

# 个人信息泄露因果关系的证明责任

——评庞某某与东航、趣拿公司人格权纠纷案

刘海安\*

## 目次

一、案件事实与法院裁判要点	易纵容泄露隐私信息的行为
(一) 案件事实	四、信息控制者因果关系证明责任及其价值
(二) 法院裁判要点	(一) 信息控制者的因果关系证明责任
二、本案的理论争点：因果关系的证明责任	(二) 信息控制者因果关系证明责任的
(一) 权利人证明权利因果关系的进路	价值
(二) 信息控制者证明因果关系的进路	五、信息控制者因果关系证明责任的适用
三、权利人因果关系证明责任对信息保护的	条件
消极影响	(一) 适用前提：原告的基础证明责任
(一) 权利人的因果关系证明责任与其	(二) 信息控制者因果关系证明责任的
证明能力不匹配	证明标准
(二) 权利人的因果关系证明责任更容	六、结语

**摘要** 通过将《民事诉讼法司法解释》与《侵权责任法》结合考察可以确定,在个人信息泄露的案件中,信息权人对信息泄露行为与损害间的因果关系这一要件事实负有证明责任。这种权利人的因果关系证明责任与其证明能力的不匹配,更容易纵容泄露隐私信息的行为。而信息控制者负因果关系证明责任更为合理。

**关键词** 个人信息 信息泄露 因果关系 证明责任

《最高人民法院关于适用〈中华人民共和国民事诉讼法〉的解释》(下文简称《民事诉讼法司法解释》)第 91 条在证明责任的分配上吸收了罗森贝克的规范说,规定主张权利受到妨害的当事人应当对权利受到妨害的基本事实承担举证证明责任。在个人信息泄露案件中,信息权人寻求救济的请求权基础主要是《侵权责任法》第 6 条关于过程侵权的一般规定。据此,信息权人对信息控制者的加害行为,加害行为与损害间具有因果关系等要件事实负有证明责任。《最高人民法院关于民事诉讼证据的若干规定》(下文简称《证据规定》)第 7 条赋予了法院根据具体情况分配证明责任

\* 中国民航大学法学院副教授、法学博士。

的权力。该条规定：“在法律没有具体规定，依本规定及其他司法解释无法确定举证责任承担时，人民法院可以根据公平原则和诚实信用原则，综合当事人证明能力等因素确定举证责任的承担。”该条适用的前提是依照现有规定无法确定证明责任的承担。而结合《民事诉讼法司法解释》和《侵权责任法》的规定，似乎能够确定个人信息侵权案件中因果关系等要件事实的证明责任在作为原告的信息权人处。然而，权利人的因果关系证明责任在个人信息泄露案件中具有现实障碍和消极影响。本文便是在指出这一问题的基础上，为信息控制者因果关系的证明责任提供理论支撑。

## 一、案件事实与法院裁判要点<sup>〔1〕</sup>

### （一）案件事实

2014年10月11日，原告庞某某委托鲁某通过去哪儿网平台订购了2014年10月14日MU5492泸州至北京的东航机票1张，所选机票代理商为星旅公司。去哪儿网订单详情页面显示该订单登记的乘机人信息包括原告庞某某姓名及身份证号，联系人信息、报销信息均为鲁某及其尾号1850的手机号。同日，趣拿公司向鲁某尾号1850的手机发送了出票通知短信。10月13日，庞某某尾号9949的手机号收到号码为0085255160529的发件人发来短信：“……您预订2014年10月14日16:10起飞19:10抵达的MU5492次航班(泸州-北京首都)由于机械故障已取消……”上述号码来源不明，未向鲁某发送类似短信。鲁某知晓上述短信后拨打东航客服电话95530予以核实，客服人员确认该次航班正常，并提示庞某某收到的短信应属诈骗短信。关于诈骗短信为何发至庞某某本人，客服人员解释称通过该机票信息可查看到开头136、尾号949手机号码及开头189、尾号280手机号码，可能由订票点泄露了庞某某手机号码。庞某某起诉东航、趣拿公司和星旅公司，要求他们就其信息泄露承担责任。庞某某提出证据证明东航和趣拿公司掌握其手机号，各方认可其真实性。

### （二）法院裁判要点

一审法院认为，当事人对自己提出的主张，有责任提供证据。如果没有证据，或者提出的证据不足以证明当事人的事实主张的，由负有证明责任的当事人承担不利后果。趣拿公司和东航在本案机票订购时未获取庞某某号码，现无证据证明趣拿公司和东航将庞某某过往留存的手机号与本案机票信息匹配予以泄露，且趣拿公司和东航并非掌握庞某某个人信息的唯一介质，法院无法确认趣拿公司和东航存在泄露庞某某隐私信息的侵权行为，故庞某某的诉讼请求缺乏事实依据，法院驳回了其全部诉讼请求。

二审法院认为，本案中的关键是看庞某某提供的证据能否表明东航和趣拿公司存在泄露庞某某个人隐私信息的高度可能，以及东航和趣拿公司的反证能否推翻这种高度可能。现有证据显示东航和去哪儿网都留存有庞某某的手机号。同时，中航信作为给东航提供商务数据网络服务的第三方，也掌握着东航的相关数据。因此，从机票销售的整个环节看，庞某某自己、鲁某、趣拿公司、东航、中航信都是掌握庞某某姓名、手机号及涉案行程信息的主体。庞某某、鲁某泄露信息的可能性很低。而从收集证据的资金、技术等成本上看，作为普通人的庞某某根本不具备对东航、趣拿公司内部数据信息管理是否存在漏洞等情况进行举证证明的能力。因此，客观上，法律不能也不应要求庞某某确凿地证明必定是东航或趣拿公司泄露了其隐私信息。东航和趣拿公司以及中航信都有能力和条件将庞某某的姓名、手机号和行程信息匹配在一起。根据东航出具的说明，如需查询旅客航班信息，需提供订单号、旅客姓名、身份证号信息后才能逐个查询。而第三人即便已经获知庞某某姓名和手机号，也很难将庞某某的订单号、身份证号都掌握在手，从而很难查询到庞某某

〔1〕 北京市第一中级人民法院(2017)京01民终509号。

的航班信息。另外,2014年间,趣拿公司和东航都被媒体多次质疑存在泄露乘客隐私的情况。因此,东航、趣拿公司存在泄露庞某某隐私信息的高度可能。东航和趣拿公司并未举证证明本案中庞某某的信息泄露的确是归因于他人;也并未举证证明本案中庞某某的信息泄露可能是因为难以预料的黑客攻击;同时也未举证证明庞某某的信息泄露可能是其自身或鲁某所为。在这种情况下,东航、趣拿公司存在泄露庞某某隐私信息的高度可能很难被推翻。东航和趣拿公司在被媒体多次报道涉嫌泄露乘客隐私后,即应知晓其在信息安全管理方面存在漏洞,但并未证明采取了专门的、有针对性的有效措施。可以认定趣拿公司和东航具有过错,应承担侵权责任。

该案后经过再审,再审法院完全认可二审判决。

## 二、本案的理论争点:因果关系的证明责任

隐私信息的泄露是隐私侵权行为的常见方式,然而被告实施了信息泄露行为与泄露行为与损害间具有因果关系,一直是受害人在民事诉讼中面临的两大难关。本案两审法院对此有不同的认识。本文将关注的焦点主要放在因果关系的证明责任上。

### (一) 权利人证明权利因果关系的进路

《民事诉讼法司法解释》第91条规定:“人民法院应当依照下列原则确定举证证明责任的承担,但法律另有规定的除外:(一)主张法律关系存在的当事人,应当对产生该法律关系的基本事实承担举证证明责任;(二)主张法律关系变更、消灭或者权利受到妨害的当事人,应当对该法律关系变更、消灭或者权利受到妨害的基本事实承担举证证明责任。”如前,这一规定被认为在很大程度上吸收了德国学者罗森贝克的规范说,虽然也有些许差别。<sup>〔2〕</sup>根据这一规定,个人信息权人对权利受到妨害的基本事实应当承担证明责任。而权利妨害的基本事实依赖于实体法的规定。针对个人信息泄露的损害进行救济的请求权基础,主要是《侵权责任法》第6条的规定:“行为人因过错侵害他人民事权益,应当承担侵权责任。”据此,权利人要获得救济,必须满足如下要件:行为人的行为,民事权益的损害,行为与损害间的因果关系,行为人具有过错。规范说要求权利人证明权利妨碍的上述基本事实(即要件事实),因果关系自然在其列。

本案一审判决采用的就是这一进路。一审法院认为,原告(即受害人)无证据证明趣拿公司和东航将其身份及行程信息泄露,而且虽然趣拿公司和东航掌握原告的个人信息,但他们并非掌握该些信息的唯一介质,无法排除其他人泄露信息的可能。实践中处理这类隐私泄露案件时,法院采用这一进路的判决很常见。比如,在一起因电信诈骗受害的案件中,法院认为:“该案公安机关尚未侦破,因此无法查明诈骗犯罪人通过何种途径获得原告在被告网络平台购物所留的个人资料,虽然原告提供的证据中有证明被告网络平台漏洞的证据,但是诈骗犯罪人是否通过上述漏洞而获得原告的个人资料,尚不能确定,而上述个人资料也有可能通过被告之外的其他途径获得,被告并不是唯一可能泄露原告个人资料的途径。”<sup>〔3〕</sup>在另一起类似案件中,法院认为:“即使被告网络平台存在漏洞,但诈骗犯罪人是否通过上述漏洞而获得原告的个人信息,尚不能确定,而上述个人信息也有可能通过被告之外的其他途径获得,被告并不是唯一可能泄露原告个人信息的途径。”<sup>〔4〕</sup>这些案件都因原告(受害人)无法证明被告(网络平台)泄露个人信息致害而败诉。可见,这种权利人证明因果关系的规则在个人信息泄露案件中给受害人带来很大的诉讼压力。

〔2〕 参见任重:《罗森贝克证明责任论的再认识》,载《法律适用》2017年第15期,第20页。

〔3〕 南京市玄武区人民法院(2016)苏0102民初1123号判决书。

〔4〕 阳江市江城区人民法院(2016)粤1702民初1098号判决书。

## （二）信息控制者证明因果关系的进路

在个人信息泄露案件中，权利人证明权利因果关系的规则给原告带来了很大的困境。比如，在网络场合，原告终端设备中安装了多款软件，原告难以确定其信息的泄露是否是被告的行为造成的。再比如，被告经原告同意从原告处获得了可识别信息，但原告无法证明其相同的可识别信息的泄露和因此带来的烦扰是因被告的行为所导致的。由此，被告行为与损害间的因果关系常难证明。原告纵然证明被告实施了与原告信息有关的一定行为（比如经原告同意进行了信息披露），往往也无法证明该行为与损害间具有因果关系，二者之间可能介入了很多客观因素，包括第三人的行为（而该第三人又常难以找到）。二审法院采用了一种新的进路，本文将之称为信息控制者证明因果关系的进路。二审法院在确认被告实施了泄露隐私信息行为之后，要求被告证明其行为与损害间没有因果关系，比如证明本案中庞某某的信息泄露的确是归因于他人，或者本案中庞某某的信息泄露可能是因为难以预料的黑客攻击，或者庞某某的信息泄露可能是其自身或鲁某所为。如果信息控制者无法证明其行为与隐私损害间没有因果关系，法院便认定这一因果关系的存在。

## 三、权利人因果关系证明责任对信息保护的消极影响

### （一）权利人的因果关系证明责任与其证明能力不匹配

#### 1. 权利人的信息处理能力无法适应该证明责任的要求

证明能力首先是一种信息处理能力，尤其是信息的获取、控制、移转等方面的知识和技能。在个人信息泄露案件中，大多数案件中的受害人（即权利人）是消费者，他们在信息处理上面临很多困难，相比作为信息控制者的被告，证明能力较差。

我们先来看个人信息泄露案件中举证面临的困难。个人信息的扩散渠道的多元性致使难以准确确定加害人。个人信息的扩散渠道往往不是单一的，个人信息的网络侵权可能发生在个人信息的收集、处理、传递、利用以及管理等各个环节。在实践中，信息权人意识到个人信息权益遭受侵害时所知信息往往集中在滥用个人信息的环节，其对于个人信息的收集者、传递者、处理者、使用者和其他帮助侵权的行为人等则难以确定。“各类‘端口’犹如‘间谍’，无处不在，‘监控’如影随形。如果说传统语境下，一篇超越了隐私边界的新闻报道，或者是网络上不当报道或言论的截图，可以用作隐私受到侵犯的有力证据的话，在新语境下，主体很难判断是在哪个场景、借助哪个端口、通过怎样的聚合方式导致隐私被窃取，或者说看似一般的个人信息通过人工智能场域怎样的技术力量催化后变成了隐私信息。”〔5〕数据收集、处理、转移以及使用等多个环节中，每个环节都可能发生数据不当泄露，信息权人很可能无法确定行为人的范围，即使确定范围后也无法证明其中哪一个是真正的行为人，即使证实是特定行为人后也无法证明后者的何种行为正是数据侵害结果发生的原因。〔6〕毕竟，受害人不熟悉信息控制者的业务流程，包括信息控制者与其合作伙伴的具体关系，也不熟悉其隐私信息的处理流程，往往也不太懂信息处理的相关技术，比如网络技术。受害人虽然认定信息控制者具有很高的泄漏可能性，但对信息流转的具体状态的了解不如信息控制者。让受害人确切地证明信息处理者泄露了其隐私信息以及损害与信息处理者间的因果关系，几乎是不可能完成的任务，这无异于否定了向信息泄露者追究责任的可能性。总之，证明信息泄

〔5〕 许天颖：《人工智能时代的隐私困境与救济路径》，载《西南民族大学学报（人文社会科学版）》2018年第6期，第168页。

〔6〕 Ignacio N. Cofone, “The Dynamic Effect of Information Privacy Law”, 18 Minn. J. L. Sci. & Tech. 552 (2017).

漏渠道的唯一性成为原告维权的最大难题。消费者在技术、人力等方面资源有限,往往无力承担上述证明责任,这也是目前侵权案件多发而维权不足的最主要原因。<sup>〔7〕</sup>

认识到受害人在举证方面的信息处理能力难以适应权利人的因果关系证明责任,并不能简单得出受害人作为原告不宜承担证明责任的结论。而通过对信息权人(受害人)与信息控制者的比较,才能够让人确信这一结论的妥当性。在绝大多数情形,信息权人在信息处理能力上都不如信息控制者。信息收集者和处理者一般是公司和企业,他们通常比个人信息权人拥有更多的资本和实力。而由于侵犯个人信息行为已经进入网络时代,对于个人信息的侵犯较之以往更具有隐蔽性、严重破坏性、无地域性等特征。这也导致了受害人证明能力上的欠缺。二者之间无论在证明能力方面,还是在诉讼活动的进展方面,都存在很大的差距。<sup>〔8〕</sup>诚如学者所指出的,个体之间的个人信息侵权行为只占少数,绝大多数情形下,都是收集、储存了大量个人信息的信息业者乃至于政府对于个人的侵权,前者在技术、资源甚至于正当性方面都具有显著的优势。<sup>〔9〕</sup>受害人证明能力的局限,事实上导致了绝大多数追究信息泄露者责任的案件都以原告败诉收场。

## 2. 受害人的信息成本无法适应该证明责任的要求

信息的处理能力受信息成本的制约,同时也影响着信息成本的大小。我们先来看信息成本对信息处理行为与能力的制约。世界上没有不需要成本的行为。信息权人获取、移转信息的行为,依赖于包括金钱、精力等在内的成本。成本的有限性决定了主体获取、移转信息的方式与效果。有的信息处理行为需要的成本高,主体如果拥有的成本有限甚至不足以支付某类信息处理行为,只能放弃该类信息处理行为,转而寻求其他方式。不同类型的信息处理行为效果很可能是不同的,从而在客观上体现为不同的信息处理能力。我们再来看信息处理能力对信息成本大小的影响。信息处理能力依赖于信息获取、移转的客观条件,要具备相应的信息处理能力,主体必须想办法迎合信息获取、移转的客观条件。比如,受害人要举证证明信息泄露的主体,依赖于对信息控制环节及每个环节对信息保护程度、披露程度等内容的掌握。如果主体不具备相应的信息处理能力,却被强制要求迎合信息获取、移转的客观条件,会给主体增加很高的新的成本,而这在很多情况下依然是难以达到相应的信息处理能力的。比如,在个人信息泄露案件中,受害人在客观上是不掌握个人信息如何泄露的充分信息的,如果法律将证明责任加在受害人身上,受害人必须想办法掌握其本来就难以掌握的信息,这一点在现实中很难实现。

就现实情况而言,信息控制者比较容易掌握信息获取、流转的现实情况,信息控制者证明这些现实情况不会付出太多的成本,至少花费的成本往往比受害人少得多。从社会效益的角度讲,对于实现同一目的而言,让花费成本较多的信息权人(即受害人)承担信息泄露因果关系的证明责任,无异于社会成本的浪费。

### (二) 权利人的因果关系证明责任更容易纵容泄露隐私信息的行为

制度规则对主体是有激励作用的。权利人证明因果关系的证明责任进路会给主体带来不好的激励。一方面,权利人的因果关系证明责任事实上封锁了权利人向信息泄漏者寻求救济的法律途径,使极有可能泄露信息的被告轻易地逍遥法外,会形成泄漏他人信息的违法成本极低、而收益可观的局

〔7〕 参见赵淑珺:《我国消费者个人信息保护实证研究——以典型司法判例为视角》,载《山东审判》2016年第2期,第70页。

〔8〕 参见尹伟民:《侵犯个人信息行为的民事责任承担》,载《中国海洋大学学报(社会科学版)》2011年第1期,第91~92页。

〔9〕 参见廖宇羿:《我国个人信息保护范围界定——兼论个人信息与个人隐私的区分》,载《社会科学研究》2016年第2期,第15页。

面。这给信息控制者泄漏他人隐私信息牟利形成了不好的激励。在一些案件中，原告就算找到了不当获得信息者也不一定能够证明信息泄露者的身份，因为不当获得信息者可能会基于利害关系考量闭口不提获得信息的渠道。<sup>〔10〕</sup>另一方面，这一证明责任进路客观上会打击信息权人保护其隐私的积极性。举证方面的劣势使信息权人负担很高的举证成本，同时面临着败诉的巨大风险。这一现实会吓退绝大多数本想尝试保护其隐私的受害人。这更进一步纵容了泄露隐私信息的行为。

## 四、信息控制者因果关系证明责任及其价值

### （一）信息控制者的因果关系证明责任

针对受害人在因果关系证明方面的困难，有学者认为，有些损害与信息泄露行为只存在条件关系，建议在认定因果关系时采用条件说，<sup>〔11〕</sup>但没有详细展开。所谓只存在条件关系，或许指的是原告（受害人）基本只能证明信息泄露行为是损害的产生条件，而无法证明泄露行为在导致损害上的充分性。条件说只要求受害人证明被告行为是损害产生的条件即可认定因果关系。这一做法试图缓和原告在因果关系证明上的困难，然而在根基上是站不住的。一方面，条件说要解决的问题只是认定因果关系中的第一步，该说只是认定事实因果关系存在的标准，而不是认定法律上因果关系的标准。而责任成立以事实上因果关系和法律上因果关系同时成立为必要。仅仅认定事实因果关系是不够的。另一方面，以条件说作为认定事实因果关系的标准既过于简单，又无法完全排除受害人在因果关系认定上的困难。就标准过简而言，条件说即“but for”标准只能认定大多数事实上因果关系，但“恰恰无法解决多因一果问题，这才有聚合因果关系、共同因果关系或择一因果关系等多数因果关系理论的出现”。<sup>〔12〕</sup>这一标准也无法完全排除因果关系认定上的困难。该标准的适用前提是证明被告存在信息泄露行为，即证明被告与信息泄露具有关联性，倘若只能证明存在信息泄露，但无法证明是谁泄露了信息，依然无法将被告与责任联系起来，条件说在这个问题上无能为力。

解决受害人在因果关系证明上的困难，不是单纯的证明标准所能解决的，更实际的做法还是宜从证明责任分配的角度出发。

### （二）信息控制者因果关系证明责任的价值

法院确定信息控制者因果关系证明责任没有给信息控制者带来过重的成本负担，而且在积极层面上也具有较强的合理性。

首先，信息控制者具有更强的能力和需要更低的成本证明其行为与信息损害无因果关系。网络安全破坏往往具有匿名性，几乎没有侵权人在实施侵权行为时会采用实名或留下真实的身份信息，因此普通用户根本无法追踪侵权人，只有网络服务提供者可以根据访问的IP地址等线索对侵权人予以追踪。<sup>〔13〕</sup>相比受害人，信息控制者具有更强的信息处理能力和信息状态的证明能力。信息控制者具有较强的获取、使用、移转信息的能力，往往是其从受害人处获得信息的基础。尤其在计算机和网络方面，信息控制者的技术和管理能力往往比受害人强很多。信息控制者对信息状态最为清楚，因而证明能力也最强。由能力匹配者承担证明责任，符合一般的公平观念。而且信息控制者在这一问题上的证明能力更强，相应的举证成本更低。举证成本是由信息控制者较强的

〔10〕 参见彬州市北湖区人民法院(2014)郴北民二初字第947号判决书。

〔11〕 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，第147页。

〔12〕 叶名怡：《个人信息的侵权法保护》，载《法学研究》2018年第4期，第96页。

〔13〕 参见王思源：《电商平台系统安全漏洞的法律责任分析——季海红诉苏宁易购案评析》，载《法律适用》2018年第12期，第74页。

信息处理能力和证明能力决定的。信息控制者知道有哪些可能引发信息泄露的环节,能够举证证明针对这些环节采取了对应的措施,从而达到否定信息泄露的目的。信息获取成本较低,因而证明成本就低,其相对于受害人的证明成本而言更低。“关于人际关系的权利义务,法律希望能降低成本,避免以高成本的方式,界定彼此的权利义务。”<sup>〔14〕</sup>使正确解决大多数案件看上去可能的原因“只不过是通常掌握真理的一方取得说服证据的成本更低”。<sup>〔15〕</sup>从社会效益的角度讲,信息泄露与否的证明由成本最低者承担最为恰当。这样既能实现证明的目的,又能够使社会效益最大化。何况,由信息控制者承担证明责任,也不会给其造成过重的负担。

其次,信息控制者的因果关系证明责任有利于促进降低信息泄露事件的概率,更好地保护隐私。隐私信息相比信息控制者的商业营利更值得保护。隐私信息与公开个人信息不同,具有浓厚的人格性,信息控制者经过隐私权人同意方有权披露隐私信息。确认信息控制者的因果关系证明责任能够更好地保护隐私。一方面,由信息控制者承担证明责任会大大增加其败诉的风险,而败诉对于信息泄露者而言具有一种激励效果,使其尽力规范自己的技术和服务能力,避免新的泄露隐私信息事件的发生。这种激励主要来自判决内容的公开对其商誉和竞争力的影响远远大于其因泄露他人隐私信息而承担的财产性赔偿责任带来的压力。如此,证明责任机制不再是信息泄露者免责的护身符,反而可以激励其采取更好的技术、采用更严谨的管理措施防止信息泄露,当然更会消除其故意泄露隐私信息的意志,进而有利于保障其他人隐私信息的安全。另一方面,信息控制者的因果关系证明责任使受害人的举证负担控制在其能够承受的范围内,会加大受害人通过诉讼保护其隐私的积极性,进一步促进隐私信息的保护。

## 五、信息控制者因果关系证明责任的适用条件

### (一) 适用前提:原告的基础证明责任

信息控制者因果关系的证明责任,随着诉讼的展开具有时间上的体系位置。因果关系仅是待证事实中的一项,众多事实的证明责任在原被告分担的情形下,自然展现出时间上的层次性。可见,这里证明责任的设置在逻辑上有一个先后顺序之分。从诉讼进程上说,原告方的证明责任须首先完成,只有在这个前提下,才发生被告方完成其证明责任的问题。如果原告方的证明责任没有完成,或根本完不成,则原告面临败诉的风险,而被告方根本不需要履行其证明责任。<sup>〔16〕</sup>那么,哪些事实需要由作为受害人的信息权人先行证明,哪些事实应当由信息控制者证明?

我们需要思考的是,受害人需要初步证明哪些事实的存在?证明责任的配置应当有利于真实地再现有争议的案件事实,因此,在分配证明责任时,应将当事人与证据的远近、获取证据的可能性以及举证的难易等作为考量因素,在综合考察当事人的证明能力基础上分配证明责任。<sup>〔17〕</sup>针对信息权人与被告间证明能力的悬殊,重新平衡信息权人与被告间的证明责任,有利于降低信息权人证明失败的风险和证明成本,减轻对信息权人维权的负激励。如何重新平衡双方的证明责任成为关键问题。为此,我们需要审视原告根据现有规定需要证明的内容,其中哪些是原告有能力证明的内容,哪些是造成原告证明压力的因素,这些因素是否适合由被告完成证明。

〔14〕 熊秉元:《正义的效益——一场法学与经济学的思辨之旅》,东方出版社2017年版,第38页。

〔15〕 [美]理查德·波斯纳:《法律的经济分析》,蒋兆康译,法律出版社2012年版,第893页。

〔16〕 参见叶自强:《证明责任的倒置》,载《中国法学》2004年第5期,第148页。

〔17〕 参见程春华:《证明责任分配、证明责任倒置与证明责任转移——以民事诉讼为考察范围》,载《现代法学》2008年第3期,第99~107页。

如前，按照《侵权责任法》第6条的规定，信息权人（即原告）要追究被告的责任，必须明确如下要件事实：被告基于过错实施了侵害原告信息的行为，信息权人因信息被侵犯遭受了损害，被告侵害行为与原告损害间具有因果关系。在这些要件中，原告确定有能力证明的只有原告遭受了损害这一事实，对被告实施了泄露信息行为这一事实的证明面临很大的困难。就此，原告通常只能证明被告具有实施加害行为的机会和能力，也能够证明存在加害行为，但常常无法证明被告确实实施了加害行为，或者说加害行为是由被告实施的。

然而，原告难以充分证明被告实施了泄露信息的行为，是否就为转换为被告承担证明责任提供了充分理由？答案是否定的。原告虽然不能为被告实施加害行为提供充分证明，但是通常有能力证明被告实施加害行为的较大可能性。比如，在庞某某案中，有能力和条件将庞某某的姓名、手机号和行程信息匹配在一起的主体是有限的，东航和趣拿公司以及中航信都有能力和条件，他们泄露的可能性很高，但庞某某及其朋友泄露的可能性是有限的，而第三人很难做到这种精确匹配。虽然没有更明确的证据，二审法院还是认定了被告泄露信息的高度可能性，进而认定了加害行为的存在。可以说，法院在可能性的证明上，降低了严格的证明标准，从而缓和了原告证明的困境。虽然法院声称原告证成了泄露信息行为的高度可能性，但实际上原告的证据对应的可能性或许更适合被认为属于较大可能性。法院声称认定了高度可能性或许是为了对应民事诉讼法司法解释第108条规定的“高度可能性”标准，可以说是一种不得已的“权宜之计”。其实，也可以像杨立新教授指出的那样，适当运用证明责任缓和规则，适当放宽原告证明的标准，在原告已经提出相当的证据证明其主张事实具有较大可能性，因客观条件限制无法继续举证，由被告举证证明；被告不能证明自己的否定主张的，认定原告的主张成立。<sup>〔18〕</sup> 崔聪聪进一步认为，只要受害人能够提出初步的证据证明侵权事实存在，且证据大致能够推断出侵权人是谁，则由“侵权人”举证证明其未实施侵权行为。<sup>〔19〕</sup>

总之，在因果关系的证明上，我们至少可以要求原告证明其有能力证明的内容。作为信息权人承担证明责任的前提，原告有义务举证证明隐私信息发生泄露的事实、信息控制者控制了其隐私信息且有泄露其隐私的高度可能性。原告针对这几点的证明责任具有证明能力且成本在可接受的范围内，具有可操作性。如果这些事实无法证明，被告便无做出实质回应的必要。其中，要证明信息控制者具有泄露隐私的高度可能性，需要证明其具有泄露隐私的能力。被告只有在原告完成前面的事实之后，才有必要和有义务证明自己行为与原告损害间没有因果关系。

有学者认为证明被告泄露隐私致害的高度可能性，需要证明其唯一性，即排除其他主体泄露隐私的高度可能性。<sup>〔20〕</sup> 但这种要求给原告同时也给被告提出了过于严格的要求。这并不是必要的，只要证明具有这种高度可能性的主体范围是有限的，而且被告泄露隐私的可能性与其他主体相比是最高的或者相同的即可。本案便是如此：东航和趣拿公司两个主体作为被告都具有泄露隐私信息的高度可能性，主体并不是唯一的，但是主体范围是有限的，而且二者泄露隐私的可能性是相同的。在逻辑上，法律并不刻意避免数人承担侵权责任的场合。

## （二）信息控制者因果关系证明责任的证明标准

信息控制者证明责任进路针对的是信息控制者是否泄露了隐私信息这一事实，该进路并不要求信息控制者证明其没有泄露隐私信息所需证明的全部内容，被告只需要排除其泄露隐私信息的高度可能性即可。这一要求符合民事诉讼证明责任的基本做法。民事责任以恢复原状、填补损害

〔18〕 参见杨立新：《侵害公民个人电子信息的侵权行为及其责任》，载《法律科学》2013年第3期，第150页。

〔19〕 参见崔聪聪：《个人信息损害赔偿问题研究》，载《北京邮电大学学报（社会科学版）》2014年第6期，第41页。

〔20〕 参见前注〔7〕，赵淑珏文，第70页。

为基本目标,责任承担不像刑事责任那样严格,对于事实的确认只要符合以证据证明高度可能性这一标准就足够了,不必像刑事诉讼法那样达到排除合理怀疑的程度。原告举证需要达到这一要求,被告举证也要达到这一要求。准此,信息控制者只要能够通过证据排除其泄露信息致害的高度可能性,即可被认为否定了因果关系。也就是说,只需要将这一可能性降低到正常情形即可。这不会给其带来过重的成本,因为他(们)最清楚信息处理的状况。将泄露信息致害的高度可能性降低到正常情形的这一要求,在很大程度上弥补了证明责任转换给信息控制者带来的不利影响。

泄露隐私信息案件中,往往数人都有泄露信息的高度可能性。此时,被告单纯地以证明其他主体有泄露信息的高度可能性为由,能否否定其行为与损害之间的因果关系?答案是否定的。从逻辑上讲,其他主体有泄露信息的高度可能性,不等于被告就没有泄露信息的高度可能性。被告若要否定自己行为与损害间的高度可能性,只能从影响可能性的因素出发来举证。德国的做法与此相通:复数控制者和/或处理者牵涉同一侵害性数据处理时,若控制者或处理者能够证明其无论如何都不应对致害事件负责,则可以免责。当然,只有在复数控制人采用大数据技术的场合,才应确立这种因果关系推定规则。<sup>[21]</sup>看起来,“无论如何都不负责”的标准比较笼统,但肯定的是,如果被告行为与损害没有因果关系,便属于无论如何都不负责的情形。单纯地认定他人具有因果关系,不足以否定被告自身的因果关系。因果关系的判断,还是要从可能性的角度来着手。

## 六、结 语

信息控制者证明责任的分配方案有必要明文规定。如果没有统一明确的规定,会发生不同法院采用不同做法的现象,不利于规则的统一理解和适用。毕竟,信息控制者是否泄露隐私信息的证明责任在实践中是有争议的,在没有法律明确规定的情形下,很多法院都采用保守的进路,将因果关系证明责任分配给权利人承担。然而,当法院不遵照上述合理平衡当事人证明能力和证明风险的做法时,会在实体上影响信息权人对其权利的维护效果,进而可能因宽松的责任导致信息产业发展发生畸形,这种畸形会不当地反作用于对权利人信息权的保护。因此,法律或者司法解释有必要明确规定信息控制者因果关系证明责任,消除争议。

---

**Abstract** Through examining the Judicial Interpretation for Civil Procedure Law and Tort Liability Law, it can be confirmed that in the case of personal information revealing, information owner has onus probandi of the causation of information-revealing action and damage. This onus probandi on the information owner does not match with his/her proving ability, and would more easily connive information-revealing action. In contrast, the onus probandi on the information controller is more reasonable.

**Keywords** Personal Information, Information Revealing, Causation, Onus Probandi

---

(责任编辑:赵秀举)

---

[21] 前注[12],叶名怡文,第97页。