法商研究 Studies in Law and Business
Vol. 42 No. 5(2025)

网络与信息法

论数据泄露受害人精神损害的认定

解 正 山*

摘 要:数据泄露不仅意味着受害人失去对其个人信息的控制,而且将导致其遭受不同程度或形式的未来侵害风险。尤其是,与这些风险关联的焦虑、恐惧等负面精神反应还将打破数据泄露受害人原本享有的精神平稳或安宁之状态。鉴于未来侵害风险的真实与否关系到精神损害的存在性与严重性,因此精神损害真实与否的司法审查首先应采高度盖然性标准对数据泄露受害人面临的未来侵害风险进行评估;其次,精神损害"严重"与否的解释论可转向客观合理性标准而非严格的可证实标准,着重对受害人精神损害的真实合理性进行审查。同时,为避免对信息控制者构成过度威慑,数据泄露受害人精神损害的赔偿应具有必要的限度。

关键词:数据泄露 个人信息 精神损害 认定标准

在数字时代,数据已成为一种新型生产要素,内含其中的个人信息正凸显它们独特的商业价值。基于图利等目的,网络黑客经常利用技术手段盗取他人收集、控制的数据。[①] 因此,有学者指出,数据泄露从来都是何时而非是否发生的问题。[②] 不同于物理或人际场景中的传统隐私泄露,本文所称数据泄露是指数字化场景中更广泛的个人信息被未经授权地访问或公开、被破坏、被盗取,进而损及这些信息的机密性、完整性或可用性。通常,传统隐私泄露多表现为直接的隐私侵权,侵害对象多为特定个体,受害人人格权受损为常态,因而精神损害的存在性几无争议,受害人甚至无须对精神损害的严重性进行证明。比较而言,数据泄露尤其是大规模数据泄露的危

* 上海对外经贸大学法学院教授
基金项目:上海市哲学社会科学规划课题资助项目(2024BFX009)

① 本文所称"数据"是指包含个人信息的"数据",不涉及未包含个人信息的其他数据,故在行文中不加区分地使用"数据"与"个人信息"。此外,鉴于"数据泄露"是通用行业术语,因此本文采"数据泄露"之称谓。

② See David W. Opderbeck, Cybersecurity and Data Breach Harms: Theory and Reality, 82 Maryland Law Review, 1006 (2023).

害性与破坏性更为严重:一方面,涉事企业将遭受竞争力受损、[①]名誉损害以及大规模侵权诉讼或巨额的行政罚款等不利影响;另一方面,还将引发一系列社会问题,尤其对个人而言,数据泄露意味着其丧失了对个人信息的控制,这不仅导致他们遭受现实的财产或人身侵害,而且将面临金融欺诈、网络霸凌、信息侵扰、行为操纵等多样的衍生侵害风险,[②]诸如身份盗用等侵害风险甚至将长期存在,这些将令受害人承受更难言明的焦虑、恐惧、不安等无形损害。

不同于财产损失,上述无形的精神不利益是否以及多大程度上能够被认定为法律意义上的精神损害已成为各国在数字时代共同面临的法律难题。首先,不同于传统的隐私泄露,数字化场景中的数据泄露所具有的规模效应、技术依赖性以及衍生侵害的多样性与潜在性等全新特征使得数据泄露受害人的精神损害认定与救济更趋复杂,诸如受害人能否在不提供精神痛苦证据的情况下直接以失去对个人信息控制为由获得赔偿、受害人精神损害在程度上是否一定比源自人身伤害的损害与痛苦轻、是否需设定最低的承认门槛等问题一直悬而未决。其次,包括精神损害在内的非财产损害概念本身就模糊不清,其包含了损害的所有负面后果且在本质上不宜用金钱评估,因而很难找到一种方式精确地描述或定义这类损失。[③] 最后,立法与理论上也存在相互矛盾的趋势,一方面,侵权法更系统地承认非财产损害且不断减少对财产损失的索赔障碍;另一方面,人们也在反思这一趋势的局限性,追问现代侵权法的边界究竟在何处——何种程度的精神损害应给予金钱赔偿?考虑侵权行为或后果的严重性是否正当?是否需要根据受害者的情况来评估损害?[④] 所有这些问题不仅是世界范围内的“司法之问”,而且理论上也颇具争议性。鉴此,本文将以数据泄露受害人精神损害为研究对象,揭示因数据泄露而生之精神损害的特殊本质,旨在破解此类精神损害认定难题,以回应精神损害赔偿这一个人信息权益保护中的疑难问题。

一、数据泄露与受害人精神损害

一般认为,个人信息的本质关乎个人的自由、尊严与隐私等人格权益。因此,授权个人控制自己的信息已成为个人信息保护法的基本原则。显然,数据泄露特别是泄露后的数据滥用行为有违“信息自决”,不仅意味着受害人失去对其个人信息的控制,而且使附着在个人信息之上的个人尊严、自由与安全陷入某种失控或不安全状态。对于这些侵害,受害人往往束手无策,唯有担忧、焦虑与不安;一旦侵害真实发生,除了可能的直接财产损失,受害人原本的精神不安宁或情绪困扰恐将雪上加霜。

(一)数据泄露导致即时侵害或未来侵害风险

数据泄露事件发生后,其侵害性首先表现为受害人丧失对其个人信息的控制。经由“同意”

① 参见金元浦:《大数据时代个人隐私数据泄露的调研与分析报告》,《清华大学学报》(哲学社会科学版)2021 年第 1 期。

② See Ido Kilovaty, Psychological Data Breach Harms, 23 North Carolina Journal of Law & Technology, 12 (2021).

③ See Jonas Knetsch, The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases, 13 Journal of European Tort Law, 135 (2022).

④ See Jonas Knetsch, The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases, 13 Journal of European Tort Law, 136 (2022).

这一基本原则，信息主体因而得以实现对其个人信息的“控制”。这也意味着把是否以及如何让渡其个人信息的决定权交予信息主体自己。因此，作为一种不法获取、公开、传播个人信息或以破坏、删除等其他方式侵害个人信息的方式，数据泄露显然妨碍了信息主体对其个人信息的“控制”。其次，数据泄露后，受害人遭受了即时的财产或人格权侵害。主要表现为以下几种情形：(1)实际发生了身份盗用、金融诈骗等衍生侵害行为，导致受害人蒙受直接财产损失或间接的人身损害，包括因防范身份盗用而支出的监控与预防费用以及因信用受损而丧失的交易机会等。2020年，河南郑州、陕西西安、湖北武汉等地多所高校数以千计学生的敏感个人信息泄露，其中，很多受害学生发现他们的身份信息被陌生公司用于偷税。① “徐玉玉案”②则进一步表明，数据泄露不仅导致受害人身份被冒用或金钱损失，而且可能导致少数受害者因蒙羞、愧疚或自责难过而选择轻生。(2)数据泄露后，不法行为人将偷盗或以其他不当手段获取的个人信息公之于众，以达羞辱或恐吓等不法目的，③致使受害人遭受隐私信息公开与生活安宁被侵扰等传统隐私权损害或在与他人的交往中遭受不当的“预测、影响甚至操纵”乃至隐性歧视等新型的隐私权损害或一般人格权损害。④ (3)遭泄露的个人信息被直接用于侵害当事人的生命权或身体权。⑤ 最后，在更多情形下，遭泄露的个人信息虽然未被即时滥用，但是未来以其为媒介侵害当事人权益的风险将显著增加。这与个人信息的本质——个人信息的有机组合能够塑造信息主体的数字人格——密不可分。一条条看似无关紧要的个人信息往往潜藏着自然人人格尊严、自由以及人身与财产安全等多元利益，更不用说那些与人身或财产关系重大的私密或敏感个人信息了。这些个人信息一般具有人身专属性，一旦泄露，受害人很难通过更改等方式阻止这些信息继续流转或被使用，这也意味着遭泄露的个人信息即便未被即时滥用，也可能在未来数月或数年内被滥用。社会与经济生活的数字化以及数据滥用形式的多样化将放大未来的侵害风险。一旦条件成熟，这些风险将转化为现实侵害，受害人将遭受不利影响。

(二)数据泄露衍生侵害导致受害人人格减损

数据泄露后，受害人一旦遭遇金融诈骗与隐私侵犯等现实侵害，随之而来的愤怒、尴尬乃至焦虑等精神不利益不难想象，这是普通人自然而然的反应。类似地，个人信息因泄露而遭扩散或在未来被滥用，无论这些信息看上去多么微不足道，也可能损及受害人的人格构建能力，而且还将对他们的选择自由构成某种程度的限制。⑥ 最终，受害人的人格“完整性”将因此受到损害。这些无形损害主要表现为受害人因未来侵害风险增加而产生焦虑、恐惧、不安、压力感等精神痛苦或情绪困扰。这是因为：当人们有合理理由怀疑自己的人身或财产因数据泄露而处于某种风

① 参见《盘点2020上半年全球重大数据泄露事件》，https://www.isccc.gov.cn/xwdt/xwkx/07/903972.shtml，2022－11－16。

② 参见山东省临沂市中级人民法院(2017)鲁13刑初26号刑事判决书。

③ See Jay P. Kesan and Carol M. Hayes, Liability for Data Injuries, 2019 University of Illinois Law Review, 302 (2019).

④ 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》，《法律适用》2022年第1期。

⑤ See Danielle Keats Citron and Daniel J. Solove, Privacy Harms, 102 Boston University Law Review, 832 (2022).

⑥ See Stephan Mulders, The Relationship Between the Principle of Effective Under Art. 47 CFR and the Concept of Damages Under Art. 82 GDPR, 13 International Data Privacy Law, 172 (2023).

险之中且难以有效化解时,自然会产生普通人很容易感同身受的恐惧或焦虑,即便不涉及令人尴尬或有失颜面的个人信息,也同样能以多种形式导致当事人精神利益受损。毕竟,现今对个人进行“数字画像”已非难事。对普通人而言,生活在诸如此类的被“计算”的阴影之中,自然也会对未来交易、获得就业机会或参与其他重要活动时可能受阻而深感忧虑。① 根据精神障碍诊断的一般标准,上述不良的精神或心理反应可被归类为精神障碍症状,只是由于在不少情形下它们并不那么严重或持久从而不足以被诊断为严重的精神障碍或精神疾病而已。②

上述不利后果并非只是理论演绎,精神病学与心理学领域的实证研究也支持这一结论。有研究表明,一旦遭遇身份盗用或欺诈,数据泄露受害人遭受的不利影响并不限于经济损失,他们还将因被欺诈或被冒犯而感到尴尬、羞愧、自责,甚而产生焦虑、抑郁、创伤后应激障碍或与家人及朋友的关系陷入紧张状态。③ 尤其是,与年轻一代相比,老年人拥有较多财富,因而更易遭遇网络诈骗等侵害行为。对这些无法通过就业弥补损失或无法获得适时指导的老人而言,一旦个人信息泄露超出控制范围,他们将承受更普遍、更不利的经济和精神后果。④ 另一份专门针对老年人身份盗用的研究进一步表明,滥用个人信息的不利影响大大超出直接经济损失,与样本中 7%的老年受害者遭遇经济损失相比,高达 34%的受害人经历了中度至重度的精神痛苦或情绪困扰,其中,被骗的钱越多,无论损失最终能否追回或得到补偿,精神痛苦的可能性就越大,尤其在犯罪行为被发现之前,个人信用被滥用的时间越长,后续财务与信用问题就越多,解决问题耗费的时间就越长,精神痛苦可能性就越大。⑤ 如何将这些事实上的精神损害转化为法律上的损害是价值判断与法律评价问题。

在学理上,一般认为损害是民事赔偿责任必备的要件且应具有确定性与可赔偿性。基于这一标准,有学者指出,数据偷盗者利用被盗个人信息牟利且使个人权益受损的推断言过其实甚至是错误的,而且“安全减损因缺乏人格权利损害因而不能主张精神损害赔偿”,因为:(1)大多数遭泄露的个人信息不会被用于真正的身份盗窃或信用卡诈骗,而是被用于与真人无关的合成身份欺诈或用于间谍活动等目的,或者,数据泄露虽然增加受害人权利受损风险,但是权利损害与否最终取决于风险发生与否;(2)在多数情形下,当个人遭受真正的身份欺诈或金融诈骗时,涉事企业即会根据法律要求或合同约定迅速纠正问题,数据泄露受害人无须承担任何费用,虽然数据泄露可能导致当事人产生某种程度的焦虑、不安,但是其难以证明或量化,因此与风险及焦虑相关的责任理论无异于一种绝对的企业责任,毕竟,这个世界从来都不是绝对安全的,这也是侵权法

① See Daniel J. Solove and Danielle Keats Citron, Risk and Anxiety: A Theory of Data Breach Harms, 96 Texas Law Review, 765 (2018).

② See Stephan Mulders, The Relationship Between the Principle of Effective Under Art. 47 CFR and the Concept of Damages Under Art. 82 GDPR, 13 International Data Privacy Law, 172 (2023).

③ See M. Button et al., Not a victimless crime: The impact of fraud on individual victims and their families, 27 Security Journal, 36−54 (2014); Marguerite DeLiema, The Financial and Psychological Impact of Identity Theft Among Older Adults, 5 Innovation in Aging, 1−11 (2021).

④ See Marguerite DeLiema, The Financial and Psychological Impact of Identity Theft Among Older Adults, 5 Innovation in Aging, 1−11 (2021).

⑤ See Yuan Li et al., Responding to identity theft: A victimization perspective, 121 Decision Support Systems, 13−24(2019); Marguerite DeLiema, The Financial and Psychological Impact of Identity Theft Among Older Adults, 5 Innovation in Aging, 1−11 (2021).

本身所极力避免的;(3)生活中类似风险增加引发焦虑之情形不胜枚举且可能更加严重,如果承认风险引发的焦虑等不利益之状态为精神损害,那么将不仅助长当事人投机或滥诉,而且是对法院自由裁量权的恣意扩大,势必偏离损害赔偿法上实质损害这一核心要求。① 这些理由并未从损害本身入手,只是基于滥诉风险或侧重于社会视角考虑承认数据泄露精神损害的负面影响。而且,这些学者并未注意到数据泄露与实物失窃之间的本质差异,实物或许可追索返还,但个人信息可被快速复制和传播,从而难以"返还"给受害人,②其内含的多元人格利益所面临的侵害风险也就无法通过追回个人信息予以化解。因此,数据泄露后,受害人即便未遭受实际财产损失或其他形式的侵害后果,也将面临显而易见的精神或心理上的不利益。

本质上,数据泄露特别是其衍生的未来侵害风险导致受害人遭受的焦虑、恐惧等负面及纷乱的精神或心理反应势将打破当事人原本享有的精神平稳与安宁之生活状态,这与隐私或名誉侵权等产生的精神损害并无根本不同,它们均可独立存在且对个人人格"完整性"而言都至关重要,所不同者在于个案中表现出的程度相异而已。因此,认为"风险引发的焦虑不属于侵权法中的精神损害""安全减损因缺乏人格权利损害而不能主张精神损害赔偿"③之观点是值得商榷的:(1)并非只有具体的人格权受侵害时才会产生精神损害,其他属于人身权益范畴但尚未被具体化的人格利益受侵害同样会产生精神损害且具有可保护性与可赔偿性;(2)无论是因身体侵权产生的精神损害,还是非因身体侵权产生的精神损害,都具有主观性这一特征,因此该学者认为"将焦虑这一主观感觉认定为精神损害将造成法律秩序的混乱"的论断忽视了风险引发的焦虑与恐惧等精神不利益状态的严重与否分析,且不应因存在可能的滥诉而否认精神损害本身。

因数据泄露而产生的精神损害具有无形性与主观性且呈分散性与风险导向,它既不像身体伤害那般具有明显外观从而让目击者对受害人精神痛苦感同身受,也不像财产损失那般易于识别与评估。正是这些特点导致它们在理论或实践中要么被忽视、要么被认为微不足道。但事实上,这些人格损害"就像是一间拥挤小屋里的那件隐形物品,人们或许无法看见它,但总能清楚地感知它,且因它的存在而改变自己并设法躲避"。④ 总之,数据泄露更多关乎"人"而非"物",⑤其后果多是间接的或只是精神与心理方面的影响,这将导致法院认定它们时宛如"走钢丝"。

二、数据泄露受害人精神损害的"真实性"审查

不可否认,因数据泄露而生的精神损害并不比衍生自人身伤害的精神损害更具客观性。但

① See Jackson Erpenbach, A Post－Spokeo Taxonomy of Intangible Harms, 118 Michgan Law Review, 478 (2019); David W. Opderbeck, Cybersecurity and Data Breach Harms: Theory and Reality, 82 Maryland Law Review, 1004－1005, 1030－1031 (2023);贺彤:《安全作为个人信息保护的法益》,《财经法学》2023 年第 3 期。

② See Jon L. Mills and Kelsey Harclerode, Privacy, Mass Intrusion, and the Modern Data Breach, 69 Florida Law Review, 817 (2017).

③ 贺彤:《安全作为个人信息保护的法益》,《财经法学》2023 年第 3 期。

④ Daniel J. Solove and Danielle Keats Citron, Risk and Anxiety: A Theory of Data Breach Harms, 96 Texas Law Review, 756 (2018).

⑤ See Jay P. Kesan and Carol M. Hayes, Liability for Data Injuries, 2019 University of Illinois Law Review, 336 (2019).

生活经验告诉我们,对潜在侵害风险的担忧或恐惧也是人之常情。因此,如何对这些“损害”事实进行法律评价关乎每个参与数字生活的当事人的权益保护。

(一)未来侵害风险宜视作损害事件而非损害本身

学理上,如何对未来侵害风险进行法律评价存在较大争议。有学者主张将未来侵害风险本身视为与侵权法上财产损害与精神损害并列的第三类损害,理由包括:(1)在可行性上,损害的“差额说”经“规范说”修正后可将特定条件风险纳入侵权法上可予赔偿之损害;(2)在必要性上,将“风险损害”纳入侵权法框架有助于风险预防与治理,彰显侵权法的威慑功能,这不仅是“风险分配的具体实现方法”,也可将行为人侵权行为成本“内化”。① 相反,也有学者强烈质疑“风险损害”的确定性,虽然他们并不否认数据泄露会导致未来侵害风险,但是认为风险本身不具有损害应具备的确定性,除非遭泄露的个人信息被滥用且产生现实的人身或财产侵害,否则,不存在所谓的损害赔偿责任。他们认为:(1)“风险损害论”本身存在逻辑不自洽之处,其一方面将未来侵害风险本身视为损害时,另一方面又将受害人为防范风险而支出的费用以及因风险引发的内心焦虑视为“风险损害”的赔偿范围,但事实上,后两种后果本身已然是真实损害而非风险本身了;(2)承认所谓的“风险损害”可能抑制行为自由,且可能因不具备因果关系之基础而构成惩罚性赔偿,造成过度威慑。② 另有一些公法学者甚至认为,仅当数据泄露侵害后果已迫在眉睫或已造成实际损失,民法上的私人诉讼机制方能发挥作用,对未来侵害风险的规制以及对尊严法益的维护则应交由公法调整,采公共执法为宜,不应过于扩张侵权法上的损害范围。③

笔者认为,“风险损害论”混淆了风险本身与其所引发的焦虑等不利后果,忽略了两者之间的因果逻辑关系。正因如此,“风险损害论”不得不把本可独立求偿的财产损失(当事人为防范风险而支出的费用)与精神损害(当事人因风险而产生的焦虑等)视为“风险损害”的赔偿内容。比较法上,不少域外法院承认的损害并非未来侵害风险本身而是与风险密切相关的其他人格权益损害。例如,美国联邦最高法院在审查是否存在“损害”时就特别强调:“真实的”损害并非一定有形,无形损害甚至是“真实损害的风险”只有与传统上作为诉讼基础的“损害”——名誉损害、私密信息被披露、不当侵入私人生活等——具有紧密关系时才可被认定为真实的、具体的“事实上的损害”。④ 更重要的是,“风险损害”还面临如何融入我国现有损害框架的困境,尤其是如何从理论上实现对我国民法现有财产损害与精神损害二元区分体系的突破?

数据泄露与其下游侵害或未来侵害风险之间存在着因果关系,两者之间既不“遥远”,也不仅仅是推测,司法上多有承认此种风险真实性的裁判。所谓侵权人承担的巨额赔偿本身并非等同于惩罚性赔偿,因为数据泄露往往涉及人数众多的受害人,即便是小额赔偿也可能累积成不成比例的巨额赔偿,为避免不成比例的损害赔偿,完全可在制度设计上考虑采取损害赔偿限制或替代

① 参见田野:《风险作为损害:大数据时代侵权“损害”概念的革新》,《政治与法律》2021 年第 10 期;朱晓峰、夏爽:《论个人信息侵权中的损害》,《财经法学》2022 年第 4 期;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》,《国家检察官学院学报》2022 年第 5 期。

② 参见谢迪扬:《侵权抑或不当得利:个人信息泄露的民事救济路径之辨》,《北京理工大学学报》(社会科学版)2024 年第 2 期;程啸、曾俊刚:《个人信息侵权的损害赔偿责任》,《云南社会科学》2023 年第 2 期。

③ 参见王锡锌:《个人信息权益的三层构造及保护机制》,《现代法学》2021 年第 5 期;王道发:《个人信息处理者过错推定责任研究》,《中国法学》2022 年第 5 期。

④ See Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016); TransUnion LLC v. Ramirez, 141 S. Ct. 2190 (2021).

措施。若只承认现实人身或财产损害甚至主张采用行政执法等公法救济应对数据泄露导致的下游侵害风险，则将阻滞私人诉讼，不仅忽视了数据泄露所致诸多无形不利后果的客观事实，而且也未意识到数字时代新型权益侵害的特殊治理需要。公法救济固然重要，但其与民法上的私人诉讼并非相互排斥，两者也非“二选一”关系，它们均有自身不足。针对数据泄露尤其是大规模数据泄露，两者协同应能发挥最大效用。

一般而言，如果未来侵害风险已经转化为现实侵害，那么数据泄露受害人将遭受实际的财产损失或人身损害。这些实际侵害导致受害人精神利益减损已为不少实证研究证实。此时，精神损害评估重点转向“严重性”审查即可。未来侵害风险不确定于何时或是否发生的情形大可不必纠缠于风险本身是否构成损害的理论纷争。其实，根据侵权损害赔偿责任中“损害事件”与“法律上可计算并予以赔偿的损害”相区分原理，数据泄露实为侵害行为，侵害的客体主要是依附于个人信息的人格权益，因其而产生的未来侵害风险则可视为“损害事件”——类似于人身侵权中诸如殴打等侵害行为所造成的具体人身伤害，[①]数据泄露受害人因该“损害事件”而遭受的精神痛苦或支付的预防风险费用才是更值得考虑是否应予赔偿的损害。此时，可将未来侵害风险视为数据泄露侵害行为的有机组成部分予以“整体”审查，并将审查重点转向数据泄露衍生的未来侵害风险的客观性与急迫性，进而对受害人精神平稳或精神安宁因该“损害事件”产生的减损或变化进行真实性与严重性评价。实践中，我国已有法院通过对未来侵害风险等级或现实性进行评估从而对受害人精神损害进行审查。[②] 其实，上述区分也与我国现有立法一般原则相一致。无论是《中华人民共和国民法典》（以下简称《民法典》）第1165条第1款、第1183条第1款，还是《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条第1款，均将“权益侵害”要件化，[③]并将其与“损害”进行明确的区分，其中，后者是侵权损害赔偿的附加构成要件。

（二）与风险相联系的精神损害真实与否的审查要素

1.不同的风险审查标准对精神损害真实性认定的影响

实践中，数据泄露受害人常以未来侵害风险的增加导致恐惧、焦虑、不安等为诉由向信息控制者等行为人提出索赔。不可否认的是，未来侵害风险增加与受害人精神利益减损高度相关，未来侵害风险仅是臆测还是真实存在关乎受害人精神损害的真实性判断。对于未来侵害风险，司法上形成了偏向保守的“确已迫在眉睫”标准与偏向开放的“客观合理的可能性”标准。“确已迫在眉睫”标准初见于美国“克拉珀案”。[④] 在该案中，针对原告诉称的重大监控风险这一所谓的未来损害，美国联邦最高法院强调，原告并无证据证明其所担心且未来可能产生的损害已在事实上产生或即将产生。这一标准后被适用于数据泄露侵权纠纷中，美国部分联邦巡回法院还进一步丰富了它的内涵。在“雷利案”[⑤]中，原告声称数据泄露增加了他们身份被盗风险且为此焦虑不堪。对此，法院认为，成为身份盗窃或诈骗受害人仅仅是当事人的臆测，原告为避免身份被冒用或被诈骗而支出的费用则是基于其所臆测的加害行为。鉴于原告个人信息并未被实际用于身份

① 参见张博文：《论个人信息泄露下游侵害风险的损害赔偿》，《南大法学》2023年第6期。

② 参见山东省济宁市任城区人民法院（2022）鲁0811民初1961号民事判决书。

③ 参见龙俊：《权益侵害之要件化》，《法学研究》2010年第4期。

④ See Clapper v. Amnesty International USA, 133 S.Ct. 1138 (2013).

⑤ See Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011).

盗窃或欺诈,因此法院认为并不存在“事实上的损害”(包括精神痛苦)。美国其他一些法院也认为,数据泄露造成的所谓损害通常都建立在当事人推测或假定基础之上,过于依赖主观上的担忧与焦虑,与那些已经发生或即将发生的损害相差甚远。① 正如美国新泽西联邦地区法院所指出的,由于索赔人对未来身份盗窃或诈骗的担忧建立在其遭泄露的个人信息将被恶意使用这一假设性结论之上,因此根本就没有合理的事实能够佐证原告所主张的精神痛苦,包括焦虑、担心成为受害人、被骚扰或遭遇尴尬等。② 还有法院认为,即使未来侵害风险足以引起某种焦虑且它们合理存在,受害人也无法仅就该风险或因此产生的精神痛苦提出索赔,除非遭泄露的个人信息被滥用的风险迫在眉睫,否则,受害人承受的精神痛苦等就不足以构成损害,且在因果关系链条上,受害人因未来侵害风险增加而产生的恐惧、焦虑等实在是过于遥远。③

与美国判例法类似,欧盟早期判例法对于精神损害等非财产损害,一般也要求该损害应是实际而确定的,纯粹假设性和不确定的损害无法获得赔偿,仅仅声称某行为“深深伤害了索赔人并给其造成相当大压力”被认为不足以构成可予赔偿的非财产损害,除非这些损害已迫在眉睫且足可预见。④ 不难看出,“确已迫在眉睫”要求索赔人证明其遭受了实际损害,包括身体损害、财产损失或精神损害等,它们应是“具体的、特定的”“实际或即将发生而非推测或假定的”。⑤ 表面上,若受害人能够证明存在这样的急迫风险,那么法院就将承认这些“未来损害”,但“确已迫在眉睫”或存在这样的重大风险之审查标准对于受害人而言过于苛刻,恐将挫败几乎所有基于对未来侵害的恐惧而提出的赔偿请求,从而大大减少当事人提起诉讼或获得救济的机会。⑥ 总之,“确已迫在眉睫”标准不仅不利于受害人利用私法手段维权,而且会对潜在侵权人构成错误激励。比较而言,“客观合理的可能性”标准对数据泄露受害人更友好。该标准并非基于遭泄露个人信息已被实际用于欺诈等现实侵害进行审查,而是把这些信息未来被滥用是否具有合理的可能性作为审查关键。实践中,法院主要根据个案中具体因素的动态评估从而对是否存在损害进行审查。例如,在“瑞米贾斯案”⑦中,审理法院即根据个人信息滥用情况、行为人主观目的、数据泄露后的安全防范措施得当与否等因素认定未来侵害风险具有客观合理的可能性。在德国发生的一起案

① See Peters v. St. Joseph Servs. Corp., 74 F. Supp. 3d 847 (S.D. Tex. 2015); Storm v. Paytime, Inc., 90 F. Supp. 3d 359 (M.D. Pa. 2015); In re Horizon Healthcare Servs., Inc. Data Breach Litig., No. 13-7418 (CCC), 2015 WL 1472483 (D.N.J. 2015).

② See Crisafulli v. Ameritas Life Ins., No. 13-5937, 2015 WL 1969176 (D.N.J. 2015).

③ See Amburgy v. Express Scripts, Inc., 671 F. Supp. 2d 1046, 1053 (E.D. Mo. 2009); In re Barnes & Noble Pin Pad Litig.,2013 WL 4759588 (N.D. Ill. Sept. 3, 2013); In re Sci. Applications Int'l Corp. Backup Tape Data Theft Litig., 45 F. Supp. 3d 14, 26 (D.D.C. 2014).

④ See Stephen Mulders, Collective Damages for GDPR Breaches: A Feasible Solution for the GDPR Enforcement Deficit?, 8 European Data Protection Law Review,502 (2022).

⑤ TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2203 (2021).

⑥ See Thomas Martecchini, A Day in Court for Data Breach Plaintiffs: Preserving Standing Based on Increased Risk of Identity Theft after Clapper v. Amnesty International USA, 114 Michigan Law Review, 1480 (2016); Jason S. Wasserman, Stand in the Place Where Data Live: Data Breaches as Article III Injuries, 15 Duke Journal of Constitutional Law & Public Policy Sidebar, 202 (2020).

⑦ Remijas v. Neiman Marcus Gorp., 794 F.3d 688, 693 (7th Cir. 2015).

例中，[①]审理法院也认为，虽然无证据表明涉案数据已被用于欺诈目的，但是因涉案个人信息敏感且范围广泛从而认定数据泄露对原告造成的影响已非对个人权利微不足道的侵犯，仅身份盗窃的风险便足以使原告就其遭受的焦虑与痛苦等提出精神损害赔偿。

鉴于数据泄露衍生侵害的未来性与隐蔽性，焦虑或恐惧等更多的是受害人遭受的主要损害。在多数情形下，这些人格利益减损都是真实而具体的，时常发生的网络霸凌或诽谤以及电信诈骗等侵害事件给当事人造成的伤害或痛苦就是例证。与个别当事人信息泄露相比，大规模数据泄露的负面影响更广泛，不仅当事人面临现实或潜在侵害，甚至整个社会都将为此付出代价。就此而言，不宜对数据泄露受害人的损害证明设置过高或过严标准，更不应等到未来侵害风险转变为现实侵害后才考虑向他们提供救济。否则，无异于将本应由危险制造者承担的风险转嫁给了弱势的数字消费者，这样既忽视了数字空间风险所具有的未来性、无形性、扩散性等特性，也不符合风险分配正义。因此，宜客观合理地认定未来侵害风险进而对数据泄露受害人因此经受的焦虑、恐惧等精神不利益进行法律评价。一旦认定未来侵害风险具有高度盖然性，那么受害人因数据泄露而产生的精神痛苦或情绪困扰也就具有了合理性与真实性。其后，即可转向对此类精神损害是否满足立法上设定的“严重”这一程度要求进行判断。如此，既可防止信息控制者等行为人将自身责任风险外化为个人或社会责任，也能更好地保护那些积极参与数字化生活的当事人，从而促进数字生态可持续发展。

2.数据泄露受害人精神损害真实性审查的具体考虑要素

实践表明，证明未来侵害风险的确定性对数据泄露受害人而言是个沉重的负担。因此，为公平起见且兼顾数字行业可持续发展利益，可在个案中根据具体情形对受害人因数据泄露而面临的未来侵害风险的等级或现实性以及与其关联的精神损害真实合理与否进行审查。

第一，应考虑遭泄露的个人信息是否私密或敏感以至于个人将遭受身份盗用或欺诈等未来侵害的高风险。通常，个人信息类型将在很大程度上决定数据泄露受害人可能面临的损害及程度。[②]《民法典》第1034条与《个人信息保护法》第28条已将个人信息区分为一般个人信息与私密信息或敏感个人信息。若是私密信息泄露或遭其他形式的违规处理，那么基于隐私权保护一般法理，受害人产生精神损害自是题中之义。对于敏感个人信息，其泄露虽然不一定涉及隐私侵权，但是会让受害人人格尊严、人身或财产面临的侵害风险陡然升高。“阿蒂亚斯案”[③]表明，诸如社会安全号码与出生日期等高风险信息，尤其当它们与姓名关联在一起时，将使当事人更可能成为身份盗窃或欺诈的潜在受害者。相反，若风险等级较低的非敏感个人信息泄露，往往不会导致当事人面临显著的未来侵害风险，因而一般就不会有所谓的损害了。[④] 对个人而言，私密或敏感个人信息的人格或财产意义重大。更重要的是，诸如生物识别、宗教信仰、医疗健康等信息很难在其泄露后通过更改等方式防范未来被滥用风险。因此，个人信息一旦泄露，受害人深陷焦虑或担惊受怕也就再自然不过了。此种情形下，不宜将其遭受的精神利益减损视为应予容忍的一

① See LG München I, Urteil vom 9. Dezember 2021－31 O 16606/20.

② See John E. McLoughlin, Standing in the Age of Data Breaches: A Consumer－Friendly Framework to Pleading Future Injury and Providing Equitable Relief to Data Breach Victims, 88 Brooklyn Law Review, 952 (2023).

③ See Attias v. Carefirst, Inc., 865 F.3d 620 (D.C. Cir. 2017).

④ See Whalen v. Michaels Stores, Inc., 689 F. App'x 89 (2d Cir. 2017).

般负面情绪。

第二,应考虑泄露的数据是否已被滥用或者是否有其他当事人因数据泄露而遭受了实际侵害,从而进一步判断未来侵害风险的现实性并据此判定精神损害的真实性。实践表明,受害人虽然无法证明自己因数据泄露而遭受实际侵害,但是如果能证明同一数据泄露事件中其他受害人个人信息被滥用,那么法院将可认定其已面临未来侵害的重大风险。① 同样,若有证据表明原告个人信息已被以其他形式滥用(如在暗网上出售),即使尚未发生实际的身份盗用,则也能支持原告已经面临身份盗用或欺诈的重大风险的结论。②

第三,应一并考虑数据泄露的方式、影响范围以及网络偷盗者的意图。如果是无意间且在有限范围内泄露个人信息,而且行为人事后采取了积极的补救措施,那么通常不会产生显著的负面后果,无论是风险本身还是其衍生的精神损害都显得极为轻微。例如,在"麦克莫里斯案"中,因只向内部员工发送错误邮件而无意中泄露了当事人个人信息,故法院拒绝认为此种限于内部的数据泄露会造成重大的次生侵害风险。③ 相反,若能证明第三方基于某种恶意而盗取他人控制的个人信息,那么当事人遭受身份盗窃或欺诈等未来侵害的风险将显著增加,④此时,他们为此而焦虑或担心不已就不应简单地被视为臆测或推断的了。"邓某某诉顺丰案"⑤进一步表明了数据泄露后受害人面临的未来侵害风险的现实性。可见,当欺诈或恶意的证据足可表明受害人将受到严重影响时,精神损害也就显而易见了。⑥

比较而言,个人信息类型是相对客观且容易确定的,而且在立法上也提供了此种分类的依据。这也是多数法院将其作为数据泄露后评估潜在危害的决定性因素的重要原因。但不可否认的是,黑客意图与实际滥用等考虑因素则存在某些不确定性。或有人质疑:如何确定黑客意图?如何确定已发生的数据滥用源自本次数据泄露?对此,笔者认为,很难想象黑客基于善意而盗取他人控制的个人信息,只不过是盗取个人信息后滥用形式或滥用时间不同而已。这与"麦克莫里斯案"中行为人无意间泄露他人个人信息具有本质差异。无论哪种形式的滥用,对数据泄露受害人而言,均意味着他们可能面临着某种形式或某种程度的权益侵害风险。至于实际滥用与数据泄露的相关性问题,其本质是信息控制者的可归因性或可归责性。实践中,存在"唯一性"与"高度可能性"两种司法判定标准:前者不仅要求受害人证明数据泄露环节的"唯一性",而且还要求他们证明信息控制者的过错;⑦后者并不要求受害人证明确实是信息控制者泄露了他的个人信息,而仅要求证明信息控制者存在泄露个人信息的高度可能即可,即只要受害人能够证明其向信

① See In re Zappos.com, Inc., 888 F.3d 1020, 1027 (9th Cir. 2018); McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 301 (2d Cir. 2021).

② See Fero v. Excellus Health Plan, Inc., 304 F. Supp. 3d 333, 341, 344－45 (W.D.N.Y. 2018); McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295,302 (2d Cir. 2021).

③ See McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295 (2d Cir. 2021).

④ See Remijas v. Neiman Marcus Grp. LLC, 794 F.3d 688, 693 (7th Cir. 2015); McMorris v. Carlos Lopez & Assocs., LLC, 995 F.3d 295, 301 (2d Cir. 2021).

⑤ 参见北京市第三中级人民法院(2020)京 03 民终 2049 号民事判决书。

⑥ See Michael Reed v. Alex Bellingham [2022] SGCA 60.

⑦ 参见江苏省南京市中级人民法院(2016)苏 01 民终字第 3947 号民事判决书、广东省广州铁路运输中级法院(2017)粤 71 民终字第 11 号民事判决书。

息控制者提供了个人信息且其遭受了与此相关的侵害事实即达到盖然性标准,[①]从而将个人信息到底由谁泄露的证明责任转由信息控制者承担。鉴于个人与信息控制者在技术能力与数据权力等方面存在的巨大鸿沟,因此由占据控制或支配地位的信息控制者负责证明数据到底是如何被泄露的或其本身是否存在疏忽显然更具合理性与正当性,较之于个人,它们更有能力且只需较低成本便能证明其是否存在过失或其过失并非原告受侵害的原因。在立法上,《个人信息保护法》第 69 条第 1 款已确立并强化了信息控制者的此种证明责任。

三、数据泄露受害人精神损害的“严重性”认定

(一)受害人精神损害“严重”与否的裁判分歧

对于精神损害程度或门槛的要求,各国的立场大相径庭。例如,我国要求受害人遭受的非财产损害尤其是精神损害应达到“严重”程度。首先,在立法上,根据《民法典》第 1183 条第 1 款的规定,精神损害赔偿应满足“严重”这一程度要件;其次,在司法上,针对索赔人声称的心理压力或困扰等精神不利益,即便法院承认数据泄露对受害人精神安宁或生活安宁构成负面影响从而间接承认存在精神损害,但如果受害人无法证明其严重性,那么他们的损害赔偿请求很难获得支持。[②] 在这些法院看来,受害人声称的精神损害过于主观,若无临床病症或直接的身体或精神表现即予承认并赔偿,恐将导致道德风险或妨碍行为自由。英国也有法院持类似立场。例如,在“沃伦案”[③]中,法院就强调,数据泄露受害人的焦虑状态并未达到临床上可识别的精神疾病,因而不足以构成损害赔偿的完整诉因。对于严重程度的坚持也是奥地利法院的立场之一。例如,在“奥地利邮政案”[④]中,原告认为被告利用其个人信息推断其政治偏好导致其极度不安、信心丧失并有一种暴露于世的感受,因而提起损害赔偿之诉。对此,奥地利维也纳地区法院与高等法院均以原告声称的不良情绪未达到一定的严重程度为由从而拒绝判令赔偿。总之,在上述法院看来,若无法证明精神损害达到了最低门槛或者它们本就微不足道,那么当事人便无权获得相应的损害赔偿。

还有一些法院则宽容得多,甚至有部分国家(如法国与比利时)的法院将以损害没有达到一定的实质性程度为由而拒绝损害赔偿的做法视为异端。[⑤] 还有法院强调,仅仅是损害无法被准确描述或其范围相对较小等情形均不应成为拒绝赔偿的理由。[⑥] 因《欧盟通用数据保护条例》(以下简称《条例》)第 82 条中“损害”的概念相对模糊,加之,根据欧盟法一般原理,除非违反等效性和有效性原则或欧盟法已对损害作了具体规定,否则,损害概念应根据成员国法律进行解释,

① 参见四川省成都市中级人民法院(2015)成民终字第 1634 号民事判决书、北京市第一中级人民法院(2017)京民终字第 509 号民事判决书。

② 参见北京市第三中级人民法院(2020)京 03 民终 2049 号民事判决书、贵州省贵阳市中级人民法院(2021)黔 01 民终 975 号民事判决书。

③ See Warren v. DSG Retail Ltd. [2021] EWHC 2168 (QB) (July 30, 2021).

④ See Case C-300/21, UI v. Österreichische Post AG [2023].

⑤ See Jonas Knetsch, The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases, 13 Journal of European Tort Law, 143-144 (2022).

⑥ See Rechtbank Noord-Nederland, 15-01-2020, C / 18 / 189406 / HA ZA 19-6.

故欧盟各成员国法院对数据泄露或滥用所导致的非财产损害(精神损害等)的认定也存在明显分歧。实践中,《条例》第 82 条规定的损害赔偿在解释或适用上存在如下疑义:(1)受害人是否须因数据泄露或滥用行为遭受具体损害才有权获得赔偿;(2)受害人因数据泄露或未来某种形式的数据滥用而产生的焦虑、恐惧等情绪能否构成应予赔偿的非财产损害,是否应以违法行为的后果或影响达到一定严重程度作为承认此种损害的前提;(3)损害赔偿的功能仅限于补偿还是兼具惩罚或威慑;(4)信息处理者责任在何种情形下可得豁免。① 对各成员国法院关于非财产损害认定的分歧或疑义,欧盟法院在“奥地利邮政案”中作了部分回应,强调无论是财产损害还是非财产损害,均无严重程度之门槛要求,且欧盟数据保护立法意旨也倡导从宽解释损害;相反,若限于严重程度的损害,如要求受害人证明其遭受了可识别的精神疾病,则不仅与立法者支持的广义损害概念相矛盾,也将导致成员国法院裁判上的不一致,从而违背数据保护法所追求的为个人提供一致和高水平保护这一政策目标。作为对成员国法院提出的恐惧等能否构成非财产损害的疑义的回应,欧盟法院解释道:“信息主体因第三方违反数据保护条例规定可能滥用其个人信息而产生的恐惧或焦虑可构成非财产损害”。② 这也是欧盟法院对《条例》“序言”第 85 条规定的宽泛“损害”的司法确认。不过,欧盟法院同时指出,虽然不宜对损害认定设定严重程度之门槛,但是受害人仍须证明其因不法数据行为而遭受某种不利后果或影响。这意味着欧盟法院并未将违反条例的侵害行为本身等同于损害。事实上,个人或集体提出的损害赔偿已被视为一种有效的数据保护规则的私人执行工具,这自然要求对包括精神损害在内的非财产损害作广义解释。③ 不少欧洲国家法院遵从这一立场,为与欧盟条例的立法旨意相一致,从而放宽了“损害”的认定标准。即便是采取严格标准的德国,在整体从严的背景下,也有一些法院不再坚持“严重”后果这一程度要件,而是强调精神损害赔偿的威慑功能,认为严重程度主要与赔偿责任大小有关,但与损害认定无关。④ 我国也有法院采宽容立场。⑤

(二)受害人精神损害“严重”与否的解释论构造

对于精神损害是否应达到一定的门槛要求,不仅司法裁判上存在分歧,学理上也存在不同看法。我国有学者认为,“侵害个人信息权益精神损害赔偿不应以‘严重精神损害’为前提条件”,如此“才能全面保护个人……人格权益和财产权益”,⑥况且“严重程度只影响赔偿数额,不能决定权利人损害赔偿请求权的有无”,⑦即便数据泄露导致的焦虑等精神损害不满足《民法典》第 1183 条第 1 款“严重”这一法定要求,也可根据《个人信息保护法》第 69 条第 2 款的规定提出精神损害赔偿请求。⑧ 此观点无异于消解了个人信息侵权精神损害赔偿的门槛限制。比较法上,也有不

① See Summary of the Request for a Preliminary Ruling, Natsionalna agentsia za prihodite, C－340/21; Request for a Preliminary Ruling, Case C －687/21.

② C－340/21, VB v. Natsionalna agentsia za prihodite [2023].

③ See Jonas Knetsch, The Compensation of Non－Pecuniary Loss in GDPR Infringement Cases, 13 Journal of European Tort Law, 145 (2022).

④ 参见王益强:《裁判视角下数据侵权损害的认定》,《华东政法大学学报》2023 年第 5 期。

⑤ 参见北京互联网法院(2019)京 0491 民初 16142 号民事判决书。

⑥ 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》,《南京社会科学》2022 年第 3 期。

⑦ 崔聪聪:《个人信息损害赔偿问题研究》,《北京邮电大学学报》(社会科学版)2014 年第 6 期。

⑧ 参见程啸:《论〈民法典〉与〈个人信息保护法〉的关系》,《法律科学》(西北政法大学学报)2022 年第 3 期。

少域外法院甚至立法对数据泄露精神损害认定采宽容立场，反对为精神损害赔偿设定任何程度的要求。对此，值得追问的是：(1)是否每一条个人信息都关乎个人私密之事或者存在有损其身体或精神完整性的风险？答案显然是否定的。尊重家庭与私人生活固然重要，但仅仅因为信息涉及个人的家庭或私人生活并不能自动地获得保护，在没有特殊事实的情况下，立法者或裁判者自然期望人们能以合理稳健且现实的方式生活。① (2)不加限制的损害赔偿是否最佳救济方案？答案也是否定的。若无任何限制或替代方案，无论对法院还是涉事企业都可能是一场灾难。正如有学者担心，大量的数据泄露受害人涌向法院将导致沉重的审判负担甚至导致某些法院的“崩溃”，代表人诉讼等替代机制虽然能有效缓解法院压力，但是对涉事企业尤其是持有数以千万乃至数以亿计个人信息的信息控制者而言，即便判决其对个人微型损害进行赔偿也可能导致其巨额的财产负担甚至因而破产，这一严重后果显然与公司“过错”不成比例。② 因此，很多法院不愿轻易承认数据泄露对个人造成的所谓损害，因为“这意味着让一家公司陷入破产，而目的只是为了给每个受害人一笔微不足道的赔偿”。③ 否则，个人虽然得到充分保护或威慑发挥了最大效用，但是于涉事企业而言不公平，构成过度威慑，这将导致它们不愿继续从事对社会有益的个人信息商用实践。何况，侵权法的“目的不在于将一般的社会损害责任强加于企业，因为司法系统既没有制度上的能力处理一般的社会危害，也没有民主上的责任去解决一般的社会危害”。④ 可见，为“损害”设置一定门槛有其必要性。

当然，立法或司法也不应囿于“严重”这一精神损害赔偿的“门槛”要求，尤其不宜简单地从字面上理解“严重”。这是因为，对于数字化场景中的人格利益减损、机会或权利丧失、歧视与操纵等新型的非财产损害而言，“单独地看，它们似乎都微不足道，例如接收不受欢迎的电子邮件或垃圾广告所导致的不便，或者未能兑现人们的期望——他们的个人信息不会与第三方共享。然而，当成百上千家公司都如此行事时，其中的危害将叠加。此外，这些微型损害/伤害通常分布于数以百万乃至数以亿计的人群之中。随着时间的推移，当人们被此起彼伏的微型损害淹没时，整体的社会影响就将变得显著了”。⑤ 简言之，从个人角度看，其因数据泄露而遭受的损害可能微不足道，但从社会角度看，个人损害的叠加则数量惊人且影响范围广泛，大规模数据泄露已经体现了此种规模效应与社会影响。就此而言，包括数据泄露在内的个人信息侵权案件中，法院可能需要考虑个人信息执法的多重目标问题，包括赔偿、威慑以及公平。⑥ 问题是，精神损害赔偿仅仅为填平受害人受损之权益，还是应包括威慑或预防功能？大规模数据泄露侵权情形下如何在这些目标之间进行取舍？显然，个案中不可能同时实现这些目标，如何取舍取决于法院针对个案具

① See Ambrosiadou v. Coward (Rev 1) [2011] EWCA Civ 409 (April 12, 2011).

② See Danielle Keats Citron and Daniel J. Solove, Privacy Harms, 102 Boston University Law Review, 817 (2022).

③ Daniel J. Solove and Danielle K. Citron, Risk and Anxiety: A Theory of Data Breach Harms, 96 Texas Law Review, 783 (2018).

④ David W. Opderbeck, Cybersecurity and Data Breach Harms: Theory and Reality, 82 Maryland Law Review, 1004 (2023).

⑤ Danielle Keats Citron and Daniel J. Solove, Privacy Harms, 102 Boston University Law Review, 797 (2022).

⑥ See Danielle Keats Citron and Daniel J. Solove, Privacy Harms, 102 Boston University Law Review, 819 (2022).

体情形进行评估。国内学者普遍认为,精神损害赔偿具有威慑或惩罚功能。[①] 在比较法上,欧盟法院则认为欧盟数据保护法上的非财产损失赔偿仅具有补偿功能。[②] 通常,若考虑社会影响,执法目标应是威慑或公平。此种情形下,如何在法律上评价损害也就不那么重要了,在私人诉讼没有启动的情况下尤为如此。此时,应重点考虑数据处理行为的违法性问题;如果行为人违法行为已受到行政制裁或者支持损害索赔的判决有违公平或导致在整体上减损社会福利等负面影响时,那么私人诉讼时法院考虑被侵权人"损害"的门槛要求就是适当的。毕竟,此种情形下赔偿是诉讼的唯一目标。但当行政执法足以威慑不法行为且不存在其他执法目标时,就应当允许法院驳回私人诉讼。[③] 较之于私人诉讼,行政执法在消除数据泄露导致的社会影响方面更具优势且效果更显著。鉴于本文重点仅在于讨论如何通过私人诉讼使数据泄露受害人"变得完整",因此对个人信息/隐私侵权执法的多重目标取舍问题不再赘述。就精神损害赔偿而言,笔者认为,数据泄露侵权裁判中,应从以下方面理解精神损害赔偿应具备"严重"这一要件。

第一,应避免过于强调精神损害对受害人身体伤害的依从性。在医疗侵权纠纷中,不少法院认为:若无直观的身体伤害,则难以认定精神损害达到了"严重"程度并据此否定受害人精神损害赔偿请求权。[④] 这些法院多强调精神损害的客观性而甚少考虑受害人的主观感受。伤亡或病残等直观且显著的身体伤害固然可以证实或直接推知受害人遭受严重的精神损害,但后者并非必然依附于身体伤害,即便没有物理性的身体或健康伤害,受害人同样可能遭受严重的精神损害后果。实践中,我国也有不少法院包括最高人民法院已不再一味强调精神损害的附随性,而是承认其独立性,即将满足法定条件或标准的纯粹精神痛苦或情绪困扰视为可予赔偿的精神损害。在"刘某某诉南阳某医院案"[⑤]中,最高人民法院即认为原告因丧失生育机会而遭受的精神痛苦具有相当特殊性,满足"严重"之精神损害赔偿标准。

第二,"严重"这一"门槛"要求是"立法者授权裁判者在个案中具体权衡权益保护与行为自由这两种价值的'通道'",[⑥]其本身具有足够的灵活性。(1)"严重"具有确立精神损害赔偿"门槛"的规范功能,即"将生活意义上的精神痛苦纳入规范评价之下,且这一规范评价还旨在区分可获赔偿与仅可获得赔礼道歉等救济的精神损害"。[⑦] 同时,基于"轻微损害不赔"视角理解并适用这一要求,意味着作为人们正常生活变化的一部分,应予容忍的一般负面情绪不应视为精神损害,以免当事人滥用精神损害赔偿请求权。[⑧] (2)该标准应包含受害人遭受精神创伤的各种方式且应允许他们通过医学或科学专家报告、精神痛苦的身体表现甚或行为人的恶意性质等证据来证明

① 参见张新宝:《侵权责任法立法的利益衡量》,《中国法学》2009 年第 4 期;王利明:《侵权责任法研究》,中国人民大学出版社 2010 年版,第 653 页。

② See C-667/21, ZQ v. Medizinischer Dienst der Krankenversicherung Nordrhein [2023].

③ See Danielle Keats Citron and Daniel J. Solove, Privacy Harms, 102 Boston University Law Review, 826 (2022).

④ 参见吉林省高级人民法院(2020)吉民申 2521 号民事裁定书、河南省高级人民法院(2020)豫民申 2977 号民事裁定书。

⑤ 参见中华人民共和国最高人民法院(2020)最高法民再 30 号民事判决书。

⑥ 李东宇:《论侵害个人信息权益的精神损害赔偿》,《财经法学》2023 年第 4 期。

⑦ 洪国盛:《民法典的精神损害赔偿体系——以功能主义为视角》,《法学研究》2024 年第 4 期。

⑧ 参见北京市第二中级人民法院(2022)京 02 民终 2009 号民事判决书。

损害的严重性,[①]避免“严重”的形式主义要求或过于强调受害人精神痛苦的主观性与个体差异从而否定它的存在。相反,应以社会一般大众所能感同身受的客观合理性标准对数据泄露受害人遭受的焦虑、恐惧与不安等精神痛苦的严重与否进行法律评价,[②]其要义在于将受害人遭受的精神痛苦或情绪困扰是否真实合理(而非受害人面临的未来侵害风险的定量分析或精确计算,更不是受害人身心是否遭受实际伤害)作为司法审查重点。这一标准已在国内外不同领域的司法实践中得到了较为普遍的适用。例如,环境侵权诉讼中,受害人常以患病风险增加导致其精神痛苦——对未来罹患重大疾病而深感恐惧——为由提起精神损害赔偿。对此,我国不少法院即基于理性人标准对受害人精神损害进行规范评价并支持原告的精神损害索赔。[③] 域外也有不少法院对环境侵权受害人遭受的恐惧等精神痛苦进行事实上的合理推定。[④] 此外,实践中一些原本不被承认的因就业歧视等行为而生之精神损害现已得到我国法院的普遍肯认且未将“严重”与否与受害人临床表现挂钩。[⑤] 这些精神损害之所以得到法院普遍承认,一个重要原因是其容易获得社会普通人的认同。[⑥] 推而论之,承认当事人因其私密或敏感个人信息泄露或遭滥用而遭受焦虑、恐惧等精神损害同样容易获得社会一般人的认同。不过,在空间性上,因为“不同地区对某一行为造成的精神痛苦的社会容忍度并不相同”,所以“应允许侵权精神损害赔偿认定存在一定程度的地域差异”。[⑦] 总之,立法或司法应该明确地告诉每个潜在的数据泄露受害人:为使他们重新变得“完整”,其所遭受的真实且超过一定门槛的精神损害有权获得赔偿,这不是他们应该忍受的“生活事实”。

四、余　论

如何向数据泄露受害人提供充分救济以凸显数字时代人的价值且不致阻碍数字化进程正在考验着各国立法者与裁判者。基于行为自由以及激励与威慑相容之原则,特别是考虑到数据泄露侵权中,信息控制者的主观状态多为疏忽而非与网络偷盗者等第三人一样具有故意;同时,为避免大规模侵权损害赔偿可能导致的过度威慑问题,精神损害认定后的赔偿应有所限制。此种赔偿限制首先表现为赔偿的“补充性”。这主要针对信息控制者存在过失之情形。根据《民法典》第1198条第2款的解释论,在第三人故意侵权情形下,信息控制者仅就其未履行或未适当履行数据保护义务之过失承担“相应的补充责任”,即限于与其过错程度相当的责任份额而非第三人

① See Jonathan G. Lester, The True Benefit of the Bargain: How Emotional Distress Damages Make Fraud Victims Whole, 62 Boston College Law Review,736 (2021).

② 参见黄薇主编:《中华人民共和国民法典侵权责任编解读》,中国法制出版社2020年版,第79页。

③ 参见江苏省南京市白下区人民法院(2011)白民初字第213号民事判决书、新疆维吾尔自治区乌鲁木齐市中级人民法院(2012)乌中民一终字第732号民事判决书。

④ See Potter v. Firestone Tire and Rubber Co.,274 Cal.Rptr. 885 (Cal.Ct.App.1990); Norfolk & Western Ry. Co v. Ayers, 538 U.S.135 (2003).

⑤ 参见北京市第三中级人民法院(2016)京03民终195号民事判决书、广东省广州市中级人民法院(2016)粤01民终10790号民事判决书。

⑥ 参见林洹民:《论人工智能致损的特殊侵权责任规则》,《中外法学》2025年第2期。

⑦ 洪国盛:《民法典的精神损害赔偿体系——以功能主义为视角》,《法学研究》2024年第4期。

未承担的全部责任,且在承担补充责任后有权向第三人追索。但当信息控制者与第三人系共同过失时,则应适用《民法典》第 1172 条的规定,两者根据各自过错程度和原因力向受害人承担按份责任或平均责任;若数据泄露系信息控制者与第三人共同故意所致,则可根据《民法典》第 1168 条、第 1169 条、第 1170 条、第 1171 条等规定,要求两者承担相应的连带责任。此种赔偿限制其次表现为非金钱赔偿责任形式的适用。本质上,精神损害赔偿的主要功能在于抚慰受害人,精神抚慰金只是其惯常的赔偿方式之一。除此之外,赔礼道歉也能发挥抚慰受害人的规范功能。因此,在解释论上,《民法典》第 1183 条第 1 款规定的精神损害赔偿理应包括精神抚慰金与赔礼道歉两种赔偿方式。而且,根据《民法典》第 179 条的规定,可以单独或合并适用这两种赔偿责任方式。

Abstract: Data breach means that the victims not only have lost control over their personal information, but also will suffer from future infringement risks in different ways and degrees. What's more, the negative mental reactions such as anxieties and fears associated with those risks will disrupt the mental stability or peace that victims originally have. Since the authenticity of future infringement risks is related to the existence and severity of emotional harms, the judicial review of the authenticity of emotional harms should comply with two principles: Firstly, adopting a high probability standard to evaluate future infringement risks suffered by data breach victims; Secondly, adopting objective rationality standard rather than strictly verifiable standard to interpret seriousness of emotional harms, focusing on reviewing the authenticity and reasonableness of the emotional harms suffered by data breach victims. Meanwhile, compensation for data breach victims' emotional harms should be reasonably limited in order to avoid excessive deterrence against information controllers.

Key Words: data breach, personal information, emotional harm, reviewing criteria

责任编辑 何 艳