主题研讨

# 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

周光权

**内容提要:**《个人信息保护法》第21条对个人信息处理者委托处理个人信息时双方的权利义务作出相应规定。就刑事司法而言,在第三方受委托处理信息、数据共享过程中,大数据相关应用技术给放贷方提供了金融数据支撑和风险防控服务,金融平台如果缺乏这些支持,其在反欺诈、风险防控业务运作上势必会面临极大考验。当委托人是灰色领域的从业者时,个人信息取得未必符合知情同意要求,且如果其对受托人处理后的个人信息使用不当,委托处理个人信息的委托人、受托人都有涉罪可能,但罪与非罪的界限并不明晰。对此,需要对个人信息保护法的相关规定以及侵犯公民个人信息罪的保护法益、客观构成要件等进行仔细梳理,从而对刑事司法实务和企业合规提供指导。考虑到委托处理个人信息时受托人的义务相对较轻,受托人的业务具有中立性特征,在受托人采取了合理保护措施的前提下,不宜轻易认定其构成侵犯公民个人信息罪。

**关键词:**委托处理个人信息　侵犯公民个人信息罪　委托合同　刑法谦抑性

周光权,清华大学法学院教授。



《中华人民共和国民法典》第111条规定,“自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的,应当依法取得并确保信息安全,不得非法收集、使用、加工、传输他人个人信息,不得非法买卖、提供或者公开他人个人信息。”为其提供保障的是作为“最后手段”和“二次性法”的刑法。《刑法》第253条之一规定了侵犯公民个人信息罪,行为人违反国家有关规定,向他人出售、提供或者非法获取公民个人信息,情节严重的,即构成侵犯公民个人信息罪。法律保护的社会利益是多元的,其保护手段也是多种多样的,而刑罚手段具有局限性,所以刑法并没有保护所有社会利益的功能与效力。对于侵犯公民个人信息行为而言,刑法的惩罚和民法、行政法的保护之间相互协调、形成合力,在运用行政法或民法予以保护即为已足的场合,刑法并不需要出面。换言之,在实务中,并

不是定罪越多越好,而是处罚越妥当越好。所以,刑法的介入也需要寻找适当的时机,遵守适当的界限。

委托处理个人信息,是指个人信息处理者将处理个人信息的事务委托给其他组织和个人,双方成立委托合同关系,一方是委托人,另一方是受托人,由受托人为委托人处理个人信息的情形。委托人可以特别委托受托人对某一种类的个人信息实施某种处理活动(如仅仅是储存或者加工),也可以委托受托人对某些种类的个人信息实施多种处理活动(如既储存,同时也加工、分析等)。[1] 对此,《个人信息保护法》第 21 条明确规定:"个人信息处理者委托处理个人信息的,应当与受托人约定委托处理的目的、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,并对受托人的个人信息处理活动进行监督。受托人应当按照约定处理个人信息,不得超出约定的处理目的、处理方式等处理个人信息;委托合同不生效、无效、被撤销或者终止的,受托人应当将个人信息返还个人信息处理者或者予以删除,不得保留。未经个人信息处理者同意,受托人不得转委托他人处理个人信息。"

实践中,在民事领域,因委托处理个人信息引发民事争议的情形大量存在,但解决相对容易,因为民法典合同编对委托合同及其履行有详尽规定,将《民法典》第 919 条至第 936 条的相关规定与《个人信息保护法》第 21 条相结合,准确理解委托合同的成立条件,就能够为民事案件的解决提供指引。但是,在刑事领域,当委托人是"灰色领域"(如高利放贷、"套路贷"等)的从业者时,信息来源正当性存疑;或者当委托人、受托人对委托处理的个人信息使用不当时,双方罪与非罪的界限不清,此时就容易出现争议。由此可见,刑事和民事领域的个人信息委托处理无论从表现形式或是认定难度上都存在一定程度的差异。基于此,本文结合《个人信息保护法》的相关规定及立法精神,对个人信息处理者委托处理个人信息时的刑法界限,尤其是侵犯公民个人信息罪的适用问题进行分析,以期对刑事司法实务和企业合规有所裨益。

## 一 刑事司法视野中的委托处理个人信息

### (一)委托人将个人信息委托给关联公司处理的情形

在委托处理个人信息案件中,如果委托人和受托人之间存在关联关系,甚至可以对其作一体性评价时,对行为性质的认定相对容易,因为在委托人非法获取个人信息的场合,其将个人信息委托、提供给关联公司或者下属公司处理时,受托人对于个人信息未取得合法授权通常具有概括的认识,甚至事前参与了非法获取个人信息的过程,因此,在委托人非法获取个人信息构成侵犯公民个人信息罪时,受托人也应构成本罪。

例如,被告人开发、运营维护"七天贷"等多款贷款 APP 以及信审云系统、信贷管理云系统、资产保全系统,在被害人登录并使用上述 APP 后,该 APP 要求被害人登记借款人姓名、手机号码、住址、紧急联系人等基本信息,并利用借款人急于用钱的心理,要求借款人

〔1〕 参见程啸著:《个人信息保护法理解与适用》,中国法制出版社 2021 年版,第 201 页。

必须上传通讯录。后被告人将在实施网络借款业务过程中非法获取的52万余名借款人身份证、手机号码等信息以及157万余条紧急联系人的姓名、与借款人关系、手机号码等信息提供给专门成立的催收公司，由后者利用上述信息，开展催收活动。〔2〕在这种情况下，被告人获取借款人之外的紧急联系人的姓名、手机号码以及通讯录信息的，按照《个人信息保护法》第14条的规定，应该取得每一个信息主体单独同意，因此，被告人该获取信息的行为是非法的。在同一非法放贷犯罪组织中，将贷款发放公司和催收公司分设，形成不同的独立法人，催收公司看似受委托处理个人信息，实质上却与非法放贷的犯罪人之间存在行为上的相互配合和犯意上的联络，因此，将委托处理个人信息的放贷者和负责催收的个人信息处理受托者视为一体就是言之成理的，受托人对于委托人非法获取信息不知情、信息获取行为得到被害人同意等辩解，都应当予以驳回。这种表面上看似存在个人信息委托处理的情形，其实质是个人信息处理者自己非法处理个人信息，实务中对此要实现准确定罪难度不大，因此不予赘述。

（二）委托人将个人信息委托给他人处理时的刑事风险

近年来，小额贷款公司、第三方数据服务公司以及在线直播平台等APP应用软件大多涉及未经用户同意就收集、使用用户个人信息的问题。其中，许多公司通过各种手段收集个人信息以后，难以对信息进行处理，往往需要将海量信息委托给没有关联关系的第三方进行处理。在这个过程中暗藏着许多法律风险，可能涉及对个人信息权利的侵犯，从而进入刑法规制的范围。

**1. 刑事领域常见的个人信息委托处理情形**

一种是金融机构进行放贷和催收的情形。在一些小额贷款公司贷款案件中，放贷人一方面在放贷时为降低风险，将借款人的个人信息提供给技术服务商、数据支撑服务商、征信服务公司等进行验证，以确认借款人的还款能力和诚信程度；另一方面在催收时为实现债权，将获取的个人信息交给独立运作的专门化催收公司，由其组织进行催收。因此，在发放贷款以及催收过程中，都涉及个人信息委托处理问题，需要厘清刑事责任。大数据运用对于产业发展十分重要，在第三方受委托处理信息的过程中，大数据的提取、应用给贷款发放提供了金融数据、风险防控方面的服务，一旦缺乏这些技术及数据支持，这些小额贷款公司在反欺诈以及风险防控等业务运作上会面临极大的考验，尤其是如果缺少数据抓取等技术提供风险控制方面的支持，一些现金贷公司和消费金融公司就必须考虑降低放贷额度，甚至只能停止其业务，因为一般的经营性公司很难有大额资金投入去开发一个数据处理和风险控制系统，其催收业务也难以开展。

但是，在信息来源多样化，受托人经营活动并不规范的情形下，委托人和受托人的刑事责任确定并非易事。例如，某网贷公司为提升催收成功率，按逾期时间长短分为不同等级，将催收业务外包给其他不同催收公司的催收员并在其内部网络平台上为其他催收公司员工开通账号和查询权限，催收员即可登录网贷公司网站后台查看被害人身份信息、人脸视频认定、银行卡信息、手机联系人、通话记录、贷款及还款情况等，以此为据实施非法

〔2〕 参见江苏省镇江市中级人民法院（2020）苏11刑终107号刑事裁定书。

催收。[3] 在本案中,某网贷公司委托催收公司处理个人信息,受托人明知其接受的个人信息中有大量涉及其他权利主体的个人信息并未获得单独同意,但是,受托人为牟取非法利益,在明知受委托处理的个人信息中有违反知情同意规则获取的情形下,仍然按照委托人的要求处理该信息的,构成侵犯公民个人信息罪的共犯。此外,当金融机构将贷款申请人的个人信息交由第三方数据公司开展个人信用验证合作时,如果受托人缓存数据,或者将海量数据予以非法出售、提供的,也可能存在刑事风险。

另一种是征信机构收集、处理公民个人信息的情况。经过特殊许可开办的合法征信机构也需要通过数据外包的方式与征信服务公司发生业务往来,从而出现信息委托处理的情形。由于合法征信机构在调取、留存公民信息方面有其便利性,与其合作的征信服务机构很容易获得、缓存大量数据。在这些征信服务机构中,有的是获得有关部门备案开展企业征信和批准开展个人征信业务准备事务的机构,有权从事个人和小微企业信用状况评估,在其受托处理个人信息的业务中如果掺杂违规业务,其违法性难以被及时发现,也不易被认定。一旦受托人基于不法目的处理这些信息,就产生了刑事责任问题,有的数据公司非法将公民身份认证端口出售或非法缓存公民身份数据等行为,都极易造成大面积个人信息泄露。例如,2015 年 3 月以来,某征信服务有限公司提供身份证照片“查询返照”业务获利数千万元,侦查机关在其公司的服务器中查获并收缴被非法获取、缓存的公民姓名、身份证号、照片等接近 1 亿条公民个人信息,这些信息包括手机号、姓名、身份证号和家庭地址等。该征信服务有限公司从上游公司(合法征信机构)获取网络接口后又违规将该查询接口出卖,并非法缓存公民个人身份信息,供下游公司(委托人)查询牟利,从而造成公民身份信息(包括身份证照片)大量泄露,该案被告人被指控犯有侵犯公民个人信息罪。[4]

上述涉刑事领域将个人信息委托给第三方处理的场合,违法和犯罪交织乱象的存在,要求刑法学对此有所回应。

**2. 个人信息委托处理可能涉及的刑法问题**

对相关行为的刑法评价涉及到如何确定侵犯公民个人信息罪的法益。由于现行法律体系中涉及个人信息保护相关的法律法规很多,刑法作为所有法律的最后保障法,必须要以法益为工具限定或合理确定犯罪的处罚范围,杜绝刑事政策的任意性,以及前置法的宽泛无边。[5] 目前学界对个人信息保护法益的争论点主要在于“超”个人与否。[6] 个人法益观认为本罪的保护法益是公民个人信息权,超个人法益观认为公民个人信息关系社会

〔3〕 参见甘肃省兰州市红古区人民法院(2020)甘 0111 刑初 38 号刑事判决书。

〔4〕 参见杨仕省、肖玉婷:《考拉征信涉“黑利益链”侵犯个人信息,公众隐私谁来保护?》,《华夏时报》2019 年 11 月 21 日第 8 版。

〔5〕 参见刘艳红:《侵犯公民个人信息罪法益:个人法益及新型权利之确证——以〈个人信息保护法(草案)〉为视角之分析》,《中国刑事法杂志》2019 年第 5 期,第 20 页。

〔6〕 具体争论可参见曲新久:《论侵犯公民个人信息犯罪的超个人法益属性》,《人民检察》2015 年第 11 期;黎宏著:《刑法学各论》(第二版),法律出版社 2016 年版;于冲:《侵犯公民个人信息罪中“公民个人信息”的法益属性与入罪边界》,《政治与法律》2018 年第 4 期;刘艳红:《侵犯公民个人信息罪法益:个人法益及新型权利之确证——以〈个人信息保护法(草案)〉为视角之分析》,《中国刑事法杂志》2019 年第 5 期;马永强:《侵犯公民个人信息罪的法益属性确证》,《环球法律评论》2021 年第 2 期;欧阳本祺:《侵犯公民个人信息罪的法益重构:从私法权利回归公法权利》,《比较法研究》2021 年第 3 期等。

公共利益、国家安全乃至于信息主权，所以具有超个人法益属性。〔7〕虽然侵犯公民个人信息罪规定了“违反国家有关规定”，但是，从侵犯公民个人信息罪的条文设置以及相关司法解释、行政法规的规定来看，侵犯公民个人信息罪的保护法益仍然是公民的个人信息自决权，不能因为对个人信息要进行公法规制就否定个人信息之上所承载的民事权益。〔8〕而且，在刑法章节设置上，侵犯公民个人信息罪被设置于刑法分则第四章的“侵犯公民人身权利、民主权利罪”一章，而非第六章的“破坏社会管理秩序罪”之中，从体系解释的角度来看，侵犯公民个人信息罪的保护法益应当与本章其他罪名保持协调。从刑法第253条本身的体系编排上看，侵犯公民个人信息罪作为刑法第253条之一，其保护法益也应与侵犯通信自由罪和私自开拆、隐匿、毁弃邮件、电报罪相协调，理应将公民的个人法益作为侵犯公民个人信息罪的主要保护法益。

对侵犯公民个人信息罪保护法益为何的争论，直接影响到本罪构成要件符合性和违法性的判断，进而决定了本罪犯罪圈的大小，这又进一步制约着个人信息或个人数据控制与共享之间此消彼长的态势。〔9〕

数据共享最关键的问题在于，在充分尊重数据主体权利的前提下，数据控制者可以在多大范围内共享数据。〔10〕在网络借贷等场景下，信息主体并不知道被共享的数据范围，也无法控制其个人信息的流向，因而存在极大的隐私忧虑。在涉刑事领域信息委托处理案件中，基本的产业链运作模式为：委托人（下游公司如金融机构）提供其获得或处理的个人信息，提出信息查验等业务需求，从受托人（如大数据公司、征信服务公司）那里获得信息服务，包括购买查询接口，或将信息提供给受托人，受托人利用自身的数据库或者将有关信息转交给更上游的公司（如合法征信机构、身份证采集或管理机构等）进行比对、验证，受托人在得到确定的验证信息后再返回给委托人。上述将个人信息委托他人处理的情形涉及多个环节，实务中指控和判定相关行为人的难度都很大。

实践中，涉案较多的个人信息委托处理典型场景是：受托人通过连接下游客户（委托人）的业务需求和上游数据源提供的数据分析产品，协助下游客户获得上游数据源提供的数据分析产品，以便于客户对信贷用户信息进行验证，为审核用户的信贷申请提供风险控制和反欺诈服务。例如，受托人乙公司通过连接下游客户甲公司的业务需求和上游数据源丙公司提供的数据分析产品，根据委托人甲提供的特定个人信息主体的查询关键字，识别特定主体的欺诈风险，协助甲公司获得上游数据源丙公司提供的数据分析产品，以便于委托人对信贷用户信息进行验证。此时，受托人乙公司提供的主要是智能风险控制、智能信用审查等服务，包括反欺诈、信用评估、风险监控预警和智能催收等。

在上述运作模式中，个人信息处理者甲公司和受托人乙公司约定，甲公司委托受托人乙公司通过一定的输出方式，提供欺诈甄别规则，受托人乙公司接受委托后，为识别特定

〔7〕 参见曲新久：《论侵犯公民个人信息犯罪的超个人法益属性》，《人民检察》2015年第11期，第5－6页。

〔8〕 参见程啸：《论个人信息处理者的告知义务》，《法治论丛（上海政法学院学报）》2021年第5期，第68页。

〔9〕 参见欧阳本祺：《侵犯公民个人信息罪的法益重构：从私法权利回归公法权利》，《比较法研究》2021年第3期，第55页。

〔10〕 参见王利明：《数据共享与个人信息保护》，《现代法学》2019年第1期，第47页。

主体的欺诈风险，再与上游丙公司签订特定输出方式调用服务协议，约定乙公司基于反欺诈目的向丙公司提供来自于委托人甲公司，且经过信息主体合法授权的数据信息，丙公司基于大数据算法，出于反欺诈目的向乙公司提供欺诈可能性反馈（欺诈指数），提供杜绝或降低欺诈行为发生的数据运算服务，即反欺诈服务，乙公司在甲公司与丙公司之间提供信息传输服务（将甲公司提供的用户信息传递给丙公司核验，再将丙公司的核验结果反馈给甲公司）。在这里，由于拥有上游数据源的最上游公司大多是资质合格、合法经营的主体，基本不涉及民事及刑事责任承担问题，值得关注的是作为委托人的下游公司（甲公司）和作为受托人的大数据公司（乙公司）各自的刑事责任边界。

目前，值得探讨的问题主要有：（1）在处于下游的甲公司的信息来源不合法时，甲乙的刑事责任如何确定？（2）在甲公司与受托人乙公司合作过程中，甲在无授权的情况下，利用数据接口产品获取、非法缓存海量公民个人信息（包括公民姓名、身份证号、地址、电话、信用积分甚至行踪轨迹等），再与其他终端不法互联网公司签订销售合同，非法提供个人信息或予以出售。此时，受甲公司委托处理个人信息的乙公司作为上游公司，如果其在与乙公司签订个人信息委托处理时对乙的行为有所约束，是否也应构成侵犯公民个人信息罪？（3）受托人缓存或不当使用委托人提供的信息时，刑事责任如何确定？这些都涉及到对侵犯公民个人信息罪保护法益的判断，以及对行为性质、犯罪故意的准确认定等问题。在当前的办案实践中，针对个人信息委托处理的复杂情形，无论是委托人还是处于受托人地位的法人，都有被以侵犯公民个人信息罪追究刑事责任的情形，由此也引发了一些争议，这说明从刑法视角切入个人信息委托处理问题有其独特意义。



## 二　委托处理个人信息中委托人的刑事责任

### （一）委托人的法律责任概说

在民事领域，上述个人信息委托处理相关规定的实现都是以委托主体是合格的、没有瑕疵的信息处理者为前提的。对于委托人而言，最不可能产生民事和刑事风险的信息处理委托行为应当是：委托人按照“告知—同意”规则获得、处理个人信息，就个人信息委托处理与受托人约定委托处理的目的、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，并对受托人的个人信息处理活动进行监督，确保受托人按照约定处理个人信息，在委托合同不生效、无效、被撤销或者终止时，接受受托人及时返还的个人信息，或者要求受托人予以删除。[11] 如果委托人在获取信息环节没有“硬伤”，即便其与受托人发生纠纷的，也仅产生民事责任。

### （二）委托人的个人信息来源及其刑事责任

正如文章第一部分所讨论的，实践中，个人信息委托处理的委托者也有承担刑事责任的风险。在委托处理个人信息过程中，委托人才是个人信息的处理者，因为个人信息处理

〔11〕 国家市场监督管理总局、国家标准化管理委员会 2020 年发布的《信息安全技术　个人信息安全规范》（GB/T35273-2020）第 9 条第 1 款详细规定了委托处理个人信息控制者委托第三方处理个人信息时的标准和监督义务。

的目的和处理方式都是由该主体自主决定的,[12]受托人只是依据委托合同的约定,按照委托人所决定的处理目的和处理方式对个人信息进行处理,该信息及其处理事务就是委托合同的标的。对于该信息的性质,按照《个人信息保护法》第21条的规定,显然特指符合知情同意要求、来源合法的个人信息。但是,在实务中,涉刑事案件的个人信息委托处理的委托人往往在获取(处理)个人信息环节的行为就存在明显法律瑕疵,那么,后续将个人信息再委托给其他数据公司、催收公司处理的行为就势必延续其非法性。

如前文所述,如果将侵犯公民个人信息罪的保护法益定位为公民个人的信息自决权,就比较容易解决实践中委托处理个人信息的委托人在个人信息处理多个环节中是否成立侵犯公民个人信息罪的判定问题。例如,"套路贷"、小额贷平台的贷款发放团伙从某些科技公司非法购买、交换个人信息,再借助于这些信息寻找网络贷款客户的,显然不属于按照"告知—同意"规则处理个人信息。此时的个人信息处理者和买卖公民个人信息数据产业链上的其他行为人(包括爬虫数据公司,以及其他作为金融风险专项整治对象的大数据公司),因其实施了非法获取公民个人信息的行为而构成侵犯公民个人信息罪的共犯。再比如,有的信息处理者故意曲解"告知—同意"规则,非法获取公民个人信息。例如,被告人在发放贷款过程中,要求借款人提供除本人之外很多其他个人的身份信息(包括紧急联系人、亲属等),这种获取信息的行为具有违法性。又如,被告人虞某在被告人庄某的提议下,决定由其出资,纠集被告人邱某、林某等人共同研发APP网络放贷软件,在APP注册过程中,通过程序非法获取借款人通讯录、通话记录等信息,上传至后台服务器,用于风险控制和逾期后催收。逾期后,催收人员会采取电话滋扰、辱骂、威胁、短信"轰炸"及发送侮辱性图片等"软暴力"手段,对借款人及其亲友进行催收。[13]

在上述案件中,被告人(信息处理者)均会辩解其在处理个人信息,以及后续委托催收公司处理个人信息时,已经履行了告知义务,且征得了权利人(借款人)的同意,因而不构成犯罪。但是,被告人的这一辩解很难成立,其获取个人信息以及委托处理个人信息的行为都不具有正当性。如果被告人确实在发放贷款时仅要求借款人本人提供其个人信息,该辩解言之成理。但是,被告人在借款人本人信息之外还要求其提供其他紧急联系人的身份信息以及通讯录,则侵犯了其他自然人的个人信息自决权,属于对以电子方式记录的与自然人有关的已识别或者可识别信息的非法获取,当然有成立本罪的可能。

此外,在委托人提供给受托人的信息极为有限,反过来必须从受托人手中购买更多个人信息内容的情况下,委托人的行为也涉嫌违法。例如,被告人闫某、牛某、王某借用甲公司之名为乙公司等从事催收服务的公司提供"失联信息修复业务",并从中获利。受委托处理个人信息的丙公司被告人张某、黄某、李某将修复的15万余条公民通讯信息出售给甲公司,甲公司又将上述信息出售给乙公司等,法院认定被告人闫某、牛某、王某、张某、黄某、李某违反国家有关规定,向他人出售公民个人信息,情节特别严重,均已构成侵犯公民个人信息罪。[14]对于本案,如果仅考虑国民的处罚直觉和"体感治安",认定被告人构成

〔12〕 参见龙卫球主编:《中华人民共和国个人信息保护法释义》,中国法制出版社2021年版,第340页。

〔13〕 参见江苏省泰州市中级人民法院(2020)苏12刑初18号刑事判决书。

〔14〕 参见山东省诸城市人民法院(2020)鲁0782刑初113号刑事判决书。

犯罪似乎是没有疑问的。但是,在委托人委托被告人“修复失联信息”过程中,对委托合同是如何约定的,受托人是否有从事该业务的权限,委托人提供的信息内容如何,特别是受托人借助于何种数据“修复失联信息”,其数据是否来源于合法的征信机构或公开获取的大数据等问题的回答,对刑事上确定被告人的行为性质起到关键作用。实践中,受托人借以“修复失联信息”的相关个人信息通常是通过非法手段爬取或者窃取的,其应当构成侵犯公民个人信息罪,委托人非法获取经受托人加工、“修复”信息的,也应当构成本罪。

(三)委托人利用交易机会擅自获取受托人信息及其刑事责任

在委托处理个人信息场合,信息处理者与受托人之间一般会订立委托合同,并约定委托合同的具体内容。从《个人信息保护法》第 21 条的规定来看,立法者是将“委托处理的目的、期限、处理方式、个人信息的种类、保护措施”与“双方的权利和义务”分开规定的,这主要是考虑到“前者涉及个人信息权益的保护,这些约定即是委托方与受托方对‘委托事务’的具体约定,也是法律规定的义务,因此,它们属于个人信息处理者委托他人处理个人信息所成立的委托合同中必须具备的条款”。〔15〕 如果委托人和受托人双方都根据第 21 条的规定,严格按照该委托合同的约定履行权利义务,是不会发生侵犯个人信息后果的,但是,实践中,极易出现与刑事案件有关联的情形。例如,个人信息处理者作为委托人,其与受托人之间在委托合同条款中虽然明确约定了委托公司调用受托公司网络接口前,应当取得特定信息主体的授权,并且还会特别约定未经受托公司同意,委托公司不得将受托公司提供的产品、服务以及输出的结果向任何第三方提供等内容,但是,在实际履行委托合同过程中,委托人违背了这一义务要求,利用委托信息处理的机会获取、使用超过其提供给受托人的额外的公民个人信息,此时就有涉罪可能性。之所以会出现这种情况,通常是由于委托人和受托人的计算机信息系统接口处于对接状态,双方具有一定信任关系,在委托处理个人信息过程中,如果委托方及其工作人员违背约定或者实施欺诈行为,在未经受托人同意的情况下擅自调用受托人网络公司接口,获取大量受托人公司所拥有的信息,原本处于提供个人信息地位的委托人就成为非法获取他人信息的行为人,其可能构成侵犯公民个人信息罪。例如,某些“套路贷”公司将借款人的姓名、手机号码提供给他人,委托他人处理个人信息实施催收行为,在发现受托人催收不力时,反复调用受托人公司网络接口获取借款人亲友的人脸识别信息,并直接对被害人亲友进行跟踪、滋扰,就属于恶意破坏受托公司保护措施的情形,其作为公民个人信息的非法获取者,有成立侵犯公民个人信息罪的可能性。

## 三 委托处理个人信息中受托人的刑事责任

(一)受托人的法律责任概说

“委托合同订立的目的是为委托人的利益,委托人选择受托人是基于对受托人的信任。在委托事务的处理过程中,具体应当如何处理,取得何种结果才最符合委托人的利益,

〔15〕 参见程啸著:《个人信息保护法理解与适用》,中国法制出版社 2021 年版,第 205 页。

委托人有权决定,自然也有权对受托人发出相关指示。"[16]委托处理个人信息时,受托人的首要义务是完成个人信息处理者所委托的具体事项。对此,《民法典》第922、923条规定了变更委托人指示和转委托情况下的同意原则和例外。个人信息保护法中则明确规定了受托人的义务,并要求其依照该法和有关法律、行政法规的规定,采取必要措施保障所处理的个人信息的安全,并协助个人信息处理者履行本法规定的义务。2020年《信息安全技术　个人信息安全规范》第9条第1款也规定了受托者在处理委托要求中应当遵循的规则。[17]

总体而言,现有的民法和行政法相关法律法规对于委托处理个人信息时受托人承担何种民事责任是相对比较清晰的。例如,如果受托人在委托合同被撤销后,仍然缓存、保留委托人之前提交的个人信息的,就违反了《个人信息保护法》第21条,但如果其缓存、保留数据仅用于实现与委托人对账及异议核查这一维护自身商业利益的特定目的,保存期限根据客户(委托人)"账期"的差异而有所不同,但未将其销售或非法提供给他人,也没有证据证明其实施了超出特定信息主体授权的行为,委托人和受托人之间的纠纷就仅仅停留在民事委托合同争议的范围内,受托人缓存或保留委托人相关数据的行为不构成侵犯公民个人信息罪。

(二)受托人可能成立犯罪的常见情形

在实务中,受托人涉嫌犯罪的情形大致可分为以下几种情况:(1)受托人在与个人信息处理者合作的过程中,违反合同约定,故意留存部分数据,再把这些数据转手倒卖给消费信贷公司,甚至是"套路贷"公司,导致公民个人信息泄露或被滥用。这种情况下,受托人构成侵犯公民个人信息罪自无疑问。(2)委托人提供的信息来源明显未经个人同意,受托人与委托人之间从未签订书面委托合同,受托人难以提供公民个人信息认证,处理产业链上涉及委托人的重要协议,且对于委托人的信息来源合法性完全不予审查,在发现个人信息来源明显存疑时不进行质疑和审核就接受并处理这些信息。这种行为的性质极有可能属于非法获取公民个人信息的范畴。(3)受托人虽然要求委托人提供公民个人对信息处理的授权,但在授权人数与实际处理的公民个人信息数量之间存在明显悬殊时仍然处理信息。这种行为也有成立侵犯公民个人信息罪的可能。(4)受托人从委托人处获取的信息极其有限,通过自己的努力非法收集个人信息后出售牟利。这种行为也可能成立侵犯公民个人信息罪。例如,被告人赖某应客户的要求,将其从客户中得知的公民身份证号码、姓名等发送给同伙帮忙查询上述公民的对应照片,再将上述照片通过"三色技术"制成动态人脸验证视频后贩卖给客户从中获利,法院以侵犯公民个人信息罪判处赖某有期徒刑1年2个月。[18] 本案中,被告人作为受托人,即便其从委托人那里获得个人信息

〔16〕 黄薇主编:《中华人民共和国民法典释义》(中),法律出版社2020年版,第1638页。

〔17〕 根据第9条第1款的规定,受委托者应当遵循以下几点规则:(1)严格按照个人信息控制者的要求处理个人信息。(2)受委托者确需再次委托时,应事先征得个人信息控制者的授权。(3)协助个人信息控制者响应个人信息主体的合理请求;(4)受委托者在处理个人信息过程中无法提供足够的安全保护水平或发生了安全事件的,应及时向个人信息控制者反馈;(5)在委托关系解除时不再存储相关个人信息。

〔18〕 参见广东省东莞市第二人民法院(2020)粤1972刑初4287号刑事判决书。

是否合法难以查明,但其未经个人信息主体同意,查询、获取他人照片并非法加工成人脸识别数据后出售的行为,属于对公民个人信息的侵害。(5)受托人接受委托后,为完成受托任务,使用非法获取的他人账户密码、人脸信息等个人可识别信息后非法侵入计算机信息系统,获取委托人之前并不掌握的被害人支付信息、行踪轨迹等个人信息的,分别触犯侵犯公民个人信息罪和非法获取计算机信息系统数据罪,应数罪并罚。比如,被告人为破解某第三方支付系统对特定账号的限制,在接受他人委托后,未经特定个人信息主体同意,并借助于从公开网络中收集的被害人照片,采用制作被害人 3D 人脸动态图的方式突破了该支付工具的人脸识别认证系统,解除了该账号的限制登录,并通过伪造被害人手持身份证、承诺函照片的方式解除了该第三方支付系统对被害人账户的资金冻结状态,法院认定被告人构成非法获取计算机信息系统数据罪和侵犯公民个人信息罪,对其予以数罪并罚。[19]

综上所述,受托人所从事的获取、提供、出售公民个人信息的行为极有可能违反国家的相关规定,或者违背信息主体的意愿,主要是侵犯了公民对个人信息的知情同意权。"信息主体的知情权是个人信息处理透明原则的基本要求,要求信息处理者以清晰、明确且易懂的方式,告知自然人个人信息处理的相关事项,尤其是有关个人信息处理目的、范围、方法以及时限等重要内容。"[20]民法典和个人信息保护法对知情和同意两方面都进行了规定,构建了一个较为全面的知情同意制度。上述受托人的行为侵犯了公民对其信息的自我决定权,从而可能构成侵犯公民个人信息罪。

(三)受托人可以提出抗辩的理由

为了支持数据外包服务的发展,提高工作效率,鼓励信息委托处理活动,减少对信息主体的不必要干扰,在委托处理个人信息的场合,对信息处理者委托第三方处理个人信息的行为不应当加以限制。[21] 一般来说,对于个人信息初始主体的知情同意权,法律应予以严格保护,但在个人信息利用、流通过程中,个人信息知情同意权的法律保护可逐渐放宽,收集者、利用者的信息权利相应地加以保护,在个人信息主体的隐私权等人格基本权利之外,知情同意可不必采取明示方式,以有利于海量个人信息流通和有效利用。对受托人可能的个人信息利用行为入罪,需要具备"违反国家有关规定"的前置性条件,仅仅违反个人信息知情同意保护的原则性规定,并不足以符合侵犯公民个人信息罪的犯罪构成,还要判断违反了何种前置性法律规范。[22] 与此相关联,受托人处理个人信息时也不需要征得信息主体的同意,且受托人处于接受委托人提供的个人信息的消极地位,法律赋予其个人信息保护义务远轻于委托人,加之受托人利用大数据处理信息的行为带有中性业务行为的性质,因此,对于受托人的行为不宜轻易认定为侵犯公民个人信息罪。实务中,受托人可以提出的抗辩理由大致有以下几方面。

〔19〕 参见成都市郫都区人民法院(2019)川 0124 刑初 610 号刑事判决书。

〔20〕 申卫星:《论个人信息权的构建及其体系化》,《比较法研究》2021 年第 5 期,第 4 - 5 页。

〔21〕 参见马新彦、张传才:《知情同意规则的现实困境与对策检视》,《法治论丛(上海政法学院学报)》2021 年第 5 期,第 101 页。

〔22〕 参见张勇:《APP 个人信息的刑法保护:以知情同意为视角》,《法学》2020 年第 8 期,第 123 页。

**1. 受托人是否有足够理由相信委托人的个人信息来源正当**

《个人信息保护法》第13条规定，除非法律有特别规定，个人信息处理者在取得个人的同意后，方可处理个人信息。《网络安全法》第42条第1款规定，“网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。”由此可见，侵犯公民个人信息罪成立的关键在于“是否未经或者违背了被收集者的同意”，如果受托者所接受的信息事实上获得了被收集者的个人同意，受托人也尽到了应尽的审查义务，就不认为侵犯了公民对其信息的个人法益，不是本罪规制的行为类型，也就不构成侵犯公民个人信息罪。最高人民法院、最高人民检察院2017年5月8日发布的《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（下称“《侵息司法解释》”）第3条第2款规定，“未经被收集者同意，将合法收集的公民个人信息向他人提供的，属于刑法第二百五十三条之一规定的‘提供公民个人信息’，但是经过处理无法识别特定个人且不能复原的除外。”从上述规定不难看出，法律和司法解释都将公民对其信息的自我决定权、处分权作为本罪的保护法益。在公民的个人法益没有被侵犯的情况下，即便行为有违反相关规定之处，也难以构成侵犯公民个人信息罪。

实务中，如果从事金融业务的各类公司作为委托人，其在向受托人申请公民信息认证等委托信息处理行为之前，已取得公民个人的授权或同意的，委托人将其委托给受托人加工处理就是妥当的，受托人有理由相信信息来源正当。如果受托人按照委托人的委托，还需要将该个人信息与其他信息比对，以确定借款人的身份真实性和信用程度，受托人此时往往需要获得上游机构（如公民身份证号码查询服务机构、征信部门等）的公民个人信息。如果上游机构之前实施的业务行为没有违反被收集者的个人同意，受托人根据其与上游机构的协议，可以在一定范围内提供公民个人信息比对服务，在此范围内，受托人为委托人处理个人信息，将委托人提供的信息与上游机构存储的信息进行核查和比对，并将特定公民个人信息的真实性、诚信度等查询结果告知委托人，其处理及反馈给委托人的信息并未实质超越委托人提供的信息范围，受托人不应当构成侵犯公民个人信息罪。故而，对于多数情形下处于中间环节的受托人而言，其实施的涉及公民个人信息的业务行为如果获得了公民的授权同意，并未违背公民个人意志的，其行为不符合侵犯公民个人信息罪的客观要件。

但是，这也并不意味着当委托人处理相关个人信息不具有合法性基础时，受托人的行为就一定非法。由于受托人不是直接面对信息主体的个人信息处理者，只是按照委托人的要求行事，因此，其对信息来源正当性的审查义务势必轻于委托人，个人信息保护法也并未要求个人信息处理的每一环节都必须直接面向该特定主体取得授权，因此，当受托人与委托人签订合同，整体业务链条以委托人取得特定信息主体对其信息进行验证、处理的授权为基础，受托人处理信息的正当性基础就被奠定。受托人只要能够足以相信客户（委托人、个人信息处理者）取得了授权，其受委托后处理信息的行为也就被认为是符合法律要求的。

所以，即便是在委托人非法收集个人信息的场合，也并不能立即得出受托人的行为也

违法的结论，因为有些信息处理行为可能带有中性业务行为的性质。对于中性业务行为是否应当犯罪化的问题，在网络犯罪领域有很多讨论，尤其是《刑法修正案（九）》增设帮助信息网络犯罪活动罪以后，对于如何判定网络服务提供者刑事责任的问题争议不断。近年来，中立行为犯罪化的司法演进态势为，司法上从追究不独立的共犯责任到追究不完全独立的正犯责任，对网络空间中的中立帮助行为，尤其是提供本身中立的技术的行为，进行了犯罪化处理：客观上追究正犯责任，主观上针对单方明知。〔23〕但是理论界并没有达成这样的一致意见。有学者指出，并非任何为他人的信息网络犯罪提供互联网技术支持或者广告推广、支付结算等帮助行为都属于中立帮助行为，是否认定为犯罪，需要符合“情节严重”的要求，所以需要运用危险分配原理，通过法益衡量和期待可能，确定中立业务行为的责任范围，如果不符合情节严重的要求，则原则上不承担刑事责任。〔24〕也有学者认为，由于网络中立业务的特殊性，在网络服务平台的日常业务过程中，鲜有证据可以证明平台提供的技术支持具有促进他人犯罪的主观意思，更遑论网络服务提供者与犯罪实行行为人之间的意思联络，所以可以采用“大半数规则”进行判断，即如果从后台的电子数据可以表明网络服务平台所服务的对象中，利用信息网络实施犯罪活动的占全部服务对象的比重超过半数以上，就可以推定中立业务服务提供者为明知。〔25〕

在委托信息处理的情形中，按照《个人信息保护法》第 21 条的规定，受托人有一定义务关注委托人是否取得个人对于信息处理的授权。实务中，要认定受托人构成侵犯公民个人信息罪，也必须查明委托人取得授权的相关情况。如果没有证据证明委托人未取得授权，要认定受托人构成侵犯公民个人信息罪就缺乏基本的事实依据；更进一步，在委托人的个人信息属于非法获取时，受托人也完全有可能做无罪辩解。例如，在从事“套路贷”业务的甲公司委托乙大数据公司处理的个人信息中，既有得到被害人同意的部分，也有非法收集的个人信息，但委托人甲伪造了部分个人授权声明材料交给乙公司，由于信息委托处理的业务是海量的，乙公司在接受信息时无法一一甄别信息来源的合法性，也不可能在后续受托处理个人信息过程中，在各个环节再去逐一核实委托人是否事先取得特定信息主体的同意，〔26〕对于这样的中性业务行为就不能按照帮助犯来定罪处罚。因为，在实践中，大量委托处理个人信息的委托人均为企业法人，且绝大多数系经依法批准开设的金融机构，委托人本身就有合理的反欺诈需求，在其与个人开展交易活动时，往往已通过签订书面协议、电子合同、电子点击等方式获取特定信息主体对于验证、处理以及委托处理个人信息的同意，因此，在委托人提供的个人授权材料中即便存在虚假内容，只要没有明显异常，受托人在正常业务活动中难以辨明其虚假性，或者无其他证据证明受托人明知委托人未取得个人授权的，就难以认定受托人个人信息获取及处理行为的非法性。因此，

〔23〕 参见郭旨龙：《网络中立行为犯罪化的反思与重构——以英美的理论和实务为比较》，《江汉论坛》2020 年第 7 期，第 103 页。

〔24〕 参见张明楷：《论帮助信息网络犯罪活动罪》，《政治与法律》2016 年第 2 期，第 13－15 页。

〔25〕 参见刘宪权：《网络黑灰产上游犯罪的刑法规制》，《国家检察官学院学报》2021 年第 1 期，第 15 页。

〔26〕 参见周光权：《中性业务活动与帮助犯的限定——以林小青被控诈骗、敲诈勒索案为切入点》，《比较法研究》2019 年第 5 期，第 35 页。

即便对那些接受“套路贷”公司委托,且委托人提供的个人信息中有部分信息未得到信息主体同意的,对为其处理个人信息的受托人也不能轻易认定为侵犯公民个人信息罪的行为人。

**2. 受托人的业务行为是否违反国家相关规定**

构成侵犯公民个人信息罪,以行为违反国家有关规定为前提。目前,国家并未对受托处理个人信息的相关业务经营资格进行特别限制,受托人只需要取得互联网信息服务业务经营许可证,具备通过互联网提供信息服务的合法资质开展活动,即属于合法经营。比较特殊的情形是个人征信业务,这要求行为人取得特别许可,否则就具有非法性。但是,实务中,受托人处理的大量信息虽与个人的信用信息相关,但并不是个人征信业务,不属于必须取得特定许可方可经营的业务。征信业务的基本特点为对信用信息进行采集、处理并对外提供个人信用信息。如果受托人从事的数据处理业务是根据个人信息进行核验的业务,即根据受托人数据库里的信息,或者受托人有权调用的上游征信机构的信息,再参考、结合其他公开信息,对委托人提供的基础信息进行验证、比对,该信息处理行为就是仅针对受托人提供的既有信息,并不会产生或提供委托人并不掌握的全新个人信息内容。此外,征信业务具有实现债权人共享信息的功能,征信机构获得信息后,有权向提供信息主体之外的人员提供已经获得的信息,从而使该类信息具有一定的通用性、公共性。但是,受托人接受委托后的个人信息处理业务完全是基于委托人的特定化需求展开的,由委托人向受托人传输的信息仍然属于委托人,受托人只能按照委托人的要求处理个人信息,而无权擅自处理,更无权向委托人之外的其他主体提供这些信息,该个人信息不具备公共属性。受托人通过与上游合法数据源签订合同的方式获取有关数据开展信息处理业务,再将委托人主动提供的信息与上游机构的信息进行核验、比对的,显然谈不上违反了国家有关规定,因此,几乎所有的受托人所从事的个人信息处理业务,尤其是数据核验业务都不属于个人征信业务,不需要取得个人征信业务许可,相关业务行为属于法律所允许的市场行为。

**3. 受托人与委托人之间是否就权利义务作出清晰约定**

一方面,在受托人与委托人之间已经通过协议约定委托人必须保证信息来源真实性、合法性、自愿性的前提下,通常可以认为受托人已经尽到了应尽的审查义务。在委托人向受托人证明其已经取得了被收集者的授权之后,受托人无须再对信息来源进行实质审查,因此,委托合同对于双方权利义务的明确约定能够为受托人的无罪辩护提供支撑,即便委托人构成侵犯公民个人信息罪,受托人也无须对委托人的犯罪行为负责。

由于大数据行业的特殊性和当前技术水平的局限,受托人不必也不可能在事前对每一份授权都进行实质审查。只要受托人在开展业务活动过程中已经保持了审慎义务,司法实务中就不应以委托人行为的违法直接推导出受托人也存在侵犯公民个人信息的主观故意,否则就会对受托人赋予过多的法律义务。受托人作为大数据业务从业者,并非行政或司法监管部门,其与委托人的权利义务关系完全建立在双方合同约定的基础之上,受托人并不具有对下游客户(委托人)进行实质监管的权限和手段。此时,可以认为受托人连监督过失都不存在,更难以认定其具有侵犯公民个人信息的犯罪故意。此时的受托人义

务只不过是根据委托合同所履行的对委托人所提供个人信息已获得个人授权的形式审查义务,不应对委托人可能涉嫌的侵犯公民个人信息行为负责。

在实务中,特别值得注意的是,如果委托合同的当事双方不仅明确约定了委托人要对信息来源的自愿性、合法性负责,还约定了更多的义务,则对受托人定罪就更需要谨慎。例如,委托人为督促受托人履行取得用户授权的义务,专门设立了授权码制度,根据该制度设计,委托人在每一次发起请求并传输个人信息之前,均需要提交数十位数且具有唯一性的授权码,受托人通过该授权码可以回溯到对应的查询记录,并对应到信息主体的授权文件;或者受托人在其公司运营过程中,通过定期或不定期内部自查的方式,对委托人取得最终用户授权的情况进行回溯性抽查和监督。受托人的上述行为都可以被认为在经营中已经完全尽到了相关的风险防范义务,其经营行为的合法性是不言而喻的,即便在委托人犯罪的情形下,也不能无视受托人所做的各种努力。

另一方面,在委托处理个人信息的场合,受托人最容易出现的风险是其将委托人提供的个人信息非法出售或提供给第三方,此时受托人很难提出抗辩理由。如前所述,受托人根据委托处理信息一般无需取得个人信息主体的同意,但受托人对外提供则需要取得个人信息主体的同意,因为此时受托人的角色发生变化,成为了个人信息保护法中规定的新的信息处理者,[27]就要受到和委托人一样程度的在知情同意、获取、使用、提供等行为上的限制要求。例如,受托人按照委托人的要求开展身份证照片"查询返照"业务,只要委托人的个人信息取得经过了个人同意,受托人的处理行为就是正当的。但是,如果受托人违反合同约定,私自大量留存委托人提供的身份证照片并非法提供给第三方使用,就有可能构成侵犯个人信息罪。如果照片清晰度可以保证,该照片就是个人肖像的载体,是特定自然人可被识别的外部特征,对于该信息的使用时需经本人单独同意或者授权。留存他人照片并提供给第三人的,即便该照片来自于委托人,对于受托人而言,其行为也属于未经同意或者授权非法利用他人肖像,他人可能通过对照片进行加工后形成人脸识别数据,实施破解安全验证等违法行为。因此,受托人违反委托合同约定实施的侵犯个人信息行为,极有可能成立本罪。

在受托人的数据库更为庞大或同时接受多个委托处理个人信息时,也可能存在委托人非法获取由受托人所控制、处理的个人信息的情形。如果受托人对此知情,甚至与委托人之间存在共同犯罪故意时,受托人应当成立侵犯公民个人信息罪。但是,如果受托人已经与委托人约定,在履行合同过程中未经受托人同意,委托人不得利用其信息系统与受托人的信息系统对接的机会非法获取由受托人所在公司控制、处理的个人信息,也不得将受托人反馈的信息、提供的产品及服务向第三方提供,当委托人违背该约定时,有可能成立侵犯公民个人信息罪,但受托人并不因此构成共犯。当然,受托人在发现委托人短时期内不断异常地发出查询服务申请,有可能利用合作信息网络的接口非法获取超越委托范围的个人信息时,其应及时关停向委托人提供的信息处理服务,如果放任侵权行为持续发

〔27〕《个人信息保护法》第 73 条规定,个人信息处理者是指在个人信息处理活动中自主决定处理目的、处理方式的组织或个人,受托人一般的处理行为不具有自主性,所以不属于这里规定的个人信息处理者。

生,也有成立侵犯公民个人信息罪共犯的可能。

**4. 受托人在信息处理过程中是否采取合理的保护措施**

《个人信息保护法》第 9 条规定,个人信息处理者应当对其个人信息处理活动负责,并采取必要措施保障所处理的个人信息的安全。这一规定虽然是针对个人信息处理者做出的,但是受托人在接受委托人提供的个人信息以后,也有义务采取必要措施保障其控制下的个人信息的安全。此外,《个人信息保护法》第 21 条明确要求委托人与受托人必须在委托合同中就个人信息的"保护措施"进行约定。在委托人违反委托合同要求调用受托人网络接口非法获取信息的情形下,需要先查明委托人获取信息的方式、次数,以及该信息能否识别特定个人,如果能够确定该信息属于个人信息,委托人未经受托人许可侵入受托人信息系统获取信息的行为就有可能构成侵犯公民个人信息罪,其超越委托合同权限获取信息的行为还可能构成非法获取计算机信息系统数据罪,与本罪之间存在竞合关系。

但是,此时的受托人是否也成立侵犯公民个人信息罪,就值得仔细推敲,尤其要考察受托人在开展业务活动过程中对个人信息是否已采取合理必要的审查和保护措施。例如,委托人甲将一部分借款人的姓名、手机号码等个人信息提供给受托人乙,由乙核验借款人过去 6 个月的主要活动区域(而非具体位置),描绘借款人的活动半径、大致活动轨迹(而非行踪轨迹),受托人如果严格按照该委托要求处理个人信息,向委托人输出的显然就是经过技术处理,不同于个人定位信息的核验结果。如果受托人网络接口的输出结果符合《信息安全技术 个人信息去标识化指南》(GB/T 37964-2019)对地理位置信息的去标识化技术要求,就属于对个人信息已采取了合理保护措施,根据该信息无法确定个人的行踪轨迹,委托人不能实时定位借款人,对受托人所反馈的信息就不能纳入个人信息的范畴。因为根据《个人信息保护法》第 4 条第 1 款的规定,个人信息必须具有可识别自然人的属性。如果受托人的位置核验接口输出信息不能直接反映特定自然人的具体坐标,就不应作为行踪轨迹信息进行认定。《侵息司法解释》第 5 条第 1 款第 3 项规定,非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息 50 条以上的,即构成情节严重。由于侵犯个人行踪信息的定罪门槛较低,对于"行踪轨迹信息"的范围,实践中应当严格把握其范围,这里的"与此相当的其他位置信息",内容上应包含特定自然人的坐标信息,精确程度上应达到与 GPS 定位信息、车辆轨迹信息同等的要求,该信息系直接反映特定自然人坐标的信息,而不应将不具有"直接性"的信息也纳入行踪轨迹信息。对于虽然也涉及公民个人轨迹但相对模糊的其他位置信息,不宜纳入个人行踪轨迹信息的范畴。如果根据在案证据,能够确定受托人乙提供的位置核验接口输出的信息系根据用户历史数据经算法得出的分值结果,反映的是输入地址与用户经常活动地的偏移度测定,是根据大数据推算的评分值,并不是特定自然人实时、真实的定位信息,不属于公民个人具体的坐标信息,受托人对信息的输出符合去标识化技术标准,已经达到《个人信息保护法》第 73 条所要求的个人信息经过处理,其在不借助额外信息的情况下无法识别特定自然人的程度,在精度上与 GPS 定位信息和车辆轨迹信息存在实质差异,则不应作为行踪轨迹进行认定,实务中也就不能简单地将委托人甲违反委托合同的规定,擅自调用受托人

乙位置核验接口的数量,评价为受托人乙非法提供或出售个人信息所产生的结果。

在现有技术条件下,受托人在信息处理过程中能够采取的保护措施总是有限的。在实践中,越来越多的平台通过开放应用程序接口(API)的方式许可第三方在协议范围内使用数据,这有助于提高数据生产力,推进数据共享,但是,这也可能导致数据的使用目的超过了当事人可以预见的范围,带来侵害个人信息的风险。〔28〕 即便受托人所采取的措施最终无法阻止他人的侵入,但只要其措施在当时的技术条件下是具有合理性的,就能够使受托人免受刑事追究,尤其是在受托人已经采取了一定程度的个人信息技术保护措施时,委托人或者第三人通过网络侵入等方式获取个人信息的,不宜简单认为受托人构成侵犯公民个人信息罪。在前述乙公司受托提供位置核验接口的案件中,乙公司所提供的位置核验接口并不具备直接反映特定自然人坐标的特点,无法直接对自然人进行定位,相关信息不属于行踪轨迹信息,在这种情形下,受托人违反委托合同约定,通过反复验证以及多数据碰撞的方式,逐步缩小位置信息范围,获得位置精准度进而对特定个人进行定位的,难以否认受托人对个人信息的保护措施是合理的、有效的。在这类案件中,应当重点评价的是非法获取个人信息的行为人(委托人)基于其犯罪故意所反复实施行为的独立性和危害性。委托人在擅自进入受托人位置核验接口之后,利用其控制的多个数据源进行数据碰撞才获取了其所意欲取得的信息,其行为系对受托人采取的信息保护措施的恶意破坏,也反证了受托人输出的验证结果不具有确定特定个人行踪轨迹的性质,由此,受托人未实施侵犯公民个人信息的行为,也不具有相关的犯罪故意。



## 四 结 语

与公民的“体感治安”相比较,实务上对侵犯个人信息犯罪的打击力度还远远不够,刑法给公民个人信息保护提供的仅仅是“低水平”的保障,目前还有大量侵犯公民个人信息的犯罪活动由于单个被害人举报的积极性不高,证明被告人情节严重的证据难以收集和固定,犯罪集团化增加侦破难度等原因没有得到应有的刑罚处罚。不过,另一侧面的问题也值得关注:在具体司法活动中,如何把案件办成“铁案”——准确理解侵犯公民个人信息罪的保护法益以及本罪的客观构成要件,防止打击扩大化,实现妥当的处罚。这是刑法谦抑性的题中之义,即刑罚作为最严厉的处罚手段,必须在其他制裁手段的处罚力度明显不充分时,才能加以使用。〔29〕 这一点,在结合《民法典》以及《个人信息保护法》的规定确定个人信息委托处理的刑法边界时显得更为重要。

侵犯公民个人信息罪的保护法益是公民的个人信息自我决定权。如果涉案公民个人信息获得个人同意,不存在相应法益侵害的,行为人当然不构成侵犯公民个人信息罪。在委托处理个人信息的过程中,由于参与处理个人信息的主体多、环节复杂,其中可能有行

〔28〕 参见包晓丽:《数据共享的风险与应对——以网络借贷平台为例》,《法治论丛(上海政法学院学报)》2021 年第 5 期,第 125 页。

〔29〕 参见周光权:《侵犯公民个人信息与妥当的刑罚处罚》,《检察日报》2020 年 1 月 13 日第 3 版。

为人涉嫌构成侵犯公民个人信息罪。但是,由于受托人并不具有独立处理个人信息的权限,其个人信息保护义务也较个人信息处理者弱,因此,在个案中,即便委托人构成侵犯公民个人信息罪,对受托人刑事责任的确定也应当极为慎重。唯有如此,才能确保刑法谦抑原则得到贯彻。

归结起来,在委托处理个人信息的情形下,受托人针对公民个人信息的授权及获取已经设置了较为完善的保护程序,并在合同中对委托人的权利义务进行约束的,就应该认为受托人已经履行了应尽义务,在委托人向其证明已经取得了被收集者的授权之后,受托人也就无须再对下游公司的行为进行实质审查;在受托人已经对个人信息采用合理的技术保护措施的情形下,委托人违反合同约定获取、提供、出售公民个人信息的,其独自对违反国家相关规定,违背信息主体的个人意愿侵犯个人信息的犯罪负责,受托人并未故意参与他人的侵权行为,不构成本罪。

[**Abstract**] Article 21 of the Personal Information Protection Law of the People's Republic of China contains detailed provisions on the rights and obligations of the two parties in an entrustment of personal information processing. In terms of criminal justice, in the process of entrusted information processing or data sharing by a third party, big data technologies provide lenders with financial supports and risk prevention and control services, without which financial platforms are bound to face great tests in anti-fraud and risk prevention and control operations. If the entruster is a practitioner in a gray field, the acquisition of personal information may not meet the requirements of informed consent, and if the personal information processed by the entrustee is not used properly, both the entruster and the entrustee may be involved in a crime, but the boundary between crime and non-crime is not clear. Therefore, it is necessary to carefully sort out the relevant provisions of the Personal Information Protection Law as well as the legal interests protected and the objective constitutive requirements in the crime of infringement upon personal information, so as to provide guidance for criminal justice practice and compliance by big data companies. Considering that, in the entrusted personal information processing, the obligations of the trustee are relatively light, and the business of the trustee is characterized by neutrality, it is not advisable to easily identify the crime of infringement upon personal information if the entrustee has taken reasonable p rotection measures.



(责任编辑:贾　元)