浙江理工大学学报,第56卷,第5期,2026年10月
Journal of Zhejiang Sci-Tech University
DOI:10.3969/j.issn.1673-3851(s).2026.05.013

个人信息泄露侵权的风险性损害认定

郭　兵,林佳慧
(浙江理工大学数据法治研究院,杭州 310018)

摘　要:与传统侵权损害不同,个人信息泄露引发的侵权损害通常不体现为即时的现实损失,更多表现为相关权益遭受侵害的风险提升。此类风险性损害具有无形性、潜在性的特征,已然超出传统损害理论的规制范畴。对此,应引入风险性损害理论,搭建适配的损害认定标准。侵权法面向风险社会的发展转型,以及风险客体本身的固有属性,共同为风险性损害的合法化确认提供了理论支撑。在具体适用中,风险性损害的认定需立足于"实质性风险"的考量框架,通过对多元要素的动态评估来实现对受害者的有效救济。此认定路径可有效化解个人信息泄露侵权后受害人遭受次生损害的风险,加强数字社会下的个人信息保护。

关键词:个人信息泄露;侵权损害;风险性损害;实质性风险
中图分类号:D923.8　　**文献标志码**:A　　**文章编号**:1673-3851 (2026) 10-0652-09

Determination of risky damage in cases of personal information leakage

GUO Bing, *LIN Jiahui*
(Institute of Data Law, Zhejiang Sci-Tech University, Hangzhou 310018, China)

Abstract: Compared with the traditional tort damages, the direct damage caused by personal information leakage does not have direct reality, but is manifested as an increased risk of being infringed. Such risky damages are intangible and potential, and are difficult to be fully encompassed by traditional damage theories. Therefore, it is necessary to introduce the theory of risky damage and establish corresponding standards for damage identification based on it. The necessity of the transformation of tort law under a risk society and the essential attributes of risk provide a theoretical basis for the legal recognition of risky damage. In specific application, the identification of risky damage should be based on the framework of "substantial risk" and a dynamic evaluation system with multiple factors should be established to achieve effective relief for victims. This identification path can effectively mitigate the risk of secondary harm suffered by victims after personal information leakage torts, thereby strengthening the protection of personal information in the digital society.

Key words: personal information leakage; infringement damage; risky damage; substantial risk

随着数字经济的快速发展,个人信息的利用价值愈发凸显,信息泄露及侵权风险也随之加剧。个人信息泄露侵权所致损害往往具有不确定性和风险导向性,难以契合传统侵权损害理论的核心要件,导致受害人的权利救济陷入制度性困境。为此,域外学者针对个人信息泄露中风险、焦虑能否作为法定损害展开论证,试图以此调和个人信息泄露所衍生的新型损害样态与传统损害理论之间的内在矛盾[1]。受域外研究的启发,时诚[2]、王雪[3]等国内学者也围绕风险性损害在我国侵权法体系下的适用可

收稿日期:2026-03-02　　网络出版日期:2026-07-02
基金项目:国家社会科学基金一般项目(25BFX152)
作者简介:郭　兵(1986—　),男,湖北大悟人,副教授,博士,主要从事数据法学方面的研究。

行性展开研究。然而,在司法实践中,我国法官对个人信息泄露侵权的损害认定大多持谨慎态度,较少突破传统侵权损害认定框架。当前,学界与实务界针对风险性损害的法律正当性仍然存在争议,但部分司法案例认可其损害属性。基于此,结合司法实践系统梳理并剖析风险性损害的认定标准,对完善案件裁判逻辑、化解司法适用困境具有重要现实意义。

一、传统损害理论在个人信息泄露侵权中的适用困境

通过案例检索与梳理可以发现,我国绝大部分法院对于个人信息泄露侵权纠纷中原告的损害赔偿请求不予支持。其理由主要包括“未造成严重精神损害”①、“未证明存在财产损害”②、“财产损害与泄露行为不存在因果关系”③等。我国损害赔偿法并未对“损害”作出明确定义,《中华人民共和国民法典》(以下简称《民法典》)同时吸纳了差额说、客观说与规范说所界定的损害内涵[4]。个人信息泄露侵权引发的损害难以认定,一定程度上源于其所致的风险性损害与上述损害学说并不契合,因此难以被纳入传统侵权损害认定框架予以评价。

(一)差额说的适用障碍

在损害赔偿法的发展历程中,差额说一直处于核心地位。差额说由德国学者弗里德里希·莫姆森提出,认为损害即“被害人因该特定损害事故所损害之利益”,此利益具体表现为“受害人之总财产状况,于有损害事故之发生与无损害事故下所生之差额”[5]119。差额说将损害视作财产数额的差值。当受害人所遭受的损害无法体现为既有财产减损时,差额说便认为受害人不存在损害,由此导致在某些特定情形下,受害人权益实际受损却无法主张损害赔偿[6]。而且,这一弊端在个人信息泄露侵权中体现得更为明显。

个人信息泄露后,受害人所遭受的直接损害包括三种类型:一是个人信息泄露导致受害人基于个人信息所具有的财产利益受到损害;二是个人信息泄露给自身带来的风险;三是因个人信息泄露衍生的其他损害,既包括电信诈骗等下游侵权引发的财产损失,以及为预防上述侵权行为发生而产生的财产支出,也包括因担心受侵害风险的增加而产生的内心焦虑、痛苦等精神损害[7]。

就第一种类型的损害而言,学界及司法实务界虽然普遍认可个人信息内含财产利益,但该类财产利益的价值实现,多集中于企业对个人信息开展的规模化处理活动中。由此便引发新的问题:当单一主体的个人信息遭到泄露时,其本人是否遭受财产损失?若答案为肯定,该类损害即可被差额说所涵摄,权利人亦能够依据《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 69 条作为请求权基础,向司法机关寻求救济。但个人信息权益与肖像权、姓名权等传统人格权益存在本质区别:后者可通过授权许可的方式为权利人创造经济收益,而个人信息权益难以依托此种模式产生相应的经济价值。即便个人信息形成了自身的交易市场,由于个人信息具有非竞争性,其泄露并不影响个人将同一个人信息以同一价格进行多次交易。因此,在个人信息被泄露的情形下,难以确切证实在泄露侵权事件发生前后,个人的总财产数额出现了某种消极的变动态势。

就第二种和第三种类型的损害而言,其核心争议要点为风险性损害,诸如因个人信息泄露所导致的侵权风险提升,为防范侵权结果发生而额外支出的财产,以及因担心未来损害风险增加而产生的内心焦虑等损害,能否被纳入侵权法所界定的可获得法律救济的损害形态范畴之内。传统侵权法体系以“损害填补”为根本功能,作为传统损害理论的主流学说,差额说同样要求损害具有不利益性、客观确定性以及可补救性[8]。因此,受害人欲主张损害赔偿一般以其遭受了“实际损失”或“客观的损害”为条件。然而,在个人信息泄露侵权中,受害人不知是否会发生以及会发生何种损害,此种风险性损害作为一种未来损害,具有无形性与潜在性的显著特点[9]。这种内在特性上的差异,使得风险性损害与“实际损失”概念之间存在天然的张力。

(二)客观说的适用障碍

在差额说理论框架下,损害被界定为受害人受损前后的财产差额,表现为具体数值,因此具体损害形态在损害概念中并无独立意义[5]120。这一特征使得差额说在处理假设因果关系(亦称为修补因果关系)问题时常难以适用[10]。所谓假设因果关系,即致使损害发生的原因行为有二,其中先行的 A 原因行为已然引发损害后果,导致后续 B 原因行为与损

① 如(2025)辽 0902 民初 3877 号、(2025)津 0104 民初 14148 号判决书。

② 如(2025)晋 0525 民初 1976 号、(2023)辽 1402 民初 415 号、(2021)湘 0182 民初 10895 号判决书。

③ 如(2024)粤 2072 民初 13599 号、(2022)浙 0192 民初 4259 号判决书。

害结果之间未能发生事实上的因果关系[5]193。依据差额说裁判假设因果关系案件,即便不存在A原因行为,该特定损害事实仍由B原因行为引发,受害人并未产生财产差额,A原因行为人便无需承担损害赔偿责任,这一结论显然有违公平正义理念①。

针对上述差额说的适用困境,客观说对其进行了修正。客观说在认可差额赔偿模式的基础上,将特定物毁损所产生的损害视为独立的损害类型,并以该标的物的客观价值划定最低赔偿额[5]126-128。然而,该学说在应对个人信息泄露侵权案件时,同样面临与差额说相似的难题,即单纯的个人信息自决权受损能否直接认定为损害。个人信息的市场价值难以确定,且个人信息权益作为人格权的一种,具有极强的人身专属性,同一信息对不同主体所承载的价值存在显著差异。此外,在个人信息泄露侵权场景中,因信息泄露而遭受诈骗、身份盗用等次生侵害风险的攀升对受害人而言更具有威胁性,而客观说同样无法对该类风险的价值予以有效界定。

(三)规范说的适用障碍

规范说就差额说下价值中立的损害概念作出了修正,主张损害作为法律上的概念,当然具有规范性[11],因此当损害无法以财产差额呈现时,可通过强调损害认定中的规范因素、价值因素来额外确定损害范围[12]。据此而言,似乎能从我国立法的规范目的出发将个人信息泄露侵权所造成的直接损害纳入法律的损害范畴。例如,我国有的法院根据《民法典》第1034条第3款的规范目的,区分了侵害私密信息与非私密信息的损害评价标准[2],主张私密信息"一经泄露即易导致个人人格利益受到损害",非私密信息"仅在被过度处理的情形下才可能使信息主体受到人格或财产损害"②。然而,在司法实践中,私密信息与非私密信息的界限并不清晰,许多非私密信息都可向私密信息转化,因此以信息私密度确定规范目的的做法过于草率。隐私法(个人信息保护法)欲有效发挥作用,必须关注危害和风险,而不是个人信息的性质。[13]

综上所述,传统损害理论之所以无法在个人信息泄露的损害认定与救济中发挥作用,根源在于其与"明确损害"之间存在矛盾,这一矛盾集中体现为个人信息权益经济价值的不确定性、损害发生的不确定性与规范目的的不确定性。因此,为化解传统损害理论对于个人信息泄露侵权案件的适用不兼容问题,应当认可个人信息泄露侵权中尚未现实化但具有较大危害性的风险性损害。但新型损害的引入不可脱离现行法律体系凭空创设,亟须对其引入的可行性与适用价值展开分析。

二、风险性损害理论适用于个人信息泄露侵权的可行性

既然传统损害理论难以应对个人信息泄露侵权引发的具有高度不确定的损害形态,那么有必要引入新型损害理论以摆脱当前司法适用困境,进而保障个人的信息权益。风险性损害理论并非缺乏制度基础。从理论与实践双重维度出发,可依托侵权法转型的现实必要性、损害本质的同一性以及司法实践经验,探寻该理论的适用空间。

(一)风险作为损害的理论依据

1. 侵权法于风险社会下转型的必要性

风险是否会演变为实际损害,并非数字时代的全新议题。德国社会学家贝克[14]早在工业社会阶段便提出"风险社会"理论,其著作指出,该理论的核心是风险的界定、分配与治理。进入风险社会后,侵权法的适用环境彻底改变,损害呈现出不确定性、无限性、不可预见性等新特征,也使侵权法难以应对频发的大规模损害[15]。为此,侵权法针对风险损害作出相应调整,医疗、环境、毒物侵权是风险损害规则应用最具代表性的三大领域[16]。

个人信息权益被侵害产生的风险性损害,与前述三类侵权所致损害特征高度相近。以环境损害为例,二者存在三点共性:受害主体的非特定性、损害后果的不可完全预见性以及损害修复的不易性[17]。这类潜在风险一旦转化为实际损害,往往会造成大额财产损失与严重精神损害,待到损害发生后再诉诸司法救济,往往会因侵权要件证明不充分而难以获得救济。例如,就目前大多数因个人信息泄露而提起诉讼的民事案件而言,"因果关系"的证明成为受害人获得救济难以跨越的门槛。若仅允许在风险落地、实际财产损失出现后主张损害赔偿,受害人不仅要举证因时间推移变得愈发复杂的因果链条,还需在层级繁杂、数据匿名流通的数字生态中追溯泄

① 举例而言,甲家的玻璃因为乙的故意损害而毁损,当夜即发生地震,甲家的玻璃全数震碎。在上述案件中,导致损害结果的原因行为分别为乙的侵权行为与地震,地震即为假设因果关系,因为地震与甲家的某一特定窗户(乙致损那一扇)破裂之间未能发生事实上的因果关系。

② 参见(2019)京0491民初16142号判决书。需要指出的是,北京互联网法院于2020年7月作出判决时,援引了当时即将实施的《民法典》第1034条第3款。

露源头,举证负担极为沉重。

事实上,个人信息保护立法的风险导向已是国际主流趋势。我国《个人信息保护法》亦体现出对风险本位方法的吸纳,该法第 11 条明确确立风险预防原则[18]。因此,为健全风险导向的个人信息保护制度,应将“基于风险的方法”融入传统的侵权损害分析体系,将权利行使节点向前推移,即当风险损害具有实质发生可能性时,即可准许权利人提起诉讼寻求司法救济。

此外,个人信息损害的微量集聚特征,还关乎社会公共利益层面的制度考量。如前文所述,信息泄露的受害对象具有不特定性。2025 年 5 月,据《上海证券报》等媒体报道,奢侈品牌迪奥被曝发生数据泄露,涉中国客户姓名、地址、电话号码等信息①。用户基础信息外泄,极易滋生电信诈骗、身份冒用等违法犯罪,让众多不特定群体陷入安全风险,进而损害社会公共利益。

综上,面对个人信息泄露催生的新型侵权形态,若继续沿用传统侵权规则,将难以适配当下的权益保护需求。对此,侵权法亟须转型,强化责任分配、风险合理预防、促进群体福利等治理功能[19],将个人信息泄露侵权中被害人所遭受的侵害风险上升为损害,这正是上述治理思路的落地。

2. 风险与损害在本质上的同一性

风险性损害并非与传统损害理论完全脱节。差额说精准揭示损害的本质为不利益,也契合损害赔偿的填补功能,长期处于德国法理主流地位[20]。但该学说在部分案件中的适用有违公平正义理念,为弥补其适用缺陷[5]120-124,规范说便应运而生。二者结合形成自然损害与规范损害的二元概念,我国民法亦采纳这一框架。学界通说认为,损害是加害行为造成的人身、财产不利后果,需客观存在且具有确定性,并可依差额说予以量化[21]。同时,寻求司法救济的损害还须符合法定构成要件。简言之,法律并非对所有不利后果都予以保护,裁判过程还应包含规范价值的考量。

具体到个人信息泄露后受害人所遭受的风险性损害,其本质亦为“法律上的不利益”,表现为受害人某种权利圆满状态的减损。当个人信息泄露后,被害人所面临的欺诈等侵权风险增加,承受了本不应发生的安全利益减损,系不利益的体现;为规避次生损害而支出的防范成本,是现实的财产损失;风险带来的焦虑与精神困扰,则构成精神层面的不利益。即便潜在损害尚未实际发生,风险本身已然是一种客观不利益,只是其内涵带有概率属性[8]。由此可见,风险性损害所对应的不利益亦是客观存在的,其与传统损害在本质上具有同一性,这也为侵权法对其予以救济奠定了法理基础。

(二)风险作为损害的实践基础

关于个人信息泄露侵权所发生的风险性损害法律是否应当认可的问题,国内外法院作出了一定的探索。

欧盟对于个人信息向来秉持着严格保护的原则,然而在个人信息泄露侵权所导致的风险性损害上,其早期态度较为谨慎。例如,在 BL v. Media Markt Saturn Hagen-Iserlohn GmbH 案②中,欧盟法院明确,通过《通用数据保护条例》第 82 条第 1 款寻求赔偿,须证明损害实际发生;仅以“数据未来可能被传播甚至滥用”为由,无法获得救济。但是,2025 年初的 Bindl v. Commission 案③呈现明显转向。法院认定,原告因个人数据被非法转移至美国,对自身数据处理状态陷入不确定性,此种状态构成非物质损害,判令被告赔偿。该案表明,单纯的个人信息自决权受损,已可被认可为非物质损害。

美国法院早期对个人信息泄露引发的风险性损害持保守否定态度,针对原告基于“未来受损风险”以及“采取预防措施以降低受损风险”提出的索赔请求,法院多以损害仅属推测、不具有现实性为由,认定原告缺乏诉讼资格,进而驳回其起诉[22]。对此,学界提出批判,认为司法层面将损害局限于直观、可感知、可量化的有形后果,认定标准过于狭隘,极大限制了个人信息泄露纠纷的司法救济空间[1]。个人信息泄露造成的损害虽然多为无形权益受损,但不可据此否认其损害实质;相反,此类损害具有现实性,应当纳入可赔偿范围。美国持续推进个人信息保护立法、完善规制体系的立法实践,也印证了此类

---

① 参见:蒋烨欢.奢侈品巨头,客户信息遭泄露!网址:https://www.cnstock.com/commonDetail/439476。

② 该案的案情为:被告由于疏忽,将包含录入自动数据处理系统数据的纸质文件交给未经授权的第三方,该纸质文件中包含原告的个人信息,由此原告认为被告的行为违反了《通用数据保护条例》,并请求赔偿。BL v. Media Markt Saturn Hagen-Iserlohn GmbH, https://curia.europa.eu/juris/document/document.jsf?text=&docid=282062&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=2684616。

③ 该案的基本案情为原告发现被告涉嫌个人数据(IP 地址)非法跨境传输,由此诉至法院请求损害赔偿。Bindl v. Commission, https://curia.europa.eu/juris/document/document.jsf?text=&docid=294090&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=2684616。

风险损害的客观存在性与权益危害严重性[1]。伴随司法实践发展,美国部分地区法院逐渐意识到全盘否定风险性损害赔偿的弊端,裁判立场发生适度转向。例如,在 In re US Office of Personnel Management Data Security Breach Litigation 案①中,华盛顿特区巡回法庭明确认可原告成立事实上的损害:案涉泄露信息包含社会安全号码等难以变更的核心身份数据,致使原告长期面临极高的身份冒用与侵权风险,该持续存在的高度风险本身即构成可救济的损害②。

我国司法实践中,认可个人信息泄露风险性损害的案件较少,但已有明确司法先例与规范依据予以支撑。在欧某与某公司等个人信息保护纠纷案③中,法院直接肯定风险可构成损害,表示"案涉个人信息确已被泄露,存在为不特定第三人获取的风险,该风险本身即可评价为上诉人欧某个人信息权益的损害"。此外,对于"采取预防措施以降低受损风险"所提出的索赔,我国亦有法律明文规定。2021年最高人民法院出台的《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》第8条第2款规定,自然人为制止侵权行为支出的合理开支,可认定为《民法典》第1182条规定的财产损失。根据最高人民法院对该条的解读,该条款的设立是鉴于人脸信息侵权通常无具体财产损失,且受害人维权成本较高,若不予赔偿会导致"维权成本高、侵权成本低"的权益失衡,因此适当扩张了财产损失的范围[23]。这一规范路径,为个人信息泄露场景中预防损害支出的费用成为现实财产损害提供了法律依据[24]。

综上所述,个人信息泄露引发的风险性损害,已在域内外司法实践中获得有限认可。但通过梳理域内外典型裁判案例可见,当前司法实践面临的核心困境在于:尚未针对不同性质、不同程度的风险性损害,构建起体系化、普适性的可救济性认定规则与裁判标准。因此,为充分发挥风险性损害理论的权利救济与侵权规制效用,需要进一步为其司法适用搭建清晰的、可操作性的框架。

三、个人信息泄露侵权中风险性损害的具体认定

风险性损害理论既顺应风险社会下侵权法的转型需求,其本质也体现了损害系"不利益"的核心属性,这是其成为法定损害类型的理论根基。同时,梳理国内外司法实践可见,风险性损害并非脱离实践的抽象概念,在个人信息等诸多领域已得到一定认可,进一步夯实了其入法的现实基础。但若要将该理论落地于司法实践、破解个人信息泄露侵权案件中损害认定的难题,关键在于构建并明晰风险性损害的司法判定标准体系。

(一)风险性损害的动态评估体系

虽然风险性损害具有一定的理论与实践基础,但法律需兼顾权益保护与行为自由,并非对所有损害都予以救济。当前个人信息安全问题频发,若要求个人信息处理者为全部风险承担赔偿责任,其大概率会因成本收益考量缩减相关业务,阻碍个人信息要素的市场化流转,这也与《个人信息保护法》"保护与利用并重"的立法初衷相悖。因此,有必要进一步明确风险性损害的法律救济适用边界。

对此,有学者④提出可采取"实质性风险"标准[25]。该标准已在美国部分案件中适用,其基本要义为:若个人信息泄露引发的风险高度具有现实化可能,或是信息遭非法利用后极易造成重大人身、财产损害,即可认定风险性损害存在[2]。但该标准仍然具有一定抽象性。为了在司法实践中精准判断风险发生概率与损害严重程度,可结合维尔伯格提出的动态系统论进行裁判[26]。该理论注重各要件要素的动态协同作用,落实到司法实践中,要求法官梳理个案相关考量因素、综合权衡各要素权重,由此得出更符合法律价值的裁判结果[27]。

前文已述,风险性损害在环境侵权领域已获得部分认可,相关规则也在实践中逐步完善,因此可借鉴该领域的认定经验,构建个人信息侵权场景下的风险性损害认定体系。环境侵权中认定"重大风险"的动态考量要素分为四项:其一,行为是否合规、有无违反法律法规禁止性规定(行为的违法性);其二,被保护对象的特殊性;其三,损害结果发生的可能性;其四,损害后果的严重性[28]。这套判断逻辑同

① 该案的基本案情为:黑客侵入了美国人事管理局(OPM)的多个数据库,据称盗窃了个人信息,影响超过1200万人。原告因此提起诉讼,声称OPM违反了保密的约定和宪法关于隐私权的规定,要求OPM予以金钱赔偿并向受影响的雇员提供终身免费的身份信息保护服务。详见 Lea Schild, Ensuring Employee Protection after a Data Breach, 28 Geo. Mason L. Rev. 1553 (2021),1575。

② 除此之外,还有部分巡回法庭认为个人信息泄露者遭受重大损害,有权提起诉讼。如 Galaria v. Nationwide Mut. Ins., 663 F. App'x 384 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., 794 F. 3d 688(7th Cir. 2015); Krottner v. Starbucks Corp., 628 F. 3d 1139 (9th Cir. 2010); In re Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154 (D. Minn. 2014)。

③ (2024)沪01民终410号判决书。

④ 持此观点的学者包括时诚、张建文、赵梓羽、程海玲等。

样适用于个人信息侵权领域。同时,我国《民法典》人格权编已吸纳动态系统论,其中第 998 条[①]便是典型代表之一[29]。个人信息权益属于人格权益范畴,该条款所列考量因素亦可参照适用。据此,判定风险性损害是否构成实质性风险,可归纳为五大考量要素。

第一,行为的违法性。法律具有规范与指引作用,违法行为必然扰乱社会秩序。《个人信息保护法》专章规定了“个人信息处理规则”与“个人信息处理者的义务”,若个人信息处理者违反前述法定义务,其行为兼具过错与风险,理应受到法律惩戒。

第二,被保护对象的特殊性。《个人信息保护法》确定了个人信息分级保护制度,将个人信息依据信息敏感度划分为敏感个人信息与一般个人信息,并对敏感个人信息设定特殊保护规则。“敏感信息泄露本身即意味着损害的发生。”[30]一般而言,由于敏感个人信息指向明确,难以更改,一旦泄露,产生风险性损害的紧迫程度更高。

第三,损害结果发生的可能性。此处风险并非宽泛的抽象风险,而是指具有现实紧迫性的客观发生概率。依据实质性风险标准,只有案涉风险具有实质化的高度可能性、对受害人合法权益构成紧迫威胁时,对风险性损害予以救济才具有现实必要性与法律正当性。

第四,损害后果的严重性。侵权法始终秉持轻微损害不予救济的原则。该原则不仅能遏制滥诉、节约司法资源,也能合理划分责任范围。同时,侵权法亦具有惩戒功能,若动辄对微小损害提供救济,在权益保护与行为自由之间显然有失平衡。因此,对于风险性损害更要持审慎的态度,避免对行为人苛以过重的责任负担。

第五,行为目的。行为目的直接影响风险判断。若行为人主观上基于非法目的获取、泄露他人个人信息,即便损害尚未实际发生,也可认定风险极易转化为现实损害;反之,若行为人主观善意、并无过错,则可相应调低风险实质化的可能性。

动态系统论除关注要素的构造外,另一重要内容是对各要素权重进行合理排序与动态协调。在上述五要素中,“损害结果发生的可能性”应作为核心要素,是风险性损害动态评估体系的基石。该要素与“实质性风险”标准所主张的“高度可能性”存在一致性,其他要素都是围绕这一核心要素展开,或为其提供辅助论证,或以该要素的成立为前提的,共同服务于风险现实化程度的精准研判。而“损害后果的严重性”则应作为次要要素。其一方面可以作为衡量风险是否具有实质化可能性的指标之一,另一方面在功能上又具有一定的独立性,关系到该损害是否应予以救济、如何救济的问题。至于其他要素,则作为补充要素发挥作用,为核心要素与次要要素的论证提供论据、补强逻辑链条。通过此权重分配,厘清各要素之间的相互关系,构建起开放但相对周延的动态评价体系。

(二)财产损害的具体认定

在财产损害的具体认定中,各要素之间主要表现为补足与背离关系。如何统筹各要素的基础判断、形成最终法律结论,是风险损害动态评估体系必须厘清的问题。结合司法适用场景,各要素形成的基础评价大致可分为以下几类情形。

第一,若各要素均得出相同的基础评价,则根据基础评价的方向判断风险性损害是否符合“实质性风险”标准。例如,在欧某与某公司等个人信息保护纠纷案[②]中,原告欧某作为投保人在被告 1 某保险公司投保后,发现在某搜索引擎中输入自己手机号即可从被告 2 某信息公司运营的网站下载详细保单信息,保单上记载着其姓名、联系方式、身份证号码、职业等信息。法院审理认为,原告欧某的案涉信息可以通过某搜索引擎等公开渠道被不特定对象检索获得,且案涉被泄露信息中包含敏感个人信息,欧某因此产生内心焦虑,符合一般社会观念。根据上述审理意见,从“损害结果发生的可能性”“损害后果的严重性”“被保护对象的特殊性”三要素出发,均可得出“具有实质性风险可能、应认定为风险性损害”的基础评价,故法院应作出“风险性损害成立”的司法认定。

第二,若部分要素之间存在矛盾的基础评价且权重不同,应当遵循权重优先原则,以高阶要素的评价结论为核心依据,判定案涉风险是否符合“实质性风险”标准,进而认定是否成立风险性损害。例如,在江西省宜春市人民检察院督促保护医疗健康个人信息行政公益诉讼案[③]中,群众举报称,在其家属办理完住院后,即有保险代理机构业务人员向其推销“手术意外险”。后江西省宜春市人民检察院查明,部分保险代理机构为精准销售保险,通过合作医院

---

① 该条对除生命权、身体权和健康权外的人格权侵权责任认定的衡量因素予以规定。

② (2024)沪 01 民终 410 号判决书。

③ 详见最高检发布的个人信息保护检察公益诉讼典型案例之四。网址:https://www.spp.gov.cn/xwfbh/dxal/202303/t20230330_609820.shtml。

违法获取大量患者的姓名、手术类型、联系电话等医疗健康信息。通过分析案件事实可知,该案件从“行为的违法性”与“被保护对象的特殊性”要素出发,可初步认定“具有实质性风险可能、应认定为风险性损害”;然而,该案件中个人信息泄露后的去向具有唯一性,即只为保险代理机构所获取并用保险销售,故从“损害结果发生的可能性”“行为目的”出发,可得出“不具有实质性风险可能、不应认定为风险性损害”的基础评价。依据前述权重分配规则,“损害结果发生的可能性”作为核心要素的权重更高,其在认定法律评价中具有决定性作用。因此,当发生类似案件原告起诉索赔时,法院不应认定风险性损害成立。但需特别指出的是,风险性损害不成立并不意味相关行为具有合法性。

第三,部分要素之间存在矛盾基础评价且权重相同。因核心要素与次要要素均仅为一个,权重相同的要素对立情形仅存在于各项补充要素之间。需要说明的是,笔者所列要素仅为司法实践中的典型考量因素,并非封闭性清单,凡是可证明损害发生可能性的相关要素,均可纳入动态评价体系之中。当各项补充要素出现评价相悖的情况时,可通过比对肯定性评价与否定性评价的数量得出结论:若肯定性评价占多数,则可认定风险性损害成立,反之则应予以否定;若二者评价数量相当,说明案涉风险的实质化程度尚未达到“实质性风险”标准所要求的“高度可能性”,无法满足风险救济的核心要件,故应作出风险性损害不成立的法律评价。

(三)精神损害的具体认定

在精神损害的具体认定中,“损害后果的严重性”系特殊考量因素。这是由于我国《民法典》第1183条已明确将后果严重列为精神损害赔偿的法定条件。因此,受害人因侵害风险增加而产生的焦虑、痛苦等情绪,是否满足我国精神损害的“严重性”要件、能否获得精神损害救济,仍存有争议。

现行法律并未界定精神损害“严重”的具体判定标准,司法实践中更多依赖于法官的个案判断。单纯侵害个人信息权益引发的精神损害通常程度较轻,大多表现为受害人心理上的焦虑不安[31]。该类情绪一般难以达到法定的“严重性”要件,因此受害人的赔偿诉讼请求常被法院驳回。例如,在凌某某与北京微播视界科技有限公司隐私权、个人信息权益网络侵权责任纠纷案①中,法院虽认可被告构成侵权且给原告造成困扰,但因原告未提供证据证明造成严重后果,最终对原告提出的精神损害赔偿请求不予支持。针对此类现象,有学者建议建立个人信息损害动态评价体系,对信息主体的精神状态进行综合判断,并结合具体场景适度放宽精神损害“严重性”的标准[32]。

此种观点与部分法院的裁判立场不谋而合。例如,在薛祥飞、浙江淘宝网络有限公司隐私权纠纷案②中,法院指出,“单纯的因侵害个人信息权益给自然人造成的精神损害,需要考虑受侵害个人信息类型、风险发生的盖然性、风险可能导致的危害及其影响范围等综合因素酌情认定是否予以赔偿;既不宜一概予以排除,设置过于严苛的‘严重性’精神损失的认定标准,也不宜全盘接受,过分降低构成精神损害的认定标准。”司法实践中,已有法院对受害人因个人信息泄露侵权引发的焦虑情绪而提出的精神损害赔偿予以支持③。

从域外立法观之,旧《德国联邦数据保护法》第8条第2款曾设“严重侵害人格权”作为索赔前提;而新法第83条第2款已接轨欧盟《通用数据保护条例》第82条,删除该要件,大幅降低信息主体精神损害索赔门槛。与此类似,我国台湾地区《个人资料保护法》第28条第3款规定,被害人若难以证明财产或非财产损害额,可请求法院依侵害情节,按每人每事件新台币500元至2万元估定,且未规定精神损害“严重性”要件[33]。由此可见,放宽个人信息侵权领域精神损害赔偿的“严重性”认定标准已有先例可循。

笔者也赞同在个人信息保护领域应对精神损害赔偿“严重性”要件予以缓和的观点,同时,为避免过度加重个人信息处理者的责任、防范司法诉讼泛滥,本文提出分层适用的认定路径:以“合理期待标准”作为精神损害赔偿责任成立的标准[34],以“严重性”要件作为裁量赔偿数额大小的依据[35]。所谓“合理期待标准”,是指结合社会一般公众认知与受害人主观感受进行综合判断,若特定个人信息泄露行为足以使人产生精神负面困扰,即可认定精神损害事实成立。具体判定规则如下:若社会一般人认为信息泄露会产生精神负面影响,但受害人未产生相应负

① (2019)京0491民初6694号判决书。类似判决还可见(2025)辽0902民初3877号、(2025)晋0525民初1976号、(2023)辽1402民初415号、(2022)辽0283民初6961号、(2022)粤1302民初19271号判决书。

② (2022)浙0192民初4259号判决书。

③ 如(2024)苏0113民初427号、(2024)鲁0283民初17201号判决书。

面感受的,不成立精神损害;若受害人主张遭受精神损害,但该损害未被社会一般人认知与认可的,亦不成立精神损害;唯有社会一般人的客观认知与受害人均认为案涉个人信息泄露会造成精神负面影响时,才认定精神损害成立。

在精神损害赔偿数额的裁量层面,可结合相关补充要素,并依据《最高人民法院关于确定民事侵权精神损害赔偿责任若干问题的解释》第 5 条的相关规定,设立层级化赔偿标准。对于受害人遭受轻微精神损害的情形,法院可通过消除影响、恢复名誉、赔礼道歉等非财产责任方式予以救济;对于一般或严重精神损害,则可依托既有司法裁判经验,结合当下社会经济发展水平,划定对应的赔偿数额区间,再由法院根据个案具体情节在区间内酌定具体赔偿金额。此种规则设计,既可全面保障受害人的合法权益、统一司法裁判尺度,又能清晰划定个人信息处理者的责任边界,避免过度归责、不当加重其经营与法律负担。

四、结　语

相较于传统侵权损害具有现实性、确定性的特点,个人信息泄露侵权造成的损害的本质属性在于风险导向性与不确定性。二者存在明显差异,若司法实践将这类风险性损害排除在救济范围外,不仅不利于个人信息保护,还会让信息主体持续陷入安全权益受损的恶性循环。据此,本文厘清风险性损害理论的适用边界,主张将个人信息泄露引发的风险性损害纳入法定损害范畴,以此构建完备的个人信息预防性救济体系。需注意的是,鉴于风险性损害具有发生概率不确定、损害后果潜在性等特征,法官应当在"实质性风险"标准下结合动态系统论,综合考量多项要素作出裁判。唯有如此,方能在个人信息合理利用与安全保障之间实现价值平衡。

本文提出的风险性损害司法认定规则与考量体系,是回应当前司法实践困境作出的阶段性探索。该体系既存在考量要素覆盖不全的局限,要素权重也会随社会发展、个案情形动态变化。伴随个人信息保护理论与实务的持续发展,个人信息泄露侵权中风险性损害的认定规则仍需不断优化迭代,最终达成逻辑自洽、体系严密、适用精准的目标。

参考文献:

[1] Solove D J, Citron D K. Risk and anxiety: a theory of data-breach harms[J]. Texas Law Review, 2018, 96(4): 737-786.

[2] 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.

[3] 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.

[4] 徐建刚.《民法典》背景下损害概念渊流论[J]. 财经法学, 2021(2): 31-45.

[5] 曾世雄. 损害赔偿法原理[M]. 北京: 中国政法大学出版社, 2001.

[6] 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.

[7] 龙松熊. 论侵害个人信息权益的损害赔偿[J]. 中国海商法研究, 2023, 34(4): 74-84.

[8] 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.

[9] 王大志, 张挺. 个人信息侵权中损害认定标准研究[J]. 信息安全研究, 2024, 10(2): 184-189.

[10] 汪志刚. 论民法上的损害概念的形成视角[J]. 法学杂志, 2008(5): 27-29.

[11] 王泽鉴. 损害赔偿[M]. 北京: 北京大学出版社, 2017: 64.

[12] 叶金强. 论侵权损害赔偿范围的确定[J]. 中外法学, 2012, 24(1): 155-172.

[13] Solove D J. Data is what data does: regulating based on harm and risk instead of sensitive data[J]. Northwestern University Law Review, 2024, 118(4): 1081-1138.

[14] 贝克. 风险社会[M]. 何博闻, 译. 南京: 译林出版社, 2004: 15-57.

[15] 刘水林. 风险社会大规模损害责任法的范式重构: 从侵权赔偿到成本分担[J]. 法学研究, 2014, 36(3): 109-129.

[16] 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.

[17] 汪渊智, 张雅宁.《民法典》中生态环境损害赔偿责任适用论[J]. 山西大学学报(哲学社会科学版), 2025, 48(2): 128-140.

[18] 张涛. 探寻个人信息保护的风险控制路径之维[J]. 法学, 2022(6): 57-71.

[19] 丁晓东. 从网络、个人信息到人工智能: 数字时代的侵权法转型[J]. 法学家, 2025(1): 40-54.

[20] 徐建刚. 论损害赔偿中完全赔偿原则的实质及其必要性[J]. 华东政法大学学报, 2019, 22(4): 149-161.

[21] 程啸, 曾俊刚. 个人信息侵权的损害赔偿责任[J]. 云南社会科学, 2023(2): 99-110.

[22] Solove D J, Citron D K. Standing and privacy harms: a critique of Transunion v. Ramirez[J]. Boston University Law Review Online, 2021, 101: 62-71.

[23] 郭锋, 陈龙业, 贾玉慧, 等.《关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》的理解与适用[J]. 人民司法, 2021(25): 37-42.

[24] 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.

[25] 张建文, 赵梓羽. 侵害个人信用信息的民事责任[J]. 征信, 2023, 41(3): 50-55.

[26] 尚国萍. 信息处理者侵害个人信息权益的民法救济[J]. 社会科学家, 2022(12): 121-126.

[27] 库齐奥, 张玉东. 动态系统论导论[J]. 甘肃政法学院学报, 2013

(4):40-47.
[28]王清军.具有损害生态环境重大风险认定的动态体系论[J].政治与法律,2025(3):95-109.
[29]王利明.民法典人格权编中动态系统论的采纳与运用[J].法学家,2020(4):1-12,191.
[30]Loos M E. Exposure as distortion: deciphering substantial injury for FTC data security actions[J]. George Washington Law Review Arguendo,2019,87:42-78.
[31]彭诚信,许素敏.侵害个人信息权益精神损害赔偿的制度建构[J].南京社会科学,2022(3):84-95.
[32]郭金良.数字经济时代个人金融信息侵权保护的困境与应对[J].法学评论,2024,42(5):120-130.
[33]叶名怡.个人信息的侵权法保护[J].法学研究,2018,40(4):83-102.
[34]杨显滨.论人格权侵权精神损害赔偿[J].比较法研究,2025(4):104-121.
[35]张新宝.从司法解释到侵权责任法草案:精神损害赔偿制度的建立与完善[J].暨南学报(哲学社会科学版),2009,31(2):2-11.

(责任编辑:陈丽琼)