风险作为损害:大数据时代侵权“损害”概念的革新*

田 野
(天津大学法学院,天津 300072)

摘 要:在个人信息的侵权法保护路径下,损害的认定陷入困境。个人信息损害因具有无形性、潜伏性、未知性、难以评估等特征,是否符合“确定性”标准存在疑问。为适应大数据时代的需求,应当对传统侵权法上的损害概念加以反思,承认风险性损害。损害的确定性不等于损害已发生,实质性的未来风险亦可满足确定性要求。信息暴露带来的风险升高、预防风险的支出和风险引发的焦虑是侵权造成利益差额的体现,皆可成立损害。个人信息风险损害的认定应以场景化为基本进路,于个案中综合考量信息的类型、处理行为的目的方式、信息误用的迹象等因素而做出判断。

关键词:个人信息;侵权;损害;确定性;风险

中图分类号:DF522　　**文献标识码**:A　　**文章编号**:1005-9512(2021)10-0025-15

DOI:10.15984/j.cnki.1005-9512.2021.10.003

在大数据时代背景下,对个人信息的侵害愈演愈烈,个人信息保护无可回避地成为焦点问题。对信息处理者追究侵权责任是一条可能的规范路径。《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条规定:“处理个人信息侵害个人信息权益造成损害,个人信息处理者不能证明自己没有过错的,应当承担损害赔偿等侵权责任。”该条对侵害个人信息的侵权责任进行了特别规定,确立了过错推定原则。然而,现实中个人信息侵权的判定仍存在不小的障碍,特别是损害的认定困难重重。无损害即无侵权,这是传统侵权法的经典信条,针对个人信息的侵权概莫能外。问题的关键在于,与一般侵权相比,个人信息侵权在很多方面具有特殊性,损害常常表现为信息泄露后被非法使用的未来风险。[①] 这些风险性“损害”是否具备足够的“确定性”以满足成立侵权责任的要求,存在巨大争议。在大量的案件中,法院以信息主体没有遭受现实的损害为由驳回诉讼请求。鉴于个人信息侵权的特殊性和高发性,有必要反思与重塑损害概念,有条件地认可风险性损害。

一、“损害”在传统侵权法上的经典界定

在侵权法框架下,“损害”对于责任的判断具有基础性意义。侵权法的首要功能即在于填补损害,

作者简介:田野,天津大学法学院教授、博士生导师。

* 本文系司法部国家法治与法学理论研究项目“个人基因信息的法律保护研究”(项目编号:19SFB2045)的阶段性成果。

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

若无损害,自无填补之必要。[②] 于侵权责任诸构成要件中,损害是前提性要件,损害若不成立,便无所谓因果关系,更无须谈论过错。《中华人民共和国民法典》(以下简称:《民法典》)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。"与已经废止的我国《侵权责任法》第 6 条第 1 款相比,它在表述上补齐了损害要件和因果关系要件,使侵权责任的构成要件更加完整和明显。[③]

究竟何谓损害? 如何认定损害? 这是一个十分复杂的问题。《民法典》及我国其他法律规范对于损害的概念均没有进行正面的界定。从域外法来看,《奥地利民法典》第 1293 条规定:"损害就是指任何人就其财产、权利或者其人身所遭受的不利益。"这是世界范围内明确界定损害的为数不多的立法例。按照民法学界一般的认知,损害(damage)就是民事主体遭受的一种不利益,包括财产上的不利益(损失)和非财产上的不利益(伤害)。[④] 关于损害的本质,历来存在着差额说与组织说之争,前者是主流学说。差额说最早由德国学者麦蒙森(Mommsen)提出,在该学说下损害是指侵权行为没有发生的假想情况下原告应当享有的利益状态(被减数)和侵权行为已经发生的现实情况下原告实际享有的利益状态(减数)之差额。[⑤] 差额说一经提出就被德国法院和学者广泛接受,对大陆法系国家损害赔偿理论产生了巨大影响。其不仅在财产损害赔偿领域中适用,而且在非财产损害赔偿领域中逐渐被认可。构成"损害"通常要满足以下三个条件。(1)损害是侵害合法民事权益的结果。所谓"合法权益"包括权利和利益。(2)可补救性。其一,损害已达到一定的严重程度,具有补救的必要性。其二,损害需具有补救的可能性。这并非意味着损害必须可以计量,而是要求其必须是依据社会一般观念应予救济的不利益。(3)确定性。损害原则上应是已经发生的客观事实,或者是有充分的现实依据证明未来将会发生,而不能是主观臆测的。[⑥] 依据不同的标准,损害可作各种分类,其中最基本的分类是根据损害的性质分为财产损害和非财产损害。在我国法上,又将非财产损害进一步区分为人身损害和精神损害。因此,三分法成为损害分类的基本格局。

在广义上,损害泛指各种不利益,而危险本身也构成一种特殊损害(即使现实的损害尚未发生),与之相对应的是消除危险等预防性责任方式。在狭义上,损害则与赔偿相对,二者如影随形,被合称为"损害赔偿"。尽管责任方式的多元化被认为是侵权法在当代的发展趋势,不过不可否认的是,损害赔偿在诸种责任方式中仍具有绝对主导地位,以至于损害赔偿常常成为侵权责任的代名词。[⑦] 已经废止的我国《侵权责任法》第二章名为"责任构成和责任方式",偏重于宣示责任方式的多元化。事实上这种多元化也是侵权责任法从传统债法中独立出来的重要论据。《民法典》第七编第二章则采用"损害赔偿"的表述,强调损害赔偿在侵权责任中的核心地位,在杨立新教授看来,这是侵权法向债法的回归。[⑧] 在《民法典》时代,损害赔偿的责任方式得到凸显,如果没有特别说明,损害通常仅指那些需要以赔偿获得填补的不利益。笔者于本文中探讨的损害,也是采用此种狭义概念。

以上界定构成了侵权法上损害认定的法理基础,其中"确定性"标准是最核心的要素,也是损害认定难点之所在。确定性要求损害必须真实客观地存在,不能是捕风捉影的主观想象。不只是大陆法系国家将确定性作为损害认定的核心,英美法系国家亦然。在美国,要提起诉讼必须要满足美国联邦宪法第 3 条规定的起诉资格(standing to sue)的基本要求:(1)其遭受了"事实上的损害"(injury－in

②参见王泽鉴:《侵权行为》,北京大学出版社 2009 年版,第 175-176 页。

③参见黄薇:《中华人民共和国民法典侵权责任编释义》,法律出版社 2020 年版,第 7 页。

④参见王利明:《侵权责任法研究(上卷)》,中国人民大学出版社 2010 年版,第 302 页。

⑤参见王泽鉴:《损害赔偿》,北京大学出版社 2017 年版,第 63 页。

⑥参见张新宝:《中国侵权行为法》,中国社会科学出版社 1998 年版,第 93-94 页。

⑦参见前注④,王利明书,第 304-305 页。

⑧参见杨立新:《〈民法典〉对侵权责任规则的修改与完善》,载《国家检察官学院学报》2020 年第 4 期。

—fact)；(2)该损害源于被告的行为；(3)该损害有通过司法裁判进行救济的可能性。其中，“事实上的损害”尤为重要，其判断又细化为若干具体标准：第一，损害必须是已发生(actual)的或者是迫近的(imminent)，不能是假设性的(hypothetical)或推测性的(speculative)；第二，损害必须是具体的(concrete)而不能是抽象的(abstract)，必须是针对特别人的(particular)而不能是集合性的(collective)。⑨这些标准与大陆法系的损害“确定性”标准异曲同工。确定性标准对于个人信息侵权原则上亦应适用，然而麻烦就在于：由于个人信息损害的无形性、未知性等个性化特征，其往往看起来不那么确定。

二、个人信息侵权中损害认定的困境

传统侵权法上关于损害的经典界定若要在个人信息侵权领域适用，在一定程度上就会面临不适应性之困境。如果针对个人信息的处理已发生实际的损害后果，则侵权损害要件成立自不待言。难点在于，如果信息泄露后尚未有现实的损害结果发生，只是有未来被侵害的风险以及由此带来的紧张焦虑，看起来信息主体什么也没有失去，故损害是否成立常常引发争议。⑩

与一般侵权造成的损害相比，个人信息侵权的损害具有明显的特殊性，突出体现在以下几个方面。其一，无形性。与财产权或物质性人格权的损害通常有形不同，个人信息以电子数据的形式为常态，其损害也是无形的，本质上是尊严之损害。这种无形损害比有形损害更加隐蔽和难以确定。其二，潜伏性。与已现实发生的损害不同，个人信息损害的后果通常并不马上显现，而是表现为泄露后被他人误用的潜在威胁。⑪ 这种威胁本身能否构成损害不无疑问。其三，未知性。在大数据条件下，个人信息被处理的频次、数量是惊人的，不断深化的数据共享更扩张了个人信息流通的范围。个人信息泄露后将流向何处，被何人获取，用于何种目的，会给信息主体造成何种不利益，很难预先判断。⑫其四，评估和计算困难。按照差额说，必须首先确定侵害发生后的利益状态，才能与损害前的状态进行比较，然而对于个人信息的潜在无形损害而言，很难加以准确评估。这种评估计算的困难不只是体现在与财产权和物质性人格权的损害相比较的情形，即使是在精神性人格权内部，姓名权、肖像权、名誉权等权利损害的评估标准也比个人信息损害明确得多。正是由于上述特殊性，个人信息侵权案件中损害的认定面临重重困境。在信息主体遭受现实的侵害之前，未来遭受侵害的风险看起来就是一种对损害的猜测而非损害本身，其是否满足“确定性”的损害检测标准显得扑朔迷离。

从损害对应的侵权责任方式来看，对个人信息泄露带来的风险可适用消除危险、赔礼道歉等非赔偿性责任方式自不待言，损害赔偿的责任方式能否适用则值得探讨。《民法典》第 995 条确立了人格权请求权，其本质是基于人格本身而产生的固有请求权，区别于侵权损害赔偿请求权。消除危险等责任方式不以过错为要件，也不适用诉讼时效。⑬ 对个人信息的损害风险可基于人格权请求权适用消除危险责任方式当无疑义，关键在于能否更进一步适用损害赔偿责任？此问题在比较法上大概形成了两种针锋相对的观点：一种观点认为，鉴于大数据时代的背景及个人信息侵权的特殊性，应对损害概念作灵活的扩张解释，承认未来风险作为损害的可赔偿性；另一种观点则固守传统的“确定性”标

---

⑨ See Emily Schmidt, *Article III Standing in Data-Breach Litigation: Does a Heightened Risk of Identity Theft Constitute an Injury-in-Fact*, 49 Cumberland Law Review 389 (2019).

⑩ 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。

⑪ 参见朱宣烨：《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》，载《法学杂志》2018 年第 11 期。

⑫ 参见阮神裕：《民法典视角下个人信息的侵权法保护——以事实不确定性及其解决为中心》，载《法学家》2020 年第 4 期。

⑬ 参见王利明：《民法典人格权编的亮点与创新》，载《中国法学》2020 年第 4 期。

准,认为所谓个人信息的未来风险充其量只是一种主观臆测。[14] 法院在司法实践中态度也不一致。

个人信息侵权案件损害认定难,这是大数据时代世界各国共同面临的挑战。美国法上关于个人信息损害认定的案例演进尤为引人注目,围绕美国联邦宪法第 3 条“事实上损害”的解释适用,各级法院存在着严重的分歧。在 Clapper v. Amnesty International 案(以下简称:Clapper 案)中,[15]原告主张《外国情报监视法》(the Foreign Intelligence Surveillance Act)违宪,理由是这部法律使政府部门很容易地获得监视授权,而原告基于工作性质不可避免地要与潜在的被监视对象存在较为密切甚至敏感的联系,因此担心自己的个人信息在监视下被泄露。原告提出的理由主要有两点:第一,在未来的某个时点对交流活动的监视将给其造成损害具有客观合理的可能性(objectively reasonable likelihood);第二,原告不得不采取措施预防风险而花费了大量成本。最初,地区法院驳回了原告的诉求。随后,在上诉审中第二巡回法院支持了原告的主张。然而,联邦最高法院推翻了第二巡回法院的判决,其主要论据是:首先,未来的威胁要成立损害,必须是“确定迫近”(certainly impending)的,而所谓“客观合理可能性”的门槛过低;其次,原告的主张是建立在高度推测性的基础上的,背后有各种各样的可能性;最后,采取预防措施的花费因为是基于凭空的揣测而难以成立。尽管美国联邦最高法院否定了原告的诉求,但并未正面否定未来风险构成损害的可能性。法官在判决书中使用了“实质性风险”(substantial risk)的概念,这意味着如果在特定场景下个人信息的未来风险满足实质性标准,也存在成立损害的可能性,只是 Clapper 案的具体情况不符合该标准。美国联邦最高法院审理的另一个重要案例是 Spokeo, Inc. v. Robins 案(以下简称:Spokeo 案)。[16] 被告 Spokeo 是一家从事消费者信用评估业务的公司,原告主张被告针对其作出的信用报告有多处信息不准确,违反了《公平信用报告法案》(the Fair Credit Reporting Act)。地区法院认为原告没有遭受实际损害,但第九巡回法院持相反观点,认为损害是特别针对原告的。联邦最高法院则强调,损害不只应是特别的(particular),还必须是具体的(concrete),两个要素不能等同,缺一不可。原告的损害确实符合特别性要件——其损害是原告个人而非集体遭受的,但是不符合具体性要求。所谓“具体”即损害必须是真实的(real),不能是抽象的。美国联邦最高法院认为“具体”不要求一定有形,无形的损害(intangible harm)也可能是具体的,但是单纯的程序性违法不能认为是具体的。

Clapper 案和 Spokeo 案具有标志性意义,通过它们,美国联邦最高法院试图确立个人信息侵权案件中损害认定的基本标准,Clapper 案强调“迫近性”标准,Spokeo 案则强调“特别性”和“具体性”标准。不过,这些标准都是高度弹性的,如何解释适用存在很大的灵活空间。对于信息泄露后的未来风险能否构成损害,美国联邦最高法院并未给出结论性的明确立场,虽然这两个案件都以否定性判决收尾,但是并不排除在其他案件的特殊场景下未来风险构成损害的可能性。各下级法院对这两个案件树立的标准所采取的立场或开放或保守,存在严重的分歧。其中第六巡回法院、第七巡回法院、第九巡回法院和华盛顿特区巡回法院倾向于对损害作扩张解释的立场,第三巡回法院、第四巡回法院和第八巡回法院则采取了严格限制解释的立场。[17] 在 Beck v. McDonald 案中,[18]存有原告个人信息的电脑丢失,原告主张身份窃取风险升高的损害赔偿。为了证明风险的实质性,原告提出了一项统计数据:33%的电脑失窃案件都会伴随后续的身份信息失窃。不过,第四巡回法院认为这一统计数据只是

[14] See Benjamin C. West, *No Harm, Still Foul: When an Injury-in-Fact Materialized in a Consumer Data Breach,* 69 Hastings Law Journal 701 (2018).

[15] See Clapper *v.* Amnesty International, 568 U.S. 398 (2013).

[16] See Spokeo, Inc. *v.* Robins, 136 S. Ct. 1540 (2016).

[17] See Jameson Steffel, *The Time between the Theft and the Injury: Standing Requirements Based on a Future Risk of Identity Theft after a Data Breach,* 88 University of Cincinnati Law Review 1189 (2020).

[18] See Beck *v.* McDonald, 848 F.3d 262, 267 (4th Cir. 2017).

一般意义上的，不符合“特别性”标准的要求，没有证据表明获得这些电脑的人瞄准了其中存储的个人身份信息并用于邪恶目的。电脑丢失后将被何人获取，为何种利用，存在各种各样的可能性，法院拒绝对捉摸不定的可能性作出猜测，否定单纯的对身份信息被窃取的恐惧构成损害。第四巡回法院在判决推理中也提出，在另外一些案件中，黑客就是以偷窃个人身份信息为明确目的，这种未来损害的风险确实是实质性的，但是该案的情况与此不同。2019 年 6 月，美国华盛顿特区巡回法院对一起政府机构泄露雇员个人信息的案件作出判决，肯定了升高的未来风险构成损害。该案被告美国人事管理办公室（the U.S. Office of Personnel Management）是负责联邦机构雇员人力资源管理的政府机构，从 2009 年开始其管理下的数据库就遭遇黑客攻击，导致约 2100 万雇员的个人信息泄露，其中包括很多敏感的个人信息（如出生日期、指纹、社会保障号码等）。法院认为，当黑客侵入数据库窃取个人信息时，欺诈或身份冒用是迟早的事。被告辩称黑客攻击是针对美国政府而非个人，但法院认为二者并不相互排斥，在个人身份信息已被窃取并已有部分受害人遭遇身份欺诈的情况下，讨论黑客的意图变得无关紧要。被窃取个人信息的敏感性也是影响法院判决的十分重要的因素。⑲

在我国，个人信息侵权的损害赔偿同样面临困境。由于个人信息损害的模糊性，在很多案件中法院往往以原告没有证明遭受实质性损害为由驳回损害赔偿的诉讼请求。⑳ 与美国情况不同的是，我国法院较少直接针对未来风险是否构成损害的问题展开正面论证，因为在我国，现实的法律框架下针对个人信息损害的赔偿方式主要是精神损害赔偿，所以损害认定的困境主要体现在个人信息精神损害赔偿适用的艰难。精神损害赔偿的适用以精神损害的“严重”为先决条件。《民法典》第 1183 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。”事实上，我国民事立法在精神损害赔偿问题上始终坚持“严重”要件，其旨在防止精神损害赔偿的滥用。在司法实践中，我国法院对这一要件的解释适用持较为严格的立场。在个人信息侵权案件中，法院常常以信息主体不能证明精神损害或者精神损害不够严重为由拒绝支持精神损害赔偿的诉讼请求。例如，在朱烨与北京百度网讯科技有限公司隐私权纠纷案中，㉑二审法院认为朱烨没有提供证据证明百度网讯公司的个性化推荐服务对其造成了事实上的实质性损害，朱烨虽然强调自己因百度网讯公司的个性化推荐服务感到恐惧、精神高度紧张，但这仅是朱某个人的主观感受，法院不能也不应仅凭其主观感受就认定损害。在邓立荣与北京顺丰速运有限公司侵权责任纠纷案中，㉒邓立荣的收件地址信息和在外兼职信息被顺丰公司泄露，导致其被原单位解雇，但法院认为没有证据证明邓立荣因信息泄露而遭受明显的精神痛苦，故对其精神损害赔偿的请求不予支持。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，㉓付全贵因订购机票信息被泄露而遭遇诈骗，法院支持了经济损失的赔偿，但是对精神损害赔偿请求，因付全贵未提供证据证明明显的精神痛苦，法院判决驳回。在这些案件中，即使是在信息主体已遭遇诈骗、因信息泄露丢掉工作的情况下，法院仍然认为其“不痛苦”或者不能证明“痛苦”，可见在个人信息侵权案件中要获得精神损害赔偿之艰难。相比之下，法院更喜欢选择适用赔礼道歉的责任方式。赔礼道歉固然有其价值，但与损害赔偿的救济功能是不同的。

美国法院在是否认可数据泄露造成的未来风险构成损害问题上的纠结，我国法院对于个人信息侵权精神损害赔偿适用的保守立场，正是数据时代损害认定困境的缩影。当需要为遭受不利益的信息主体提供民事救济时，寻找损害成为很难逾越的门槛。这并非只在极少数案件中发生，而是数据时代全球范围的典型图景和主要矛盾。面对这样棘手的问题，裁判者常常陷入左右为难的窘境。

⑲ See AFGE *v.* OPM (In re United States OPM Data sec. Breach Litig), 928 F. 3d 42 (D.C. Cir. 2019).

⑳ 参见北京市第二中级人民法院（2016）京 02 民终 3276 号民事判决书。

㉑ 参见江苏省南京市中级人民法院（2014）宁民终字第 5028 号民事判决书。

㉒ 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。

㉓ 参见北京互联网法院（2018）京 0491 民初 1905 号民事判决书。

三、认可个人信息风险性损害的正当性

针对前述个人信息侵权中损害认定的困境，需探索新的解困路径，认可风险成立损害是一条富有希望的出路。基于风险社会的背景、损害概念扩张的国际趋势、相关领域风险损害获得承认的既有实践以及风险与确定性标准的兼容等多维度考量，承认个人信息的风险性损害有充分的正当性基础。

（一）现实基础：风险社会背景下的信息风险分配

承认针对个人信息的风险性损害，是因应风险社会的现实需要。风险社会的概念为德国著名社会学家乌尔里希·贝克所首倡，他在 1986 年出版的《风险社会：新的现代性之路》一书中对风险社会进行了系统论述。根据贝克的观点，“风险可被定义为以系统的方式应对由现代化自身引发的危险和不安”。[24] “在风险社会里，‘过去’丧失了它决定‘现在’的权力，取而代之的是‘未来’。”[25]风险社会的特征可大概描述为以下几个方面。第一，风险社会是现代化和科学技术进步的产物。先进科学技术在提高生产力、创造财富以推动现代化的同时，也带来了环境污染、核辐射、生态破坏等一系列“副作用”，这些风险如此恼人却又如影随形般难以摆脱。第二，风险社会中的所谓风险具有人为性而不同于自然风险，与人类自主的活动脱离不了干系。[26] 第三，如果说风险社会之前的社会主要矛盾是物质财富的短缺和分配不平等，那么风险社会的主要矛盾则是风险损害的缓解与分配。贝克将前者归结为“我饿”，而将后者归结为“我怕”，在风险社会“共同的焦虑取代了共同的需求”。[27]

风险社会大约始于 20 世纪中叶，大数据时代的来临则是晚近以来的事情。大数据时代并非居于风险社会之外而是处于其中，是风险社会的“新版本”。数字信息技术的进步带来了新的风险元素，使本就严峻的形势雪上加霜。在大数据时代背景下，对个人信息的处理无时无处不在进行。人们对数据、信息是如此依赖，以至于难以想象，如果没有各种应用程序（App），社会将如何运转，是否会陷入停滞。在个人信息处理常态化的社会条件下，风险不可避免地被裹挟而至，个人信息保护遂成为焦点议题。动辄涉及几百万甚至上千万人的个人信息泄露事件已经不是什么罕见的新闻，而是频繁见诸报端。处于风险中心的信息主体急需获得法律的庇护。问题在于，在风险转化为现实的身份窃取和诈骗之前，信息主体可以做什么？可以主张自己受到了损害而诉请赔偿吗？风险社会“已成为人们生活的基本场域和现实环境”。[28] 在此情况下，“风险”应该成为人们思考问题和解决问题的根本出发点，法律治理的理念、模式和手段亦应根据风险社会的特点做出因应性的调整，其中一个最基本的问题就是风险的分配。如贝克所言，和财富一样，风险也需要分配。[29] 具体到个人信息保护领域，由于人们已离不开信息，不可能因为风险的存在就放弃个人信息处理，如何分配风险才是关键。在信息主体和处理者之间由谁承担风险更符合法的价值？信息处理者应承担更多的风险，理由在于：其一，处理者制造了风险，是信息风险之源；其二，与信息主体相比，处理者有更强的能力控制风险；其三，处理者从个人信息处理中获益，按照权利义务相一致原则理应承担更大的责任；其四，处理者有能力通过提高产品或服务价格、购买责任保险等方式分散风险；其五，令处理者承担风险有利于敦促其采取更积极的措施降低风险，从而起到预防损害的作用。

在侵权法的视野下，将满足一定条件的风险视为可赔偿的损害，是风险分配的具体实现方式。当

---

[24] [德]乌尔里希·贝克：《风险社会：新的现代性之路》，张文杰、何博闻译，译林出版社 2018 年版，第 7 页。

[25] 同上注，乌尔里希·贝克书，第 24 页。

[26] 参见刘水林：《风险社会大规模损害责任法的范式重构——从侵权赔偿到成本分担》，载《法学研究》2014 年第 3 期。

[27] 参见前注[24]，乌尔里希·贝克书，第 48 页。

[28] 杨知文：《风险社会治理中的法治及其制度建设》，载《法学》2021 年第 4 期。

[29] 参见前注[24]，乌尔里希·贝克书，第 3 页。

然，从风险社会概念中抽象意义的风险到具体法律责任构成要件意义上风险的转化，尚有许多工作要做。从世界范围来看，最新的个人信息保护立法皆十分重视风险。例如，具有重大影响力的欧盟《个人数据保护通用条例》（以下简称：GDPR）将风险评估作为个人信息保护的重要方法，《个人信息保护法》四次使用了“风险”概念，将风险评估设定为信息处理者的重要义务。在笔者看来，风险在个人信息保护中的意义不应止于风险评估，而是还应包括在侵权责任判定中被视为损害。

（二）损害概念扩张的国际趋势

损害认定的困难已经成为个人信息侵权案件中受害人获得救济的障碍，这是世界各国共同面临的挑战。如何破除这些障碍，为信息主体的救济扫平道路，成为比较法上被热议的话题。鉴于困境源于传统侵权法上的损害认定标准对于个人信息损害的不适应性，寻找解困之路的大方向是因应大数据时代发展的需要，基于个人信息损害的特殊性，对损害的概念加以革新。所谓革新并非意味着要彻底抛弃侵权责任的损害要件或者是确定性标准，而只是对损害的概念作更为灵活开放的解释。事实上，作为对大数据时代挑战的回应，侵权损害概念的扩张在国际上已经成为一种大趋势。呼吁对损害概念作更加开放性界定的声音日益高涨，一些国家和地区正在司法实践中实行着这一主张，甚至已在法律条文中明确宣示这一精神。例如，GDPR“鉴于”部分第 146 段明确指出：“损害应根据欧盟法院的判例法作广义解释，并充分反映本条例的目标。”这一表述毫不隐讳地表明了扩张损害概念的立场，在 GDPR 的规则下社会性歧视、精神痛苦、人格自由发展之障碍等皆可成立损害。GDPR 第 82 条规定：“由于违反本条例的行为而遭受重大或非重大损害的任何人均有权就所受到的损害从控制者或者处理者处获得赔偿。”据此，可以获得赔偿的损害不需要重大，即使是非重大损害亦可获得赔偿。在 GDPR 上述精神的指引下，德国也在扩张损害解释的道路上前行。2018 年新修订的《德国联邦数据保护法》第 83 条第 2 款规定：“信息主体可以主张对非物质性损害的赔偿。”这一新规则改变了旧法中非物质性损害赔偿的“重大性”条件限制。评论者指出：“侵害人格权本身就足以构成损害。依照审判实践，损害的概念应当宽泛地解释。”[30]在美国，联邦最高法院在针对数据泄露类型案件的判决中，针对未来误用的风险能否构成损害采取了较有弹性的立场，未来风险如果是“实质性”的、“迫近”的，仍可能构成损害。法院系统内部存在分歧，不过有不少法院认可个人信息的未来风险损害。

至于个人信息损害概念扩张的具体进路，国内外学者提出了各种各样的主张。有学者认为，个人信息的暴露本身即为损害，无须再寻找其他的损害。[31] 有学者主张，应将数据泄露造成的风险升高视为损害。[32] 有学者建议，应当对个人信息的无形损害实行损害的推定。[33] 还有学者对个人信息领域出现的新型损害进行了类型化研究，并主张对这些新型损害应采取部分认可的立场。[34] 总之，在个人信息侵权案件中缓和损害要件，对其作灵活宽松的解释，已经成为大数据时代的大势所趋。

（三）承认风险性损害的既有实践

事实上，关于风险能否作为损害的讨论不是近些年才开始的，也不只局限于个人信息侵权领域，而是很早就在更广阔的私法领域中存在。其中，医疗损害责任、环境污染和生态破坏责任、毒物侵权是风险性损害获得较多认可的三个典型领域。

医生的不当诊疗行为往往会增加患者在未来遭受严重健康损害的风险，在现实的危害发生之前，

---

[30] 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。

[31] See Maxwell E. Loos, *Exposure as Distortion: Deciphering Substantial Injury for FTC Data Security Actions,* 87 George Washington Law Review Arguendo 42 (2019).

[32] See Jennifer Wilt, *Cancelled Credit Cards: Substantial Risk of Future Injury as a Basis for Standing in Data Breach Cases,* 71 SMU Law Review 615 (2018).

[33] 参见徐明：《大数据时代的隐私危机及其侵权法应对》，载《中国法学》2017 年第 1 期。

[34] 参见前注[30]，叶名怡文。

风险性损害表现为在未来患病的概率。尽管缺少认可风险损害(risk damage)的明确立法,但在司法层面存在一些支持风险构成损害的案例。在 Petriello v. Kalman 案中,[35]医生的过失损伤了原告的肠道,导致原告有 8%到 16%的在未来患肠梗阻的风险,法院最终认可了此种风险构成损害,并判决给予原告赔偿。在英国 Hoston v. East Berkshire Area Health Authority 案中,[36]法院也认为被告延误五天治疗使原告患缺血性坏死概率升高 25%的风险构成损害。[37]

在环境侵权领域,加害行为对生态环境造成的负面影响往往不会立即显现,生态损害一旦现实发生则经常具有不可逆性,这就涉及未来的风险能否成立损害的判断。在中国生物多样性保护与绿色发展基金会与雅砻江流域水电开发有限公司环境民事公益诉讼案中,[38]法院认为被告负责的牙根梯级电站建成后可能存在对濒危珍稀植物五小叶槭原生存环境造成破坏、影响其生存的潜在风险,判决被告暂停电站建设直至环境影响报告审批通过。在"云南绿孔雀"公益诉讼案中,法院认定中国水电顾问集团新平开发有限公司建设的戛洒江一级水电站淹没区对国家一级保护动物绿孔雀栖息地及热带雨林整体生态系统存在重大风险,判决被告中止工程建设。[39] 这两个案例的典型意义在于将未来的生态风险认定为损害,在不可逆的生态灾难发生之前就采取行动,避免了亡羊补牢的被动局面。

毒物侵权类型的案件中,原告多主张因接触有毒有害物质(如化学物质、生物物质)而遭受健康损害威胁,不过在现实的损害发生之前接触这些物质只是带来了患病的风险。从域外法来看,尽管有分歧,但部分法院支持将此种风险作为损害。例如在 Barker v. Corus U.K. Ltd 案中,[40]原告主张因其在作为被告的雇员工作期间接触石棉粉尘而面临罹患肺部间皮瘤(mesothelioma)和其他与石棉粉尘有关的严重肺病的风险,并主张因对患病的恐惧而陷入焦虑。法院最终认可上述风险成立损害。

上述三个领域树立了未来风险可成立损害的先例,这些领域中的风险与个人信息风险虽然在具体表现形式上不同,但在本质上是相通的,这就为个人信息风险性损害的成立提供了有力的佐证。需要特别指出的是,与前述三个领域相比,个人信息侵权带来的风险性损害问题更加突出和具有普遍性,风险化是数据时代个人信息损害的一般特征。

(四)风险与"确定性"矛盾之解释论调和

诚然,风险概念直观传达的是一种面向未来的可能性,因此表面看起来与损害的确定性标准之间存在一道天然沟壑。不过,二者的冲突并非在根本上不可调和,可通过解释论的方法予以妥善化解。损害的确定性不能与损害已发生画等号,满足一定条件的风险仍可能符合确定性要求。

面对大数据时代个人信息被过度处理的现实,若将个人信息扩张保护作为政策目标,不一定需要采取另起炉灶的方式确立一套独特的损害判断标准,只需对传统的"确定性"标准予以"升级",赋予其在数据时代之新意涵。在经典的界定中,损害原则上应是已发生的事实,现实的损害是损害的常态。不过,未来的损害也可能符合确定性要求,二者并不相互排斥。在法国法上,"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"。[41] 在比利时,也认可未来损害的确定性。[42] 所谓"确定",不能狭隘地理解为"已发生",若有充分的证据证明损害"将发生",也可以说是确定的。在大陆法系,鲜有法条对损害下明确的定义,更无针对风险损害的特别条文,不过辩证地看,这也为损害的灵活解

[35] See Petriello *v.* Kalman,576 A.2d 474 (Conn.1990).

[36] See Hoston *v.* East Berkshire Area Health Authority, 1987 2 W. L. R. 287,rev'd. 1987 A.C. 750.

[37] 参见[美]戴维.G.欧文主编:《侵权法的哲学基础》,张金海等译,北京大学出版社 2016 年版,第 333 页。

[38] 参见四川省甘孜藏族自治州中级人民法院(2015)甘民初字第 45 号民事判决书。

[39] 参见云南省昆明市中级人民法院(2017)云 01 民初 2299 号民事判决书和云南省高级人民法院(2020)云民终 824 号民事判决书。

[40] See Barker *v.* Corus U.K. Ltd,[2006]UKHL 20, [2006] 2 A.C. 572 [Barker].

[41] 欧洲民法典研究组、欧洲现行私法研究组编著:《欧洲私法的原则、定义与示范规则(欧洲民法典草案)(第五、第六、第七卷)》,王文胜等译,法律出版社 2014 年版,第 236 页。

[42] 同上注,欧洲民法典研究组、欧洲现行私法研究组编著书,第 236 页。

释提供了可能的空间。正如 GDPR 所明确表达的立场，在大数据时代对个人信息损害作开放性解释是可能的，也是必要的。在司法实践中，这种开放性解释的立场正在被越来越多的法院采纳。

当然，并非所有的未来风险都当然符合确定性标准，那些捕风捉影的臆测不能被认为是确定的，只有那些有据可循的“实质性风险”(substantial risk)才可谓“确定”。实质性风险标准在一些案件中得到了很好的诠释。在 Attias v. CareFirst, Inc.案中，[43]被告健康保险公司未对消费者数据加密导致其被黑客窃取。美国华盛顿特区巡回法院基于两点考虑认可了原告事实上损害的成立：第一，黑客获取的信息中包括银行卡号码、社会保障号码等具有高度身份识别特征的信息，这些信息有高度的可能被用于身份欺诈；第二，该案与美国联邦最高法院审理的 Clapper 案场景不同，如果说后者的风险是建立在各种不确定可能性的高度推测基础上，那么前者在黑客攻击业已发生的情况下，对信息误用风险的担忧就不只是一种猜测，而是具有相当程度的确定性。[44] 这一判决推理颇具有启示意义。在大数据时代背景下，对损害的“确定性”标准应作灵活解释，未来损害的风险如果是“实质性”的，则可认为其满足确定性标准的要求。当然，未来风险是否是实质性的，有赖于个案中综合考虑各种因素。并非所有未来风险均构成损害，必须区分那些毫无根据的主观臆测与客观合理的风险。

综上所述，在个人信息侵权领域承认风险性损害具有充分的现实基础和法理基础。认可风险成立损害，是侵权法对大数据时代和风险社会的真切反映，是化解前述个人信息保护困境的有效出路。这并不是推倒重来式的法律变革，只需要通过适度弹性地解释损害认定的标准即可实现。

四、个人信息侵权中风险性损害的认定与适用

若认可风险具备成立损害的可能性，则需要进一步探讨的问题是，个人信息侵权案件中究竟哪些风险可以成立损害？须满足的条件要求是什么？应当看到，将风险纳入损害范畴，将不可避免地对法律的稳定性造成一定程度的冲击，引发滥诉之忧虑。笔者虽对个人信息风险性损害持赞同立场，但同时主张应对其适用予以严格限制。不是所有的风险都构成损害，必须将那些过于遥远的风险从可赔偿的风险之中排除。至于实现风险性损害救济的路径，应通过法律解释的方法。现实中个人信息风险的情况千差万别，通过法律条文加以规定既不可能也无必要，而只能由法官在个案中根据具体案情进行判断。侵权责任的一般条款即《民法典》第 1165 条第 1 款应作为风险性损害判断的基本依据。这一条文是高度概括的，只提及损害的概念而未进行更细致的界定，其既未肯定也未排除风险成立损害的可能性，这就留下了解释的空间。事实上我国民事法律中没哪个法律条文对损害认定的标准正面进行明确规定，诸如确定性等标准都是学者在理论上的阐发，在纠纷解决中则依赖法官的解释。进言之，个人信息侵权案件中风险损害的认定大概可从两个大的面向展开：一是寻找利益差额，将风险具象为各种类型化的不利益；二是明确风险是否满足确定性要求的具体判断标准，甄选若干关键考量因素，并放在个案场景下予以灵活适用。这两者均非另起炉灶，而是基本遵循了传统侵权法上的损害分析框架。

(一)寻找利益差额：风险性损害的态样

按照差额说，甄别损害的基本方法是对待认定损害发生前后的利益状态进行比较。个人信息侵权的风险性损害亦应将寻找利益差额作为损害认定的切入点。个人信息的风险作为无形的非财产损害，不容易通过直观的方法计算利益差额，但并非绝对不可评估。在进行利益差额的甄别时，通过类

[43] See Attias *v.* CareFirst, Inc., 865 F.3d 620, 627 (D.C. Cir. 2017).

[44] See Jameson Steffel, *The Time between the Theft and the Injury: Standing Requirements Based on a Future Risk of Identity Theft after a Data Breach,* 88 University of Cincinnati Law Review 1189 (2020).

型化方法将风险予以细分，有利于法律分析的精确化。

1.个人信息暴露导致的风险升高

个人信息侵权带来的风险性损害首先体现为信息暴露带来的风险水平的变化。在个人信息暴露之前，信息主体面临的风险为零或者是水平极低；而个人信息暴露之后，信息主体遭受侵害的风险陡升。将升高后的风险与暴露前的零风险或低风险相比较，就可窥见利益差额。以基因信息为例，其原本天然存在于人体之中隐而不宣，故不存在被非法处理的风险。然而，处理者通过基因检测的手段将 DNA 中碱基对的排列顺序(即基因信息)揭示出来，这就增加了基因信息被非法收集、传播和利用的风险。这是一种真实的客观存在的利益差，尽管其难以像有形财产损害那样精确计算。

信息暴露带来的风险升高体现在诸多方面，最普遍的风险就是身份窃取与诈骗。身份证号、银行卡号及密码等重要身份信息的泄露可能导致银行卡被盗刷，使信息主体蒙受经济损失。偷窃者可能冒用这些身份信息开立信用卡并恶意透支，导致不良个人信用记录，使信息主体在买房贷款、出行、消费等社会生活的各个方面遭遇障碍。除了财产损失，个人信息风险性损害还体现在人格权益方面。例如，基因信息的泄露可能导致个人隐私受损，使信息主体在就业、保险等各个方面遭遇歧视，还可能带来族群污名化的问题。人脸、指纹等生物识别信息的泄露导致的风险更加令人生畏。在现代社会个人信息面临的风险难以列举穷尽，所谓风险，有很多已经在各种损害事件中被证实。这些风险在成为现实损害之前看起来风平浪静，实则暗流涌动，一旦爆发，想要补救为时已晚。因此，有必要在悲剧发生之前认可风险本身即是一种可获赔偿的损害。

与一般的风险相比，个人信息损害风险具有很多方面的特殊性。首先，很多个人信息是不可更改或删除的，例如基因信息、生物识别信息。这些信息一旦泄露，信息主体没有办法通过更改的方式避免风险，这是十分可怕的。其次，个人信息风险在未来何时爆发具有不可测性。风险演化为现实损害的时间跨度，因泄露的信息类型不同而存在差异。银行卡信息的泄露导致的身份窃取一般在数小时内发生，因为信息主体通常会很快通过挂失、更换账号密码的方式避免风险。然而，另一些个人信息风险则会潜伏更长的时间，一些狡猾的偷窃者可能会在数年之后才非法利用这些信息。个人信息风险就像是一颗“不定时炸弹”。最后，个人信息风险具有继发性和广泛性。在个人信息处理无处不在的当下，泄露的个人信息将被多少下游处理者获取难以估计，损害可能无限多次地发生。在一些大规模的数据泄露事件中，数以千万计自然人的个人信息面临被不确定数量的偷窃者反复侵害的处境。

2. 预防风险的支出

在个人信息被泄露以后，身份窃用和欺诈的风险上升，信息主体因此需要采取一些预防措施以抵御风险，为此花费的时间、精力、金钱及其他支出，可被视为一种特殊类型的损害。这些预防性措施的成本在个人信息被泄露之前是不需要支出的，在泄露发生之后则成为必要，利益差额是较为明显的。针对这一问题，在市场上有专门的提供风险监控和管理的商业服务如保险、信用状况监督等等，购买这些服务需要花费金钱。在部分案件中，保存并不慎泄露了个人信息的处理者为信息主体在一定时间内免费提供此类服务，不过在大部分情况下信息主体需要自己买单。[45] 此外，信息主体采取更换银行卡或者服务商等预防性措施也可能会产生变动成本，如定期存款的利息损失、利率变化带来的损失。这些风险预防性措施支出本质上是财产性损失，易于计算。有争议者在于：这些所谓预防性支出是否建立在合理可靠的未来风险预测基础上。在部分案件(如前述 Clapper 案)中，法官拒绝承认此类支出构成事实上的损害，主要理由是：这些支出所据以发生的未来风险本身是信息主体自我想象的，并不真实存在，因此所谓预防性支出损害实为无源之水、无本之木。不过，也有部分法院支持此类支出构成事实上的损害。在根本上，信息泄露案件中的预防性支出能否构成损害，还是要回归到未来

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

受害的风险是否是实质性的这一前提性问题上来。在我国,对于当事人提出的成本性支出赔偿的诉讼请求,法院也有支持的范例。例如在沈晴与上海容蓁汽车用品有限公司姓名权纠纷案中,[46]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沈晴的身份信息,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,法院最终判决被告向原告支付包括维权成本在内的损失 2500 元。维权成本通常包括公证费、律师费、诉讼费等等,其中有些维权措施是预防性的,而有些在严格意义上不能等同于预防性措施。未来我国法院对个人信息侵权案件中的预防性支出应当持开放性立场,在未来风险满足实质性标准的情况下,支持此类损害赔偿的主张。《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》第 12 条第 1 款规定:“被侵权人为制止侵权行为所支付的合理开支,可以认定为民法典第一千一百八十二条规定的财产损失。合理开支包括被侵权人或者委托代理人对侵权行为进行调查、取证的合理费用。人民法院根据当事人的请求和具体案情,可以将符合国家有关部门规定的律师费用计算在赔偿范围内。”这一条款将制止侵权行为的合理支出明确纳入损害赔偿范围。笔者认为,对其中所称的“制止侵权行为”“合理开支”等可作广义解释,它们包含针对未来风险采取预防性措施的支出。

3.风险引发的焦虑

信息主体因个人信息的泄露而陷入焦虑不安之中,焦虑不安能否作为私法上的损害而获得赔偿值得探讨。因为焦虑是一种精神状态,所以其损害救济主要寄希望于被纳入精神损害赔偿。在解释论上,个人信息风险引发的焦虑能否构成《民法典》第 1183 条所称的“严重精神损害”,是法律适用的关键。详言之,可从以下两个方面加以判断:第一,风险性焦虑能否被解释为精神损害的一个子类型;第二,如果前一判断成立,那么焦虑型精神损害是否足够严重。

精神损害是一个高度抽象的概念,其具体的表现十分复杂,侵害不同的人格权益可能带来不同的精神损害。例如,侵害健康权造成的精神损害直观地表现为疼痛,侵害名誉权造成的精神损害常表现为羞辱。这些精神损害都是针对已经发生的侵害而存在的,是法律认可的精神损害的常态。相比之下,侵害个人信息造成的精神损害则常表现为对未来风险的焦虑、不安,其更不容易被认可。[47] 在真实的信息误用发生以前,信息主体的焦虑、不安是有依据的吗?符合确定性标准吗?焦虑、不安与疼痛、羞辱等精神损害相比,看起来在损害的明显程度上尚有差距。与前述预防性措施支出损害证成的困境如出一辙,焦虑与不安要成为损害,最大的瓶颈仍在于其所赖以建立的未来风险的确定性程度。焦虑不安究竟是信息主体凭空制造的心理压力,还是有理有据的担忧,是判断精神损害是否成立的关键。在大数据时代,为了生产生活的便利,对个人信息的频繁处理不可避免,不能令信息处理者动辄对信息主体赔偿精神损害。然而,在一些大规模的数据泄露事件中,已经有部分受害者遭遇身份偷窃,尚未遭受实际损害的信息主体对于未来的担忧并非杞人忧天,应肯定其为真实的精神损害。

“严重”是我国民法上精神损害赔偿适用的重要限制条件,而在个人信息侵权场域下,以焦虑、不安形式存在的精神损害往往看起来不那么严重。严重性条件的本意是对精神损害赔偿的适用作出限制,以防止滥用。不过,这种限制的合理性正在受到越来越多的质疑。[48] 从民事权利的位阶理论来看,人身权高于财产权。[49] 然而吊诡的是,在财产权领域里侵权损害赔偿责任却不以重大为要件,而是奉行全部赔偿原则,即使是轻微损害也给予赔偿。按照举轻以明重原则,侵害人身权益的损害赔偿不应弱于财产权。在传统侵权法对损害的经典界定中,轻微的不利益不构成损害。不过当法律条文中出现“损害”字眼时,就意味着已达到需要救济的程度,换言之,在民法条文中出现的“损害”自然蕴

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

[47] 参见前注⑩,解正山文。

[48] 参见前注㉚,叶名怡文。

[49] 参见王利明:《民法上的利益位阶及其考量》,载《法学家》2014 年第 1 期。

涵着“严重性”。按照《民法典》第 1183 条,在“精神损害”前加上“严重”二字,有画蛇添足之嫌。这一表述在逻辑上还可能推导出构成损害却不赔偿的结论,与侵权法填补损害的宗旨相违背。在个人信息侵权案件中,如苛求精神损害的严重性,则对于信息主体的保护构成障碍。从司法实践来看,在一些个人信息侵权案件中法院判决支持的精神损害赔偿数额很低,例如在李志刚与上海商数信息科技有限公司网络侵权责任纠纷案中,[50]被告未经原告同意使用了原告淘宝账户的相关信息,法院判决被告向原告支付人民币一元的精神损害赔偿。法院既然支持了精神损害赔偿请求,就意味着认可其严重性,然而对应一元赔偿的精神损害能有多严重是值得怀疑的。低数额的精神损害赔偿判决并不鲜见,这从一个侧面反映了“严重”要件事实上的不合理性。在域外法上,放宽精神损害赔偿的条件限制是一个重要动向,前述新修订的《德国联邦数据保护法》摒弃旧法中精神损害赔偿的严重性要件就是一例。在我国,既然《民法典》短期内不可能修改,要破除精神损害赔偿“严重性”条件的障碍,只能通过法律解释。笔者认为,可将“严重”解释为损害概念中本来具有的损害救济必要性要素,而非额外限制。

针对个人信息侵权中精神损害隐蔽化和难以证明的困境,一个潜在的解决思路是实行限额酌定赔偿。由法官在限额内对不易证明和计算的个人信息精神损害酌定赔偿数额,可以有效化解困境。我国法上也存在限额酌定赔偿的相关规定,不过只适用于财产损害赔偿,未来有必要将其扩展至精神损害赔偿领域。

(二)认定风险性损害的考量因素

为应对大数据时代的挑战,应当对个人信息损害的概念加以扩张,承认前述若干形态的风险性损害。然而,损害概念的扩张也不能毫无边界,应当看到,除了填补损害,数据的利用、产业经济发展及公共利益的维护也是不可忽视的价值。过于严苛的法律责任可能使信息处理者因频繁的赔偿而背上沉重的包袱,从而阻碍新兴数字经济的发展。作为侵权责任成立的首要条件,损害认定的门槛不能无限降低。就风险性损害而言,只有那些“实质性”风险才能成立损害。然而,某一风险究竟是实质性的还是非实质性的,在认定上有一定困难。事实上,对风险的实质性是不可能预判的,由于现实中个人信息侵权的情况千差万别,实质性风险的标准难以整齐划一,只能放在个案的具体场景中进行甄别。风险的实质性是一个应由法官裁量的事项,因而裁量时需要考虑的因素至关重要。个人信息风险性损害的认定应以场景化为基本思路,甄选若干关键考量因素,由裁判者在个案中综合判断。

1.个人信息的类型

自然人的个人信息是海量的,其类型多种多样。这些信息的性质与内容不同,对维护人格尊严而言的重要性不同,因此在损害的认定标准上也存在差异。一般而言,个人信息越重要、越敏感,其被侵害后成立风险损害的可能性就越高。[51]《民法典》和《个人信息保护法》皆对个人信息进行了分类,《民法典》中最重要的分类是私密信息和非私密信息,《个人信息保护法》则将个人信息分为敏感个人信息和非敏感个人信息。在数据开发利用的视角下,自然人对一般个人信息被处理有更高的容忍义务,私密信息和敏感信息因重要性更高,而受到更高层级的特别保护。张新宝教授曾提出,应当对个人信息实行分而治之的策略:一般信息强调利用,私密信息强调保护。[52] 私密信息(通常也是敏感信息)的泄露或非法处理将给自然人造成严重后果,故其损害成立的门槛理应更低。

比较法上一种颇具代表性的观点认为,私密信息的暴露(exposure)本身即是损害,无须再费力地

---

[50] 参见河北省石家庄市中级人民法院(2019)冀 01 民终 10531 号民事判决书。

[51] See Terry Wong, *Characterizing the Harms of Compromised Genetic Information for Article III Standing in Data Breach Litigation,* 53 Columbia Journal of Law and Social Problems 461 (2020).

[52] 参见张新宝:《从隐私到个人信息:利益再衡量的理论与制度安排》,载《中国法学》2015 年第 3 期。

证明其他损害。[53] 笔者对此深表赞同。私密信息的特质就在于“不愿为人知晓”的隐私属性，而加害行为使这种本来的私密状态丧失，必然使信息主体的尊严受损，其损害的确定性是明显的。试想个人的身份证号码、银行卡号码及密码被泄露，必然引发诈骗或身份窃取的疑虑，即使真实的诈骗或银行卡盗刷尚未发生，仅仅是信息失密及其所引发的风险本身，亦有高度的可能成立损害。相比之下，如果只是个人姓名、网上浏览记录、购买记录等一般个人信息泄露，则往往难以仅凭泄露本身认定风险损害成立。在不少案件中，法官都将个人信息的私密（敏感）性作为重要的考量因素。[54]

私密信息损害的宽松解释在立法上也不乏依据。《民法典》第 1033 条规定：“除法律另有规定或者权利人明确同意外，任何组织或者个人不得实施下列行为：……（五）处理他人的私密信息……”据此，只要无法律特别规定或未经权利人同意，处理他人私密信息本身即构成侵权，是否造成其他实际的损害后果在所不问。已经废止的我国《侵权责任法》第 62 条曾规定：“医疗机构及其医务人员应当对患者的隐私保密。泄露患者隐私或者未经患者同意公开其病历资料，造成患者损害的，应当承担侵权责任。”《民法典》第 1226 条规定：“医疗机构及其医务人员应当对患者的隐私和个人信息保密。泄露患者的隐私和个人信息，或者未经患者同意公开其病历资料的，应当承担侵权责任。”经对比可以发现，《民法典》第 1226 条删除了前者规定的“造成患者损害的”要件。在解释论上，这一修改并非意味着侵权的成立不需要损害，而是泄密本身即构成损害，无需其他危害后果。在这里，损害扩张的思想体现得尤为明显。另外，根据《个人信息保护法》第 28 条，敏感个人信息的处理以禁止为原则，以许可为例外，除非具有特定的目的和充分的必要性，否则处理敏感个人信息本身即构成损害。

侵害敏感个人信息造成的风险更容易成立损害，对此不乏案例支撑。在著名的 Rosenbach v. Six Flags Entertainment Corporation 案中，[55]原告因被告游乐园未经同意对其未成年儿子进行指纹识别而起诉。根据《伊利诺伊州生物识别信息隐私法》（Illinois’ Biometric Information Privacy Act，BIPA），伊利诺伊州最高法院认为，鉴于生物识别信息的高度敏感性，被告单纯违反法律的行为本身即足以构成损害而得诉请赔偿。在另一起被全球瞩目的案件中，Facebook 公司擅自对用户上传的照片进行了人脸识别，引发规模浩大的集体诉讼。[56] 2021 年 1 月，联邦法院正式批准了 Facebook 与原告达成的和解协议，Facebook 同意向伊利诺伊州约 160 万名原告每人支付 338 美元赔偿，合计 6.5 亿美元（约 42 亿人民币）。在这些案件中，原告方看起来都并没有遭受什么现实损害，但仍旧索赔成功。这表明，尽管风险性损害要获得普遍认可尚步履维艰，但起码在生物识别信息等特殊个人信息领域取得了局部胜利。由此推之，笔者认为，我国若要承认风险性损害，可率先从敏感个人信息入手，针对一般个人信息的风险暂不宜认可其成立损害，这样有利于平衡个人保护与数据利用的关系。

2.信息处理的方式和目的

个人信息以何种方式被非法处理，对于损害的判断非常重要。在数据泄露类型的案件中，身份窃用的风险是主要的担忧。最终真实的信息误用是否会发生，与未知的加害行为人获取数据的目的息息相关。在找到实际的加害人并查实其获取数据的目的之前，该目的只能通过间接的方式推知。

在有形的财产失窃（例如存有客户信息的电脑、手机、存储磁盘丢失）导致信息风险中，加害行为直接针对的对象是有形的财产而非信息，然而偷窃者实施该行为的目的究竟是获得这些财产，还是窃

[53] See Maxwell E. Loos, *Exposure as Distortion: Deciphering Substantial Injury for FTC Data Security Actions,* 87 George Washington Law Review Arguendo 42 (2019).

[54] See AFGE *v.* OPM (In re United States OPM Data sec. Breach Litig), 928 F. 3d 42 (D.C. Cir. 2019)；Remijas v. Neiman Marcus Grp., 794 F.3d 688, 693 (7th Cir. 2015).

[55] See Rosenbach *v.* Six Flags Entertainment Corporation., 2017 IL App. 2d 170317 (2017), rev'd, 129 N.E.3d 1197 (Ill. 2019)

[56] See Jessica Robles, *Patel v. Facebook, Inc.: The Collection, Storage, and Use of Biometric Data as a Concrete Injury under BIPA,* 50 Golden Gate University Law Review 61（2020）.

取其中的个人信息并冒用个人身份信息实施诈骗，尚难从该行为本身进行判断。存在风险的个人信息的命运有各种可能性，其中也包括被用于诈骗或身份窃取，但这只是众多可能性之一，推测的色彩较为强烈。在这样的场景下，将未来的风险认定为损害的难度较大。Beck v. McDonald 案的情况就是如此，对于丢失的电脑里存储的个人信息将被如何处置，法院拒绝猜测，故不认可损害的成立。[57]

在泛网络化时代，更多的数据泄露事件是在无形的网络空间发生的。信息泄露最典型的场景就是黑客攻击，未知的第三方通过技术手段非法侵入存有海量个人信息的数据库。与前述有形财产失窃的情形不同，黑客攻击直接瞄准的对象就是数据本身。在这种情况下，通常可以对个人信息被误用的风险作出肯定性推断。当然，即使是在该场景下也存在多种可能性，或许黑客攻击数据库的目的并不在于日后使用其中的个人信息。虽然黑客攻击与个人信息误用之间并不存在必然联系，但是具有高度的盖然性联系，这种高度盖然性足以支撑损害的认定。在 Remijas v. Neiman Marcus Grp.案中，[58]全球著名的奢侈品百货尼曼公司的数据库被黑客攻击，其中存储的大量消费者个人信息被泄露，法院在分析中指出：黑客攻击的目的还能是什么别的呢，信息误用是迟早的事。在黑客攻击的特定场景下，实施攻击者主观上存在故意，攻击手段经过精心设计，有明确瞄准的攻击目标，在具备这些特征的情况下，肯定风险满足损害成立的确定性要求并不牵强。

3.信息误用的迹象

数据泄露发生后，随着时间的推移，个人信息误用的端倪会逐渐显现，其对于损害的认定具有佐证意义。从近些年世界范围内发生的若干重大数据泄露事件来看，泄露涉及的受害者人数众多是一个突出特征。从诉讼程式来看，数据泄露常常引发集体诉讼，其中部分受害者已遭遇身份窃取或欺诈，这表明对未来风险的担忧并非空穴来风。对于那些在同一事件中个人信息泄露但尚未遭受现实欺诈的信息主体而言，这些已发生在他人身上的欺诈和身份窃取是有利的证据，表明自己在未来也有受到类似损害的风险。以航空信息为例，乘客姓名、电话、航班信息的泄露常常引发诈骗，此类事件并不罕见。在庞理鹏与北京趣拿信息技术有限公司等隐私权纠纷案中，[59]原告庞理鹏收到航班信息取消的诈骗短信，法院在分析推理中提出，被告趣拿公司和东航被媒体多次质疑存在泄露乘客隐私引发诈骗风险的情况，将此作为重要的考量因素。实践中，航班信息的诈骗日益高发，使信息主体对于个人信息泄露风险的担忧看起来有理有据。上述案件中，对庞理鹏之外的其他被泄露身份及航程信息但尚未遭受诈骗的消费者而言，其风险切实性可从庞理鹏身上得到印证。相反，如果随着时间的经过没有发生泄露的信息被非法使用的迹象，这对于损害的认定起到消减作用。在前述 Beck v. McDonald 案中，到诉讼进行时存储个人信息的电脑丢失已三年多，其间未发生任何欺诈或身份窃用的事件，也没有其他信息误用的迹象，这成为判决的重要考量因素。

认定个人信息损害要考虑的因素众多，上述列举不能穷尽一切。裁判者应根据个案中的具体场景，将各种因素结合，综合考量，以判断信息主体所遭受的不利益是否满足确定性要求而构成损害。

五、结　论

在大数据时代向纵深发展的背景下，对个人信息的侵害问题日益突出。在以侵权法为路径对信息主体提供保护时，损害要件不易证明成为拦路虎。侵害个人信息造成的不利后果常常表现为在未来遭受侵害的风险，与损害的“确定性”标准发生抵触。如果信息泄露后，要等到身份窃取和诈骗等损

[57] See Brandon Ferrick, *No Harm, No Foul: The Fourth Circuit Struggles with the Injury-in-Fact Requirement to Article III Standing in Data Breach Class Actions*, 59 Boston College Law Review 462 (2018).

[58] See Remijas*v.* Neiman Marcus Grp., 794 F.3d 688, 693 (7th Cir. 2015).

[59] 参见北京市第一中级人民法院(2017)京 01 民终 509 号二审民事判决书。

害已现实发生,受侵害人才能主张侵权损害赔偿,则有违公平正义。要扫清挡在个人信息保护道路上的障碍,必须对传统的损害概念及其认定标准加以反思,承认风险在一定条件下可成立损害。实现风险损害化的法律进路不是推倒重来式的法律变革,只需通过解释论的方法对损害认定的标准予以重新解读,根据大数据时代的需要和个人信息侵权的特点进行灵活开放的解释。损害的确定性不能被僵化地解释为已发生,个人信息风险客观上也存在符合确定性标准之可能。个人信息暴露带来的风险升高、预防风险的成本支出和风险引发的焦虑皆可成立损害。当然,不是所有的风险都自动成立损害,必须将那些过于遥远的风险排除出去,而只认可那些实质性的风险。风险是否具备实质性的认定应当放在个案的场景下进行,由裁判者综合考量个人信息的类型、信息处理的方式目的和信息误用的迹象等因素进行判断。损害概念的扩张和革新,将是侵权法因应大数据时代挑战的一次升级。

(责任编辑:陈历幸)

Risks as the Harm: Redefining "Damage" of Tort in Big Data Era

TIAN Ye

Abstract: It is difficult to recognize the "damage" under the framework of protecting personal information through the tort law. The damage to personal information is intangible, latent, obscure and difficult to evaluate, so it is doubtful whether it satisfies the "certainty" test. In order to meet the needs of big data era, the concept of damage in traditional tort law should be reconsidered, and damage of risks should be recognized. The certainty in damage does not mean that the damage has already occurred and material risks in the future can also meet the requirement of certainty test. The increased risk caused by information exposure, the expense for risk prevention and the anxiety caused by the risks are the manifestations of the interest differences caused by infringement and thus can constitute damage. The recognition of damage of risks to personal information should be made by taking the contextualization as the basic approach and decision should be made by comprehensively considering facts such as the type of information, the purpose and method of information processing, signs of information misuse in individual cases.

Keywords: Personal Information; Tort; Damage; Certainty; Risk