

论数据信息损害的承认与救济

张凌寒*

内容提要 无损害则无赔偿,承认损害是民事救济的前提。个人信息和数据非法处理等行为可能引致非物质性数据信息损害,但其却因与传统损害要素不兼容而难获法律承认。本着风险分配与公共治理的观念,发挥侵权制度的个体救济与风险预防功能,承认数据信息损害的独立性具有制度必要性和学理可行性。回溯从工业时代到数字时代的社会生产方式变革可以发现,传统损害概念实质是基于社会生产方式而建构的。这为承认数据信息损害提供了充分的法理依据,可解决不确定性、因果关系和个体显著性的制度障碍。数据信息损害救济的实现一方面需要将已经发生的个人信息数据被非法收集、访问、泄露与丢失等直接数据信息损害法定化,并对后续数据信息损害进行类型化扩容,承认典型常见的非物质损害类型;另一方面,对微小系统性的数据信息类损害应采用公益诉讼的方式进行救济,并以法定赔偿方式加以衡量。

关键词 数据信息损害 个人信息 损害法定化 公益诉讼 法定赔偿

目 次

- 一、问题的提出
- 二、数据信息损害独立性之证成
- 三、承认数据信息损害的法理依据
- 四、数据信息损害的救济规则调整
- 五、结语

* 中国政法大学数据法治研究院教授。本文系2023年度国家社科基金重点项目“生成式人工智能的法律定位与分层治理研究”(项目批准号:23AFX009)的阶段性成果。

一、问题的提出

损害既是大陆法系侵权法的核心概念,也是民事责任存在的前提。无损害则无赔偿,因他人的不法行为而引发的损害赔偿请求权,须以受有实际损害为要件。我国《民法典》延续了现代侵权法“损害—赔偿”模式的法律制度,于第1165条第1款规定:“行为人因过错侵害他人民事权益造成损害的,应当承担侵权责任”。某种特定类型的后果是否能被认定为损害、在何种程度上被计入损害,直接决定了法律责任的有无与范围。

近年来,个人信息和数据的处理已经成为数字经济运行和政府公共治理的必需,但数据非法收集、滥用、泄露等频频给个人造成物质与非物质损害,且影响广泛。其中,因个人信息和数据非法处理造成的物质损害(如虚拟财产被盗)在实践中的认定和衡量几无争议,但就非物质损害(以下简称“数据信息损害”)在法律上的界定与赔偿衡量等则尚未有明确规则。由于此类损害为非物质性且难以计算,法院往往以原告没有证明遭受了实质性损害为由驳回其损害赔偿的诉讼请求。例如在“朱烨诉百度案”中,朱烨主张定向广告侵害其隐私、造成精神痛苦,百度上诉后,法院以信息处理行为并未对受害人造成“事实上的实质性损害”为由,不支持受害人个人信息权益的侵权损害赔偿请求。^①在“付全贵与北京三快信息科技有限公司等网络侵权责任纠纷案”中,原告的财产损害赔偿请求获得了支持,但精神损害赔偿请求被驳回。即使原告遭遇诈骗,法院仍然认为其并未遭受严重的“精神痛苦”。^②对数据信息损害难以直接适用传统损害赔偿制度,使得个体获得损害赔偿救济面临困境。

然而,相比个人的数据信息损害难以获得损害赔偿,企业的数据信息损害在司法实践中已经获得广泛承认与救济。例如,平台企业可通过知识产权保护与反不正当竞争法获得数据信息损害的赔偿救济;在多个“流量劫持”案件中,法院均认定无形的“流量”损失构成企业遭受的“损害”;^③甚至损害的“未来不确定性”也并未成为认定损害赔偿额度的障碍,法院承认网络不正当竞争行为对未来预期利益的损害,并在被告获利基础上追加部分赔偿额度。^④

个人遭受的数据信息损害无法被传统损害认定规则涵摄,造成了诸多不公正后果。首先,个人无法获得有效救济。在许多场景中,隐私、个人信息保护、消费者保护和平台劳工权益保护等本应通过损害启动的救济,却因个人遭受的数据信息损害不被侵权法所承认而无法获得充分的保护。其次,由于数据信息损害无法被准确预测和精确化,个人

^① 参见江苏省南京市中级人民法院(2014)宁民终5028号民事判决书。

^② 参见北京互联网法院(2018)京0491民初1905号民事判决书。

^③ 参见上海知识产权法院(2019)沪73民终241号民事判决书;浙江省杭州市中级人民法院(2020)浙01民终8743号民事判决书;北京知识产权法院(2021)京73民终1092号民事判决书。

^④ 例如,在腾讯公司诉科贝公司不正当竞争案的判决中,法院考量了被诉不正当竞争行为对腾讯公司产业生态造成损害的各种情节,追加了部分赔偿额。参见杭州铁路运输法院(2018)浙8601民初1020号民事判决书。

无法获得有效、完全的赔偿,或者赔偿数额极低。最后也最重要的是,私权救济路径的不畅导致此类损害的救济过于倚重行政监管,形成路径依赖。然而受制于资源和法律授权限定,行政监管往往是不充分的,在应对灵活多变的数据信息损害问题时难免捉襟见肘。因此,亟需革新并发展损害认定与计量的法理依据与法律规则,以使数据信息损害能够获得充分而精准的司法救济。

二、数据信息损害独立性之证成

数据信息损害具有不可忽视的独立性,具备获得法律承认的必要性与可行性。国外已有立法关注到了这一问题。例如,欧盟《通用数据保护条例》(GDPR)第82条第1款规定,“任何因为违反本条例的行为而遭受物质性或非物质性损失的人,都有权就所遭受的损失获得数据控制者或者数据处理者的赔偿”。然而,我国现有立法尚未充分承认数据信息损害的独立性,使得大量损害难以被认定和衡量,进而导致法益保护出现空白地带。从法释义学层面证成数据信息损害的独立性,成为当务之急。

(一) 个人数据信息损害类型

从类型化视角看,依据损害与权益被侵害之间因果远近的不同,可将数据信息损害分为直接损害和后续损害两类。^⑤

数据信息直接损害指个人信息与数据被非法收集、访问、不当处理、泄露与丢失等。侵害个人信息和数据权益引发的直接损害后果主要有两种类型:一是同时引发的对《民法典》已确定的人格权的损害;二是人身和财产安全风险上升。就前者而言,要么数据信息损害被人格权损害吸收,要么侵害个人信息权益可能并未牵连侵害隐私权、名誉权等其他人格权,但当事人无法证明精神损害的存在。^⑥单纯的数据信息加害行为在民事诉讼中大多诉诸隐私权纠纷或个人与信息保管者的合同纠纷。然而,隐私权损害范围要明显小于数据信息类损害,且其判断以“严重的精神损害”为标准,而一般数据信息类的民事侵权难以达到这一标准。例如在“王取、中国联合网络通信有限公司天津市分公司一般人格权纠纷案”中,原告败诉的原因即未证明被告使用原告个人信息的行为造成了实际损失。^⑦就后者而言,单纯的安全风险上升并不被前风险社会的“自然损害”概念所涵盖,因而也无法被主流民法学说认定为损害。例如,数据信息损害如果尚未造成信用卡盗用等结果,即无法被实定法认定为损害。因此,尽管个人信息泄露会使受害人

^⑤ 也有学者将其分为侵害信息安全与信息权利的损害,个人信息权利的直接损害与间接损害,上游下游损害等。参见商希雪:《侵害公民个人信息民事归责路径的类型化分析——以信息安全与信息权利的“二分法”规范体系为视角》,载《法学论坛》2021年第4期,第100页;程啸:《论侵害个人信息的民事责任》,载《暨南学报(哲学社会科学版)》2020年第2期,第44页;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23页。

^⑥ 参见前注^⑤,程啸文,第46页。

^⑦ 参见天津市第二中级人民法院(2020)津02民终4520号民事判决书。

在未来发生次生损害的风险显著增加,但都很难基于“差额说”获得认可。^⑧英美法国家的状况与此基本相同,在美国一系列数据泄露案件中,即便受害人对数据保管者提出诉讼,被告的一般回应也是:既不否认数据泄露的发生,也不辩解自身的行为是否是造成数据泄露的罪魁祸首,而是声称原告没有遭受“事实上的伤害”,除非原告能证明第三方滥用数据造成了金钱损害。^⑨

数据信息后续损害,指由于个人信息与数据的滥用与泄露造成的后续损害后果,包括但不限于身体或精神损害、身份被盗用、失业或遭受歧视性待遇、个人丧失机会或福利、个人受到监视的行为限制等。此类损害后果多样,但大多因形式不被法律承认的无形损害所容纳、因果关系难以证明和个体显著性不足而难以被认定为可赔偿的损害。典型的后续损害体现为:(1)歧视与机会丧失。诸如银行借助算法从海量用户中挖掘出“优质”客户;招聘者利用算法从应聘者中筛选出“完美”员工等自动化决策的不利后果体现为个人未来机会的丧失而非既有利益的剥夺,如银行不予提供贷款、公司不予录用等。^⑩当这类自动化决策可能构成对群体的系统性歧视,如女性在共享经济平台招聘与分配工作机会时遭受不利待遇^⑪、互联网金融与保险广告屏蔽女性与老年人^⑫等。虽然物理世界中的歧视是违法的,由此导致的机会丧失在部分国家和地区也有可能获得赔偿,但基于数据信息造成的此类歧视却往往不受约束。美国社交媒体“脸书”截至2020年已面临三起诉讼和两个平等就业机会委员会的投诉,却仍能基于其互联网服务提供者地位免除法律责任。^⑬个人无法证明歧视与机会丧失,也难以证明因此遭受了人身和财产损害,由此造成的困境需要通过扩张法律承认的非物质损害来解决。(2)个体遭受操纵与控制。如内容平台通过“无底碗”认知理论或随机奖励鼓励用户“沉迷”,^⑭操纵个体的行为与情感体验^⑮等。物理世界中,因欺诈、乘人之危、强迫交易等违背个体意思自治缔结的合同之效力存在问题,但基于数据信息轻推与操纵个体自主决策目前并未被认为是违法行为,因而也不产生合同效力瑕疵的问题。

⑧ See Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, Texas Law Review, Vol.96:737, p.751 (2018).

⑨ See Seth F. Kreimer, “Spooky Action at a Distance”: *Intangible Injury in Fact in the Information Age*, University of Pennsylvania Journal of Constitutional Law, Vol.18:745, p.763 (2016).

⑩ See Pauline T. Kim, *Data-Driven Discrimination at Work*, William & Mary Law Review, Vol.58:857, p.885 (2017).

⑪ See Naomi Schoenbaum, *Gender and the Sharing Economy*, Fordham Urban Law Journal, Vol.43:1023, p.1048-1049 (2016).

⑫ See Jonathan Stempel, *Facebook Sued for Age, Gender Bias in Financial Services Ads*, Reuters (Nov. 1, 2019), at <https://www.reuters.com/article/us-facebook-lawsuit-bias-idUSKBN1XA2G8> (Last visited on Apr. 21, 2024).

⑬ See Pema Levy, *Should Facebook Be Held Liable if Its Advertising Algorithm Discriminates?*, Mother Jones (Jun. 9, 2021), at <https://www.motherjones.com/politics/2021/06/facebook-discrimination-lawsuit-ads/> (Last visited on Apr. 21, 2024).

⑭ See Pelle Guldberg Hansen, *The Definition of Nudge and Libertarian Paternalism: Does the hand Fit the Glove?*, European Journal of Risk Regulation, Vol.7:155, p.164 (2016).

⑮ See Tristan Harris, *How Technology is Hijacking Your Mind — From a Magician and Google Design Ethicist*, Medium (Apr. 7, 2019), at <https://medium.com/thrive-global/how-technology-hijacks-peoples-minds-from-a-magician-and-google-s-design-ethicist-56d62ef5edf3> (Last visited on Apr. 21, 2024).

上述数据信息各类细分损害毫无疑问都构成了无形的不利益。但损害虽然是自然概念,何种损害得以请求赔偿却是规范上的评价,^{①⑥}并非所有客观上的损害都能获得法律上的救济,只有在法律上被认为具有补救的可能性和必要性时,才产生民事责任^{①⑦}。因此,数据信息损害能够获得法律承认、进而获得民事救济,需要满足学理和制度层面的必要性与可行性。

(二) 承认数据信息损害的必要性

如上所述,各类数据信息损害都构成了无形但具有现实性的不利益,在数字时代,法律承认数据信息损害为“可赔偿的损害”具有学理和制度上的必要性。

首先,从个体层面看,承认数据信息损害为可获赔的损害是保护个人权益与使数据处理者谨慎行事之必需。个人信息与数据是数字社会生产之必需,在各国制度中,知情同意都是个人授权数据信息参与社会生产的主要方式。与其他物质类生产要素不同,数据作为生产要素在被收集之后仍能够持续地影响数据主体的利益,因此数据信息损害具有连续性,如果数据信息损害不被承认,则信息一旦被授权则个体很难再主张“合理控制”的权利。这种连续性使得承认数据信息损害成为必要——只有使涉及的潜在当事人个体在事后获得损害赔偿,方可对个人信息权益提供有效保护;^{①⑧}同时,也只有通过认可事后的损害赔偿,方可敦促数据处理者始终谨慎行事,避免过度处理数据信息,并更有动力投资合理的安全措施。

其次,从治理层面看,只有承认数据信息损害才能彰显法律态度、回应社会问题并实现风险控制。第一,承认数据信息损害可体现数据信息侵权行为的高度可责性。就制度目的而言,承认数据信息损害与其说是为了补偿个体受到的损失,不如说是彰显法律对侵害行为的惩罚性态度以及对正确行为的引导。第二,不法行为过高的独特性使得启动“繁琐而昂贵的国家机器”并不必要,^{①⑨}但现实生活中数据信息侵权损害的案例并非偶然发生,而是大量且日益增多的,其数量及社会影响之大迫切需要法院和立法予以回应。第三,损害赔偿、惩罚性赔偿、行政罚款、刑事罚金在责任威慑功能上具有同质性。在数字社会生产的风险防范立法中,应当根据风险行为的致害程度,依次协调运用民事损害赔偿制度、行政监管处罚、刑事责任,修正现有数据信息风险重监管处罚轻民事责任的现状。公法直接通过行为管制来重新分配并防控风险,私法则主要借助损害赔偿这种责任威慑手段来激励行为人主动采取防控措施。公法重在事前防控,私法则重在事后的责任威慑,二者在数字生产风险的规制领域殊途同归并实现价值统合,如此方能恰当配置责任,实现治理体系内部自洽。

再次,从社会总体成本角度来看,承认数据信息损害有助于降低社会总体交易成本

^{①⑥} 参见王泽鉴:《损害赔偿》,北京大学出版社2017年版,第68页。

^{①⑦} 参见王利明:《侵权责任法研究》(上卷),中国人民大学出版社2010年版,第306-307页。

^{①⑧} See Amy Kapczynski, *The Cost of Price: Why and How to Get beyond Intellectual Property Internalism*, UCLA Law Review, Vol.59:790, p.1009 (2012). 此文解释了通过个人知情同意远不足以保护个人隐私信息。

^{①⑨} See Oliver Wendell Holmes Jr., *The Common Law*, The Belknap Press of Harvard University Press, 2009, p.88.

并实现更好的社会效果。在数字时代,对数据信息的不当处理和过度披露是不可避免的社会预期成本,而具体到每个个体,数据信息损害的发生却非必然。但如果数据信息损害不被承认,就势必导致社会交易成本的提高——个体可预见到其知情同意的预期成本,因此会要求一个较高的价格以弥补事后可能发生的无法追偿的损害。^{②①}如果平台等生产者每次收集个人信息都要征求个人的同意并支付预期成本,那么其社会生产成本实际上总体要高于承认数据信息损害的成本。显然,就社会效果而言,承认数据信息损害优于将其排除在损害赔偿范围之外。

最后,在社会成本分配层面,只有承认数据信息损害才能实现公平分配社会成本、平等保护弱势个体。科斯在《社会成本问题》中提出“损害相互性”(reciprocal nature of harm)——社会主体之间总会在自行其是时相互影响,法律无论如何界定权利,都并非“一碗水端平”,只能要么允许甲方妨害乙方、要么允许乙方妨害甲方。^{②②}在数字时代,数字社会生产资源的初始配置显著失衡,私法层面被预设为平等的法律主体分化为数字生产者与个人。比起农业社会与工业社会,个人对生产资料的占有、参与生产的方式、与资源控制者力量的对比均处于极为弱势的地位,私法自治的平等性与互换性基础基本被消解。否认数据信息损害,实际上是将数字社会生产和信息经济中的现有权力分配模式假定为正当模式与利益分配的基线,默认个体应无条件加入数字社会生产中,并由其自己负担对个人数据信息失去合理控制的成本。因此有学者直言,信息隐私的主张实际上不过是对人们尚未接受的经济和技术进程的不公平性的笼统主张。^{②③}不承认个体层面的数据信息损害而仅依靠行政监管,势必造成对个人权利的进一步侵蚀。承认数据信息损害,则更倾向于将数字社会生产的成本在一定程度上分配给生产者,而非全部由作为生产要素提供者的数据个体负担。换句话说,应将个人在法律体系之外感知到的不公平与不合理,变成法律可以解决的问题。

(三) 承认数据信息损害的理论可行性

由前文分析可知,数据信息损害无以获得民事救济的根源在于民法学坚持非物质损害认定的实定化前提,而数据信息损害的各细分损害不符合此法释义学条件。但笔者认为这一制度障碍并非不可克服。由于《民法典》中并没有明文规定“损害”的内涵和外延,更没有对非物质损害作出限定,因此,民法教义学的立场是否能够作出合理调整为问题之关键。对此,可结合民法中的损害认定要件从以下几方面分析:一是就损害的“质”而言,承认数据信息损害的前提条件可通过法释义学一定范围的扩展得到满足;二是从损害的“量”上来看,虽然就个人而言,数据信息损害之量不足以启动民事救济,但其总和之量不可忽视,在价值保护需求上甚至足以导致专门的立法(如《个人信息保护

^{②①} See Ignacio N. Cofone, *The Dynamic Effect of Information Privacy Law*, Minnesota Journal Law Science & Technology, Vol.18:517, p.547 (2017).

^{②②} 参见戴昕:《数据界权的关系进路》,载《中外法学》2021年第6期,第1566页。

^{②③} See Julie E. Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism*, Oxford University Press, 2019, p.147.

法》)的出现,具有补救的必要性和可能性;三是从因果关系认定来说,数据信息损害可被损害概念所附带的因果关系范式接纳,进而将风险纳入损害之内。

第一,从“质”上来说,承认数据信息损害可通过法释义学在损害涵义上的适当扩展得到满足。在损害认定的传统要件中,首要前提条件即是民事权益受侵害。^{②③}但由于《民法典》并未就个人信息或数据确立具体的人格权益,使得数据信息损害的前提条件在静态传统学理层面似乎无法得到严格满足,进而导致其通过损害赔偿的可救济性存疑。不过,《民法典》第1165、1166条规定的前提分别为“侵害他人民事权益”和“造成他人民事权益损害”,此处的“权益”包含了法律上的利益,而个人信息之法益已在《民法典》中得到了明确承认,《民法典》第127条更是以特殊的准用性规范形式承认了其他法律规定中的数据法益,因此,即便个人信息和数据相关法益未被完全权利化,也仍能作为认定数据信息损害之前提。

事实上,民事权益受侵害这一前提条件在法释义学层面也容许一定范围的扩展。《德国民法典》迄今为止并未定义“损害”概念,德国主流观点基于自然损害(natürlichen Schadensbegriff)的概念,将“任何非自愿的、物质的或非物质性财产和利益的损失”都视为损害,从而与自愿牺牲资产的“费用”(Aufwendungen)区分开来;但自然损害仅仅是界定“损害”的基础,损害的具体范围则受到规范的修正。^{②④}例如,为防止侵权责任漫无边际、妨碍人们合理行为自由,实定法对非物质损害的范围加以限制,使其只有在符合法律规定要件时才能得到赔偿。^{②⑤}当然,规范的修正不一定完全只起限制作用,也可以根据法学理论对“损害”作扩展的理解。例如,德国民法就将“受害方为防止迫在眉睫的损害和消除或尽量减少已发生的损害而发生的费用”也纳入损害概念的覆盖范围,因为这些费用的支出并非出于自愿,从受害人角度看是合理且必要的。^{②⑥}这一界定方式承认了将防御风险费用纳入损害的必要性,实际上为数据信息损害的认定、衡量和救济间接奠定了基础。目前,民法学中承认的防御风险费用是受害人因确知损害的存在而现实支出的。依此,针对“如果受害人不知道相关侵害的存在,但一旦知悉将整体上倾向于支出一定成本以防止未来权益损害的发生”的情形,将现实支出条件扩展为合理支出条件就是必要的。由此,即便不承认个人信息本身可以作为“民事权益”,只要受害人支出此类防御风险费用的迫切需要确实存在,承认数据信息损害的“权益受到侵害”前提就是可行的。

第二,从“量”上来说,数据信息损害满足提供民事救济所要求的严重性程度。在损害的传统认定要件中,满足法律意义上的严重程度(也称为“显著性”)也是一项重要标准。其目的一是通过要求个体层面的显著性将损害赔偿诉讼资格限制在特定当事

②③ 参见程啸:《侵权责任法》(第3版),法律出版社2021年版,第227页。

②④ Vgl. Dirk Looschelders, Schuldrecht Allgemeiner Teil, 19. Aufl., 2021, § 45 Rn.1-2.

②⑤ 参见前注②③,程啸书,第230页。

②⑥ Vgl. Dirk Looschelders (Fn. 24), § 45 Rn.1.

人身上,如美国《宪法》第3条要求的起诉资格具有“特定的事实伤害”^{②7};二是损害的严重性使损害的民事救济具备制度效率,既可防止滥诉,也便于计算赔偿额度。

数据信息损害往往呈现出弥散化、微量形态,例如,虽然大规模数据泄露的危害已经足够证成对数据控制者高额罚款的正当性,^{②8}但是具体到个体层面,个人信息泄露的实际损害结果又被普遍认为“微不足道”,这使得就个体的数据信息损害启动民事救济似乎变得不经济。但这只是技术性障碍,并非不可克服。关键在于,在讨论是否承认数据信息损害时,应注意区分个体显著性与总量严重性。具体而言,应区分个体显著性带来的民事救济技术性问题以及与损害严重程度关联的民事救济必要性问题。与个体显著性相关的应由谁代表起诉、如何计算及如何分配赔偿金额是救济制度设计的技术性问题,不应当妨碍数据信息损害本身的认定,毕竟“撇开琐利不计规则,损失额对于具有法律相关性的损失是否存在这一问题并无意义”^{②9}。数据信息损害与国家安全、文化遗产等方面的损害不同,后几者是从属性和逻辑上就难以还原为当前时空中的个别损害,而前者在理论上却完全是当前时空中个人损害的直接加总。相较而言,由于数据社会生产中涉及的个人多以百万级量计,数据信息损害实际上更类似于环境生态损害,呈现出损害往往是集体的而难以个人化、个人具体和特殊的伤害难以证明的特点。实践中,环境生态损害已被法律认可,并通过民事集体诉讼、公益诉讼等制度得到一定程度解决。相应地,对个体层面的数据信息损害,同样可通过以保护公共利益为目的的个人信息保护公益诉讼等途径来实现保护。事实上,实践中已有此类案例,如最高人民检察院典型案例“浙江省宁波市‘骚扰电话’整治公益诉讼案”^{③0}就突破了从个体层面认定数据信息损害的局限。可见,在学理层面承认数据信息损害完全可以通过解决救济制度设计的技术问题来实现。

第三,数据信息损害可被损害概念所附带的因果关系范式接纳。传统的损害责任界定包含了对因果关系的考量,因果关系过于遥远的损害会被排除出可赔偿的损害范围之外。^{③1}启动民事救济必须确保因果关系处于一定门槛之上,即便损害仍未完全成为现实,也至少应具备成为现实的高度确定性。^{③2}就数据信息损害而言,关于因果关系认定的难题在于:一旦因果链条过长,损害可能会被无限扩大。然而就数据信息损害而言,尽管个人信息泄露会使受害人在未来发生后续损害的风险显著增加,但无论是个人信息泄露的

^{②7} Lujan v. Defenders of Wildlife, 504 U.S. 555 (1992).

^{②8} 参见孙莹:《大规模侵害个人信息高额罚款研究》,载《中国法学》2020年第5期,第109-116页。

^{②9} [德]克里斯蒂安·冯·巴尔、[英]埃里克·克莱夫主编:《欧洲私法的原则、定义与示范规则:欧洲示范民法典草案》(第5、6、7卷),王文胜等译,法律出版社2014年版,第227页。

^{③0} 2018年上半年,宁波市发生120热线被骚扰事件。截至5月下旬,120急救电话累计接到楼盘推销电话1600余个,其中最多一天接到90多个,均为“0574-2”开头的联通电话号码,严重影响宁波市急救中心的正常工作秩序。参见《最高检发布检察公益诉讼十大典型案例》,载中华人民共和国最高人民检察院网站, https://www.spp.gov.cn/spp/zxjy/qwfb/201812/t20181225_403489.shtml, 2024年4月18日访问。

^{③1} 参见前注^{②3},程啸书,第227页。

^{③2} See Clapper v. Amnesty International. USA, 568 U.S. 398 (2013).

后续侵害风险,抑或是歧视、身份盗窃或欺诈等后续损害,都难以依据“差额说”获得认可。^③多因素介入问题使得损害的具体范围难以被认定,如何把握“确定赔偿范围的因果关系”给法律实践提出了更高的要求。

不过,现代法学早已开始接受“风险损失”,无论是德国民法中的风险预防费用还是刑法释义学中将“升高风险”作为犯罪构成的判断要件,都表明风险损失已经得到了法理层面的独立认可。在风险社会中,由于因果关系的复杂化,最终损失的因果链条难以被清晰判断,因此在因果链条上的关键节点认定风险损失就成为一个有用的替代方案。数据信息损害正好位于一系列后续损害的关键直接节点,其独立性认定的需求尤为突出。

总而言之,数据信息损害应当被法律所承认,具有进一步获得民事救济的制度必要性与学理可行性。由于数据信息损害在客观上广泛存在,法律对之承认与否不能完全由侵权责任体系内部的技术、理论考虑所驱动,而应反映法律体系之外的世界对这些损害行为的态度。从上述分析来看,数据信息损害尽管已具备认定之基础却仍然难以获得民法教义学充分接纳的深层原因在于,传统的损害认定属于工业社会时代建构的侵权赔偿法律制度,但其已经不适应信息社会的社会关系架构。对这一深层原因作抽丝剥茧的解剖,有助于革新损害概念的法理认知,从而为数据信息损害建立完整的界定规则。总体而言,欲实现我国数据信息损害的承认和救济,首先须从法理层面对损害认定理念进行重构;其次要在制度层面从成本和政策角度建构对数据信息损害予以救济的可行规范。

三、承认数据信息损害的法理依据

传统损害的概念与认定规则是以工业革命时代社会生产方式为基础而形成的。通说所认为的身体机能受损、精神痛苦、经济收益减损等不利后果所对应的损害行为大多是工业时代的外部损害活动,如大规模工业生产、车祸撞击、高空抛物等。但是在数字时代,数据信息损害大多具有无形性、未来风险不确定性、间接性等特征,故而有必要在法理层面重新全面认识损害及其认定规则,以彻底解决承认数据信息损害所面临的前述障碍和问题。事实上,回溯损害概念的发展可以发现,传统损害概念本身就是随着社会发展而被不断建构的。从工业时代到数字时代的社会生产方式变革,为承认数据信息损害提供了充分的现实和法理依据。

(一) 关于数据信息损害不确定性的理论回应

关于数据信息损害不确定性的质疑可以归结为三点:一是数据信息损害具有计算的不确定性,难以从损害范围计算实际的经济损失,因而无法满足法律层面损害认定的确定性要求;二是数据信息损害往往具有非及时性,部分经济损失结果可能是在数据泄露等损害事实发生后的一段时间内才发生,数据信息损害的认定存在将未来损失纳入法律范畴的弊端;三是数据信息承载了复杂的利益关系,在数据权属尚未明确的当下,过早

^③ See Daniel J. Solove & Danielle Keats Citron, *supra* note 8, 771.

地区分事实层面与法律层面的数据信息损害实属操之过急。^{③④}概言之,数据信息损害因为数额的不确定、发生时间的不确定和对应权益的不确定,无法被纳入法律承认的损害范畴。但笔者认为,计算的不确定性不应成为承认数据信息损害的障碍,而发生时间和承载权益的不确定性乃基于数字社会生产方式而产生,可通过理论完善予以回应。

第一,损害概念的扩张史显示,损害早已内嵌了不确定性,数据信息损害的不确定性完全可通过规则调整予以容纳。回顾损害概念逐步扩张的历程可以发现,损害确定性本身是被建构的。首先,随着工业大规模生产造成人身损害的发生频率和严重程度增加,原本局限于财产意义的“损害”扩张至无形的人身损害,相应地,法律上的损害概念被迫放弃了对“有形”的要求,但仍通过人身损害追偿理论坚守“具体与确定”的特点(例如,认为身体受到的伤害与精神痛苦本质上是可以预期的,追偿的范围包括工资损失、财产损失、可折抵为抚养费与未来工资损失的劳动能力丧失等)。^{③⑤}这掩盖了人身损害的追偿并非具体、确定与精确的事实,使人们忽略了损害追偿制度的本质是将不可知的未来转化为可衡量的现在的复杂过程。^{③⑥}其次,知识产权等无形财产的发展使得损害概念进一步扩张,促使法律对抽象损害追偿理论作出调整,例如部分类型的著作权利益主张的损害是抽象的,但是法律却赋予其具体明确的特定价值。由此可见,对损害确定性的界定是随着社会发展而逐渐放宽的,不确定性不应成为承认数据信息损害的理论障碍。

第二,承认数据信息损害的不确定性,并非将所有未来发生的损害结果皆视为数据信息损害,而旨在使损害认定以保护权益主体为导向,确定数据信息损害的可问责性。损害概念的扩张史同样容纳了发生时间不确定的损害。如法律早已承认并救济的医疗损害、不动产妨害、贬值损失赔偿等均为未来合理的、不确定的损害。^{③⑦}但法院之所以并未仅从侵权事实中推定不可挽回的损害,而是选择性地承认未来合理的、不确定的损害,是因这些损害认定对社会有重大影响,存在权衡侵权行为未来风险的必要性。同样,数据信息损害的承认与否也应取决于“该类损害是否存在对应的社会资源生产活动的减损效果”。只有社会数据资源创造活动受到负面影响时,发生于未来且不确定的数据信息损害才有可能被纳入到“损害”的法律概念范畴中。一方面,观之数据泄露、数据毁损等数据信息损害事件,均存在加剧社会公众对数据处理活动安全性不信任、进而削减个人和企业推动数据流动意愿的后果,具备法律救济的必要性。另一方面,实践中早已存在确定并量化数据信息承载财产利益的尝试,如隐私经济的理论和实证研究开始关注个人数据交易市场的建立、数据去标识化的经济影响,以及定向广告和差异化定价的研

^{③④} 参见前注①,江苏省南京市中级人民法院(2014)宁民终5028号民事判决书;前注②,北京互联网法院(2018)京0491民初1905号民事判决书;前注⑦,天津市第二中级人民法院(2020)津02民终4520号民事判决书。

^{③⑤} See Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, Southern California Law Review, Vol.80:241, p.295-296 (2007).

^{③⑥} See Ryan Calo, *Privacy Harm Exceptionalism*, Colo. Tech. L.J., Vol.12:361, p.364 (2014).

^{③⑦} 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35页。

究等。^{③⑧}由此可见,发生时间的不确定也非理论上难以逾越的难题,可通过制度设计解决。

第三,数据信息承载权益的不确定性是基于社会生产方式变革而产生的变化,不应成为承认数据信息损害的障碍,而数据信息损害是切实存在的,因而必须从理论层面及时予以回应。在工业时代,传统损害中对非物质损害确定性要求针对的是分散的、物质化的生产方式,换言之,需要通过确定性要素避免法律干预遥远的、复杂的技术活动。而在数字时代,社会生产围绕着数据信息的生产、流转与利用,生产方式本身是非物质化的,生产要素更是承载着多重权益的数据信息——在个体层面,个人信息上既承载着人格利益又天然具有财产属性,不仅具备可识别、标表特定自然人特征,也满足商业需要且有可控性和稀缺性;^{③⑨}在企业层面,平台等市场主体投入资源进行数据资源的开发利用,企业多将数据资源的控制看作企业的竞争性权益与核心竞争力,实践中通过反不正当竞争法保障其一定限度的排他性权益。在这种生产方式和要素变化发展的背景下,数据信息损害切实存在已经成为共识,亟需从损害理论上予以调整和回应。

综上所述,不确定性本身天然内嵌于损害概念内。只有认识到损害存在不确定性,才能真正解决从工业时代到数字时代的变迁带来的损害从实定化到风险化转变的问题。目前反对将风险纳入损害赔偿范围的观点认为,这会过度扩张侵权责任保护范畴、虚置侵权责任制度的损害填补功能。^{④⑩}对此需特别强调:承认损害如“道”,衡量损害为“术”,损害的确定性本身是被建构的属性,且该确定性已经随着生产方式变革被逐渐消解;“损害认定”与“损害金额计算”是两个问题,不宜以数据信息损害赔偿金额的不确定性来否定数据信息损害在损害范围、损害形式层面可通过制度设计实现的确定性。从当前数字经济发展现实出发,理论与制度应及时回应数据信息损害的不确定性,以实现有效救济。

(二) 数据信息损害因果关系的推定化

因果关系的功能在于确定损害赔偿范围,本质是基于生产方式与政策目标的建构选择,因此也非一成不变的。数据信息的强流动性与非排他性使得数据信息损害因果关系具有概率性与复杂性。因此,对数据信息不应仅延续物理世界中对静态财产的直觉认知和想象,而应引入推定性因果关系判断标准,以适应数字时代的变化。

第一,数据信息损害因果关系的概率性和复杂性主要来源于数据信息的强流动性与非排他性,应延长因果关系链条对之予以延纳。数据是不断大量生成且流动性极强的动态对象,其损害从行为到发生呈现了风险的不确定性。由于数据信息的非排他性(可复制性),侵害可反复持续发生、影响范围广。例如,数据泄露是个人或者数据控制者丧失了对数据信息的控制,可能引发个人的数字身份盗用,继而导致信用卡盗刷、遭受骚扰等物质与非物质损害。在一些情况下,若数据还在暗网、深网等常人难以追寻踪迹的网络环境中流转,就会使得因果关系的衡量呈现更强的概率性。不过,因果关系的概率性完

^{③⑧} See Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs, 2019, p.66.

^{③⑨} 参见彭诚信:《论个人信息的双重法律属性》,载《清华法学》2021年第6期,第82页。

^{④⑩} 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51页。

全可以通过延长因果关系链条来解决。例如,产品责任兴起时期,为应对工业生产过程和分销链所引起的因果关系概率性,法律通过延长因果关系链条,开始将处理产品伤害的主要法律依据转向侵权法,使得产品制造商对损失责任增加。由此可见,当无法通过可追溯的物理痕迹获得因果关系的准确推定时,因果关系如何构建更多取决于政策选择与价值衡量。同样,当概率性成为数字时代数据信息损害因果关系的常态时,我们也应及时引入推定技术修补因果链条的视野断裂。

第二,数据信息损害因果关系的概率性和复杂性可通过法律直接建立因果关系模型予以解决。在数据与个人信息流转迅速、可能被多个主体进行数据处理的情景下,很难确定个体的损害是由哪一个环节造成的。如敏感个人信息(如种族)被雇主用来进行雇员画像,很难证明就是这个因素导致了个人收入与晋升机会的损失——也很可能存在其他因素的介入。正因如此,在“庞某某诉趣拿及东航案”中,一审法院要求数据泄露受害人证明两被告是掌握其隐私信息的“唯一个体”,否则无法确认原告之隐私信息是两被告泄露的。^①但既往侵权理论会通过因果关系模型回应复杂性问题,在某些特殊侵权领域,法律会通过因果关系推定来解决因果关系复杂性造成的难以证明的问题。如在德国,艾滋病血液污染制品事件直接推动了《药品法》修改,通过废止受害人说明药品的研发缺陷和制造缺陷的要求,建立了使用药品和造成法益损害之间推定的因果关系模型。^②因此,针对复杂的数据信息损害因果关系,法律同样可考虑通过直接建立因果关系模型予以解决。理论上,准确还原现实生活中原因与结果之间的复杂逻辑关系不具有可操作性,因此“相当性”被用于解释加害行为导致损害结果的盖然性,并成为通说。^③在损害认定层面,相当因果关系说的理论功能在于对事实损害结果进行范围限定,以违法行为为认定基础,辅之以政策考量和价值权衡,以筛除不具有相当因果关系的损害事实。处理数据信息损害因果关系的概率性与复杂性时,需要参考常态下的风险水平以及风险发生盖然性的增加幅度来加以判断。此处可借鉴广泛应用于医疗损害、毒物侵权诉讼、药物损害的机会丧失理论,即“当获得有利结果或者避免不利后果的机会受损时,受损人应当得到赔偿,且赔偿金额应当被适当评估,而不是陷入全赔或不赔的境地。机会丧失本身就是一种可赔偿的利益”^④。例如,医疗侵权中生存机会的损害赔偿的对象是(因机会丧失而)增加的机体痛苦(physical pain)或其他身体损害(physical losses)、情感损害(emotional losses)和间接损害(consequential damages)。^⑤同理,在数据泄露与现实损害结果之间的因果关系难以认定而“个人信息安全”的概率却显著降低时,这种

① 参见北京市第一中级人民法院(2017)京01民终509号民事判决书。

② 参见[德]马克西米利安·福克斯:《侵权行为法》(原书第5版),齐晓琨译,法律出版社2006年版,第313-315页。

③ 关于因果关系理论早年曾存在“一般化理论”和“个别化理论”,但因难以适用而讨论逐渐减少。参见[美]哈特、[美]托尼·奥诺尔:《法律中的因果关系》(原书第2版),张绍谦、孙战国译,中国政法大学出版社2006年版,第393页。

④ 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.1354 (1981).

⑤ 参见季若望:《侵权法上生存机会丧失的损害赔偿论——以美国法为借鉴》,载《华东政法大学学报》2018年第3期,第173页。

不利结果增加的可能性本身就是一种可赔偿的利益,即机会损害。数据泄露造成的机会损害具体体现为因数据泄露增加的现实损害风险、焦虑和痛苦等精神损害,以及为避免损害支付的预防费用。机会丧失案件中的最终损害结果发生与否不应当成为影响损害赔偿的因素。^{④6}易言之,可以将侵害数据信息权益所造成的“制造风险”或“升高风险”之后果推定为损害,而不必等待因果关系链条上后续共同致害原因的实际介入。

正如英国法官丹宁爵士所言,以损害是否具有因果关系来决定被告的责任实在是基于政策的考量,旨在适当限制被告的责任。^{④7}因果关系的概率性与复杂性不应成为承认数据信息损害的障碍,只需进行恰当的制度设计来限制数据信息损害的范围、达到各方利益的平衡即可。

(三) 数据信息损害显著性的评价调整

在数字社会生产方式下,数据信息损害多呈现总量严重、个体显著性不足的形态,这使其超越了个体性而兼具私益与公益性质。因此,有必要基于社会生产方式的变化,对数据信息损害要素是否须具备个体显著性进行评价调整,即承认数据信息损害取决于损害总体严重程度,个体显著性仅决定了救济的诉讼方式。

第一,针对数据信息损害具有弥散化与微小化但总量惊人的特点,可通过降低对个体显著性的要求来实现救济。传统损害的个体显著性要求是基于工业时代早期生产方式建构而来的。在工业时代,个人对物质实体的占有呈分散状态,因此侵权的模式以“一对一”的过错侵权为典型。^{④8}传统的损害赔偿是个性化的、离散性的,因此要求个体启动诉讼逐个解决纠纷。事实上,损害的个体显著要求已随着工业大规模生产和高危作业的普及而进行了适应性调整。例如,在19世纪,死亡及肢体残缺才是法律承认的个体损害,但到了20世纪中期,环境污染、产品责任等归因复杂的大规模侵权初现,工业废物造成的环境污染和致癌、致畸化学品造成的慢性疾病就被纳入侵权法所承认的损害范畴中。^{④9}到数字时代,数据的经济价值往往表现为数据要素积聚所形成的规模化效益,尤其是在大数据等信息技术的支持下,数据的数量、类型越多,所能挖掘的信息内容就越有价值。平台等数据控制者只有集合大量个人数据才能提取符合格式的海量数据产品,以驱动企业行为并实现数据产品的转化。所以,数字时代的损害必然呈现规模化的特征——数据泄露的用户数据为百万计量级、处于同一业务链的数据处理者遭遇集体性的信息服务中断等故障。如果不承认数据信息损害,则加害人可以把所有损害均匀地“碾碎”,以使得单个微小的请求权无法成立,进而规避责任。^{⑤0}

第二,数据信息损害是否具备个体显著性仅能决定救济启动方式,而不应影响法律

^{④6} 参见前注^{④5},季若望文,第178页。

^{④7} See *Spartan Steel & Alloys Ltd. v. Martin & Co. (Contractors) Ltd.*, [1973] QB 27.

^{④8} 参见张平华:《揭开集合侵权的面纱——从术语翻译到制度建构的追问》,载《法律科学》2013年第6期,第109页。

^{④9} See Julie E. Cohen, *supra* note 22, 182.

^{⑤0} 参见[德]格哈德·瓦格纳:《损害赔偿法的未来——商业化、惩罚性赔偿、集体性损害》,王程芳译,中国法制出版社2012年版,第182页。

对整体损害的承认。数据信息损害呈现规模化特征,受害人众多却个体显著性不足。这决定了个体损害救济的式微,以及大规模损害救济的集体诉讼、代表诉讼等方式逐渐兴起。数据信息损害的性质既含个人对数据合理控制的私益,也兼具数字社会生产安全的公共利益。在此类不具备个体显著性的损害越来越常见的背景下,法院不仅要约束个人行为和市场规范的偏离活动,更要对系统性的社会运行和市场行为作出回应。随着集合性损害出现,侵权损害论的概念、原则、规则不断分化,成就了更为专业化的应对体系;^①司法上也产生了集体诉讼、公益诉讼等制度,作为对大规模工业生产的调适回应。典型如生态环境损害,由于该类损害突破了公私法之间的藩篱,最高人民法院确认了生态环境损害赔偿优先、环境民事公益诉讼为补充的审理顺序。此外,如果仅因个体显著性不足就认定损害不成立,还会导致加害人明显丧失按照标准谨慎行动的动力。按照目前的赔偿计算方法,数据信息损害的规模化特征使得赔偿额度总数对于企业而言难以承受,对个人而言却又杯水车薪。如2017年美国的Equifax数据泄露事件中,1.47亿个纳税人的财务信息落入不明身份者手中,在与联邦贸易委员会和消费者金融保护局的和解中,该公司同意支付4.25亿美元,但相当于每个受害者只可获得不到3美元的赔偿。^②可见,从损害发生范围和整体损失额度等方面设定新的显著性标准,方为损害认定要件更新之要点。

概言之,工业时代形成的传统损害概念无法容纳数字社会化生产中数据信息损害的不确定性和因果关系的概率性和复杂性。若以此拒不承认数据信息损害,无论对于当事人的法律救济还是社会的公平而言都极为不利,也必将使得一直以个体救济为主要运行逻辑的司法审判活动在数字时代成为逐渐被边缘化的纠纷解决机制。损害的理念更新与规则调整迫在眉睫。

四、数据信息损害的救济规则调整

欲使数据信息损害获得民事救济,需针对其特点进行民事救济规则的调整,通过制度解决数据信息损害与传统损害救济规则不兼容的问题。具体而言,针对传统损害救济规则对确定性的要求,可通过数据信息损害认定的法定化与类型化来解决;而对传统救济损害的个体显著性要求,则可通过诉讼制度与赔偿方式的调整来回应。

(一) 数据信息损害认定的法定化

数据信息损害的法定化是规范数据处理活动的应然选择,也是促使侵权法体系与数据处理实践相匹配的关键环节。法定化的核心目的是实现《数据安全法》《个人信息保护法》等法律法规所追求的“兼顾安全与发展”之立法目标。一方面,通过从直接损害

^① 参见窦海阳:《环境损害事件的应对:侵权损害论的局限与环境损害论的建构》,载《法制与社会发展》2019年第2期,第153页。

^② See Federal Trade Commission, *Equifax Data Breach Settlement*, at <https://www.ftc.gov/enforcement/refunds/equifax-data-breach-settlement> (Last visited on Apr. 17, 2024).

与后续损害两个层次分别实现数据信息损害法定化,可以明确侵权法认可的数据信息损害,避免数据处理者对未来不确定风险承担“无限责任”;另一方面,通过法定化特定数据信息损害类型实现直接依法认定大规模侵权、牵连式侵权事件中的因果关系,解决数字时代个人权利救济所存在的“成本过高”“举证困难”等问题。如上所述,数据信息损害分为直接损害与后续损害两类。从比较法看,有的国家承认直接的数据信息损害;有的国家将直接损害限于隐私侵权,将特定类型的后续损害作为加重法律责任的要素。各欧盟国家基于 GDPR 第 82 条的判决也不一致:奥地利和荷兰的法院在一些案件中支持了私人因遭遇数据泄露而基于个人数据权益受损所主张的赔偿;^⑤而爱尔兰和英国等国就 GDPR 第 82 条是否应该被作为支持私人索赔的依据仍存在争议^⑥。下文基于我国已有立法与判例对数据信息直接损害和后续损害分别进行讨论。

1. 数据信息直接损害认定的法定化

目前在司法实践中,以侵害个人信息为主要目的的案件数量占个人信息侵权案件的大多数,且主要是以隐私权纠纷出现。^⑤然而,个人对数据与信息的安全保有与合理控制在很多情况下并不能被隐私权保护容纳,尤其是,隐私权的民法保护不能完全涵盖敏感个人信息,导致直接数据信息损害存在法律保护空白。例如,当侵害数据信息产生直接损害而未牵连隐私权等具体人格权益时,受害人一般不能主张精神损害赔偿。因此,应将数据信息直接损害认定法定化,承认特定种类的数据信息直接损害,并辅以明确损害的特定范围。具体而言,即规定个人信息与数据的非法收集处理、数据泄露与个人信息记录错误等特定损害类别,附以对信息类型与侵权行为规模的限定。如此既可呼应实践中最为常见的直接数据信息受侵害情况,也可防止数据信息损害无限化。

我国法律实际承认数据与信息的保有与安全本身就是重要的法益,就数据信息直接损害也有相关的规定,如《刑法》第 253 条就规定了侵害公民个人信息罪,而适用该条的司法案例多为惩治黑客入侵数据库系统、工作人员超越权限获取信息等。举重以明轻,应将刑法对相关法益的保护扩张至民法,承认数据信息直接损害,并通过法定化的方式限制类型和范围。进行扩张的理由在于:一方面,非法收集个人信息与数据意味着实质性地提升了数据滥用的风险,因此相比数据泄露,应降低损害认定的难度;另一方面,现有案件统计显示,“个人信息记录错误”“未经同意使用个人信息”以及“个人信息泄露”三类行为涉案数量最多,^⑥扩张具有实际意义。事实上,我国法律早已承认信息的获取与真实表达是一种权益。例如,在知识产权法领域中,不实陈述被认定为是一种侵权行为,

^⑤ Austria: First Award of Immaterial Damages under GDPR, Computer Law Review International, Vol.5, p.147 (2019); nr. 7560515 CV EXPL19-4611, Gericht Amsterdam, 2. September 2019.

^⑥ See Eoin O'Dell, *Compensation for Breach of the General Data Protection Regulation*, Social Science Electronic Publishing, 2017, p.23-29.

^⑤ 参见前注^⑤,程啸文,第44页。

^⑥ 参见王伟、朱宜烨、高阳、王明志:《从个人信息涉诉案件情况看企业数据合规注意要点——大数据合规系列之二》,载植德律师事务所网站, <http://www.meritsandtree.com/index/news/detail?id=167&eqid=f3dd1bf900029b110000000664255e3f>, 2024年4月4日访问。

受损害方可向违反真实义务一方请求赔偿因其实施不实陈述行为而支出的律师费、交通费、住宿费。^{⑤7} 这充分说明,即使后续损害尚未发生,数据与信息的保有与安全,乃至真实表达本身受到的侵害已被法律正视。

国内外司法实践中均有承认直接数据信息损害的判例。如具有里程碑意义的“Gulati 诉镜报案”,该案是对电话黑客攻击引起的私人信息滥用的索赔。法院将其归类为滥用私人信息的侵权行为案件,并认定失去对隐私的控制本身是一种损害,滥用私人信息本身是可以赔偿的(即不需要证明滥用造成了损害)。^{⑤8} 我国也有类似的判决,如在“凌某某诉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”中,北京互联网法院认定被告未经授权收集和使用原告个人信息的行为违法,在判决停止侵害、赔礼道歉的同时,判决抖音赔偿原告凌某某经济损失 1000 元和维权合理费用 4231 元。不过,在英国“劳埃德案”中,法官认为,即使可以为失去控制权提供损害赔偿,仍有必要确定对每个数据主体数据的非法处理程度。^{⑤9} 因此,在将直接数据信息损害进行扩张的同时,应以法定化方式限定损害赔偿范围。笔者认为,为防止直接数据信息损害范围无限化,应区分敏感信息与非敏感信息,敏感个人信息被获取或泄露本身即构成损害。^{⑥0}

2. 后续数据信息损害的类型法定化

如前文所述,非物质损害范畴的界定决定了民事救济是否能成为保护个人数据与信息的有效手段:损害范围越宽泛,民事私权救济就越有效。这与其说是法学问题,不如说是一个政策问题。^{⑥1} 目前实践中关于后续数据信息损害的认定存在较大争议,在现有案例中,只有当个人信息失控导致银行卡盗刷、虚拟财产丢失等物质损害时,个人才能获得损害赔偿。因此笔者认为,对后续数据信息损害等非物质损害的界定同样应法定化,并通过限定特定类型防止损害无限化,以在有效救济与责任限制中取得平衡。具体而言,对后续数据信息损害的认定应基于数据信息在数字时代对个人名誉、信用、机会、职业、福利、资格的重要影响,减轻个人请求民事救济的举证负担。可将此种后续损害界定为对原告的安宁生活、信息自主权或名誉的侵犯,或者是对法律认可的准财产权的侵犯(类似于对知识产权的侵犯)。

某些常见的数据信息后续损害已经得到国外立法承认。如美国联邦贸易委员会(FTC)将消费者信息性损害列举为欺骗性伤害或颠覆消费者选择、财务伤害、健康或安全伤害、无端入侵的伤害和声誉伤害。欧盟 GDPR 在序言第 75、83、85 条规定,个人数据权益的损害是指任何非法处理个人数据造成的身体、物质或非物质损害,包括歧视、身

^{⑤7} 参见商建刚:《不实陈述的民事赔偿责任规制》,载《中国知识产权(网络版)》2021 年 11 月(总第 177 期),载中国知识产权网, <https://www.chinaipmagazine.com/journal-show.asp?id=3806>, 2024 年 4 月 7 日访问。

^{⑤8} See Gulati v. Mirror Group Newspapers, [2015] EWCA Civ. 1291.

^{⑤9} See Lloyd v. Google LLC., [2021] UKSC 50.

^{⑥0} 参见前注^{⑤7},谢鸿飞文,第 21-37 页;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 25-39 页。

^{⑥1} See Jonas Knetsch, *The Compensation of Non-Pecuniary Loss in GDPR Infringement Cases*, Journal of European Tort Law, Vol.13:132, p.145 (2022).

份盗用或欺诈、经济损失、名誉受损、未经授权的去匿名化以及其他显著经济或社会损失等。《印度个人数据保护法》(2019年)第3条第20项也以列举的方式规定了数据信息损害的类型,具体包括:身体或精神损害;身份的丧失、扭曲或失窃;财务或财产损失;丧失声誉或受到羞辱;失业;遭受歧视性待遇;遭受勒索或敲诈;对数据主体进行评估决策而拒绝或撤回服务福利或相关利益;因出于对被观察或监视的恐惧而构成对言论行动或其他行为的直接或间接限制;数据主体无法合理预期的观察或监视等。一向保守的德国法也开始承认若干新型数据信息损害,如歧视、身份窃用或诈骗、金融损失、信誉受损、数据泄密、擅自实施的去匿名化以及显著的经济或社会不利后果等。^{⑥2}

我国《民法典》第1165条并未细致界定损害的要件,为适度扩容非物质损害留下了解释空间。结合数据信息在数字社会生产中的流动传播与处理的生产环节,后续数据信息损害应法定化为以下两种类型,并参照知识产权法探索的衡量方法进行法定赔偿额度确定。其一,身份盗用、冒用。如利用他人的身份信息将他人登记为公司的股东、法定代表人或者董事、监事等,银行及工作人员利用数据主体的身份信息开立账户等。如在“沈晴与上海容蓁汽车用品有限公司姓名权纠纷案”中,被告容蓁公司未经原告沈晴许可,在办理税务设立登记时擅自使用了其身份信息,导致沈晴的身份信息被税务机关登记于容蓁公司的财务负责人事项中。^{⑥3}其二,个人状态与行为信息的篡改造成重大权益的机会丧失与福利减损。最典型的就是征信系统错误记载他人的信用信息。如个人和银行并无借款合同,但征信中心却有该个人存在不良贷款信用记录。^{⑥4}这两类数据信息损害要么对个体进行了错误识别,要么对个体状态与行为进行了错误表达,均可能导致重大权益的机会丧失与福利减损。司法实践中对此类非物质性损害的困扰是,其无法像财产损害一样可明确衡量赔偿数额。笔者认为,对于机会丧失与福利减损的损害衡量可参考知识产权侵权案件探索出的衡量方法进行推导。例如参考著作权案件中无法证明实际损害的原告可主张法定损害赔偿的做法,允许数据信息损害案件的原告主张法定赔偿。以作品未经同意被收录为例,法院会根据著作权人失去的许可机会可能获得的收益来衡量原告的法定赔偿额。^{⑥5}相应地,当个体因个人信息中的错误丧失了贷款机会、获取居住证的机会或者就业机会等时,也可根据其可能获得的收益来衡量赔偿。

(二) 数据信息损害的诉讼方式与计算规则

若法院在数字时代仍沿用工业时代的个体诉讼来应对大规模侵权问题,就难以处理数字社会结构性或系统性的不公正问题。要解决工业时代发展起来的个体主义的救济模式与数字化社会生产中大规模信息聚合、处理的矛盾,就需要通过诉讼制度调整来探索解决个体显著性不足问题,并明确微小的系统性数据信息损害的赔偿方式。

⑥2 参见叶名怡:《个人信息的侵权法保护》,载《法学研究》2018年第4期,第91页。

⑥3 参见上海市闵行区人民法院(2019)沪0112民初26438号民事判决书。

⑥4 参见山西省大同县人民法院(2016)晋0227民初63号民事判决书。

⑥5 参见北京知识产权法院(2021)京73民终838号民事判决书。

1. 数据信息损害的诉讼方式调整

大规模个人信息侵权中的损害赔偿与集合财务侵权（mass financial tort）情形相类似。在集合财务侵权案件中，消费者仅遭受了轻微损害，法院通常拒绝受理受害人单独诉讼，但可由受害人群体提起诉讼。^{⑥6}然而，传统的集合财务侵权并不支持未发物质性损害而单纯遭受精神损害的受害人。此外，本土诉讼制度也影响着大规模个人信息侵权中的救济：在大陆法系中，受侵害者必须事先加入一个集体才能获得赔偿；而在普通法系中，受侵害者可以在法院决定对该集体进行赔偿后证明自己是集体成员。例如，在“劳埃德案”中，原告败诉的重要原因之一是法院认为代表人诉讼并不适用于数据信息的损害赔偿案件，因为代表人诉讼要求对每个个体的损害进行评估，而法院认为在该案中“每个人所遭受的损害程度并不相同”。但也有观点认为，每个索赔人在法律上有一个单独的诉讼理由，只要集体成员之间没有真正的利益冲突，就不应成为代表诉讼的障碍。这一观点已被澳大利亚、加拿大和新西兰的最高法院采用。^{⑥7}

在我国现有法律体系中，集体但微小的数据信息损害可适用《反垄断法》第60条第2款、《个人信息保护法》第70条以及《消费者权益保护法》第47条规定的公益诉讼。例如，网约车、酒店预订、网上购物等商务平台利用算法实施“大数据杀熟”的算法价格歧视行为，会损害消费者的隐私权、公平交易权、知情权等权益，可通过消费民事公益诉讼救济；平台未依法履行网络保护义务，并运用后台算法向具有浏览儿童内容视频喜好的用户直接推送含有儿童个人信息的短视频，从而致使侵犯儿童个人信息权益的，检察机关可以依法综合提起未成年人保护民事公益诉讼和行政公益诉讼。只是，现实案例中多以行政公益诉讼为主，且鲜少真正进入诉讼环节，^{⑥8}而数据信息损害的民事救济需要的是民事公益诉讼。值得注意的是，《民事诉讼法》第58条将“人民检察院”列为提起公益诉讼的第二顺位主体，排在“法律规定的机关和有关组织”之后；而《个人信息保护法》第70条将人民检察院列于其他公益诉讼主体之前，与法律规定的消费者组织和由国家网信部门确定的组织并列，在一定程度上强调了人民检察院在履行保护公民个人信息上的重要职责地位。因此，可预见未来一段时间内，数据信息损害的公益诉讼将由人民检察院主要负责提起，且多为“民事公益诉讼+行政公益诉讼诉前程序”的方式；对于明显涉及消费者公平交易权、知情权等权益的，则可以消费者协会提起民事公益诉讼为补充。不过，最高人民检察院的相关负责人在答记者问中也坦言，在个人信息保护检察公益诉讼上面临“立法供给不足、调查核实手段欠缺、公益损害认定难、修复难”

^{⑥6} See Deborah R. Hensler & Mark A. Peterson, *Understanding Mass Personal Injury Litigation: A Socio - Legal Analysis*, Brooklyn Law Review, Vol.59:961, p.965-1050 (1993).

^{⑥7} 参见范晓亮：《论我国消费损害赔偿特别代表人诉讼机制的构建》，载《法学》2022年第12期，第118页。

^{⑥8} 实践中人民检察院向行政机关提出检察建议后，行政机关基本都会在法律规定的时限内依法履行相关职责予以整改，鲜少真正进入诉讼环节。在最高人民检察院发布的11例“检察机关个人信息保护公益诉讼典型案例”中“行政公益诉讼”占6例，且均仅进展至“调查和督促履职”阶段，并无向法院提起诉讼的环节。参见《检察机关个人信息保护公益诉讼典型案例》，载中华人民共和国最高人民检察院网站，https://www.spp.gov.cn/spp/xwfbh/dxal/202104/t20210422_517106.shtml，2024年2月13日访问。

等问题,^⑨可见,检察公益诉讼相关制度和实践操作方法的构建仍任重道远。

2. 数据信息损害的赔偿制度调整

《民法典》未专门针对个人信息侵权案件规定法定赔偿额或惩罚性赔偿制度,而《个人信息保护法》将《民法典》第1182条侵害人身权益造成财产损害赔偿额的衡量方法照搬到个人信息权益侵权领域。这造成个人信息侵权损害赔偿额的衡量不具有可操作性,也未能充分体现数据和信息所承载的人格利益与财产利益。而且,由于对个人的损害主要是非物质损害,遵循赔偿填平原则的补偿性赔偿无论是对个体救济还是对侵权者的震慑而言均显不足。特别是在大规模数据和个人信息侵权案件中,单个主体受到的损害往往与违法者所获利益并无数量上的直接关系,因此对大规模侵权造成之微小的系统性损害不宜以差额说为基础进行补偿性赔偿,而宜通过司法实践逐步确立法定赔偿额或惩罚性赔偿制度,并积极拓展新的损害赔偿承担责任承担方式。

部分国外学者提出,数据泄露事件发生后个人对于隐私泄露、私密信息等未发生事件的担忧同样有可能构成侵权法意义上的损害,可分别将行为人的社会责任以及后续损害的发生情况划分为1—5级,并将相应级别综合相加,为之后损害赔偿的具体数额衡量提供相应标准。^⑩也有学者提出可以个人信息内容的重要性、实际损害程度等因素作为衡量损害赔偿金额的具体标准。^⑪韩国司法实践有类似的损害赔偿认定与衡量标准(如图1):如果1和2均不存在,则不构成损害;如果1和2存在且需要满足“存在信息已经泄露给第三方但信息主体无法控制的情况”和“泄露的原因是企业的过错导致的”两个要件的,即构成损害,则根据3和4确定损害大小。^⑫

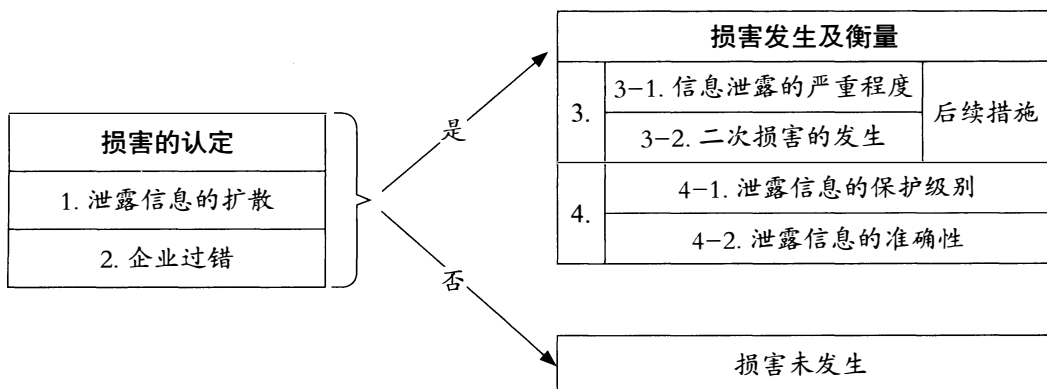


图1 韩国司法实践的信息泄露损害认定与衡量

^⑨ 参见《最高检就检察机关个人信息保护公益诉讼典型案例答问》,载中华人民共和国国务院新闻办公室官网, http://www.scio.gov.cn/xwfb/gfgjxwfb/gfgjfbh/zgj/202307/t20230705_726501.html, 2024年2月13日访问。

^⑩ See Dong-Hee Lee & Tae-Sung Kim, *A Framework for Calculating Damages of Personal Information Leakage Accidents*, in Wookey Lee & Carson K. Leung eds., *Big Data Applications and Services 2017*, Springer, 2018, p.20.

^⑪ See Cha Geon-sang, *A Study on the Criteria to Estimate the Compensation from the Infringement of Personal Information*, Doctoral thesis, Soongsil University, 2011, p.84-85.

^⑫ See Dong-Hee Lee & Tae-Sung Kim, *supra* note 70, 20-21.

上述主张意味着法律完全可以针对微小的系统性损害发展出新的衡量模式与赔偿标准,就此,韩国司法实践的层次化认定与衡量模式值得参考。未来我国相关法制的完善除有必要建立类似的层次化损害认定与衡量机制外,还应发展与此相关的损害救济机制,其中应特别注意充分考量两个要点:

第一,基于数据信息损害的特殊性,其责任承担方式不宜以财产赔偿为限,而应发展更多的损害救济方式。财产与非财产损害的界限并非泾渭分明,“得否以金钱衡量”本身就蕴含了价值判断的成分。^⑦例如,针对数据信息被篡改引发的声誉损害,应在财产赔偿的同时引入声誉修复机制,以使损害的救济手段与损害的认定和衡量结果一致。

第二,应引入损害赔偿模型。为平衡产业发展与个体救济,初期可通过损害赔偿模型化实现损害赔偿的概括化,即不区分财产损害和非财产损害,采用“一并请求”的法律技术,根据受害者的损害后果得出统一的损害赔偿额。后期可通过专门的立法进一步明确建立损害赔偿模型,如美国《石棉伤害公平处置法》就规定了联邦政府对石棉受害者损害赔偿的价目表。随着数据信息损害的日益频发、个体权益保护倾向的增强,数据信息损害的赔偿模型很可能将像海上油污损害、石棉损害等逐渐通过司法案例确立,并最终被纳入正式的法律规定之中。如此,对损害中不确定性风险的认定与衡量就能够通过清晰的模型传递至最终的救济结果。

五、结 语

在数字经济时代,侵权法正在面对数据信息损害的挑战。延续传统的损害认定模式和损害衡量标准显然已经无法适应当下数据泄露、网络勒索攻击频发的安全态势,故而有必要进行调整。其一,在推进数据要素市场化配置的背景下,应承认数据财产权益的存在,并认可数据泄露等事件所导致的数据信息损害属于侵权法意义上的损害结果。其二,对相当因果关系认定理论进行扩充,并结合举证责任分配规则,规定自然人对信息处理者的侵权行为与损害结果之间的因果关系证明仅需满足“信息处理者持有个人信息”“发现个人信息泄露的时间、地点与信息处理者的数据处理行为之间存在相当关联性”以及“自然人未主动泄露个人信息”三个要件,信息处理者则需要就“数据泄露并非由自身造成”进行举证。其三,对于数据泄露导致的牵连性损害结果,应有限度地承认业务链直接的数据信息损害,类型化业务链后续的常见数据信息损害(即“身份盗用、冒用”“个人信息和行为数据篡改”导致“影响重大权益的机会丧失与福利减损”),同时积极扩展损害赔偿责任承担方式,并引入损害赔偿模型来解决损害赔偿的计算问题。

回首过去,1960年至1985年是侵权法历史上最有活力的时期,因工业大规模生产带来诸多社会问题,在汽车、环境、药品、耐用消费品等领域推动了侵权责任法“巨大的

^⑦ 参见李昊:《损害概念的变迁及类型建构——以民法典侵权责任编的编纂为视角》,载《法学》2019年第2期,第77页。

动荡和爆炸”。^⑭ 历史总是惊人的相似——如何在侵权制度中评价、认定数字时代无形、不确定、系统且微小的损害,又成为当前数字时代侵权制度亟待解决的重大问题。毫无疑问的是,数据信息损害的承认与救济不仅有助于保障个体合法权益,也有助于重新厘清数据财产化过程中需要解决的权益损害难题。通过损害认定与计算制度的革新,可以使侵权责任制度参与重塑社会生产方式变革中的社会权利分配,解决大量被现行损害认定及赔偿计算规则挡在法院门口的救济需求,更有助于深入关切每个个体的冷暖枯荣,真正实现数字时代的公平正义。

Abstract: The principle of ‘no harm, no compensation’ means that the recognition of harm is a prerequisite for civil remedies. Actions such as the illegal processing of personal information and data may cause non-material data and information harm. However, this form of harm is difficult to gain legal recognition due to its incompatibility with traditional elements of harm. With the concepts of risk distribution and public governance in mind, it is institutionally necessary and theoretically feasible to acknowledge the independence of data and information harm, leveraging the tort system’s functions of individual relief and risk prevention. Firstly, there should be a shift in mindset to understand that the traditional concept of harm is constructed based on the social mode of production. The transformation from the industrial age to the digital age provides ample legal basis for recognizing data and information harm, addressing institutional barriers related to uncertainty, causality, and individual significance. Secondly, remedial rules should be adjusted. On one hand, direct data and information harm, such as illegal collection, access, leakage, and loss of personal information data, should be legalized, and subsequent data and information harm should be expanded in a typified manner, acknowledging common types of non-material harm. On the other hand, for minor systemic data and information harm, public interest litigation should be used as a remedial measure, with statutory compensation methods employed for quantification.

(责任编辑:任彦)

^⑭ See Gary T. Schwartz, *The Beginning and the Possible End of the Rise of Modern American Tort Law*, Georgia Law Review, Vol.26:601, p.604-606 (1992).