

敏感个人信息的风险损害赔偿

□ 宋素红 吕建茹

[中图分类号]G206[文献标识码]A[文章编号]1009—5322(2025)04—0107—6

【内容提要】敏感个人信息侵害后果具有全面性、不可逆性、无形性、潜伏性和持续性特征,因此,其损害不仅包括现实的财产、人身损害,而且有产生风险损害的可能性,而实际损害的民事赔偿标准难以弥补这些损害,也难以对侵害产生遏阻作用。风险损害内容主要包括持续性精神损害、财产价值和预防费用,对此虽然理论上有所共识,但司法实践仍有分歧。本文借鉴美国、韩国等国家和地区的立法经验,认为我国立法或司法解释应当明确敏感个人信息的风险损害内容;在相关个人信息保护的立法或司法解释中,应确立预定赔偿金与惩罚性赔偿制度,并缓和个人信息侵害中的精神损害赔偿要件。

【关键词】敏感个人信息;风险损害;预定赔偿;惩罚性赔偿

世界各国对个人信息类型划分的通行方法一致,我国将个人信息分为一般个人信息和敏感个人信息。《中华人民共和国个人信息保护法》规定,敏感个人信息是指一旦泄露或者非法使用,容易导致自然人的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。^①

个人信息一旦受到侵害,对于个人信息主体而言,通常的维权手段是提起民事诉讼,请求民事赔偿。依据《中华人民共和国个人信息保护法》,个人信息损害的民事赔偿标准是基于填补损害的赔偿标准,即受害人实际损失标准或侵权人侵权所得标准^②,但并没有对一般个人信息和敏感个人信息进行区别规定。司法实践中,有两个对涉及敏感个人信息损害赔偿结果产生广泛影响的司法判决——被称为国内“人脸识别第一案”的杭州市民郭某诉杭州野生动物世界有限公司案和“天津人脸识别第一案”的顾某诉某物业公司个人信息保护纠纷,原告分别得到1038元和6200元的“合理费用”的赔偿^③。显然,在赔偿额既不能弥补公认的信息主体损害,更无法震慑非法信息使用者的情况下,与社会生活中普遍存在、频繁发生的敏感个人信息侵害相比,少有信息主体诉诸司法。

敏感个人信息损害赔偿在司法实践中遭遇的尴尬,主要源于我国个人信息民事损害赔偿适用的实际损害赔偿标准未考虑风险损害内容,无法适应这一新

类型无形损害。本文基于比较法视角,探讨相关解决方案。

一、敏感个人信息损害特征及其风险损害的共识

风险损害是与已发生的实际损害相对应、尚未发生但可能发生的损害,分为必然发生、极可能发生和未必发生三种。正因为存在“未必发生”的情形,有观点认为,个人信息侵害中的风险不具有“确定性”,在没有实际损害的情形下,强行扩张损害的概念并判决个人信息处理者承担巨额的赔偿责任,等于变相承认了惩罚性赔偿责任^④。判断上述观点是否成立,首先需要梳理民事损害赔偿理论的演进,并辨析敏感个人信息的损害特征。

(一)损害赔偿理论学说的演进

传统民事损害标准是实际损害标准,以填补损失为指导思想,所谓“无损害则无赔偿”,其依据是“差额说”,即判定受害人的总财产在侵权行为发生的前后是否存在利益差额,若存在,则损害成立。^⑤“差额说”的显著局限是其主要针对财产损害^⑥,而且是针对有形财产,总体财产状况变化的评估在非财产损害和无形财产损害中显然难以发挥其功能。

为弥补“差额说”的不足,产生了“广义差额说”^⑦,其强调损害的确定是一个价值评估的过程,而不是一个简单的自然事实。据此,被害人是否受到损害的实质就是法律规范所保护的利益是否受到损害,或受法

【作者简介】宋素红,北京师范大学新闻传播学院教授、博士生导师。

吕建茹,北京师范大学新闻传播学院博士生。

【基金项目】本文系国家社科基金重点项目“大数据背景下个人生物识别信息的法律保护”阶段性成果,编号:21AXW004。

律保护的状态是否不同。^⑧“广义差额说”的立法代表是《德国民法典》，其规定“债的关系按其内容，使得一方当事人对他方负有考虑他方之权益、法益及利益之义务”^⑨，事实上可以将预期收益纳入。但此说仍然难以适用现代社会个人信息风险损害等在内的无形损害。

随着科学技术的快速发展，尤其是信息科技对社会生活的全面渗透，人类面临的风险大幅增加。在风险社会背景下，现代侵权法强调权益侵害即构成损害，即损害的观念化和抽象化，对损害的确定性要求大为降低——现实的损害是损害的常态，未来的损害即风险损害也可能符合确定性要求。在法国和比利时，“如果存在令人信服的理由表明损害会发生，未来损害也是确定的。”^⑩由此，“预期侵权”制度应运而生。

（二）敏感个人信息损害特征

与一般个人信息损害相比，敏感个人信息的损害特征，除了信息主体的弱（无）自决性，即在场景层面的无感与弱感性，以及在技术与服务层面的无奈性外，其损害及损害风险的严重性主要体现在以下三方面。

1. 损害的全面性。敏感个人信息一旦被泄露或非法使用，个人往往丧失对信息扩散范围和信息用途的控制和决定权，而失控的后果必然威胁到自然人的人身安全或财产安全。同时，其中的一些敏感个人信息，如生物识别信息，其与信息主体之间明确的、唯一的对应关系^⑪，是自然人最本质的自然属性和人格的一部分，因此，对其侵害不可避免地会损害自然人的人格尊严。

2. 损害的不可逆性。敏感个人信息权益受到侵害，与一般个人信息受到损害以及其他人格要素，如名誉等受到损害都有所不同。例如，家庭电话号码泄露，可以更换；名誉受到损害，可以即时恢复，但生物识别信息、特定身份是固定的，是不可更改或极难更改的。此类信息一旦泄露，就意味着将产生永久的不利后果，损害是无法挽回的。

3. 损害的无形性、潜伏性和持续性。包括敏感个人信息在内的个人信息的损害与有形财产损害不同，其具有无形性，很少以具象化、可观测的形式出现^⑫，而且其具有潜伏性，表现为被他人非法利用造成财产、精神损害的潜在威胁。^⑬

根据预期侵权理论，结合上述敏感个人信息损害特征，在敏感个人信息侵害中，风险损害是必然的逻辑结果——虽然泄露的个人信息将在何时、被多少下游处理者处理、被处理多少次均难以预测，但可以确定的是，损害可能会多次甚至无限次发生。

（三）关于敏感个人信息风险损害的主流观点

从个人信息保护制度的目的而言，其并非主要为救济非法处理造成的现实损害，而主要是“为了规制个人信息处理风险，防范与救济个人数据处理与利用活动可能产生的侵害后果”^⑭，若固守实际损害的赔偿模式，即必须有具体的损害发生，一方面，等于纵容信息

处理者肆无忌惮地使用信息，并将风险转嫁给无辜且缺乏预防能力的信息主体^⑮；另一方面，可能导致侵权法的预防功能弱化，因为实际损害观念的司法实践结果要么是被告全部赔偿，要么丝毫不赔偿，在一些案件中原告受到的损害可能难以得到救济。^⑯因此，预期侵权理论下，敏感个人信息的风险损害是世界各国的题中之义。

美国传统侵权损害奉行实际损害赔偿标准。然而，针对风险社会背景下损害赔偿起诉资格，美国联邦最高法院在20世纪90年代就确认了损害赔偿三个要素之一是“损害必须已实际发生或确定即将发生”^⑰。显然，确定即将发生的损害也可得到赔偿，这为承认风险损害奠定了基础。

欧陆之外的成文法国家在这一主题上的探索更超前，包括预期损害已进入各国民法典。1960年生效的《埃塞俄比亚民法典·债编》，“非契约责任与不当得利”（第13题）的“损害赔偿”部分中就有相关规定，“确定会发生的将来损害，得予以赔偿而毋庸等到其实际发生。”^⑱2017年大修后的《日本民法典》，“对于因特别情势产生的损害，当事人应预见其情势时，债权人得请求其赔偿”^⑲，同样是针对预期损害。上述规定均可对个人信息风险损害赔偿起到直接参照作用。

我国民法学界主流也认可风险损害。由于敏感个人信息损害的上述特征，其泄露后的风险当属重大（实质性）风险或一般风险，而基于预防风险、减少风险损害发生的目标，学界认为敏感个人信息的损害赔偿需要借鉴“风险损害”的理念。甚至有观点认为，风险可直接作为损害，依据风险投保的成本来评估，并结合个案权衡，如在个人数据泄露中，考虑未来损害发生的可能性和后果、数据敏感度和数据暴露成本、预防措施的可能性等。^⑳总之，以“差额说”为依据的实际损害标准针对的是有形财产损害，不适应个人信息风险损害等在内的无形损害。而敏感个人信息特殊的法律特征，尤其是其损害后果的全面性、不可逆性和持续性，说明传统的实际损害问题并非敏感个人信息损害的实质问题，也决定了实际损害赔偿标准难以对此类损害进行弥补。因此，问题的解决需要首先确定风险损害的具体内容。

二、敏感个人信息风险损害内容及司法认定现状

对于敏感个人信息泄露与传播导致的实际损害，包括现实的人身、财产损害及伴随的合理开支（含调查、取证费用、律师费用等诉讼开支）等损害赔偿，通常并无异议，其分歧主要在于损害风险引发的风险损害——持续性精神损害、财产损害（商业价值）和预防费用。

（一）敏感个人信息风险损害中的持续性精神损害

传统侵权法对精神损害赔偿的门槛较高，不仅要求已发生，而且要求达到“严重”程度，学界甚至认为须

以法律特别规定为前提。^②德国、英国和奥地利的法院传统上都倾向于受害人因未来损害风险而产生的焦虑情绪并不构成精神损害。^③然而,个人信息保护纠纷中精神损害要件问题已经引起了各国立法部门的关注,并体现在立法中,如欧盟《通用数据保护条例》规定,只要违反该条例即可获得精神损害赔偿^④,而并不要求“严重”精神损害。该条例生效后,欧洲国家普遍修改本国个人信息保护法律制度,删除“严重”要件,降低了个人信息侵害纠纷精神损害赔偿的门槛。英国《个人数据保护》第168条至第169条明确指出,精神痛苦属于个人信息损失。^⑤总体上,“严重精神损害”(包括“实际经济损失”)要件在个人信息与数据侵害场合下的缓和已是一种趋势。^⑥

目前美国学界主流观点认可个人信息侵害会产生精神损害,原因在于个人信息,尤其是敏感个人信息被泄露,信息主体不仅有上述现实和未来的财产、人身安全风险损害,还必然因担忧未来可能的权益损害而产生担忧等负面、破坏性的情绪困扰,即“焦虑”。长期担忧和恐惧其财务、就业、名誉等遭受损失,这种焦虑相当于一慢性疾病,足可构成一种精神损害。^⑦美国法学会也在2020年《数据隐私法律原则》中明确规定,情绪损害(emotional harm)和“寒蝉效应”(chilling effect)属于个人信息领域可认定之损害^⑧。这种精神损害不是因个人信息侵害导致的已发生的实际精神损害,而是面向未来的持续性精神损害。

我国个人信息侵害中的精神损害与国外迥异。《中华人民共和国个人信息保护法》对包括敏感个人信息在内的个人信息侵害确立的赔偿标准,是实际损害或侵权人侵权所得标准。在《最高人民法院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》(以下简称《人脸识别民事规定》)中,仅将自然人为制止侵权行为所支付的“合理开支”认定为实际损失,其包括该自然人或者委托代理人对侵权行为进行调查、取证的合理费用及合理的律师费用。^⑨至于精神损害赔偿,《中华人民共和国民法典》中只保护“严重精神损害”^⑩,一般受害者难以获得精神损害赔偿。司法实践中,虽然存在造成后果无法更改的敏感信息处理行为,但我国法院在精神损害赔偿方面也往往以未达到“严重”程度为由不予保护,如在“程某等与某村卫生室侵权责任纠纷案”中,被告错误录入原告疾病,且录入信息已无法在系统中修改,法院最终判决,被告在《开州日报》上予以澄清并登报致歉。这在一定程度上对原告的精神带来抚慰,即承认原告有精神损害,但判决不保护原告精神损害赔偿请求。^⑪总之,即使个人信息已经被泄露,我国法院也很少认可对个人信息泄露的焦虑不安属于精神损害。^⑫另有学者统计,我国敏感个人信息侵害纠纷中,获得精神损害赔偿比例仅占22%。^⑬在前述两起国内人脸识别民事纠纷判决结果中,不仅已经发生的现实精神损害未有赔偿,且

风险损害下持续的精神损害赔偿也未得到任何体现。

(二)敏感个人信息风险损害中的财产损害

这里的财产损害指敏感个人信息本身作为财产受到的损害,而不是信息主体对侵权行为进行调查、取证的合理费用及合理的律师费用。

尽管司法实践中敏感个人信息,如人脸、行踪轨迹的财产价值因难以证明、评估、确认而无法得到保护,但个人信息是精神性和物质性利益兼具的人格权益,民法学界普遍承认(敏感)个人信息的财产价值。^⑭个人信息(数据)的财产价值包括以下类型:一是“货币价值”,即个人信息是新时代的一种重要货币,而且价值在不断增长,这就是美国企业迅速从这一趋势中获利的原因。^⑮有研究得出结论,一个互联网用户的信息价值从15美元到40美元不等,甚至更多。^⑯另一项研究发现,一个人的在线身份可以在网上以1200美元的价格出售。^⑰二是商业资产价值,即个人信息具有明显而巨大的经济价值。个人的特征和属性(如年龄、地址、性别、收入、偏好……他们的点击量、网上发表的评论、社交媒体上更新的照片等)日益被视为商业资产。^⑱正因个人信息是宝贵的财产,美国目前产生了相关市场交易,互联网用户可以出售或变现他们自己的个人生物识别信息和互联网使用信息。^⑲三是其他无形价值,如就业利益。例如,在秦某等诉山东某电力工程有限公司等个人信息保护纠纷案中,三被告无合法理由(因工作人员操作失误)为原告缴纳企业养老、失业、工伤保险数月。法院最终认定,被告的行为有可能导致原告无法以应届毕业生身份择业,该侵权行为可能导致的后果尚未发生,但仍会给原告带来一定的精神困扰和担忧。法院酌情判令三被告分别向原告赔偿5000元^⑳。该案中的社保账号显然是一旦泄露就容易导致信息主体财产安全受到危害的敏感个人信息。

我国的司法实践中,承认个人信息财产价值的案例虽不多,但已经有少数判决进行了认可,并提及风险损害。^㉑如在特殊场景中,一般个人信息(如电话号码)也被法院认定为敏感个人信息。法院认为,“客户的电话号码一旦被泄露或非法使用……导致众多不特定人员的信息长期面临受侵害的风险,并导致危害人身和财产安全,在未采取补救措施的情况下可视为损失仍在持续。”^㉒

(三)敏感个人信息风险损害中的预防费用

敏感个人信息泄露后,信息主体为防止损害进一步扩大或预防损害的发生,通常会采取预防性措施。如在人身安全的预防方面,家庭门禁需更换门禁信息类型(将人脸识别改为指纹、虹膜识别)或彻底更换安保系统;在涉及个人金融安全、银行账号识别方法需更换时,因我国许多银行App大额转账只接受人脸识别,所以一旦人脸信息泄露,不仅造成重大威胁,而且信息主体需向银行特别申请或只能到银行柜台办理相关业务,导致精力与时间损失和财务成本的增加。

传统侵权法上,世界各国承认为防止损害扩大而导致的成本可认定为损害,而对单纯预防损害发生的费用,则不归为损害。^④然而,在新型侵权中,风险损害的承认可解决此问题,因为损害的扩大与发生无法区分,区分也没有意义。因此,《人脸识别民事规定》第九条中关于“自然人为制止侵权行为所支付的合理开支”,尽管只列举了对侵权行为进行调查、取证和律师费等合理费用,但不应视为封闭式列举,即应包括信息主体的预防费用。

敏感个人信息损害中,持续性精神损害属于尚未发生的风险损害;财产价值的损失和预防性费用则可能属于已经发生的实际损害,或尚未发生的风险损害。然而无论如何,敏感个人信息的风险损害包括以上三种类型已成为理论共识,为损害赔偿奠定了基础。但风险损害作为专门界定个人信息损害领域的纯粹理论概念,需要法律上对应的赔偿标准,更需要立法支持。

三、敏感个人信息风险损害的赔偿标准比较研究

如前所述,以填补损失为原则的实际损害赔偿标准是以已发生的有形物损害为基础的,其不适应包括个人信息侵害等导致的无形损害,不能反映风险损害的内容。因此,部分国家和地区在立法中以预定赔偿和惩罚性赔偿来解决此问题。

(一)敏感个人信息损害的预定赔偿

包括敏感个人信息在内的个人信息侵害的法定赔偿,多采用预定赔偿,目前有两种模式。

第一,不考虑实际损害,直接规定预定赔偿额。这又可分为两种情形:一是确定每个信息主体的赔偿数额。如美国伊利诺伊州的《生物识别信息隐私法案》所规定的权利救济形式为违约赔偿的民事诉讼救济,任何个人可向州巡回法庭或联邦地区法院提出损害赔偿诉讼;信息主体可申请实际损害赔偿或法定赔偿,以两者间较大数额为准;过失损害的赔偿数额为实际损失或1000美元;故意或重大过失造成损害的赔偿数额为实际损失或5000美元;诉讼费用由违约一方承担;同时还可申请禁令等其他救济措施。^⑤二是确定信息处理者最高赔偿数额。美国得克萨斯州《生物特征符获取或使用法》规定,每次违反该法的信息处理者所受处罚不超过25000美元;州总检察长可提起此类诉讼。^⑥相比之下,这种救济不仅给予信息处理者最高赔偿额度的保护,而且还在救济渠道上安排了类似我国民事公益诉讼的“检察公益诉讼”。

第二,考虑实际损害赔偿,即在实际损害无法证明的情形下,适用固定金额赔偿。如我国台湾地区,其规定受害人如难以或无法证明实际损害的金钱价值,可请求法院依损害之严重程度,每人赔偿新台币五百元以上二万元以下的赔偿金。当然,因同一事件侵害多

个信息主体权利的,该信息处理者的赔偿总额不超过新台币2亿元。^⑦

(二)敏感个人信息损害的惩罚性赔偿与预定赔偿的结合

惩罚性赔偿指判定的损害赔偿金不仅是对原告的补偿,而且也是对故意加害人的惩罚。《布莱克法律辞典》将惩罚性赔偿界定为“当被告的行为是轻率、恶意、欺诈时,(法庭)所判处的超过实际损害的部分,其目的在于通过处罚做坏事者或以被估计的损害做例子对其他潜在的侵犯者产生威慑。”^⑧如前所述,敏感个人信息与信息主体的人身安全与人格尊严密切相关。在我国产品侵权纠纷中,对自然人的人身安全造成损害,可以与补偿性赔偿金同时适用惩罚性赔偿金。因此,从敏感个人信息的特殊性来看,设定惩罚性赔偿金具有类似的正当性。

此外,个人信息侵害在相当多情形下可归为大规模侵权。而以填补损害为目的的补偿性赔偿对大规模侵权具有局限性——不利于填补大规模侵权损失,不利于遏制大规模侵权发生,不利于激励受害人主张权利。^⑨而惩罚性赔偿的功能与预防、遏制大规模侵权的目的具有一致性。学界认为,应把大规模侵权作为一种特定侵权类型来对待,规定包括惩罚性赔偿在内的特殊保护措施,并且要和配套的实施细则或相应的法规相衔接,使之具有较强的可操作性。^⑩因此,对属于大规模侵权的侵害敏感个人信息案件,应当与著作权纠纷、证券市场纠纷及消费者权益纠纷一样,适用惩罚性赔偿。^⑪

韩国和美国华盛顿州的相关法规如下:韩国《个人信息保护法》第三十九条第3款规定,个人信息处理者因故意或重大过失导致个人信息的丢失、盗窃、泄露、伪造、变造、损毁,对信息主体造成损害的,法院在不超过损失数额三倍的范围内确定损害赔偿金(惩罚性赔偿)。除此之外,信息主体还可请求三百万元以内的损害赔偿金。^⑫美国华盛顿州2017年通过的《生物识别隐私法》规定,违反该法的行为将被视为不公平或欺骗性的行为,或者不公平的竞争方法,适用《华盛顿州消费者保护法》的相关规定——法庭可判决给予信息主体实际损害的三倍、但最高不超过25000美元的民事赔偿。^⑬

综上,尽管相关国家和地区尚未对敏感个人信息的风险损害赔偿进行系统、全面的立法,但预定赔偿金或惩罚性赔偿是其个人信息保护综合立法及个别敏感个人信息(生物识别信息)民事保护立法领域相关规定的共同选择。

四、结论与建议

个人信息非法披露等非法行为的实质性损害风险已被社会所共认。而损害内容与损害赔偿标准是紧密关联的问题,前者决定后者,后者是前者的逻辑结果;

没有对损害内容的科学界定,就不可能有客观的损害赔偿标准。敏感个人信息损害赔偿也是如此,如果对其损害风险,即持续性精神损害、财产价值和预防费用不予认定,就无法对具体损害内容进行相关立法,从而无法对敏感个人信息侵害设置特别的民事赔偿责任,进行特别保护。

《中华人民共和国个人信息保护法》中将敏感个人信息进行单独列举,最高人民法院亦专门制定相关民事纠纷的司法解释,凸显了这一问题的重要性。但由于未对损害内容进行界定,也未规定特别的损害赔偿标准,因而削弱了侵权法在该领域的保护功能,也未发挥对侵权的威慑作用。国外相关制度及司法实践为敏感个人信息的民事赔偿提供了有益借鉴;我国《中华人民共和国消费者权益保护法》也已将侵害个人信息的民事赔偿规定为消费者实际损失的二倍或交易额的三倍^⑧,行政处罚规定为违法所得一倍以上十倍以下或五十万元以下的罚款^⑨,这也为敏感个人信息的民事赔偿奠定了制度基础,提供了建设性思路。

鉴于正式立法修改的成本与成文法简约性的传统,目前相关部门可修订司法解释,进一步完善敏感个人信息的民事赔偿责任。

第一,明确个人信息损害包括持续性精神损害、财产价值及预防性费用。个人信息损害的内涵可界定为,“因违反个人信息处理规则导致对信息主体的实际损害、风险损害、精神损害、合理支出和财产价值损失等。”至于外延列举,可借鉴前述印度《个人数据保护法案》对损害的列举,即身体或精神伤害,身份丢失、歪曲或盗窃,财务损失或财产损失;名誉损失或屈辱,失业,任何歧视性待遇,遭受勒索和敲诈,任何因对数据主体做出评估决定而拒绝或撤销向其提供服务、利益或好处,任何因担忧被观察、监视引起的对言论、行动施加限制或被施加限制,数据主体无法预期的任何观察或监视。^⑩

第二,设立梯状预定赔偿金与惩罚性赔偿。法律之所以将个人信息分为一般个人信息和敏感个人信息,本身就是要强化对后者的保护。因此,侵害敏感个人信息原则上可视为损害风险是可预测的,而不是抽象的,应适用预定赔偿金与惩罚性赔偿。

在立法或司法解释中可采取列举式对有关行为进行分类,设立预定赔偿金:一是根据信息处理主体的主观恶意综合进行判断。就主观而言,如信息处理主体存在过失行为,可以设定较小数额的预定赔偿金;如果信息处理者存在故意行为,则可以设定较高数额的预定赔偿金。二是针对侵权行为的性质进行判断。如果信息主体对敏感个人信息的收集表示认同,信息处理者仅改变存储时间,没有逾越种类与范围的限制收集的敏感个人信息,则可以设定较小数额的预定赔偿金;如果收集的敏感个人信息的种类与范围超越同意的范畴,则可以设定较高数额的预

定赔偿金。

风险损害赔偿理念下,有关敏感个人信息损害赔偿的一个重要功能在于预防与震慑有关违反法定程序行为的发生。因此,设立惩罚性赔偿金具有一定必要性。借鉴《中华人民共和国消费者权益保护法》第五十五条和第五十六条,对信息处理者故意侵害敏感个人信息,赔偿额可为信息主体实际损害或信息处理者侵权所得的三倍,或者处以十万元以下的赔偿。

第三,精神损害赔偿的要件的缓和。鉴于“严重精神损害”(包括“实际经济损失”)要件在个人信息与数据侵害场合下的缓和已是一种趋势,可在《中华人民共和国个人信息保护法》修订或在司法解释中,删除个人信息侵害精神损害赔偿的“严重”要件,降低此类纠纷精神损害赔偿的门槛。■

参考文献与注释:

- ①②参见《中华人民共和国个人信息保护法》第二十八条、第六十九条第二款。
- ③参见浙江省杭州市中级人民法院(2020)浙01民终10940号民事判决书;天津市第一中级人民法院(2022)津01民终349号民事判决书。
- ④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。
- ⑤曾世雄:《损害赔偿法原理》,中国政法大学出版社2001年版,第118页。
- ⑥⑦王泽鉴:《损害赔偿》,北京大学出版社2017年版,第63页、第64页。
- ⑧韩世远:《合同法总论》,法律出版社2011年版,第778-779页。
- ⑨汪志刚:《论民法上的损害概念的形成视角》,《法学杂志》2008年第5期。
- ⑩参见《德国民法典》第241条第2款。
- ⑪欧洲民法典研究组、欧洲现行私法研究组编著,王文胜等译:《欧洲私法的原则、定义与示范规则(欧洲民法典草案)》(第五卷、第六卷、第七卷),法律出版社2014年版,第236页。
- ⑫付微明:《生物识别信息法律保护问题研究》,中国政法大学2020年博士学位论文。
- ⑬杨垠红、章彤:《个人信息侵权风险性损害的认定路径》,《福州大学学报(哲学社会科学版)》2022年第6期。
- ⑭朱宣桦:《新时代个人信息民事保护路径研究——以存在第三方信息处理者情况下的民事责任分配为视角》,《法学杂志》2018年第11期;杨垠红、章彤:《个人信息侵权风险性损害的认定路径》,《福州大学学报(哲学社会科学版)》2022年第6期。
- ⑮王锡铎:《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。
- ⑯⑰赵贝贝:《个人信息私法救济中的“损害赔偿”困境与应对路径》,《财经法学》2022年第5期。
- ⑱王泽鉴:《损害赔偿法上的酌减条款》,《法令月刊》2016年第6期。
- ⑲Lujan v. Defs. of Wildlife. 504 U.S. 555(1992).
- ⑳参见《埃塞俄比亚民法典》第2092条。薛军译:《埃塞俄比亚民法典》,厦门大学出版社2013年版,第293页。
- ㉑参见《日本民法典》第416条第2款。
- ㉒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》,《国家检察官学院学报》2021年第5期。

②刘云:《论个人信息非物质性损害的认定规则》,《经贸法律评论》2021年第1期。

③《欧盟通用数据保护条例》第82条规定:“任何因为违反本条例而受到物质或非物质性伤害的人都有权从控制者或数据者那里获得对损害的赔偿。”

④Date Protection Act 2018, Article 168-169.

⑤叶名怡:《个人信息的侵权法保护》,《法学研究》2018年第4期。

⑥Solove, D. J., & Citron, D. K. (2017). Risk and Anxiety: A Theory of Data-Breach Harms. Texas Law Review, 96, p. 765.

⑦Ali Principles of the Law, Date Privacy, §14(2020).

⑧参见《最高人民法院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》第八条。

⑨《中华人民共和国民法典》第一千一百八十三条规定:“侵害自然人人身权益造成严重精神损害的,被侵权人有权请求精神损害赔偿。”

⑩参见重庆市开州区人民法院(2020)渝0154民初5749号民事判决书。

⑪陈蓉、杨玉华:《敏感个人信息精神损害赔偿之检视与制度建构》,《重庆邮电大学学报(社会科学版)》2023年第2期。

⑫王利明:《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》,《现代法学》2013年第4期。

⑬Schwartz, P. M. (2003). Property, Privacy, and Personal Data. Harv. L. Rev, 117(5), p. 2056.

⑭The World's Most Valuable Resource Is No Longer Oil, but Data, THE ECONOMIST (May 6, 2017), <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>.

⑮Maria LaMagna, The Sad Truth About How Much Your Facebook Data is Worth on the Dark Web, MarketWatch (June 6, 2018), <https://www.marketwatch.com/story/spooked-by-the-facebook-privacy-violations-this-is-how-much-your-personal-data-is-worth-on-the-dark-web-2018-03-20>.

(上接第106页)

ment: Cognitive Mapping and Spatial Behavior (pp. 63-78). Chicago: Aldine.

⑮Guo, L., & McCombs, M. (2011). Network Agenda Setting: A Third Level of Media Effects. Paper Presented at the International Communication Association (ICA), Boston.

⑯Guo, L. (2015). A Theoretical Explication of the Network Agenda Setting Model: Current Status and Future Direction. In L. Guo & M. E. McCombs (Eds.), The Power of Information Networks: New Directions for Agenda Setting. London: Routledge.

⑰蒋俏蕾、程杨:《第三层次议程设置:萨德事件中媒体与公众的议程网络》,《国际新闻界》2018年第9期。

⑱黄敏:《议题关联与关系建构——〈纽约时报〉有关中国扶贫报道的媒体网络议程分析》,《新闻与传播研究》2020年第3期。

⑲韩晓宁、郭玮琪、巴亚岭:《疫情议题多元话语主体多层次议程设置效果研究》,《当代传播》2021年第2期。

⑳基欧汉(Keohane, R. O.)、奈(Nye, J. S.)著,门洪华译:《权力与相互依赖:转变中的世界政治》,北京大学出版社2012年版,第34-35页。

㉑Mansbach, R. W., & Vasquez, J. A. (1981). In Search of Theory: A New Paradigm for Global Politics. Columbia Universi-

ty Press. pp. 96-103, pp. 113-124.

㉒Alessandro Acquisti et al. (2016). The Economics of Privacy, J. Econ. Literature, 54(2), p. 442, p. 444.

㉓Kevin Mercandante, 10 Apps for Selling Your Data for Cash, BEST WALLET HACKS(Apr 20, 2023), <https://wallethacks.com/apps-for-selling-your-data/>.

㉔参见山东省济宁市任城区人民法院(2022)鲁0811民初1958号判决书;山东省济宁市任城区人民法院(2022)鲁0811民初1961号判决书。

㉕①①参见湖北省宜昌市猇亭区人民法院(2022)鄂0505刑初59号刑事附带民事判决书。

㉖①[德]马格鲁斯著,谢鸿飞译:《欧洲统一侵权法:损害与损害赔偿》,法律出版社2009年版,第268页。

㉗③ See The Biometric Information Privacy Act 740 ILL. COMP. STAT. §20/1, 20/2, 20/3, 20/4(2008).

㉘④ See Texas Business and Commerce Code § 503.001 (d) (2009).

㉙⑤参见《台湾个人资料保护法》第28条。

㉚⑥Bryan, A. Garner(Editor in Chief). (2019). Black's Law Dictionary. Thomson Reuter's Co, p. 491.

㉛⑦李建华、管洪博:《大规模侵权惩罚性赔偿制度的适用》,《法学杂志》2013年第3期。

㉜⑧齐喜三:《论大规模侵权的多元化救济模式》,《河南师范大学学报》2014年第5期。

㉝⑨罗斌:《传播侵权研究》,国家图书馆出版社2018年版,第196页。

㉞⑩参见韩国《个人信息保护法》第39条之二第1款和第3款的规定。

㉟⑪ See Washington Revised Code §19.86.090 c 371(2009).

㊱⑫⑬参见《中华人民共和国消费者权益保护法》第五十五条、第五十六条第一款。

㊲⑭参见印度《个人数据保护法》第3条第20款。

㊳⑮ Livingston, S. G. (1992). The Politics of International Agenda-Setting: Reagan and North-South. pp. 314-326.

㊴⑯韦宗友:《国际议程设置:一种初步分析框架》,《世界经济与政治》2011年第10期。

㊵⑰杨娜、程弘毅:《理解国际议程设置:议题传播与框架互动》,《当代亚太》2022年第5期。

㊶⑱张发林:《化解“一带一路”威胁论:国际议程设置分析》,《南开大学学报(哲学社会科学版)》2019年第1期。

㊷⑲金凤君、刘会远、陈卓等:《中国与东盟基础设施建设合作的前景与对策》,《世界地理研究》2018年第4期。

㊸⑳朱新梅:《国际化智能化加速中国剧集全球传播》,《视听界》2025年第3期。

㊹㉑越南称南海为“东海”(East Sea),主要是出于其对南海部分海域的非法主权诉求。越南试图通过改变名称,从文化和认知层面强化其对南海相关海域的主张,将其纳入自身的“海洋权益”范畴,这种做法是对中国南海主权的严重侵犯,且缺乏历史和法律依据。

㊺㉒李欣:《构建海洋命运共同体:思想意蕴与中国实践》,《国际问题研究》2024年第6期。

㉓㉔中国政府网:《“一带一路”蓝色合作倡议》及蓝色合作成果清单发布, https://www.gov.cn/lianbo/bumen/202311/content_6913613.htm.