

doi:10.16060/j.cnki.issn2095-8072.2021.01.006

大数据时代个人信息中间商模式分析^{*}

桂 祥

(东华大学人文学院, 上海 201620)

摘 要: 大数据时代, 公民个人信息经济价值进一步凸显, 传统公民个人信息保护模式遇到前所未有的挑战, 非法交易公民个人信息现象异常猖獗。单纯抑制型行政管理措施无法消除非法交易公民个人信息的土壤。堵不如疏, 构建合理的个人信息交易制度不仅能有效破解现有个人信息保护难题, 还可以最大限度促进数字经济发展。在个人信息交易中, 涉及信息源头、中间商、使用者等多个主体, 其中最为重要的网络中枢节点应当是个人信息中间商的定位。合理的信息中间商模式, 可以使得个人信息准确配置到合适的市场主体, 有效发挥资源配置作用。当然为了防止信息中间商在实际交易中出现角色异化现象, 应当结合现有制度框架, 对信息中间商准入资格、交易标准、具体交易方式、政府监管措施及承担的法律 responsibility 等方面进一步规范。

关键词: 大数据; 信息中间商; 场景一致; 信息交易

中图分类号: D912.29 **文献标识码:** A **文章编号:** 2095 — 8072(2021)01 — 0076 — 12

一、大数据产业发展对我国个人信息交易现状的影响

(一) 公民个人信息交易现状分析

近年来, 随着大数据、云计算、人工智能等信息技术的不断创新和广泛应用, 公民个人信息的价值进一步凸显, 使得公民个人信息交易有了现实需求, 同时在中央相关政策支持下, 数据交易产业得到不断发展, 各地数据交易市场也逐渐建立。就数据交易规模而言, 据不完全统计, 数据交易市场规模在2015年已达到33.85亿元, 到2020年数据交易则有望达到545亿元。^①而就数据交易市场而言, 各地也纷纷建立数据交易市场, 最典型如贵阳大数据交易所、上海大数据交易中心、东湖大数据交易中心等机构的成立。在数据交易品种上, 交易的数据不仅涉及个人信息, 更包括行业数据、政府部门数据等, 涵盖诸多领域。由于考虑到个人隐私、商业秘密的保护, 目前交易场所交易的数据一般是经过交易所数据清洗、建模、分析后得到的数据结果, 而非原始数据的直接交易。在数据交易主体上, 目前数据交易场所基本执行交易会员制, 即只有成为交易场所会员, 才能进场参与数据交易, 而对于非会员主体只有通过交易所会员来实现数据交易。在具体的交易服务上, 则通常包括数据供应、交易撮合、数据定制服务及其他服务(如数据托管、数据确权、数据应用等)。^②虽然大数据行业面临广阔的发展机遇, 但是由于数据交易所内交易的数据是经过匿名化处理、

^{*} 基金项目: 本文受上海市立法研究所2018年度课题“上海市个人信息保护立法研究”的资助。

^① 数据来源于贵阳大数据交易所发布的《2016年中国大数据交易产业白皮书》。

^② 资料来源于贵阳大数据交易所发布的《贵阳大数据交易所702公约》。

无法被复原的数据。但它的竞争对手，黑市中的数据大多不脱敏，追求精准，这让合法大数据交易失去竞争优势（张瑶，2018），一些合法大数据公司迫于生存压力，也存在利用收集的非法个人信息进行交易的灰色行为。

其实，在规范的数据交易之外还存在着大量的公民个人信息的非法交易，造成侵犯公民个人信息、获取经济利益的案件频发，特别是2016年发生的徐玉玉因个人信息被非法买卖而遭到电话诈骗不幸身亡一案，引发社会对个人信息保护的极大关注。虽然总体上国家严厉禁止个人信息非法交易，但由于利益驱使，使得非法交易公民个人信息行为屡禁不止，且俨然发展成为分工明确的“黑色产业链”。^①在这条黑产业链上，由行业“内鬼”、黑客利用盗窃、网络攻击等手段非法获取公民个人信息，充当着数据源头；由数据掮客对公民个人信息进行“注水”、拼接、转售，充当着产业链的数据中间商；由犯罪组织、商业营销、大数据公司等主体购买公民个人信息，充当着产业链中的数据终端。作为产业链中间商的数据掮客通常都以小团伙的组织形态存在，交易手段也较为简单，主要通过QQ群和支付宝等社交平台 and 支付平台来实现与产业链上下游之间的沟通，但交易过程中其基本不做实际意义的数据分析处理，所交易的数据一般都是未经“去识别化”的原始公民个人信息。由于个人信息非法交易始终处于隐秘发展状态，因此其具体规模无法准确统计，但从公安部公布的侦破侵犯公民个人信息案件数量来看，公民个人信息非法交易的市场规模应比规范的数据交易规模更为庞大。

（二）大数据行业发展更强调个人信息的动态利用

随着信息通讯技术的高速发展，人们日常生活、经营过程中持续生成着海量的数据，原有碎片化的数据在数据挖掘、数据整合、数据分析等技术条件的支持下产生了新的价值，我们也由此进入了大数据时代。根据维克托·迈尔和肯尼思合著的《大数据时代》所总结的，大数据的“大”主要体现为具有4V特征，即规模性（volume）、高速性（velocity）、多样性（variety）和价值性（value）等方面的优势。（迈尔-舍恩伯格和库克耶，2012）但这些优势特征是建立在单个数据集合的基础上，并且呈现出数据量越大价值越大的非线性增长关系，可以说大数据的高价值是由碎片化的数据喂养而成，也因此要求数据材料应当具有一定的自由流动性。而传统的个人信息保护制度是呈现以增强信息主体对信息控制权为中心的单边、静态保护框架，与之相配套出现的是个人信息集中于各商业机构的“信息孤岛”现象。由此可见，大数据行业的健康、高速发展其实离不开个人信息交易渠道的畅通。

虽然新颁布的《民法典》将个人信息规定于《人格权编》，诸多学者也倾向于认为在赋予信息主体同意权、知情权、删除权等诸多权利的情况下，个人信息已然升格成为具体人格权利。但不可否认的是在数字经济时代，个人信息不再单纯关乎信息主体人格尊严或者个人隐私，更多与市场经营联系在一起，个人信息的财产属性明显增强了，

^① 如2019年7月，广东省公安厅协同兄弟省市开展“净网7号”专案收网行动，打掉“猎头搜”特大侵犯公民信息团伙，查获被非法收集的公民信息2亿余条，成为目前破获的全国最大的非法侵犯公民个人信息案。

且个人信息的人格权定位也并不当然否认其商业化运用,因此个人信息的保护和共享利用两者不可偏废。另一方面,在大数据技术条件下,通过对数据进行融合与交叉验证,可以通过多重不能识别信息主体的信息识别信息主体,也就是说大数据分析技术的运用,使得“个人身份可识别信息”与“非个人身份可识别信息”的两分法没有实际意义(刘迎霜,2019)。实际在技术层面,仅需交易不可识别信息或者“去识别化”信息,并通过相应技术手段即可重新得到可识别个人信息。因此,传统的可识别信息不可交易、不可识别信息可交易的简单“二分法”面临现实挑战。综上所述,在大数据时代,从个人信息本身来看,单纯强调静态控制也并不能做到保护和利用的最优均衡,更需要在保障个人信息有序流动的前提下实现保护和利用的动态均衡。

二、公民个人信息交易境内外法律规制分析

(一) 我国对公民个人信息交易相关规定分析

2009年,为打击非法交易公民个人信息的猖獗行为,全国人大常委会通过刑法修正案(七),在原来第253条的基础上增加了第253条之一,新增了两个罪名:(1)出售或非法提供公民个人信息罪;(2)非法获取公民个人信息罪。2015年,全国人大常委会通过刑法修正案(九),对原刑法第253条之一进行了修改,将原来的出售或非法提供公民个人信息罪修改为侵犯公民个人信息罪,这次修改不仅是单纯罪名的调整,更将犯罪主体从特殊主体转变成一般主体。如果“违反国家有关规定,向他人出售或者提供公民个人信息”,不论何种主体,其交易公民个人信息的行为都可入刑。既然如此,那现有法律规定中是否还存在公民个人信息交易的制度空间呢?我们可以看到其实存在逐渐转变的过程。2012年通过的《全国人民代表大会常务委员会关于加强网络信息保护的决定》(以下简称《决定》)第3条规定:“网络服务提供者和其他企业事业单位及其工作人员对在业务活动中收集的公民个人电子信息必须严格保密,不得泄露、篡改、毁损,不得出售或者非法向他人提供”。此条配之以上述刑法规制,基本是不存在公民个人信息交易的制度空间。但在2016年的《网络安全法》中,对个人信息交易的表述则存在些许差异,《网络安全法》在主体范围方面更宽泛,但是对行为约束方面更明确,体现在《决定》规定是严格禁止出售公民个人电子信息的,但是在《网络安全法》中则体现为禁止“非法出售”。可以看出,《网络安全法》对于出售公民个人信息行为进行了限缩,只有非法出售公民个人信息才是禁止的,亦即存在合法出售个人信息的可能性,并非所有的出售个人信息行为都要进行刑法规制。而在2020年公布的《民法典》第1038条也规定:“信息处理者不得泄露或者篡改其收集、存储的个人信息;未经自然人同意,不得向他人非法提供其个人信息,但是经过加工无法识别特定个人且不能复原的除外”。由此可见,信息处理者在经自然人同意的情况下,向他人提供个人信息并不被认为是当然违法,且明确了经“去识别化”的个人信息的出售不需经自然人同意,这和实践中的数据交易场所做法一致。可以看到,在数字经济迅猛发展浪潮的推动下,理论界也对个人信息交易、

商品化等问题开展了系列研究（洪玮铭和姜战军，2019；陈星和梁丁，2020；李德恩，2020），法律层面对公民个人信息有序流动、合理交易正逐渐认可，目前交易个人信息、发展信息中间商已存在一定的制度空间。但同时也应当看到，《民法典》对于“信息处理者”的规定是笼统的，其“处理”的内涵包括了收集、存储、使用加工、传输、提供、公开等环节，并未明示个人信息的交易主体，现有相关规定还过于原则和模糊，具体的交易模式、机制还有待进一步厘清及法律确定。

（二）域外个人信息交易法律规制考察分析

1. 美国数据经纪商模式

美国对个人信息的保护起源于对隐私权的关注，沃伦和布兰代斯在《论隐私权》一文中对隐私做了经典定义，即“免受外界干扰的、独处的”权利（Warren and Brandeis, 1890）。而后随着信息时代的到来，上述隐私权的内涵也随着数字经济的发展而不断将对个人信息的控制也囊括其中。总体而言，美国的个人信息保护模式呈现出“大隐私权保护模式”特征，即通过不断丰富隐私权的内容来应对网络时代的个人信息问题（郑志峰，2019）。但因为个人信息的控制实际与美国宪法所保障的言论及出版自由存在一定冲突，且美国政府也高度重视数字经济产业的快速发展，因此在不严重侵犯个人隐私权的前提下美国更倾向于个人信息的自由流动，与之相对应，其对个人信息的保护也并没有形成统一的立法，而是分散在不同的法律中予以规定。^①在此背景下，美国形成了规模庞大的数据交易市场，也产生了专门提供数据交易服务的数据经纪商（data broker）。这些数据经纪商不仅无孔不入地收集所有人的用户信息，还在数据交易市场中出售收集到的信息（包括经处理过的信息和原始信息），且其具体交易行为管理更多依靠市场自律来实现，长期以来并没有专门的数据经纪商监管立法或者专门监管机构，^②因此可以说长期以来美国在对待个人信息的态度上更加偏重于利用、交易而忽视了保护，这也引发了美国公民对隐私泄露风险的担忧。

2. 欧洲个人信息交易分析

与美国大隐私权保护模式不同，欧洲更多将个人信息划归为**人格权**，侧重于维护信息主体人格尊严和人格自由。在此理念下，欧洲相关立法都给予信息主体诸多权利，如可携带权、被遗忘权、知情权等，保证其对自身个人信息的绝对控制、支配，且这种权利与生俱来无法转让与放弃。正是因为这种立法理念，使得2016年4月27日欧洲通过的《一般数据保护条例》被称为史上最严格的数据保护立法，当然也有诸多学者批评如此严格的传统信息保护立法并不符合数字经济发展趋势。而在实践中，欧盟也较为严格地执行数据保护规范，并建立专门的数据保护监督机构（龙卫球，2017）。因此，虽然由于国际竞争压力使得欧盟也逐渐放宽了对个人数据合理利用的态度，但其在实践中并没有形成规模化的数据交易市场或者数据经纪商，并一般将个

^① 如《隐私法》《儿童在线隐私保护法》《公平和准确的信用交易法》《电话消费者保护法》《视频隐私保护法》等。

^② 2018年5月，佛门特州通过了数据经纪商监管法案，成为美国历史上第一部数据经纪行业专项立法。

人数据的去识别化作为可交易的前提条件。

由此可见,各国的个人信息交易法律规制与其政治、文化、经济等因素密切相关,美国注重自由及经济发展,但失之过松,对数据经纪商基本没有严格监管,导致数据交易巨头对普通公民隐私侵犯风险高企。而欧洲国家则认为个人信息事关个人尊严,对个人信息交易采取较为严格的限制,这也限制了数字经济的进一步发展。因此,我国在构建信息中间商制度时有必要结合自身情况,在有效监管信息中间商的同时保障有序的个人信息交易。

三、公民个人信息交易中间商应然性分析

市场上存在巨大的个人信息交易和使用需求,而现有法律原则性限制了个人信息的交易(同时也留下了调整的空间),因此导致了个人信息交易“黑产”链条的野蛮生长和合法数据商的市场劣势地位,那么我们需要进一步分析的是个人信息合法交易以及信息中间商存在的应然性。

(一) 经纪商亦或是中间商?

严格来说,经纪并非严格的法律术语,根据国家工商总局颁布的《经纪人管理办法》第2条规定:“本办法所称经纪人,是指在经纪活动中,以收取佣金为目的,为促成他人交易而从事居间、行纪或者代理等经纪业务的自然人、法人和其他经纪组织”。而在《民法典》中与其较为接近的概念应当是第二十六章的中介合同相关内容。通过这些规定我们可以知道经纪行为最为重要的特征其实是促成他人交易,收取佣金,其基本上并不成为一方交易主体,也不改变所有交易标的。而从美国佛蒙特州数据经纪商监管法案的相关定义,可以看到个人经纪信息被定义为一个或多个被计算化的消费者数据,如果出于传播的目的被分类或整理给第三方。而认定数据经纪商则被定义为有意向第三方收集和銷售或许可与该企业没有直接关系的消费者个人经纪信息的企业。其数据经纪活动则必须具备数据的进、出两个环节(彭星和万雨娇,2019)。在此定义以及数据交易实践中,美国的数据经纪商其实存在购入、收集信息和出售信息两次基本独立法律行为,其收益来源并非信息主体或者信息使用者支付的佣金而来自于信息价差,且其对交易信息拥有相应的权利,也需要进行分类或者整理。而从我国的法律语境来看,其实际并非严格符合“经纪”行为特征。因此,将专门从事此类个人信息交易服务的主体定位为信息经纪商并不妥当。

中间商相对于经纪商其实是更加泛化的概念,从广义来看,中间商可以包含经纪商的概念,但从狭义来看,较为典型的中间商应当是要素交易链条中的一环,其深入参与到交易关系中成为一方交易主体,对交易要素拥有相应的权利,获取价差收入并要承担一定的损失风险,如货物贸易中的批发商、零售商,又如金融活动中的银行、保险公司等。由此可知,个人信息交易中的“经纪商”行为模式较为符合典型中间商的特征。做市商属于中间商的一种,且其进行证券买卖的行为和信息交易也存在类似之处,但由于做市商更多是证券金融市场的专用名词,且做市商本身不仅承担了市场交

易的功能,更承担了“做市”“造市”等稳定市场功能,这和金融市场本身的价格波动风险紧密相关。而信息交易中最重要风险并非信息价格波动,而应当是信息泄露、信息滥用风险,因此将上述信息交易中的商主体命名为信息做市商并不妥。综上所述,本文采用信息中间商来定位专门从事个人信息收集、出售双向交易的商主体。

(二) 公民个人信息中间商的市场价值分析

市场各方的供需分析是微观经济学的核心内容,西方经济学者认为市场具有自动调节作用,只要价格可以自由波动,那么就可以达到“市场出清”的效果。但是市场机制并不是总是完美的,而存在“市场失灵”现象,此时市场机制就不能实现最优的资源配置。信息不对称是导致市场失灵现象最常见的因素之一。为了优化市场资源配置,最大程度地消除信息不对称,市场自发或者法律强制会采用多种手段来进行信息交流。如市场主体自发采用广告的形式,使更多的消费者知悉产品或者服务的信息。再比如法律强制上市公司采用信息披露的方式向投资者公布公司重大经营信息。由于市场竞争机制的完善,绝大多数商品都处于“买方市场”状态,需要由消费者来选择商品,最了解商品信息的不是消费者而是生产者,而且在市场上生产者较消费者也具有更强的经济实力,因此无论是广告还是上市公司信息披露都是由卖方向买方进行商品信息的输送,呈现出一种“单向性”。这种单向性的信息输送无疑对市场竞争优化是有积极作用的,如“广告向消费者传递所销售物品的价格、新产品的存在和零售店的位置等信息。这种信息可以使顾客更好地选择想购买的物品,从而提高市场的有效配置资源的能力”(曼昆,2012)。但也要看到的是,这种单向性的信息输送又存在一定的缺憾,由于卖方对买方的信息缺失,因此单向性信息输送范围通常是宽泛的,难以精确的。而又因为信息传输过程中也是存在成本的,因此这种单向性的信息输送因缺乏针对性和精准性而体现为高成本,典型如现实中高额广告费,且这部分多余的成本基本属于社会资源的“无谓损失”。

这种商品信息输送成本浪费的根源在于信息输送的单向性,因为在非信息时代,信息搜寻成本的高昂而近乎无法解决的,当时更多的解决方法是通过人工的模糊统计以及大致的估计。在信息时代,大数据、云计算、人工智能则为信息的双向传输提供了更为精准的工具,为高效解决信息不对称的市场失灵问题提供了新的途径,即卖方可以通过信息技术知悉买方相关信息、偏好等进而精准营销,从而控制信息输送范围、降低信息成本。当然,在信息中间商定位偏差的情况下,可能会出现“信息错配”的现象。相对而言,规范运营的信息中间商则可以通过自身专业化的信息处理和传输技术来实现信息资源的正确配置。理想状态下,信息中间商交易个人信息如由市场化进行调节应当具有较高经济价值,相较于现在“信息黑市”可以定价较高,而这可以较好地将一些低质量生产商、服务商拒之门外,防止信息主体受到假冒伪劣生产商、服务商的不当或者虚假信息骚扰,另一方面由于信息输送的精准性,信息成本或者营销价格较以往如广告等方式也会有所降低,这也为规模较小的企业进入市场提供了新的途径,从整个市场来看可以增强市场竞争的有效性。同时正如前文所述,以往单向性商品信息输送几乎都会存在“无谓损失”,但在信息中间商模式下,更加突出

个人信息的财产价值, 卖方支付的信息成本有一部分要流入信息主体手中, 也即这种模式在很好控制“无谓损失”的基础上还增进了整个社会的福利水平。

(三) 个人信息处理多元主体分类管理的需求

《民法典》第1035条规定: “个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等”。同时, 从《民法典》第1037条、第1038条相关规定中“信息处理者”的表述来看, 并没有如欧盟《一般数据保护条例》一样区分“数据控制者”“数据处理者”与“受委托处理者”, 而是笼统地赋予其各种义务(王洪亮, 2020)。但是不可否认, 在个人信息处理过程中, 各类参与主体实际应具有不同的功能定位及承担不尽相同的权利义务。比如, 信息收集主体应当更加注重收集个人信息的正当性, 包括目的的限定, 信息主体的同意等; 而对于信息处理主体而言则应更加注重防止个人信息的滥用及对信息控制主体数据财产权的保护。因此, 虽然目前《民法典》对相关主体仅做了原则性的规定, 但在未来的个人信息保护专门立法中, 构建更为具体的信息处理多元主体分类管理体系不失为可行之策。

在目前个人信息的实际流转过程中, 基本存在以下几类主体, 分别是: 信息收集者, 信息存储者, 信息加工者, 信息传播者以及信息使用者等。需要明确的是此处的信息传播者实际并非本文所定义的信息中间商, 其更多是传播、出售信息产品或者“去识别化”的个人信息, 而并非是原始未经处理的个人信息。由此可见, 在个人信息存在流转、利用必要的大数据时代, 我国尚未存在专门、规范的主体进行个人信息交易服务。但在完整的信息产业链条中, 信息产业参与者均有各自专门技能, 不容易相互取代, 比如由信息收集者直接和信息加工者进行信息交易并不合适, 可能涉及到交易渠道, 交易需求的不同, 这也将导致交易成本的提升。因此, 个人信息中间商作为专门交易个人信息的产业参与者, 对个人信息进行整理、分类, 维护个人信息交易渠道, 防止个人信息的滥用, 有其存在的必要性。相关法律中同时也应当对其有明确的定位, 并对其相关权利义务关系进行相应的规定。

四、大数据时代我国公民个人信息中间商制度构建

前文我们从法律、经济等方面论证了个人信息交易及信息中间商的积极意义, 但个人信息和个人人格、财产等基本权利紧密相联, 不规范的交易制度必然将导致个人信息的滥用和信息主体权益损害。因此, 我们在构建公民个人信息中间商制度时必然要考虑到社会利益和个人利益的平衡, 妥善设定信息中间商的权利义务关系。

(一) 个人信息中间商准入资格管理

“由于择优连接的客观性, 一些具有较大聚集度(影响力)的主体, 往往成为其他主体择优连接的对象, 最终处于社会网络的中心位置, 拥有较大的社会影响力, 决定着社会治理的内容、方向和结果。”(范如国, 2014)从优化社会治理网络节点角度看, 信息中间商是公民个人信息使用、流动中的中枢节点, 决定着个人信息交易对

社会的作用。由于不加控制的信息中间商可能在实践中发生角色异化,成为滥用个人信息、侵害信息主体利益的源头,因此需要严格信息中间商的资格准入。笔者认为,在未来的信息交易产业中,交易未经“去识别化”个人信息的信息中间商应当进行牌照化管理,即只有经过特许批准的机构才能进行此类个人信息交易,其他主体未经批准包括个人信息交易的受让方都不能进行个人信息交易。同时应当明确,个人信息交易其不仅仅是单纯利润最大化的商业活动,而且其还涉及到社会公众、信息主体等多元利益保护,另鉴于我国目前个人信息保护有待完善的现状及美国数据经纪商实际经验,信息中间商如完全由私人投资者组建、控制,则可能因追求利润最大化而忽略了多元利益的保护。因此,在当前个人信息保护现状中,信息中间商应当由国有资本控股、运营并在一定程度上降低经济效益指标考核,增加社会效益指标考核。

具体的准入审批标准中,在资本要求方面,信息中间商主要进行个人信息交易,而非金融资金金融通,其经营风险主要并非来自于资金的期限错配而来自于信息泄露导致的信息主体权益损害,因此其资本金规模要求不必对比金融机构规模。但由于信息泄露可能实际导致信息主体的人格、财产权益现实损害,而这需要信息中间商进行实际的赔偿,因此其需要有相应的资金能力,其资本方面则应当是实缴资本且应当是现金出资;在技术方面,信息中间商应当有技术对个人信息进行妥善的存储,防止黑客恶意攻击。应当有技术对个人信息的应用场景进行分析,保障个人信息的交易、使用符合信息主体的期望,可以对个人信息泄露风险进行一定合理的评估。应当有技术实现个人信息的加密传输,保证个人信息交易的安全性。应当应用元数据、区块链等技术实现对所交易个人信息的溯源追踪;在专业人员岗位方面,信息中间商应当具备满足个人信息顺利交易的技术、法律、金融人才,为了满足对个人信息保护的需求,应当设立专门机构或具有相应资质的专门人员(数据保护官),负责本单位个人信息保护日常工作,包括参与涉及个人信息保护所有重大决策的个人信息影响风险评估、负责拟定个人信息保护政策、与相关个人信息保护主管部门或行业自律组织联络等(周汉华,2018);在内部管理制度方面,信息中间商应当构建严格的“防火墙”等隔离制度,如信息交易人员和信息分析、信息保护人员岗位分开。此外,信息中间商还应当构建完善的信息交易、信息存储等制度。

(二) 个人信息中间商交易的标准

个人信息交易有关优化市场、正确配置信息资源的积极功能实现必然伴随着信息交易的规范化,否则必将出现滥用个人信息的违法犯罪行为,因此其交易必须要设定一定的标准。《民法典》第1035条规定“处理个人信息,应当遵循合法、正当、必要原则,不得过度处理,并符合下列条件:(三)明示处理信息的目的、方式和范围”;同时明确“个人信息的处理包括个人信息的收集、存储、使用加工、传输、提供、公开等”。因此在目前有限的个人信息转移活动中,理论界一般理解为应遵循目的限定原则。但随着数字经济的发展,该原则也越来越多受到质疑,认为单纯地使用限定的预判是抽象僵化的,无法适应大数据时代个人信息使用场景多元的需求(范

为, 2016)。因此有学者主张采用“情境脉络完整性”理论中的“场景”概念来限定信息的使用范围, 即个人信息原始收集时的具体语境应得到尊重, 其包含了信息主体对其个人信息使用场景的期望, 在其后续传播及利用不得超出原处的情境脉络。比如, 在网络购物场景中产生、收集的个人信息再次用于类似商品的营销中则可理解为场景一致, 而在医疗服务场景中产生、收集的个人信息用于相关药物、保健用品的推销或者相关互联网服务中则不能理解为场景一致。场景一致要求可以扩展个人信息使用和流转范围, 在符合信息主体预期的前提下促进个人信息的合理利用。因此, 本文认为信息中间商对个人信息的交易前提, 应当是交易受让方的使用场景与个人信息产生场景具有一致性。在这种场景一致的标准下, 信息主体对其个人信息的使用场景是已有预判的, 因此信息中间商不需要再征得信息主体的同意, 但是为保护信息主体的信息自决权利, 应当赋予其无条件选择“退出”的权利。而这与现行《民法典》的相关规定其实也并不矛盾, 仅需要我们对现有“目的、方式和范围”要求作综合的理解, 当然也更需要今后在个人信息保护专门立法中明确。

场景一致标准可以较好解决信息中间商交易的部分合规问题, 但场景一致的要求对于日常海量的信息交易仍然太过严苛, 且无法实现对信息的充分利用。应当明确场景一致标准仅是个人信息交易的前提条件之一, 而对于场景不一致的情况下, 信息交易、使用的场景和信息主体被收集信息的场景存在完全不同的体验, 可能会出现隐私泄露风险扩大或者减小的情况, 原则上信息中间商应当不能直接进行个人信息交易, 而需要进一步对信息交易、后续使用等进行信息泄露、滥用的风险评估。此处的风险评估应当结合个人信息的识别性、与信息主体人身财产权益的紧密度、后续使用场景的开放性及交易对象的存储、处理技术手段等方面进行。

经过信息泄露风险评估后, 如果确实可能造成信息泄露风险增加的, 则信息中间商不能直接交易个人信息, 在征得信息主体明示同意后可以在许可范围内进行交易, 也即赋予信息主体明确选择“进入”的权利; 而如果评估结果显示交易可能造成信息泄露风险减少的, 则信息中间商应当将评估报告及时告知信息主体, 如果信息主体没有及时明示拒绝, 信息中间商可以视信息主体默认而直接进行个人信息交易。

(三) 个人信息中间商的交易方式

目前的个人信息交易可以大致分为场内交易(各类大数据交易平台)和场外交易, 而场外交易则鱼龙混杂。在当前我国社会信用体系尚不健全, 市场主体的诚信意识还不够高, 个人信息被非法采集与转让的问题比较严重的情况下, 本文认为信息中间商的信息交易应当采用场内交易的方式, 其一, 与人们印象中的非法买卖个人信息黑色产业链相区分; 其二, 也更易于对信息中间商的交易行为进行有效控制; 其三, 能较好保障信息主体的合法权益(邢会强, 2019)。为保证个人信息产生场景可预期性, 并实现信息产业链各参与主体的专业性, 应当明确由互联网服务企业来收集个人信息, 而信息中间商则不能主动向信息主体收集个人信息, 只能与交易场所内的会员企业进行交易, 会员企业之间也不能直接进行原始个人信息的交易行为。在与会员企

业进行个人信息交易过程中，信息中间商则主要从事对个人信息的初步分类、整理，实现符合场景一致的信息流动，对场景不一致的信息流动进行风险评估等工作。个人信息的受让方在受让个人信息后，可以按照相关场景要求处理个人信息的，但同时也应当采取必要的技术手段保障个人信息的安全，且由于原始个人信息交易业务范围系特许批准，受让企业也不能进一步在场内或者向场外企业交易相关个人信息。

前文提及了个人信息中间商与做市商概念间的差异，虽然本文不赞成采用个人信息做市商的概念，但在交易方式上可以借鉴其相关做法。即由信息中间商对个人信息进行双向报价，接受会员企业的买卖要求，其利润来源主要来自于信息中间商信息买卖报价的差额。这种交易方式可以较好的回避信息经纪交易或者实践中数据交易平台交易中对信息定价较为困难、协商成本较高等问题，也可以在一定程度上促进个人信息的有效流转、合理利用，但也可能会造成信息中间商对信息交易市场的垄断及对信息交易价格的操纵，当然这需要法律的精准规制（孟令星和郑春玉，2017）和相关部门的有效监管。由此，形成“去识别化”个人信息由数据交易平台挂牌交易和未“去识别化”个人信息由信息中间商双向报价直接交易并存的“双轨制”交易态势。

（四）政府监管及个人信息中间商责任

信息产业的发展必然伴随着相应的风险，而要最大程度减少信息产业中可能存在的风险，发挥其对社会经济发展的积极效应，政府的监管介入必不可少。目前由于个人信息保护专门法律的缺失，个人信息保护的主管机关及信息产业的监管机关尚未确定，我国信息产业管理目前呈现出“九龙治水”的态势，且各个部门之间并未形成相应的协调机制。随着数字经济的快速发展，有必要设立专门的机构对实践中的信息产业进行监管，并通过法律赋予其与监管职能相匹配的权力，如定期和临时检查、对不法行为的惩罚等。而由于数字经济尚属新兴产业，强有力的行政监管则可能会抑制其发展壮大，尤其在个人信息交易产业中政府监管应当确立不同的监管理念，在强调必要的事前准入审批和事后违规惩戒监管同时，需更加注重交易过程中的信息泄露风险评估监管、以向监管机构公开算法规则及交易规则等为重点的信息披露监管、对日常动态交易信息的实时技术监管及根据具体场景风险大小而采取的差异化监管等理念和措施。此外，交易场所作为信息交易一线管理者，也应当承担必要的监管职能，包括对交易数据的分析，对会员交易资格的审核等方面。

信息中间商在进行个人信息交易过程中，必将涉及信息主体、信息供给方、信息需求方等多方主体，在不同主体间由于权利义务的不尽相同，使得信息中间商所要承担的法律风险也可能出现较大差异。在信息市场上，信息中间商无疑是处于绝对的优势地位，掌握了大量的技术、资金等资源，一旦出现了不规范的信息交易行为，信息主体往往处于弱势地位，因此应当在法律上明确信息主体的相关权利，包括同意权、知情权、删除、更正权等。而相应的，信息中间商在交易过程中也有告知、防止信息泄露、进行客观风险评估等义务，而如果信息中间商违反相应的法律义务，如擅自交易场景不一致信息、应删除不正确个人信息但仍进行交易等情形，并给信息主体带

来损害,则应当承担损害赔偿 responsibility,且为了更便于信息主体维护自身利益,应当构建“使用者责任”机制,明确这种损害赔偿 responsibility 采取举证责任倒置的过错推定责任。在具体的责任承担方式上,除了一般的停止侵害、恢复原状、赔偿损失、消除影响等侵权责任承担方式外,因为个人信息往往与个人人格、尊严紧密联系,因此在责任承担上还应当更加注重精神损害赔偿的运用。另一方面,信息中间商在与会员企业进行信息交易过程中,和会员企业其实属于平等地位,因此基本不存在偏向某一方的倾斜保护,而更多体现为因违约导致损害对方信息财产权的法律责任。这里违约的情况包括但不限于交易信息不符合信息受让方要求、信息受让方违反约定处理信息、交易的信息不合法、信息受让方违反保密义务等。而具体的归责原则方面则应当采用过错责任,由过错方对自身过错承担责任,并在诉讼过错中由受害方承担相应的举证责任。责任承担的方式一般可以主张财产损害赔偿,但也可以根据情况主张停止使用,删除信息等责任承担方式。

五、结语

大数据时代,网络已成为经济发展的新引擎,公民个人信息也成为大数据经济的核心和基础,数字经济快速发展的现状对个人信息的保护和利用也提出了更高的复合要求。为了更好实现党的十九大报告提出的建设网络强国、数字中国、智慧社会的战略目标,通过相关法律手段建立与完善建立权重明确、保护有效、利用规范的制度规则。2020年10月13日,十三届全国人大常委会第二十二次会议第一次审议了《个人信息保护法(草案)》,其对个人信息处理者尚未在分析、交易、使用等环节进行角色细化,但已对个人信息处理者向第三方提供个人信息进行了原则性的规定。而在上海数字经济的具体实践中,也还存在着个人数据流动性欠佳、数字经济发展赋能增效有待进一步提高的问题,而这些问题的解决不仅有赖于政府数据平台的设立,更需要发挥市场的力量,通过对个人信息中间商进行赋权,规范个人信息的有序流动。

在此背景下有必要利用现有的制度空间,借鉴境外数据交易的相关经验,结合我国个人信息保护和利用现状,构建规范化的个人信息中间商模式。主要体现在:第一,在个人信息中间商资格准入方面,应当只允许经过批准的机构才能进行个人信息交易,且在个人信息中间商的资本、技术、专业人员、内控制度等方面构建完善的准入标准;第二,在个人信息中间商交易标准方面,对于符合场景一致要求的,不需要再征得信息主体的同意,但应当赋予其无条件选择“退出”交易的权利;而对于场景不一致的情况下,则可以在经过信息泄露风险评估后,赋予信息主体明确选择“进入”交易的权利;第三,在个人信息中间商交易方式方面,形成“去识别化”个人信息挂牌交易和未“去识别化”个人信息由信息中间商双向报价直接交易的“双轨制”交易;第四,在政府监管方面,应当设立专门监管机构,同时明确数据交易场所的一线管理职能;在个人信息中间商责任方面,应当构建个人信息中间商的“使用者责任”机制,在归责原则上采用过错责任。

参考文献

- [1] 陈星, 梁丁. 大数据时代个人信息利用的法律规制[J]. 重庆理工大学学报(社会科学), 2020(6):86-93.
- [2] 范如国. 复杂网络结构范型下的社会治理协同创新[J]. 中国社会科学, 2014(4):98-120.
- [3] 范为. 大数据时代个人信息保护的路径重构[J]. 环球法律评论, 2016(5):92-115.
- [4] 洪玮铭, 姜战军. 数据信息、商品化与个人信息财产权保护[J]. 改革, 2019(3):149-158.
- [5] 李德恩. 数据权利之法律性质与分段保护[J]. 理论月刊, 2020(3):113-123.
- [6] 刘迎霜. 大数据时代个人信息保护再思考——以大数据产业发展之公共福利为视角[J]. 社会科学, 2019(3):100-109.
- [7] 龙卫球. 数据新型财产权构建及其体系研究[J]. 政法论坛, 2017(4):63-77.
- [8] 迈尔-舍恩伯格, 库克耶. 大数据时代——生活、工作与思维的大变革[M]. 周涛, 等译. 浙江: 浙江人民出版社, 2012.
- [9] 曼昆. 经济学原理(微观经济学分册)[M]. 梁小民, 梁砾, 译. 北京: 北京大学出版社, 2012:345.
- [10] 孟令星, 郑春玉. 做市商法律问题原论[M]. 北京: 中国检察出版社, 2017:273.
- [11] 彭星, 万雨娇. 美国佛蒙特州数据经纪商法案浅析及启示[J]. 武汉金融, 2019(2):46-50.
- [12] 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.
- [13] 邢会强. 大数据交易背景下个人信息财产权的分配与实现机制[J]. 法学评论, 2019(6):98-110.
- [14] 张瑶. 谁在盗贩公民信息——个人隐私交易黑市起底[J]. 协商论坛, 2018(9):39-43.
- [15] 郑志峰. 人工智能时代的隐私保护[J]. 法律科学(西北政法大学学报), 2019(2):51-60.
- [16] 周汉华. 探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向[J]. 法学研究, 2018(2):3-23.
- [17] Warren, S. D., and L. D. Brandeis, "The Right to Privacy", *Harvard Law Review*, 1890,4(5):193-220.

【作者简介】桂 祥: 东华大学人文学院讲师, 法学博士。研究方向: 经济法学。

Analysis on the Middleman Model of Personal Information in the Era of Big Data

GUI Xiang

(College of Humanities, Donghua University, Shanghai 201620, China)

Abstract: In the era of big data, the economic value of citizens' personal information has been further highlighted. The traditional protection mode of citizens' personal information has encountered unprecedented challenges, and illegal transactions of citizens' personal information are rampant. Simple administrative control measures can not eliminate the soil of illegal trade in citizens' personal information. Building a reasonable personal information transaction system can not only effectively solve the existing personal information protection problems, but also promote the development of the digital economy to the maximum extent. In personal information transaction, it involves multiple subjects such as information source, middleman and user, among which the most important network hub node should be the positioning of personal information middleman. The reasonable information middleman mode can make the personal information accurately allocate to the appropriate market subject and effectively play the role of resource allocation. Of course, in order to prevent the information brokers in the actual transaction of the phenomenon of role alienation, should be combined with the existing institutional framework, the information brokers access to qualifications, trading standards, specific trading methods, and government regulatory measures and assume legal responsibility and other aspects of further standardization.

Keywords: big data; information brokers; scene is consistent; information trading

(责任编辑: 黄志瑾)