



损害确定归责模式下的个人信息风险性损害救济

秦语悦,刘海安

(天津大学法学院,天津 300072)

摘要:在个人信息风险性损害扩张场景中,损害确定性认定路径存在判断依据不明和操作性不足的问题,亟需在传统侵权法损害赔偿归责模式下寻求破解路径。该研究聚焦于化解个人信息风险性损害的难预测性、无形性特征,与传统损害认定所要求的确定性、可计量性之间的适配冲突。合理预防费用与隐私信息泄露导致的机会利益损失,可被认定为确定性损害并纳入赔偿范围;而个人信息泄露导致的风险本身提升,以及消费操纵、“大数据杀熟”等算法区分损害,则不应纳入可赔偿范围。在损害计量方面,预防费用损害采用差额标准计算,隐私信息泄露所致机会利益损失数额可通过许可使用费标准予以确定。设定法定最低赔偿额,既能够有效保障信息主体的维权积极性,又能够适度彰显对信息主体人身利益的尊重及救济。

关键词:风险性损害;损害确定;个人信息;救济;预防费用;机会利益

中图分类号: DF52

文献标志码: A

文章编号: 1673-3851 (2026) 08-0513-09

Remedies for risk damage of personal information under the attribution mode of determinative damage

QIN Yuyue, LIU Hai'an

(Law School, Tianjin University, Tianjin 300072, China)

Abstract: In the context of the expansion of personal information risky damages, the identification path of damage certainty suffers from ambiguous criteria and insufficient operational feasibility. It is urgent to explore solutions within the framework of the liability imputation model for damages in traditional tort law. This study focuses on reconciling the inherent conflict between the unpredictable and intangible characteristics of personal information risky damages and the certainty and measurability required by traditional damage identification. Reasonable prevention costs and the loss of opportunity benefits caused by the disclosure of privacy information can be compensated under the traditional determinative damage standard; however, the risk increase caused by the disclosure of privacy information, as well as algorithm-based discriminatory damages such as consumer manipulation and "big data-based price discrimination", should not be included in the compensable scope. In terms of damage measurement, the damage of prevention costs shall be calculated using the difference standard, and the amount of opportunity interest losses caused by the leakage of private information can be determined through the license fee standard. The establishment of a statutory minimum compensation amount can not only effectively protect the enthusiasm of information subjects to safeguard their rights, but also properly demonstrate respect for and relief of the personal interests of information subjects.

Key words: risk damage; determinative damage; personal information; relief; prevention costs; opportunity benefits

收稿日期:2025-07-01 网络出版日期:2026-02-02

基金项目:司法部法治建设与法学理论研究部级科研项目(24SFB2015)

作者简介:秦语悦(2000—),女,山西晋城人,硕士研究生,主要从事民商法方面的研究。

通信作者:刘海安, E-mail: shineark@163.com

个人信息保护旨在维护数字社会中自然人的人格尊严与人格自由,确保自然人身份建构的自主性和完整性免受大数据技术的侵蚀^[1]。当前,个人信息泄露致信息主体受损的情形日益严峻,其引发的负面效应呈指数级扩散,亟需通过法律规范的完善与实施来发挥预防作用^[2]。有学者主张以未来侵权风险为赔偿对象,实现对信息主体的救济^[3-4],即设立风险性损害赔偿制度。但是,风险的“或然性”特征与侵权法损害确定归责模式存在冲突。为调和此冲突,有学者提出将损害“确定性”的证明标准放宽至具有“客观合理的可能性”^[5];还有学者认为,损害证明标准应当由立法者在平衡信息主体权益保护与信息处理者行为自由的基础上权衡确立^[6]。实践中,法官常以缺乏信息处理者造成实际损害的证据为由,不支持信息主体要求信息处理者承担侵权责任的请求^①。然而,在单条个人信息被非法处理或利用的直接损害较小情形下^[7],若对未来可能发生的风险性损害置之不理,将挫伤信息主体维权的积极性,进而使侵权现象泛滥。

回归传统侵权法损害赔偿归责模式,对于避免司法实务混乱具有积极意义。本文在确认风险性损害之救济价值的基础上,针对风险性损害与传统侵权法损害确定归责模式存在的冲突,结合各类风险性损害的特性,区分考量其是否适配传统侵权损害规则。本文创新构建三重损害赔偿标准协调机制,即在保留传统损害差额计算标准的基础上,引入许可使用费标准作为重要补充,并以法定最低赔偿额制度提供兜底保障,借此回应大数据时代个人信息风险性损害救济需求,以期在损害确定归责模式下实现对数字人权领域个人信息权益的有效保护。

一、救济困境:风险性损害与传统规则的冲突

虽然信息主体对风险性损害的救济需求迫切,但风险性损害赔偿在司法实践中面临着双重困境:赔偿责任能否成立存有争议,赔偿责任如何分配亦是难题。造成该困境的根源在于,风险性损害具有的难预测性、无形性,与侵权法损害确定归责模式要求的确定性、可计量性存在直接冲突。

(一)风险性损害难预测性与损害确定性的冲突

在当前司法实践普遍坚持损害确定性标准的背景下,风险性损害因具有难预测性而无法满足传统侵权归责模式要求。这种难预测性与确定性相违背,动摇了风险性损害赔偿责任成立的正当性根基。

在传统侵权法理论中,损害应当具有客观真实

性和确定性^[8],即损害必须是现实发生的具体损害而非主观推测的抽象损害。这一理论以保障法律秩序的稳定性与可预测性为价值根基,使得损害确定性作为民事赔偿的前提而存在^[9]。“无损害则无救济”原则作为传统侵权法理论内核的体现,发挥着关键的排除功能,明确将尚未现实发生的损害排除于救济范围之外,即便有充分的现实依据证明损害在未来某一时段一定会发生或者损害已经迫在眉睫也不例外。由此可见,传统侵权法理论将“损害的既成事实”作为连接不法行为与民事责任的桥梁,彰显了传统侵权法理论事后救济的核心价值取向。

区别于传统损害的确定性,风险性损害的核心特征在于难预测性,其难以预测的本质集中体现为损害现实化过程的高度不确定性,具体表现为,既无法确定风险性损害是否会转化为现实损害,也无从预判其将会于何时转化。在大数据时代,以数据为依托的个人信息复制程序简单,其所具有的非排他性使得多个主体可以共同享有信息资源,个人信息可能以惊人的数量和速度在信息处理者之间流动,而各环节的信息处理者是否会违法滥用信息造成实际损害难以预测。这便使得风险性损害究竟是否会转化为现实损害难以预测。同时,以数据为载体的个人信息早已突破纸质信息不易保存的局限,可以实现较长时间内完整地保存。只要泄露的信息以数据形式保存在行为人手中,则任何时候都有可能发生个人信息泄露,而且一旦泄露即意味着在互联网中永久存在,随时可能引发后续的诈骗、盗窃、伤害等侵害行为^[10]。可见,风险性损害转化为现实损害的时间难以预测。

损害“确定性”要求损害必须具有客观、可验证的具体形态,而风险性损害本质上具有多维难预测性——既无法预判其是否会转化为现实损害,也难以确定其转化的时间。此种“难预测性”与“确定性”之间的对立,体现了风险性损害与传统损害之间存在的冲突。由于风险性损害的难预测性使其无法适配传统侵权归责模式,因此,风险性损害赔偿责任成立的正当性有待证成。风险性损害转化为现实损害的概率难以预测,无法完全排除风险性损害在特定情形下并未转化为现实损害的可能。例如,在个人信息泄露后,因信息处理者尽到了相应的信义义务^[11],而使得风险并未转化为现实。在此情形下若对风险性损害进行赔偿,会使得信息主体无损害发

① 参见(2023)京02民终8736号民事判决书。

生而获得利益,这与“禁止不当得利”原则相违背,直接动摇了风险性损害赔偿责任成立的正当性基础,使得信息主体权利救济面临困境。

(二)风险性损害无形性与损害可计量性的冲突

传统侵权归责模式下要求损害可计量,但风险性损害因其无形性而难以计算赔偿金额,两者之间存在冲突。能否化解该冲突,对于风险性损害赔偿责任成立后责任如何承担至关重要。

在传统侵权归责模式下,损害计量对于损害赔偿实现具有重要制约作用。传统计算损害赔偿金额的标准建立在差额说的基础上,其关注的是侵权行为发生后主体的财产状况与主体未遭受侵权行为时应当享有的财产状况的差额。在完全赔偿理念要求下,侵权人应在财产层面将受害人的状态恢复到损害并未发生时的假设状态^[12]。只有量化计算损害具体赔偿的金额,才能精确填补受害人的损失,从而实现侵权损害赔偿事后救济的目的。

然而,风险性损害的发生与实现时点呈现分离状态,损害发生时大多悄无声息,只有在实现那一刻才显现为有形损害,其具体的侵害路径与方式无从确证。这使得风险性损害既无法被精确估价,也缺乏客观的鉴定标准^[13]。

风险性损害的无形性特点与传统归责模式下损害可计量要求相悖而行,两者之间存在冲突。可计量性以经济价值转换作为救济前提,要求损害能够通过货币进行精确量化与举证;而风险性损害表现为动态发展的长期风险,不但使信息主体无法及时识别损害发生,损害的范围也无法通过传统评估方式衡量。一方面,信息主体面临损害识别难题。大数据侵权具有无形性与隐蔽性^[14],信息主体作为技术层面的弱势群体,可能连个人信息何时何地被人侵犯都无从知晓,如何获得救济更无从谈起。另一方面,赔偿金额的计算缺乏参考依据。信息一旦泄露或由他人非法获取,便会迅速流向互联网的汪洋中并难以收回。即便是信息处理者,也很难完全抹去信息泄露后留下的全部痕迹。这导致无法直接计算财产损害赔偿金额。

总之,风险性损害的无形性给风险性损害救济带来了困难,此种量化体系的失灵极易导致司法裁判陷入困境。

二、路径抉择:传统损害确定性的认定

不同学者对于损害要件的可确定性标准,主要形成了两种不同的解释路径:一种是损害确定性认

定的传统路径;另一种是损害确定性认定的扩张路径^[3-4]。在后者面临众多质疑时,前者的相对合理性凸显。

(一)损害确定性标准的两种认定路径

损害确定性认定的传统路径实质是主张坚持损害现实发生的确定性标准,并在此基础上将个人信息泄露后现实发生的损害纳入赔偿考察范围。该立场所主张的“无损害则无救济”原则在多领域都有体现。例如,在美国著名的石棉致害大规模侵权诉讼案中,法院对潜在受害人的请求不予支持^[15]。医疗领域规定,在已披露风险实现损害或虽未披露但未发生损害的情形下,受害人不得以专业过失侵权为由对医生提起诉讼^[16]。

鉴于大数据时代个人信息受损风险不断提升,部分学者认为传统路径救济有限,故而提出以扩张解释损害确定性认定标准为核心的扩张路径,将满足一定条件的未来损害纳入赔偿范围。但扩张解释后的新标准并不统一。美国的部分司法实践采取了“实质性风险”的标准,即未来损害必将发生或迫近发生也构成侵权法上的损害^[17]。也有学者认为以“客观合理的可能性”为判断标准更为合适^[5]。

(二)传统认定损害确定性路径的坚守

对传统认定路径的证成,不仅需剖析扩张认定路径的不当,更需从制度功能与法理基础出发正面阐述其价值,二者共同构成其合理性的完整支撑。

1. 扩张认定路径的不当性

损害确定性认定的扩张路径主张把损害状态从现在时扩展至将来时,在法理与实践层面均存在不当之处。

在法理层面,扩张认定路径中的确定性标准不统一且无合理依据,极易导致同案不同判的司法混乱。支持扩张解释的立场主要以“实质性风险”或者“客观合理的可能性”标准代替传统损害确定性标准。依据类推解释方法,扩张标准的设定理应达到与“现实发生”具有同等确定性高度的要求,但扩张路径实则降低了对确定性的要求,且降低的理由与幅度均未得到充分证成。这些标准主观性过强,缺乏统一的衡量标准,严重侵蚀了扩张认定路径的正当性根基。

在实践层面,若未能充分证成风险性损害的现实与紧迫,则不仅会动摇损害确定性的根基,也使扩张认定路径本身丧失正当性与必要性。个人信息权天然地存在个人信息被泄露致信息主体受损的风险,但该风险可通过相关措施予以降低,尚无打破侵

权法固有理论基础的必要性。例如,面对个人信息泄露导致群众收到诈骗短信或电话情形,预防诈骗受损的措施卓有成效。2023年国家反诈中心累计下发资金预警指令940.6万条,会同相关部门拦截诈骗电话27.5亿次、短信22.8亿条,处置涉诈域名网址836.4万个^[18]。由此可见,扩张解释损害确定性并不符合现实需求。

2. 传统认定路径的合理性

坚守传统认定损害确定性路径的原因在于,其既深刻植根于损害计算的实践理性,又紧密契合侵权法的核心功能。

就损害赔偿金额计算而言,作为当前主流学说的差额说决定了损害必须是现实发生的。未来发生的损害本身具有高度盖然性,不仅是否会有差额实际产生无法确认,而且其造成的财产变化也无法确定。要求损害现实发生,还可以避免出现因信息主体主观臆测请求过多赔偿而加重信息处理者负担的情形。基于实用主义考量,损害现实发生更有利于确定权利主体财产变动的具体差额。同时,在传统侵权理论中,侵权法侧重事后救济而非事前预防。以数据为载体的个人信息具备可复制性,这使得损害实际发生的时间和次数无法被预测。即便要求当前的信息处理者提前赔偿,也难以确保能够弥补该信息在后续流转中给信息主体造成的全部损失。可见,个人信息保护适用事后救济方式更具合理性。

除此之外,损害确定性认定的传统路径不仅在理论上具有正当性,在司法实践中也得到了支持。多数法院在判决中支持了赔礼道歉以及支付公证费、律师费等诉求^①;个别法院支持了受害人关于精神损害赔偿的诉求^②;针对信息泄露可能引发其他损害而提出赔偿的请求,法院通常以无实际损害发生为由判定案件缺乏充分的事实及法律依据,驳回原告诉讼请求^③。

由此可见,相较于扩张认定路径,坚守传统认定路径维系了侵权责任构成的清晰边界,在实践上更具可行性。

三、范围确认:风险性损害可赔偿类型的界定

当前对风险性损害的划分类型很多,有学者主张将其划分为个人信息泄露导致的风险提升、预防风险的支出以及风险引发的焦虑三类赔偿损害^[4]。有学者则认为风险性损害应当包含人身安全受损风险、潜在的经济损害、预防未来损害的支出^[3]。有学者提出了更为细致的四分法,即风险性损害、情感性

损害、经济性损害、信息性损害^[13]。还有学者强调“新型损害”,如社会分选与歧视、消费操纵与关系控制等^[12]。虽然学界对风险性损害的类型化研究视角多元,但部分损害并未满足损害赔偿责任成立的要件,因此必须审慎甄别以划定合理的风险性损害赔偿范围。

(一)传统确定性标准下的可赔偿损害

在个人信息泄露后、下游损害实际发生前,信息主体支出的合理预防费用以及隐私信息泄露导致的机会利益损失,本质上属于现实发生的财产损害,应纳入可赔偿损害范围。

1. 合理预防费用

当前多数学者赞同将预防风险所支出的费用作为一种财产损害适用侵权损害救济规则进行赔偿^[3]。信息主体为了阻止信息进一步泄露或避免损害风险现实化,采取购买信用监控、身份盗窃预防服务、重新更换信用卡等预防措施,应当获得赔偿^[19]。

损害赔偿额既不能超出损害从而使当事人获益,也不能少于损失使当事人无法获得完全赔偿^[20]。赔偿预防费用极易给信息主体留有恶意“制造”项目支出费用而获利的空间,这与“禁止从损害中获益”原则相抵触。预防费用能否纳入赔偿范围内,关键在于能否防止信息主体滥用权利,以及能否保证预防费用是“为制止侵权行为所支出的合理费用”。具体可以参考以下标准判断:

第一,必要性标准。信息主体所采取的措施应当符合并满足预防目的,如果预防措施不是为了达到该目的或者根本无法实现该目的,则难以认可该措施的必要性。可借助因果关系判断予以认定。因为下游损害并未实际发生,所以不存在事实上的因果关系,只能判断法律上的因果关系。一方面,要参照相当因果关系标准,确定预防措施能否实质性地提高信息主体的风险防范能力,即预防措施能否实质性地降低信息泄露的致害风险。另一方面,要确认信息所致损害是否在法律价值观保护的范围内。如果损害不在法律保护范围内,则纵然预防措施能够实质性地预防该损害,也不应就该措施成本提供补偿。

第二,适当性标准。首先,该标准强调预防措施的成本应当低于损害成本。预防成本的具体数额需

① 参见(2019)京0491民初16142号民事判决书。

② 参见(2022)鲁02民终11156号民事判决书。

③ 参见(2022)京0491民初17326号民事判决书。

要以信息主体提供实际支出费用凭证为依据来确定;损害成本具体数额的计算可参考汉德公式,即预计损害大小乘以事故发生的概率^①。在此标准下,信息主体所支出的费用不能大于其想要保护的利益。对于市价低廉却蕴含极高情感价值的物品,必须拟制其经济价值,作为判断预防措施是否适当的基准。其次,预防措施的选择应当兼具效率占优考量。当存在多种利益保护措施时,信息主体原则上应选取费用更低、见效更快的措施,但该标准旨在排除效率过低或过于“奢侈”的方案,并不意味着选择非效率占优措施就必然不当。

2. 隐私信息的机会利益损失

合同具有价值,机会也有价值^[21]。隐私信息泄露导致的机会利益损失,实际上是指信息主体利用其未公开的隐私信息获取利益的有利条件丧失,主要表现在信息主体许可他人使用隐私信息而获利的机会丧失。例如,明星未公开的婚姻状况信息,一旦被他人知晓并公开传播,该明星便失去商业化利用该信息的可能。此类损害是真实且不可逆的,将其纳入赔偿范围具有合理性。

一方面,信息主体享有许可他人使用信息而获利的权利。《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)第四条规定了处理个人信息的含义,法条的不完全列举给信息主体的许可使用权利创造了合法空间。尽管学者们对个人信息财产权是否独立于人格权成立存在争论,但是多数学者认可人格权利兼具财产基因^[22]。信息主体享受财产利益的主要方式是通过许可他人使用自己的个人信息而实现的。典型的例子是明星商业化利用自己的姓名、照片等个人信息获利。他们不仅可以通过签订广告合同实现商业化利用,还可以通过电视节目或网络媒体自曝隐私而吸引粉丝、增加流量^[23]。在实践中,不少普通人也借助互联网技术在社交平台上公布自己的个人信息博取点击量、转载率,不断吸引大众视线从而实现了“流量变现”。

另一方面,只有隐私信息泄露才会导致机会利益损失。隐私信息的特点在于其一旦泄露为公众所知晓,便丧失了商业价值,即无法再为信息主体许可他人使用而获利。同时,这种机会利益的损失是隐私信息泄露后必然发生的一种现实损害。无论信息主体当下是否知晓隐私信息被泄露,都会因为信息被公开而直接丧失商业化许可使用获利的机会。姓名、照片等类型的个人信息泄露,并不会必然导致机会利益的损失。例如,尽管有行为人恶意使用信息

主体的照片营利,信息主体依旧可以许可他人使用自己的照片,并不存在照片本身失去价值导致信息主体无法许可他人使用而获利的情形,所以这类信息的泄露并没有出现现实机会利益损失。虽然这类信息的泄露可能会进一步导致隐私信息泄露而最终出现机会利益损失,但是其中的因果关系过于遥远。出于平衡个人信息保护和利用的考量,应当只对隐私信息泄露导致的机会利益损失进行赔偿。

(二)传统确定性标准下的不可赔偿损害

对因个人信息泄露导致风险提升进行赔偿,实质上无法避免将风险作为损害的逻辑矛盾。即使将个人信息泄露所可能引发的一切不利益归纳为新型损害,也无法直接适用传统侵权损害救济规则。

1. 个人信息泄露导致的风险提升

个人信息权自带因信息主体信息泄露而遭受人身财产安全损害的风险。在个人信息泄露后,信息主体遭受损害的风险确实会升高。尤其以数据为载体的个人信息泄露后,因其易复制的特性会使得更多主体持有该信息。在多个主体拥有该信息时,信息主体遭受下游损害的风险远远大于自己保有信息时遭受损害的风险。

信息泄露引发对信息主体生活安宁的干扰事件不胜枚举,规模化的泄露风险更加隐蔽,对主体的威胁还会产生积累效应^[24]。当前存在很多因为信息主体居住地址、户籍信息等暴露而引发跟踪、杀害等恶性犯罪的案例^[8],因此有学者主张将风险提升纳入赔偿范围。但这种做法存在不合理之处。

第一,风险并非损害本身,不符合归责要件要求。主张将风险认定为损害的学者认为,风险与损害具有同质性,两者实质上都是法律上的不利益。法律作为兼具工具理性和价值理性的利益调控手段,应当认定风险可以作为损害,风险性损害因此可以获得赔偿。但是该观点忽略了最基本的逻辑要求。风险实际受损害发生的概率与损害大小的双重影响,将损害发生的概率定义为损害本身,理论上便存在逻辑矛盾。有风险存在仅意味着有损害现实发生的可能,“或然性”是其本质特征,不能将风险本身认作损害。而填补损害作为侵权法的首要目标,若无现实的损害需要填补,则无侵权责任成立的必要^[25]。

① 汉德公式: $B < PL$,是法官汉德在美利坚合众国政府诉卡罗尔拖轮公司一案中提出的。 B 指预防事故的成本; L 指一旦发生所造成的实际损失; P 指事故发生的概率; PL 指(事先来看)事故的预先损失。只有在潜在的致害者预防未来事故的成本小于预期事故的可能性乘预期事故损失时,行为人才负过失侵权责任。

第二,风险升高不等于损害发生,不符合损害构成要件。即便能确定风险提高,也无法确定风险提升幅度;即便从风险发生概率30%升至80%,也难以达到100%的发生概率。无法确定损害是否会现实发生,使得计算损害赔偿存在困难,因此无法适用侵权损害救济规则。

第三,难以确定责任主体以及责任分配形式。在个人信息泄露的情形下,可能持有该信息的主体数量众多且不易锁定信息泄露源头。而法院通常要求信息主体作为原告证明被告是掌握或泄露信息的“唯一主体”,信息主体囿于调查能力和调查成本而举证不能,只能承担相应的败诉后果^[26]。应当认识到,“危险开启者”并不必然等同于“责任承担者”。从危险中获取经济利益者经常被视为具有制止危险义务的人,但是“危险开启者”的义务并非防止全部风险的现实化,而是在其能力所及的范围内合理防范风险。对于可能因个人信息泄露而引发的电信诈骗、身体损害、严重精神失常等,因超出个人信息处理者的预见范围以及预防能力范围,而无法认定其存在过错基础^[27]。除此之外,各信息处理者持有该信息,对信息主体遭受实际损害风险的具体提升比例难以确定,也使得各信息处理者之间应当以何种形式承担责任尚存在争议^[28]。

2. 算法区分损害

“算法区分损害”是指信息处理者基于算法将其收集信息对应的信息主体区别对待而导致的损害,主要包括消费操纵与“大数据杀熟”等。消费操纵是指信息处理者会潜在影响信息主体的自主决定。比如,商业主体可能通过广告精准投放来引诱信息主体消费。“大数据杀熟”是指向不同用户提供相同商品或服务时索取不同对价。

支持对上述新型损害进行赔偿的学者认为,虽然不存在现实的财产差额,但是信息主体的利益状态已经发生变化,所以在修正差额说的基础上认定可以适用侵权损害救济规则^[12]。除了修正差额说是否具有合理性尚存争议,该观点还存在其他问题,即信息主体的利益状态是否因算法区分对待而实际发生不利变化存在极大的不确定性。“大数据杀熟”的行为主体一般是大型网络应用平台。平台确实有因商业运营而收集信息的需求,但其实际上也会受到很多信息收集规定的约束。不能因为平台有收集信息的需求,便认定只要存在信息泄露,平台就一定

会利用该信息对信息主体进行歧视或操控。同时,信息主体仅在知悉个人信息泄露的条件下,很难用

证据证明平台将会利用信息实施“大数据杀熟”。也许现实中这些平台确实准备利用信息对信息主体进行“杀熟”,但信息主体在没有证据证明的情况下只能作为一种推测,无法满足传统认定损害确定性的标准。

四、责任承担:可计量要求下赔偿金额的认定

风险性损害赔偿责任成立后,还需要进一步确定责任承担的方式。如何计算具体的赔偿金额,满足损害的可计量性要求,是能否真正实现风险性损害救济的关键。

(一) 损害赔偿金的计量

在司法实践中,法院大都支持公证费的赔偿^①,只有个别法官依法酌定侵权人赔偿受害人一定数额的合理开支等经济损失^②。由此可见,当前对个人信息赔偿金额的计量还存在很大的讨论空间。

1. 合理预防费用的计量

金钱赔偿的目的在于使受害人的财产利益状态恢复至损害未发生前。对于信息主体所支出的合理预防费用的赔偿金额计算,应当参考信息主体实际支出的金额。除此之外,还应当将附带财产损失(如误工费、利息亏损等^[29])计入其中。具体而言,在银行卡信息泄露时,信息主体需要更换账户,因此将其支付的工本费作为损害赔偿金额没有异议。然而,因为换户导致存款可获得的利息亏损部分也应当算作附带财产损失予以赔偿,这样才能满足信息主体状态恢复的要求。所以,信息处理者不仅要赔偿信息主体不应减少的损失,其本应当获得的利益也在赔偿范围内。当然,对该部分费用也应当适用必要性原则和适当性原则,如此才能确保其不超出“为制止侵权行为所支出的合理费用”范围。

总之,个人信息种类丰富、内容涉及利益众多,泄露的个人信息不同,所采取的降低风险的措施自然也不相同,需要法官根据案件具体情况作具体分

① 参见(2021)浙06民终3129号二审民事判决书。

② 参见(2019)京0491民初16142号民事判决书。

③ 参见(2022)粤0192民初20966号民事判决书。

析。但是,依照信息主体支出的合理预防费用和附带财产损失两部分总和来确认赔偿金额,是具有合理性的。

2. 隐私信息泄露导致机会利益损失的计量

对于隐私信息泄露导致机会利益损失的赔偿金额计量,可以通过在信息主体和信息处理者之间构建虚拟的许可使用合同、设定许可使用费用的方式确定具体的赔偿金额,理由如下:

第一,所受损失与所得利益标准难以奏效。《个人信息保护法》第六十九条规定了损害赔偿责任的确定。该条以信息主体信息泄露受到的损失或者信息处理者因此获得的利益优先作为赔偿确定依据。只有依照前述办法难以确定的,才由法官根据实际情况酌定赔偿数额。在实践中,对于隐私信息泄露导致信息主体机会利益损失的赔偿金额计算,很难通过计算信息主体的损失或者信息处理者的获益进行确定。一方面,信息主体损失涉及的范围难以确定。信息主体最直接的损失是个人信息本身的价值,将个人信息作为财产利益看待,不仅会出现赔偿额较低的情形^①,实际上也没有兼顾个人信息人身属性的价值。另一方面,信息处理者因个人信息而获益的数额难以计算。个人信息具有规模聚集效应,若将集合信息的整体价值分散于个体层面,单个信息的价值将被严重稀释,其原生损害几乎可忽略不计^[30];而作为集合体存在时,又难以判断每条个人信息为信息处理者获益的贡献。同时,获取个人信息通常只是信息处理者采取后续获利行为的前提,如何区分后续行为所获得的利益与个人信息本身为信息处理者带来的利益,也存在困难。

第二,许可使用费标准的采用。法官往往需要根据实际情况酌定赔偿金额。“实际情况”作为法官确定数额的唯一依据过于空泛,不利于限制法官的自由裁量权,也不利于形成统一的司法实践。因此,需要提出新的标准。信息主体许可他人使用所对应的费用或可成为参考标准,主要通过信息主体与信息处理者之间构建虚拟许可使用合同的方法实现。法官可以通过模拟理性的信息主体和信息处理者可能考虑的许可使用的相关因素,在构建以个人信息本身价值和该信息的市场价值总和作为最低许可费的基础上,结合个案的特殊情况并列出影响因素,对这个基础的许可费用作出进一步修正。通过该方法,将法官构建许可使用合同确定许可使用费的过程充分展现,能够在充分发挥法官自由裁量权的同时,又提供相关的参考依据限制其权利,具有多

重积极价值。

(二)法定最低赔偿额的设定

个人信息损害计量的结果可能因赔偿数额过低而产生不如意的后果。因此,设定风险性损害法定最低赔偿额规则的设想涌现。该规则是指当信息侵权造成的客观经济损失数额过小时,适用法定最低赔偿额代替实际的经济损失作为最终的赔偿金额。

1. 法定最低赔偿额设定的必要性

在当前司法实践中,信息主体作为受害者所获赔偿金额过低,难以实现有效救济。在吕某与车之家公司网络侵权责任纠纷案^②中,法院便以原告主张1元的赔偿且个人信息的价值确实难以估量为由,最终判决被告赔偿1元。在王某与佑顺公司网络侵权责任纠纷案^③中,尽管因为王某主动撤回了请求精神损害赔偿的请求,法官没有对精神损害赔偿作出判决,但法院最终在认定个人信息侵权成立的基础上,仅判决信息公司向王某赔偿退订短信资讯费0.1元。此种“象征性赔偿”不仅挫伤信息主体的维权意愿,而且可能纵容信息处理者的违法行为,最终陷入“侵权易、维权难、信息泄露频发”的恶性循环。为打破此循环,亟需设定合理的法定最低赔偿制度。

首先,法定最低赔偿额规则是激励信息主体维权积极性的关键。当维权难度大、经济成本高、投入精力多,但赔偿金额微薄时,理性的主体自然会放弃维权^[31]。法定最低赔偿额能够在一定程度上覆盖部分维权成本,有助于激励信息主体的维权积极性。其次,法定最低赔偿额规则是彰显对信息主体人格尊严保护的关键。个人信息风险性损害通常表现为宏观的大规模经济损害,但分摊至单一个体时的经济损害数额往往较小。法院仅仅依照信息本身的对价判决赔偿金额,是对个人信息所承载的人格尊严的忽视。设定法定最低赔偿额,正是法律对个人信息人格利益的保护。无论是单一的个人信息,还是汇集的个人信息,都具有重要的保护价值。最后,法定最低赔偿额是赋能公益诉讼的关键。稳定、可预期的赔偿金额,有助于公益诉讼主体履职。公益诉讼主体的介入有助于促使法院裁判超越个案赔偿,转而更关注维护公共秩序与社会稳定,并以此倒逼信息处理者主动维护信息安全。

① 参见(2023)京0116民初1296号民事判决书。

② 参见(2021)京0491民初46779号民事判决书。

③ 参见(2021)粤0192民初44778号民事判决书。

2. 法定最低赔偿数额的具体设定

现有《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》确认了法院可以在 50 万元以下酌定赔偿数额，但是因为没有规定下限，依旧无法解决赔偿过少而降低信息主体维权积极性的问题。所以，还需要通过设定具体的法定最低赔偿额来完善赔偿制度。

一方面，应当依照个人信息的类型区分设定最低赔偿额。当前《个人信息保护法》第二十八条规定了敏感个人信息类型^①，我国国家标准 GB/T 35273—2020《信息安全技术个人信息安全规范》不仅规定了敏感个人信息的类型，还在附录中规定了判定方法^②。敏感信息在立法层面具有比一般信息更加严格的保护措施，在设定法定最低赔偿额时，可以作出敏感信息最低赔偿额高于一般信息的区分处理。应当认识到，立法上未被界定为“敏感”的一般个人信息，一旦经大规模聚合与利用，完全可能引发与敏感个人信息具有损害相当性的风险，应当具体情况具体分析^[32]。

另一方面，最低法定赔偿数额需要明确。《中华人民共和国消费者权益保护法》第五十五条规定的“三倍赔偿以及最低赔偿额兜底”条款具有借鉴意义。在个人信息保护领域，建议作如下设定：信息主体有权依照其被泄露信息价值的三倍请求赔偿，赔偿数额难以确定或者未达法定最低数额的，可以直接请求侵权人赔偿法定最低数额。至于法定数额是否设定为 500 元，尚值得进一步讨论。有观点认为，设定适当的百分比代替具体的数字作为最低赔偿标准，可以更加贴合当前经济发展变化情况。但是考虑到以比例代替数字会给法官增加调查当地居民收入状况的负担，以及存在无法与“50 万元”上限相呼应的问题，所以建议使用“三倍赔偿以及最低赔偿额兜底”的赔偿模式，同时提高最低赔偿额金额。例如，将一般信息的最低赔偿标准设定为 500 元或者 1000 元，敏感信息设定为 1000 元或者 2000 元^[33]。由此在调动信息主体维权积极性的同时，也让信息处理者更加谨慎地处理收集的信息，从而解决因为赔偿数额过低导致个人信息保护悬空的窘境。

五、结 语

对信息主体的风险性损害救济，应该保持在传统损害可确定的归责模式下进行，将风险性损害的可赔偿范围定义为合理预防费用的支出以及隐私信息泄露导致的机会利益的损失等。在传统损害差额

计算标准的基础上，本文创新地引入许可使用费标准以化解机会利益损失难以计算的难题，主张设置法定最低赔偿额制度以保障信息主体维权积极性，最终可实现个人信息保护良性循环的目标。本文虽然为构建适用于数字时代个人信息损害量化体系提供了理论雏形与法理基础，但无法忽视的是，人工智能技术迅猛迭代，尤其是算法推测能力的跃升，正在深刻重塑个人信息处理的格局。生成式人工智能在模型训练阶段所使用的数据会涵盖各种类型的个人信息，算法推测技术也会使不同类型的个人信息无法完全分割。随之而来的新型、聚合性系统自主性歧视风险损害形态，不但涉及算法自主侵权如何归责的问题，而且在整个环节中信息处理者之间的法律关系复杂多样，亦无法轻言责任分配。这对传统以损害确定为核心要件的归责模式提出了前所未有的严峻挑战。未来应聚焦于回应生成式人工智能带来的新型个人信息风险性损害，着力深化对算法风险本质的法理认知，强化预防性救济措施的核心作用，以期实现在人工智能时代有效平衡个人信息权益保护与技术创新发展的双重目标。

参考文献：

[1] 莫杨桑. 个人信息权益侵权法保护的动态体系论[J]. 人权, 2024 (1): 119-144.

[2] 张红. 生命数字化进程中的文化转向与制度因应: 以数字自我的法律保护为中心[J]. 求索, 2025(3): 158-168.

[3] 王雪. 个人信息泄露的风险性损害之证成[J]. 南大法学, 2023 (3): 172-192.

[4] 田野. 风险作为损害: 大数据时代侵权“损害”概念的革新[J]. 政治与法律, 2021(10): 25-39.

[5] 王益强. 裁判视角下数据侵权损害的认定[J]. 华东政法大学学报, 2023, 26(5): 70-84.

[6] 程海玲. 个人信息侵权风险性损害的证成与认定[J]. 重庆大学学报(社会科学版), 2023, 29(5): 198-211.

[7] 吕炳斌. 个人信息处理的合法性对数据财产权的影响[J]. 国家检察官学院学报, 2025, 33(3): 58-72.

[8] 张新宝. 侵权责任法[M]. 5 版. 北京: 中国人民大学出版社, 2020: 27.

[9] 王雪. 个人信息双重风险性损害判定与赔偿框架的重塑[J]. 人权, 2024(5): 136-158.

[10] 叶雄彪. 个人信息侵权的理论反思与规范构建[J]. 齐鲁学刊,

① 敏感个人信息一旦泄露或者非法使用，容易导致自然人的 人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

② 个人敏感信息包括财产信息、健康生理信息、生物识别信息、身份信息和其他信息。

2023(6):88-101.

[11] 潘雨祥. 论个人信息处理义务的分配正义:以信息处理必要性的分层调整为展开[J]. 甘肃政法大学学报, 2025(3):83-97.

[12] 朱晓峰, 夏爽. 论个人信息侵权中的损害[J]. 财经法学, 2022(4):51-66.

[13] 项焱, 张雅雯. 大数据时代个人信息无形损害的正当性基础与认定规则[J]. 江苏行政学院学报, 2022(5):127-136.

[14] 杨垠红. 大数据使用情境下个人信息的侵权救济[J]. 福建师范大学学报(哲学社会科学版), 2022(6):144-155.

[15] 曹京徽. 论大规模侵权案件中潜在受害人的救济[J]. 江西社会科学, 2020, 40(1):200-211.

[16] 尹志强, 冯超. 违反医疗告知同意损害归责的反思与建构[J]. 内蒙古社会科学, 2025, 46(3):139-148.

[17] 谢鸿飞. 个人信息泄露侵权责任构成中的“损害”:兼论风险社会中损害的观念化[J]. 国家检察官学院学报, 2021, 29(5):21-37.

[18] 庄华, 马忠红. 电信网络诈骗犯罪预警的失灵与优化[J]. 情报杂志, 2025, 44(2):116-123.

[19] 彭诚信, 许素敏. 个人信息权益侵权损害赔偿应然范围探讨:基于数字社会的场景[J]. 社会科学, 2023(7):166-177.

[20] 王利明. 违约救济原则新探[J]. 东岳论丛, 2025, 46(6):43-57.

[21] 崔建远. 论机会利益的损害赔偿[J]. 法学家, 2023(1):27-41.

[22] 彭诚信. 重解个人信息的本质特征:算法识别性[J]. 上海师范大学学报(哲学社会科学版), 2023, 52(3):68-81.

[23] 程啸. 论人格权的商业化利用[J]. 中国法律评论, 2023(1):42-56.

[24] 冯源. 数字法治时代弱势群体最大利益的实践进路[J]. 学习与探索, 2025(5):59-68.

[25] 焦艳玲. 人脸识别的侵权责任认定[J]. 中国高校社会科学, 2022(2):117-128.

[26] 谢妮轩. 个人信息泄露侵权的归责路径与诉讼证明[J]. 甘肃政法大学学报, 2024(5):26-41.

[27] 谢迪扬. 侵权抑或不当地得利:个人信息泄露的民事救济路径之辨[J]. 北京理工大学学报(社会科学版), 2024, 26(2):136-149.

[28] 赵贝贝. 个人信息诉讼保护的程序展开:从实体与程序的规范联动切入[J]. 安徽大学学报(哲社版), 2024, 48(5):89-97.

[29] 赵贝贝. 个人信息私法救济中的“损害赔偿”困境与应对路径[J]. 财经法学, 2022(5):95-106.

[30] 时诚. 个人信息泄露风险损害的赔偿责任[J]. 现代法学, 2024, 46(2):136-150.

[31] 孙鹏, 杨在会. 个人信息侵权惩罚性赔偿制度之构建[J]. 北方法学, 2022, 16(5):91-107.

[32] 夏庆锋. 个人信息分类处理规则的解释适用:基于损害风险的视角[J]. 法学评论, 2025, 43(4):96-107.

[33] 杨立新. 私法保护个人信息存在的问题及对策[J]. 社会科学战线, 2021(1):193-202.

(责任编辑:何淑燕)