Reconstructing the Framework for Determining and Compensating Dual Risk-Based Damage to Personal Information

WANG Xue[*]

Abstract: *In the era of big data, the dual risk-based damage associated with personal information leakage presents unique challenges. The unrealistic nature of objective risk-based damage without benchmarks and the high threshold for determining subjective risk-based damage have become obstacles for information subjects seeking compensation. Traditional approaches to supporting risk-based damage are inadequate in the realm of personal information. The theoretical support and compensation mechanisms for dual risk-based damage to personal information need re-exploration. The information subject's control over the value of personal information assets based on the right to know forms the theoretical basis for objective risk-based damage. Additionally, the independence of mental suffering and the relaxation of the "serious" standard allow for a broader interpretation of subjective risk-based damage. In addressing claims by information subjects, first, courts need to assess and quantify the level of risk-based damage; second, legislation should introduce a statutory compensation system to define the range of personal information asset value, with a focus on the fault of personal information processors in civil liability; finally, establishing a special representative litigation mechanism can effectively address collective disputes over personal information infringement and alleviate the litigation burden on information subjects.*

Keywords: information subjects ♦ personal information processors ♦ objective risk-based damage ♦ subjective risk-based damage ♦ right to know

The frequent occurrence of personal information[1] leakage has seriously threatened the personal information rights and interests of information subjects. In order to strengthen the exclusive protection of personal information rights and interests, China promulgated the *Personal Information Protection Law* in 2021, stipulating in Article 69 that personal information processors shall be liable for damages from infringement of personal information rights and interests. However, the determination of "damages" has become a major obstacle to the information subjects' claim. The reality and certainty of damage is the premise of civil claims, since the law pursues stability and predictability of order. But the social phenomena handled by law are inherently complex and probabilistic matters, featuring inevitable uncertainty.[2] In most leakage cases, the information subject faces the risk of property damage and mental anxiety, which are not realistic and certain, and are thus called "risk-based damage" hardly recognized by the court.

Scholars at home and abroad have conducted certain studies on the risk-based damage caused by personal information leakage. Professor Solove, a scholar from the United States, initially affirmed the risk-based damage to personal information, arousing the attention of the academic community.[3] Some scholars in China have taken a positive attitude toward the risk-based damage to personal information by demonstrating the harm of substantial risks.[4] On the

[*] WANG Xue (王雪), Lecturer at Inner Mongolia University Law School, Doctor of Laws from Nankai University. This paper is a phased result of "A New Round of Reform and Reconstruction of the International Dispute Settlement Mechanism for Intellectual Property Rights and China's Countermeasures" (Project Number 21BFX101), a 2021 General Project of the National Social Science Foundation of China.

[1] Personal information and personal data have the same connotation at the legislative level, and no distinction is made in the course of the article's argumentation.

[2] Nancy Levit, "Ethereal Torts," 61 *George Washington Law Review* 1 (1992): 136-137.

[3] Daniel J. Solove and Danielle Keats Citron, "Risk and Anxiety: A Theory of Data-Breach Harms," 96 *Texas Law Review* 4 (2018): 737.

[4] Tian Ye, "Risks as the Harm: Redefining 'Damage' of Tort in Big Data Era," *Politic Science and Law* 10 (2021).

other hand, some civil law scholars insist that "risk and anxiety about risk are excessively uncertain" and therefore no compensation shall be imposed for risk-based damage to personal information.[5] However, scholars have basically reached a consensus on the view that the reasonable costs incurred by the information subject in taking preventive measures to prevent the occurrence of downstream damage after the leakage of personal information can be compensated. Moreover, the view is in line with the provisions of Paragraph 1, Article 12 of the *Provisions of the Supreme People's Court on Several Issues Concerning the Application of Law in the Trial of Civil Disputes Involving the Use of Information Networks to Infringe on Personal Rights and Interests* (hereinafter referred to as the "*Provisions*"), and is thus more acceptable in judicial practice. It is worth noting that existing research has not discussed the concept of risk-based damage in depth, ignoring the particularity of risk-based damage to personal information, and tends to be generalized in demonstrating the compensation for risk-based damage to personal information. This paper begins with the concept of risk-based damage to summarize the research in this area into three topics. First, what are risk-based damages caused by personal information leakage, and what makes them special compared with risk-based damage in other fields? Second, what are the legal bases for different types of risk-based damage to personal information? What are the conditions for receiving compensation? Third, can the existing civil compensation system meet the compensation needs for risk-based damage to personal information, and if not, how can the insufficiency be addressed? This article will demonstrate those issues and present its own opinions as a reference in the hope of advancing research in the field.

I. Definition and Particularity of Dual Risk-Based Damage to Personal Information

Due to the divergencies in the theory of risk-based damage, there are also many controversies over whether risk-based damage in the field of personal information should be compensated. The determination and compensation of dual risk-based damage to personal information must consider the particularity of personal information.

A. Personal information leakage causes dual risk-based damage

Personal information leakage is the most common situation that causes risk-based damage, and the misuse of personal information after leakage will cause different types of risk-based damage. With the information subject as the core, the risk-based damage caused by the leakage of personal information can be classified into objective risk-based damage and subjective risk-based damage.

1. Objective risk-based damage to personal information

Objective risk-based damage involves external actions related to personal information after itsleakage. Unauthorized actors may use the leaked personal information for identity theft, telecommunications fraud, etc. to obtain monetary benefits.[6]

Chinese courts do not recognize the risk caused by personal information leakage to the property rights and interests of information subjects. In the case of Sun X vs. China Mobile Communications Group Shandong Co., Ltd. Binzhou Branch, although the courts of first and second instance both recognized the defendant's misuse of the plaintiff's personal information, they rejected the plaintiff's claim for property damage caused by the defendant's misuse of personal information.[7]

Likewise, courts in the United States are also faced with the issue of judging the objective risk-based damage to personal information. Subject to Article 3 of the United States

[5] Cheng Xiao and Zeng Jungang, "Liability for Damages of Personal Information Tort," *Social Sciences in Yunnan* 2 (2023): 103.

[6] Ido Kilovaty, "Psychological Data Breach Harms," 23 *North Carolina Journal ofLaw & Technology* 1 (2021): 43.

[7] See the Civil Judgment of People's Court of Bincheng District, Binzhou City, Shandong Province (2021) Lu 1602 MC No. 83 and the Civil Judgment of Binzhou Intermediate People's Court of Shandong Province (2021) Lu 16 MZ No. 2594.

Constitution, the plaintiff must sustain "injury in fact" to be eligible for litigation, that is, the information subject must prove that their legitimate rights and interests have been infringed, and that such infringement is specific or imminent. In the famous case of Clapper vs. Amnesty Int'l USA, the United States Supreme Court held that an information subject could only file litigations if the risk-based damage is proved to have met the "substantial risk" standard, while the speculated probabilities in the case could not prove that future damage from potential surveillance was imminent. So it denied the plaintiff's standing to sue.[8] Accordingly, the trial path of the Court of Appeals for the Federal Circuit of the United States since the Clapper case is to determine whether the risk-based damage faced by the information subject is substantial. However, the determination of the "substantial risk" has not been clarified. The decisions of different courts of appeals for the Federal Circuit have also been starkly different. The author summarizes the rulings of the Court of Appeals for the Federal Circuit in the United States, as shown in Table 1.

Table 1: Summary of the Rulings of the Court of Appeals for the Federal Circuit of the United States on the Risk-Based Damage

Court	Typical case	Position on the risk-based damage	Basis for the ruling
Federal Supreme Court	TransUnion LLC vs. Ramirez, 141 S. Ct. 2190 (2021)	Rejected	Inaccuracies in the internal credit file will not cause specific damage if they are not disclosed to a third party.
Court of Appeals for the Second Circuit	Whalen vs. Michaels Stores, Inc., 689 F. App'x 89 (2d Cir. 2017)	Rejected	The credit card was quickly canceled after the breach, the identity was not stolen, and the plaintiff was unable to justify the risk of future fraud.
Court of Appeals for the Third Circuit	Clemens vs. ExecuPharm Inc., 48 F. 4th 146 (3d Cir. 2022)	Supported	The hacker stole the plaintiff's personal financial information, putting him at future risk of identity theft and fraud. This satisfies the substantive risk standard.

[8]See Clapper vs. Amnesty Int'l USA, 568 U.S. 398, 133 S. Ct. 1138 (2013).

Court of Appeals for the Fourth Circuit	Beck vs. McDonald, 848 F. 3d 262 (4th Cir. 2017)	Rejected	The theft of the laptop revealed veterans' personal information, but there was no evidence that the personal information was misused, failing to demonstrate a substantial risk of future damage.
Court of Appeals for the Sixth Circuit	Galaria vs. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016)	Supported	The main purpose of the hacker's theft of data is to defraud, and the plaintiff is exposed to the risk of identity theft and financial fraud, posing a substantial risk.
Court of Appeals for the Seventh Circuit	Lewert vs. P.F. Chang's China Bistro, Inc., 819 F. 3d 963 (7th Cir. 2016)	Supported	The restaurant's computer system has been hacked, and some credit cards have been fraudulently consumed; the risk is imminent. So, the plaintiff is eligible to claim compensation.
Court of Appeals for the Eighth Circuit	Alleruzzo vs. SuperValu, Inc., 870 F. 3d 763 (8th Cir. 2017)	Rejected	Card information was compromised, but the plaintiff was unable to adequately allege the substantial risk of identity theft.
Court of Appeals for the Ninth Circuit	Krottner vs. Starbucks Corp., 628 F. 3d 1139 (9th Cir. 2010)	Supported	Computer theft has led to the leakage of employees' personal information, and the future risk of identity theft is sufficient to constitute de facto damage.

Court of Appeals for the Eleventh Circuit	Resnick vs. AvMed, Inc., 693 F. 3d 1317 (11th Cir. 2012)	Supported	The theft of the computer resulted in the disclosure of members' sensitive personal information, and the bank accounts of two members were already overdrawn without authorization. The risk of identity theft is recognizable.

In summary, the United States Supreme Court and the Court of Appeals of the Second, Fourth, and Eighth Circuit adopted a negative view of the objective risk-based damage caused by the leakage, while the Court of Appeals of the Third, Sixth, Seventh, Ninth, and Eleventh Circuit maintained a supportive position. Satisfaction of the "substantial risk" standard is central to the U.S. court ruling. The Federal Court of Appeals for the Third Circuit interpreted substantial risk as "the present risk that the plaintiff will suffer direct harm."[9] However, this interpretation is too vague. Even if the circumstances of personal information leakage are similar, for example, a hacker attack or computer theft, the judgment of different courts can be completely different, essentially of the judge's free will.

2. Subjective risk-based damage to personal information

Unlike objective risk-based damage, subjective risk-based damage occurs within the information subject, and the core consists of mental damage. In the event that personal information is illegally obtained by an unknown subject, the information subject may experience a number of psychological or emotional changes, for example, fear, anger, or depression.[10]

Prior to the promulgation of the *Personal Information Protection Law*, personal information leakage was classified in practice as a privacy dispute in China. Therefore, at present, the adjudication path of Chinese courts for subjective risk-based damage to personal information mainly adopts the rationale of mental damage after privacy infringement on privacy. According to Article 1183[11] of the *Civil Code*, the information subject must prove that they have suffered serious mental damage due to personal information leakage in order to obtain compensation. It is worth mentioning that in China's judicial practice, there have been cases in which compensation for the subjective risk-based damage to personal information is supported. In 2022, the plaintiff Pang XX successively filed lawsuits in the People's Court of Rencheng District, Jining City, Shandong Province, the Zhanhua District People's Court of Binzhou City, and the People's Court of Decheng District, Dezhou City (hereinafter referred to as the "Pang XX Series Cases"). The defendants included different companies, but the cause of action of the plaintiff was broadly the same, that is, the defendants infringed on the personal information of the plaintiff by paying social insurance for him as an employee without signing an employment contract with him and without his consent. This behavior may disqualify the plaintiff from finding a job as a fresh graduate and may narrow the scope of his career choice and prevent him from enjoying the talent subsidy after graduation. Although the consequences of the infringement have not yet occurred, the above-mentioned courts ruled

[9] Clemens vs. ExecuPharm Inc., 48 F.4th 146 (3d Cir. 2022), para. 153.

[10] Ido Kilovaty, "Psychological Data Breach Harms," 23 *North Carolina Journal of Law & Technology* 1 (2021): 42 and 43.

[11] Article 1183 of the *Civil Code*: "Where the infringement upon a natural person's personal rights and interests causes serious mental suffering, the infringed party shall have the right to claim compensation for mental suffering. Where a natural person has suffered serious mental suffering as a result of intentional or gross negligence infringement of property with personal significance, the infringed party shall have the right to claim compensation for mental suffering."

that the defendants' act will cause mental distress to the plaintiff and awarded different amounts of mental impairment.[12] It can be seen that although the proportion of cases in which claims for mental impairment due to personal information is low, some courts do have a positive attitude toward claims for subjective risk-based damage compared to the fact that objective risk-based damage is not recognized.

The standard for U.S. courts to adjudicate subjective risk-based damage to personal information is consistent with that for objective risk-based damage, that is, the "substantial risk" standard. When the court finds that the fear, anxiety and depression faced by the information subject meet the standard, the subjective risk-based damage will be recognized by the court. As in Krottner vs. Starbucks Corp. where the theft of a laptop led to leakage of sensitive personal information of the plaintiff, the Court of Appeals for the Ninth Circuit held that the plaintiff had general anxiety and stress that could constitute de facto damage. In the Beck vs. McDonald case, the Court of Appeals for the Fourth Circuit held that the "emotional disturbance" and "fear of identity theft and financial fraud" caused by the personal information leakage were far from posing substantial risks, and rejected all subjective and objective risk-based damages caused by the personal information leakage.

B. The particularity of the dual risk-based damage to personal information

The special status of personal information processors and the special nature of personal information rights and interests have given risk-based damage to personal information certain particularities.

1. The special status of personal information processors

First, personal information processors have a strong control of personal information. Personal information processors, especially large internet companies, handle vast amounts of information around the world. Some of them hold even more personal information than developing countries with weak technological capabilities. Those companies have been hailed as a new type of "country."[13] Personal information processors can not only monitor user behavior but also manipulate it by pushing tendentious content, influencing user judgment, and interfering with user choices. The information subjects cannot interfere with the method and purpose of the personal information processors for processing their own personal information. The asymmetry between personal information processors and information subjects also further exacerbates the difficulty of individual claims for personal information infringement.

Second, personal information processors enjoy certain regulatory powers. In view of the massive amount of personal information in their possession, administrative authorities have to rely on the cooperation of personal information processors in exercising regulatory functions. China's *Cybersecurity Law* stipulates in Article 47 that once a network service provider discovers the publication or transmission of information prohibited by laws or administrative regulations, it shall immediately stop transmitting it and take measures to prevent its spread. This means that personal information processors need to review the legality of users' speech and thus enjoy some of the public power that originally belonged to law enforcement agencies. In view of the extensive use of online social media platforms by users, the prohibition measures of personal information processors for illegal speech also have a more effective "punitive" function. In 2021, social media giant Twitter announced a "permanent ban" on Donald Trump's account "for his risk of inciting violence," which was against its prohibition on glorifying violence.[14] However, the opacity of the standards and procedures of personal

[12] See the Civil Judgment of the People's Court of Rencheng District, Jining City, Shandong Province (2022) Lu 0811 MC No. 1961, the Civil Judgment of the People's Court of Zhanhua District, Binzhou City, Shandong Province (2022) Lu 1603 MC No. 404, and the Civil Judgment of the People's Court of Decheng District, Dezhou City, Shandong Province (2022) Lu 1402 MC No. 2953.

[13] Zhai Zhiyong, "The New Order of Governance in the Era of Data Sovereignty," *Dushu* 6 (2021): 99-100.

[14] "Three Important Issues of U.S. President Trump's Ban by Tech Giants Sparks Controversy," BBC News Chinese, accessed April 11, 2023, https:/www.bbc. com/zhongwen/simp/world-55666142.

information processors for censorship has led to a lack of remedies for users, and the legitimacy of their right to censor speech has also faced considerable controversy.

2. The public-private nature of personal information rights and interests

In China, personal information rights and interests are regarded as independent personality rights by the civil law, and the law first protects the personality rights and interests attached to personal information.[15] For example, Article 111 of China's *Civil Code* stipulates personal information as a civil right, and Chapter 6 of the Personality Rights section distinguishes it from the right to privacy for separate protection. China's *Personal Information Protection Law* 2021 uses the expression "rights and interests in personal information," and Chapter 4 stipulates that the content of rights and interests in personal information includes the right to know, the right to access, the right to copy, and the right to delete. Rights and interests in personal information are considered to appear in the form of a right to request personality rights in the law.[16] They are based on the self-determination of personal information, and the information subjects have control over the personal information according to their free will and can dispose of it according to their needs. The information subjects can not only take passive defensive measures against infringement on their personal information rights and interests, such as requesting cessation of infringement or damages, but also take positive measures, such as directly using personal information for transactions.[17]

At the same time, the right to personal information as a "bundle of rights" also includes constitutional and administrative law rights.[18] Article 1 of China's *Personal Information Protection Law* stipulates that "The Law has been enacted in accordance with the Constitution," so the constitution shall be the legal basis for protecting personal information. Personal information rights and interests are essentially tools given by the state to information subjects for protecting their personal information, while the state's obligation to protect information subjects is the constitutional basis for personal information rights and interests.[19] In addition to civil protection, China also adopts criminal protection and administrative protection for personal information rights and interests. Article 66 of the *Personal Information Protection Law* stipulates the administrative liabilities of personal information processors for breach of obligations, including warning, fines, etc.; Paragraph 1 of Article 253 of the *Criminal Law* stipulates the crime of "infringement on citizens' personal information," regulating the serious infringement of citizens' personal information by criminal liability. It can be seen that personal information rights and interests are both public and private, and they should be protected by both public law and private law.

II. Core Obstacles to Determining the Dual Risk-Based Damage to Personal Information

Chinese courts mainly hold negative evaluations of the dual risk-based damageto personal information, but the core obstacles encountered in determining the objective and subjective risk-based damageto personal information are different. Therefore, they must be discussed separately.

A. Objective risk-based damage: unreality without reference

Even though unreality is a common feature of risk-based damage in different fields, there is no realistic reference for judging objective risk-based damage to personal information.

[15] Zheng Weiwei, "The Right of Personal Information: Attributes, Jurisprudential Basis and Protection Pathway," *Law and Social Development* 6 (2020): 136.

[16] Yao Jia, "On the Civil Liability of Personal Information Processors," *Tsinghua University Law Journal* 3 (2021): 53.

[17] Zhang Li'an and Han Xuzhi, "The Private Law Nature of Personal Information Rights in the Big Data Era," *Legal Forum* 3 (2016): 127.

[18] Wang Xizin, "Re-thinking Legal Mechanisms for the Protection of Personal Information Rights: Administrative Regulation or Civil Litigation," *Chinese Journal of Law* 5 (2022): 6.

[19] Wang Xizin, "The Package of Personal Information Rights Seen from the Perspective of State Protection," *Social Sciences in China* 11 (2021): 120-121.

Long before the advent of the big data era, the court applied the concept of risk-based damage to three types of cases: loss of opportunity interest,[20], toxic substance tort,[21] and traumatic accident. In cases of loss of opportunity interest, U.S. courts at first only allowed plaintiffs to bring claims if they initially had more than a 50 percent chance of survival, and gradually some allowed claims for any measurable risk of loss of opportunity interest.[22] In the case of Herskovits vs. Group Health Coop., Herskovits lost the opportunity for timely treatment due to the failure of Group Health to diagnose the disease, and his probability of survival was reduced from 39% to 25%. The Washington Superior Court ruled in favor of the plaintiff's claim, holding that the plaintiff did not need to prove that the patient's chance of survival was 51% and that the evidence of a diminished chance of survival was sufficient.[23] Some courts in China also take a positive attitude towards the loss of patients' opportunities and interests as risk-based damage. In the medical damage liability dispute case of Xu XX and Dai XX, the hospital's negligence objectively led to the delay in the diagnosis of the patient's advanced cardia adenocarcinoma, and the court recognized the establishment of liability for damages.[24] In cases of toxic substance tort, the damage caused by exposure to toxic substances is usually a disease with a certain latent period; the incubation period can vary depending on the constitution of the infringed person, the type of poison and the length of exposure, and may even last decades. However, after the end of the incubation period, the scope of the infringer and the infringed party may have become unclear, making it even more difficult to prove the causal relationship.[25] Since the traditional tort law can hardly cope with this type of mass tort case because of the scope of damage, the British court expanded its interpretation in Barker vs. Corus UK Ltd., holding that if the employer negligently exposes the employee to asbestos, the significant risk of mesothelioma shall be considered damage.[26] In addition to the loss of opportunity interest and toxic substance tort cases, U.S. courts have also recognized compensation for future risks arising from traumatic accidents. In the Jordan vs. Bero case, the plaintiff suffered severe brain contusion as a result of a collision between the plaintiff's bicycle and the defendant who was driving a car. The attending physician testified statistically that a significant number of people who suffered this type of brain injury were known to have permanent sequelae. The West Virginia Supreme Court of Appeal held that the manifestations of permanent damage might be latent and unpredictable in the future, and that there is positive medical evidence that the trauma was permanent, which was sufficient to support compensation for the future risk of the trauma.[27]

The three types of cases in which the above-mentioned risk-based damage was applied have certain commonalities regarding the application of objective risk-based damage. First, the infringed party suffered actual damages, including actual personal injuries and economic losses arising there from. For example, in Hagerty vs. L & L Marine Services, Inc., a typical case of toxic substance infringement in the United States, due to the defect of the company's equipment for loading chemicals, the plaintiff was completely sprinkled with chemical carcinogens while working as a company oilman and then developed dizziness, nausea, and

[20] Most of the cases of loss of opportunity interest are medical disputes, that is, due to the doctor's diagnosis error or failure to treat in time, the patient's chance of recovery is reduced, or the risk of further deterioration of the patient's condition and death in the future increases.

[21] Toxic tort refers to the act of illegally exposing others to poisons (asbestos, toxic waste, etc.), for example, accidental leakage, workplace exposure to hazardous substances, long-term exposure to pesticides, etc. See Tu Yongqian, *Latent Poison Tort* (Beijing: Intellectual Property Publishing House, 2014), 14.

[22] Nancy Levit, "Ethereal Torts," 61 *George Washington Law Review* 1 (1992): 155.

[23] Herskovits vs. Grp. Health Coop., 99 Wash. 2d 609, 664 P.2d 474 (1983).

[24] the Civil Judgment of the People's Court of Taizhou Pharmaceutical High-tech Industrial Development Zone, Jiangsu Province (2022) S 1291 MC No. 1093.

[25] Yang Yinhong, "Non-Property Damages in the Torts of Toxic Substances in the Era of the Civil Code," *Cross-strait Legal Science* 4 (2020): 17.

[26] Barker vs.Corus UK Ltd. [2006] UKHL20.

[27] Jordan vs. Bero, 158 W. Va. 28, 210 S.E. 2d 618 (1974).

other symptoms. Though he was not diagnosed with cancer, he had to continue medical examinations and pay medical expenses. This provided proof for the determination of objective risk-based damage, which was considered by the Court of Appeals for the Fifth Circuit as a "sufficient truthful indication."[28] In cases where the opportunity interest is lost, the misdiagnosis or delayed diagnosis will prolong the plaintiff's illness and increase the cost of treatment, not to mention that the plaintiff has suffered severe trauma in a traumatic accident case. Second, the opinions issued by professionals speculate on the risks to be suffered by the plaintiff in the future, and the probability that the risks will be turned into reality can be determined, thus proving the possible property losses. As in the case of Jordan vs. Bero, where medical testimony proved that the plaintiff's brain had sustained permanent damage as a result of the car accident, the court examined whether the assumptions provided by the medical certificate were reasonable. If future risks could reasonably be ascertained, then medical expenses and lost wages arising from future risks should be compensated.

However, there is no realistic reference for the judgment of objective risk-based damage to personal information. Nor can the court adopt the judgment path of risk-based damage in existing types of cases. First, under normal circumstances, the information subject has not suffered actual personal injury or property loss. Although the overall leakage may cause huge economic losses or lead to personal injury, the economic damage suffered by individual information subjects is not obvious. In most cases, the information subject did not suffer physical attacks. Thus the court cannot infer the future property risk to the information subject on the basis of actual damage. Second, in the field of personal information, there has been no effective advice provided by professionals. In the medical field, doctors can make professional estimates about the probability of a patient's future risk converted into actual damage and get the recognition of the court. However, big data is a new type of discipline, and there is no authoritative professional to provide proof of the infringement damage caused by personal information leakage to the information subject. Therefore, it is impossible for the court to judge the probability of objective risk-based damage to personal information. Third, the property value of personal information is not clear. In the above three types of cases where risk-based damage was applied, there were clear calculation criteria for both medical expenses and wage income. However, in the field of personal information, even if the court upholds the claim for objective risk-based damage, it will not be able to quantify the property loss of the information subject due to the lack of a path for externalizing the property value of personal information.[29]

B. Subjective risk-based damage: the determination threshold is relatively high

According to Article 1183 of the *Civil Code*, the information subject must prove serious mental damage as a result of the personal information leakage in order to be eligible for compensation. Although there have been judgments in favor of subjective risk-based damage to personal information in China, the high threshold of "serious" has led to a low proportion of cases in which the court supported compensation for mental damage of information subjects.[30]

"Serious," as a qualifier of mental damage, is based on the rule of "floodgate theory" and "ignoring minor damage" in tort law. In the case of the "floodgate theory," negative emotions are an integral part of the daily life of a natural person, so their regulation should be one of the matters for which they are responsible. Moreover, negative emotions depend on subjective feelings, which lead to marked differences in the emotional responses of different people under the same event. If the court upholds a claim for mental damage for any negative emotion, it may encourage the guise of mental anguish; therefore, the conditions for mental

[28] Hagerty vs. L & L Marine Servs., Inc., 788 F. 2d 315 (5th Cir. 1986) .

[29] Peng Chengcheng and Shi Xiaoyu, "The Reconstruction of Value Externalization Path of Personal Information Property," *Contemporary Law Review* 2 (2023): 62.

[30] Zhao Beibei, "The Dilemma and Response Path of 'Damages' in the Private Law Remedies of Personal Information," *Finance and Economics Law* 5 (2022): 96.

damage claims should be raised to prevent abusive litigation.[31] On the other hand, the rule of "ignoring minor damages" focuses more on bundling mental damage with personal injury. From the perspective of traditional tort law, the adverse physical reaction caused by personal injury or mental injury suffered by the infringed party becomes a prerequisite for the court to award compensation for mental damage.[32] For example, in the case of Jordan vs. Bero, Judge Haden held that from the fact that the plaintiff's trauma is proven to be permanent, it could reasonably be inferred that he would continue to suffer mental anguish in the future and that future pain and suffering should be allowed as one of the elements of risk-based damage. However, this inference was based on permanent physical trauma and past mental anguish suffered by the plaintiff. In cases of personal information infringement where no personal injury has been sustained, it is difficult for the court to determine that the mental suffering of the information subject due to the risk-based damage has reached the degree of being "serious." In 2012, in the case of Fed. Aviation Admin. vs. Cooper, the United States Supreme Court dismissed the pilot's claim for compensation for medical information leakage, ruling that the suffering caused was insufficient, and that the element of "actual damage" should be satisfied. [33]

In personal information infringement cases, the "serious" element forces the information subject to bear a heavier burden of proof, making it impossible to claim for subjective risk-based damage to personal information. The risk of personal information infringement often arises from the negative emotions of the information subject, and even the mental anguish is likely to be the only damage suffered by them. However, it is precisely because of the information subjects' failure to prove the physical manifestations of their mental anguish that the personal information processor only needs to bear the responsibility of apologizing and stopping the infringement even for factual infringement on personal information rights and interests.[34]

C. Insufficient theoretical support for risk-based damage

In the 20th century, scholars already began to discuss the theoretical basis of risk-based damage, and the current affirmation of the dual risk-based damage to personal information mainly follows the theoretical basis of that in the past, for example, the allocation of responsibility in a risk society, the expansion of the damage concept, and the deterrent function of tort law. However, this argument path fails to note the particularity of the dual risk-based damage to personal information.

First of all, the theory of risk and social responsibility allocation cannot furnish a basis for making the personal information processor bear the civil liability for risk-based damage. In a risk society, the risks are man-made and not naturally generated. Risk-based damages are latent and not obstructed by national borders, and can hardly be judged contemporarily. The latent risk and the issue of liability make it difficult to identify the responsible entity.[35] Since the original legal norms cannot meet the needs of adjusting the new type of legal relationship, risk control and risk allocation have become the focus of legal regulation of the risk society.[36] At the legal level, tort liability has become one of the main ways to allocate risks in the risk society. With the help of the preset "behavior-liability" mechanism, holding the risk maker

[31] Xie Hongfei, "Three Key Words of Mental damages," *Studies in Law and Business* 6 (2010): 14.
[32] Ido Kilovaty, "Psychological Data Breach Harms," 23 *North Carolina Journal of Law & Technology* 1 (2021): 43 and 61.
[33] Fed. Viation Admin. vs. Cooper, 566 U.S. 284, 304 (2012).
[34] Peng Chengcheng and Xu Sumin, "System Construction of Mental Damage Compensation of Infringing Rights and Interests of Personal Information," *Nanjing Journal of Social Sciences* 3 (2022): 86.
[35] Ulrich Beck, "The Terrorist Threat: World Risk Society Revisited," 19 *Theory, Culture & Societ* 4 (2002): 41.
[36] Ioannis Agrafiotis, Jason R.C. Nurse, Michael Goldsmith, Sadie Creese, and David Upton, "A Taxonomy of Cyber-harms: Defining the Impacts of Cyber-attacks and Understanding How They Propagate," 4 *Journal of Cybersecurity* 1 (2018): 3.

accountable for adverse consequences has become the main way to allocate risks in tort law.[37] However, risk allocation does not mean that the personal information processor must compensate for the damage that did not occur. It should be emphasized that the legislative recognition of the possible risk-based damage does not constitute an expansion of the scope of civil compensation. The theory of responsibility allocation in a risk society only explains that the risk maker should bear the adverse consequences through tort liability. However, as mentioned above, large-scale tort cases in a risk society, for example, toxic substance torts, all show certain personal damage, but personal information infringement cases do not satisfy this premise. In view of the dual nature of personal information rights and interests, the legal protection measures for them are also multi-dimensional, including civil compensation, administrative penalties and criminal sanctions. Article 66 of the *Personal Information Protection Law* and Clause 1 of Article 253 of the *Criminal Law* can still regulate personal information violations that cause risks. Under the circumstance that the protection path of public law can punish personal information processors, the theoretical basis for personal information processors to bear civil liability for risk-based damage needs to be further explored.

Second, the extension of the theory of damage determination is insufficient to support the establishment of risk-based damage to personal information. Mommsen, a well-known scholar in Germany, proposed the "differential hypothesis," advocating comparing the property status after the infringement accident to that if there was no infringement accident.[38] In view of the drawbacks of the "differential hypothesis," German injury theory has been continuously making revisions in the two directions of "objectification" and "standardization." It has successively developed the "objective damage theory" and the "standard damage theory." The former puts greater stress on the deterioration of the equity status rather than simply considering the difference, while the latter places greater emphasis on determining the scope of damage based on value judgments.[39] Although the evolution of the damage concept from the differential hypothesis to the standard damage theory has extended the scope of damage, a certain degree of "reality" of damage is still required. The court's speculation on the risk-based damage in other fields is still based on actual damage, which is unable to deal with the "unreferenced unreality" of the objective risk-based damage to personal information. Nor can it explain whether the subjective risk-based damage needs to meet the serious standard. U.S. scholars have a broader understanding of "damage" than their German counterparts, generally recognizing it as a setback to legitimate interests or welfare.[40] However, there are also objections to civil compensation for risk-based damage. For example, scholars Goldberg and Zipursky argued that before the defendant can be held liable, the plaintiff must establish that fault has become a reality. Although physical harm caused by exposure to a high level of danger is recognized to result in reduced welfare of the parties, it does not constitute sufficient grounds for the plaintiff to obtain compensation.[41]

Finally, the deterrent function of tort law cannot provide an explanation basis for the risk-based damage to personal information. As we all know, tort law can deter infringement by requiring the infringer to compensate for damages.[42] Judge Calabresi pioneered the theory of "cheapest cost avoiders," seeking to minimize the cost of damage, the cost of preventing damage, and the administrative cost of accident and making them the core of the theory of

[37] He Guoqiang, "Risk Society, Risk Allocation and the Reform of Tort Liability Law," *Social Sciences in Guangdong* 3 (2018): 230-231.
[38] Wang Zejian, *Compensation for Damages* (Beijing: Peking University Press, 2017), 64-65.
[39] Xu Jian'gang, "The Evolution of the Concept of Damage in the Context of the Civil Code," *Finance and Economics Law* 2 (2021): 37-39.
[40] Joel Feinberg, *Harm to Others* (Oxford: Oxford University Press, 1984), 31-38.
[41] John c. P. Goldberg, Benjamin C. Zipursky, "Unrealized Torts," 88 *Virginia Law Review* 8 (2002): 1634.
[42] Huang Qinghua, "The Power of Thought, Analysis Tools and Criticism — On Aristotle's Concept of Justice Regarded as Philosophy of Tort Law," *Law Journal of Xiangjiang Youth* 1 (2015): 279.

deterrence in tort law.[43] Civil recourse in tort law operates in a dual direction, not only to remedy private infringements but also to meet the needs of social regulation because the factors that constitute civil fault often stem from the need for social regulation.[44] However, the deterrent function of tort law places greater emphasis on the containment of illegal acts of personal information and cannot explain the justification of compensation for risk-based damage to personal information. In addition, the deterrent function of tort law can also be achieved via civil public interest litigation provided for in Article 70 of the *Personal Information Protection Law*. Given the special status of personal information processors, there is a huge disparity in the strength between information subjects and personal information processors. There is a significant imbalance between the costs and benefits of civil litigation by information subjects, so there may be a lack of incentive to file private litigation. Compared with civil lawsuits filed by a single civil entity, civil public interest litigation can strengthen social supervision by leveraging the professionalism of the public interest litigation entity and claims against personal information processors. In this context, taking the deterrent function as the basis for compensating for risk-based damage to personal information has a "distorted" theoretical connection.

III. The Theoretical Basis for the Determination of Dual Risk-Based Damage to Personal Information

The reasons for the negative evaluation of objective risk-based damage and subjective risk-based damage to personal information are different, so it is necessary to explore their theoretical basis separately.

A. The protection of the right to know breaks the shackles of objective risk-based damage

In a risk society, the focus of the law is risk control, the premise of which is to learn about the situation, probability and preventive measures of risk occurrence.[45] However, the supply and free flow of information only exist in the ideal hypothesis, and information asymmetry is the norm in a risk society.[46] Since information asymmetry cannot be regulated by the market itself, the law constructs the behavior model of "informed consent" and applies it to the construction of many legal relations in the medical field, product liability and so on.[47]

1. Application of the right to know in tort law

First, in the medical field, the right to know protects the patient's right to evaluate all important information to make a final decision on treatment, but the decision made in a fully informed manner is not the focus of the court. Instead, the patient's exclusion from the deliberate decision-making process is at the heart of the cause of action.[48] In the case of Beijing Meizhongyihe Women's and Children's Hospital Co., Ltd. vs. Liu XX et al., the hospital failed to inform the family of the consequences of fetal abnormalities during the prenatal examination, and the Beijing No. 3 Intermediate People's Court ruled that the hospital should bear the liability for compensation at the 30% liability ratio.[49]

[43] Catherine M. Sharkey. "Modern Tort Law: Preventing Harms, Not Recognizing Wrongs," 134 *Harvard Law Review* 4 (2021): 1433.
[44] Guido Calabresi and Spencer Smith, "On Tort Law's Dualisms," 135 *Harvard Law Review Forum* 4 (2022): 184.
[45] Yu Darhan, "On the Legislative Improvement of the Protection of Consumers' Right to Know on Food Safety," *Journal of Soochow University (Philosophy & Social Science Edition)* 5 (2018): 97.
[46] Xu Jun, "The Dilemma and Change of Consumers' Right to Know in the Intelligent Era," *Journal of Central South University (Social Sciences)* 3 (2021): 16.
[47] Yao Jia, "On the Civil Liability of Personal Information Processors," *Tsinghua University Law Journal* 3 (2021): 52.
[48] Aaron D. Twerski & Neil B. Cohen, "Informed Decision Making and the Law of Torts: The Myth of Justiciable causation," 1998 *University of Illinois Law Review* 3 (1988): 649.
[49] See the Civil Judgment of Beijing No. 3 Intermediate People's Court (2022) Jing 03 MZ No. 3698.

Second, compared with medical malpractice cases, the right to know is more widely used in product liability. At the legislative level, China's *Law on the Protection of Consumer Rights and Interests* respectively stipulates in Article 8 and Article 16 that consumers' right to know and operators' obligation to inform. At the judicial level, in 2019, the China Consumers Association released a typical case Xu XX vs. a Defendant Telecommunications Service Contract, and the Intermediate People's Court of Mudanjiang City, Heilongjiang Province, ruled that the defendant return the fee on the ground that it did not inform the plaintiff of the fee standard, and violated the plaintiff's right to know and the right to choose.[50]

To sum up, the development of the market economy and the specialization of the product structure inevitably leads to a huge "information gap" between the two parties of the transaction, and the right to know as a procedural right is the key to reversing the unequal status of the two parties. The civil compensation remedies based on the right to know can not only achieve procedural justice, but also compensate for all kinds of damages caused by violations of the "informed consent" pattern of behavior in individual cases.[51]

2. Recognition of the property value of personal information in the context of the right to know

It is on the premise that when the right to know is guaranteed, the information subjects independently control the sharing and transfer of the property value of personal information. China's *Personal Information Protection Law* stipulates in Articles 14 and 44 of the rules of "informed consent" for processing personal information to protect the right to know of information subjects.

On the one hand, personal information has natural property attributes, and the information subjects have a property interest in personal information. The utility, scarcity and circulation of personal information give it exchange value and make it the object of legal property rights.[52] On the premise of providing or allowing access to personal information, the information subjects obtain the digital products or services provided by internet enterprises. Although many internet companies seem to provide online services for free or at a discounted price, in fact, the products or services are purchased by information subjects with personal information as payment.[53] In other words, personal information can be used instead of money to pay for digital content, and the payment model has changed from "monetary payment" to "data payment."[54] Article 13 of the preamble to the 2015 Proposal for a *Directive of the European Parliament and of the Council on Certain Aspects Concerning Contracts for the Supply of Digital Content*[55] (hereinafter referred to as the "*Directive*") already points to the existence of a "data payment" model, saying that "in the digital economy, personal information is often seen by an increasing number of market participants as having a value comparable to money." Article 3 (1) of the *Directive* also explicitly covers contracts where consumers use personal information as payment consideration to obtain a supplier's digital products or services.

[50] See the Civil Judgment of the Intermediate People's Court of Mudanjiang City, Heilongjiang Province (2019) Hei 10 MZ No. 456.

[51] Gretchen Larsen & Rob Lawson. "Consumer Rights: An assessment of Justice," 112 *Journal of Business Ethics* 3 (2013): 522.

[52] Peng Chengcheng, "The Dual Legal Attributes of Personal Information," *Tsinghua University Law Journal* 6 (2021): 82.

[53] Gianclaudio Malgieri and Bart Gusters. "Pricing Privacy-the Right to know the value of your personal Data,. *34 Computer Law & Security Review* 2 (2018): 292.

[54] Zhang Xinbao, "'General Free Mode + Specific Payment Mode': A New Thinking on Personal Information Protection," *Journal of Comparative Law* 5 (2018): 5-6.

[55] Proposal for a directive of the European parliament and of the council on certain aspects concerning contracts for the supply of digital content 2015/0287 (COD).

On the other hand, the information subjects' control over the property value of personal information depends on the realization of the right to know.[56] Based on the understanding of the processing of personal information and digital products, the information subjects decide whether to share or transfer the property value of personal information. Their participation in the property value of personal information is mainly based on passive participation, supplemented by active participation.[57] However, the strong control of personal information processors over personal information undermines their right to know. In personal information leakage, they lose control over the property value of personal information due to infringement on their right to know. Therefore, the basis for determining the objective risk-based damage to personal information lies in the loss of the property value of personal information under the impairment of the right to know. In the case of Ling XX vs. Beijing Weibo Shijie Technology Co., Ltd., although neither party provided relevant evidence of the property losses suffered by the plaintiff due to the infringement of personal information rights and interests or the benefits obtained by the defendant, the Beijing Internet Court held that the personal information itself has property value and would bring economic benefits to the defendant's commercial operations, and awarded a discretionary compensation to the amount of 1,000 yuan.

In summary, the claim for objective risk-based damage to personal information does not need to have actual damage; the key is that the loss of the right to know leads to the deprivation of the property value of the information subjects' personal information.

B. A lenient interpretation of the determination of subjective risk-based damage

Taking "serious" as the standardfor determining the subjective risk-based damage to personal information not only ignores the independent value of the damage, but also cannot achieve the goal of personal information protection.

1. The subjective risk-based damage to personal information has independent value

The subjective risk-based damage suffered by the information subject is not dependent on personal injury or other property losses, and it has independent value. First, personal information leakage can lead to human dignity damage. Article 38 of the *Constitution* clearly stipulates that "the personal dignity of citizens of the People's Republic of China is inviolable." Accordingly, human dignity has become the value basis and logical starting point of human rights. Article 109 of the *Civil Code* provides for the general protection of human dignity in accordance with the constitution, and regards human dignity as the primary value in the section on personality rights.[58] Protecting human dignity from infringement is also an issue highlighted in the *Personal Information Protection Law*. The leaked personal information may be viewed or reused by unknown subjects, and the information subject will suffer damage to personal dignity, and will be in a state of anxiety and fear. However, the impairment of human dignity does not necessarily bear physical manifestations; nor is it necessarily related to personal injury, let alone property loss.[59] The Court of Appeals for the Fifth Circuit of the United States upheld this view in Hagert Y vs. L & L Marine Services, Inc., stating that the plaintiff should be entitled to compensation for mental anguish arising from the fear of cancer, regardless of whether there was physical harm or effect, as long as the plaintiff's fear was reasonable and there was a causal link to the defendant's negligence.

Second, personal information leakage harms personal freedom. While personal information leakage violates the information subject's right to know, the information subject's right to independently control or choose to disclose personal information is also deprived. Nowadays, the disclosure of personal information has become an integral part of the daily life

[56] Xiang Qin and Gao Fuping, "On the Property Attribute of Personal Information Rights and Interests," *Nanjing Journal of Social Sciences* 2 (2022): 98-99.

[57] See the Civil Judgment of Beijing Internet Court (2019) Jing 0491 MC No. 6694.

[58] Wang Liming, "Personal Dignity: The Primary Value of the Title of Personal Rights in Civil Code of China," *Contemporary Law Review* 1 (2021): 3

[59] George Ashenmacher, "Indignity: Redefining the Harm caused by Data Breaches," 51 *Wake Forest Law Review* 1 (2016): 48.

of the information subject, but it should be a voluntary act of the information subject. Freedom of personality applied to the field of personal information is manifested as freedom and choice without coercion, and leakage causes the use of personal information to be manipulated and coerced.[60] The personal dignity and freedom of the information subject are impaired, and this damage can be separately recognized by the court. In the case of Google Inc. vs. Vidal-Hall & Ors, the three plaintiffs claimed that Google's misuse of their personal information had undermined their personal dignity, autonomy and integrity, and demanded compensation from Google for the anxiety and pain caused. The British Court of Appeal held that the damages caused by personal information infringement include mental damage and that the core of personal information protection should be privacy rather than economic rights, and ruled that it was feasible for the plaintiff to claim only mental anguish without proving other losses.[61] This ruling affirmed the independent value of the subjective risk-based damage to the information subject, and that it is not related to personal injury or property loss.

2. Downplaying the "serious" standard

There is a divergence between the *Personal Information Protection Law* and the *Civil Code* on the civil liability rules for personal information infringement. And the divergence has led to controversy over whether the "serious" standard needs to be downplayed.

From the perspective of rights hierarchy, the protection of personality rights and interests, including personal dignity and personal freedom, should precede the protection of property interests. Traditional civil law is centered on property law, and the compensation for property losses is based on losses, and not premised on the "serious" standard.[62] The compensation standard for personality rights and interests should not be higher than that for property losses. If compensation for subjective risk-based damage to the information subject is allowed when only the "serious" standard is met, we would not only violate the primary value concept of protecting human dignity in China's *Civil Code* and deviate from the goal of personal information protection but also conflict with the hierarchy of rights. Globally, the European Union's *General Data Protection Regulation,* the most influential personal data protection law, explicitly stipulates in Article 82 (1) that information subjects who have suffered immaterial damage are entitled to compensation. It further states in Article 146 of the preamble that "the concept of damages shall be interpreted broadly in the light of the circumstances of the case before the court so as to accurately reflect the objectives of the *Regulation*." It can be seen that there is a legal basis for downplaying the standard of "serious" for subjective risk-based damage to personal information.

From the perspective of judicial adjudication, judges have also begun to gradually abandon the "serious" standard in personal information leakage cases. There is no necessary connection between the subjective risk-based damage to personal information and the actual personal injury and property loss, so using the "serious" standard as the premise of compensation has seriously hindered the goal of personal information protection. Whether the mental damage caused by the risk of leakage is serious should be one of the influencing factors rather than a precondition for the compensation liability. In the Pang XX Series Cases, the People's Court of Rencheng District, Jining City, Shandong Province, the People's Court of Decheng District, Dezhou City, and the People's Court of Zhanhua District, Binzhou City, all recognized the risks brought by personal information infringement to the plaintiff and ruled that the defendant should compensate the plaintiff for the mental pain caused by future risks. However, they did not require the plaintiff to prove that the damage had met the "serious" standard in the hearing and used the expression "certain mental distress and worry" in judgment.

[60] Ibid., 33.

[61] Google Inc vs.Vidal-Hall & Ors [2015] EWCACiv 311.

[62] Chen Rong and Yang Yuhua, "Inspection and Improvement of Mental Damage Compensation for Sensitive Personal Information: A Case Analysis of 45 Settled Cases," *Journal of Chongqing University of Posts and Telecommunications (Social Science Edition)* 2 (2023): 47.

IV. Assessment of Dual Risk-Based Damage to Personal Information and Their Compensation

There is a theoretical basis for identifying the dual risk-based damage to personal information, but personal information in all links of circulation contains different degrees of risks, and zero tolerance for risk-based damage will hinder the operation of the digital economy.

A. Assessment of the dual risk-based damages to personal information

The key to whether the dual risk-based damage to personal information should be compensated lies in assessing the risk faced by the information subject in specific cases. In the United Kingdom, the Information Commissioner's Office considers risk assessment to be measuring the likelihood of a risk actually occurring and the severity of the consequences.[63]

1. Likelihood assessment

Likelihood assessment serves to determine the probability for risk-based damage to transform into actual damage. First, it considers whether the perpetrator of the personal information leakage has subjective malice to infringe on the rights and interests of personal information. Unlike the accidental disclosure of personal information, hackers who steal personal information using phishing links or virus software have the subjective malice to defraud or fraudulently use the identity of the information subject, and the risk-based damage is more likely to actually occur in such cases. Second, it evaluates the sensitivity and scarcity of the personal information that has been compromised. Generally, the probability of the actual occurrence of risk-based damage to personal information is directly proportional to the sensitivity and scarcity of personal information. China's *Personal Information Protection Law* divides personal information into sensitive personal information and general personal information, with the former including personal property information, personal health and physiological information, personal biometric information, etc. It is precisely because of the special nature of sensitive personal information that its disclosure means the occurrence of damage.[64] The scarcity of personal information is easily overlooked, but the value of personal information comes not only from sensitivity, but also from scarcity, such as sexual orientation. Scarcity is an integral part of personal information value, and personal information processors can focus on the nature of the leaked personal information to determine the likelihood of the infringer using it for blackmail, humiliation, or exposure.[65]

2. Severity assessment

Severity assessment serves to assess the severity of the risk-based damage caused by personal information leakage. First, it assesses the risk-based damage that may be caused by the leaked personal information in light of specific cases. For example, the objective risk-based damage may be manifested in the payment of additional expenses and unwarranted debt burden. The assessment of the severity of subjective risk-based damage can be based on the opinions of psychologists, psychiatrists and lawyers.[66] Second, it considers the amount and scope of personal information leakage. The greater the amount of personal information leaked, the greater the overall damage caused by the breach. In addition, the risk naturally differs for cases where the personal information leaked is completely exposed to the internet and cases where it is only accessed by specific subjects without permission. In the former cases, the risk-based damage caused cannot be controlled; However, for the latter, personal information processors can ensure the security of personal information through agreements with specific

[63] Information Commissioner's Office, "Understanding and assessing risk in personal data breaches," https:/ico.org.uk/for-organisations/sme-web-hub/understanding-and-assessing-risk-in-personal-data-breaches/.

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

[65] Ido Kilovaty, "Psychological Data Breach Harms," 23 *North Carolina Journal of Law & Technology* 1 (2021): 43 and 53-56.

[66] Ibid., 43 and 59.

subjects. Finally, it considers whether the personal information processor has taken measures to reduce risks. The measures to be taken include not only fraud monitoring of bank accounts, but also psychological counseling services for information subjects.

After the likelihood assessment and severity assessment are completed, it is more important to classify the risk level to which the information subject is exposed. The author uses the risk level chart published by the Data Protection Network of the United Kingdom as a reference, in a bid to distinguish the risk-based damage (see Figure 1).[67] The results of the likelihood assessment can be divided into 4 levels, namely, extremely unlikely (Level 1, 0-25%), likely (Level 2, 25%-50%), very likely (Level 3, 50%-75%), and extremely likely (Level 4, 75%-100%). Corresponding to the likelihood, the results of severity level assessment can also be divided into 4 levels, namely, almost no impact (Level 1, 0-25%); with property damage or emotional anxiety that can be overcome (Level 2, 25%-50%); with more serious economic losses such as misappropriation of funds, being blacklisted by the bank, or obvious mental fear and pain (Level 3, 50%-75%); with significant financial damage, such as high debt, or mental distress, such as suicidal tendencies (Level 4, 75%-100%). Undeniably, it is difficult to measure this assessment precisely, and judges only need to classify the probability and severity of the likelihood in different levels in view of the specific cases. For example, if the judge assesses the probability to be Level 2 (25%-50%), and the severity to be Level 3 (50%-75%), the two are multiplied to Level 6. If the final assessment of risk-based damage is below Level 8, or the proportion is under 50%, the risk-based damage will be deemed to be within the acceptable range; If the level is at or higher than 8 (in red), the risk-based damage will be deemed to exceed the information subject's tolerance and have reach a high degree of probability, so the court should recognize the information subject's claim for damage.

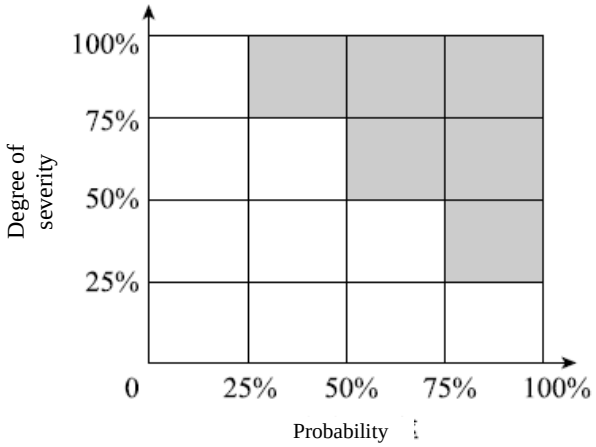

Figure 1: Risk-based Damage Assessment Level

B. Determination of the liability scope for dual risk-based damage to personal information

After assessing the dual risk-based damage to personal information, the court needs to further determine the liability scope for the personal information processor.

1. Introducing a statutory compensation system

According to Article 69, Paragraph 2 of the *Personal Information Protection Law*, it is difficult to determine the losses suffered by the information subject or the benefits obtained by the personal information processor. As a result, the scope of compensation for the risk-based damage to personal information depends on the discretion of the court. Paragraph 2 of Article 12 of China's *Provisions* allows the court to support compensation for the infringed party whose personal rights and interests have been damaged to an amount of less than

[67] Data Protection Network, "2022 Data breach Guide" (March 2022), https:/dpnetwork.org.uk/wp-content/uploads/2022/03/DpN-Data-Breach-Guide-2022. pdf.

500,000 yuan. However, this has an exceedingly large scope of discretion and does not provide clear guidance.

The statutory compensation system can effectively address the difficulty for information subjects to prove the amount of damages.[68] Article 28, Paragraph 3[69] of the *Personal Data Protection Act* of Chinese Taiwan provides for a statutory compensation system by providing a ceiling and floor of a fixed numerical range for information subjects who cannot prove the amount of damage. Some advocated its introduction, but it was ultimately not endorsed by the legislature. The main reason is that once a personal information leak occurs, the number of information subjects involved is extensive; even if the floor of the statutory compensation scope is low, the personal information processor can still face huge compensation.[70] The key to the statutory compensation system lies in fixing the scope of the property value of personal information and changing the status quo of the property attributes of personal information being unrecognized. The statutory upper and lower limit for compensation for personal information infringement established by legislation not only provided a reference for court rulings, but also served the dual functions of compensation and prevention, encouraging personal information processors to strengthen personal information security management.[71] In addition, personal information processors do not compensate for all risk-based damages to personal information. Therefore, it is unreasonable to deny the establishment of the statutory compensation system on the grounds of concern about the huge amount of compensation for personal information processors, and the *Personal Information Protection Law* may introduce a statutory compensation system based on Paragraph 3 of Article 28 of the *Personal Data Protection Act* of Chinese Taiwan.

2. Allocation of responsibilities of personal information processors under fault determination

When the risk-based damage to personal information reaches the risk assessment level, the criterion of causation has been satisfied. Regarding compensation for mental damages, Article 5 of the 2020 *Interpretation of the Supreme People's Court on Several Issues Concerning the Determination of Liability for Mental Damages in Civil Torts* stipulates that the degree of fault of the infringer shall be the primary criterion for deciding the amount of mental damages. However, for the property losses caused by future risks, the principle of complete compensation cannot be applied because they cannot be accurately measured; so, the subjective fault of the personal information processor becomes an important factor in determining the scope of liability.

Depending on the subjective intent, fault can be roughly intentional or negligent. In the latter case, it can be further divided into gross negligence and ordinary negligence. On the one hand, if the personal information processor actively discloses or knowingly allows the stealing of the personal information of information subjects, the circumstances should be justified as"intentional."[72] In re Target Corp. Customer Data Sec. Breach Litig., Target knew that the consumer's bank card information had been stolen by hackers, but continued to accept bank card payments to avoid influence on the sales of the shopping season, and can be regarded as "intentional."[73] On the other hand, the scholar Zeng Shixiong interprets

[68] He Yudong, "The Alienation and Returning of Legal Compensation in IP Law," *Tsinghua University Law Journal* 2 (2020): 144-146.

[69] This article stipulates: According to the preceding two circumstances, if it is not easy for the victims to prove the actual amount of damage, they may request the court to calculate the amount of NT$500 to NT$20,000 per person per incident according to the circumstances of the infringement.

[70] Cheng Xiao and Zeng Jungang, "Liability for Damages of Personal Information Tort," *Social Sciences in Yunnan* 2 (2023): 106.

[71] He Yudong, "The Alienation and Returning of Legal Compensation in IP Law," *Tsinghua University Law Journal* 2 (2020): 145.

[72] Wang Lei, "System of Identifying the Scope of Compensation due to Infringement Damage," *Law Science* 4 (2021): 71-72.

[73] In re Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. 2014).

negligence as "failure to exercise the duty of care."[74] And the difference between gross negligence and ordinary negligence consists in different standard of duty. The breach of the duty of care of an ordinary person constitutes gross negligence, while the violation of the duty of care of a good manager is ordinary negligence.[75] Chapter 5 of China's *Personal Information Protection Law* stipulates that personal information processors have the obligation to take a series of internal management measures to protect personal information. If the personal information processor has subjective intent or gross negligence, it is reasonable for him/her to bear a higher amount of compensation.[76] In the privacy dispute between Zhao X and Yang XX, the real estate company HomeLink required the broker to upload the customer's ID card, real estate certificate and contract information photos to the company's intranet, and did not take any measures to protect them. It is foreseeable that a reasonable person can foresee that this will greatly increase the possibility of infringement on customers' personal information. In this case, HomeLink will be grossly negligent. The People's Court of Chaoyang District, Beijing, recognized the property value of personal information and awarded compensation of 100,000 yuan for damages, reflecting the fault of HomeLink.[77] It is worth noting that if the leaked information is not sensitive personal information, the personal information processor is only guilty of general negligence, and if they take remedial measures to contain the occurrence of risk-based damage, then their liability may be mitigated or even exempted.

C. Establishment of a litigation mechanism for a special representative for compensation for damages to personal information

The special representative litigation mechanism is based on the theory of arbitrary litigation responsibility, in which a third party or organization outside the legal relationship initiates a lawsuit as a party for its own interests or on behalf of others, and the effect of the court ruling extends to the rights subject of the case.[78] The special representative litigation mechanism established by Paragraph 3, Article 95[79] of the *Securities Law* of the People's Republic of China provides institutional experience for compensating for personal information damages.

1. The public interest corporation serving as the subject of special representative litigation

Personal information infringement features a wide range of subjects, little damage to single subjects, and difficulties for information subjects to file a lawsuit for damages, including high cost and long time. Although Article 70 of the *Personal Information Protection Law* provides for public interest litigation on personal information, it is difficult for information subjects to receive compensation in public interest litigation. The establishment of a special representative litigation mechanism in the field of personal information can not only improve the efficiency of litigation, but also address high litigation costs for information subjects.

[74] Zeng Shixiong, *Principles of Damages Law* (Beijing: China University of Political Science and Law Press, 2001), 81.

[75] Wang Lei, "System of Identifying the Scope of Compensation due to Infringement Damage," *Law Science* 4 (2021): 72.

[76] Zheng Xiaojian, "Review on Complete Compensation Principle in Infringement Indemnity," *Law Science* 12 (2017): 171-172.

[77] See the Civil Judgment of People's Court of Chaoyang District, Beijing (2018) Jing 0105 MC No. 9840.

[78] Ji Gefei, "Research on the Types of Arbitrary Litigation from the Functional Perspective," *Oriental Law* 2 (2020): 159.

[79] Paragraph 3 of Article 95 of the *Securities Law*: "Upon entrustment by 50 or more investors, an investor protection institution may represent them to participate in the litigation and shall, pursuant to the preceding paragraph, register with the people's court the investors who are identified as eligible claimants by a securities deposition and clearing institution, except for those investors who have clearly expressed their unwillingness to participate in the litigation."

It is more reasonable to use a public welfare organization as a special representative in a lawsuit. First of all, public welfare organizations have a public interest nature, which can resolve disputes caused by recommending representatives among the information subjects, and are easier to obtain the support of all information subjects.[80] Precisely because of their public interest nature, public welfare organizations will not abuse litigation because the risk-based damage to personal information is recognized.[81] Second, non-profit organizations, such as consumer associations, have the experience and expertise in litigation to help reverse the asymmetry between information subjects and personal information processors. Finally, since the information subjects in personal information leakage cases can spread to the entire country, public welfare organizations can transcend geographical restrictions and equally protect the rights and interests of each information subject.

The relevant regulations of Chinese Taiwan can be of reference. Paragraph 1 of Article 34 of its *Personal Data Protection Act* clearly establishes a special representative litigation system, stipulating that in the event of infringement on the rights of a majority of the parties due to the same cause and with the same facts, a foundation or a public interest corporation may file a lawsuit for compensation for damage to personal information as a party after being entrusted by more than 20 information subjects. In addition, Article 39 of the *Personal Data Protection Act* stipulates that compensation for litigation obtained by a foundation or a public interest corporation shall be paid to the entrusting information subject separately after deducting the necessary costs for litigation.

2. Explicit inclusion under information disclosure

There are two ways for parties to participate in special representative litigation, namely, the opt-in system and the opt-out system.[82] The former emphasizes that the parties need to explicitly express their willingness to join the litigation to the court in accordance with certain procedures, while the latter acquiesces that all parties with standing to the litigation participate in the litigation in full, unless individual entities explicitly withdraw from the litigation. The withdrawal system is advantageous in that it ensures that all parties can obtain relief, but its application to the field of personal information is not feasible. Personal information leakage can involve millions or tens of millions of information subjects, and some do not even know about the leakage. The court is simply unable to determine the parties involved, let alone make a ruling. The reason for Paragraph 3 of Article 95 of the *Securities Law* of China to adopt the withdrawal system is that the securities registration and clearing institution can effectively provide a list of investors, but there is no similar authority in the field of personal information.

Compared with the opt-out system, the opt-in system can help the court to quickly confirm the scope of information subjects involved in the litigation and respect their willingness to litigate. Paragraph 2 of Article 34 of the *Personal Data Protection Act* of Chinese Taiwan provides for the implementation of an express opt-in system, in which the court announces or notifies the information subjects who have suffered infringement due to the same factual reason, and the information subjects need to grant the litigation right to the foundation or public interest corporationwithin a certain period of time. However, it is undeniable that the court's use of traditional media notices such as announcements and newspapers will greatly limit the participation of information subjects, so the way of information disclosure is extremely important.[83] On the one hand, public interest corporations

[80] Feng Guo and Xiong Yuqing, "The Development and Improvement of the Special Representative Litigation System for Securities Disputes," *Yangtze Tribune* 5 (2022): 69.
[81] Tang Weijian, "Security Representative Lawsuits with Chinese Characteristics," *People's Judicature* 28 (2020): 43-44.
[82] Feng Guo and Xiong Yuqing, "The Development and Improvement of the Special Representative Litigation System for Securities Disputes," *Yangtze Tribune* 5 (2022): 68.
[83] Fan Yuting, "A Review of the EU Directive on Representative Actions for the Protection of Consumers' Collective Interests," *Judicial Think Tank* 1 (2021): 228.

can use a variety of electronic methods, such as websites and official accounts, to disclose the progress and results of the representative litigation. On the other hand, the court may expand the scope of the notice with the help of a database composed of big data technology,[84] such as IP addresses, and may require the personal information processor to provide the contact information of the information subjects in its possession, for example, mobile phone number and email.

V. Conclusion

As scholar Adler has argued, some risks are acceptable, while others are clearly unacceptable.[85] The theoretical support for the determination of dual risk-based damage to personal information does not mean that they can be fully accepted by the court, which needs to assess and quantify the level of risk-based damage. In view of the difficulties in determining the property value of personal information in China, a statutory compensation system may be introduced to provide a reference basis for the court. Since most of the personal information leakage cases have not yet caused property losses, it is difficult for the court to rule according to the principle of full compensation. So, it is necessary to shift to the fault of the personal information processor as the key consideration factor in determining the scope of liability. In addition, the establishment of a special representative litigation mechanism, with public interest corporationsas the litigation subject and the express participation of information subjects, can reduce the burden of litigation on the information subjects and ensure that they are compensated from the compensation amount.

(Translated by *QIAN Chuijun*)

[84] Fan Xiaoliang, "On Construction of Litigation Mechanism of Special Representatives over Dispute of Consumption Damages in Our Country," *Law Science* 12 (2022): 121.

[85] Matthew D. Adler, "Risk, Death and Harm: The Normative Foundations of Risk Regulation," 87 *Minnesota Law Review* 5 (2003): 1417-1418 .