

论数字时代个人信息的侵权法保护

李凤霞, 李楚晴

(中国石油大学(华东)文法学院, 山东 青岛 266580)

摘要:数字时代的个人信息已成为自然人生活生产、社会交往的重要媒介。实践中,信息处理者非法获取、擅自公开、过度使用个人信息等行为频发,严重侵害了个人的信息权益。大数据技术的广泛应用使得信息处理者在数据控制中占据显著优势,导致侵权行为往往具有高度隐蔽性。加之信息主体与处理者间的举证能力严重失衡,这给个人信息的私法保护带来严峻挑战。尽管《民法典》与《个人信息保护法》已规定个人信息侵权责任,但司法实践中仍存在适用僵化的问题。对此,需进一步规范个人信息侵权责任的适用。引入无过错责任原则,构建过错与无过错并存的二元归责体系;修正传统“差额说”理论,科学界定侵权损害范围;从确定损害赔偿数额范围和明确参考要素两方面完善精神损害赔偿数额的计算规则,以更有效地保障数字时代的个人信息权益。

关键词:数字时代;个人信息;归责原则;精神损害赔偿

中图分类号:D9

文献标识码:A

文章编号:1008-7699(2025)03-0040-08

随着云计算、物联网、大数据技术的快速发展,我国已全面进入数字社会,个人信息正日益成为重要的沟通媒介和推动数字经济发展的关键生产要素。在个人信息流通与商业化利用的过程中,个人信息权益受侵害风险显著提升、侵权事件频发,个人信息保护成为当今学界的热点问题。《中华人民共和国民法典》(以下简称《民法典》)第一百一十一条和第一千零三十四条至第一千零三十九条对个人信息权益保护作出了专门规定,旨在规范信息处理者的收集、处理行为,防范其对信息主体造成的损害风险。2021年11月1日实施的《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》)作为我国首部专门规范个人信息处理活动的法律,显著提升了我国个人信息权益的保护水平。《个人信息保护法》第六十九条(以下简称“第六十九条”)专门规定了个人信息侵权责任,确立过错推定原则作为处理者侵权损害赔偿责任的归责原则。同时,明确区分权益侵害与侵权损害,规定了三种损害赔偿数额计算方法,为司法实践提供了明确指引。

然而,数字时代的个人信息权益侵害在侵权方式、损害后果等方面与传统侵权存在显著差异,导致第六十九条在司法适用中面临现实困境,亟待通过理论研究和制度完善予以解决。鉴于此,本文首先论证数字时代个人信息侵权法保护的必要性,继而从归责原则、损害认定、精神损害赔偿数额计算三个维度,系统分析第六十九条立法的不足,最终提出体系化完善方案。

一、数字时代个人信息侵权法保护的必要性

在数字时代,个人信息被赋予了崭新价值与独特特征,个人信息侵权行为在侵权方式与损害后果等方面具有特殊性。近年来个人信息侵权事件频发,亟待进一步完善侵权法规则,为信息权益人提供更有效的保护。

(一)数字时代个人信息的新特征

与线下社会中的个人信息相比,数字时代流转于网络媒体间的信息被赋予了崭新特征。详言之,其

收稿日期:2025-01-09

作者简介:李凤霞(1972—),女,山东潍坊人,中国石油大学(华东)文法学院副教授,硕士生导师。

一,个人信息具有显著的商业利用价值,常被大规模收集与利用。例如,金融信息既包含信息主体的基础信息,还涉及信用和资产情况等,因而往往成为不法分子的侵害对象。利用海量泄露的金融信息实施的犯罪行为,例如盗窃、金融诈骗等,已成为个人信息侵权的主要表现形式。^[1]其二,个人信息具有可识别性。^[2]可识别性——通过该信息可以识别特定自然人——是个人信息的核心要件。此种识别既包括对个体身份的识别,也包括对个体特征的识别。其判断应结合具体场景,从信息特征以及信息处理方的角度综合考量。其三,个人信息具有复制便利性与传播即时性。在赛博空间中,个人信息的复制成本极低、传播速度极快,导致信息主体未来受侵害风险显著提升。一旦个人信息权益遭到侵害,其损害后果往往很难完全消除,将对信息主体的隐私、财产以及社会关系产生持久影响。

(二)数字时代个人信息侵权的特殊性

与线下空间相比,数字时代的个人信息侵权行为具有鲜明特殊性。具体而言,其一,处理者的侵权行为为具有高度隐蔽性,这主要源于数字时代信息处理手段的技术性与专业性。数字企业信息处理的高度隐蔽性使得个人在数据控制中处于弱势地位,难以知悉其信息是否处于安全、私密的状态,以及其信息被收集后的处理方式与用途。受害人无从知悉其信息是否已遭到侵害,也无法判断泄露其信息的平台或企业是否已尽到相应的注意义务和法律保护责任,也就更难以证明处理者的行为是否有过错。以大数据“杀熟”为例,算法技术的日益隐蔽化,导致消费者往往难以发现价格歧视,更难以举证自身利益已遭受侵害。^[3]其二,信息主体与处理者间的举证能力严重失衡。自动化处理技术的快速发展一方面为个人生活与生产活动创造了更多经济价值,但另一方面也加剧了信息主体与处理者在信息控制能力与地位上的不平等。信息技术日趋复杂化和专业化的背景下,在信息或数据生成和处理的过程中,信息主体囿于对科技知识了解的匮乏以及对个人信息重要性的认识不足,对信息处理者作出的信息收集和使用等服务的承诺常常并不关心。他们通常认识不到潜在的风险,对信息处理主体处理其个人信息信息缺乏应有的警惕。

二、数字时代个人信息的侵权法保护困境

鉴于数字时代个人信息侵权行为的特殊性,第六十九条在归责原则、损害认定与损害赔偿数额计算三个维度上争议颇多,同时在司法适用中也面临诸多困境。

(一)个人信息侵权单一归责原则救济力度不足

第六十九条规定过错推定责任原则系个人信息侵权责任的归责原则,这一规定引起了理论界与实务界的广泛关注。在个人信息侵权场景中,过错推定责任原则是指,处理者若不能证明其处理行为合法或已尽到个人信息保护义务,则推定其存在过错。^[4]过错推定原则在个人信息侵权案件中的应用不无正当性,例如,有学者指出,适用过错推定责任原则有充分法理基础。^[5]具体而言,由于处理者与信息主体双方在信息掌握与技术能力上存在较大差距,双方间举证能力严重失衡,个人难以举证侵权人的主观过错,因此,相较于一般过错责任来说,过错推定责任更有利于处于信息和技术弱势地位的个人有效维护其信息权益。

然而,有学者指出,“一刀切式”的过错推定原则难以应对多样化的个人信息保护需求,也难以充分保护个人权益,因此亟待进一步优化。^[6]笔者认同这一观点,适用单一过错推定原则存在以下局限性。第一,过错推定责任原则的适用范围缺乏合理限制。^[7]数字时代,个人信息处理活动具有泛在性,信息主体所受人身、财产损害都可能与处理行为有关,过错推定原则的严格遵循将导致其适用范围的过度扩张。第二,适用单一过错推定原则难以充分保护多样化的个人信息。根据商业利用价值、敏感程度等维度,个人信息可分为敏感个人信息和一般个人信息。敏感个人信息相较一般个人信息具有更高价值,一旦泄露并被非法收集、使用,可能会对个人造成更严重的损害,因此,对一般个人信息与敏感个人信息适用同样的归责原则欠缺合理性,难以体现区分保护的法律思维。第三,过错推定原则仍难以应对算法技术引发

的证据偏在难题。^{[8][15]} 处理者仍可凭借突出的数字技术优势证明其已履行合理注意义务或已采取必要防护措施,从而影响法官裁判。为追求商业利润,某些互联网公司甚至故意采用不正当的数字处理技术,以规避可能的诉讼风险。第四,过错推定原则未能有效解决信息权益人因果关系举证的难题。在个人信息侵权场景中,因果关系包括侵权责任的成立与范围两个层面。^[9] 如前所述,数字时代个人信息侵权行为具有显著特殊性,在算法黑箱的决策机制下,处理者尚且难以知悉并说明信息权益遭受侵害的原因与过程,更遑论在经济能力与信息获取能力上都处于弱势地位的普通用户。侵权行为的隐蔽性与侵权环节的多重性导致信息主体难以确定具体侵权人,因此,信息主体难以证明侵权责任成立层面的因果关系。此外,在个人信息侵权引发下游犯罪的场景中,如电信诈骗等,损害与侵权人的处理行为之间的因果关系也难以确定。

综上所述,当前个人信息侵权归责适用过错推定责任原则仍存在不足,难以从根本上解决当前信息主体权益保护不足的困境。

(二)个人信息侵权损害范围认定困难

损害填补是侵权法的首要功能。^[10] 损害是启动侵权法保护功能的“钥匙”,无损害则无赔偿。大多数学者认为,损害后果是引发赔偿的必备条件,受害人只有遭受法律认可的损害,才能要求加害人承担损害赔偿赔偿责任。长期以来,鲜有国家在法律层面对损害的概念进行明确的界定,我国《民法典》《个人信息保护法》等现行法律对此也无规定。在损害认定中,德国学者提出的“差额说”占据重要地位,该理论主张通过对比受害人在侵权行为发生前后的利益状态来确定损害,将两者间的差额认定为损害数额。^[11] “差额说”在物质损害与非物质损害赔偿领域均得到学界认可,同时在司法实践中得到广泛适用。损害的构成通常须满足三个要件:侵害合法民事权益、可补救性与确定性。其中,确定性是核心要素,要求损害后果客观真实,或损害在未来必然发生,而不能基于受害人主观臆测或推断。^[12] 数字时代个人信息侵权导致的损害具有其特殊性,这使得传统侵权法的损害认定规则面临严重挑战。

首先,数字时代个人信息侵权产生了新型损害,这些损害已明显超出传统侵权法规范场域。例如,在商业利益驱动下,侵权人利用算法对消费者信息进行不合理的收集、分类与筛选,给信息主体贴上不同标签实施不公平的差别化服务,从而对部分消费者形成歧视,造成了消费者权益的损害。

其次,数字时代个人信息侵权所致损害往往难以通过“差额说”科学量化,这与损害认定的“确定性”要素存在抵牾。与传统侵权损害相比,此类损害具有以下特点。一是无形性。数字时代的算法技术导致个人信息侵权损害往往较为抽象,难以直接观测。二是潜在性。个人信息侵权所致风险通常不会立即对信息主体产生不利影响,而是对其财产状况与精神状态构成潜在威胁。三是不确定性。个人信息流转速度较快、频率较高,信息主体难以确定其信息是在收集、存储、共享的哪一具体环节中遭受侵害,更难以准确评估由此造成的损失。尽管第六十九条第一款规定个人信息侵权责任的承担以损害后果为前提,但当前并未明确以下问题:该损害是仅指现实损害,还是也包含风险性损害;损害范围是仅限信息泄露本身,还是亦涵盖下游损害;损害范围是否包括精神损害。立法的不足导致司法实践中个人信息侵权纠纷救济不够,侵权人通常仅需承担赔礼道歉等非赔偿性民事责任,而受害人财产损失与精神损害赔偿诉求往往难以获得法院支持。

再次,以风险性损害为基础,衍生出两种新型损害。其一,预防性费用,即受害人为防范风险转化为现实损害而采取预防措施的合理开支,例如,信息泄露后受害人购买防盗保险、信息安全监测服务等支出;^[13] 其二,精神损害,即信息泄露后受害人对未来可能遭受身份盗窃、财产损失等不利后果产生焦虑、恐惧等不良情绪。当前,理论界与实务界对这两类损害项目的认定存在较大争议:一是预防性费用可否纳入财产损害范畴从而获得赔偿;二是受害人因风险产生的内心焦虑情绪,如何克服精神损害赔偿“严重”要件的限制,从而获得法律救济。

总体而言,当前立法对个人信息侵权场景中的损害认定问题,特别是风险性损害的认定问题,无论在学理研究还是司法实践层面均未达成共识,这挫伤了受害人维权的积极性,对个人信息保护产生了不利影响。

(三)个人信息侵权精神损害赔偿规则过于笼统

数字时代个人信息具有双重利益属性,一是固定的人格属性,二是天然的财产价值。有学者将这两者概括为个人信息的自主价值与使用价值。自主价值强调信息权益人对信息的自主控制,旨在保证个人身份完整性;使用价值则体现为信息通过公开流转为个人带来经济效益。^[14]因此,个人信息侵权损害赔偿需同时兼顾财产利益和精神利益。第六十九条第二款规定了个人信息侵权损害赔偿数额的计算规则,分为两个层次,第一层次为“实际损失”赔偿规则与“侵权人获利”赔偿规则,二者为平行关系,即分别根据受害人所受损失或侵权人所获利益确定赔偿数额;第二层次为“法院酌定”赔偿规则,即在第一层次的两重赔偿方式无法确定赔偿数额时,由司法机关结合具体案情确定赔偿数额。

就个人信息侵权所致财产损失赔偿而言,适用第六十九条的损害赔偿规则并无不妥。例如,在个人信息泄露导致受害人遭受电信诈骗时,可适用“实际损失”赔偿规则,确定直接经济损失为赔偿数额。此外,受害人为防范未来风险而支出的合理预防性费用,以及聘请律师等的正常维权费用,均可纳入“实际损失”的范畴获得赔偿。

当前主要争议在于,第六十九条第二款关于个人信息侵权精神损害赔偿数额如何计算,在理论界与实务界均存在较大争议,相关规则亟待进一步完善。

首先,在理论层面,第六十九条第二款关于损害赔偿的性质问题引起了学界广泛讨论。部分学者主张该条款性质为“财产损失说”,认为其仅是个人信息侵权财产损害赔偿的请求权基础,并不适用于精神损害赔偿。其理由在于:从我国现行法律体系来看,第二款中的“损失”通常指物质上的纯粹经济损失,不包含“精神损害”。^[15]笔者认为,上述观点有失偏颇,从条款内容看,尽管该条款来源于《民法典》第一千一百八十二条,但二者在表述上明显不同,前者表述为“前款规定的损害赔偿责任”,而后者则具体指明为“财产损失”,即“侵害他人人身权益造成财产损失”。^[16]因此,第六十九条第二款“损害赔偿”的性质应理解为“全部损害说”,即侵害个人信息权益所造成的财产损失和精神损害,都可适用该条款确立的损害赔偿数额计算规则。目前,该学说已获得学界多数学者的支持。^[17]

其次,尽管第六十九条第二款可作为信息权益受害人精神损害赔偿的请求权基础,但其具体适用却存在明显缺陷。具体表现为:在精神损害赔偿中,“实际损失”赔偿规则与“侵权人获利”赔偿规则缺乏适用空间。一方面,精神损害往往具有无形性与难以计量性,使得受害人难以举证侵权行为前后的实际损失数额;另一方面,侵权人获利涉及数据企业的商业秘密,受害人通常难以取证。此外,当前对处理者商业化利用个人信息的获利欠缺统一与合理的计算标准。因此,就精神损害赔偿而言,无论是“实际损害”还是“侵权人获利”赔偿规则均难以适用。因此,个人信息侵权精神损害赔偿数额往往由法官根据案件实际情况酌情确定。

最后,由法院根据案件实际情况酌情确定赔偿数额的方式也存在不足。其一,第六十九条第二款损害赔偿规则未明确法院酌定数额具体范围,可能导致司法机关自由裁量权的不当扩张。一方面,发生大规模个人信息侵权案件时,如果侵权人为数据企业,赔偿数额上限缺失可能会给侵权人带来沉重经济负担,侵权人对具体赔偿数额难以形成合理预期,这不利于数字产业健康发展;另一方面,赔偿数额下限缺失可能导致受害人诉讼成本与所获赔偿数额之间严重失衡,这将打击受害人维权的积极性,不利于保护个人信息权益。其二,第六十九条第二款损害赔偿规则未明确司法机关在确定侵权赔偿数额时的具体考量因素,导致该规则可操作性差,无法应对频繁发生的个人信息侵权案件。

综上所述,第六十九条第二款在计算个人信息侵权精神损害赔偿数额时,“实际损失”赔偿规则与“侵权人获利”赔偿规则的适用存在一定局限性,“法院酌定”赔偿规则存在数额范围不明确、考量因素不具体等缺陷,亟待进一步完善。

三、数字时代个人信息的侵权法保护完善建议

鉴于第六十九条在归责原则、损害认定、精神损害赔偿数额计算三个维度存在的不足,有必要基于数

字时代个人信息侵权的特殊性优化相关规则。

(一)构建个人信息侵权二元归责体系

随着科学技术的快速发展,人们对损害赔偿的理解进一步深化,导致侵权法领域诞生了无过错责任原则,其适用迅速扩展至工伤事故、交通事故和产品责任等私法领域。近年来,无过错责任原则的普遍化适用一直是学界讨论的热点话题。当前,无过错责任原则的适用已逐渐延伸到个人信息侵权领域。鉴于单一适用过错推定原则的局限,有必要引入无过错责任原则,以构建更完善的归责原则体系。

首先,个人信息侵权领域适用无过错责任原则在比较法上已有先例。2018年德国《联邦数据保护法》第八十三条第一款规定,处理者使用自动化技术侵害个人信息时,适用无过错责任原则。^[8]^[15]域外有学者主张在个人信息侵权领域应适用无过错责任原则。例如,有学者认为,对于公权力机关侵害个人信息权益的行为应适用无过错责任原则,因为公权力机关的信息获取、控制能力较强,在数据利用上具有显著优势,采用无过错责任原则有助于强化其对个人信息的注意和保护义务。^[18]

其次,个人信息侵权领域适用无过错责任原则有助于解决证据偏在难题,进而从根本上改善个人信息保护不充分的现状。在自动化技术的加持下,信息处理者在相关证据的掌握上占据显著优势,仅依靠过错推定责任原则难以打破双方诉讼能力不对等的局面,只有引入无过错责任原则,才能根除“过错”要件对受害人救济的制约,有效维护其合法权益,实现实质公平。

最后,个人信息侵权领域适用无过错责任原则有助于实现《个人信息保护法》信息保护与利用的平衡目标。数字社会中,个人信息具有双重价值:一方面,个人信息体现了信息权益人的主体价值,承载着个人的尊严与行动自由,应当强化信息安全保护;另一方面,个人信息具有显著的社会和商业价值,应当促进其有效流通与利用。针对不同个人信息类型,保护与利用的侧重应不同。对一般信息,应侧重其流通与有效利用;而对敏感信息,则应对其严格保护。因此,在个人信息侵权纠纷中,针对不同个人信息类型适用不同归责原则是更合理的选择。在敏感个人信息侵权案件中引入无过错责任原则,能够提供更有力的保护。例如,有学者主张,鉴于金融账户信息财产属性突出、利用价值较高,应对其区分适用过错推定与无过错责任原则:对于一般个人金融信息适用过错推定原则,而对于含有“金融”属性的个人金融信息及其他衍生信息则适用无过错责任原则。^[19]另有学者认为,鉴于生物识别信息具有唯一性与强身份识别性,适用无过错责任原则更符合其固有特征,从而能更有效地保护个人人身和财产安全。^[20]

总之,在过错推定原则基础上引入无过错责任原则,对于不同个人信息类型提供差异化保护,这种“分而治之”的策略能够为信息主体合法权益提供更合理的保护。

(二)科学认定个人信息侵权损害范围

风险性损害可否归入传统损害范畴并获得赔偿,学界尚未形成共识。进入数字时代,个人信息处理活动所致风险日益凸显。在此背景下,修正传统损害概念,认可侵害个人信息权益所致风险成立损害具有正当性。

首先,个人信息侵权领域认可风险成立损害,可有效分配风险,从而有助于治理风险社会。大规模个人信息侵权案件频发,表明当前社会风险程度正持续升高。承认风险性损害成立,一方面让开启危险源并获得收益的处理者负担风险,从而抑制其对信息的滥用,能够更有效地保护信息主体合法权益;另一方面,与信息主体相比,数据企业具有更强的风险防范能力。通过敦促其积极采取风险防范措施,可有效预防、分散风险。

其次,认可风险成立损害在其他领域已有先例。风险能否纳入损害范围的争议在其他领域早有讨论,并非始于也并不仅限于个人信息侵权领域。在环境侵权、医疗损害责任与毒物侵权领域,风险性损害已获得普遍认可。例如,在医疗侵权领域,医生的误诊行为可能导致患者未来出现严重损害后果的风险显著增加,这种风险变化即构成损害。我国立法尽管尚未承认该风险性损害,但比较法上已有先例予以认可。例如,在英国 *Hoston v. East Berkshire Area Health Authority* 案中,医生延误诊治导致原告患缺血性坏死疾病的风险增加了 25%,法院认为该风险变化构成损害。^[21]因此,个人信息侵权领域认可风险成

立损害有助于有效地保护个人人身、财产利益,从而进一步完善我国侵权损害赔偿制度。

再次,个人信息侵权领域认可风险成立损害,不会对现有法律制度和传统理念产生过大冲击。如前所述,认定传统损害可采用“差额说”作为判断依据,而侵权法意义中的损害还需满足“确定性”要件。具体到个人信息侵权领域,一方面,当前鲜有立法明确规定损害概念,可通过修正差额说承认风险性损害。在具体适用时,不应将“差额”僵化解释为损害数额的差额,而应灵活解释为侵权行为发生前后的“状态差额”。非物质性损害通常不如物质性损害直观和具体,难以通过数值差直接呈现,但二者共性在于均导致受害人发生“状态变化”。因此,通过“状态差额”能够更好地兼顾物质性与非物质性损害。另一方面,尽管个人信息权益侵害风险与损害的“确定性”要件之间确实存在一定差距,但二者间矛盾并非不可调和。损害真实确定并不等于损害已然发生,符合特定条件的风险仍可能满足损害“确定性”要件。可扩张解释传统损害“确定性”要件,以顺应数字时代发展,赋予其新内涵。欧盟《通用数据保护条例》(GDPR)明确表示,数字时代有必要对个人信息侵权所致损害灵活解释。^[22]此外,部分域外学者主张扩张解释损害范围,认为个人信息侵权行为具有隐蔽性、复杂性、技术性特征,应认可个人数据泄露所致风险构成损害的可能性。^[23]司法实践中,多数法院认为,如果未来风险满足“实质性”标准,则可视满足损害“确定性”要件。这需要法官在个案中合理考量相关因素以判断侵害风险是否足够“实质”与真实客观,进而排除那些毫无根据、捕风捉影的主观臆测。因此,数字时代,对侵害个人信息所致风险不宜采取“全有全无”的认定标准,而应在修正传统“差额说”与损害“确定性”标准的基础上,由法官在个案中具体判断,选择性地承认那些在未来可能真实发生的客观合理风险。

最后,因个人信息侵权风险产生的预防性费用与精神焦虑,应分别纳入财产损失与精神损害赔偿范围。第一,信息主体因风险性损害产生的预防性费用,可通过扩大解释将其纳入维权费用范畴,从而获得赔偿。该做法合理性在于,预防性费用与维权费用在侵权法视角下具有共性,维权费用是受害人为防止损害进一步扩大所付费用,其源于侵权法补偿功能;预防性开支则是受害人为防止风险进一步现实化所付费用,其源于侵权法预防功能。由于侵权法的补偿与预防功能间本就密切联系、相互配合,因而维权费用与预防性支出本质相同。值得注意的是,预防性支出要纳入维权费用需满足一定条件,即并非所有预防性支出均有可赔偿性。法官应结合具体案情,以侵权风险的确定性、危险性、紧迫性为基础,以正常人生活标准为参照,考虑信息类型与私密程度等相关要素,综合判断受害人预防性支出费用的必要性,超出正常人合理预期的部分不应予以赔偿。第二,信息主体因风险性损害所致焦虑情绪,可通过动态系统论突破“严重”要件对精神损害赔偿诉求的制约。应明确的是,在个人信息侵权领域中,精神损害赔偿仍需满足“严重”要件。原因在于,“严重”是我国民法上具有价值开放性的不确定概念,^[25]其设置旨在使法官在个案中平衡信息主体民事权益保护与处理者经营自由两种价值取向,进而灵活判断信息主体精神损害是否达到“严重”程度。若第六十九条未延续《民法典》第一千一百八十三条精神损害“严重”要件,则可能导致受害人因收到垃圾短信等轻微损害即主张行为人赔偿其精神损害,不利于保障处理者行为自由。明确个人信息侵权精神损害后果仍须满足“严重”要件后,可引入动态系统论考量精神损害。动态系统论旨在通过兼具多元性与层次性的评价要素,促进法律效果的弹性认定,从而克服审判要件过于“僵化”的弊端。具体而言,以《民法典》第九百九十八条规定的三项评价因素为基础,再辅以信息类型、数量等要素,以适应个人信息侵权领域损害认定的特殊性。首先,行为人与受害人职业是首要考虑的因素。原因在于:职业所涉公共利益将影响损害结果认定,行为人职业若与舆论监督等公共利益相关,法官不应认定损害后果;若原被告在技术能力上差距明显,法官可适当放宽证明标准,对损害后果综合认定。个人信息侵权行为具有损害无形、技术垄断等特点,被告往往在证明责任中占据优势,法官应充分考虑受害人不利处境,对其损害后果从宽认定。其次,损害后果辐射范围与行为目的、方式、后果均属于损害评价体系中的一般性要素。损害后果辐射范围越广,则越容易认定损害后果的发生。最后,应对信息类型、数量进行更深入考量。与一般信息相比,敏感信息更易对个人人格尊严、财产安全造成损害,应放低“严重”要件认定

标准;行为人一次性侵犯个人多条信息时,更容易证明损害存在。

(三)优化个人信息精神损害赔偿规则

针对第六十九条第二款法院酌定精神赔偿数额规则的不足,应从“赔偿数额区间不确定”与“具体考量因素不清晰”两个维度分别予以完善。

首先,应确定科学合理的精神损害赔偿数额区间。一方面,应规定最低赔偿限额,惩治处理者的侵权行为,切实保护信息主体合法权益;另一方面,应规定最高赔偿限额,在保护受害人精神利益时,充分考量行为人的经济承受能力,避免出现“天价赔偿”。我国侵害个人信息权益精神损害赔偿最低与最高赔偿数额的确定,应立足我国经济发展实际情况。具体而言,有学者认为,最低赔偿数额可根据我国居民月人均可支配收入确定,而最高赔偿数额不得超过上一年度我国居民年人均可支配收入。^[25]笔者认为,依据这种方式确定最高与最低限额具有显著合理性及科学性。一方面,设定赔偿数额具体上下限有利于增强可操作性;另一方面,这种计算方式具有一定的发展性,即该上下限额并非固定不变,而是根据我国社会发展变化而持续调整,能够与时俱进,因此更为科学。

其次,在确定精神损害赔偿数额上下限之后,有必要进一步确定法官酌定数额的考量因素,以进一步增强赔偿数额的可接受性,实现个案正义。在选择考量因素时,较全面稳妥的做法是,从最高人民法院认定精神损害赔偿数额的参考要素中进行合理选择。《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》(以下简称《精神损害赔偿解释》)第五条规定了确定精神损害赔偿数额的六种参考因素。^①然而,在认定个人信息侵权精神损害赔偿数额时,部分因素显然不具有适用性,应予去除。例如,“侵权行为所造成的后果”这一要素,缺乏具体参考标准,受害人在举证时无从下手;又如,“侵权人的获利情况”与“侵权人获利”赔偿规则一致,前文已述及其存在较大缺陷,难以有效救济受害人信息权益,在此不再赘述;再如,“受理诉讼法院所在地的平均生活水平”这一要素也不全面,在大规模个人信息侵权案件中,受害人通常分布广泛,仅根据受理法院地区平均生活水平确定精神损害赔偿数额,显然不具合理性。

最后,应结合数字时代个人信息侵权的特殊性,对考量因素进行合理补充。例如,有学者提出,在酌定具体数额时,可参考侵权人身份、侵权行为目的、个人信息类型与数量及损害持续时间等因素。^[26]有学者认为,可依据侵权人主观状态、行为方式及损害后果影响范围确定具体赔偿数额。^[27]结合数字时代侵害个人信息权益精神损害的特殊性,在对《精神损害赔偿解释》第五条中酌定要素进行合理取舍与梳理学界观点的基础上,笔者认为可按如下方式确定具体损害数额:将考量因素划分为个人信息处理活动、受害人个人信息与损害后果情况三个维度分别确定。在个人信息处理活动层面,可选取行为人的主观状态、身份背景及侵权目的确定赔偿数额;在受害人个人信息层面,可根据个人信息的利用价值、受害人个人信息数量确定赔偿数额;在损害后果层面,可依据损害后果持续时间、损害后果影响的地域范围确定赔偿数额。根据以上考量因素确定总体赔偿数额后,可从以下两方面对数额适当酌减:一是行为人的经济负担能力。若其难以负担法院酌定的赔偿数额,可适度进行酌减;二是侵权人事后采取补救措施的积极性及处理效果。由于个人信息侵权行为发生与下游侵害风险转化为现实损害之间往往存在较长时间间隔,在损害发生前,处理者可采取一定措施补救。此时,如果行为人通过及时修复系统漏洞、上缴侵害个人信息权益所得或协助信息主体采取合理措施等以降低未来风险,则可适当酌减赔偿金额。

四、结语

信息之于数字经济如同石油之于工业革命,信息已成为数字时代的核心战略资源,对人们的生产生活方式产生了深远影响。与其他权益相比,个人信息承载着多元利益和价值,容易成为不法分子牟利的

^① 《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条规定:“精神损害赔偿数额根据以下因素确定:(一)侵权人的过错程度,但是法律另有规定的除外;(二)侵权行为的目的、方式、场合等具体情节;(三)侵权行为所造成的后果;(四)侵权人的获利情况;(五)侵权人承担责任的经济能力;(六)受理诉讼法院所在地的平均生活水平。”

侵害对象,个人信息侵权事件高发,个人信息安全问题日益严重。在《个人信息保护法》已实施的背景下,如何进一步优化个人信息权益保护规则,是当前理论界与实务界关注的热点问题。

在个人信息私法保护视角下,应对第六十九条个人信息侵权保护规则进行升级,以适应数字时代个人信息保护需求。在归责原则方面,应在现有过错责任推定原则的基础上引入无过错责任原则,使兼顾个人信息权益保护与促进个人信息合理流通的立法目的得以落实。在损害认定方面,承认下游侵害风险成立损害具有相当的正当性,在更新“差额说”的基础上可将满足特定条件的风险纳入损害范畴;此外,应将预防性支出与信息主体内心焦虑分别纳入财产损失与精神损害范畴进行赔偿。在精神损害赔偿数额计算方面,主要采取法院酌定赔偿规则,可从确定赔偿数额区间与明确具体考量要素两个维度进行优化。

参考文献:

- [1] 叶名怡. 个人信息的侵权法保护[J]. 法学研究, 2018(4): 83-102.
- [2] 段莉琼, 谭静宜. 大规模个人信息侵权中非物质性损害的要件认定及救济导向——广州市越秀区人民检察院与郑某、任某等个人信息保护公益诉讼案[J]. 法治论坛, 2024(1): 241-250.
- [3] 韩世鹏. 算法价格歧视的规制困境与治理新解——基于算法解释权的视角[J]. 科技与法律(中英文), 2022(6): 90-98.
- [4] 程啸. 侵害个人信息权益的侵权责任[J]. 中国法律评论, 2021(5): 59-69.
- [5] 王道发. 个人信息处理者过错推定责任研究[J]. 中国法学, 2022(5): 103-121.
- [6] 吴诗怡, 余向阳. 敏感个人信息侵权法律适用之完善——以 23 个司法案例为样本[J]. 黑龙江省政法管理干部学院学报, 2024(3): 87-92.
- [7] 袁俊宇. 个人信息侵权责任的归责困境与消解路径[J]. 数据法学, 2023(1): 61-76.
- [8] 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+172.
- [9] 程啸, 李西岭. 论个人信息侵权责任中的因果关系[J]. 郑州大学学报(哲学社会科学版), 2023(1): 19-25+127.
- [10] 王泽鉴. 侵权行为[M]. 北京: 北京大学出版社, 2016: 175-176.
- [11] 叶雄彪. 个人信息侵权的理论反思与规范构建[J]. 齐鲁学刊, 2023(6): 88-101.
- [12] 钱进. 个人信息侵权的规范构造[J]. 中国政法大学学报, 2023(5): 186-201.
- [13] 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(5): 198-211.
- [14] 李昊. 个人信息侵权责任的规范构造[J]. 广东社会科学, 2022(1): 249-260.
- [15] 郭明龙, 杨孝康. 论个人信息大规模微额损害的私法救济路径完善[J]. 天津法学, 2023(4): 86-98.
- [16] 程啸, 曾俊刚. 个人信息侵权的损害赔偿赔偿责任[J]. 云南社会科学, 2023(2): 99-110.
- [17] 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.
- [18] SCHMITZ A J. Secret consumer scores and segmentations: Separating “Haves” from “Have-Nots”[J]. Michigan state law rereview, 2014(5): 1411-1433.
- [19] 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(5): 120-130.
- [20] 朱沛智. 个人生物识别信息侵权责任研究[J]. 甘肃政法大学学报, 2024(5): 42-51.
- [21] 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.
- [22] 刘云. 论个人信息非物质性损害的认定规则[J]. 经贸法律评论, 2021(1): 60-72.
- [23] WILT J. Cancelled credit cards: Substantial risk of future injury as a basis for standing in data breach cases[J]. SMU law review, 2018(2): 615-621.
- [24] 朱震. 论侵害人格权精神损害赔偿中的“严重”[J]. 法制与社会发展, 2022(2): 136-153.
- [25] 邓环宇. 侵害个人信息权益所致精神损害的赔偿额计算[J]. 北方法学, 2024(2): 141-160.
- [26] 李东宇. 论侵害个人信息权益的精神损害赔偿[J]. 财经法学, 2023(4): 134-148.
- [27] 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.

(下转第 57 页)

- [42] 韩世远. 合同法总论: 第四版[M]. 北京: 法律出版社, 2018: 834.
- [43] 郑爱青. 从英法劳动法判例看劳动法上的忠实义务与竞业限制条款——对我国《劳动合同法》规范竞业限制行为的思考和建议[J]. 法学家, 2006(2): 144-145.
- [44] 法国民法典[M]. 罗结珍, 译. 北京: 北京大学出版社, 2023: 661.
- [45] 史尚宽. 债法总论[M]. 北京: 中国政法大学出版社, 2000: 523.
- [46] 雷继平. 违约金司法调整的标准和相关因素[J]. 法律适用, 2009(11): 24.
- [47] 谢德成. 涉密型雇员流动的法律规制[J]. 法学, 2021(8): 180.

Applying the Civil Law Rules to Adjust Damages for Breach of Non-Compete Agreements

SUN Haoran

(Civil, Commercial and Economic Law School, China University of Political Science and Law, Beijing 100091, China)

Abstract: Article 23 of the *Labor Contract Law of People's Republic of China* stipulates that an employer may enter into a non-compete agreement with a specific employee and specify liquidated damages for breach of the agreement. Given the significant disparity in status and negotiating power between employers and employees, employers often impose substantial liquidated damages, which threatens the basic economic interests of employees. Although the current statutory referral mechanism for adjusting non-compete penalties to civil law rules encounters impediments, these impediments are demonstrably surmountable. To surmount these impediments, the adjustment of non-compete liquidated damages should be divided into two stages: adjustment of the agreed-upon amount and adjustment of the performance amount. Factors, such as “contracting parties”, “negotiating strength”, “fault”, and “performance”, should be specifically applied to the adjustment process in both stages.

Key words: non-compete; adjustment of liquidated damages; pressure imposed by liquidated damages; applying by reference

(责任编辑: 董兴佩)

(上接第 47 页)

On the Legal Protection of Personal Information in the Digital Age

LI Fengxia, LI Chuqing

(School of Humanities and Law, China University of Petroleum, Qingdao, Shandong 266580, China)

Abstract: In the digital age, personal information has become an essential medium for the life, production activities and social interactions of natural persons. However, in practice, frequent occurrences of information handlers illegally obtaining, arbitrarily disclosing, and excessively using personal information severely infringe upon individuals' rights to their information. The widespread application of big data technology gives information handlers a significant advantage in data control, making such infringements often highly concealed. Moreover, the severe imbalance in the ability to provide evidence between information subjects and handlers poses a serious challenge to the private law protection of personal information. Although the *Civil Code* and the *Personal Information Protection Law* have stipulated liability for personal information infringement, there are still issues with rigid application in judicial practice. To address this, it is necessary to further standardize the application of liability for personal information infringement. In this context, it is imperative to introduce the principle of non-fault liability, and to establish a dual liability framework that includes both the principles of fault and no-fault liability. This involves revising the traditional “Discrepancy Theory” to accurately clarify the boundaries of personal information infringement. Furthermore, to protect personal information rights in the digital age, it is also essential to enhance the mechanisms for calculating compensation for mental damages, which can be achieved by determining the scope of damages and clarifying the factors to be considered in such calculations.

Key words: digital era; personal information; principle of attribution; compensation for mental damages

(责任编辑: 董兴佩)