rights and interests of information subjects and maintains public interests, providing solid legal safeguards for the healthy development of the digital economy.

5. Establish A Unified Rule for Recognizing Risk-Based Damages

Judges often need to comprehensively consider the balance of multiple interests during the judgment process. In today's society, it is necessary to acknowledge a growing and concerning issue—the increasingly severe infringement of personal information. At the same time, it is also important to pay attention to the challenges faced by the information subject when seeking compensation for risks caused by information infringement, given the covert and complex nature of such risks. On the other hand, it is necessary to recognize that the normal operation of society requires a certain tolerance of risk, and not all risks can be included in the category of "damage." When determining which risks should be compensated for under the law, it is inappropriate to adopt overly rigid and absolute criteria that lean towards one extreme. Such a one-size-fits-all approach often overlooks the complexity and diversity of risks associated with the infringement of personal information, making it difficult to truly reflect the fairness and reasonableness of the law. Instead, a more flexible and dynamic evaluation standard system should be established based on the unique characteristics of personal information infringement damage compared to traditional damage. This system should fully consider the characteristics of personal information infringement and, in different situations, actually link to specific cases for a comprehensive and thorough evaluation. Judges need to carefully analyze the specific facts of the case, including the infringement behavior, and refer to relevant legal norms and legislative purposes for a comprehensive consideration. Through such an evaluation method, it can more accurately assess the recognition, extent, and scope of personal information infringement risk

damage, thereby making a more just and reasonable judgment. This not only protects the legitimate rights and interests of the information subject, maintains social fairness and justice, but also serves as a warning and deterrent to potential infringers, promoting social harmony and stability.

The theory of dynamic systems explains the justification of legal norms or legal effects through "the collaborative effect corresponding to the quantity and intensity of elements" [14]. It is built on two pillars: "elements" and "fundamental evaluations or exemplary principles" [15]. The collaboration among elements is the "dynamic" aspect of dynamic systems theory, while "fundamental evaluations or exemplary principles" provide the standards and baseline for judgment. Based on these fundamental evaluations or exemplary principles, and by weighing the elements, the final legal effect is derived.

5.1 Standards for Recognizing Risk Damage from Personal Information Infringement

Standards for recognizing risk damage are the fundamental evaluations in the dynamic systems analysis framework. These standards should be reasonable and moderate, avoiding overly strict criteria that make it difficult to effectively remedy the rights of the information subject, thus reducing the effectiveness of protecting the rights of the information subject; or overly lenient criteria that hinder the freedom of behavior of information processors, hindering the sustainable development of the digital economy.[16]

For the standard of recognizing risk damage, compared to the lower standard of "objective reasonable possibility," most U.S. courts that recognize risk damage compensation prefer the "substantial risk" standard. They believe that damages cannot be reasonable or merely a slight possibility; they must be specific and individualized actual damages, a "specific and particular" rather than a broad and general one. In Germany, courts require proof that the processor has caused an "objectively significant and obvious" disadvantage, taking into account factors such as the severity of the infringement and the level of rights, and excluding concerns of unauthorized use of information that may be misused.

Although there are differences in the standards for recognizing risk damage between the U.S. and Germany, in principle, they are the same. The recognition of risk damage should follow the core standard of "substantial risk," which requires that the damage must be significant and obvious in an objective sense, while considering factors such as the level of rights and the severity of the infringement to ensure the protection of the rights of the information subject while also taking into account the reasonable rights of the information processor.

Specifically, when discussing the standard for recognizing the increased risk of future damage, the "substantial risk" standard highlights its unique importance. This standard not only emphasizes the probability factors inherent in the risk but also stresses the uncertainty and potential severity of this risk. When the risk of damage escalates to a substantial level, the rights of the information subject are placed in a more prominent position. Compared to the information processor, the rights of the information subject should be given priority. This shift not only helps to establish the compensability of damage but also achieves the dual functions of damage prevention and compensation at a deeper level, thus effectively protecting the legitimate rights and interests of the information subject.

Based on the rich judicial practice experience in the U.S., the connotation of the "substantial risk" standard can be further understood. This standard means that future damage should not merely remain at an abstract or theoretical level but should be specific and particular. In other words, this damage should be real and perceptible, and it should be targeted at a specific information subject rather than a collective or group in general. This specificity ensures the precision of damage recognition and allows the information subject to receive more effective relief when they suffer damage.

It is worth noting that the "substantial risk standard" and the "reasonable standard" are both considered abstract subjective standards in judicial practice. This subjectivity grants judges the discretion to make judgments in the adjudication process, allowing them to make more just and reasonable judgments based on the specific circumstances of each case and relevant considerations. However, this discretion is not unlimited; judges must fully explain and argue their decision-making basis

when exercising this power to ensure the fairness and reasonableness of the judgment.

In actual practice, when judges determine whether the risk of damage has reached a substantial level, they can consider the following factors: the possibility of damage, the severity of damage, the legality of information processing, and the consent of the data subject, among others. By comprehensively considering these factors, judges can more accurately determine whether the risk of damage has reached a substantial level and make fair judgments accordingly. At the same time, this comprehensive consideration also helps to improve the credibility and acceptability of judgments, enhancing public confidence in judicial fairness.

5.2 Consideration Factors for Assessing the Risk of Damage in Personal Information Infringement

Determining the consideration factors for assessing the risk of damage can provide clear operational guidelines for judges, reducing confusion and subjective speculation during trials, and also better regulating the behavior of information processors. By studying various judicial practices and academic research, this article believes that the factors to be considered in determining the risk of damage in personal information infringement should include the type of personal information involved, the purpose, method, impact consequences, and scope of impact.

(1) The type of personal information involved. In the field of personal information, the "Personal Information Protection Law" has a special definition for sensitive information. Information that the information subject hopes will not be disclosed or concealed, such as account numbers and passwords, are closely related to personal interests. If these in formation are infringed, it will have a profound and lasting impact on the individual. In contrast, when dealing with non-private, non-sensitive, or publicly available information, relevant parties need to show greater tolerance and understanding. Since such information often lacks high confidentiality or personal privacy, information subjects need to have a higher tolerance for the processing of such information to maintain the efficiency and smoothness of information processing. The consequences of the leakage of sensitive information are much more severe compared to ordinary information. Such information often involves personal privacy, reputation, and other personal interests. If leaked, it will have a profound impact on an individual's life, work, and social relationships. Given the severity of the leakage of sensitive information, it must be protected at a higher level. In the era of informatization, the value of data is increasingly prominent, and the data industry has also developed rapidly. However, the protection of personal information and the normal operation of the data industry are not always in harmony. To find a balance between the two, it is necessary to clearly distinguish the nature of information and adopt different recognition attitudes. Specifically, for private and sensitive information, special attention must be given. If these information leak, they should be considered as damage and strict protection measures should be taken to prevent them from being illegally obtained, misused, or leaked. However, for general personal information, although there is also a certain risk, its harmfulness is relatively small. Therefore, it is not advisable to consider this type of risk as damage.

(2) Purpose, method, and the possibility and consequences of realizing risks with respect to personal information infringement. When deeply evaluating whether the risks triggered by personal information infringement have reached the level of damage, it is necessary to comprehensively consider the purpose and method of information processing. First, from the perspective of the purpose of the behavior, if the purpose of the information infringement is clearly for further illegal use or sale, the subsequent risks of information leakage are obvious. Therefore, for such information leakage originating from malicious attacks, it must be given high importance, and its potential risks must be confirmed. Second, the method of information processing also needs to be examined. When the information processing behavior exceeds the reasonable expectations and tolerance of the public, such behavior itself may pose a serious threat to personal information security. For example, if a company uses a user's personal information for commercial promotion or data trading without the user's explicit consent, this

behavior clearly violates the public's reasonable expectations regarding personal privacy rights and should be regarded as a serious threat to personal information security. When assessing these information processing methods, judges need to consider multiple factors comprehensively. They need to carefully review every link of information processing, understand how information is collected, stored, used, and shared, and only after fully considering these factors can judges make an accurate judgment. Finally, the consequences of the behavior also need to be considered from the perspective of the consequences. The greater the consequences caused by the infringement behavior, the greater the risk faced by the information subject. Additionally, the likelihood of the risk materializing as damage also needs to be considered, which further enhances the rationality of damage recognition.

(3) Scope of impact. The scope of impact of personal information infringement often directly reflects the extent of infringement on the rights of the information subject. Especially in the network environment, this scope of impact can quickly expand and cause more serious consequences. Therefore, in cases involving infringement implemented through network technology, multiple factors need to be considered comprehensively to assess its scope of impact, including but not limited to click volume, re-posting volume, duration, and dissemination range, all of which to some extent reflect the extent of information diffusion. When the dissemination range of personal information reaches a certain breadth and depth, the existence of risk-based damage can be recognized.

6. Conclusion

In the era of big data, the recognition of risk-based damage has become a major issue that cannot be ignored by legislation, judiciary, theory, and practice. Its recognition is of great significance for the protection of personal information rights. However, relying too much on traditional methods of recognizing damage may lead to inadequate protection of personal information rights. Therefore, starting from the essence of damage, it is necessary to re-examine and revise the traditional differential theory, and explore feasible recognition standards to better adapt to this new type of damage. To achieve this goal, it is necessary to establish a unified standard for recognizing risk-based damage in the field of personal information protection. This standard should comprehensively consider the type of personal information infringed upon, as well as the purpose, method, consequences, and scope of impact of the behavior. Through such a comprehensive assessment, it can be more accurately determined whether risk-based damage exists.

It is evident that the legal system plays a crucial role in the protection of personal information rights. By continuously improving relevant laws and regulations, it is possible to clarify the standards and norms for recognizing risks and damages to personal information, ensuring that data processing activities operate within a legal and compliant framework. At the same time, the legal system can provide strong legal safeguards for information subjects. When their personal information rights are infringed upon, they can seek legal remedies and obtain timely and effective relief. Therefore, establishing a unified system for recognizing risks and damages is key to achieving a balance between protecting personal information rights and promoting the development of the data industry. It is necessary to continuously strengthen the feasibility and timeliness of legal concepts, and enhance the relevance and operability of judicial practice. Only in this way can we ensure the healthy development of the data industry while maximizing the protection of personal information rights and safeguarding the legitimate rights and interests of information subjects. Of course, recognizing risks and damages is a complex and detailed process that requires courts to make individual judgments based on the specific circumstances of each case. In the short term, judicial practice may not reach consensus on all cases, but this does not hinder the importance of acknowledging the legitimacy of recognizing risks and damages. In fact, this is the first step in promoting information subjects to actively initiate private litigation and protect their own rights and interests. Through continuous judicial practice and legal exploration, it is believed that a more complete and effective legal system for protecting personal information can be gradually established.

Acknowledgments

I would like to express my gratitude to my supervisor, Teacher Xu Nanxuan. I am not a student of extraordinary talent and my knowledge reserve is not yet complete. However, in my opinion, the teacher's care and attention to me are meticulous. Thank you, teacher, for your patient teaching.

References

[1] Xiaodong Ding. From Individual Relief to Public Governance: On the Judicial Response to Personal Information Infringement. Journal of National Prosecutors College, 2022, 30(05): 112.

[2] Xin bao Zhang. Tort Law of China. 2nd Edition. Beijing: China Social Sciences Press, 1998: 94.

[3] Jidong Chen. Personal Information Infringement Relief. SJTU Law Review, 2019, (4): 52.

[4] Jian wen Zhang, Shi Cheng. The New Tort Form of Personal Information and It's Relief. Law Science Magazine, 2021, 42(04): 21-37.

[5] Jangang Xu. An Examination of the Origin of the Concept of Damage in the Context of the Civil Code. Law and Economy, 2021, (2): 32.

[6] Zhiwen Liang, Liu Xiao. The Types of Personal Data Damage and Its Determination. Journal of Jishou University (Social Sciences), 2022(2):74.

[7] Tian Ye. Risks as the Harm: Redefining "Damage" of Tort in Big Data Era. Political Science and Law, 2021(10): 25-39.

[8] Wang Xue. Justification of Risky Damage from Personal Information Leakage. Nanjing University Law Journal, 2023, (03): 174.

[9] Yi qiang Wang. Recognition of Data Infringement Damage from a Judicial Perspective. ECUPL Journal, 2023, 26(05): 76.

[10] Euroean Civil Law Research Group, European Current Private Law Research Group. Principles, Definitions, and Model Rules of European Private Law: Draft Common Frame of Reference (DCFR). Beijing: Law Press, 2014: 236.

[11] Thomas Martecchini, A Day in Court for Data Breach Plaintiffs: Preserving Standing Based on Increased Risk of Identity Theft after Clapper v. Amnesty International USA, 114 Michgan Law Review, 2016.

[12] Xu Ming. Privacy Crisis in the Era of Big Data and Its Legal Response under Tort Law. China Legal Science, 2017(01): 25-29.

[13] Jianyuan Cui. On the Compensation for Mental Harm in Breach of Contract. Journal of Henan University of Economics and Law, 2008(1): 48-51.

[14] Yamamoto Keiji, Xie Gen. Systems Theory in Civil Law. Civil and Commercial Law Review, 2003(23): 172-266.

[15] Xie gen, Bantianke. Misunderstood and Overestimated Dynamic Systems Theory. Chinese Journal of Law, 2017(2): 41-57.

[16] Hailin Cheng. The justification and cognizance of risky damage about personal information infringement. Journal of Chongqing University (Social Science Edition), 2023(5): 201.

