

Doi:10.11835/j.issn.1008-5831.fx.2022.03.003

欢迎按以下格式引用: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.

Doi:10.11835/j.issn.1008-5831.fx.2022.03.003.

Citation Format: CAO Mingde, ZHAO Feng. Civil law regulation of entrusted processing of personal information [J]. Journal of Chongqing University (Social Science Edition), 2022(4):203-215. Doi:10.11835/j.issn.1008-5831.fx.2022.03.003



# 委托处理个人信息的私法规制

曹明德,赵峰

(中国政法大学民商经济法学院,北京 100088)

**摘要:**委托处理个人信息是信息流动、共享与利用的必然选择。《个人信息保护法》第21条专门为委托处理个人信息提供了规范基础,填补了《民法典》《电子商务法》《网络安全法》等规范空白,但就该条的规范内容如何解释适用,对委托处理私法规制的目的、对象及方式等要素的具体展开,仍需藉由解释论予以完善。由于司法实践中,信息处理者通常会援引其与第三人之间存在合同或其他交易安排,系由他人造成了损害而与自身的处理行为无关,给信息主体的权益保护带来了挑战,这构成了委托处理私法规制的核心。作为对委托处理进行私法规制的基础论证,委托处理的法律结构不同于共同处理,信息处理者与受托人之间为从属关系,信息处理者决定了处理的目的、方式,受托人只能按信息处理者的指示处理个人信息。为了更好地保障信息主体的合法权益,委托处理关系内部合同应当包含必备条款以确保受托人合法处理数据,且信息处理者可以检查受托人是否遵守这些规定。相较于《个人信息保护法》第20条由内部主体约定各方的权利义务,第21条第1款详细列举委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等事项,是值得肯定的立法选择。结合《个人信息保护法》第21条第2款以及域外法的通常规则,受托人应当承担依指示处理、服务结束后的返还(或删除)、保密三项法定义务。此外,在转委托、告知同意以及适当化任命与监督上不能适用委托合同的一般规则,其目的在于确保受托人正确、合适地履行职责,遵守个人信息保护法规。对于各方的责任承担,《个人信息保护法》第69条规定了损害赔偿,同时,依靠《民法典》规范实现体系拓展,使信息主体的权益救济不仅可以通过人格权编加以解决,还可以通过侵权责任编进行兜底保护。然而,《个人信息保护法》第21条并未规定信息处理者与受托人之间如何进行责任划分,构成法律漏洞。为消解委托处理中责任主体不明的救济困境,应当通过连带责任规则实现信息主体的权益救济。具体而言,在漏洞填补上可以借助共同危险行为理论,类推适用《民法典》第1170条的规定,除非能够证明损害确实是由对方引起,否则要求信息处理者与受托人就同一处理中的损害承担连带责任。

**基金项目:**司法部国家法治与法学理论研究资助项目“人工智能产品法律责任研究”(18SFB039);中国政法大学大健康法治政策创新研究项目资助(Y2020005)

**作者简介:**曹明德,中国政法大学法学教授;赵峰,中国政法大学博士研究生,Email:cupl\_zf@163.com。

关键词:委托处理;个人信息;从属关系;连带责任

中图分类号:D923;D922.16;D922.294

文献标志码:A

文章编号:1008-5831(2022)04-0203-13

大数据时代,企业经常使用第三方机构来实现其日常活动的一个或多个功能。在欧盟语境下,一些外包活动诸如生成银行账户对账单、由代理人分发保险合同、运作呼叫中心或者人力资源服务,必然包括委托承包商处理个人信息<sup>[1]</sup>。我国商业实践中,委托处理个人信息同样是一种普遍的应用现象。比如,在东芝的隐私协议中,关于“委托处理:本业务中的某些模块或功能由外部供应商提供。例如我们会聘请服务提供商来协助我们提供客户支持”<sup>[2]</sup>。正是基于上述需要,如今许多企业的主营业务为数据、信息的委托处理工作。根据工商资料显示,以通联数据股份公司为例,公司登记经营范围即为“数据处理服务,接受金融机构委托从事金融信息技术、金融业务流程、金融知识流程外包等”。

可以说,委托处理个人信息是信息流动、共享与利用的必然选择,通过分工、合作促进个人信息的合理利用,实现经济价值,更好地服务社会生活。但由于委托处理中,信息处理者并非单一的处理主体,也并非实际地处理个人信息,因此其往往会通过与受托人之间的合同转嫁法定义务的要求,更容易危及信息主体的权益。此时,如何通过事前、事后的规则建构,体系化解决不当的委托处理行为,无疑成为制度运用中亟须解决的重要议题。基于此,《中华人民共和国个人信息保护法》(全文简称《个人信息保护法》)虽在权利义务设置上以信息主体和个人信息处理者(全文简称“信息处理者”)双方关系为蓝本,但还是在第21条为委托处理个人信息提供了规范基础,填补了《中华人民共和国民法典》(全文简称《民法典》)、《中华人民共和国电子商务法》(全文简称《电子商务法》)、《中华人民共和国网络安全法》(全文简称《网络安全法》)等规范空白。不过就该条的规范内容如何解释完善,对委托处理私法规制的目的、对象及方式等要素的具体展开,仍有理论精进之必要。

## 一、委托处理个人信息的规制目的

### (一)解决司法实践的需求

对司法实践进行梳理发现,诉讼中当原告的个人信息权益受侵犯时,信息处理者通常会援引其与第三人之间存在合同或其他交易安排,系由他人造成了损害而与自身的处理行为无关。对此,法院会援引过失相抵等规则让原告承担部分损失,甚至通过举证责任直接驳回其请求,给信息主体的权益保护带来了挑战。

兹举例加以说明:周裕婵在快客公司运营的“KK馆”APP上购物,后向在线客服申请退货,次日接到“售后楚楚”的电话并添加了微信。在微信聊天中,“售后楚楚”将周裕婵的购物详情(包括快递单号、收货人手机、订单信息等)发送给了周裕婵,周裕婵误以为是售后服务人员,被骗支付49990.96元。该案中,快客公司、易得公司辩称未泄露周裕婵的信息,将“售后楚楚”的行为解释为公司将信息一并打包给供应商、快递公司等第三方,不排除是供应商、快递公司泄露了周裕婵的信息。法院虽判决网络运营者应当对其收集的用户信息严格保密,并建立健全用户信息保护制度,对因用户信息泄露导致的损失应当承担一定的责任。但同时认为消费者在进行网络购物时,因疏忽

大意受骗,应当自行承担部分损失<sup>①</sup>。在类似案件中,受制于行为主体的多元化以及处理行为的复杂性,使原告很难证明哪一环节造成了实际损害。实践中,困囿于举证责任上的困难,不少法院认定信息主体没有举证证明被告侵犯了个人信息权益,并据此以信息主体对侵权构成要件承担客观证明责任为由,驳回了其诉讼请求<sup>②</sup>。

## (二) 充分保障信息主体权益

信息主体在委托处理中处于不利地位,使权益保护成为私法规制的基点。无论是委托处理内部合同,还是对信息主体的责任承担,均要受此牵制。也就是说,对于委托处理而言,只有充分、合理地保障了信息主体的信息权益,才能充分发挥其制度功能。

一方面,对于信息主体的权益保护,能够避免大数据背景下数据处理的“丛林法则”。事实上,伴随着技术的发展演进,与个人相关的数据被无限制应用,通过关联算法、图谱分析和数据挖掘技术等工具,精准定位个人信息的新型侵权手法更加突出,危害结果更加多样化且程度更为严重<sup>[3]</sup>。

另一方面,对于信息主体的法律保护而言,事后救济不再是“万能钥匙”,事前的法律规制手段更为重要。在委托处理中,由于信息处理者将个人信息委托给受托人进行处理,借助受托人进行深度挖掘、二次挖掘等,实现了经济利益最大化,但同时,也大大增加了个人信息被泄露、篡改、丢失的风险,可以说,每一次委托背后行为主体和处理过程的增加乃使信息主体受损害的可能性随之提高。此时,通过合同事前规范处理进程、加强监督同样是控制风险的绝佳方式。

综上所述,委托处理相较于单一处理者处理个人信息,更加凸显了保护信息主体的必要性。实际上,合理确定信息主体的权益保护范围,也就划定了信息处理者的处理标准和行为界限,在此区间内进行数据处理利用,最终实现正向激励。

## 二、委托处理与共同处理之间的关系

作为多数人处理个人信息的方式,《个人信息保护法》第20条、第21条分别规定了“共同处理”与“委托处理”。因此,作为对委托处理进行私法规制的基础论证,必须对委托处理中各方关系进行厘清,区分《个人信息保护法》第20条和第21条之间法律关系的异同。共同处理个人信息的法律关系如图1所示,委托处理个人信息的法律关系如图2所示。

### (一) 内部法律关系的差异化

信息处理者与受托人构成了委托处理的内部法律关系。根据《个人信息保护法》第21条第1款“个人信息处理者委托处理个人信息的,应当与受托人约定……”,可以发现,信息处理者作为信息处理的行为主体和责任承担者,将信息主体的个人信息委托给受托人进行“处理”,此时其所委托的不限于物理上的处理活动,而是包括收集、存储、打标签、用户画像、数据分享、跨境传输等所有处理行为<sup>[4]</sup>。在此层面,委托处理与共同处理在内部法律关系上存在本质差异。

<sup>①</sup>参见:广东省深圳市中级人民法院(2019)粤03民终3954号民事判决书。

<sup>②</sup>参见:广东省深圳市南山区人民法院(2016)粤0305民初8160号民事判决书;云南省昆明市盘龙区人民法院(2015)盘法民初字第936号民事判决书;广州铁路运输中级法院(2017)粤71民终11号民事判决书;广州铁路运输第二法院(2016)粤7102民初385号民事判决书。

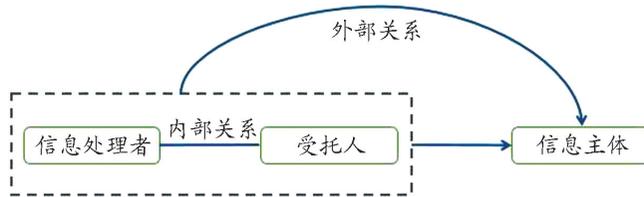


图1 共同处理个人信息的法律关系图

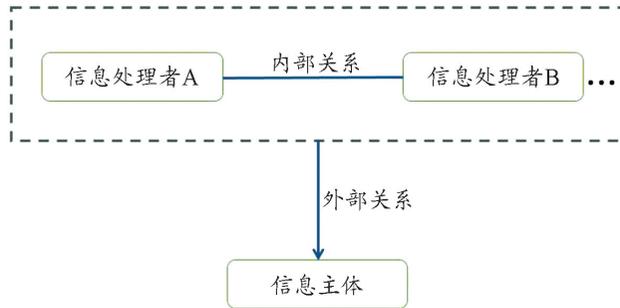


图2 委托处理个人信息的法律关系图

根据《个人信息保护法》第20条规定,共同处理最核心的特征在于“两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式”,而委托处理则源自“控制—处理”的二分法。其中,2018年《欧盟通用数据保护条例》(General Data Protection Regulation, GDPR)第4章专门就“控制者和处理者”加以规定。GDPR下的“控制者”(controller)指的是“那些决定(不论是单独决定还是共同决定)个人数据处理目的与方式的自然人或法人、公共机构、监管机构或其他实体”;而数据处理者(processor)是指为数据控制者处理个人数据的自然人或法人、公共机构、监管机构或其他实体。2018年德国《联邦数据保护法》(BDSG)第46条规定委托处理(Auftragsverarbeitung)同样采此区分。由于《民法典》和《个人信息保护法》统一使用“信息处理者”概念予以涵盖,因此,GDPR中的“处理者”概念在《个人信息保护法》中只能由“受托人”指代之。

至此,本文认为,虽然《个人信息保护法》第21条第2款明确信息处理者与受托人之间为“委托合同”所羁绊,但委托关系并未触及委托处理安排的核心。根据《民法典》第919条,受托人接受委托处理委托人之事务,皆为委托关系所涵盖,针对具体情况,委托处理第三人事务时,可能构成个人提供劳务、雇佣或承揽等,甚至可能构成教唆、帮助他人侵权。因此,委托处理个人信息作为一种具有特定意蕴的交易安排,此种委托应当进一步理解为“从属关系”。所谓“从属”表明由信息处理者决定信息处理的目的、方式,受托人可以独立行事,但只能按信息处理者的指示行事<sup>③</sup>。可见,相较于单纯的委托而言,从属关系包含着信息处理者对受托人更多的控制,使得受托人的工作非常有限<sup>[5]</sup>。在此背景下,信息处理者与受托人之间的委托合同,其目的仅在解决受托人的处理权限,实现信息处理者对受托人的补偿与追偿。

除此之外,上述结论也导致委托处理与共同处理在法律后果上的不同。针对共同处理,《个人信息保护法》第20条第2款规定信息处理者共同处理个人信息时,应当就损害承担连带责任。而《个人信息保护法》第21条所规范的是,信息处理者允许服务提供商受托处理个人数据,但这些服务提供商却不对数据处理的目的和方式拥有任何决策权。因此,在责任承担上需进行特殊考量(后

③BeckOK DatenschutzR/Spoerr, 34. Ed. 2020, BDSG § 62 Rn. 9.

文详述)。

## (二) 外部法律关系的同质性

实证法下对“处理者”采广义概念,只要实际对个人信息进行了处理,无论何种处理类型,均在处理者项下受到规制,不必区分受托人与否。此时,信息处理者与受托人,作为“处理者”,与信息主体构成了外部法律关系。对于信息主体而言,委托处理与共同处理在外部法律关系上具有一致性,均由内部关系上的所有处理者共同组成、共同负责。

关于外部法律关系的性质,学理上,张新宝教授主张以“两头强化,三方平衡”理论为基础,即在强化个人敏感信息基本人格权保护的同时,又强化个人一般信息经济价值的利用<sup>[6]</sup>。而王利明教授则认为《民法典》第1035条明确了处理个人信息的基本原则,该规范构建出权利人与信息处理者之间的基本权利义务框架<sup>[7]</sup>。对此,本文认为,信息处理者与信息主体之间处于单项拘束关系,这种拘束性表现为信息主体请求信息处理者为或不为特定的信息处理行为,而单向性则突出这种请求仅信息主体得以主张,反之不然。

其一,实证法对信息主体的信息权益予以充分保护,这种保护更多地体现为对信息处理者处理活动的限制或禁止。由于个人信息处理并非一个一次性同时开展的过程,而是发展为两个阶段:第一阶段是个人信息收集及第一次使用;第二阶段是个人信息增值应用<sup>[8]</sup>。衡诸《民法典》《网络安全法》及《个人信息保护法》,均完整地展现了信息主体的两阶段救济图像。在信息收集阶段,告知同意原则成为信息主体权益保障的第一道屏障,其要求信息处理者在收集个人信息之时,应当对信息主体就有关个人信息被收集、处理和利用的情况进行充分告知,并征得信息主体的明确同意<sup>[9]</sup>。因此,商业企业在收集用户个人信息时,不能简单地以告知同意原则作为任何情况下不当收集个人信息的合格抗辩<sup>[10]</sup>。在第二阶段,权利行使成为信息主体权益保障的第二道屏障。《民法典》第1037条列举了信息主体的查阅(复制)权、更正权、删除权等具体人格权能,信息主体可通过援引第995条以下条款主张权益保护。为此,上述两阶段构成了对信息处理活动的正当、必要限制。

其二,信息处理者虽在特定情况下可以豁免处理个人信息之违法性,但这并不构成对单向拘束的突破。《个人信息保护法》第13条基于履行法定职责、应对突发事件、实施新闻报道等特殊需要,赋予信息处理者一定的信息处理自主权。不过,上述事由仅构成信息处理者处理个人的违法性阻却,无法成为信息处理者拘束信息主体的正当化依据。例如,为准确评价个人信用状况,可使用直接用户画像,但用于推送商业广告目的时,则宜使用间接用户画像。再比如,将所收集的个人信息用于学术研究或得出对自然、科学、社会、经济等现象总体状态的描述,属于与收集目的具有合理关联的范围之内;但对外提供学术研究或描述的结果时,应当对结果中所包含的个人信息进行去标识化处理。总之,即便信息处理者可以在特定情况下不经信息主体同意处理信息,但仍应当以合法、正当的方式进行,遵循诚信原则<sup>④</sup>,同时,还需限于实现处理目的的最小范围,不得进行与处理目的无关的个人信息处理<sup>⑤</sup>。

个人信息保护法旨在确保公平、透明地处理个人信息,从根本上授予信息主体以权利,并对处理个人数据的信息处理者施加义务<sup>[11]</sup>。此时,委托处理安排并不影响单向拘束关系的存在。信息处理者

<sup>④</sup>参见:《个人信息保护法》第5条:处理个人信息应当遵循合法、正当、必要和诚信原则,不得通过误导、欺诈、胁迫等方式处理个人信息。

<sup>⑤</sup>参见:《个人信息保护法》第6条:处理个人信息应当具有明确、合理的目的,并应当与处理目的直接相关,采取对个人权益影响最小的方式。

作为委托人,可以移转一部分的处理权限或职能于受托人,但其仍然负责遵守数据保护法规,而受托人也应当尽到谨慎义务,采取必要措施保障个人信息的安全,并协助信息处理者履行法定义务。可以说,个人信息保护规则体系中的“信息处理者”可以涵盖从事个人信息处理的所有行为主体<sup>[12]</sup>。在此,内部关系上的所有行为主体共同对外部的信息主体负责,无需考察具体交易构造。

### 三、委托处理过程中信息主体的权益保障

为确保内部和外部责任的透明分配,受托人的处理行为应当由与信息处理者之间的合同或其他具有拘束力的法律行为所涵盖<sup>[13]</sup><sup>1084</sup>。因此,委托处理过程中,有必要通过合同予以事前、内部规制。为此,《个人信息保护法》第21条就合同内容、法定义务和转委托三种情况加以规定,以下分别展开讨论。

#### (一)法定的必备条款

对于委托处理内部的合同内容,究竟是赋予当事人更多的意思自由,还是课以更多的行为标准,值得思考。对此,本文认为,基于保护信息主体的要求,合同应当具备法定的必备条款。

第一,法定必备条款是保护信息主体的需要。由于信息处理者与信息主体之间处于法定拘束关系,这种法定拘束旨在保障信息主体的合法权益,同时也划定了信息处理者的行为边界。在此基础上,当信息处理者将处理活动通过合同交由受托人完成时,合同内容的强制性在于贯彻该价值考量:保护信息主体。否则,信息处理者会通过内部合同以“架空”实证法对其的法定拘束。

第二,法定必备条款是落实内部从属性的要求。在委托处理个人信息中,信息处理者交由受托人完成一些处理活动,并非亲力亲为。在此,完备的合同条款将保障内部从属性得以实现。一方面,通过合同内容明晰双方的处理界限、权利义务、保护措施等,更有利于确定二者的职责划分,实现信息处理者对受托人活动的监督;另一方面,若处理过程中收集、存储、使用等环节损害了信息主体的权益,合同内容将成为责任分配的标尺,一旦信息处理者或者受托人由于他人的过错承担了赔偿责任,借助合同内容可实现内部追偿权的合理化。

第三,法定必备条款与国际主流立法接轨。域外经验上,关于信息处理者与受托人之间的合同内容,皆列举了诸多必要条款。例如,GDPR第28条规定处理者的处理应当受某类合同或其他欧盟法与成员国法的约束,这类合同或法律应当规定处理者相对于控制者的责任、主体事项、处理期限、处理性质与目的、个人数据的类型、数据主体的类型以及控制者的责任与权利。同时,该款建议此类合同或法律尤其应当对如下情形作出规定,并列举了8种具体事项。BDSG第62条第5款列举了处理的目的、处理时间、类型和目的、数据主体的类别以及负责人的权利和义务等,另外就9项特殊事项加以考虑。目前,德国、丹麦等国家的数据保护监管机构也已制定出标准合同条款,可供企业参考使用<sup>[14]</sup>。

因此,信息处理者与受托人之间的合同应当包含必备条款以确保受托人合法处理数据,并且信息处理者可以检查受托人是否遵守这些规定。相较于《个人信息保护法》第20条由内部主体约定各方的权利义务,第21条第1款详细列举了委托处理的目的、期限、处理方式、个人信息的种类、保护措施以及双方的权利和义务等事项,是值得肯定的立法选择。

#### (二)受托人的法定义务

《个人信息保护法》第21条第2款规定了受托人的两项义务:其一是按照约定处理个人信息,

不得超出约定的处理目的、处理方式等进行处理;其二是在提供和处理服务结束后的返还或删除义务。有实务工作者认为,受托人的上述义务不仅是对委托者的合同义务,还兼具法定义务性质,理由在于,个人信息的委托处理关系通过处理者与受托人之间的协议构建,双方权利义务的具体内容由双方通过协议约定<sup>[15]</sup>。对此,本文持否定观点,认为上述义务仅构成受托人的法定义务。

一方面,法定义务要求信息处理者与受托人之间必须就个人信息的处理目的和处理方式达成一致,且受托人应当严格遵循。之所以将二者视为合同必要之点,原因在于信息处理者是决定处理过程中某些关键要素的主体,需一并确定处理的目的和方式,即决定处理的原因和方法。此时,可以由受托人实施一些更实际的方面,但处理目的和方式必须由信息处理者决定。根据 GDPR 第 28 条第 10 款、BDSG 第 62 条第 7 款的经验,如果系受托人自主确定处理的目的与方式,则在本次处理中被视为控制者。其背后的价值判断在于:根据指定的标准进行信息处理,使受托人接受信息处理者的指示,这也是从属关系的规范内涵<sup>⑥</sup>。因此,法定义务强调受托人需依指示处理,不得超出处理目的和方式,即便合同未规定,受托人仍受此拘束。在此基础上,如何理解本款“等”字,则应当满足信息处理者控制职能的需要。个案中,如果双方看重敏感信息的处理权限,则信息的“种类”便可纳入“等”内解释,成为受托者的法定义务。

另一方面,法定义务旨在确保在“与处理有关的服务提供”结束后,个人信息将受到适当的保护。对此,《个人信息保护法》规定该义务产生于“委托合同不生效、无效、被撤销或者终止”等所有服务结束情形,并强调受托人“不得保留”。作为受托人的一项法定义务,在此表明无论是合同权利义务终止还是效力瑕疵,也无论该后果是否可归责于受托人,信息处理者有权决定在服务结束后如何处理个人信息,即可以在处理开始前通过书面合同或者即时的书面通知确定是否返还或删除。不过,合同或其他法律行为应当反映信息处理者在服务提供结束之前更改选择的可能性,法条规定的“返还或删除”也说明了这种选择权原则上应当由信息处理者享有。如果信息处理者选择删除个人数据,则受托人还应当确保以安全方式执行删除操作,以符合《个人信息保护法》第 50 条处理个人信息的安全规定。同时,基于诚信原则,受托人还应当向信息处理者确认“删除”已在约定的时限内完成,并且除非法律要求进一步存储,否则受托者必须删除所有现存数据副本。

另外,作为类型化工具,《个人信息保护法》第 21 条款仅积极列举了受托人要依约处理个人信息、事后返还或删除,并未勾勒出受托人法定义务的全貌。为此,还需借鉴 GDPR 和域外立法例的规则,考虑信息本身的经济价值,确认受托人在处理过程中具有保密的义务,即消极的不作为。对此,本文认为,解释上可适用《民法典》第 509 条第 2 款、第 558 条之规定,肯定在委托处理关系中,受托人需履行法律上的适当保密义务。

### (三) 适用委托合同的特殊性

在从属关系上,信息处理者需监督受托人妥善处理;在法定拘束关系上,受托人需延续对信息主体的权益保护。因此,处理个人信息下的内部合同,即便采用委托合同形式,在规则适用上也具有一定的特殊性。

#### 1. 转委托规则

基于这种高度人身性的信任关系,在委托合同场合,受托人原则上没有转委托的权利。《个人

<sup>⑥</sup>Gola/Heckmann/Paschke/Scheurer, 13. Aufl., 2019, BDSG § 62 Rn. 23.

《个人信息保护法》第21条第3款同样确认了这一规则。不过,该规则绝非对《民法典》第923条的重述,其仍有独特之处。

首先,在法条的语词结构上,前者使用“未经……同意,受托人不得转委托他人处理个人信息”。而后则规定“应当亲自处理……。经……同意,可以转委托”,即便未经同意,委托人仍可以事后“追认”以补正转委托的权限瑕疵。故在体系解释上,受托人转委托他人处理个人信息时,有义务在打算参与或更换第三人之前通知信息处理者,事先得到其书面批准,不能事后追认<sup>⑦</sup>。其次,即便信息处理者事先正确地表示同意,在责任分配上与单纯的委托合同仍具有显著差异。《民法典》第923条明确转委托经同意或追认的,受托人仅就第三人的选任及其对第三人的指示承担责任。学理上通常认为,该责任为过错责任,如果受托人对第三人的选任或指示没有过失,委托人只能请求第三人承担责任<sup>[16]</sup>。而对于前者,宜认为,即便经过信息处理者同意,如果第三人未能履行根据《个人信息保护法》所承担的义务,受托人仍对信息处理者承担履行此类义务的责任。最后,针对紧急转委托,《民法典》第923条创设了例外规则。不过,该规则同样不能适用于委托处理个人信息。原因在于处理事务标的的特殊性,在应然状态下不能仅仅“为了维护委托人的利益”而放弃对信息主体权益之维护,故处理个人信息情形下应当排除任何受托人主动转委托的可能性。

## 2. 告知同意规则

在信息处理者与信息主体二元关系下,信息处理者处理个人信息需取得个人同意,且这种同意与信息处理者充分告知这一前提牢牢绑定,难以分离。在委托处理中,坚守告知同意规则具有正当性,但适用中究竟由谁履行告知义务?依据委托合同的一般法理,受托人实际处理事务,仅由其告知即可。但本文认为,需以信息处理者和受托人双重告知为基础,取得信息主体对信息收集、处理以及对信息处理者转委托之同意。

其一,理论上,信息收集的告知同意规则应当适用于所有个人信息处理的行为,而不仅限于个人信息的初次处理行为<sup>[7]</sup>。从信息主体的角度看,委托处理个人信息实际也是对个人信息的收集、处理行为,该行为同样受到告知同意规则的调整。其二,在技术上要求所有主体的同意,具有可行性。如学者所言:“信息社会的高级段智能社会已经到来,在收集、处理信息的各个环节取得信息主体同意,在技术上是可行的;所有的信息处理者处理个人信息都需要经过信息主体同意,不会增加成本,也不会形成数据流动的障碍。”<sup>[17]</sup>其三,从我国司法实践来看,已有法院采纳上述立场。例如,在“北京淘友天下技术有限公司等与北京微梦创科网络技术有限公司不正当竞争纠纷案”中,双方当事人通过 OpenAPI 开展合作,但被告在合作过程中不当抓取原告的用户个人信息。在该案中,北京知识产权法院提出三重授权规则,即用户授权+平台授权+用户授权,合作开发模式中数据提供方向第三方开放数据的前提是数据提供方取得用户同意<sup>⑧</sup>。

总之,在个人信息处理中,同意是最核心的要件,于委托处理场合,仍应当严格恪守。《个人信息保护法》第21条未就此明确加以规定。法律适用上,可类推适用《个人信息保护法》第14条第2款的规定,要求信息处理者重新取得个人同意。积极确信上,上述法律理由均旨在保障信息主体对本人事务自决之行为,亦是判定企业能否处理用户行为信息的关键节点。消极确信上,目的、方式

<sup>⑦</sup>Paal/Pauly/Gräber/Nolden, 2. Aufl., 2018, BDSG § 62 Rn. 5.

<sup>⑧</sup>参见:北京知识产权法院(2016)京73民终588号民事判决书。

及种类变更,与实际处理者之变更,其不同之处不能排除这种法定评价。故二者在法律评价有决定性意义的方面一致,应当被相同评价。

### 3. 适当性任命及监督规则

在委托合同项下,委托人基于自身信任而选择受托人,受托人的忠实、智力、能力等客观情况系为委托人处理事务所匹配,委托人享有绝对的选择自由。同时,为解决信息不对称,实证法配置受托人遵守指示<sup>⑨</sup>、报告<sup>⑩</sup>和转交<sup>⑪</sup>等义务,以保障委托人的权益。不过,由于涉及信息主体的权益保护,信息处理者在委托处理场合应当强化对受托人的选择与监督。

一方面,在委托处理时,信息处理者应当履行适当性任命义务,并非自由选择受托人。此时,信息处理者只能任命可以采取适当技术和组织措施以符合法律要求的受托人,且信息处理者需在调试之前了解(潜在)受托人可用的选项,在处理数据之前对受托人进行审查。对此,在张新宝教授主持的个保法专家建议稿中,明确称其为信息处理者的适当性任命义务<sup>[18]</sup>。《个人信息保护法》第55条也建立了个人信息保护影响评估制度。

另一方面,信息处理者作为委托人,其还负担一定的监督义务,例如对受托人的能力进行定期测试。在BDSG的规范框架下,所需能力测验的范围不应当以抽象和一般的方式确定,而应当单独确定。信息处理者必须定期(但不是永久性地)审查处理者对数据的处理,委托处理的程度,受影响者的潜在风险、创新程度、处理数据的敏感性以及委托所涉及法人实体的能力差异等<sup>⑫</sup>。对此,《个人信息保护法》第21条第1款后段明确指出“对受托方的个人信息处理活动进行监督”。

综上,为了保护信息主体的信息权益,信息处理者与受托人之间的适当性任命和监督规则是必要的。该规则不仅有别于委托合同的一般做法,还确保了受托人正确、合适地履行职责,遵守个人信息保护法规。可以说,对个人信息的私法规制而言,预防性措施较于事后救济或追偿更为关键。

## 四、委托处理个人信息的责任承担规则

一直以来,有学者主张:“建构健全的权利救济制度对信息主体至关重要。”<sup>[19]</sup>可见,当委托处理安排造成信息主体权益受损害时,责任承担规则作为事后、外部的救济手段,有助于促使信息处理者适当履行义务。

### (一) 责任承担方式

如果存在《个人信息处分协议》的约定,对个人的信息自决权利以违约责任方式提供法律救济是理想的救济方式。然而,实践中个人信息处理往往不依赖于协议,如公共场所的图像采集,自动化决策等场合,信息主体无法主张合同救济。不过,由于一切个人信息均属侵权法的保护范围,因此通过侵权规则事后规制委托处理是正确的救济方向<sup>[20]</sup>。

为此,《个人信息保护法》第69条规定了损害赔偿责任。同时,借助《民法典》规范实现体系拓展。在《民法典》视域下,信息主体的权益救济,不仅可以通过人格权编加以解决,还可以通过侵权

<sup>⑨</sup>参见:《民法典》第922条:受托人应当按照委托人的指示处理委托事务。需要变更委托人指示的,应当经委托人同意;因情况紧急,难以和委托人取得联系的,受托人应当妥善处理委托事务,但是事后应当将该情况及时报告委托人。

<sup>⑩</sup>参见:《民法典》第924条:受托人应当按照委托人的要求,报告委托事务的处理情况。委托合同终止时,受托人应当报告委托事务的结果。

<sup>⑪</sup>参见:《民法典》第927条:受托人处理委托事务取得的财产,应当转交给委托人。

<sup>⑫</sup>BeckOK DatenschutzR/Spoerr, 33. Ed. 2020, BDSG § 62 Rn. 30.

责任编辑进行兜底保护。司法适用中,人格权编中的救济规制仅限于要求侵权人停止侵害、排除妨碍、消除危险等所谓自我救济措施,超出该范围,涉及损害赔偿等属于侵权责任编任务<sup>[21]</sup>。具体到委托处理情形,信息主体对其个人信息保护既可以提起基于支配权(权益)的请求,也可以在个人信息受到侵害后提出损害赔偿请求。前者包括停止侵害(删除、屏蔽、断开链接等)、更正不实个人信息、保障个人信息的真实性、完整性和安全性等,后者包括精神损害赔偿和附带的财产损失赔偿<sup>[22]</sup>。

## (二) 连带责任规则适用

上述论述虽解决了信息主体的救济方式,但委托处理本质上为多数人侵权,故对责任主体方面还应当进行特别考虑。相较于《个人信息保护法》第20条明确共同处理个人信息下的法律责任,《个人信息保护法》第21条并未规定信息处理者与受托人之间如何进行责任划分,构成法律漏洞。为消解委托处理中责任主体不明的救济困境,应当通过连带责任规则实现信息主体的权益救济。

所谓连带责任的前提是,至少有两个机构参与才能证明造成的损害。在委托处理下,信息处理者和受托人就损害对外承担连带责任是为了促进因果关系的证明:请求权人不必证明因何人的行为充分损害了其个人信息<sup>③</sup>。其核心价值判断在于,保障信息主体获得救济的权利不能因为人工智能(委托处理)的应用而减损。不过,区别于共同处理中多个信息处理者共同决定处理目的和方式,具有整体性效果,其效果即为连带,委托处理场合中连带责任的特殊性表现为在因果关系上举证责任的转换。个案中,如果信息处理者或受托人能够证明损失的事件是由对方导致的,那么其责任便可以免除。如此,也激励了委托处理内部协商的精细化,更好地明确各方的行为界限。

因此,在漏洞填补上,应当类推适用《民法典》第1170条的规定,要求在信息处理者与受托人参与同一处理行为造成损害时,每个信息处理者都应当对损失负有连带责任,除非能够证明损害确实是由对方引起的除外。

其一,连带责任规则符合主流的域外立法。其中,GDPR第82条第4款规定,每个控制者或处理者都应当对损失负有连带责任,以确保对数据主体进行有效赔偿,这一规定可以看作是《欧盟基本权利宪章》第47条所规定的基本权利以及第8条规定个人数据保护权获得有效司法保护的结果<sup>[13]1967</sup>。BDSG第83条第3项同样规定:“在个人信息的自动化处理场合,如果无法查明数个参与处理的控制者中谁造成了损害,则每一控制者或者权利行使者均负有责任。”此时,信息主体无法了解公共数据处理内部发生的情况,应当将风险置于所有责任机构身上,是他们之间的互动使信息主体的证据复杂化。巴西2018年《通用数据保护法》第42条、印度2018年《个人数据保护法》第75条等立法也采此规则。

其二,连带责任的法律基础在于共同危险行为。学理上,有学者支持复数处理人场合下的因果关系推定,适用共同危险行为<sup>[23]</sup>。对此,从属关系为共同危险的适用提供了坚实的基础。一方面,因从属关系的存在,信息处理者决定了信息处理的方式、目的等,受托人系按照信息处理者的指示开展处理行为。从信息主体的角度观之,信息处理者并未在委托后脱离处理过程,受托人更是实际处理了个人信息,二者作为处理者共同创设了权益侵害的危险。另一方面,信息处理者通过数据处理获得了财产收益,受托人亦基于内部委托合同获得补偿,二者作为危险的受益者,理应承担控制

<sup>③</sup>BeckOK DatenschutzR/Quaas, 33. Ed. 2020, BDSG § 83 Rn. 30.

危险的责任<sup>⑭</sup>。不过,考虑处于从属地位的受托人保护,此时的连带责任不同于共同处理下的连带责任<sup>⑮</sup>,后者的法律基础在于共同侵权,二人同为侵权人,共同承担责任。而委托处理中,信息处理者和受托人仅为共同危险人,能够确定的是损害事实由数人的危险行为所致,但无法确定具体是由哪个或者哪几个人的行为所致。故受托人若能证明损害确实是由委托人的指示所引起,不承担赔偿责任,反之亦然。

其三,连带责任的适用需借助追偿权予以优化。诚然,“对数据主体进行充分有效的补偿”是任何补偿措施的目标。但是,应当允许信息处理者或受托人对处理所造成的损害,内部按比例分配赔偿。对此,GDPR第82条第5款规定,当控制者或处理者已经根据第4段的规定对所受损失进行全额赔偿,该控制者或处理者可以按照第2段所规定的条件,要求另一控制者或处理者返还其造成的那部分损失。因此,在信息处理者和受托人涉及同一处理时,即便对外承担连带责任或者一方无法通过举证来完成责任的豁免,鉴于二者内部存在合同拘束,可通过追偿权将损害风险在内部实现重新分配,以实现公平正义。

## 五、结语

委托处理个人信息是大数据时代的常见现象,为此,《个人信息保护法》第21条专门进行规定,具有重要的实证法意义。实践中,信息处理者会通过其与受托人之间的合同转嫁法定义务的要求,危及信息主体的权益,构成了私法规制的核心任务。在事前的规制手段上,应当要求委托处理关系内部合同以法定必备条款,课以受托人依指示处理、返还或删除、保密三项法定义务。同时,在转委托、告知同意以及适当化任命与监督规则上应当进行特殊考虑。在事后的规制手段上,《个人信息保护法》第21条并未规定委托处理的责任承担规则,实为法律漏洞。针对个人信息权益受损害时,信息主体如何进行事后救济这一问题,法律适用上应当借助《民法典》第1170条共同危险理论,通过因果关系的转换,更好地实现信息主体的权益保护。

### 参考文献:

- [1] KRZYSZTOFEK M. GDPR: General Data Protection Regulation (EU) 2016/679: Post-reform personal data protection in the European Union[M]. Holland: Kluwer Law International BV, 2018: 148.
- [2] 东芝(中国)有限公司. 个人信息收集、使用同意书[EB/OL]. [2021-02-17]. [http://www.toshiba.com.cn/service/personal\\_home/agreement.html](http://www.toshiba.com.cn/service/personal_home/agreement.html).
- [3] 王晓锦. 人工智能对个人信息侵权法保护的挑战与应对[J]. 海南大学学报(人文社会科学版), 2019(5): 126-134.
- [4] 齐爱民, 张哲. 识别与再识别: 个人信息的概念界定与立法选择[J]. 重庆大学学报(社会科学版), 2018(2): 119-131.
- [5] 克里斯托弗·库勒. 欧洲数据保护法: 公司遵守与管制[M]. 旷野, 杨会永, 译. 北京: 法律出版社, 2008: 74.
- [6] 张新宝. 从隐私到个人信息: 利益再衡量的理论与制度安排[J]. 中国法学, 2015(3): 38-59.
- [7] 王利明. 民法典人格权编的亮点与创新[J]. 中国法学, 2020(4): 5-25.
- [8] 何俊志, 孙婧婧. 个人信息应用的保护设计与实证进路: 基于《民法典》同意原则的博弈分析[J]. 贵州社会科学, 2020

<sup>⑭</sup>参见: 北京市朝阳区人民法院(2018)京0105民初36658号民事判决书。

<sup>⑮</sup>参见: 《个人信息保护法》第20条: 两个以上的个人信息处理者共同决定个人信息的处理目的和处理方式的, 应当约定各自的权利和义务。但是, 该约定不影响个人向其中任何一个人个人信息处理者要求行使本法规定的权利。个人信息处理者共同处理个人信息, 侵害个人信息权益造成损害的, 应当依法承担连带责任。

(9):74-81.

- [9] 齐爱民. 信息法原论:信息法的产生与体系化[M]. 武汉:武汉大学出版社,2010:76.
- [10] 张新宝. 个人信息收集:告知同意原则适用的限制[J]. 比较法研究,2019(6):1-20.
- [11] ZUIDERVEEN BORGESIJUS F J. Improving privacy protection in the area of behavioural targeting[M]. Holland:Kluwer Law International BV,2015:303.
- [12] 郭北南. 个人信息的民事法保护与救济[J]. 国家检察官学院学报,2021,29(2):151-161.
- [13] KUNER C, BYGRAVE L A, DOCKSEY C, et al. The EU General Data Protection Regulation (GDPR): A Commentary[M]. New York:Oxford University Press,2020:1084,1967.
- [14] 陈际红,蔡鹏,韩璐,等. EDPB《GDPR下数据控制者及数据处理者概念的指南》解读兼谈《个人信息保护法(草案)》关于处理者的定义[EB/OL]. (2020-11-17) [2021-02-11]. <http://www.zhonglun.com/Content/2020/11-17/1408315833.html>.
- [15] 袁立志,潘舒然. 关于个人信息保护法草案的七个疑问[EB/OL]. (2020-11-09) [2020-12-24]. <http://www.jingtian.com/Content/2020/11-09/1729311245.html>.
- [16] 崔建远. 合同法[M]. 第6版. 北京:法律出版社,2016:442.
- [17] 王洪亮. 《民法典》与信息社会:以个人信息为例[J]. 政法论丛,2020(4):3-14.
- [18] 张新宝,葛鑫. 《个人信息保护法(专家建议稿)》重磅首发[EB/OL]. (2019-10-17) [2021-03-15]. <https://www.civillaw.com.cn/gg/t/?id=36127#>.
- [19] 肖少启. 个人信息法律保护路径分析[J]. 重庆大学学报(社会科学版),2013(4):119-126.
- [20] 叶名怡. 个人信息的侵权法保护[J]. 法学研究,2018(4):83-102.
- [21] 尹志强. 侵权法的地位及与民法典各编关系的协调[J]. 华东政法大学学报,2019(2):25-40.
- [22] 张新宝. 《民法总则》个人信息保护条文研究[J]. 中外法学,2019(1):54-75.
- [23] 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[J]. 法学家,2020(4):29-39,192.

## Civil law regulation of entrusted processing of personal information

CAO Mingde, ZHAO Feng

(Civil, Commercial and Economic Law School, China University of  
Political Science and Law, Beijing 100088, P. R. China)

**Abstract:** Entrusted processing of personal information is an inevitable option of information flowing, sharing, and using. Article 21 of the Personal Information Protection Law (PIPL) specifically provides a regulatory basis for entrusted processing of personal information, filling the normative gaps of the Civil Code, the Electronic Commerce Law and the Network Security Law. However, how to interpret and apply the regulatory content of this article, and the specific development of the purpose, objects, methods and other elements of the entrusted processing still needs to be improved through interpretation. In judicial practice, information processors often cite the existence of contracts or other transaction arrangements with a third party, in which the damage is caused by others rather than their own processing behaviors, which brings challenges to the protection of the rights and interests of information subjects. This is the core of civil law regulation of entrusted processing. As the basic argument of private law regulation of entrusted processing, the legal structure of entrusted processing is different from joint processing, in which there is a subordinate relationship between the information processor and the entrusted party. The information processor decides the purpose and method of processing, and the entrusted party can process the personal information only as instructed by the information

processor. In order to better safeguard the rights of information subjects, the internal contract of entrusted processing relationship must include mandatory provisions to ensure that the entrusted party legally processes data and the information processor can check whether the entrusted party has complied with these provisions. Compared with Article 20 of the PIPL which stipulates the rights and obligations of each party shall be agreed upon by an internal person, Article 21. 1 that lists in detail the purpose, duration, and method of the entrustment, types of personal information, protection measures as well as the rights and obligations of the parties is a positive legislative choice. In accordance with Article 21. 2 of the PIPL and the general rules of foreign law, the entrusted party shall bear three statutory obligations, including process as instructions, return or deletion, and keep confidentiality. In addition, the general rules of entrustment contracts cannot apply to sub-entrustment, notification of consent, as well as appropriate appointment and supervision, which are for the purpose of ensuring that the entrusted party can correctly and appropriately perform its duties and comply with the regulations on the protection of personal information. As for the assumption of liability of the parties, Article 69 of the PIPL provides for the liability for damages. Meanwhile, the system is expanded by relying on the norms of the Civil Code. Therefore, the remedy of the rights and interests of the information subject can not only be solved through the Personality Rights Part, but also be protected through the Tort Liability Part. However, Article 21 of the PIPL does not provide for the division of responsibilities between the information processor and the entrusted party, which constitutes a legal loophole. In order to alleviate the relief predicament of liability subject, the rights relief of the information subject should be realized through joint and several liability rules. Specifically speaking, the theory of joint dangerous acts may be used, and by analogy the provisions of Article 1170 of the Civil Code may be applied, which requires the information processor and the entrusted party to be jointly liable for damages in the same transaction, unless it can be proved that the damages are actually caused by the other parties.

**Key words:** entrusted processing; personal information; subordinate relationship; joint liability

(责任编辑 袁虹)