收稿日期:2025-12-20

委托处理关系下个人信息侵权民事责任的承担

王 勤[1],肖伽琦[2]
(1. 中国矿业大学 人文与艺术学院,江苏 徐州 221000;2. 上海市第一中级人民法院,上海 200336)

摘要:《个人信息保护法》第二十一条未明确个人信息侵权中委托方与受托方的民事责任分配,学界对此亦存在显著分歧。应类推适用《民法典》雇主责任规定,由委托方承担侵权责任。二者在"控制力"与"利益归属"上的一致性为类推适用提供合理依据。委托方对受托方享有实质控制力,与雇主对雇员的控制力具有一致性。委托方与雇主均为另一方行为的最终获益者,两者具有利益归属的相似性。作为处理活动的最终获益者,由委托方承担责任符合"谁获益、谁负责"原理。从比较法看,亦有立法支持委托方责任模式,为此观点提供比较法参鉴。由委托方承担责任能有效降低信息主体维权成本,避免因受托方身份不明导致的维权障碍。委托方承担责任后可再行向受托方追偿,这将更便于查明个人信息由谁泄露的客观事实,更好保障委托方、受托方和信息主体三方间的利益平衡。委托处理关系中的个人信息侵权与共同危险行为存在明显差异,不应类推适用共同危险行为理论要求双方承担连带责任。

关键词:委托处理;个人信息;侵权;责任归属
中图分类号:D923 **文献标识码**:A **文章编号**:1003-6873(2026)03-0104-11

基金项目:国家社会科学基金项目"算力全国统一大市场建设的竞争法治保障研究"(25BFX057)。
作者简介:王勤(1993—),女,安徽铜陵人,中国矿业大学人文与艺术学院助理研究员,博士,主要从事民商法研究;肖伽琦(1995—),女,江苏泰州人,上海市第一中级人民法院二级法官助理,硕士,主要从事民商法研究。
DOI:10.16401/j.cnki.ysxb.1003-6873.2026.03.012

《个人信息保护法》第二十一条对个人信息委托处理进行了规定,该条分三款分别明确了委托方义务、受托方义务及对受托方转委托的限制等事项。然而对于在委托处理关系下发生个人信息侵权时,委托方与受托方如何承担民事责任这一问题,该条并未言明,学术界目前对此亦存在较大分歧,主要有以下几种观点。委托方责任说,即认为受托方受委托处理个人信息行为的法律效果应当直接归属于委托方。当发生个人信息侵权时,应由委托方承担责任[1]。受托方责任说,即认为应类推适用民法典第一千一百九十三条定作人责任的规定,当发生个人信息侵权时,应当主要由受托方承担侵权责任。委托方仅在对受托方的指示或选任存在过错时,才承担责任[2]。连带责任说,即认为应当借鉴共同危险行为理论,除非能够明确证明损害完全由一方引起,否则委托方与受托方应承担连带责任[3]。类型化区分说,即认为应当依据具体案情的不

同情形采用差异化的认定机制,例如区分是否存在擅自转委托、是否存在共同侵权等情形进行分别认定[4]。

委托处理个人信息的场景广泛存在。例如,商业银行在处理贷款申请时,可能因自身数据资源有限,将客户信用评估工作外包给第三方征信机构,银行提供必要的客户个人信息,征信机构负责核查客户身份、信用记录、财务状况及法律纠纷等,最终由银行依据评估报告作出贷款决策。部分企业将收集的用户网络信息、设备标识符、地理位置等分享给广告合作伙伴,以实现更为精准的广告推送和投放,同时监测广告的效果并获得相关统计数据[5]。此类委托处理模式通过专业化分工有效提升了信息处理效率,但也因参与主体的多元化,导致在个人信息侵权事件发生后,侵权责任的认定往往陷入复杂境地,可能涉及委托方单独侵权、受托方单独侵权、双方共同侵权以及具体侵权方难以明确等多种情形。在法律并未明文规定,学术界观点存在明显分歧的现状之下,如何确定侵权责任的归属,有理论和现实的必要性。本文支持委托方责任说,认为在此类委托处理关系中,个人信息侵权责任应由委托方承担。本文将从委托方和受托方法律地位的差异出发,首先,阐明委托方才是个人信息处理的最终控制者,受托方并不具备独立的个人信息处理者法律地位;其次,论证类推适用雇主责任推导出个人信息侵权责任应当由委托方承担的合理性;再次,从权利救济的实践层面说明由委托方承担侵权责任可有效降低信息主体的维权成本,更为周全地保障其个人信息权益;最后,进一步厘清委托处理关系下个人信息侵权与共同危险行为的本质差异,指出不应通过类推适用共同危险行为理论得出委托方与受托方承担连带责任的结论。

一、 委托方与受托方法律地位的差异

《个人信息保护法》第二十一条对个人信息的委托处理作出了规定,但并未明确“委托处理”的含义。学界一般认为,委托处理是指个人信息处理者(委托人)与其他组织或个人(受托人)通过委托合同建立关系,由受托方按照委托方的指示处理个人信息的情形[6]。因此在委托处理关系中便存在两方主体,即委托方和受托方。

(一) 受托方并非“个人信息处理者”

《个人信息保护法》第七十三条明确界定“个人信息处理者”为“在个人信息处理活动中自主决定处理目的、处理方式的组织和个人”,其核心特征在于决定处理目的和方式的“自主性”。而该法第二十一条对委托处理的规定显示,个人信息处理者(委托方)需与受托人约定处理目的、期限、方式等核心要素,并对受托方的处理活动进行监督;受托人则必须严格按照约定处理信息,不得超出授权范围,显然不具备“自主决定”处理目的和方式的权限。由此可见,受托方因受制于委托方的指示与监督,缺乏《个人信息保护法》所要求的“自主性”,故不属于该法界定的“个人信息处理者”范畴。

从比较法视角观察,欧盟《通用数据保护条例》(GDPR)明确区分“控制者(controller)”与“处理者(processor)”。根据该条例第二条第七款,“控制者”指单独或共同决定个人数据处理目的和方式的自然人、法人等主体。第八款则将“处理者”定义为为控制者处理个人数据的主体。美国《统一个人数据保护法案》(UPDPA)和英国《2018年数据保护法》(Data Protection Act 2018)亦采用类似分类。美国《统一个人数据保护法案》第二条第三款将“控制者”界定为单独或与他人共同决定处理目的和方式的主体,第二条第十二款将“处理者”定义为代表控制者处理个人数据的实体。英国《2018年数据保护法》(Data Protection Act 2018)第三十二条第一款规定,“控制者”指单独或与他人共同决定个人数据处理目的和方式的机构;第三十二条第二款指出,“处理

者”指代表控制者处理个人数据的任何人。

我国个人信息委托处理关系中的“委托方”与“受托方”,大致可分别对应上述立法中的“控制者”与“处理者”。不同之处在于,我国《个人信息保护法》并未采用“控制者、处理者”二分体系,仅使用“个人信息处理者”这一单一概念。此外,我国个人信息委托处理中的受托方,还可类比新加坡《个人数据保护法案》(PDPA)第二条所规定的“数据中介(data intermediary)”,即代表其他组织处理个人数据的组织。

(二) 委托方是个人信息处理活动的最终控制者

根据《个人信息保护法》第七十三条规定,判断“个人信息处理者”的关键,并不在于是否直接实施处理行为,而在于是否自主决定。从处理方式上看,个人信息处理者既可以直接参与处理,也可以通过委托他人处理的方式间接参与。即便未直接实施处理活动,只要其“自主决定”处理的目的和方式,就属于该法界定的“个人信息处理者”。因此,在委托处理关系中,只有作为委托方的一方符合“自主决定处理目的和方式”的核心特征,属于《个人信息保护法》所规定的个人信息处理者;受托方因不具备这一自主性,不属于该范畴。

委托方是个人信息处理活动的最终控制者。个人信息处理委托方对个人信息处理活动的控制力,贯穿于信息处理的全过程,体现在权限来源、过程监督及权限终止三个维度上。

受托方处理权限来源于委托方授权。从权限来源与边界看,受托方信息处理权限完全源于委托方的授权,其处理目的、方式等均受委托合同约束,必须严格按照委托方要求处理个人信息,不得超出约定范围。即使在合同履行过程中,委托方如果得知或者发现受委托者未按照委托要求处理个人信息,或未能有效履行个人信息安全保护责任,也有权解除委托处理关系,要求受托方停止处理并删除信息。

受托方处理活动始终受委托方监督。《个人信息保护法》第二十一条明确赋予委托方对受托方的监督义务,这种义务并非形式化要求,而是包含实质内容的控制权配置。委托方需通过合同约定受托方的责任义务、开展个人信息安全影响评估、对受托方进行审计[7],且监督需随信息处理的动态性保持“动态监督”,包括定时或不定时审查处理记录、共同管理数据库权限、调整数据传输接口等。这些措施表明,委托方对受托方的处理行为拥有全程干预权,可通过具体操作直接管控信息处理的关键环节。

从处理活动的终止来看,在处理服务完成后,受托方应按照委托方指示删除或向该委托方返还全部个人数据并删除复制件。受托方转委托需经委托方事前同意,这使得委托方的控制范围延伸至受托方,进一步强化了委托方对信息处理链条的全程管控[8]。

综上,委托方通过授权边界设定、监督义务履行及最终终止权行使等多个维度,实现对个人信息处理活动的“最终控制”,受托方仅为其意志的执行者。

(三) 委托方与受托方关系

委托方与受托方关系是基于委托合同的“控制—服从”型从属关系,而非平等独立的法律主体关系,核心特征体现为“依附性”与“受控性”。受托方的从属地位主要体现在如下几个方面:

其一,法律地位依附性。受托方并非独立的个人信息处理者,其处理行为的合法性完全依附于委托方授权和信息主体同意。与信息共享、转让中“新控制者”的独立性不同,受托方仅能在授权范围内处理信息,数据始终处于委托方的控制之下,受托方不具备对信息的独立控制权。《信息安全技术个人信息安全规范》将委托处理与共享、转让区分,明确委托处理中受托方无需单独取得信息主体同意[7],原因即在于,受托方与信息主体通常无直接联系,仅依据委托方指示

处理个人信息,其行为通常被视为委托方处理活动的延伸。这一区分亦佐证了受托方的非独立地位。

其二,权利义务受控性。受托方的义务内容由委托方设定。受托方需严格遵守处理权限,不得超出委托方设定的范围。委托合同效力消灭(不生效、无效、终止等)后,受托方必须返还或删除信息,不得保留。上述义务本质上是对委托方信息控制权的维护,体现了受托方对委托方意志的服从。

综上,委托方与受托方的关系是"控制—服从"型从属关系。委托方是信息处理的主导者,受托方是其意志的执行者,二者通过委托合同共同构成"委托方控制、受托方执行"的信息处理模式。

需要回答的问题是,《个人信息保护法》第九条规定,个人信息处理者应当对其个人信息处理活动负责。根据上文分析,受托方不属于该法所界定的"个人信息处理者"。那么,若对第九条作反对解释,是否意味着受托方无需为其在受托处理个人信息过程中发生的侵权行为承担责任,而应由委托方对该行为的最终结果承担责任?

二、 委托处理关系下民事责任的承担可类推适用雇主责任

《民法典》第一千一百九十一条规定,用人单位的工作人员因执行工作任务造成他人损害的侵权责任应当由用人单位承担。这一规则可类推适用至个人信息委托处理场景下的侵权责任分配。

(一) 类推适用雇主责任的理论证成

雇佣合同和委托合同同属劳务给付合同[9]。二者均围绕劳务给付形成权利义务关系。尽管两者存在劳务性质、主体范围等差异,而雇佣合同则多以低级劳务或不自由劳务为标的。雇佣合同中的雇员限于自然人,而委托合同中的受托人并无此类限制[9]。但二者在核心法律特征即"控制力"和"利益归属"上的一致性为在委托处理关系中类推适用雇主责任提供了合理依据。

1. 控制力的一致性:委托方与雇主均对另一方行为享有实质支配力

在雇主责任体系中,"控制力理论"是雇主对雇员行为承担责任的核心理论基础之一。雇主因对雇员具有实质性支配地位,因此应对雇员在执行工作任务中的侵权行为负责[10]。雇佣合同的核心特征在于"雇主对雇员的支配地位"以及"双方在合同履行中实质上的不平等关系"[11]。雇主通过对雇员的选择、培训和日常管理形成实质控制力,雇员必须服从雇主的指令,在工作过程中接受雇主监督、控制与管理。这种控制力不仅体现在具体工作安排上,更贯穿于对雇员行为方向的主导和结果的约束。

这一逻辑同样可以适用于个人信息委托处理关系。委托方对受托方的控制力与雇主对雇员的控制力具有高度相似性,为类推适用雇主责任提供了坚实基础。根据《个人信息保护法》第二十一条规定,委托方在委托处理个人信息时,必须与受托方明确约定处理目的、处理方式、期限、个人信息种类、保护措施及双方权利义务,并对受托方的处理活动进行全程监督。受托方则需严格按照约定处理信息,不得超出委托范围处理个人信息。申言之,尽管委托方并未直接参与受托方处理个人信息的具体操作流程,其通过合同条款的设定(如处理标准、安全要求等)和监督机制的运行(如信息安全影响评估、过程审计等),对受托方信息处理活动形成了实质性控制。

这种实质控制力体现在两个层面:一方面,委托方主导着信息处理的核心环节,从处理目的

的设定到处理方式的选择,均由委托方最终决定;另一方面,委托方通过监督义务的履行,能够及时纠正受托方的违规行为,确保处理活动始终符合自身要求。例如,在专业信息处理场景中,委托方可能会在合同中设定细致的技术标准、安全加密要求及定期汇报机制,这种基于专业领域的控制虽与雇佣关系中日常工作的直接指令形式不同,但本质上都是一方对另一方行为方向和结果的主导与控制。与之形成鲜明对比的是承揽合同。在承揽合同中,定作人与承揽人之间并不存在这种紧密的控制与从属关系。定作人通常不会对承揽人进行全程监督,而是在交付工作任务后,由承揽人保持相对独立的作业空间,承揽人可自主安排工作方式、组织人员调配,仅需按照合同约定的标准完成并交付劳动成果即可。故笔者并不赞同个人信息委托处理关系中侵权责任的归属可类推适用定作人责任的观点。

从制度功能角度将责任归属于委托方,能形成更为有效的风险预防机制。雇主责任通过将雇员行为风险归属于雇主,可以促使雇主强化对雇员的管理与监督,通过建立严格的规章制度,如绩效奖惩、纪律处分等,防止损害发生[10]。同理,让委托方对受托方侵权行为负责,也能够更好促使委托方在选择受托方时更为审慎,如更为细致地审查其资质、技术能力;在合作过程中强化监督,如定期进行审计,审查受托方对保密义务的落实、处理记录的保存、数据安全措施等,从而从源头上减少个人信息的侵权风险。反之,若仅要求受托方承担责任,可能会纵容委托方放松对受托方监督,毕竟其无需为损害结果负责,反而增加个人信息侵权风险。

2. 利益归属的相似性:委托方与雇主均为另一方行为的最终获益者

雇主责任另一法理基础是“报偿理论”[10],也即“利益与风险共生”“谁获益,谁担责”。雇员的劳动是雇主经营活动的有机组成部分,雇员的劳动成果直接转化为雇主的商业利益,如企业通过员工的生产、销售行为实现利润增长,因此雇主需对雇员在履职过程中的侵权行为负责。这种“获益者担责”的机制,本质上是对权利义务对等原则的践行,即享受利益者必须承受相应风险,这符合公平正义的价值理念,也能通过责任机制倒逼获益方加强风险管控。

将这一逻辑迁移至个人信息委托处理关系中,委托方与雇主在利益归属上的高度相似性为其承担侵权责任提供了另一重要理论支撑。在个人信息委托处理活动中,受托方处理行为本质上是委托方信息处理目的的延伸,受托方是代替委托方实施处理行为的“工具”[12],处理结果最终服务于委托方的核心利益。例如,商业银行委托第三方征信机构评估客户信用,其目的是通过专业机构的核查结果降低贷款风险,最终实现信贷业务的安全运营与利润获取;互联网企业将用户数据交由广告合作伙伴处理,是为了通过精准投放提升营销效率,进而扩大市场份额、增加营收。受托方虽能通过提供服务获得报酬,但这种报酬仅是劳务对价,并非信息处理的利益核心所在。真正从信息处理中实现经营目标、获取商业利益的,始终是委托方。

依据权利义务对等原则,委托方既然通过受托方的处理活动实现了自身利益,就应当对处理过程中可能发生的侵权风险承担责任。这一责任分配方式符合“谁获益、谁担责”的朴素正义观,也与法律制度中“权利义务相统一”的基本原则相契合。

综上,在个人信息委托处理关系中,委托方作为信息处理结果的最终获益者,与雇佣关系中的雇主在利益归属上具有本质一致性。这种一致性决定了委托方应当像雇主对雇员行为负责那样,对受托方的侵权行为承担责任,这既是权利义务对等原则的要求,也是保护信息主体权益,从源头降低侵权风险的现实需要。

(二) 比较法上的法律支撑

从比较法视角观察,已有立法明确支持委托方承担责任模式,尤其体现在新加坡与欧盟及

其成员国的法律规范中。新加坡《个人数据保护法案》(PDPA)直接采用了以委托方为核心的责任模式。该法案第四条第三款规定,对于由数据中介代表某一组织并为该组织之目的处理的个人数据,该组织在本法项下承担的义务,与该组织自行处理该个人数据时所承担的义务相同。申言之,即便侵权行为实际发生在受托方处理环节,法律仍将责任直接归属于委托方,不允许其以"侵权行为由第三方实施"为由规避责任。这一规定强化了委托方对数据处理全流程的终极责任,确保了权利受损者能直接向最具控制力的主体主张救济。

欧盟层面的《数据保护指令》同样构建了以控制者(即委托方)为核心的责任体系。其第二十三条第一款明确规定,对于因不合法数据处理或违反规范行为遭受损害的个人,有权直接向控制者主张赔偿,且该请求权的相对方仅限定为控制者,排除了个人信息主体直接向受托方索赔的可能性。

作为该指令的转化者,德国旧《联邦数据保护法》进一步细化了这一规则。其第七条明确赋予个人信息主体向控制者索赔的独立请求权,即便损害实际由受托方的行为引发,控制者仍需承担全部赔偿责任;第十一条则再次强调,即便个人信息采用了委托处理方式,第七条提及的损害赔偿请求权依然是由个人信息主体向个人信息处理委托人主张。尽管该法在极特殊情况下允许个人依据民法中"一般人格权侵害"的规定向受托人索赔,但这一例外情形的适用范围被严格限制,要求一般人格权受损必须达到严重程度,本质上仍是对"委托方承担责任"规则的补充,而非否定。

值得注意的是,欧盟现行立法对委托人承担责任的态度有所调整。2016 年通过的《通用数据保护条例》(GDPR)第八十二条改变了此前《数据保护指令》的委托方承担责任模式,规定个人信息主体既可以直接向控制者主张损害赔偿,也可以直接向受托人主张赔偿,标志着欧盟从委托方责任转向了认可委托方与受托方连带责任。德国新《联邦数据保护法》随之删除了旧法中限定请求权对象为控制者的第七条,不再将个人信息主体的请求权对象仅限定于控制者[12]。不过,这种立法变化并不意味着我国必须随之吸收采纳。欧盟曾明确主张由委托方承担责任,本身即表明委托方承担责任的观点具有一定的合理性与实践价值。至于欧盟为何转变观点,具体原因尚不明确,我国立法无需盲从欧盟调整,仍可基于本土制度逻辑选择委托方承担责任模式。

综上,无论是新加坡的明确规定,还是欧盟及德国曾采用的规则设计,均在立法层面体现了"委托方为数据处理侵权责任承担者"的立场。即便欧盟后来的观点有所调整,也无法掩盖这一模式在比较法上所获得的认同。

三、 诉讼效益分析:由委托方承担侵权责任可有效降低诉讼成本,平衡多方利益

由委托方承担侵权责任能够有效降低信息主体的维权障碍,避免因受托方身份难以确定导致的维权困难。鉴于个人信息处理的专业性和个人信息泄露环节的复杂性,由委托方承担责任后自行向受托方追偿,更易查明个人信息由谁泄露的客观事实,有效降低诉讼成本,提升诉讼效率,实现委托方、受托方与信息主体间利益失衡。

(一) 受托方承担侵权责任为信息主体维权设置了多重障碍

部分观点主张由受托方承担侵权责任,该主张虽在理论上可能具有一定的合理性,但在实践中会大幅增加信息主体的维权难度,并非妥当的责任配置方案。在实践中的多数情况下,用户直接交互并授权处理个人信息的对象是委托方,通常仅知晓委托方身份,而对受托方的具体身份、资质等信息往往并不知情。以常见的隐私协议为例,《微博个人信息保护政策》仅提及为

提升信息处理效率,可能会委托第三方处理用户个人信息,未明确指出具体受托方;《淘宝网基本功能隐私政策》虽说明可能委托合作方处理信息,但同样未披露受托方详情。

鉴于信息主体对受托方身份并不知情,若认为应由受托方承担侵权责任,信息主体必须首先向委托方请求披露受托方信息才能获知被告身份进而提起诉讼,这无疑将增加维权的复杂性。相较于直接起诉委托方,要求委托方披露信息既不便捷,还需额外耗费时间和精力。更为关键的是,委托方与受托方往往存在紧密的商业合作关系,属于利益联系更为密切的利益共同体。出于保护商业伙伴的考虑,委托方可能推诿、拖延甚至拒绝披露受托方信息,导致信息主体维权陷入停滞。

尽管信息主体可能因维权受阻放弃使用委托方服务或公开表达对于委托方的负面评价,进而给委托方声誉带来负面影响,但单个或少数用户的诉求对于委托方商业利益的冲击往往有限,难以促使委托方主动配合。即便信息主体通过诉讼方式要求委托方披露受托方信息,仍需经历起诉、申请调查令等复杂流程,耗时费力。

从规范层面看,根据我国《个人信息保护法》第二十三条规定,个人信息处理者在向其他个人信息处理者提供其处理的个人信息时,应向信息主体告知接收方的名称或姓名等身份信息。并未要求个人信息处理者在委托处理个人信息时,需向信息主体告知受托方身份信息,可知现行法律并未赋予委托方向信息主体披露受托方身份的法律义务,这无疑将进一步加剧信息主体的维权困难。因此,让受托方承担侵权责任在实践中为信息主体维权设置了多重障碍,并非合理方案。

(二) 委托方承担责任更有助于在民事诉讼中实现多方利益平衡

实践中,信息主体通常通过隐私政策或隐私协议授权委托方处理个人信息,其合同关系的直接相对方为委托方,而与受托方并无直接法律关系。信息主体通常可能是为了获取委托方的服务,如贷款、社交、购物等,才授权其处理个人信息,其信任对象为委托方,其让渡个人信息权益所换取的利益(如便捷服务)也直接来源于委托方。对信息主体而言,委托方的身份明确可知,若发生个人信息侵权事件,其可便捷地直接以委托方为被告提起诉讼。

而在司法实践中,尽管目前尚未出现直接涉及委托处理关系下个人信息侵权的案例,但从个人信息提供关系中的相关案例来看,信息主体普遍倾向于直接起诉收集其个人信息的提供方。《个人信息保护法》第二十三条明确规定,在个人信息提供关系中,提供方需向信息主体披露被提供方的身份信息。但从司法实践案例可以看出,即便信息主体知晓被提供方的具体身份,仍会倾向于选择起诉与自身存在直接关联的个人信息提供方。由此“举轻以明重”,在委托处理关系中,由于法律并未要求委托方向信息主体披露受托方信息,信息主体更难知晓受托方身份,自然会更倾向于直接起诉委托方。

另一个值得探讨的问题是:由委托方承担责任,是否会造成委托方与受托方之间的利益失衡?具体而言,当侵权行为实际由受托方实施时,若仅让未直接实施侵权的委托方承担责任,而将真正的侵权主体受托方排除在责任承担之外,这对委托方是否过于不公?对此,笔者认为,由委托方承担侵权责任并未排除其向受托方追偿的权利,因此并不存在利益失衡问题。正如上文所说,信息主体难以通过公开渠道获悉受托方的真实身份,也无法得知个人信息泄露的具体路径。但对于直接处理个人信息的受托方和监督个人信息处理活动的委托方而言,个人信息在两者之间流通,处理活动也处于双方控制之下,两者具有技术和信息获取的优势地位。由委托方向受托方追偿,双方均可利用技术优势和获取信息的便捷性进行举证,更利于法院查明个人信息由谁泄露的事实。对外层面,由委托方向信息主体承担侵权责任,可保障信息主体的权益实

现;对内层面,委托方和受托方可通过自行协商或诉讼的方式解决责任划分问题,委托方还可根据双方之间的委托合同追究受托方违约责任。这一责任承担模式既能有效降低诉讼成本,提升诉讼效率,同时便于厘清各方责任,从而保障委托方、受托方与信息主体利益的相对平衡。

此外,由委托方承担侵权责任的观点,已在部分企业的实践中得到明确印证。以《顺丰速运隐私政策》为例,其第2.1.2条明确向客户说明:为实现具体产品的业务功能,可能会委托合作方协助提供相关服务,将在委托范围内就其受托行为向客户承担责任。这一条款设计不仅体现了该企业对"委托方责任"的认可,更能通过明确责任归属增强用户信任,体现了企业的责任担当。用户无需弄清复杂的委托链条,只需基于与委托方的直接法律关系主张权利,这将大幅降低用户维权成本,扫清用户维权障碍。

四、 委托方和受托方之间并不构成共同危险行为

在实践中,信息主体往往难以证明究竟是委托方还是受托方侵害了其个人信息权益,导致事实陷入因果关系不明的状态。以个人信息泄露为例,个人信息处理环节复杂,经常涉及多方参与者,具体哪方泄露个人信息往往难以准确确定。针对这一问题,我国不少学者认为应当类推适用共同危险行为制度加以解决[13]。也有部分学者对共同危险理论持反对观点。例如,有学者认为,个人信息侵权行为及危险性评价与共同危险行为规则相去甚远,证据损害现象也并非类推共同危险行为的充分和必要条件,类推适用共同危险行为观点难以适用[14]。个人信息侵权行为并不符合共同危险说与证据损害说的构成要件[15]。

笔者同样认为,在个人信息侵权案件中,尤其当多个参与者之间存在委托处理关系时,能否类推适用共同危险行为理论,值得商榷。

第一,共同危险行为通常只有单一损害源,而个人信息侵权可能存在每个主体都侵权的情况。共同危险行为指的是两个或两个以上的行为人分别实施了可能危及他人人身、财产安全的行为[16]。在共同危险行为中,损害后果由某一方侵权行为造成,只是具体侵权方难以确定,因果关系不明。一个经典的共同危险行为案例是两个猎人同时向同一方向射击,受害者中弹受伤,但无法确切知道究竟是哪个猎人发出的子弹造成了损害。在此情境中,仅有一颗子弹击中目标,并非两颗子弹同时命中。然而,在涉及多个主体处理个人信息的情形下,情况则可能有所不同。每个参与主体都有可能实施了侵权行为。以个人信息泄露侵权为例,假设某电商平台用户的姓名、电话、收货地址等信息被批量泄露,经调查发现该平台委托了第三方公司进行数据处理,但用户无法证明信息泄露究竟是源于电商平台,还是第三方处理机构,抑或是双方均泄露了个人信息。申言之,即个人信息委托处理关系中的委托方和受托方既可能只有一方泄露了个人信息,但同时也可能双方都泄露了个人信息。

易言之,与传统意义上的共同危险行为相比,在个人信息侵权案件中,可能并非只有一个责任源头,而是存在多条潜在的信息侵权路径。若将前文提及的猎人射击案类比于个人信息侵权事件,当存在多个信息处理主体时,可能存在每个主体都侵害了个人信息权益的情况,这就好比两个猎人射出的子弹同时击中了受害者。在这种情况下,并非单一主体的行为导致了损害结果,而是所有相关主体的行为都造成了对信息主体权益的侵害。这与传统意义上仅有一方行为实际造成损害结果的共同危险行为明显不同。因此,简单套用共同危险行为理论分配责任显然无法全面反映问题本质。

第二,个人信息处理行为本身未必"危及安全",且委托方与受托方缺乏共同危险行为所需的时空同一性,因此难以适用共同危险行为理论。共同危险行为的核心要件之一是行为人共同实施"危及他人人身、财产安全的行为",例如数人同时向同一方向投掷石块致人损害。但在个

人信息委托处理关系中,委托方的核心行为是确定处理目的、方式并监督受托方,受托方则是按照委托指令执行具体操作(如数据录入、分析等),这些行为本身是信息处理活动的常规环节,若符合法律规定和合同约定,很难被认定为“危及他人人身、财产安全的行为”。正如学者指出的,个人信息处理行为的风险更多体现为潜在的权益侵害,如信息泄露、滥用,而非直接的、即时的危险,这与共同危险行为所要求的“危险性”存在本质差异[14]。此外,共同危险行为要求各行为人的行为在时空上具有同一性[17],即“数人行为均在同一时间、同一地点实施,且均有造成损害的可能性”。而在委托处理关系中,委托方与受托方的行为往往存在明显的时空分离。委托方可能在A地A时发出指令,受托方在B地B时执行处理。这种异时性、异空性与共同危险行为所要求的时空同一性存在显著差别,自然也无法适用该理论进行责任分配。

第三,委托方与受托方存在明确的管理控制关系,这与共同危险行为中行为人之间的无关联性存在显著区别,进一步否定了共同危险行为理论的适用空间。在共同危险行为经典模型中,各行为人之间通常缺乏事先的意思联络或特殊关联,彼此处于独立状态,他们的行为之所以被归为“共同危险”,仅仅是因为在同一时空下各自实施了具有危险性的行为,且无法确定具体加害人。但在个人信息委托处理关系中,委托方与受托方的关系具有鲜明的不平等性和从属性。根据《个人信息保护法》第二十一条,委托方不仅有权决定处理目的、方式,还需与受托方约定处理范围、期限及保护措施,并对受托方的处理活动进行全程监督;受托方则必须严格按照委托指令行事,不得超出授权范围。这种“控制—服从”的关系结构,使得两者的行为并非相互独立,而是受托方行为是委托方意志的延伸与执行。企业委托第三方处理数据时,委托方往往会通过合同条款、技术手段对受托方的操作进行约束,如共享数据访问权限、要求定期审计等,这种管理控制显然与共同危险行为中行为人之间的无关联性截然不同。因此,将两者关系等同于共同危险行为中的松散主体关系,既不符合事实,也忽视了委托处理关系的结构特征。

第四,在委托处理关系中类推适用共同危险行为可能导致责任分配不公,不利于从源头防范个人信息侵权风险。《民法典》第一千一百七十条规定:“二人以上实施危及他人人身、财产安全的行为,其中一人或者数人的行为造成他人损害,能够确定具体侵权人的,由侵权人承担责任;不能确定具体侵权人的,行为人承担连带责任。”如果在个人信息处理中,认为委托方与受托方存在委托关系时应适用此条款,那么当能证明侵权由受托方造成时,似乎应由受托方单独承担责任。然而,与共同危险行为中各方无特殊关系不同,个人信息委托处理中,受托方由委托方挑选授权,处理方式和目的由委托方决定,且需接受委托方监督,处于其管理控制之下。因此,简单判定由受托方单独承担责任会带来两方面不利影响:一方面,信息主体往往对受托方情况不知情,例如用户在使用某应用程序时,通常只知道运营主体(委托方),对背后的众多受托方一无所知,要求其直接向受托方主张权利不切实际;另一方面,这会削弱委托方筛选和管理受托方的动力,因为按第一千一百七十条规定,只要能证明侵权系受托方所为,委托方即可免责,这显然不利于从源头上减少个人信息侵权风险。

我国《民法典》第一千一百七十条明确,共同危险行为的责任分配规则为:“二人以上实施危及他人人身、财产安全的行为,其中一人或者数人的行为造成他人损害,能够确定具体侵权人的,由侵权人承担责任;不能确定具体侵权人的,行为人承担连带责任。”若将此规则类推适用委托处理场景,则会产生明显的实践弊端。具体而言,当侵权行为可明确归因于受托方时,依此规则似乎应由受托方单独担责。但这一结论完全忽视了委托处理关系的特殊性:与共同危险行为中各方无关联、无控制的松散状态不同,受托方由委托方筛选,处理目的与方式由委托方决定,处理过程受委托方全程监督,其行为本质上是委托方意志的延伸。在此前提下,要求受托方单独担责将引发双重不利后果。一方面,信息主体通常仅知晓委托方身份(如应用程序运营者),

对受托方的名称或姓名等身份信息毫不知情,甚至难以确认受托方存在。若强行根据该条规定要求信息主体直接向受托方主张权利,会因信息不对称大幅提高维权门槛,实质上剥夺了其获得救济的可能性。另一方面,这一规则将变相弱化委托方的管理义务。按照共同危险行为的逻辑,只要委托方能证明侵权系受托方所为即可免责,这会降低委托方筛选受托方时的审慎程度,也会削弱其监督受托方合规处理的动力——毕竟"举证免责"的成本可能远低于主动防控风险的成本。这种责任机制显然不利于从源头遏制个人信息侵权行为的发生。

综上所述,仅因为难以确定哪个具体环节或主体导致个人信息侵权,就认为应类推适用共同危险行为,逻辑推理并不充分。以笔者之见,即便无法确切证明委托方与受托方中何者实施了侵权行为,亦不应径行援引共同危险行为规则认为双方应承担连带责任。

五、 结语

本文围绕个人信息委托处理关系中的责任归属问题展开探讨,核心结论为:在个人信息委托处理场景下,当发生个人信息侵权时,应类推适用《民法典》中的雇主责任由委托方作为责任主体承担侵权责任。二者在核心法律特征上的契合为类推适用提供了坚实理论基础。委托方对受托方的处理活动享有实质控制力,与雇主对雇员的管理支配控制力具有一致性;委托方作为个人信息处理活动的最终获益者,与雇主作为雇员劳动成果归属者的利益格局高度相似,由委托方承担责任既符合"利益与风险共生"的侵权法基本原理,也与比较法上部分立法例所确立的委托方责任模式形成呼应。同时,这种责任分配模式具有鲜明的实践价值:既能有效降低信息主体的维权成本,避免因受托方身份不明导致的维权困境,又能通过强化委托方责任意识,促使其在选择合作伙伴时更为审慎,在日常管理中加强对受托方的监督,从源头上遏制个人信息侵权事件的发生。

此外需要明确的是,委托处理关系中的个人信息侵权与共同危险行为存在本质差异,不应简单套用共同危险行为理论要求双方承担连带责任。唯有立足委托处理关系的特殊性,构建以委托方责任为核心的规则体系,才能在平衡各方利益的基础上,为个人信息权益提供更为周全的保护,实现法律规制与实践需求的有效衔接。

参考文献

[1] 杨合庆. 中华人民共和国个人信息保护法释义[M]. 北京:法律出版社,2022:78.
[2] 程啸. 个人信息保护法理解与适用[M]. 北京:中国法制出版社,2021:209.
[3] 曹明德,赵峰. 委托处理个人信息的私法规制[J]. 重庆大学学报(社会科学版),2022(4):203-215.
[4] 阮神裕. 个人信息委托处理中受托人的地位、义务与责任[J]. 当代法学,2022(5):110-119.
[5] 陈龙江,郑淑琳. 论个人信息委托处理的私法规制[J]. 海南大学学报(人文社会科学版),2023(5):130-140.
[6] 周光权. 委托处理个人信息与侵犯公民个人信息罪:结合《个人信息保护法》第21条的分析[J]. 环球法律评论,2021(6):23-39.
[7] 全国信息安全标准化技术委员会. 信息安全技术 个人信息安全规范:GB/T 35273—2020[S]. 北京:中国标准出版社,2020.
[8] 龙卫球.《中华人民共和国个人信息保护法》释义[M]. 北京:中国法制出版社,2021:91-95.
[9] 游冕.《民法典》第919条(委托合同的定义)评注[J]. 南大法学,2023(4):175-191.
[10] 程啸. 侵权责任法[M]. 3版. 北京:法律出版社,2021:445-446.
[11] 最高人民法院研究室. 最高人民法院新民事案件案由规定理解与适用:上[M]. 北京:人民法院出版社,2021:542-543.
[12] 云晋升. 控制归责理论下个人信息处理民事责任的分配:以《中华人民共和国个人信息保护法》第21条为中心

的分析[J]. 东北师大学报(哲学社会科学版),2025(2):128.
[13] 叶名怡. 个人信息的侵权法保护[J]. 法学研究,2018(4):83-102.
[14] 田野,张耀文. 个人信息侵权因果关系的证明困境及其破解:以相当因果关系理论为进路[J]. 中南大学学报(社会科学版),2022(1):61-62.
[15] 方程. 贝叶斯定理认定因果关系的逻辑展开:从个人信息侵权案切入[J]. 浙江工商大学学报,2023(4):142-156.
[16] 张新宝. 中国民法典释评:侵权责任编[M]. 北京:中国人民大学出版社,2020:29.
[17] 王利明. 论共同危险行为中的加害人不明[J]. 政治与法律,2010(4):76-83.

Determination of Civil Liability of Personal Information Infringement in Entrusted Processing Relationships

WANG Qin[1], XIAO Jiaqi[2]
(1. School of Humanities and Arts, China University of Mining and Technology, Xuzhou, Jiangsu, 221000, China; 2. Shanghai No. 1 Intermediate People's Court, Shanghai, 200336, China)

Abstract: The division of civil liability between the entrusting party and the entrusted party is not stipulated in Article 21 of the Personal Information Protection Law, which has remained debatable in academic circles. The provisions of employer's liability in the Civil Code should be applied by analogy, and thereby the entrusting party should bear the tort liability. The consistency between the two in terms of control and benefit attribution is the premise for such application. The substantial control over the entrusted party is consistent with that over employees. Both the entrusting party and the employer are the beneficiaries of the other party's actions, being analogous to each other in terms of benefit. The entrusting party should bear the liability, which is in conformity with the principle of the beneficiary as the bearer of liability. From the perspective of comparative law, the viewpoint of entrusting party bearing the liability is also supported in legislation. It can significantly reduce the enforcement cost of the infringed party, averting the uncertainty as to the infringing party. After assuming liability, the entrusting party can still file a claim of compensation from the entrusted party. It is conducive to identifying the unlawful disclosure of personal information, so as to strive for the balance between the interests and rights of entrusting party, entrusted party and personal information subjects. The infringement of personal information in the entrusted processing relationships is clearly different from the joint dangerous acts, therefore, the principle of bearing joint and several liability for losses cannot be applied here.

Key words: entrusted processing; personal information; infringement; liability determination

〔责任编辑:朱 根〕