Study on the Determination of Infringement Damage of Personal Biometric Information

Yujia Duan
Changchun University of Science and Technology, Changchun, Jilin, China.

How to cite this paper: Yujia Duan. (2024) Study on the Determination of Infringement Damage of Personal Biometric Information. Journal of Humanities, Arts and Social Science, 8(2), 340-344. DOI: 10.26855/jhass.2024.02.008

Received: January 30, 2024
Accepted: February 28, 2024
Published: March 27, 2024

*Corresponding author: Yujia Duan, Changchun University of Science and Technology, Changchun, Jilin, China.

Abstract
Damage is a necessary element for establishing infringement of a person's biometric information. Under the backdrop of big data, new forms of harm continue to emerge. The traditional doctrine of difference in determining tort damages faces challenges when it comes to cases involving the infringement of personal biometric information. This situation complicates the protection of personal biometric information from infringement. Therefore, the introduction of risky damage as a criterion for assessing the infringement of personal biometric information becomes essential. However, not all risks of infringement are suitable to be included in the category of damage. Due to the intangible, uncertain, and difficult-to-measure characteristics of risky damage, judges should consider factors such as the sensitivity of the information, how it was handled, its intended purpose, the level of exposure and impact, and any related downstream offenses when adjudicating.

Keywords
Personal biometric information, doctrine of difference, risky damage

1. Formulation of the issue
In recent years, with the rapid development of data technology, the technology of acquiring, collecting, and storing personal biometric information has become more and more mature. While technologies such as "face swipe" payment and "fingerprint" authentication have brought convenience to daily life, they have also given rise to new types of legal infringement. Compared with Article 6 of the Tort Liability Law, the first paragraph of Article 1165 of the Civil Code adds the element of damage, which solves the problem of confusion between "infringing" behaviour and "damaging" results (Xu Jianguang, 2021). This provision of the Civil Code is also applicable in the field of personal information infringement, and Article 69 of the Personal Information Protection Law follows this line of thought by making damage an indispensable element in pursuing liability for infringement of personal biometric information.

As the legal saying goes, "No damage, no remedy", all damages are basically aimed at filling the victim's damages. (Xie Hongfei, 2021). However, in the era of big data, new types of damages continue to appear, and to judge whether these new damages can be included in the category of damages in tort law, it is not possible to start only from the traditional types of tort damages. Individual biometric information is part of personal information, and unlike traditional tort damages, the damages caused by the disclosure of this type of information are often risky damages (Wang Xue, 2023). Such damage, which is often difficult to meet the requirements of tangibility and certainty in traditional tort law, generally manifests itself in the form of information leakage, which in turn leads to or contributes to downstream offenses, social sorting, discrimination, consumer manipulation, and relationship control. In addition, personal biometric information is highly sensitive and, once leaked, poses a great risk to the subject of the information (Ye Mingyi, 2018). In judicial practice, victims of the new types of damages are often unable to prove the existence of actual damages and bear the risk of losing the case. This phenomenon is not uncommon at present, which reflects the current lack of understanding of the risks arising from the leakage of personal biometric information that can meet the criteria for determining

DOI: 10.26855/jhass.2024.02.008
damage in the elements of infringement. The dilemma of damage determination in personal biometric information infringement, the special features of risky damage, the necessity of the introduction, and how to properly determine the risky damage are the main research issues in this paper.

2. Difficulties faced in determining infringement damage to personal biometric information

2.1 Emergence of new types of damage

Firstly, it increases the risk of downstream crimes for those who have been compromised. Nowadays, the collection and use of personal biometric information is more common, and the submission of biometric information such as face and fingerprints by individuals has even become a prerequisite for the application of many Internet applications. If the database of such personal biometric information is breached, stolen, bought, or traded, the personal biometric information data will be out of the control of the lawful processor and then used by lawless elements, which will lead to the emergence of downstream crimes, such as the infringement of the rights holder's person. A case of intentional homicide announced by the Huangdao District People's Procuratorate in Qingdao City, Shandong Province in 2021 reflects the huge threat posed by the leakage of personal biometric information to the personal safety of rights holders.

Second, it creates the risk of social sorting and discrimination against those who have been compromised. Information processors screen and process information according to specific purposes to serve their own purposes. On the one hand, information processors may analyse a large amount of personal biometric information in their possession, such as the age and economic status of the subject of the information from facial data. Based on this analysis, they may provide preferential treatment or exclusion to a specific subject. Alternatively, certain merchants may accurately target advertisements to a specific audience. On the other hand, there is evidence that personal biometric information can reveal the probability or tendency of suffering from specific diseases, which may lead to discrimination in the field of employment, etc.

Third, it induces unpredictable anxiety in those who have been compromised. Personal biometric information is unique and unchangeable, and once leaked, there is a permanent risk of infringement. The information subject is unable to predict and grasp the possible risks after the leakage of personal biometric information and thus is in a state of mental anxiety, which is not the actual damage suffered by the infringement of property or personal rights and interests, but the worry about future risks.

2.2 Inadequacy of the doctrine of difference

Traditional tort law mainly applies the difference theory to the determination of damage, but in the field of personal biometric information infringement, the difference theory faces certain difficulties. In 1855, Monson published an article entitled "The Doctrine of Interest", which introduced the doctrine of difference. It highlighted that damage refers to the variance in interest between two states, specifically the contrast between the state of interest without the infringement and the state of interest with the infringement. This difference can either diminish existing property or hinder future property growth (Zhu Xiaofeng, 2022). The concept of damage under the doctrine has a tendency to de-value, but the damage itself has the attribute of value, if the value connotation is removed, there will be a lot of inappropriate in practice. Based on the inadequacy of the doctrine of difference, the academic and practical circles have conducted many reflections. After the emergence of objective damage theory, normative damage theory, and other amendments to the doctrine of difference.

Objective damage makes up for the shortcomings of the doctrine of difference's subjective consideration of damage, while normative damage focuses on the use of norms to give legal evaluation to the natural concept of damage, thus effectively resolving individual cases such as kinship care costs. But because of the difference and damage to fill the function of a high degree of compatibility, so that the doctrine has been the core doctrine of tort damage determination. But this does not mean that the difference can cope with the new situation of all tort damage determination. The emergence of the objective damage theory and normative damage theory said the inadequacy of the doctrine of difference in the context of a particular era.

Infringement arising from the leakage of personal biometric information can be divided into two situations, the first of which is where actual damage has been caused, in which case there is no question as to the determination of the elements of damage. In the second case, the information leakage has not yet caused actual damage, in which case there is a risk of future infringement, and it is impossible to judge how much damage has been caused. As a result, whether the damage is established in this situation has been more controversial in recent years. There is a view that, in view of
the current big data, artificial intelligence, and other rapid developments, personal information infringement in the field of damage should be interpreted expansively, the risk of damage into the determination of damage. Another viewpoint still holds a conservative attitude, which believes that the future risk of personal information infringement is only subjective imagination, and the increased risk of future unlawful infringement due to personal information leakage does not belong to the damage (Cheng Xiao & ZengJungang, 2023). This paper argues that the current information leakage has brought great potential danger to the point of having to take measures. If we stick to the traditional point of the “doctrine of difference”, it is bound to bring great obstacles to the protection of personal biometric information infringement law.

3. Suggestions for Improving the Determination of Personal Biometric Information Tort Damage—Introduction of Risk-based Damage

3.1 Characteristics of risk-based damage

Baker points out that in the process of modernisation, the rapid growth in productivity has unleashed an unprecedented level of danger and potential threats. We live in the digital age, where personal information is collected all the time, and once the personal information of the subject of the information has been collected, the subsequent processing of that information is completely out of the control of the subject of the information. As a result, there is a future risk of infringement. This future risk is characterised by the following aspects:

First, intangibility. In the era of big data, after the leakage of personal biometric information, unlike the consequences of traditional tort damages, not in the form of tangible personal or property damage, and even the time, place, and manner in which the damage occurs, the subject of the right has no way of knowing.

Second, uncertainty. After the leakage of personal biometric information, whether the future risk is converted into actual damage is uncertain; leakage of information is not certain whether the abuse of uncertainty; information is often batch leakage, which suffers from the risk of damage to the subject is uncertain; risk is converted into the actual damage to the time, the way is not certain; the final acquisition of information subject to the purpose of what will give the subject of the information of the personality rights and interests, the right to bring what kind of property damage is uncertain, the above these uncertainties in the actual damage. These uncertainties are difficult to predict accurately before the actual consequences of damage occur.

Third, difficult to measure. In the traditional tort law to fill the damage as the principle of the legislative framework, the damage needs to be quantified in order to have the possibility of relief, which is also the difference in the determination of the damage to stand. The risk of infringement posed by the leakage of personal biometric information is invisible and unmeasurable until it is converted into actual damage. Although Article 69 of the Personal Information Protection Law partially stipulates the method of calculating the amount of damages, in practice, it is difficult to determine both the individual’s loss and the profit made by the processor of the personal information, and judges often use their discretion to determine the amount of damages based on the actual situation.

3.2 The need to introduce risk-based damage

In the current context, personal information, once leaked, is out of the control of the information subject. Personal biometric information is highly sensitive and closely related to the subject of the information, which poses an even greater risk. If the law does not actively respond to the risk of infringement and waits until the risk of infringement is transformed into a real infringement before providing relief, on the one hand, it is contrary to the concept of the law to protect the legitimate rights and interests of civil subjects; on the other hand, for the information subject, it is the best time to lose the opportunity to protect their own rights and interests. One of the most effective ways to regulate the risks that may be caused by the leakage of personal biometric information is to incorporate the specific risks before the actual damage occurs into the scope of the regulation of tort law.

Not all future risks arising from information leakage can be recognised as damages. Scholars’ views on whether to recognise risk-based damages as part of the scope of damage in tort vary widely, with viewpoint one arguing that recognising specific risks arising from the infringement of personal information as damages in tort expands the interpretation of damages in traditional torts. The second point of view is that the increased risk of future unlawful infringement due to the leakage of personal information is not damaged (Cheng Xiao & Zeng Jungkin, 2023). Both views have their practical considerations. The author is in favour of the first point of view, because in the context of big data, artificial intelligence, and other rapid developments of science and technology, personal biometric information is wantonly collected, stored, leaked, or even traded frequently, a certain period of time did not appear the consequences of the damage,
but there is a real risk of damage in tort. In view of the high sensitivity of personal biometric information, the introduction of risky damage and its scientific legal protection is an issue that needs to be studied urgently.

3.3 Considerations for determining risk-based damage

In this paper, it is argued that the following factors should be considered in the determination of risk-based damages:

3.3.1 Sensitivity of information

Personal biometric information belongs to sensitive personal information, but judging from the current legal provisions in China, legislators have not made a precise definition of the scope of biometric information, which results in uncertainty as to what information is more sensitive and should be categorised as biometric information for special protection. In the Civil Code and the Law on the Protection of Personal Information, personal biometric information appears in the legal provisions in an enumerated manner, without a precise definition of biometric information. In recent years, some judicial interpretations, local regulations, and national standards have defined the concept of personal biometric information, but the shortcomings are twofold: firstly, the relevant documents are of a lower rank and not authoritative enough; and secondly, the existing documents do not define personal biometric information in a uniform manner. In addition, with the rapid development of biometric technology, the scope of biometric information that can accurately identify a specific identity is getting wider and wider, but the lag in legislation has indeed brought about certain difficulties in the protection of personal biometric information.

Some scholars believe that once personal sensitive information is leaked, there is damage, so the subject of the information does not need to prove the existence of damage. In other words, personal biometric information is personal sensitive information, once leaked, the damage has been established. The author is not in favour of this view. On the one hand, our understanding of personal biometric information is still in its infancy and will be further deepened with the development of biometrics and other technologies, and the degree of disclosure, sensitivity, and importance of physical and physiological information as well as behavioural information is not the same. On the other hand, with the leakage of personal biometric information, there is a future risk of infringement, but the generalisation that this type of information, once leaked, constitutes damage, the author believes that it is too harsh, and has a subversive change to the basic concept of tort law. This paper argues that the future risk arising from the leakage of personal biometric information should be taken more seriously than the future risk arising from the leakage of general personal information and that the judge should be more convinced of the possible risk arising from the leakage of this type of information when deciding on the case.

3.3.2 Modes and purposes of information processing

Firstly, information processing methods. Big data technology has superb information processing capabilities, and many information processing methods are naturally threatening to personal information, such as high-altitude surveillance, human flesh search, and other behaviours clearly exceeding the tolerance limit of the general public, the court may presume the occurrence of damage based on the infringement of the personal information rights and interests of the natural person; and for the behavioural marketing, targeted advertising, personalized recommendation and other information processing methods that partially meet the reasonable expectations of the public, in addition to meeting the For some information processing methods such as behavioural marketing, targeted advertising and personalised recommendations that meet the reasonable expectations of the public, in addition to satisfying the elements of infringement of rights and interests such as the use of the network to disclose personal information, some courts have also taken substantive damage in fact as a necessary condition for damage to occur. In addition, the consequences of the infringement of personal information are diverse, and in addition to the severity of the actual damage, whether or not the act of information processing increases the potential risk of infringement of a natural person's personal rights and interests or property rights and interests is also one of the factors that should be taken into account in determining the consequences of the act. However, if the results of the infringement caused by the act of information processing are relatively minor, it belongs to the category of minor harm that can not be remedied, and no damage of legal significance occurs.

Second, the purpose of personal information processing. The more personal information processing is based on public interest purposes, the more legitimate the information processing behaviour is, and the more difficult it is for the court to prove the existence of damage. For example, when the information processing behaviour is intended to maintain public security, strengthen social security, implement scientific research activities, and maintain public order and morality, the public interest can be used independently as a personal information infringement exemption. On the contrary, if personal information is processed solely to satisfy the private interests of the information processor, or even to the
detriment of the realisation of the public interest, it is more likely to result in damage.

3.3.3 Degree of exposure and scope of influence of information

The degree of exposure and the scope of influence of personal information are key factors in determining the degree of risk of substantial harm. Generally speaking, the deeper the degree of exposure and the wider the scope of influence of the information, the greater the risk of substantial damage, because it means that more unspecified and potential infringers have a higher probability of coming into contact with the personal biometric information, the deeper the understanding will be, and the stronger the risk of future damage to the subject of the right. First, the degree of exposure is a reflection of the precision with which the personal biometric information is associated with the subject of the information. If high-definition face information is leaked, or face, fingerprint, iris, and other information is leaked at the same time, then the likelihood of infringement damage is higher. Secondly, the scope of impact is an intuitive reflection of the severity of the damage. The wider the scope of impact caused by the infringement of personal information, the easier it is for the court to confirm the existence of the damage. In cases where the internet is used to infringe on personal information, the scope of impact can be evaluated in relation to factors such as the click-through rate, reprint rate, duration, and spreading area of the information. If the personal information has been disseminated in a narrower area and has not yet spread to an unspecified group of people, the victim will usually not be able to obtain relief.

3.3.4 Relevant downstream offences

Downstream crimes refer to illegal activities in which perpetrators use personal biometric information as a tool. The leakage of personal biometric information often triggers crimes against individuals or property. Offenders frequently engage in telecommunication fraud, extortion, and identity theft. In such cases, the individuals whose information has been compromised may face significant risks of harm, even if the crime is only attempted. In cases of large-scale bulk information leakage, only some individuals may have experienced actual harm. However, it is crucial to acknowledge that other individuals are still vulnerable to potential risks such as identity theft and property fraud. Therefore, it is reasonable to assert that these individuals are also at significant risk of harm and fall within the category of reparable damage.

References


