

大数据时代个人信息的司法保护

□万发文 胡贤君

大数据，是指伴随着可作为处理对象的数据外延不断扩大，依靠新的数据收集、传输和处理模式的一种新型数据挖掘和应用模式。大数据对隐私权的威胁，无论在技术层面还是现有的社会治理机制上，都无法根本防范。在我国的司法实践当中，基本达成了这样一个共识，即个人信息是一种隐私利益。因此，针对公民个人信息保护范围的认定，基本上是沿袭隐私权所遵循的隐私利益主观化认定的立场，只有对符合隐私利益的公民个人信息，才给予民法上的保护。法院经常采取隐私权的保护方法为个人信息的权利人提供救济，然而当前法律框架下的责任范围并不足以完成保护隐私权的使命，侵权法作为一种平衡各种利益的制度设置，理应可以做出适当调整以发挥更多的作用，以提高救济的可能性。

一、模糊的边界:个人信息权与隐私权的立法困境

个人信息是指与特定个体相关的并反映个体特性的具有可辨认性的符号系统,包含个人身份、工作、家庭、健康等各方面的资讯。在个人信息保护立法工作已经完成的国家中,由于法律体系的不同以及法律理念的差异,个人信息侵权保护的方式大致分为两种:一是采取统一的个人信息保护法典的直接保护方式。二是包含在隐私权的权利范围内的间接保护方式。在我国立法上,个人信息权尚未获得法律的确明确承认,直到2010年7月开始实施的《侵权责任法》,才确立了隐私权作为一项独立的人格权的地位,与肖像权、名誉权、姓名权等并列,遗憾的是在制定法中并未涉及隐私权的具体内容,对其内涵和外延的认识还要归于学理和判例的讨论。2012年全国人大常委会出台《关于加强网络信息保护的決定》规定了个人电子信息保护的相关内容,但未能对个人信息权与隐私权作出明确区分。2017年《民法总则》第111条首次对个人信息的保护予以明文规定,但对个人信息的内涵与外延均未明确界定。个案中系争的利益是否属于受法律所保护的隐私利益,往往成为隐私权诉讼中的焦点。

二、乏力的救济：我国对个人 信息隐私权保护的司法 实践检视

我国的司法实践中，法院往往采取隐私权的保护方式为个人信息权利人提供救济。在现有的对个人信息采取隐私权保护的框架下，法院在审判实践中无一例外地采取了一般侵权的归责模式。按照我国通常的侵权行为构成要件理论，要认定隐私权侵权责任，需采取过错归责原则，即必须存在具备侵犯隐私权的行为并造成损害事实，损害行为和损害事实之间有因果关系，而且侵权人还必须存在主观过错。

为考察我国《侵权责任法》实施以来涉个人信息的隐私权纠纷案件的司法实践状况,笔者通过中国裁判文书网收集了自2010年至2016年全国隐私权纠纷案件一审民事判决书共计122份,其中涉及个人信息的纠纷的判决仅为15件,这些案件的发生相对集中于经济较发达地区,如北京、江苏、上海、浙江等。《关于加强网络信息保护的决定》第1条规定:国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息。其中既规定了个人信息,也规定了个人隐私,但并未提出两者区分的标准。涉个人信息的隐私权纠纷案件数量虽不多,但笔者查阅这些判决书发现,原告的诉请得到法院全部或者支持的仅有4件,其余均被驳回。被驳回的原因以及法院裁判的理由:难以认定侵权主体的主观过错;难以证明侵权行为存在;难以证明侵权行为与损害结果的直接因果关系;难以量化损害结果。

三、削足适履：传统隐私权保护模式对个人信息保护不足之原因分析

我国现有制度架构并没有基于个人信息侵权的特点为其设计特殊的举证规则,对于个人信息的保护只能止步于防御他人对信息隐私的侵害,无法拓展到对于个人信息的积极控制和维护。削个人信息之“足”以适狭义隐私之“履”,这决定了隐私权保护模式在面对现实中个人信息保护需求的乏力。

（一）技术层面：大数据对隐私的天然侵

数据收集技术的发展增加了隐私侵权的可能性，数据分析、挖掘是一种在大数据库中发现或推定未知事实的模式，它不依赖于因果关系而依赖相关性进行预测和推断，以人们看不见的方式进行，即使当事人怀疑被侵犯，也缺乏必要的证据证明侵权者的责任和赔偿的要求，此外，隐私侵权的后果也因而发生变异，网络空间的可搜索性和永久存续性使人们冀望于随时间而淡忘的期待落空，导致精神损害、名誉损害的长期化，从而加重损害的结果。

(二) 制度层面：个人信息范围和种类

不确定

隐私与个人信息并不具有完全对应的关系,对公民隐私利益的界定,司法实践倾向于采取主观化的认定标准,强调隐私是一种“权利人不愿对外公开”或“本人不愿意为他人所知晓”的事项,是个人生活安宁和生活秘密不受他人披露和干涉的状态;而个人信息的本质,司法实践普遍认为个人信息通常包含权利主体的联络方式、工作单位、婚姻状态、财产收入、指纹记录、血型 and 家族病史等与个人密切关联的各类具体信息。我国《侵权责任法》明确规定了隐私权作为一种法定的具体人格权利,《民法总则》也只是规定个人信息受法律保护,而未明确法定赋予个人信息作为一种民事权利存在,亦未对其内涵与外延作出界定。该情况下,司法实践中并没有形成一致的意见,很难给予完整的保护。

(三) 举证责任：当事人地位不平衡

大规模信息处理一方往往占据技术和资源方面的优势地位,使得被侵权人一方的举证变得十分困难,司法判决层面对个人信息的保护只能止步于对个人隐私信息公开范围和对象的

四、路径探索：要件审判方法下个人信息隐私权保护的技术分析

要件审判方法，是以权利请求为出发点、以实体法律规范构成要件分析为基本手段的审判方法，围绕当事人的权利请求基础，将审判活动划分为环环相扣的步骤。

(一) 请求权基础规范分析

基础规范，也称为权利请求基础，一般是指一方当事人向另一方当事人主张权利请求的实体法律规范。《侵权责任法》顺应了隐私权发展的趋势，把隐私权作为一项独立的人格权列入。此外，《宪法》从一般人格权层面上间接地保护了隐私权。但具体到个人信息问题，虽《个人信息保护法》早已列入立法计划，但并未制定公布。《民法总则》规定自然人的个人信息受法律保护，可以作为请求权基础规范，但对于何为个人信息，仍无明确法律界定。从价值取向看，个人信息隐私的价值仍可归结于三个方面：其一，人格尊严与自主决定；其二，私密空间内的情感释放与自我评估；其三，社会信任与契约精神。目前可通过隐私权的方法保护个人信息，对隐私的解释上，至少如下层次的个人信息均应纳入隐私保护之内涵：第一，涉及私生活领域的个人信息，如个人的社会关系秘密，如亲戚关系、恋人关系以及与他人不正当关系等；个人之财产情况，如个人的合法储蓄和其他经济收入等。第二，可以指向某一具体个人的信息，如个人之家庭住址、工作单位、职业职务等。对这些信息的披露和滥用将使个人遭受非其所意愿滋扰，从而影响正常的安宁生活。

（二）抗辩权基础分析

由于侵犯个人信息隐私的请求权基础仍属于侵权损害赔偿请求权,因此关于一般侵权行为责任的免责事由均可适用,如受害人同意等。除此之外,在信息时代环境下,也应考量个人信息特殊性。个人信息的保护需求必然与他人利益、公共利益、国家利益发生冲突,也就面临需要协调平衡与受到合理限制的问题。隐私的边界本来就存在着不确定性,对隐私的保护在于一个合理人对隐私的期待。因此,对于个人信息的保护必须符合诚实信用原则和公序良俗原则,权利主体不能滥用权利,也不能妨碍他人利益的正当

享有和他人权利的正当行使。司法审判中可以采取两种审判分析方法。一是利益衡量的方法，基本的思路是：首先确定对个人信息的具体侵害强度，其次衡量与其相竞争的另一法益的重要性，最后要判定满足后一法益是否重要到可以限制个人信息的保护。按照德国学者阿列克西提出的“三合标尺”模型，对权利的具体侵害强度可以三个层级来涵括：轻微、中度、严重。轻微损害的法益应让步于中度和严重损害的法益。因此，在个案中应对侵犯个人信息是否基于对其他更为重要的法益进行权衡。如住酒店被盗窃而调取相关监控录像；错误转账至他人账户而调取他人账户信息等。虽侵犯他人信息，但相较于财产可能遭受的直接损失显属轻微。二是诚实信用原则的检验，“对权利行使的一个最重要的限制是遵守诚实与信用原则，……，它适用于所有的合法的特定的当事人之间的应遵守的关系，以及在此范围内形成的义务关系并对权利行使做了限制。”^[1]基于该原则，权利人在行使权利时不得违背设置该项权利的目的。如银行将其掌握的储户信息提供给其下属的保险公司进行推销保险，虽其系征得储户同意取得信息，但其使用明显超出应有范围。

(三) 要件归入与作出裁判

个人信息隐私侵权案件审理要件的归入，并非简单的将各个要件事实与法律规范进行比对归入，而应当结合个人信息隐私侵权案件的特点，综合考虑公众的价值取向。

行为之表现

法律、法规保护隐私权益的目的在于保护权利主体对他人在何种程度上可以介入自己私生活的控制权,以及对自己是否向他人公开隐私和公开的范围决定权。因此,个人信息的私密性是其重要内容,只要有未经许可向第三人披露个人信息的事实存在即可构成侵害,就侵害的成立而言,无须考虑第三人究竟给原告带来的是利益还是损害,也不以当事人的名誉贬损或者社会评价降低为必要,即私人信息为当事人所不欲的第三人所知本身即为损害。至于第三人知悉的范围以及名誉贬损与否,可以作为判断精神损害是否严重的考虑因素。具体包括如下形态:非法收集、存储个人信息资料、

支配,对于是否能够保护一般的个人信息,赋予信息主体查阅的权利,要求信息控制者承担报告的义务,或是举证责任的变更以及在具体责任承担方式上都限于隐私权本身的制度架构,即便通过法律解释也很难有所突破。

（四）事实认定：司法调查权与事实查明的现实需求不匹配

大数据时代，大数据的掌控愈来愈呈现出集中化的趋势。大数据库的持有者对其掌控的大数据视若珍宝，同时在本身涉及诉讼并有可能被追究民事责任后，往往设置种种障碍阻却事实的查明。《民事诉讼法》第 67 条规定：人民法院有权向单位和个人调查取证，有关单位和个人不得拒绝。法院具有一定的司法调查权。但《宪法》第 40 条规定：中华人民共和国公民的通信自由和通信秘密受法律的保护。除因国家安全或者追查刑事犯罪的需要，由公安机关或者检察机关依照法律规定的程序对通信进行检查外，任何组织或者个人不得以任何理由侵犯公民的通信自由和通信秘密。实践中，以此为由拒绝法院依职权调查者亦常发生。

个人信息数据二次开发利用等。

过错之推定

过错推定原则，是指在法律有特别规定的情况下，基于损害事实的客观存在推定加害人为有过错，并因此承担赔偿责任。在现有的侵权责任法框架中，为改变诉讼双方能力的不足，一些特殊类型侵权已经广泛使用了过错推定原则。对于个人信息的隐私侵权来说，受害人发现信息收集、加工、利用过程中的过错非常困难，加害人极易作出无过错抗辩以规避责任，采取过错推定原则，不仅存在诉讼便利和经济价值，还可以促进信息收集者强化安全意识，营造一个良好的网络环境。

损害结果之识别

在基于损害——赔偿模式的现代侵权法律制度中,损害结果无疑是第一要素。大数据背景下个人信息隐私权的损害结果不应局限于精神损害,其范围还应扩张到以下方面:(1)无形损害。比如,社会评价降低的范围和程度很难进行量化分析,与之相应的是索赔金额的合理性,经济损失的数额难以量化,对此可以采用推定损害的方法,即根据侵权内容的点击率、转载率来间接地推定损害结果的严重程度;(2)期待利益的损害。数据泄露导致的冒用身份、诈骗等往往给受害人造成严重的损失。虽然冒用身份及诈骗行为,往往因为直接行为已经构成其他侵权行为甚至犯罪,可以不经过程侵权来救济,但对于网络营运商单纯泄露信息的行为,也可以令其单独或者连带负隐私侵权的责任。因果关系之认定相对于传统隐私侵权,大数据背景下的信息获取方式更具隐蔽性,很多侵权事件都是由大量并且分布广泛的主体参与的,对侵害行为与损害后果之间因果关系的判断要更加复杂。对此,我们可以根据原因力理论,来解决这一困境,原因力是指违法行为或其他因素对于损害结果发生或扩大所发挥的作用力,因果关系是侵权责任成立的不可或缺的要件,原因力则是因果关系是否成立的一个重要判断因素。在引起同一损害后果的多种原因中,通过每个原因行为对于该损害结果引发或扩大所产生的影响,来衡量侵权行为中的各个原因力,判断这些行为是否具有因果关系。作者单位:浦东新区人民法院川沙法庭