数据泄露损害赔偿中“基于风险的方法”的应用

刘 颖,何明鑫
(暨南大学 法学院/知识产权学院,广东 广州 511443)

摘要:欧盟和中国在个人信息保护法律中都采用了“基于风险的方法”,强调个人信息保护风险控制的理念,数据保护影响评估或个人信息保护影响评估是其集中体现。当发生数据泄露时,“基于风险的方法”在个人寻求损害赔偿的救济途径中也应得到重视及应用,即将“风险”有条件地认定为“损害”,并且根据该方法评价风险性损害。“基于风险的方法”对“风险性损害”的评价要素可分为四个维度,包括个人信息的敏感程度、个人权益可能受危害的程度、发生危害的可能性及个人信息可能的利用方式。同时,需利用个人信息风险评价矩阵衡量风险性损害。“基于风险的方法”在个人信息损害赔偿中的应用既是风险社会的需要,也为个人信息提供了更完备的保护。

关键词:“基于风险的方法”;个人信息保护影响评估;数据泄露;风险性损害;风险评价矩阵

中图分类号:D923 **文献标志码**:A **文章编号**:2096-028X(2025)04-0041-10

数字经济时代,个人信息侵权具有无形性、潜伏性、分散性及未知性等风险特征,传统损害赔偿救济机制难以发挥实效。一些国家或地区的个人信息保护法律引入了“基于风险的方法”。注重风险控制成为个人信息保护的理念。欧盟《一般数据保护条例》(*General Data Protection Regulation*,简称GDPR)与《中华人民共和国个人信息保护法》(简称《个人信息保护法》)均体现了“基于风险的方法”。① 然而,受前数字时代法律传统的影响,在个人信息损害赔偿案件中,确定性损害仍是裁判的主要依据,不确定的风险往往被排除在外。② 个人信息保护法律的实践反映了保护理念与救济实际的割裂。如何在个人信息损害赔偿中贯彻“基于风险的方法”,形成完备的基于风险的个人信息保护制度体系,是亟须解决的重要问题之一。

一、“基于风险的方法”在损害赔偿中的可适用性

风险本身与不确定性相联系,具有多种含义。有学者认为,“风险”的概念与损失密不可分,其指损失发生的可能性或可能发生的损失。③ “基于风险的方法”超越了传统狭隘的“基于伤害的方法”。后者只关注确定性的损害,而前者考虑每一种实际的和潜在的不利影响。④

(一)基于风险的现有损害赔偿方案之检视

传统损害赔偿方案的不足引发了国内学者对风险性损害的讨论。中国现有的与风险性损害相关的观点可归纳为风险性损害类型说、风险损害差额说和公共预防说。

1.风险性损害类型说

风险性损害类型说将损害划分为风险引发的焦虑、预防费用与风险升高。⑤ 有学者主张人身安全受损的风险和潜在的经济损害也应属于风险性损害。⑥ 该说主张对风险性损害的识别受到了美国学者Solove和

基金项目:2025年度广东省社科联青年学术工作坊项目“粤港澳大湾区跨境数据流动规则衔接研究”(2025GZF06)

作者简介:刘颖,男,暨南大学法学院/知识产权学院教授、博士生导师;何明鑫,男,暨南大学法学院/知识产权学院国际法专业博士研究生。

① 参见张涛:《个人信息保护的整体性治理:立法、行政与司法的协同》,载《电子政务》2023年第6期,第54-55页。

② 参见赵贝贝:《个人信息私法救济中的“损害赔偿”困境与应对路径》,载《财经法学》2022年第5期,第95-96页。

③ 参见刘颖:《电子银行风险法律问题研究》,法律出版社2016年版,第12-13页。

④ Article 29 Data Protection Working Party, *Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks*, European Commission(30 May 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

⑤ 参见田野:《风险作为损害:大数据时代侵权“损害”概念的革新》,载《政治与法律》2021年第10期,第34-35页。

⑥ 参见王雪:《个人信息泄露的风险性损害之证成》,载《南大法学》2023年第3期,第175-176页。

Citron 提出的未来损害的概率和规模、数据敏感度和数据暴露、缓解措施及预防措施的合理性四个要素的影响。[①] 该说在一定程度上更新了传统的以确定性为基本特征的“损害”概念，但依然存在诸多未决问题。第一，风险的类型十分广泛，有学者认为该说有过度扩张侵权责任保护范围之嫌，主张否认抽象风险，重拾以实际发生损害为前提的“基于伤害的方法”。[②] 第二，如何将风险性损害具化为明确的赔偿数额仍是该说悬而未决的问题。虽然该说提及了若干评估要素，但要素较为抽象化，个人信息主体及法院难以运用学者提出的要素确定具体的赔偿金额。

2.风险损害差额说

风险损害差额说认为，以差额说为基础的“损害”概念经过发展已经足以解决个人信息侵权的难题，无需再诉诸构建独立的风险损害赔偿框架。该说认为，德国学者蒙森在19世纪提出的差额说经后续的发展演变，已不是原先仅指财产损失的差额，而是侵权行为发生前后的状态差额，囊括了精神损害，具有较强的兼容性。其认为，风险性质的财产损害等于个人信息主体采取预防措施的合理成本。[③] 该说的合理性值得商榷。首先，差额说的本质是寻找确定的利益差额，与具有概率性质的不确定风险存在根本不同。其次，预防措施的合理成本无法涵盖未能控制的剩余风险，采取预防措施不等同于风险已然得到控制，尽管采取措施的合理成本可作为赔偿的考量因素之一。最后，在数据泄露场景下，因数据处理具有复杂性，第三方滥用个人信息导致的个人信息权益受到侵害的风险往往难以预料。

3.公共预防说

公共预防说认为，《个人信息保护法》与欧盟GDPR中的个人信息权利之渊源都可追溯到宪法层面，具有公法的性质，因此，《个人信息保护法》第69条是公私融合的司法救济措施。因为个人信息侵权具有风险性质，损害赔偿难以实现，所以该说主张个人信息侵权诉讼不必关注如何完成损害赔偿的任务，而应注重威慑治理，以发挥侵权法公共预防的功能。[④] 该说借鉴美国侵权法理论中有关产品侵权应采取公共预防进路的观点，有助于从不同维度观察个人信息保护多主体参与的特性。[⑤] 然而，该说值得进一步探讨：其一，即使个人信息损害赔偿存在困难，也不能放弃个人信息侵权的私法救济途径。[⑥] 其二，损害赔偿兼具填补损害与预防的功能，不能仅关注公共预防，还应关注损害赔偿的损害填补与个案预防。[⑦]

为解决以上问题，笔者主张引入“基于风险的方法”，将风险性损害评估要素明确化，在确定法定最高赔偿金额的基础上，通过风险评价矩阵和为评估要素赋值百分比的方式量化评估风险性损害。

（二）“基于风险的方法”适用的必要性与可行性

欧盟第29条数据保护工作组（Article 29 Data Protection Working Party）发布的《关于基于风险的方法在数据保护法律框架中的作用声明》指出，“基于风险的方法”是对“基于伤害的方法”的优化，并从义务承担与责任分配的角度说明“基于风险的方法”的作用。[⑧] 在个人信息保护领域，“基于风险的方法”以关注实际的和潜在的不利影响为核心，以控制不确定性为主要内容，根据风险的大小设计风险预防义务及分配风险责任，兼具伸缩性和成比例性。“基于风险的方法”适用于数据泄露损害赔偿框架具有必要性和可行性。

首先，“基于风险的方法”是个人有限理性的弥补性解决方案。个人从行使相关的个人信息权益到寻求个人信息权益救济机制，都面临着“理性困境”。实践中，繁琐冗杂的隐私政策难以让个人做到真正的知情同意，无法有效保护相关个人信息权益。[⑨] 与“风险”概念相联系的不确定性，是指“对相关系统的完全确定

---

① Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, Texas Law Review, Vol.96: 737, p.738(2018).

② 参见宁园：《“个人信息侵权”方案的反思及其重塑》，载《当代法学》2024年第1期，第44页。

③ 参见张博文：《论个人信息泄露下游侵害风险的损害赔偿》，载《南大法学》2023年第6期，第145-146页。

④ 参见丁晓东：《从个体救济到公共治理：论侵害个人信息的司法应对》，载《国家检察官学院学报》2022年第5期，第105-113页。

⑤ Guido Calabresi, *Civil Recourse Theory's Reductionism*, Indiana Law Journal, Vol.88: 449, p.467-468(2013); Richard A. Posner, *Instrumental and Noninstrumental Theories of Tort Law*, Indiana Law Journal, Vol.88: 469, p.470(2013).

⑥ Benjamin C. West, *No Harm, Still Foul: When an Injury-in-Fact Materializes in a Consumer Data Breach*, Hastings Law Journal, Vol.69: 701, p.710(2018).

⑦ Guido Calabresi & Spencer Smith, *On Tort Law's Dualism*, Harvard Law Review, Vol.135: 184, p.184(2022).

⑧ Article 29 Data Protection Working Party, *Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks*, European Commission(30 May 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

⑨ 参见丁晓东：《个人信息保护：原理与实践》，法律出版社2021年版，第94页。

性知识之任何偏离”，包括认知的不确定性和可变的不确定性。① 个人信息主体出于缺乏专业知识、欠缺数据统计手段等原因，难以认知个人信息处理行为对个人的影响。在万物互联的时代，社会生活复杂多变，某一事实的发生与其产生的影响具有概率的特性愈发明显，个人信息主体进一步陷入认知困境。个人信息处理者作为收集处理信息并因此而获益的一方，显然比个人更具备控制不确定性的实力，将风险责任归于个人信息处理者具有可行性和合理性。风险分配实质上是“风险成本、风险责任、风险损失在主体间的承担”，② 让获得利益的一方承担更多风险是实现风险分配正义的应有之义。

其次，在司法裁判中，确定性与不确定性并非截然对立的两个概念，证据证明的事实并非等同于客观事实，而是一种高度盖然性。有论者指出：“在一个司法审判系统寻求认定事实、适用法律解决民事纠纷之同时，该系统亦必须认识到一个痛苦的事实：我们活在一个不确定的世界中，并无法完美地确定过去的历史事实。”③“基于伤害的方法”需要明确个人信息主体是否实际受到侵害。在数据泄露场景下，证明存在确定的损害事实并分配责任、予以救济成为现实难题。④ 风险的“不确定性”不等于对个人信息主体产生不利影响的客观事实没有发生。风险不仅包括将来可能造成的不利影响，还包括已经造成或正在造成却因难以认知而无法确定的不利影响。新近侵权法的发展历程表明，“损害的预防胜于损害补偿”，重视风险已成为现代侵权法发展的趋势之一。⑤ “基于风险的方法”在个人信息损害赔偿中的应用，可反映该类型的损害赔偿兼具填补和预防的双重目的，即填补实际的不利影响及预防潜在的不利影响，契合了在复杂多变的数字环境下保护个人信息、维护个人权益的需要。⑥ 从“基于伤害的方法”到“基于风险的方法”，是从静态、确定的义务承担与责任分配向动态、不确定的义务承担与责任分配的转变。

最后，欧盟与美国的相关法律实践表明，在损害赔偿中适用“基于风险的方法”具有可行性。欧盟 GDPR 第 82 条第 1 款规定：“因违反本条例而受到物质或非物质性损害的任何人，均有权从控制者或处理者造成的损害中获得赔偿。”至于非物质性损害为何，其并无明确解释。⑦ 欧盟 GDPR 的制度设计采取的是“基于风险的方法”，其序言第 146 条第 3 句规定“损害概念应按照立法目标进行广义解释”，从体系解释的角度分析，这意味着个人信息损害赔偿中存在一类将一定程度的“风险”认定为“损害”的“风险性损害”。⑧ 据此，个人信息主体因数据泄露产生身份盗窃、欺诈或者声誉受损等风险时，有权要求个人信息处理者承担损害赔偿责任。⑨ 在欧盟法院裁判的“VB 案”中，黑客未经授权进入保加利亚国家税务局的信息系统，将数百万保加利亚国民和外国公民的各种税收和社会保障信息公布在互联网上，欧盟法院认为个人数据泄露后对数据可能被滥用的担忧构成非物质性损害。⑩ 该案中，对数据可能被滥用的担忧并非传统侵权法意义上的确定性损害，而是一种风险性损害。美国法上也存在诸多案例承认风险性损害。⑪ 如有法院认为未来数据滥用风险的提高足以构成损害。⑫ 因此，认定损害的关键是把焦点转移到风险上，而非确定性上。⑬

二、“基于风险的方法”对侵权责任构成要件的反思与重塑

在数据泄露的司法案件当中，个人信息主体很难提供证据证明自身所遭受的损害与数据泄露之间存在因果关系。基于此，个人寻求获得赔偿的可行路径离不开改进传统因果关系的证明思路。

---

① 参见张涛：《风险预防原则在个人信息保护中的适用与展开》，载《现代法学》2023 年第 5 期，第 57 页。

② 参见徐钝：《社会风险分配失衡的社会资本矫正——以法理型社会资本培育为中心》，载《学术论坛》2013 年第 7 期，第 70 页。

③ 黄国昌：《民事诉讼理论之新展开》，北京大学出版社 2008 年版，第 59 页。

④ Ira S. Rubinstein & Woodrow Hartzog, *Anonymization and Risk*, Washington Law Review, Vol.91: 703, p.730(2016).

⑤ 参见王泽鉴：《侵权行为》（第 3 版），北京大学出版社 2016 年版，第 10 页。

⑥ 参见王泽鉴：《损害赔偿》，北京大学出版社 2017 年版，第 25-35 页。

⑦ 参见刘云：《论个人信息非物质性损害的认定规则》，载《经贸法律评论》2021 年第 1 期，第 60 页。

⑧ 参见王益强：《裁判视角下数据侵权损害的认定》，载《华东政法大学学报》2023 年第 5 期，第 81 页。

⑨ 参见解正山：《数据泄露损害问题研究》，载《清华法学》2020 年第 4 期，第 145 页。

⑩ Judgment of the Court (Third Chamber), 14 December 2023, Case C-340/21.

⑪ *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015); *Lewert v. P. F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016); *In re U.S. Office of Personnel Management Data Security Breach Litigation*, 928 F.3d 42 (D.C. Cir. 2019).

⑫ *Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015); *Lewert v. P. F. Chang's China Bistro, Inc.*, 819 F.3d 963 (7th Cir. 2016).

⑬ Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, Texas Law Review, Vol.96: 737, p.777(2018).

（一）因果关系

因果关系证明难的问题主要集中在如何确定个人信息处理者的数据泄露行为导致了不利后果。学界现有解决方案包括转换证明责任、降低证明标准或者引入比例（概率）因果关系理论等。[①] 实务中，有法院认为，若个人信息主体能证明个人信息处理者存在数据泄露的高度可能性，则可初步完成因果关系的举证责任。个人信息处理者应提供反证推翻该高度可能性。如若不能，数据泄露与损害事实之间就存在因果关系。[②] 然而，当数据泄露产生的损害本身都难以证明时，如何证明因果关系？此时，应当将损害与因果关系作为整体进行考量。将数据泄露受害者在泄露时造成的直接伤害视为损害，可以有效解决因果关系证明难的问题。[③] 该认定方式已经在美国下级法院的司法实践中被证明是可行的。例如，美国联邦地区法院认为，由于数据泄露造成隐私侵犯，故数据泄露本身可以被视为一种损害，受害者具备起诉资格。[④] 中国司法实践中也有根据此认定方式解决因果关系问题的案例。例如，在“林某与四川航空侵权责任纠纷上诉案”中，法院认为，举证责任的承担应该综合当事人举证能力等因素确定，林某作为远离证据材料、缺乏必要的证据收集条件和手段的消费者，证明存在数据泄露的事实已经是尽己所能。要求林某进一步举证，显然超出其举证能力，有违公平原则。[⑤]

虽然有论者提出，证明个人信息侵权案件中的因果关系可以使用数学公式中的贝叶斯定理，但司法实践中使用过于复杂的数学公式不具备可操作性。[⑥] 因此，多数情况下，个人信息主体只要证明个人信息处理者存在数据泄露的事实，即可成为适格的诉讼主体。但数据泄露成立个人信息侵权诉讼应有预设前提，即泄露的数据至少是可能对个人权益造成侵害或危害的个人信息，否则，几乎任何对诉讼有兴趣的人都可以声称他们的利益将受到负面影响，从而要求赔偿损害。[⑦] 无限制条件地认定数据一经泄露即构成损害会造成极大的不公平，也容易给不法分子可乘之机。

（二）过错

《中华人民共和国民法典》（简称《民法典》）第1038条是关于个人信息处理者信息安全保护义务的规定。《个人信息保护法》第51条、第57条将义务的内容进行细化。有论点认为，个人信息损害赔偿应采无过错归责原则。[⑧] 实践中，要求小微型平台和大型平台采取同样的高成本措施防止数据泄露显然是不合理的。个人信息损害赔偿不应适用无过错归责原则，也不应仅以个人信息处理者是否履行了法律规定的义务推定其是否有过错。但履行法定义务可作为减轻赔偿责任的依据。

评价过错应基于合理性与程度性的标准，结合具体的数据处理场景综合判断过错程度。标准的考量因素包括以下三项：第一，个人信息处理者是否存在过错与个人信息风险程度相适应。《个人信息保护法》将个人信息分类为一般个人信息与敏感个人信息，前者风险程度较低，后者风险程度高。即使客观上处理者违反了相关法律义务，但如果数据泄露没有对个人信息主体造成实质影响，也有可能推定处理者没有过错。[⑨] 比如，在“AT案”中，政府未经同意在互联网上发布了个人信息主体的姓名，法院认为，虽然政府的公开行为违反了欧盟GDPR的规定，但姓名为一般个人信息，没有证据表明政府的公开行为对个人信息主体造成了负面影响，违反法律的行为并不能被当然评价为过错。[⑩] 而当处理者在处理敏感个人信息时未履行相对应的强化义务，比如没有对敏感个人信息进行脱敏加密处理，造成个人信息处理风险不可控或使得个人信息主体面临人身权益、财产权益遭受侵害的高风险，那么应认定处理者存在过错。第二，与个人信息风险程度对应的安全措施。当一般个人信息泄露时，通常情况下，个人信息处理者履行通知义务并及时弥补内部安全漏

---

① 参见谢鸿飞：《个人信息处理者对信息侵权下游损害的侵权责任》，载《法律适用》2022年第1期，第33页。

② 参见杭州互联网法院民事判决书，（2022）浙0192民初4259号。

③ Jordan Elias, *Course Correction-Data Breach as Invasion of Privacy*, Baylor Law Review, Vol.69: 574, p.581-586(2017).

④ *Rowe v. Unicare Life & Health Insurance Co.*, No. 09 C 2286, 2010 WL 86391 (N.D. Ill. Jan. 5, 2010).

⑤ 参见四川省成都市中级人民法院民事判决书，（2015）成民终字第1634号。

⑥ 参见方程：《贝叶斯定理认定因果关系的逻辑展开——从个人信息侵权案切入》，载《浙江工商大学学报》2023年第4期，第147页。

⑦ Jennifer Wilt, *Cancelled Credit Cards: Substantial Risk of Future Injury as a Basis for Standing in Data Breach Cases*, SMU Law Review, Vol. 71: 615, p.618-619(2018).

⑧ 参见蒋丽华：《无过错归责原则：个人信息侵权损害赔偿的应然走向》，载《财经法学》2022年第1期，第41-42页。

⑨ 参见程啸：《论个人信息侵权责任中的违法性与过错》，载《法制与社会发展》2022年第5期，第205-207页。

⑩ *VX and AT v. Gemeinde Ummendorf*, Case C-456/22.

洞，就可以认定尽到了合理注意义务。当敏感个人信息泄露时，个人信息处理者除履行以上义务外，还需要其采取对应预防措施，比如为相关信息主体进行风险投保、追踪数据泄露的去向及控制数据泄露的影响等。如果处理者没有采取对应预防措施，即使履行了通知义务，也应推定其存在过错。第三，数据泄露之后是否采取措施及所采取措施是否有效影响过错程度认定。个人信息处理者在数据泄露之后没有及时采取措施，且在个人信息主体提出明确要求之后依然拒绝回应或不予理睬，其过错程度为重大过失甚至故意。如果处理者采取了预防措施，但该措施缺乏有效性，那么其过错程度至少为过失，除非该措施与其现有的专业能力和经济实力相匹配且其已经尽其所能。

（三）“损害”概念的再解释

在传统侵权法中，损害是指“因一定的行为或者事件使某人受侵权法保护的权利和利益遭受不利益的影响”。[①] “损害”概念经历了从差额说到客观损害说、规范损害说的演变。[②] 客观损害说认为损害是权利人既有权益的恶化，要求损害事实上已经发生。规范损害说认为损害的认定可以从法律的价值评判上考量。[③] 客观损害说指出了损害的本质是一种权益的恶化，但其所要求的认定客观损害事实很难适用于个人信息损害赔偿案件中。规范损害说的积极意义在于认识到损害的认定受法律价值的影响，具有规范性的特征。

许多学者意识到个人信息损害赔偿案件中风险的实际存在，并有较为成熟的论述。司法实践中，法院之所以对“风险作为损害”这类观点持保守态度，主要考虑的可能是集体诉讼难、缺乏可操作的风险量化评估工具及担心高额赔偿影响个人信息处理者的生存利益等。[④] 但随着社会的发展，认定责任存在较大的不确定性成为数字经济的常态。“基于风险的方法”应在个人信息损害赔偿领域中发挥作用，运用动态灵活的风险理念重新解释损害的概念，将损害扩大解释为能为法律所认可的不利影响，包括实际的和潜在的、确定的及不确定的不利影响。总的来说，损害的概念并非一成不变，其所具有的规范性特质，使概念内涵随着社会的发展和法律价值的变化而不断发展。

三、“基于风险的方法”对风险性损害类型的再划分

将作为新型损害的风险性损害类型化有助于明确不同类型损害的责任承担方式及确定赔偿金额。个人信息兼具人格价值和财产价值。[⑤] 数据泄露损害赔偿中，可将风险性损害划分为非物质性损害与物质性损害。非物质性损害是指难以通过金钱衡量计算，也不能根据市场交易将其物化为具体财产类型的损失，具体表现为因数据泄露引发的精神上的焦虑、不安、担忧等心理痛苦。物质性损害则是指可用金钱衡量计算的财产损失，主要包括数据泄露导致的维权费用损失及下游侵权产生的高度盖然性的财产损失。[⑥]

（一）非物质性损害

数据泄露会引起个人信息主体对信息失控导致的不确定性的担忧、焦虑及恐惧等心理痛苦。依据立法实践与学界通说，个人信息保护被置于人格权体系中。[⑦] 当个人信息泄露侵害的是个人的人格权益时，涉及的主要是精神性损害。[⑧]《民法典》第 1034 条至第 1039 条关于个人信息的规定位于人格权编中即为典型例证。与传统的精神损害相比，数据泄露产生的精神性损害不以具体人格权受到侵害为基础。有研究表明，数据泄露引发的焦虑能让个人信息主体“身患抑郁症、焦虑症和创伤后应激障碍”，因此，承认这一非物质性损害并不违背传统精神损害认定要求。[⑨] 在个人信息侵权案件中，对难以认知、未来可能发生的不利影响产生担忧、忧虑的精神性损害，应该适用人格权的相关规定。

有论点认为，《个人信息保护法》第 69 条规定的过错推定责任不是普遍性责任，该条也不是侵害人格权

① 参见张涛：《探寻个人信息保护的风险控制路径之维》，载《法学》2022 年第 6 期，第 61 页。
② 参见徐建刚：《〈民法典〉背景下损害概念渊流论》，载《财经法学》2021 年第 2 期，第 31 页。
③ 参见徐建刚：《〈民法典〉背景下损害概念渊流论》，载《财经法学》2021 年第 2 期，第 39 页。
④ 参见谢鸿飞：《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》，载《国家检察官学院学报》2021 年第 5 期，第 22 页。
⑤ 参见刘颖、谷佳琪：《个人信息去身份化及其制度构建》，载《学术研究》2020 年第 12 期，第 58 页。
⑥ 参见杭州互联网法院民事判决书，（2022）浙 0192 民初 4259 号。
⑦ 参见曹博：《个人信息可识别性解释路径的反思与重构》，载《行政法学研究》2022 年第 4 期，第 135 页。
⑧ 参见张博文：《论个人信息泄露下游侵害风险的损害赔偿》，载《南大法学》2023 年第 6 期，第 146-147 页。
⑨ 参见时诚：《个人信息泄露风险损害的赔偿责任》，载《现代法学》2024 年第 2 期，第 148 页。

益的精神损害赔偿条款。[①]《民法典》第995条规定，在人格权受到侵害时，受害人有权请求侵权人承担民事责任。该条表明，人格侵权不以行为人过错推定为要件，也不适用诉讼时效规定。《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》（简称《规定》）第11条规定，侵害他人人身权益，造成财产损失或者严重精神损害的，被侵权人有权请求损害赔偿。因此，在《个人信息保护法》第69条中的损害不包括精神性损害的情况下，个人也可以依据《民法典》第995条与第1183条及《规定》第11条的规定请求精神损害赔偿。

（二）物质性损害

《个人信息保护法》第69条解决的主要是财产损失的赔偿责任问题。[②] 数据泄露案件中，维权费用损失确定较为容易。然而，个人信息主体遭受的未来发生或者已经发生却难以认知计量的物质性损害，因其无形、潜伏、长期及具有概率的特性，难以通过《个人信息保护法》第69条第2款“个人因此受到的损失或者个人信息处理者因此获得的利益”的规定直接确定。该损害实质是一种机会损害。机会损害的概念来源于侵权法上的机会丧失理论。该理论在1981年由美国学者Joseph H. King正式提出，旨在解决侵权案件中因果关系证明难与“全无或全有赔偿原则”适用难的问题，并为此提供了比例赔偿的思路。[③] 该理论在医疗侵权领域有较多的应用案例。[④] 在法律层面上，机会是指获得利益或者避免损害的可能性，机会与风险相伴而生，获得利益的机会实质上是获利可能丢失的风险，避免损害的机会则是损害可能发生的风险。[⑤]

个人信息侵权案件面临与医疗侵权同样的因果关系证明难与赔偿难的问题。借鉴机会丧失理论，在数据泄露案件中，个人信息主体受到的机会损害体现为财产损失可能发生的风险。个人信息损害赔偿案件应有限制条件地将风险认定为损害，如此可以有效平衡个人信息处理者与个人信息主体的信息利益。况且，因数据泄露产生的风险不一定具有可赔偿性，也不必然引发隐私侵权时精神上的痛苦或焦虑。[⑥] 当风险性损害属于物质性损害时，其为高度盖然性的财产损失。高度盖然性包括两种情形：一是数据泄露导致财产损失的事实可能是未来会发生的，该事实未来发生的概率具有高度盖然性；二是已经发生但难以被认知的财产损失，该损失存在的概率具有高度盖然性。比如，数据泄露导致的信用评分降低使个人信息主体实际遭受了多大程度的财产损失难以被直接举证，但财产损失的概率往往能被证明。

四、“基于风险的方法”在损害赔偿中的量化评估

厘清“基于风险的方法”在法律中的体现及作用，有助于解决损害赔偿责任的确定问题。

（一）“基于风险的方法”在法律上的评价要素

欧盟GDPR第35条的数据保护影响评估（Data Protection Impact Assessment，简称DPIA）与中国个人信息保护影响评估中提供的一些评价要素，有利于对风险进行可靠和相对客观的评估。当然，在欧盟GDPR中体现“基于风险的方法”的法律条款并不仅仅是第35条，还包括第32条关于处理过程的安全性及第33条、第34条的数据泄露通知等。[⑦] 在欧盟GDPR框架下，“基于风险的方法”要求数据控制者有义务在数据生命周期中评估各个阶段可能因数据处理失当造成侵害数据主体的权利和自由的高风险。[⑧]《个人信息保护法》中的诸多条款与欧盟GDPR类似，如第55条、第56条的个人信息保护影响评估，第57条的个人信息泄露通知等。

DPIA要求数据控制者在处理可能发生高风险的数据前，科学、客观地评估处理行为的性质、范围、内容

---

① 参见王道发：《个人信息处理者过错推定责任研究》，载《中国法学》2022年第5期，第103页。

② 参见朱晓峰：《个人信息侵权责任构成要件研究》，载《比较法研究》2023年第4期，第135页。

③ Joseph H. King, *Causation, Valuation, and Chance in Personal Injury Torts Involving Preexisting Conditions and Future Consequences*, The Yale Law Journal, Vol.90: 1353, p.1387(1981).

④ *Delaney v. Cade*, 255 Kan. 199, 873 P.2d 175 (1994).

⑤ 参见冯德淦：《侵权法中机会丧失理论之构建》，载《华侨大学学报（哲学社会科学版）》2022年第1期，第140页。

⑥ 参见梅夏英：《社会风险控制抑或个人权益保护——理解个人信息保护法的两个维度》，载《环球法律评论》2022年第1期，第16页。

⑦ Article 29 Data Protection Working Party, *Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks*, European Commission(30 May 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

⑧ Maria Eduarda Gonçalves, *The Risk-Based Approach Under the New EU Data Protection Regulation: A Critical Perspective*, Journal of Risk Research, Vol.23: 139, p.142(2020).

等，避免个人数据安全事件的发生。这些高风险的处理行为包括但不限于：基于数据的自动化处理、大规模处理特殊类型个人数据、处理有关犯罪和违法的个人数据、对公共区域的大规模系统化监控。《个人信息保护法》则在第 55 条规定，处理敏感个人信息，利用个人信息进行自动化决策，委托处理个人信息、向其他个人信息处理者提供个人信息、公开个人信息，向境外提供个人信息等应当进行个人信息保护影响评估。另外，欧盟 GDPR 第 9 条对特殊类型个人数据设置了严格保护。《个人信息保护法》第二章第二节对敏感个人信息的处理规则作了单独且严格的规定。特殊类型个人数据虽在范围上与敏感个人信息并非完全一致，但此类个人信息均具有对隐私、人格尊严等构成严重威胁的性质。在这个意义上，特殊类型个人数据、敏感个人信息的规定，隐含先验的、抽离于具体场景的高风险推定，即对敏感个人信息的处理可能对个人、群体或者整个社会产生较高的不利影响。① 结合上述条款内容，可将“基于风险的方法”的评价要素归纳为个人信息的敏感程度、个人权益可能受危害的程度、发生危害的可能性和个人信息可能的利用方式。

（二）“基于风险的方法”评价要素的量化

1.个人信息的敏感程度与个人权益可能受危害的程度

敏感个人信息是认定风险性损害的核心内容。中国个人信息保护制度体系已经确立了个人信息的分层次治理模式。《个人信息保护法》第 28 条规定了敏感个人信息的类型。敏感个人信息是指会对个人的人格尊严、人身安全或者财产安全造成高概率、高危害程度影响的信息。个人信息的敏感程度与个人权益可能受危害的程度相关联。敏感程度越高说明个人权益可能受危害的程度越高，个人信息风险危害等级也就越高，故笔者将“基于风险的方法”中的个人信息的敏感程度和个人权益可能受危害的程度一并进行讨论。

国家市场监督管理总局、国家标准化管理委员会发布的《数据安全技术 数据安全风险评估方法》（简称《评估方法》）提供了风险评估量化公式与赋值逻辑，有助于厘清个人信息损害赔偿中的风险性损害认定问题。参考《评估方法》附录 C.1 的风险危害程度分级框架，并依据附录 D 的风险评估量化分析逻辑，聚焦个人信息损害赔偿领域，可将个人信息泄露引发的风险危害程度划分为四个等级，即极度危害（赋值区间[75%，100%]）、高度危害（赋值区间[50%，75%]）、中度危害（赋值区间[25%，50%]）、轻度危害（赋值区间[0%，25%]）。各等级的具体表现与影响特征如下：其一，极度危害表现为个人信息主体可能遭受重大且不可消除的影响，极易导致人格尊严、人身财产安全遭受严重侵害，如背负无法承担的债务；其二，高度危害表现为个人信息主体将面临较大影响，如遭单位解雇、健康状况显著恶化等；其三，中度危害表现为个人信息主体会遭遇明显困扰，但此类困扰仍处于可通过合理措施克服的范围，如引发轻微生理疾病；其四，轻度危害表现为个人信息主体仅会受到轻微影响，且该影响多为短期、可逆的，如短期内名誉出现小幅下降。敏感个人信息泄露的危害程度属于高度危害（个人信息主体可能遭受较大影响，个人信息主体克服难度高，消除影响代价较大）以上，表示区间为[50%，100%]。风险危害程度分析遵循就高从严、整体分析的原则，如果该风险涉及多个个人信息，则取其中个人信息风险危害等级最高的参数用于整体判断。除了有明确规定的敏感个人信息类型之外，某些个人信息因其潜在用途也会被认定为敏感个人信息。

现实生活中，数据往往并不单独使用，敏感个人信息的形成可能是非敏感个人信息与其他数据产生“聚合效应”的结果。② 例如，收件地址具有一定范围的公开性，并不敏感，但是当其与不愿为外人知晓且对现有工作造成影响的兼职单位信息结合则会构成隐私信息，对个人造成损害。③ 该类有可能与其他数据聚合形成敏感个人信息的一般个人信息泄露的危害程度属于中度危害，表示区间为[25%，50%]。该类个人信息与其他数据组合会构成敏感个人信息，其泄露的危害程度存在由中度危害向高度危害甚至极度危害的转化可能。因此，在认定风险性损害的案件中，法官应该谨慎分析个人信息是否具备敏感性，不能因为某类个人信息表面上为一般个人信息就判定该信息的泄露不会造成损害。

2.发生危害的可能性

《评估方法》附录 B.1 提及了风险的分类，对司法裁判有重要的借鉴作用。参考附录 B.1，常见的数据安全风险类别有数据泄露风险、数据篡改风险、数据破坏风险、数据丢失风险等。在个人信息泄露损害赔偿的

① 参见张涛：《探寻个人信息保护的风险控制路径之维》，载《法学》2022 年第 6 期，第 64 页。

② Daniel Solove, *The Digital Person: Technology and Privacy in the Information Age*, New York University Press, 2004, p.44-47.

③ 参见北京市第三中级人民法院民事判决书，（2020）京 03 民终 2049 号。

场景中,参考《评估方法》附录C.2风险可能性等级的分析框架,可将数据泄露发生危害的可能性大小划分为很高(赋值区间[75%,100%])、高(赋值区间[50%,75%])、中(赋值区间[25%,50%])、低(赋值区间[0%,25%])四个等级。

发生危害的可能性大小与个人信息处理者采取的安全措施有关。安全措施能否控制风险要从合规性与有效性两个层面判断。比如,在"薛祥飞、淘宝隐私权纠纷案"中,法院认为个人信息处理者需要证明其是否采取了个人信息保护必要的合规措施及采取的措施是否与其专业能力相匹配。① 如果均无法证明,则法院可据此认定发生危害的可能性高或者很高。

3.个人信息可能的利用方式

对个人信息可能的利用方式进行推断,是法院认定风险性损害的补充环节。一方面,法院可以根据类案经验,评估不同类型的个人信息在类似场景下数据泄露后发生的实际滥用行为,如身份信息泄露后被用于虚假注册。法院也可以结合本案的数据特征,研究评估数据泄露中涉及的不同类型个人信息的潜在利用可能性,如健康医疗信息可用于恶意推销、高铁行程信息可用于改签欺诈等。法院应调查个人信息的使用或披露将如何影响个人的财务安全、声誉或情绪状态。被黑客盗窃并发布在身份信息交易网站上的个人信息很有可能被用于欺诈,但若黑客盗窃的是匿名化的个人信息,则很难据此证明存在身份盗窃的重大风险。

另一方面,为了确定损害是实际的或迫在眉睫的,法院应考虑原告是否合理地主张第三方(如黑客)有"意图和能力使用原告的数据"。② 先前存在第三方滥用个人信息的行为可以推断第三方具备相应的能力。比如,在"美国人事管理办公室数据安全漏洞案"中,华盛顿特区巡回法院认为,未来损害风险的提高可以构成事实上的损害。法院通过对第三方行为的推测,包括黑客可能如何利用个人信息,从而确定损害是否存在。该案中,存储在被告网络中的敏感个人信息被黑客窃取,其中一部分原告声称,自数据泄露以来,他们已经经历了欺诈和身份盗窃。已有的个人信息利用行为表明,黑客"很老练,显然很有耐心",原告仍然面临着由这次入侵引发的未来身份遭遇盗窃的重大风险。③ 总的来说,先前存在的数据利用行为、同类型数据通常的利用方式及数据泄露的影响程度等可以作为法官推断利用方式的合理依据。

(三)风险性损害的衡量与责任承担

关于数据泄露造成的损害如何界定,目前尚无一致或连贯的司法方法。虽然风险难以精确测算,但也具备可以量化的因素。④

1.个人信息风险评价矩阵

根据上述个人权益可能受危害的程度及发生危害的可能性大小,参考《评估方法》9.3关于数据安全风险评价的分析逻辑,可对个人信息泄露场景下的风险进行评价,风险评价矩阵如表1所示。

表1 个人信息风险评价矩阵

可能性	危害程度			
	极度危害	高度危害	中度危害	轻度危害
很高	重大风险	高风险	中风险	低风险
高	高风险	高风险	中风险	低风险
中	中风险	中风险	低风险	轻微风险
低	低风险	低风险	轻微风险	极轻微风险

个人信息风险评价矩阵有两个维度:一是危害程度,即风险总是具有负面影响;二是可能性,即风险是"可能"发生的事件。结合表1的评价方法及实际情况进行量化评价,计算公式如下:$R_i = \sqrt{\sigma_i \times V_i}$。其中,$R_i$为第$i$个数据的风险评价分值,$\sigma_i$为第$i$个数据危害程度赋值,$V_i$为第$i$个数据发生危害可能性赋值。⑤ 根

① 参见杭州互联网法院民事判决书,(2022)浙0192民初4259号。
② *In re U.S. Office of Personnel Management Data Security Breach Litigation*, 928 F.3d 42 (D.C. Cir. 2019).
③ *In re U.S. Office of Personnel Management Data Security Breach Litigation*, 928 F.3d 42 (D.C. Cir. 2019).
④ 参见张涛:《探寻个人信息保护的风险控制路径之维》,载《法学》2022年第6期,第70页。
⑤ 参见《评估方法》附录D.3。

据该计算公式，个人信息风险评价矩阵中，各风险评价结果的分值区间（保留两位小数）如下：重大风险［75.00%，100.00%］、高风险［50.00%，86.60%］、中风险［25.00%，70.71%］、低风险［0.00%，50.00%］、轻微风险［0.00%，35.36%］、极轻微风险［0.00%，25.00%］。每个风险评价结果的分值区间取对应“危害程度×可能性”组合的最小值（最小赋值乘积开根号）与最大值（最大赋值乘积开根号），确保覆盖所有可能情况。其中，各风险评价结果分值区间存在重合之处，体现了风险层级在特定条件下可以相互转化的实际情况。因此，在司法裁判中，法院不能仅凭分值区间直接判定风险层级，而需结合具体案件事实，对“危害程度”与“可能性”进行精准赋值，以明确最终的风险评价结果。比如，第 a 个数据的 σ_a 赋值为 30%、V_a 赋值为 30%，则 R_a 风险评价分值为 30%。风险评价结果为高风险以下。该个人信息的泄露对个人权益影响较小，其引发的风险不应被认定为风险性损害。评价结果中的高风险和重大风险有可能对自然人的人格尊严等直接造成较为严重或严重的侵害或危害。这两种风险至关重要，构成风险性损害。

责任承担方式与损害赔偿金额的确定会根据风险评价层级的不同而有所区别。法官可根据风险评价结果（重大、高、中、低、轻微、极轻微）对案件作出裁量。

首先，在风险性损害中，高度盖然性的风险性损害是指危害程度数值与发生危害可能性数值同时大于50%的情形，即评价结果为重大风险和高风险的风险性损害，可适用损害赔偿。敏感个人信息被非法处理或者泄露意味着危害程度大于 50%。个人信息处理者缺乏安全措施则表明发生危害的可能性大于 50%。比如，在“Rosenbach 案”中，游乐园未经监护人同意对未成年人进行指纹识别，美国伊利诺伊州最高法院认为，生物识别信息具有高度敏感性，且该州严格保护未成年人的个人信息。对未成年人进行指纹识别是非法处理行为，该行为本身足以构成侵权。① 该案中，生物识别信息泄露的危害程度为高度危害以上，游乐园非法处理生物识别信息表明其缺乏相应的安全措施。该处理行为发生危害的可能性是高以上。因此，涉案处理行为引发的风险可被评价为高风险以上，构成风险性损害。在“Attias 案”中，健康保险公司的消费者个人信息被黑客窃取，其中包括患者信用卡号码、社会保障号码等敏感个人信息。华盛顿特区巡回法院认为，因健康保险公司没有对涉案信息进行加密，缺乏安全措施，所泄露的个人信息被用于身份盗窃具有高度的可能性。② 该案的风险评价结果同样是高风险以上，构成风险性损害。实务中，处理行为超过合理限度并造成实质性影响，泄露方式、范围、后果超出合理预期等也可能造成风险性损害。③

其次，评价结果为中风险的，一般是未达到严重程度的精神性损害，不适用损害赔偿。个人信息处理者承担责任的方式主要是赔礼道歉、采取相关措施弥补个人信息主体可能的损失及尽可能地控制不利影响。比如，法院认为，被告的数据泄露行为虽构成对原告人身权益的损害，但因损害程度较轻，故不支持原告的赔偿请求，仅判令被告作出书面赔礼道歉。④

最后，低风险、轻微风险及极轻微风险不宜在司法裁判中被认定为风险性损害，不适用损害赔偿，一般也无需个人信息处理者承担赔礼道歉的民事责任。⑤ 这三类情形的补救方式一般为个人信息主体与个人信息处理者协商，由双方共同采取相关措施控制不利影响。

以风险评价矩阵的评价结果衡量赔偿的合理性可通过侵权法中的机会丧失理论证成。根据该理论，在因医疗过失导致患者生存机会丧失超过 50%的典型案件中，对患者予以比例赔偿当无疑义。⑥ 这就意味着当患者的生命健康权遭受严重危害的风险大于 50%时可获得赔偿救济。与医疗侵权相比，个人信息侵权案件中敏感个人信息的泄露导致个人信息主体的人身财产权益遭受侵害的风险大于 50%同样会对个人产生严重影响，以此作为将个人信息风险纳入赔偿范围的标准，具备合理性。

此外，可借鉴机会丧失理论提出比例赔偿思路。比例赔偿突破了全无或全有赔偿的固定模式，能同时兼顾损害赔偿的补偿与预防双重功能，而非仅实现其中某一项功能。⑦ 这也是“基于风险的方法”作为一种比

① *Rosenbach v. Six Flags Entertainment Corporation*, 432 Ill.Dec. 654, 129 N.E.3d 1197 (Ill. 2019).
② *Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017).
③ 参见北京互联网法院民事判决书，(2019)京 0491 民初 16142 号；北京市第一中级人民法院民事判决书，(2016)京 01 民终 3257 号。
④ 参见广东省深圳市中级人民法院民事判决书，(2017)粤 03 民终 7378 号。
⑤ 参见江苏省南京市中级人民法院民事判决书，(2014)宁民终字第 5028 号。
⑥ 参见王浩然：《侵权法生存机会丧失理论的重构》，载《财经法学》2023 年第 2 期，第 170 页。
⑦ 参见郑晓剑：《损害赔偿的功能与完全赔偿原则的存废——利益平衡视角下之反思》，载《河南社会科学》2018 年第 2 期，第 59 页。

例式的方法应用在损害赔偿中的实操路径。风险性损害的赔偿金额可参照《规定》第12条第2款的规定，按风险评价层级成比例地确定，即如果评价结果达到了高风险以上，则可以比照50万的金额，按比例设定相应的赔偿金额上限。根据风险评价矩阵的评估结果，可进一步细分损害赔偿的档次。未来应出台相关司法解释对《个人信息保护法》第69条第2款的法定赔偿数额的上限予以明确规定。

2.预防措施的合理成本

个人信息主体采取预防措施的合理成本是风险性损害赔偿的基本构成部分，也即风险性损害赔偿范围的下限。个人信息主体采取预防措施产生的成本构成风险性损害赔偿中的一部分有其合理性。[①] 有观点认为，应通过法律规定损害赔偿的下限。[②] 然而，通过法律规定风险性损害赔偿的下限，会出现预防措施的合理成本远高于该下限的情形。并且，司法实践中，损害赔偿的下限可以由原告自主决定，无需法律予以明确。比如“孙某诉搜狐等人格权纠纷案”中，原告主张的赔偿数额仅为1元，显然低于涉诉行为的损失，但法院认为原告的主张属于对自己的民事权利和诉讼权利的合法处分，应予以支持。[③] 因此，赔偿下限不应由法律规定，而应根据个案中个人信息主体支出的预防措施的合理成本及诉讼主体的意愿确定最低的赔偿金额。在认定存在风险性损害的前提下，个人信息主体采取预防措施的合理成本可在损害赔偿中获得赔偿。另外，预防措施的合理成本应包括《规定》第12条第1款所规定的调查、取证的合理费用和律师费用。

五、结语

“基于风险的方法”已体现在《个人信息保护法》的具体条款当中。数据泄露损害赔偿也应运用“基于风险的方法”，将高度盖然性的风险认定为《个人信息保护法》第69条第1款项下的损害，以形成完备的个人信息保护之风险路径。实践中，可以出台相关司法解释，明确风险性损害的存在。在没有相关司法解释的情况下，法院审理案件时可根据以上提及的考量因素，有条件地认定风险性损害。“基于风险的方法”修正了传统理论僵化的部分，为风险社会中的个人信息保护提供了理论补充。将风险认定为损害须结合个案判断，目标是在保护个人信息权益与促进数字经济发展之间取得平衡。同时，风险性损害的认定问题有待中国法律实践的进一步探索。

Application of the “Risk-Based Approach” in Data Breach Damages

LIU Ying, HE Mingxin

(Law School & Intellectual Property School, Jinan University, Guangzhou 511443, China)

Abstract: The EU and China have both incorporated the “risk-based approach” into their personal information protection law. This approach emphasizes the concept of risk control of personal information protection, and is embodied in the data protection impact assessment or personal information protection impact assessment. When a data breach occurs, the “risk-based approach” should also be emphasized and applied to individual’s claims for damages, by conditionally identifying risk as damage and evaluating risky damages accordingly. The elements of a “risk-based approach” to evaluating risky damages can be divided into four dimensions including the sensitivity of personal information, the extent to which personal rights and interests may be compromised, the likelihood of harm occurring, and the ways in which personal information may be used. Meanwhile, measuring risky damages should use a personal information risk evaluation matrix. The application of the “risk-based approach” to personal information damages is a need of a risk society and provides a more complete protection of personal information.

Key words: “risk-based approach”; personal information protection impact assessment; data breach; risky damages; risk evaluation matrix

① 参见王益强：《裁判视角下数据侵权损害的认定》，载《华东政法大学学报》2023年第5期，第81页。
② 参见王雪：《个人信息泄露的风险性损害之证成》，载《南大法学》2023年第3期，第190页。
③ 参见北京互联网法院民事判决书，(2019)京0491民初10989号。