□ 数据治理

□ 数据开放与利用

□ 个人信息保护

财经法学 No. 4，2021
pp. 3 - 22

社会信用建构：基于大数据征信治理的探究

黎四奇*

内容提要：社会信用是社会秩序维系、人际关系和谐、交易规范与拓展、民富国强的基础，其对于构建社会主体命运共同体具有时代性的意义。大数据正以其技术性特质改变着传统征信模式、方法与观念，对征信治理的推陈出新产生诱导性的进化效应。大数据时代，大数据征信以其技术优势推动与加速社会信用的建构，促成信用国家的形成。法律是社会利益的调节器与社会秩序的稳定器，当征信治理制度滞后于社会信用发展的需求及科技的进步而衍生供求矛盾时，从目标定向、理念明确、利益保护平衡、市场安全及尊重互联网精神等角度进行法律的因时与因势而进就是一种理性选择。

关键词：社会信用　大数据征信　信用中国

为了实现“信用社会”这一宏伟目标，我国推出了一系列纲领性文件，如 2014 年 6 月的《社会信用体系建设规划纲要（2014—2020）》（以下简称为《信用纲要》）、2019 年的《关于加快推进社会信用体系建设构建以信用为基础的新型监管机制的指导意见》。虽然信用社会的形成不可避免地依存于传统、风俗与制度等，但是其更应通过对社会主体行为进行评价的方式得以落实。在前大数据〔1〕时代，囿于互动应景与技术等原因，与社会主体相关的信用信息呈现出破碎化、零散化的特点。让数据“发声”的大数据技术开启了重大的信用评价转型。研讨大数据征信治理对社会信用建构具有举足轻重的作用。

* 黎四奇，湖南大学法学院教授。

〔1〕“数据”与“信息”是两个相互联系的概念，数据本身就是信息，是信息具体的表现方式。信息经过数字化处理后才能复制、存储与传输。对此，我国《网络安全法》第 76 条第（四）项规定：“网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。”

一、社会信用建构的机遇与挑战：大数据征信

（一）大数据征信的识别

信用国民、信用社会、信用国家是我们孜孜以求的目标。当大数据与征信相结合时，它标志着大数据征信已在事实上开启一个国家诚信建构的新模式与新时代。概念是人类认识和把握世界的重要手段。为了廓清“大数据征信”这一关键词，研究者进行了诸多解释。“大数据征信是指将大数据技术运用于征信活动，通过采集、分析、挖掘多维度的海量数据信息，并借助机器学习等模型算法来描述信息主体的信用状况，为多样化的应用场景提供征信产品。”〔2〕“大数据征信是指基于大数据技术设计征信评价模型和算法，通过多维度的信用信息考察，形成对个人、社会团体、企业的信用评价。”〔3〕“大数据征信从其本质上来看，是将大数据应用到征信活动中，突出强调的是处理数据的数据量大、刻画信用的维度广、信用状况的动态呈现、交互性等特点。”〔4〕

在结构上，大数据征信即“大数据”与“征信”的结合，它意味着大数据对传统征信的渗透与影响，如在信息上，强调总体性，而非局部性，强调信息之间的相关性，而非因果性。客观上，“征信以采集、保存、分析大量的信息为主，大数据技术为征信提供了一种全新的数据处理模式”〔5〕。由于大数据与互联网之间密不可分的关联，在研究中，亦有人使用了“互联网征信”这一概念，并将其界定为“采集个人或企业的互联网信息数据，并结合线下渠道采集的信息，使用大数据、云计算等技术来评估信用的活动”〔6〕。

大数据征信与互联网征信实为一个问题的两个方面，前者突出的是数据的收集、整合与分析能力，后者强调平台与数据的传输能力。由于数据流动于网络之间，若我们拟对大数据征信有个全面、客观、科学的理解，就必须立于技术的层面对互联网有个基本的认知。互联网是一个由不同类型和规模、独立运行和管理的计算机组成的集合性网络。互联网的关键在于“联”，它表明任何人、任何事物、任何时间与任何地点的实时在线与实时联动。正由于“互＋联＋网”的特性，人们将互联网精神凝练为开放、平等、协作与共享，而这也决定了与传统征信相比，以网络为依托的大数据征信具有以下新的技术特征。

1. 征信数据的广泛性

社会信用是一项体系性的工程，它张扬的是，一处失信，则处处受限，即“意味着失信人在一处出现失信行为，就会处处受到限制”〔7〕。为了确保社会中的每个人都能坐言起行与言而有信，征信数据多多益善。由于分析技术及数据源狭窄等原因，传统征信难以全面有效覆盖。当下，互联网、移动智能终端的普及和大数据挖掘技术的发展已使这一难题迎刃而解，大数据征信

〔2〕 陈小梅：《我国大数据征信业发展实践与完善路径》，载《福建金融》2017 年 12 期，第 59 页。
〔3〕 刘晓：《我国大数据征信个人敏感数据保护困境及保护机制研究》，载《西南金融》2019 年第 1 期，第 30 页。
〔4〕 孔德超：《大数据征信初探——基于个人征信视角》，载《现代管理科学》2016 年第 4 期，第 39 页。
〔5〕 鞠卫华：《大数据征信特点及其风险探析》，载《金融科技时代》2017 年第 2 期，第 30 页。
〔6〕 余丽霞、郑洁：《大数据背景下我国互联网征信问题研究》，载《金融发展研究》2017 年第 9 期，第 46 页。
〔7〕 沈岿：《社会信用体系建设的法治之道》，载《中国法学》2019 年第 5 期，第 29 页。

的征信对象可以无遗漏地覆盖全部网络使用者。同时，用户行为属性具有多样性，其遗留的数据已全方位地涉及人们物质与精神生活的方方面面。大数据使传统征信正面临一种脱胎换骨式的变革，因为“大数据征信将传统征信的金融借贷扩展到其他的生活场景，从信用主体的消费、出行等行为信息也可推断出其相关的资质和能力，为信用评估提供多角度的评判场景”〔8〕。

2. 征信数据的海量性、低成本性与实时性

大数据的首要特征在于其数据产出量与存储量的巨大。虽然这些数据具有价值低密度性，但是它向人们展现了以下事实：我们正生活于一种不断变化但却日趋被严密监视的状态中。我们的一举一动都可以在某个数据库中找到对应的线索。大数据第一次毫无歧视地为我们每一个人保留了详细的行为记录，而这为信用评价提供了丰富的素材。互联网信息具有实时、全貌及线上与线下相结合的特点，而传统征信的信息来源渠道狭窄、单一，且多以昨天的信用记录对今天的信用状况进行评估。虽然在网络技术的支撑下，大数据征信优势显著，但是其开放、平等、自由等特点也使得征信市场应有的安全、公平、利益平衡等底线价值面临严峻的挑战，如“平台征信数据具有较强的时效性，但同时也会产生大量无用、虚假的信息噪音，而互联网技术并不能从海量的信息中辨别、遴选出真正有用、真实的信息”〔9〕。

3. 数据存储的便捷性与处理的智能性

大数据征信的亮点在于大数据接入、大数据存储、大数据共享与交换、大数据展现及大数据分析与挖掘技术，而这彻底革新了征信的观念与模式，从而极大地推进了社会信用的建设。随着数据技术的发展，数据多以电子邮件、视频、语音、图像等非结构化或半结构化的方式体现，且存储工具与模式日益翻新与多样化。人工智能是大数据的时代技术标签。“随着数据量呈几何级数的增加，征信机构甚至可能并不需要投入硬件来建立实体数据存储设备，而是通过技术创新，形成由大规模计算机集群组成的‘云’存储大数据。”〔10〕

在大数据技术下，智能化的数据平台可自动完成信息生成、传送、收集、整理、加工、分析等一整套工序，平台多具有强大的信息捕捉、组织、排序与检索功能，可低成本、高效率地满足信用评价的数据需求。更重要的是，借助大数据与云计算，还可将大量破碎、难以量化的“软信息”提炼为可以进行信用识别与定性的“硬信息”。

4. 征信数据使用范围的宽广性

这主要表现在以下几个方面：一是信用评价趋于生活化与常态化。在用途上，不再局限于传统的银行信贷融资，而被广泛地应用于网购、住宿、医疗、出行等日常活动。二是被用于网络借贷的资信评估。为了控制信用额度与风险，一些网贷企业通过自身的数据征集对借款人的信用度进行考评，如“芝麻信用”就从客户的信用历史、履约能力、行为偏好、身份特色和人际关系五个方面来采集信息，以作为发放贷款的重要条件。三是应用于学术评价，遏制学术不端行为。庞大的数据库可以集中海量的学术成果，数据查重系统可以提供学术信用评价。四是为社会治理提供有力

〔8〕 贾拓：《大数据对征信体系的影响与实践研究》，载《征信》2018年第4期，第19页。

〔9〕 陈小林：《我国互联网金融征信体制建设路径思考》，载《征信》2015年第1期，第29页。

〔10〕 戈志武：《大数据征信监管研究》，载《西南金融》2017年第4期，第14页。

· 5 ·

的数据支持。信息的占有量、种类及定性分析等直接关系到政府对行为人行为模式、遵纪守法性的预判，这可以极大地提升社会治理效率，降低治理成本及对风险进行事前防控。

（二）亟待解构的法律治理问题

大数据征信不仅意味着社会信用与价值在互联网、云计算、人工智能等技术激励下的放大与升级，更意味着一种利益的重置与法律的革新。在探究社会信用法律治理改良时，在顶层设计上，以下问题应纳入深思的范畴。

1. 数据特性的协调

大数据给征信创新提供了历史机遇，但是人们依然对以下问题心怀忧虑：这些数据能否全部用于征信、如何确保数据的客观性与准确性、如何防范大数据的黑箱操作等。大数据、网络与云计算是大数据征信的基础，但是如果我们致力于将这种方式融入法律化的生活，那么就不得不面临以下现实："执迷于精确性是信息缺乏时代和模拟时代的产物。只有 5％的数据是结构化且能适用于传统数据库的。如果不接受混乱，剩下 95％的非结构化数据都无法被利用，只有接受不精准性，我们才能打开一扇从未涉足的世界的窗户。"〔11〕

"传统的信用评价模式主要是关注、分析考察对象的历史信息，数据少且时效性差，而大数据征信将注意力从数据的精确性转移到数据的相关性上。"〔12〕因此，有人认为，大数据无法消除不确定性，而不确定性即意味着风险。如果由于大数据的零碎、"噪音"等缺陷而在征信观念、模式上裹足不前，那么不仅会导致社会信用评价资源的浪费，而且自限的做法也会抑制新事物的萌芽与成长。实际上，大数据征信面临两种可能性：一是丰富与多元的信息使信用评价结果更加客观、科学与公正；二是信息"噪音"或"脏度"过大影响评价结果的精确性。大数据时代，虽然人们可获取的信息量巨大，但是低劣、虚假、失真的信息也混杂其中，数据漏报、错报、假报等现象也频频发生。数据是征信机构的重要资产，为其安身立命之本。信用国家建构中，确保征信数据的真实性、关联性与完整性应是关注的重点。

2. 利益平衡下的安全保障

大数据技术的迅猛发展正在日益刷新人与人、人与社会、人与自然之间的关联模式，使传统法律秩序遭受巨大的挑战，如信息传递、采集的广度、深度、速度等特质使得信息越来越公开与透明，而这进一步使得隐私权保护变得举步维艰。当人类共同体的利益与安全受到威胁与冲击时，借助法律的方式寻求妥协与平衡就成为必然。在社会善治中，法律被寄寓了平等、自由等多种理想元素，但安全是其他价值的基础。与传统征信相比，大数据征信使得数据安全问题更加突出，这主要表现为：数据的过度采集会干扰人们的日常生活，无度挖掘会深度触及公民的隐私或企业的商业秘密，计算机网络系统的故障、黑客攻击与无处不在的木马程序等使消费群体的金融与隐私数据时刻面临可能的外泄风险。

法律治理的目的不是自由，而是安全与平等。虽然大数据革新了征信模式，但是若不能通过法律治理给予民众网络信息的安全感，那么很有可能我们会为其发展付出更多的成本。信用国家

〔11〕〔英〕肯尼思·库克耶等：《大数据时代——生活、工作与思维的大变革》，盛杨燕等译，浙江人民出版社 2013 年版，第 45 页

〔12〕 植凤寅：《大数据征信与小微金融服务》，载《中国金融》2014 年第 12 期，第 91 页。

建构中，作为公民，我们有义务让社会了解我们的信用记录，但我们的隐私权与数据安全权也理应得到社会的尊重。然而，我们不得不面对一个困境，即数据保护与隐私权是否为同一概念，或者说隐私权保护本身是否包括了数据保护。“作为一种价值，隐私是一个非常复杂、既相互配合又自相矛盾的概念，它被塞满了各式各样确切的意图。如果想将之彻底解决，这是件令人沮丧的事情。”〔13〕

法律为善良与正义的艺术，事关和谐与统一。在时下的法律体系中，人们惯于从因果关系的角度来理解行为、责任、权利与义务之间应有的正义关联。然而，当大数据盛行及大数据与征信结合时，这一熟知的“公理”将会被打破。大数据预测与信用评价下，在社会治理中，行为人将不是因为做了什么而受到惩罚，相反，是因为将要做什么而受到惩罚。理性而言，基于未来可能行为的惩罚是对正义的亵渎，因为正义的基本逻辑是，行为人只对其所作为承担责任。虽然大数据预测为我们打造一个更安全、更和谐、更有秩序的社会提供了技术支撑，但也否定了我们人之为人的一个重要价值，即自由选择与责任自负的能力。当大数据及大数据征信成为集体选择的工具时，我们也不得不弱化或放弃意志的自由。法律是利益固化与风尚引领的方向标，大数据征信治理中，利益如何平衡也是法律必须厘定的问题。

3. 数据共享与利益冲突

虽然网络技术的发展推进了信息传播、搜集与共享，但是其仍不足以为大数据征信提供全面的支撑。当下，底层数据缺乏，如日常的教育、住房、社保、医疗、学术诚信等基础数据尚未完全并网，社交数据与支付数据等亦相互闭锁，“信息孤岛”现象严重阻滞了社会信用的建构。征信意在从社会整体上防范与惩戒失信。然而，大数据征信却落入了一个故步自封的陷阱，这不仅是对互联网共享、协作精神的背离，而且私利驱动下的“自我封锁”也必然造成大数据征信行业标准的缺失与征信资源的浪费。行业标准的缺失会引发以下连锁性反应：各大数据征信平台推出自设的征信标准→类似的数据在不同的征信平台形成截然不同的评价结果→消费者受到不公正待遇→恶性竞争→市场紊乱→社会信用受挫。

本义上，征信特指为了弱化或消除信息不对称现象，专业的第三方机构依法采集、存储、整理与加工有关自然人、法人等的信用信息，并以此为基础，帮助经济主体判断和控制交易风险的信用中介服务活动。因此，专业、中立与公正是对征信业的必然要求。然而，就现实而言，许多大数据征信平台既当“裁判员”，又当“运动员”。如“阿里巴巴办理征信的天生缺陷就是不具备独立于金融交易双方的第三方资质，一个企业不能既从事金融交易，也做征信”〔14〕。京东亦顺手将京东商城海量的消费数据作为信用评价的依据，以向客户营销其金融信用产品。

4. 立法模式选择

在研讨大数据征信中，有必要辨识其与传统征信的异同，因为这直接涉及法律体系的分类建设。在追求法律的科学性与严密性中，立法者往往将人、物与行为归于一定的类别，并依据共同的标准对其进行调整。就法律治理而言，如果大数据征信与传统征信具有高度的同质性，那么理

〔13〕 Post，Robert C.，Three Concepts of Privacy，89 *The Georgetown Law Journal*，2087－2098（2001）.

〔14〕 刘新海：《阿里巴巴集团的大数据战略与征信实践》，载《征信》2014 年第 10 期，第 12 页。

所当然地，其应属于同一个法律体系，而无须分置立法。反之，则不然。实质上，大数据征信只是征信技术、方法与模式等的改变，其传统的以社会信用为目标的征信功能与价值并没有改变，更贴切地说，大数据征信只是数字技术支撑下传统征信的更新换代。

（三）社会信用建构：大数据征信治理的目标

“无物不互联、无处不数据”的大数据时代，征信业务大数据化已是大势所趋。在这种浪潮下，一些原有的征信机构也主动开始转型，如北京安融惠众征信、北京宜信至诚信用评估等。此外，腾讯、京东等互联网企业也嗅到了这一商机，这些新动向必然会推动征信业法律治理的变迁。任何一种制度与理论都应是针对某个特定时代的问题所作出的一种经验性回应。现实是，大数据正在润物细无声地创新人类的思维方式，使我们的思维模式从串联性的因果关系向并联性的相关关系发展，使我们的物质与精神生活立于数据之上。凡物皆可数、数据人、数据资产已成为我们这个时代的特征。

法律是人类生活经验与理性的浓缩，代表一个社会最具有权威性的价值准则。网络化的大数据征信不仅使原局限于银行征信数据的时代一去不返，而且也彻底革新了传统征信的理念，因为它“强调一切数据皆为信用、所有信息看关联不看因果、错的信息也是关键信息”〔15〕。在法律还没有及时介入时，逐利性使得大数据征信在电子商务、网络社交平台等的推动下获得蓬勃发展。当法律演进滞后于技术创新时，由于法律体系外的漏洞，现时的征信制度不可能对大数据征信从一个“入市→运营→退出”的生命周期作出事无巨细的安排。然而，这并不表明，在互联网精神的统摄下，这一领域就成了一个绝对自由、可随意侵犯他人隐私、侵蚀国家主权的“飞地”。人民的安全是至高无上的法律。在信息的攫取、占有等几乎无孔不入的情况下，或许这句格言能指引我们信用法律治理前进的方向。

大数据技术使人类正处于一个变动不居的世界中，而这使得社会信用建设尤为紧迫。“世界的变化与突发事件使得人们无论行动与否都处在一种风险之中，风险是不可回避的。人们化解或预防风险之道在于信任，由于熟悉导致的信任变得有限，社会需要一种系统信任，即制度化的信用。”〔16〕虽然我们日渐接受了法律理性的论断，但是又不得不承认作为理性产物的法律还与人类的经验紧密相关，而这也是大数据征信治理必须考虑的问题。大数据并不完美，在有关大数据征信的不同观点之间的针锋对垒中，法律治理之路究竟该何去何从？在法律的勾勒中，大数据征信是作为外在经验而存在的，如果立法者的意图是拟配置与其相适的法律规则，以引领、规范、保障其发展，从而促进信用社会与信用国家的建构，那么从“问题是什么→法律是什么”的角度来审视就是一个事半功倍的研究方法。

二、社会信用建构的瓶颈：我国征信治理存在的问题解析

（一）宏观上的短板：应有法律理念的缺位

在人类的繁衍与发展中，功利主义对人们行为的选择总是充满着难以抗拒的诱惑力。受利益

〔15〕 刘旭、赵玉清：《大数据环境下互联网征信发展与监管研究》，载《河北金融》2016 年第 4 期，第 6 页。

〔16〕〔英〕安东尼·吉登斯：《现代性的后果》，田禾译，译林出版社 2000 年版，第 6－8 页。

的驱使，在法律的进化中，它也直接左右了法律人的方法论，使人们更多不是从最先的事物、原则、范畴和假定是必需的东西出发，而是将最后的事物、收获、效果作为选择的标准。虽然目的正当决定手段正当提高了制度创制的效率，但是还必须深刻地认识到，功利性的法律还必须接受理念的监督与守望。“法律是按照其意义必须服务于法律理念之物。”〔17〕我国征信法律治理起步相对较晚，在理念体现与贯彻方面，其仍存在以下值得深思之处。

1. 立法缺乏前瞻性

法律必须时刻具备成长的原则，这决定了法律必须紧跟时代发展的诉求。我国征信法律制度的建设也只是近几年来的事情，如较早的《征信业管理条例》便诞生于 2013 年 1 月。同期，一些大数据征信平台也应景而生，如上海资信旗下的“互联网金融征信”（NFCS）推出于 2013 年 6 月，“安融惠众信用信息共享平台”（MSP）于 2013 年 3 月正式上线。这种状况表明，我国的征信制度构建与大数据征信之间并不存在明显的时差。然而，纵观这些规范文件，我们难以从其字里行间里捕捉到与大数据征信直接相关的内容。

大数据语境下，“大数据既是一种资源，也是一种分析、预测工具，可以将过去难以计算、存储、分析、共享的事物变得有利用价值，并可预测未来，帮助人们认识世界”〔18〕。大数据为社会信用度量提供了一个全新的广角，基于充沛、多途径、交叉互补的数据，征信机构可以将行为人多属性的零碎性的信息串联起来。“虽然征信活动的实质和征信业务开展的原则并不发生根本性的改变，但是大数据征信改变了数据采集、整理、保存、加工、提供的方式和手段。”〔19〕尽管大数据征信与传统征信存在源流关系，但是大数据征信却会带来一系列破局性的改变，如数据特质、征信理念、征信方式、征信内容、评价方式，甚至评价结论都会发生根本性的变化。法律的与时俱进、法律先于立法说明理性的立法必须为明天时刻准备着。客观而言，新技术应景下，未来性思考的缺失是我国时下征信法律治理应着力解决的瑕疵。

2. 法律问题政策化与道德化

为了践行社会信用体系与巩固诚信的社会价值观，近年来我国推出了一些纲举目张的政策性文件。虽然这些文件是我国社会信用建设的方向标，但是“建设法治化的社会信用体系，需要统一的信用立法，划定社会信用制度的规则界限”〔20〕。依法治市中，“信用不再仅是道德约束或法律解释的对象，而是须通过具有权威性、可量化、可公开的信息来表征的特定主体的守法或履约状态”〔21〕。依法治国代表了认识大同，以法律的方式，而非政策或道德的方式就是我国征信法律治理前进的路标。

民无信不立，业无信不兴，国无信则衰。虽然道德的教化能塑造与固化人们的诚信观念，使人修身正行，但是人自利的劣根性决定了诚信的确立与维护更是一个刚性的法律制度建构问题。“法律反映或符合一定道德的要求，尽管事实上往往如此，然而不是一个必然的真理。”〔22〕以法

〔17〕〔德〕拉德布鲁赫：《法哲学》，王朴译，法律出版社 2005 年版，第 73 页。
〔18〕连镇殿等：《大数据背景下城市公共信用信息平台建设研究》，载《宏观经济管理》2017 年第 2 期，第 61 页。
〔19〕宋媚：《大数据征信背景下的信息质量度量与提升研究》，上海交通大学出版社 2016 年版，第 8 页。
〔20〕李林芳、徐亚文：《社会信用体系法治化原理探析》，载《学习与实践》2019 年第 11 期，第 29 页。
〔21〕王瑞雪：《政府规制中的信用工具研究》，载《中国法学》2017 年第 4 期，第 159 页。
〔22〕〔英〕哈特：《法律的概念》，张文显译，中国大百科全书出版社 1996 年版，第 181－182 页。

• 9 •

律，而不是纯以道德来强化诚信有助于人们认清法律组织性的权威与强制，并可防止法在“应该这样的”道德评判中化为乌有。“鉴于信用立法是社会信用体系建设的关键环节，因此将政府赋能的社会信用体系建设模式，转变为以法赋能的社会信用建设模式，是新时代社会信用体系建设进一步快速发展的关键。”〔23〕客观上，将诚信建设拉回法治的轨道，无论其是否存在这样或那样的缺陷，这本身就是正义的宣告与胜利。大数据之下，如果我们以信用为核心的征信治理是一个历史、进化的命题，那么它的完善、精致或拙劣等都必须接受“肯定即否定”的检讨。

3. 欠缺体系性

体系即依一定的原则所构成的知识整体，意味着周密、逻辑、整体与一致，是衡量人类对客观事物的认知是否科学的重要标杆。自不待言，征信是一个体系性的系统，“征信体系是指采集、加工和分析信用信息并对外提供信用信息服务的相关制度和措施的总称，包括征信制度、征信标准、信息采集、征信机构和信息市场、征信产品和服务、征信监管等”〔24〕。这种阐释表明在征信治理法律制度的构造上，其应该是一个内部条理清晰、结构严谨的系统，而不应是一个由数个单行文本组合而成的零散体系。

市场需要信息交换，没有信息交换的市场是不存在的。因此，征信法治化对我国向市场与法治国家转型的意义是不证自明的。自 2009 年以来，我国紧锣密鼓地出台了《征信业管理条例》《征信机构管理办法》等文件。遗憾的是，从这种“碎片”式的规范文本制作中，很难得出我国征信法律治理体系化建设的结论。哲理上，人不能两次踏进同一条河流，但是文件名称措辞高度雷同的《征信机构监管指引》与《征信机构管理办法》再次给人一种“踏进同一条河流”的感觉。虽然这些规范文件起到了短平快的应急效果，但是其急功近利与短视也使得我国在征信法律治理的建构上与法律应有的体系性渐行渐远。

在法律制度的创制中，我国立法呈现出浓厚的功利性。虽然在这一思想的宰制下，我国已快速地创建了特色性的信用规范体系，但是规则之间的不一致性、上位法粗放性以致必须依赖下位法或解释来救急等弊端也彰而不隐。作为“冰山的一角”，我国征信法律制度不可避免地存在功利主义的痕迹，如《征信业管理条例》理应顺势基于大数据背景对体系中所涉的征信产品、征信机构、信息采集与使用等规定得面面俱到，但是该条例包括附则在内也只有简单的 47 个条文。也正是由于条文过于单薄，2013 年 11 月中国人民银行推出《征信机构管理办法》，2015 年 10 月又发布《征信机构监管指引》。如此高频的“打补丁”不仅人为地打破了征信制度应有的体系，而且也导致监管权威、治理效果与规则确信的边际效应递减。法律并不是由一个个孤零的条文汇成的综合体，而是作为一个整体性的过程、事业、生活方式而存在。否则，现实存在的法律，只是徒有形式的躯体。

（二）微观上的缺憾：大数据征信具体指引上的难点

大数据已从社交、医疗、支付、电商等多个角度嵌入人们的生活，使人类的生活网络化与数据化。虽然法律必须具有恢宏的灵魂，但是其毕竟又要以一种服务于人类生活细节的方式存在。

〔23〕 谢新水、吴芸：《新时代社会信用体系建设：从政府赋能走向法的赋能》，载《中国行政管理》2019 年第 7 期，第 34 页。
〔24〕 唐明琴等主编：《征信理论与实务》，中国金融出版社 2015 年版，第 16 页。

· 10 ·

在这一点上，既存的征信制度与大数据之间接轨的不畅使得许多细节问题还没有被纳入治理的范畴。同时，法律侧重稳定性与大数据动态性之间的反差也使得有些法律不是作为大数据征信的激励因素，而是作为制约因素存在。

1. 大数据征信平台的市场准入问题

虽然在市场自发力量下，我国已产生了一批大数据征信平台，但是在缺乏准入许可的情况下，这些平台面临适法性问题。2015 年 1 月 5 日，中国人民银行印发了《关于做好个人征信业务准备工作的通知》，要求腾讯征信、芝麻信用、中智诚征信、鹏元征信、拉卡拉信用、北京华道征信、深圳前海征信、中诚信征信八家机构在六个月内做好个人征信业务的准备工作。虽然从该文件，我们可以对大数据征信存在的“合法性”作正面的解读，但它毕竟不是对《征信业管理条例》第 6 条〔25〕核准制的正式松绑。大数据征信是一种创新性业务，在监管者对其合法性没有给予正式认可前，其存在就处于一种适法不明的状态。

此外，“随着数据的积累和扩展，部分企业也有意申请中国人民银行征信牌照，向其他组织、机构有偿提供系统内部数据，开展市场化征信业务”〔26〕。然而，依什么样的标准给大数据征信企业颁发许可证或让传统征信业进行大数据化的提质是一个需要慎重考虑的问题。如果不加分别地适用《征信业管理条例》第 6 条的规定，则可能人为地掩盖或忽视大数据征信平台的特殊性。虽然一脉相承，但是大数据征信毕竟与传统征信有所不同，其特色在于大数据与云计算下信息的互联互通与高效的智能处置。如果从二律背反的思维出发，那么以下可能性就必须引起高度的重视，即“通过互联网采集、传输和提供网络征信服务，容易受到网络黑客和病毒的攻击，一旦出现信用信息被非法访问、截取和篡改，信息系统遭到不可逆转的破坏性影响，将对个人隐私和客户权益保护构成重要威胁，而且网络风险的扩散性和破坏性更大”〔27〕。我国大数据征信刚起步，信息安全体系建设与风险控制经验不足，数据库防护网的大量技术包更是加剧了系统性安全风险。在这一状况下，如果不针对大数据的风险点配置相应的入市条件，则悖于大数据征信应服务于社会信用建构的目标定向。大数据征信最突出的优势是大数据，而这也决定了数据库技术、数据收集、数据处理、数据分析、数据系统安全等是其安身立命之本。因此，除了一般性要求外，数据挖掘技术、数据安全保障、大数据处理能力也应是认证大数据征信必备的资质条件。

2. 数据采集的法律风险

信息的充分获取是大数据征信运作的必要条件。当下，以电商、第三方支付、网络交际等为基础的大数据征信平台多在用户不知悉的情况下采集信息，如“芝麻信用就先利用阿里云业务对搜集的信息进行储存和初步处理，然后对其进行结构化的清洗”〔28〕。如此，就存在违规与侵犯用户权益的法律风险。在用户信息保护上，我国采取的是严格保护主义，如《征信业管理条例》第 13 条即规定：采取个人信息应当经信息主体本人同意，未经同意，不得采集。《网络安全法》第 22 条第 3 款规定：“网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得

〔25〕 该法第 6 条规定，设立经营个人征信业务的企业，必须符合法定的条件，并且经国务院征信业监督管理机构的批准。

〔26〕 方增平：《互联网金融背景下发展新型征信机构的思考》，载《征信》2015 年第 5 期，第 38 页。

〔27〕 黄玺：《互联网金融背景下我国征信业发展的思考》，载《征信》2014 年第 5 期，第 51 页。

〔28〕 李蕾、王雪：《论我国互联网征信业务发展》，载《征信》2016 年第 8 期，第 36 页。

同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。”此外，如果大数据征信机构不经意间采集了宗教信仰、基因、既往病史、存款、商业保险、不动产及纳税额等敏感信息，则违背了《征信业管理条例》第 14 条的禁止性规定；若在征信体系或评估中设立“黑名单”，则涉嫌违反《征信业管理条例》第 15 条的规定，即“信息提供者向征信机构提供个人不良信息，应当事先告知信息主体本人”。

技术使得数据信息可以被物化为书籍、影视作品等，但是同时它又具有非物质性。数据信息能否商品化是一个无定论的问题。“不管怎样，信息无论是在定义上，还是在概念上，均满足不了作为商品所应具备的条件。因此，在人们关注某一危机中，就引入了一个关于信息本身内在根据的学术论题。”〔29〕在已被实然商品化的时下，一个简单而流行的认识是，信息就是能被数字化的一切。既然如此，在信息商品是依存于信息的情况下，基础性的信息究竟属于谁？属于采集人，还是属于信息的制造者（用户）？对此，人们的观点不一。如有人认为：“个人应有权出售自己的信息，并因此会使公司将它们外在化的成本内在化。数据主体将参与数据交易，并可能为隐私自行定价。”〔30〕另有学者则认为：“无论如何，在美国，征信机构确实是数据的所有者，并由此能更自由地使用数据……到目前为止，只有弱小的权力被赋予个人来阻止公司将数据用于营销目的。”〔31〕当下，虽然各大数据征信机构都在几乎零成本地使用用户遗留的数据，但是在法律还没有白纸黑字地确定其权属时，征信业确实整体面临一个“釜底抽薪”的权属争议风险。

3. 信息主体权益保护与征信权利之间的失衡

信用信息共享是一国信用体系构建的核心，是降低信息不对称、遏制欺诈、营造诚信环境的重要手段。互联网时代，“每个人都成为了信息提供者及需求者，各种公私机构都在无时无刻提供并获取信息，而互联网、搜索引擎的检索及查询功能又加速了个人信息的传播、利用及共享”〔32〕。大数据时代，“数据割据、数据孤岛和数据质量是最典型的三大数据治理问题”〔33〕。其中，大数据安全尤为急切，大数据技术能源源不断地为征信机构输送与整理海量的信息，提升了信用评价的效率，但是信息采集的边界与范围日渐模糊，这也导致信息权与数据保护等成为时代焦点。

在表象上，虽然大数据征信导致隐私权衰落与信息不再隐秘，但是信息利用与保护所体现的效率与公平依然是法律中不变的主题。移动支付、网络交际、电子商务、共享经济等与日俱增地加重人类对数字科技的依赖。“无数据，不人权”已成为这个时代的权利诉求。“数字科技必须以人为本，必须把人的利益进而把人的权利作为其最高价值，以人权尺度为其划界，以人权作为评价科技进步的根本标准。”〔34〕在大数据征信体现信息公开的同时，也必须张扬信息的严格保密。否则，在技术与知识的非对称下，就可能滋生肆意采集和泄露信息、监守自盗信息等侵犯信息主体权益的风险。“芝麻信用”就是一个缩影，因为根据不能讨价还价的《芝麻信用服务协议》，用户授权“芝麻信用”采集信息，并同时默示同意在第三方查询非贷款类及其他非涉及商业秘密信

〔29〕 Babe. R. E，*Information and Communication in Economics*，Kluwer Academic Publishers，1994，p. 42.

〔30〕 Samuelson，Privacy as Intellectual Property? 52（5）*Stanford Law Review*，74（2000）.

〔31〕〔德〕尼古拉·杰因茨：《金融隐私——征信制度国际比较》，万存知译，中国金融出版社 2009 年版，第 24－25 页。

〔32〕 张继红：《论我国金融消费者信息权保护的立法完善》，载《法学论坛》2016 年第 6 期，第 93 页。

〔33〕 赵国栋等：《大数据时代的历史机遇：产业变革与数据科学》，清华大学出版社 2013 年版，第 47 页。

〔34〕 张文显：《无数字，不人权》，载《北京日报》2019 年 9 月 2 日，第 15 版。

息时，其可以直接向第三方提供相关信息。大数据征信开启了一个社会信用建构的新时代，但是“信息处理过程的网络化、数字化使得法律监管难以受到有效的监督，成为了法律监管难以企及的法外空间”〔35〕。虽然随着法治国家观念的深入及个体意识的觉醒，我国对个人信息的法律保护已有所建树，但未来仍是长路漫漫。大数据背景下，在个人信息保护上，我国仍存在以下缺陷：

一是所涉法律条文有限、分布零散、适用范围窄，且未体系化。“在个人信息保护方面，我国仍未出台专门保护个人信息及隐私权的法律，如《个人信息保护法》《个人隐私保护法》等。”〔36〕体系化思维的缺席使得我国信息主体保护的法律呈现出一种“群龙无首”与“杂乱无章”的乱象。

二是缺乏对信息主体利益的实质性保护。在保护的法律手段上，我国多重刑罚与行政追责，而轻民事确权与归责，从而导致在遭受侵权之害时，信息主体的财产与非财产损失得不到或难以得到合理与有效的补偿。

三是对基本范畴缺乏应有的明确法律规定。个人信息是一个与个体的生活安宁、不希望他人侵犯或干涉相关的隐私问题。在隐私权保护上，我国《民法典》已有了历史性的突破，“隐私”一词出现了 14 次，尤其难得的是，《民法典》第 1032 条第一次对隐私定义如下：隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。然而，“私密”的概念循环并没有达到准确无误澄清隐私的效果。同时，“空间”“活动”“信息”都是模棱两可的表述。事实是，何谓“隐私”仍然是一个有权者自由裁量的解释问题。

4. 信息采集标准与共享困境

数据开放与共享是大数据征信的基础，而数据标准化是高效共享的前提。征信数据的标准化建设不仅关系到评价结果的权威性与准确性，而且也益于跨机构、跨行业间的数据资源共享。对于这一问题，自 2005 年起，中国人民银行就启动了征信标准化建设，先后推出了《征信数据元个人征信数据元》等金融行业标准。此外，为了抑制“以卡养卡”及“拆东墙补西墙”等失信行为，2020 年 1 月中国人民银行征信中心正式启动了第二代征信系统，以填补第一代系统的信息真空。尽管如此，在数据共享与标准化建设方面，我国仍面临以下问题：

一是还没有建立全国统一的信用信息行业标准。实践中，各部门、各行业和地方政府都各自依据自己的判断与利益来建构征信信息系统，从而导致协调性、共享性、效率性差，如“在缺乏统一的信息统筹协调机构下，信息的跨区域、跨系统调配与交流较为混乱”〔37〕。

二是在互联网数据快速增长的当下，各大数据征信机构都根据各自的来源数据、评价模型、统计口径、评级标准等进行信用评估，如此不仅造成同一信息主体在不同大数据征信机构评价结果上的差异性，而且因“数据壁垒所形成的恶性竞争也可能会削弱互联网公司评级结果的公信力”〔38〕。客观上，“存在信息孤岛、数据壁垒未打通、信用信息共享没有畅通渠道是我国当前大

〔35〕 吴双、冯果：《论大数据征信时代下“技法结合”的个人信息保护》，载《科技与法律》2017 年第 4 期，第 42 页。
〔36〕 苏志伟等：《世界主要国家和地区征信体系发展模式与实践》，经济科学出版社 2014 年版，第 24 页。
〔37〕 李真：《P2P 网贷信用征信：金融分析与法律建构》，载《当代经济管理》2015 年第 7 期，第 88 页。
〔38〕 邓舒仁：《关于互联网征信业发展与监管的思考》，载《征信》2015 年第 1 期，第 15 页。

数据征信乃至整个征信行业面临的现实问题”〔39〕。在征信中，大数据征信机构不能获取中国人民银行征信中心的信贷数据，而只能借助关联度较弱的互联网数据来建构信用评价模型。信用数据分割及法律协调的滞后已严重制约了我国社会信用的发展与提质。

（三）小结：破旧立新

“共享经济的不断壮大需要进一步引入信用机制，加快推进信用体系建设，构建以信用为核心的共享经济发展体系。”〔40〕研究表明，“在一个经济体中，如果人与人之间的普遍信任关系越强，那么这样的经济体更倾向于选择市场主导型的金融体系”〔41〕。虽然近年来，我国征信治理的法律制度在不断推进，以中国人民银行为主导的公共征信系统已初具规模，但是在互联网、大数据等技术的催化作用下，信息交换与传递的方式、数据处理、新的征信观念等无不提醒决策者与监管者，世易时移，法律应因时制宜。破茧而出的大数据征信具有一定的“草根性”，其明显的市场性是对政府主导下征信机制的有力制衡与竞争。当社会关系的发展超越于法律之时，法律就处于变革前的十字路口。正视大数据的功效，通过法典的方式对大数据征信进行法律治理的改良就是时代正确与时代必须。

大数据场景与社会信用下，对于我国征信法律治理的走向，以下问题值得深思：需要什么样的理念来引领中国征信的法律治理；如何在宽严相济之间为大数据征信铺设一条成长的康庄大道；信息保护和大数据挖掘之间的角力如何摆脱非此即彼的困境；征信数据如何共享；如何确保信用评价结果的真实性与准确性，从而不偏离预设的社会信用目标……大数据代表了人类文明的进步与自由度的伸展，其既是创新，又是挑战。然而，“文明是诅咒，还是福音呢？在过去，文明既是诅咒，又是福音。至于将来怎么样，则取决于人类是将过去文明中积累起来的知识用于破坏，还是用于建设”〔42〕。

三、社会信用建构的路径：以大数据征信善治为依托

社会信用问题已严重制约了我国的进一步发展，构建一个以“善治”为核心的社会信用评价体系是时代所需所急，因为“善治本身蕴含了主体之间自觉、自愿、自发地达成善，而不是外界强加的治理理想状态”〔43〕。而这也决定了大数据征信必须立足于社会信用这一时代主题。“社会信用治理中，制度、技术与文化三者不可或缺。”〔44〕其中，制度是关键。大数据不单纯意味着人类超算技术的突飞猛进，更昭示着一场法律制度“革命”的到来。如何实现“数据人→诚信人”的转变是大数据时代下征信法律治理必须积极回应的导向问题。

〔39〕 李友元、寇纲：《我国大数据征信的挑战及对策》，载《大数据》2017 年第 1 期，第 31 页。

〔40〕 于凤霞：《完善社会信用体系促进我国共享经济发展的思考与建议》，载《电子政务》2018 年第 8 期，第 81 页。

〔41〕 陈雨露、马勇：《社会信用文化、金融体系结构与金融业组织形式》，载《经济研究》2008 年第 3 期，第 37 页。

〔42〕〔美〕斯塔夫里·阿诺斯：《全球通史：从史前到 21 世纪》，吴象婴译，北京大学出版社 2012 年版，第 195 页。

〔43〕 何哲：《“善治”的复合维度》，载《公共管理与政策评论》2018 年第 5 期，第 46 页。

〔44〕 程民选、李晓红：《社会信用协同治理：制度、技术与文化》，载《华东师范大学学报（哲学社会科学版）》2015 年第 3 期，第 26 页。

（一）法律治理的宏观进路

1. 尊重与敬畏互联网精神

每一种法律制度都是它所处时代的产儿。大数据征信是传统征信的换代，信息共享是征信功能最大化的保障。互联网下的征信大数据“主要涉及传统央行的征信数据、经营数据、身份数据、社交数据、消费/财务数据、日常活动数据、特定场景下的行为数据等”〔45〕。如果法律是从事物的本质出发来寻找其必然关系，那么大数据征信法律治理的进路就必须遵从互联网自由、平等、开放与共享的精神。自由与平等是社会发展的基础。如果我们认同这一观点，那么政府就必须恪守以市场为导向，激励征信机构使用新技术，〔46〕升级其产品与服务，营造良好的技术创新氛围。文明进程中，我们应对市场精神予以足够的肯定与尊重。我们正身处于一个全新的数字时代，经济数字化已对社会信用建构提出了严峻的时代诉求，我国应致力于打造与数字时代相匹配的社会信用体系。

大数据、互联网代表的是这个时代的文明与气息，它不仅是人类科学探索的进步，而且与人类苦求的自由、平等、协作等人文精神不谋而合。这种精神元素无疑是对我国传统中一些根深蒂固的思想、观念，如保守、特权、等级等进行稀释的中和剂。故而，我国大数据征信法律治理改良应以自由、平等、协作、共享精神为导向，从而为其生存与发展留足市场空间，并在具体的规范之间体现中立、客观、公正的社会信用评价功能。同时，以下思想尤为重要：大凡数据，皆可反映信用，借助大数据及云计算等技术手段让数据“保真”与“发声”是大数据征信的根本所在。

“随着移动宽带技术、网络接入技术的迅速提升，更多的传感设备、移动终端能够随时随地接入网络，加之云计算、物联网等技术的带动，中国移动互联网也逐渐步入大数据时代。”〔47〕庞大的用户群体和应用市场使我国成为世界上为数不多的大数据国家，探索大数据征信及其治理，是市场秩序规范、守法守约意识强化、失信惩戒等的重要手段。技术会改造人的思维模式，并决定法律创新的走向，中国大数据征信治理也必须体现与这个时代相得益彰的技术思维，即在互联网、大数据、云计算等技术的支撑下，对市场、企业价值链、整个商业生态圈、治理法律作时代性的考察。

自由是一个规范的概念，在具有利己性的同时，亦具有利他性。如此推演，就是无论产权的归属与所有制形式如何，在大数据征信市场上，任何人都有依其意愿与法定条件决定入市或不入市的权利。法律在其市场准入的态度上应该是，也最好是注册制，而不应该是存在寻租空间的核准制。就平等而言，我们可以从两个层面进行解读：一是不能因入市者身份、产权者等的不同而采取差别待遇，当禁止在立法与监管中进行不公正、不合理的分类时，在大数据征信平等对待的阶梯上，我们就朝前迈进了一大步；二是征信入市与征信业务机会均等。对此，下述观点是发人深省的：“每一个对于一种平等的基本自由之完全适当体制都拥有相同的不可剥夺的权利，而这

〔45〕《互联网征信》课题组：《大数据时代下的互联网征信》，经济科学出版社 2016 年版，第 168 页。

〔46〕技术是一柄双刃剑，如果技术缺乏伦理，那么就如同人缺乏良知。为了消除不确定性，在技术的研发与利用中，必须通过法律的方式对技术设定严格的伦理要求。

〔47〕肖云鹏等：《移动互联网安全技术解析》，科学出版社 2015 年版，第 7 页。

• 15 •

种体制与适于所有人的同样自由体制是相容的。”〔48〕就协作与共享而言，互联网之所以被称为互联网就在于其“相互”与“联接”，其传导的是“团结就是力量”的合作。在市场运转中，竞争从来不是目的，只是更有效合作的手段，对于大数据征信而言，其理亦然。“任何社会在构想和建设社会信用体系时都隐含着对自身社会和文化的预设和理解，不同的社会和文化思维方式影响着社会信用的路径选择。”〔49〕在体现特色时，大数据征信应体现互联网精神。

2. 利益平衡保护

数据是征信业的核心资产，直接影响与决定着行业的命运。大数据给征信业带来的机遇体现在信息源的广阔性、处理的迅捷性、内容的丰富性及征信应景的多样性。然而，“大数据并不是灵丹妙药，作为一种前沿和创新的工具与技术手段，是传统信息技术的延伸和升华，但还不够成熟，还处于尝试阶段。大数据的负面问题——对消费者的隐私侵犯也是不容忽视”〔50〕。在流程上，大数据征信涉及不同的利益，如：在私人利益上，它表现为征信机构的信息采集、使用的商业化利益与信息主体利益之间的对立与紧张；在公共利益上，它关系到征信市场规范、商业秘密与隐私权保护、数据安全及社会信用等公共利益。

社会需要妥协与和平，就必须削弱与杜绝人们之间的相互争斗，将强力法则归属于更权威的规范。大数据征信所涉利益的分切不公直接影响到该行业的发展及社会信用的营造，在监管权、征信权、信息主体权益保护的博弈中，以下思想显得弥足珍贵，即：没有任何一种利益是绝对权利的，也没有任何一种利益是绝对权力的。隐私权保护是大数据征信治理中的前置问题，但是“任何保护隐私的道德义务并不包括限制大数据的义务，因为大数据应用于商业、社会稳定、公共健康和安全感所带来的福利应优于对隐私的关注”〔51〕。

3. 安全原则

互联网开启了一个大数据的信息时代，在这个时代中的人都是数据化的信息人。信息安全与每个社会主体的生存利益密切关联。在丧失强力保护的情形下，人们无异在阳光下“裸奔”。虽然在大数据征信治理的变革中，平等、自由、共享等思想迎合了互联网精神的本质，但是在法律精益求精的设计中，这还并不是价值的全部，它还必须优先考虑安全因素，因为安全是至高无上的法律，安全是利益平衡下大数据其他价值实现不可或缺的基石。

一个公理性的认识是，发展依于安全与秩序，自由与共享等也只有在安全的佑护中才具有真实性，因为“安全有助于使人们享有的生命、财产、平等和自由等其他价值稳定化，并使其尽可能地延续下去”〔52〕。如果大数据征信法律治理的改良是为了实现我中华长久的国泰民安与繁荣富强，那么在我国社会信用建构的开拓进取中，以下思想值得铭记：一个旨在实现正义的法律制度，会致力于在自由、平等、安全等方面创设一种切实可行的综合体，且赋予人的自由、平等和安全应当在最大程度上与人类的共同利益保持一致。

---

〔48〕〔美〕罗尔斯：《作为公平的正义——正义新论》，姚大志译，上海三联书店 2002 年版，第 70 页。

〔49〕黄晓晔：《社会信用建设的逻辑及其路径选择》，载《贵州社会科学》2014 年第 5 期，第 46 页。

〔50〕刘新海：《征信与大数据》，中信出版社 2016 年版，第 7 页。

〔51〕Anita L. Allen, Protecting One's Own Privacy in a Big Data Economy, 130 *Harvard Law Review Forum*, 74 (2016).

〔52〕Christian Bay, *The Structure of Freedom*, Stanford University Press, 1958, p. 19.

4. 体系化思维

体系化是法律科学的必然要求，社会信用治理亦是一项体系性的社会工程。对此，《国家十三五规划纲要》在第 17 篇“加强和创新社会治理”中就专门强调社会信用体系完善，其内容包含健全信用信息管理制度、强化信用信息共建共享、健全守信激励和失信惩戒机制及信用服务市场培育。《信用纲要》的诚信建设就系统地覆盖了政务诚信、商务诚信、社会诚信与司法公信四个方面。就征信而言，“征信体系的建立，有助于识别和监测信用风险、激励借款人按时偿还债务和履约，促进金融和经济发展”〔53〕。社会信用构建是一个政府、市场与社会三方关系理性厘定的系统工程。为了对社会信用体系提供应有的支持，我国大数据征信治理法律的体系化可从以下三个方面进行突破：

一是走法典化的道路，而尽可能地避免走“细则”“暂行”“试行”等解燃眉之急的老路。在这一点，欧盟是比较成功的典范。2018 年 5 月欧盟《一般数据保护条例》（GDPR）正式生效。为回应法律落差与时代需求，该法从管辖范围、数据主体权利强化、数据处理者责任、执法与处罚等方面对前期的规则进行了系统性的革新。法典是通向自由的“圣经”。鉴于当下形散的情况，我国有必要对《征信业管理条例》《征信机构管理办法》及通知类等文件进行归整，使其系统化与整体化。

二是实现辅助性法律对征信治理体系化的外部支撑。独木难成林，体系内的征信治理法律的有效运转、市场规范与利益平衡等还需要体系外的制度扶持，从而形成一个良好的内外循环系统。在该问题上，美国的做法是值得借鉴的，如除了《公平信用报告法》，其还专门配备了《公平债务催收法》《金融隐私法》等多部法律，形成了一个完整的征信法律体系。

三是建立体系性的社会信用。根据《信用纲要》等文件的精神，构建一种系统的社会信用体系是国家治理的目标。“由于我国建立的是广义的社会信用体系，因此还需要围绕公共信用信息管理、信用监管、红黑名单管理、联合奖惩等方面建立有中国特色的信用立法。”〔54〕政府信用、企业信用与个人信用是社会信用体系三大鼎立的支柱，而在这之中，政府守信是重中之重，为法治政府的要义所在。在大数据征信治理中，有必要对征信对象作扩张性规定或解释，征信对象不仅应包括自然人、营利法人，同时也应包括社会团体、事业单位、社会服务机构、基金会等非营利性法人及特别法人，以最大可能地让大数据征信覆盖社会中的每一个角落，而无论其是权利者，还是权力者。

（二）微观关键性问题的应对之策

1. 大数据征信准入条件

当下，一些无牌照、无约束甚至非法的机构和个人正在通过各种途径采集、倒买倒卖公众信息，以牟取暴利，从而对正规征信机构产生劣币驱良币的逆淘汰效应。因此，严格规范大数据征信平台的市场准入标准是当务之急。虽然对于入市条件，《征信业管理条例》《征信机构管理办法》等从股东信誉、最低注册资本金、任职资格、信息系统安全等方面作了硬性要求，但是大数

〔53〕 郭熙保、徐淑芳：《全球征信体系的制度安排及其影响因素》，载《学术研究》2005 年第 11 期，第 31 页。

〔54〕 韩家平：《关于加强社会信用立法的思考与建议》，载《征信》2019 年第 5 期，第 5 页。

据与互联网语境下，仍有必要对入市条件作更细致的推敲，以应对技术的要求。大数据意味着，“新的信用风险体系的一个颠覆性的基本思想是一切数据皆信用，这需要大数据技术来支撑”〔55〕。是故，除了注册资本等常规性的准入条件外，对拟新设的大数据征信机构与业务拟大数据化的原征信机构更应注重信息安全保障的软硬件设施、数据处理能力及内部控制等审慎要求。2017 年 6 月开始实施的《网络安全法》涉及网络运行安全、信息安全、监测预警与应急处置等重大内容，它标志着网络空间必须依法而治，这也为我国大数据征信机构的软硬件配置标明了底线条件。数据是大数据征信的基石，除了一般要求外，还必须通过法律明确大数据生命周期安全的概念，强调“大数据生命周期的安全以数据为中心，重点考虑大数据生命周期各环节中的数据安全问题”〔56〕。

由于个人数据直接涉及隐私权，且在财产数据化的时下，个人数据关系到公民的财产安全，所以对经营个人征信业务的征信机构的信息安全保障标准应高于经营企业征信业务的标准。虽然个人征信与企业征信存在一些差异，如企业征信市场发展自主性强，不涉及隐私权保护，但是当这两种业务混同于同一机构时，应将风险隔离墙作为入市的重要标准。如此，不仅可以防止信息泄露风险在同一机构不同部门之间传递，而且也可以作为一种未来可能涉诉案件的防御性抗辩。在具体要求上，征信机构应采取物理空间隔离、人事独立、财务分置、网络系统分离、业务分开等方式构筑个人与企业征信业务风险交叉传染的防火墙。

2. 大数据征信规则的优化

虽然《征信业管理条例》对信息采集范围、采集程序与方式、负面信息保留期限等进行了规定，但只是确定了基本原则，专业性与操作性不强。针对这种现象，可从以下几个方面进行精进：

一是进一步明确数据采集与加工的合法边界。采集的合法性不仅关系到大数据征信机构数据产品商业化目的之实现，而且也可以保证各主体之间的利益平衡。在这一点上，我国《个人信息保护法（草案）》已有了实质性的突破，如该文件将个人信息界定为：以电子或其他方式记录的与已识别的自然人有关的各种信息，不包括匿名化处理后的信息。个人信息处理应采用合法、正当的方式，并遵守公开、透明与诚实信用原则。同时，文件在明确个人敏感信息的基础上，确立了强力保护的规则，如必须取得信息主体的同意，并事前告知可能的影响等。

二是确保征信信息的准确性。征信数据质量不仅事关信用状况的公正评价，而且也关系到征信社会信用功能的实现，如美国 1996 年的《消费者信用报告改革法》就强调，征信机构必须对消费者投诉的不准确信息进行查实，将核查结果告知消费者，且必须通过全国征信机构的联合通知系统将该结果向其他征信机构公开。若经调查，信息失实，则必须在 30 天内予以删除，且不得重新写入。

三是强化信息主体的制衡作用。信息主体的异议权与投诉权不仅益于信息的准确性，而且也能督促大数据征信机构在信息采集与加工中尽到谨慎与勤勉的义务。社会信用建构中，“阳光”

〔55〕 刘新海、丁伟：《大数据征信应用与启示——以美国互联网金融公司 ZestFinance 为例》，载《清华金融评论》2014 年第 10 期，第 98 页。

〔56〕 陈兴蜀等：《大数据安全保护技术》，载《四川大学学报（工程科学版）》2017 年第 5 期，第 4 页。

是失信行为最好的消毒剂。为了保证信用评价的客观性，应强化征信机构免费为信息主体提供其个人信用报告的义务。

为了不让这一目的落空，有必要对信息主体的诉讼救济作以下安排：当信息主体对征信机构的异议权不能实现时，其可以通过民事诉讼的方式来维护其权益。同时，在证据规则上，可考虑实行举证责任倒置。“如果要求消费者来证明信用报告机构存有过错，这将置其于不利地位，因为后者很可能占有所有信息。在诉讼中，信用报告机构占有绝对的资源优势，且实际损害极难证明。”〔57〕征信的目的在于失信惩戒，但是“信用联动奖惩机制设计的初衷并不是要一棒子将失信者彻底打死，而是要让失信主体付出代价后，知晓守信的重要性，给予失信主体改过的机会”〔58〕。因此，在大数据征信治理中，本着社会信用的目标，应允许失信人在法定条件下享有信用修复与补救的权利。

3. 隐私权保护强化

大数据时代，由于个人信息的获取、存储、传播等所涉环节错综复杂，由此形成了一条盘根错节的黑色利益链。App 泛滥之下，对个人信息的过度开发与采集使公民的隐私面临前所未有的危机。客观上，“只有遵守保护个人信用信息隐私权的一系列原则，征信活动才能在正当范围内进行”〔59〕。因此，在大数据征信法律治理的解构中，对该隐私权保护的程度与有效性直接影响到征信制度的正义。虽然《征信业管理条例》用排除法圈定了信息的可采集区域，但这是否就意味着，凡不在排除范围内的信息，均可自由采集呢？在公民因信息外泄而不堪其扰时，这是一个必须认真对待、兼有法律性与政治性的复合性问题。实质上，强力保护网络用户的个人隐私与大数据征信是两个并行不悖的问题。对个人隐私的有效保护能使网络用户无后顾之忧地使用网络，从而通过消费等促进互联网及大数据征信的发展。大数据征信蕴藏着巨大的公共利益与秩序，隐私代表着私人空间与权利。大数据下，如果法律不能在公域与私域之间做到泾渭分明，那么隐私权保护的前景也并不乐观，因为“在政策是否有必要调整上，我们过去的探讨多集中于原则，但是现在我们的讨论越来越务实，比较关注保护的成本”〔60〕。

大数据技术加剧了隐私的“电光化”风险，这也促使我们不得不在新形势下对隐私权作出时代性的解读。时下，如果我们对隐私权的认知仍停留于传统的“个人安宁的生活不受干扰”的消极权利，那么这显然背离了互联网、云计算等社会技术背景。实际上，大数据催生了个人信息隐私权走向何方的时代命题。虽然我们可通过单行的规则来应对这一问题，如将向他人出售、提供公民个人信息情节严重的行为入罪，但是相对于个人信息的系统保护而言，这只是“杯水车薪”。如果我们治理的目标是致力于构造厚实的个人信息保护的“法律长城”，防止征信机构等权利/权力的滥用，那么就有必要出台专门性的“个人信息保护法”，并重点考虑以下几个问题：

---

〔57〕 Austin H. Krist，Large-scale Enforcement of the Fair Credit Reporting Act and the Role of State Attorneys General，115 *Columbia Law Review*，2319－2322（2015）.

〔58〕 肖卫兵：《我国社会信用立法若干问题探析》，载《电子政务》2017 年第 6 期，第 68 页。

〔59〕 张晓军：《论征信活动中保护个人信用信息隐私权之目的特定原则》，载《中国人民大学学报》2006 年第 5 期，第 86 页。

〔60〕 Gus Hosein，Returning to A Principled Basis for Data Protection，84 *Chicago-Kent Law Review*，803－809（2010）.

一是与时俱进地明确隐私权的内容。虽然对隐私权进行抽象的概括能起到指引的效果，但是为了消除“市场假象”，还必须对隐私进行详细的列举。数据隐私时代，增强数据主体权利是对抗不法侵害最有力的武器。欧盟的 GDPR 就体现了这一思想，如该法专门确立了数据主体的更正权、删除权、限制处理权与携带权。

二是将“从设计着手保护隐私权”的思想植入到软件产品研发与销售的管理中。“在电子化时代，数据保护面临诸多挑战，为了强化对个人隐私权与数据的保护，在新的法律框架中应要求相关企业将保护隐私权的概念融入其产品设计中，而不是完全依赖于那些没有多少人愿意读的隐私保护政策。”〔61〕同时，可考虑将隐私权保护纳入大数据征信机构的日常合规管理，“公司应该持续地对其数据采集、储存、分析与使用的政策进行评查”〔62〕。

三是可考虑根据信息的敏感度不同，确立强弱相宜的保护标准。虽然我国《个人信息保护法（草案）》已体现了这一精神，但是这些纲领性的规定更多只是指明了保护的方向，难以满足现实的保护诉求。为了解决这一困境，有必要采取列举的方式对一般类和敏感类数据进行说明，如敏感性数据包括种族、宗教信仰、政治倾向、健康状况、世界观等。对敏感类数据，根据侵害程度、情节等的不同，分层级性地给予严格的保护，并规定除法定例外情形外，不得对敏感数据进行处理。

四是严格控制与规范金融、征信、电信、交通、教育、医疗等大众型服务机构对消费者的信息保密义务。同时，对政府部门利用公权力泄露个人信息的行为进行重点遏制。在个人信息采集上，确立有序开放原则，即“个人信用信息的开放、收集、加工、披露和使用，都应制定并遵守一定的法律规则，力戒个人信息无序开放和随意滥用现象的发生”〔63〕。

4. 征信信息共享机制的建构

“征信的本质是实现信息分享，全面反映信息主体的信用状况”〔64〕，从而降低当事人的逆向选择风险，防范可能的道德风险，并对风险进行准确定价。“在我国，政府主导下的征信体系建设取得了显著的进步，但是征信体系建设的目标并非一个完全由政府控制的公共征信体系，而应是一个高效的面对市场的征信体系。”〔65〕市场是一个比较优势理论下，开放、共享、协作的概念。由于体制的原因，目前大量的信用信息分散存留于工商、税务、法院、公安等部门或政府搭建的信用数据系统。“走向成熟的社会主义市场经济途中的当代中国，必须把信用与诚信意识作为一种经济、政治、文化的准则，全面融入社会生活中。”〔66〕大数据下的社会信用建构急需破除“数据孤岛”，坚持中立的第三方信用评价，注重市场机制效应，从而体现信用社会治理的公开、公平与公正。

对于数据共享，我们可以采取分步走的方式：一是在整合的基础上，推进政府各部门的信息数据与金融信用数据库的“紧密对接”，从而加快跨部门、跨区域的信用数据资源的共享、开发

〔61〕 Rebecca Wong，Data Protection：The Future of Privacy，27 *Computer Law & Security Review* ，53－57（2011）.
〔62〕 Hugh J. Watson，Addressing the Privacy Issues of Big Data，19 *Business Intelligence Journal*，6（2014）.
〔63〕 吴国平：《个人信息开放与隐私权保护》，载《法学杂志》2005 年第 3 期，第 75 页。
〔64〕 王晓明：《征信体系构建制度选择与发展路径》，中国金融出版社 2015 年版，第 10 页。
〔65〕 李清池等：《信用征信法律框架研究》，经济日报出版社 2008 年版，第 102 页。
〔66〕 俞思念：《对我国社会信用体系建设的再思考》，载《湖北社会科学》2018 年第 1 期，第 26 页。

与利用。二是指引、鼓励不同类别的征信机构之间的信用数据共享。为了打破自我循环，我国应尽可能地统一线上与线下的征信标准，统一接口规范，确立平台、机构之间数据资源互通有无的指导性规则。同时，由于征信的目的在于信用风险识别，所以在征信大数据应用时，不能奉行“全部拿来主义”，而应剔除一些无关联或关联度不大的数据，只筛选房租缴纳、遵纪守法、话费交付、公共事业缴费、支付交易、信贷记录、学术诚信等关键数据，并以此作为共享的基础。三是鼓励大数据征信平台数据库系统的建设。若大数据征信系统与金融信用基础库之间存在映射关系，则可以考虑将其收纳为中国人民银行征信系统的子系统。四是有条件地尝试将成熟的大数据征信企业接入中国人民银行的征信系统，从而实现数据资源的共享与共建。

征信数据资源共享是一个与征信标准化建设相关的问题。当下，我国在征信标准化方面还远没有实现数据接口、信息分类及资料定义等基础技术标准的统一。为了打破这一僵局，我国可以考虑由中国人民银行牵头制定全国统一的信用信息采集与分类标准、信息主体标识与基本术语规范及接口标准等，并根据大数据征信的特点，对相关标准进行针对性的改造，以保证其标准性、科学性与效率性。同时，鼓励龙头性的大数据征信平台根据自身的行业要求研发征信标准，在经过认证与评估后，可考虑将其升级为国家行业标准。

5. 法律责任完善

制度不可能建立在无私的爱与宽容之上。为了权威、尊严及宣告法律的激励或惩罚信用，法律必须有牙齿。虽然我国《征信业管理条例》等用专章规定了征信机构不作为的法律后果，但是其存在责任主体覆盖范围狭小与民事责任虚置等缺点。而且，“征信机构与被征信的消费者个人权利义务存在严重的不对等”〔67〕。若大数据征信机构意图与政府携手在信用中国打造中扮演一个不可替代的角色，那么依法依规征信，并保证信用评价的公正性就是其职责所在。为了确保处于强势地位的大数据征信机构在运营中不偏离预设的社会信用与信用国家目标，就必须增加其违规的成本。为此，我国可以已设定的“法律责任”为基础，构建一个“民事→行政→刑事”由弱渐强的法律惩罚信用责任体系。

服务于社会信用治理是大数据征信机构存在的理由，但其又是市场的，为了生存与逐利，基于利润最大化，在征信中，其可能存在角色滥用风险，且大数据的运作模式更是放大了这种风险。是故，一个基本的逻辑是，为了对征信机构可能的失信行为进行惩戒，其责任与苛刻程度应大于其他社会主体的失信行为。在该问题上，可从以下三个层面进行规划：一是私益保护方面。作为链接存在的网络化数据是大数据征信的基础，为了保护公民隐私权、企业商业秘密及保证信用评价的客观性等，必须加大征信机构失信的民事赔偿责任。二是公益保护方面。征信具有高度的公共利益性，若大数据征信机构的所作所为违背了这一宗旨，那么就必须快速高效地进行高强度的行政责任问责。对涉嫌犯罪者，则雷霆式地依法追究当事人应承担的刑事责任。三是法律责任形式均衡问题。在责任承担中，应避免重行政责任而轻民事责任，或以刑代民的倾向。虽然行政与刑事责任能让失信的征信机构与直接责任人有“切肤之痛”，但这并不是“雪藏”民事责任的理由。为了让私益与公益都能得到平等的保护，在实践中，必须避免以行政或刑事责任替代民事责任的误区。

〔67〕 李晓安：《我国社会信用法律体系结构缺陷及演进路径》，载《法学》2012 年第 3 期，第 150 页。

• 21 •

四、结语：一个以社会信用为本位的主题

“信用制度建设的目的不是单靠严厉的外控，更在于通过长期的约束机制最终使人们将外在的行为约束变成一种行为习惯，让诚信和信任再度恢复。”〔68〕毋庸置疑，服务于长效性的社会信用是大数据征信的时代性主题。大数据征信是一个与创新相关的命题。创新即创造性的破坏，它意味着旧观念、旧秩序与旧制度的消融、解体，及新思维、新秩序、新制度的萌芽与解构。大数据是现代征信模式的标签，“在宏观上，大数据是认识论的变革，大量对象从不可知到可知，从不确定性到精确预测，从小样本近似到全样本把握，是认识世界和改造世界能力的升华”〔69〕。这种成长的力量也使得传统的征信与治理面临一场迫在眉睫的“变革”或“被变革”。变革中，我们应先盯住的是社会信用与人类命运共同体的宏大目标，而后才是我们究竟需要什么样的法律。

在倡导兼容并包精神的社会中，如果殚精竭虑地试图从法律是什么的角度来实现社会成员之间友爱共处共存的目标，还是远远不够的，因为除了稳定与安全，现实的法还应服从于正义性目标。社会信用的确立、维护与矫正需要私人与国家之间的紧密协作。然而，问题是如何恰到好处地把握国家权力介入的程度。在强烈体现国家强力意志的法律创新中，适度引入自然法的理念无疑能够对我国大数据征信的法律治理起到警惕与监督作用，因为“自然法的重要性也许不在于解决一个文明制度中出现的正常问题，而在于它有助于决定什么才是一个文明的法律制度”〔70〕。此外，在新的事物还没有最终尘埃落定之前，尊重市场优胜劣汰的自然法则，给予一定的发展空间，保有适度的耐性与宽容也是非常必要的。

Abstract：Social credit is the basis for the maintenance of social order，harmony of interpersonal relation，normalization and development of transaction，people's richness and prosperity of the nation，which is of great significance for construction of destiny community. The big data is changing the mode，way and idea of traditional credit investigation and produces the evolutionary effect on the renewal of the governance of credit investigation. Big data investigation promotes the construction of social credit and the formation of credit nation. As the modifier of social interests and stabilizer of social order，when the crediting regulatory law obviously lags and creates contradiction between supply and demand，it is a reasonable selection to initiate the innovation from social credit，specified idea，balanced protection of interests，market safety and respect of the nature of internet.

Key Words：social credit，big data credit investigation，credit china

（责任编辑：刘权　赵建蕊）

〔68〕 黄晓晔：《信用与社会控制——解读社会信用危机的新视角》，载《学术研究》2013 年第 12 期，第 79 页。
〔69〕 王达：《美国互联网金融与大数据监管研究》，中国金融出版社 2016 年版，第 182 页。
〔70〕〔美〕波斯纳：《法理学问题》，苏力译，中国政法大学出版社 2002 年版，第 303 页。

财经法学 No. 4，2021
pp. 41 - 51

论流量传导行为对数字经济平台市场力量的影响

杨　东　王　睿*

内容提要：流量传导行为不等同于数据的传输或集聚，其具有独立于数据而被单独讨论的意义。鉴于平台导流行为的表现形式因平台商业模式的不同而有所区别，故应对该行为分场景予以分析。从宏观层面来看，导流行为使杠杆效应更易实现，并且提高了市场的进入壁垒。根据这些效果，可以认定导流行为有增强平台市场力量的作用。从这一效果的具体实现路径来看，流量传导行为对平台的直接影响是带来流量即用户注意力，精确匹配的算法又极大地提高了流量价值的转化率，加强了流量利用的确定性。而且，流量传导的过程同时也是数据积累的过程，其通过提高平台数据的更新速度，助力平台将流量优势转化为数据优势，加剧数字经济平台领域的“赢者通吃”现象。

关键词：流量传导行为　平台　市场力量　垄断

数据作为一种新型生产要素，已经进入了法律规范的视野。《中华人民共和国反垄断法》（以下简称《反垄断法》）修订草案在“滥用市场支配地位”一章中，将“掌握和处理相关数据的能力”作为认定平台经营者具有市场支配地位的考量因素。但是，对静态数据的关注不足以完整展现数字经济平台市场竞争的逻辑和全貌。考虑到平台商业模式需要以流量为依托，且流量与数据之间具有紧密联系并相互作用，数据价值实现的各环节离不开流量的传导。因此，对动态的流量传导，以及促成流量传导的经营者行为更应予以重视。

在工业经济时代，流量被用来描述线下商铺的人流量。人流量大意味着有更多的人光顾商家，商家卖出商品、获取盈利的可能性也就越大。在数字经济时代，流量从线下转移到线上，被

* 杨东，中国人民大学法学院未来法治研究院教授，中国人民大学民商事法律科学研究中心研究员；王睿，中国人民大学法学院硕士研究生。

本文为国家社科基金重大项目“在法治轨道上促进平台经济、共享经济健康发展研究”（21ZDA025）的阶段性成果。

赋予新的内涵。有学者指出，流量是用来描述访问一个网站用户数量以及用户所浏览页面数量等的相关数据指标。〔1〕还有学者就这些指标进行了罗列，认为其包括独立访问量、重复访问量、页面浏览数、每个访问者的页面浏览数等。〔2〕

数字经济平台获取用户流量的方式可分为两种，一种是通过产品研发、宣传推广等方式吸引用户参与或使用，实现流量的“从无到有”。这一方式往往为初创企业使用，需要时间进行流量积累，对平台市场力量的影响见效较慢。另一种则是通过流量传导，直接、快速获取大量用户的注意力。鉴于数字经济平台对流量的高需求、强依赖，流量传导无疑会对接受传导的平台产生正向反馈，深入影响平台的市场力量。

流量传导现象并非总是自然而然地发生，其背后往往存在平台经营者有意的行为。实际上，能够加快流量传导速度、操控流量传导方向的流量传导行为已被普遍应用于同一平台生态之中，或不同平台生态之间。流量传导行为常被看作是平台企业的自主商业策略或宣传手段，而被法律规范所忽视。但在数据竞争加剧竞争动态性、跨多边市场竞争和未来竞争要求规制链条前移的背景下，〔3〕流量传导行为在《反垄断法》语境下的意义值得特别审视。探究流量传导行为对数字经济平台市场力量的影响，有助于把握平台的发展趋势和市场力量的延伸方向，评估导流行为的反竞争效果，从而为规制提供理论基础。

一、流量传导行为的场景及传导效果

数字经济平台基于公域流量掌握着流量入口，并倾向于利用流量控制权增强市场力量。流量传导行为就是平台行使流量控制权的一种重要表现形式。流量传导的效果可以通过两种方式实现：其一，平台通过流量在自身生态间的传导，利用杠杆效应推动平台市场势力的快速扩张；其二，平台通过流量传导行为可以制造“流量池”，直接提高市场的进入壁垒，限制潜在竞争对手的发展。

（一）流量传导行为的场景分析

流量可以承载数字经济平台的商业运营模式，互联网平台的经营实际上就是建立在庞大流量上的经济行为。不同场景中的流量种类和利用方式有所不同，而平台和场景并非处于一一对应的关系。这意味着，尽管是同一平台上的流量，也不能一概放在同一场景中看待，如微信广告的流量合作生态就是由朋友圈流量与公众号、小程序、小游戏的流量共同构成。〔4〕同样的，流量传导行为也应该被置于场景下进行分析。

需要先行明确的是，流量传导行为作为一种推广措施，可以由任何互联网企业甚至个人实施。但受实施主体不同、产品或服务对用户的吸引力高低不同等因素影响，流量传导的效果会有所区别。鉴于数字经济平台掌握着流量入口，其实施流量传导行为的效果更为显著，导流行为对

〔1〕 参见季境：《互联网新型财产利益形态的法律建构——以流量确权规则的提出为视角》，载《法律科学》2016 年第 3 期。
〔2〕 参见马晓明、翟静芳：《网络不正当竞争损害赔偿研究——以流量、数据为视角》，载《电子知识产权》2019 年第 12 期。
〔3〕 参见陈兵：《因应超级平台对反垄断法规制的挑战》，载《法学》2020 年第 2 期。
〔4〕 参见《微信广告首次对外公布流量数据：月入 10 万以上的流量主超过 600 个》，载《城市党报研究》2019 年第 2 期。

市场力量造成的影响更易观察，故接下来关于流量传导行为的论述，都是围绕“数字经济平台”作为该行为的实施者这一前提展开。

流量传导行为并不等同于数据的传输或集聚，其表现形式是多样化的。流量传导行为可能发生在同一个平台生态中，即平台为自己的不同服务类别提供流量传导路径，以拓展业务范围。如微信在其平台上为短视频、移动支付等功能提供了跳转的接口，用户通过点击“视频号”“支付”可以进行跳转，此时就实现了移动社交领域的用户流量向短视频、移动支付等市场的传导。

流量传导行为也可能发生在不同的平台生态之间，即平台为那些向自己支付流量对价的主体提供导流服务。如微信的“朋友圈”和 QQ 的“动态”中时常出现的嵌入式广告，就展现了腾讯的流量传导行为。这些广告会展示相关商品或活动的图片、视频，并搭配文字表述，提供跳转链接。微信和 QQ 的用户一旦打开朋友圈或 QQ 动态，就有机会看到这些广告，并可能被广告吸引而点击相关链接，跳转到广告主提供的页面上，或者直接进入另一个应用，由此实现腾讯用户流量向广告主的导入。

总而言之，流量传导行为具有多样态的特征：既可能是单向的，也可能是双向的；既可能是有偿的，也可能是无偿的；实施主体可能是单方的，如平台企业为自己旗下的新产品导流，也可能是双方或者多方的，如平台向与其达成合作协议的主体导流。

（二）导流行为使杠杆效应更易实现

在数字经济中，市场与市场之间的边界变得不再清晰，超级巨头跨界实施控制的成本很低。再加上网络效应在互联网行业常表现出正反馈，大型网络对用户更具有吸引力，并倾向于变得更大。〔5〕因此，数字经济平台大多具有向其他市场传导力量的倾向。

流量传导行为是数字经济平台常用的一种传递市场力量的方式。流量本身就具有可流动性，其能够在各个平台间、平台的各板块间流通，并因此成为平台多元业务协同的纽带。平台借助导流行为，可以将现有的优势传导到通讯、社交、阅读、支付、购物、交通出行等其他市场，〔6〕从而实现垄断的自我强化。如腾讯的核心领地虽在社交、游戏、第三方支付方面，但也在不断向短视频、云计算等领域进攻。字节跳动在短视频、秀场直播、信息流媒体方面占据优势地位，但也没有放弃向传统电商、O2O 电商、教育、游戏等领域的发展。各互联网巨头都倾向于多条战线“作战”，希望能够通过发展多元自有业务提升流量变现的效率。有学者将这一过程概括为“平台通过增强及扩张服务，进入新的领域，将在新的领域形成第二轮垄断、第三轮垄断”〔7〕。

数字经济平台利用其在一个市场上的垄断力量来获得在另一个市场上的垄断力量，从而同时控制两个市场的现象，可以用“杠杆效应”来描述。传统理论通常认为搭售、捆绑销售、独家交易等行为具有杠杆效应，但在数字经济时代，杠杆效应的内涵已经发生了变化。一方面，在垄断力量的衡量上，应将平台的用户数量和活跃度，以及平台获取数据的能力纳入考虑。因为控制着流量入口的数字经济平台，往往更有能力利用综合优势向其他市场渗透，通过“杠杆”形成在新

〔5〕 参见张素伦：《互联网背景下反垄断法实施理念研究》，载《河南师范大学学报（哲学社会科学版）》2016 年第 4 期。
〔6〕 参见杨东：《警惕数字平台“赢家通吃”》，载《人民政协报》2020 年 11 月 26 日，第 7 版。
〔7〕 参见李勇坚：《互联网平台寡头垄断：根源、影响及对策》，载《人民论坛》2021 年第 Z1 期，第 14 页。

市场领域的竞争优势。〔8〕另一方面，互联网平台滥用杠杆优势的行为外观与搭售、限制交易等排他性行为存在根本差异。在“可口可乐并购汇源案”中，执法机关认为若允许并购，可口可乐公司将有能力把其在碳酸饮料市场上的支配地位传导到果汁市场，削弱、剥夺其他果汁生产商与其竞争的能力，使消费者被迫接受更高价格、更少种类的产品。〔9〕可见，传统说理更强调对搭售“强制性”的论证。但具有免费模式、动态竞争等特点的平台经济显然难以适用这一论证思路。〔10〕

互联网平台不需要通过强制手段传导市场力量，平台的流量传导行为足以使杠杆效应更容易实现，且这种市场力量传导的方式具有非强制性和隐蔽性。有学者提出，在平台经营模式下，互联网企业的竞争在平台接口层面、应用层面分别或者综合地展开。〔11〕这意味着，互联网平台不需要通过强制手段要求其他经营者、消费者接受搭售的产品或者与其独家交易。平台只要能够把握端口，也就是控制流量的传导，就可以直接实现市场力量的传递。如 2017 年 6 月，谷歌因滥用支配地位操纵搜索结果，不公平地把客户引向自己的购物服务，被欧盟处以 24.2 亿欧元的罚款。2020 年 12 月，谷歌因通过实施“搜索歧视”将自有资源的搜索结果置顶，被美国 38 位州和地区总检察长组成联盟提起诉讼。〔12〕在这两起案例中，谷歌都试图通过其在搜索引擎市场的支配地位，用非强制性的手段获取在购物服务等其他领域的市场力量，佐证了流量传导的非强制性使杠杆效应更易实现的观点。

（三）导流行为提高了市场进入壁垒

有学者提出，测算市场力量的潜在思路是，评估在位者因忌惮新进入者而在商业行为方面制造障碍的程度，〔13〕即观察市场中的现有竞争者通过实施某些商业行为，能否有效提高市场的进入壁垒。有学者提出了“数据池”的概念，认为“数据池”的组成成员不愿对外共享池中的数据，从而为反竞争协作的达成提供了条件。〔14〕虽然流量传导行为不同于“数据池”的组建，但是特定范围内的流量传导可以被看作在这一范围内划定了“流量池”，同样具有将流量传导范围外的经营者置于竞争劣势地位的作用。

流量传导行为正是这样一种制造“流量池”以提高市场进入壁垒的商业行为。具体而言，流量传导行为可以使流量通过两种方式成为市场进入壁垒。一方面，流量可以作为数据的来源和基础，间接构成市场进入壁垒。另一方面，流量也可以作为平台“获取数据的能力”的表征，单独、直接构成市场的进入壁垒。

前者的逻辑在于，流量可以为平台带来用户，用户在使用平台时则会留存数据。因此，流量

〔8〕 参见前引〔7〕，李勇坚文。

〔9〕 参见邓峰：《传导、杠杆与中国反垄断法的定位——以可口可乐并购汇源反垄断法审查案为例》，载《中国法学》2011 年第 1 期。

〔10〕 参见叶明、黎业明：《互联网平台滥用杠杆优势行为的反垄断规制研究》，载《管理学刊》2021 年第 2 期。

〔11〕 参见张江莉：《互联网平台竞争与反垄断规制：以 3Q 反垄断诉讼为视角》，载《中外法学》2015 年第 1 期。

〔12〕 参见王先林、方翔：《平台经济领域反垄断的趋势、挑战与应对》，载《山东大学学报（哲学社会科学版）》2021 年第 2 期。

〔13〕 参见王璐、方燕：《互联网领域垄断行为界定与市场力量测度》，载《中国流通经济》2021 年第 2 期。

〔14〕 参见时建中、王煜婷：《“数据池”共享行为的竞争风险及反垄断法分析》，载《江淮论坛》2021 年第 2 期。

可以被看作是基于用户使用行为而形成的一系列数据集合。又由于数据具有一定程度的排他性、质量和价值的差异性、高昂的收集成本、锁定效应和转换成本以及网络效应等属性，故其会提高数据市场的进入壁垒。〔15〕但数据作为市场壁垒的观点也遭到了一些质疑。有观点认为，数据的时效性可能使数据掌握者的优势地位被削弱，且企业的竞争劣势受到算法技术、产品质量、经营策略等多方面因素的影响，数据持有量本身不足以构成市场壁垒。〔16〕

流量作为数据来源，间接构成市场进入壁垒的观点，因学界对“数据”作为市场壁垒的质疑而受到了一定冲击。但这些质疑反而证实了动态的流量与静态的数据量相比，更可能帮助平台形成竞争优势，也即流量能够脱离数据而单独构成市场壁垒。平台的建立和发展往往需要以大量流量为依托，其商业模式能否成功实现，与流量的获取速度和质量密切相关。若流量已经被集中于少部分企业，重新获取流量难度较大或所需时间过长，则新进入的企业无疑会面临现实阻碍。换言之，当代表“获取数据的能力”的流量被作为平台从事市场竞争的前提条件，而市场新进入者又无法收集类似数据或购买访问权限时，现有企业拥有的访问数据的权限就构成了一种市场进入的障碍。〔17〕

当前，执法机关也已经关注到了数字经济时代存在特殊的市场壁垒。2021 年 4 月 10 日，国家市场监督管理总局对阿里作出的《行政处罚决定书》提到，“网络零售平台在平台一边获得足够多的用户”是实现“有效市场进入”的关键。鉴于“用户数量”是可以衡量“流量”大小的因素，可以认为《行政处罚决定书》的这一表述佐证了流量单独构成市场进入壁垒的观点。

二、流量传导行为影响平台市场力量的具体路径

平台的流量传导行为使杠杆效应更易实现，且会提高市场的进入壁垒。这两种效果的叠加无疑增强了实施导流行为的平台的市场力量。但是，就“流量传导行为”和“市场力量”之间关系的观察，不应仅停留在对导流效果的宏观分析层面。流量传导行为增强平台市场力量的具体路径需要进一步阐释，特别是流量传导行为与用户注意力之间的关系、算法对流量利用率的提高作用、流量优势向数据优势的转化等问题。

（一）导流行为带来用户注意力

正如前文所述，流量可以用用户数、浏览量等数值衡量，而这些数值又能够被用来描述用户注意力或关注度的多少。因此可以认为，流量与用户注意力的内涵相近，流量是用户注意力的具象化。注意力是当今越来越重要的一种资源，互联网经济的本质就是注意力经济。依赖于注意力市场的注意力经济商业模式是目前许多社交、科技平台的主要商业模式。但用户注意力的总体规模是有限的。有学者曾提出，互联网的人数乘以平均上网时长，就是国民线上总时间。由于所有网上消费都在这个时段内进行，因此可以认为，这相当于互联网消费市场规模的边界。〔18〕

〔15〕 参见殷继国：《大数据市场反垄断规制的理论逻辑与基本路径》，载《政治与法律》2019 年第 10 期。
〔16〕 参见陈兵：《“数据垄断”：从表象到本相》，载《社会科学辑刊》2021 年第 2 期。
〔17〕 参见任超：《大数据反垄断法干预的理论证成与路径选择》，载《现代经济探讨》2020 年第 4 期。
〔18〕 参见《数字经济，解构与链接——人文清华讲坛江小涓演讲实录》，载微信公众号“人文清华讲坛”，2020 年 11 月 22 日。

在用户注意力有限而互联网企业众多的情况下，抢占注意力无疑成为各互联网企业的重点策略。流量传导行为就是互联网企业抢占用户注意力的一种表现形式。有学者将注意力经纪概括为：注意力经纪人通过向公众提供新闻、娱乐、免费服务以吸引其注意力，再将注意力转卖给广告商以获取现金收益。〔19〕这一商业模式就是一种有偿的流量传导行为。其特点在于，接受流量传导的主体如广告商，不需要第一时间直接接触用户群体，而由直接面对用户群体的注意力经纪人如数字经济平台，负责通过提供免费服务等方式吸引用户。之后由注意力经纪人通过流量传导行为为广告商提供推广，并从广告商处获取报酬。除这种有偿获取流量传导的方式外，互联网企业也可以选择不通过注意力经纪人，而凭借自身发布的广告、补贴等方式，向其潜在的或现有的用户推送新产品、新服务。但这一模式在该互联网企业本身就具有一定的用户基础，也即建立起自己的流量生态时，才能起到较好的流量传导效果，实现新产品和新服务的推广。

对平台而言，流量传导行为的最大意义在于其能够带来用户的注意力，为自己或与其达成合作的广告商提供更多的交易可能性。从这个角度来看，流量也可以被理解为交易的机会。交易机会正是互联网经营主体争夺的对象，也是经营主体能够量化的价值体现。〔20〕当然，流量传导行为的最终效果仍取决于用户的兴趣和接受度。用户是否同意接受推送、是否对推送内容感兴趣并愿意点开链接，决定着流量传导的效果如何。因此，从某种程度上来说，流量传导行为只是给被传导者提供了一个“被展现给用户的机会”，而不必然给被传导者带来有黏性的用户。当然，不成功的流量传导也并非没有讨论意义。实际上，在关注“行为”的我国反垄断法的分析框架中，可能带来用户注意力转移的“流量传导行为”本身就具有讨论价值。不过，由于不成功的流量传导行为难以为平台带来经济利益，无法据此论证平台市场力量的强化路径，故本文不对此展开论述。

（二）算法分析提高流量利用率

流量是用户注意力的具象化，数字经济平台实施流量传导行为的目的在于吸引用户注意力，获取更多的交易机会。但正如前文所述，流量传导行为的效果具有不确定性：既可能导致用户完全抛弃一个平台而转向另一个平台，也可能只是短期的吸引用户而不能达到较高的用户黏性；既可能使用户接受推广并进行消费，也可能遭到用户的拒绝和反感。概言之，流量传导行为所带来的交易机会的大小不能一概而论。特别是在缺乏算法分析的情况下，传导来的流量很可能与接受传导方的需求缺乏匹配度，从而使得接受传导一方的目的落空。

导流效果的不确定性，在一定程度上减损了流量利用的价值。在没有进行算法分析的情况下，单纯的流量传导行为虽然能够带来用户的注意力，但此种注意力的经济价值不能被很好地挖掘和评估。有学者提出，流量的价值在于“转化率”。如用户对广告的注意力转化为广告产品的购买量，体现了用户输入型流量的价值。百度用户输入的搜索词，可以成为百度市场需求分析的数据源，体现了用户输出型流量的价值。〔21〕没有经过加工和匹配的流量，其价值难以被准确衡量，既不利于实现流量的价值转化，从长远看也不利于流量传导交易的开展。

---

〔19〕 See Wu T，Blind Spot：The Attention Economy and the Law，82 *Antitrust Law* Journal，771（2018－2019）.

〔20〕 参见刘佳欣：《反不正当竞争法视角下的流量劫持——以流量劫持典型案例为分析样本》，载《法律适用》2019 年第 18 期。

〔21〕 参见王潺：《互联网不正当竞争法律评价的法经济学分析》，载《广东财经大学学报》2020 年第 6 期。

算法与流量结合才能够实现平台市场力量的拓展。平台作为数据集合体的中心，天然就具有利用算法进行分析的需求。〔22〕精确匹配的算法极大提高了流量价值的转化率，有利于加强流量利用的确定性。从算法分析发挥流量价值的实现路径考量，可以发现，算法对流量价值的挖掘主要从两个维度进行。

其一，数字平台通过算法分析，能“预测用户偏好、支付意愿、最高保留价格，设计目标用户群精密的差别定价、数据利用的个性化服务”〔23〕，以提高自身对市场和用户行为的预判力，从而确定经营战略。换言之，企业对消费者的了解越多，就越能够更好地满足消费者需求，将他们与他们可能喜欢的内容相匹配，促使消费者支付更多，实现注意力的货币化。〔24〕有学者将这一实现路径称为“用户反馈回路”。通过此种反馈循环还可以产生规模经济，即当平台拥有大量用户，获得更多的用户数据时，就能更好地洞察消费者需求，进而提高服务质量以吸引更多用户。〔25〕

其二，算法分析除了能预测用户偏好、提升平台的服务质量之外，还可以实现更为精准的广告投放，使平台获得更多的在线广告收入，促进流量价值的变现。互联网广告是互联网平台的基本盈利模式之一，对于不直接通过销售产品获取利润，或不以平台销售为主要发展方向的平台而言，提供推广服务、获取广告收入往往是其利润的主要来源。当前，数字经济时代的发展已经给广告行业带来了日新月异的变化，广告主从漫无目的的量化式投放，过渡到更倾向于精准到消费者个人的精细化投放。能够满足广告主这一需求的平台无疑会更受青睐，获取更多的广告服务机会，收取更高的广告推广费用。

（三）流量优势转化为数据优势

对数字经济平台而言，流量和数据有着密不可分的关系。平台本质上就是流量入口的数据集合体，它以数据生产要素为核心，通过算法设计与操作创造市场价值，驱动平台、数据、算法三维结构的市场竞争新格局。〔26〕一方面，流量是数据的来源和基础，用户的每一次浏览和点击都会在平台上留下自己的痕迹。平台在取得用户许可的前提下可以对这些痕迹进行收集和加工，实现流量到数据的转化。从这个角度来看，流量传导的过程也可以被看作数据积累的过程。另一方面，流量传导行为可以为平台带来新的用户和关注度，从而提高平台所收集的数据的更新速度。在数据时效性凸显的数字经济时代，能够较快地更新数据无疑是平台保持自身竞争力的关键。

当然，流量与数据在价值层面上也存在显著的差异。其一，动态的流量传导固然具有财产价值，但是由于传导的效果不能确定且难以衡量，在这个环节难以明确其价值。而当流量传导带来的数据积累完成后，流量价值会转变为数据价值，其将更为客观、易于感知。其二，流量传导的价值主要体现在传导者和被传导者之间，其往往是一种商业行为，普通用户难以分享这一行为产生的价值。相较而言，数据价值则更可能被广泛分享，因为数据生成是由用户行为带来的，用户对其所提供的数据内容有一定控制力。或许在将来可以通过发行“共票”的方式使互联网用户也

〔22〕 参见杨东：《论反垄断法的重构：应对数字经济的挑战》，载《中国法学》2020年第3期。

〔23〕 杨东、臧俊恒：《数字平台的反垄断规制》，《武汉大学学报（哲学社会科学版）》2021年第2期，第165页。

〔24〕 See Ryan Calo，Alex Rosenblat，The Taking Economy：Uber，Information，and Power，117 *Columbia Law Review*，1623－1690（2017）.

〔25〕 参见贾晓燕、封延会：《网络平台行为的垄断性研究——基于大数据的使用展开》，载《科技与法律》2018年第4期。

〔26〕 参见前引〔23〕，杨东、臧俊恒文。

能分享数据价值。〔27〕

平台为增强其市场力量，往往会将自身的“流量优势”转化为“数据优势”，以尽量多获取、更好利用“数据”这一生产要素，并借此拓展自身的市场力量。“流量优势”向“数据优势”的转化会加剧数字经济平台领域的“赢者通吃”现象。从经济学角度分析，使用两种竞争产品的边际成本大于收益时，就可能发生市场的单一导向。〔28〕对平台而言，当其掌握了大量流量时，用户在该平台及其提供导流服务的平台上满足需求的成本更低也更为便利，因此会更倾向于使用这些服务。当流量和数据随着用户的聚集而聚集在少数互联网巨头手中时，就会形成数字经济平台领域的“赢者通吃”现象。〔29〕关于平台如何利用流量传导行为增强其在本市场和其他市场上的力量，本文将在下一部分以社交平台为例予以详细论述。

三、流量传导行为增强平台市场力量的实例分析

鉴于流量的无体性和传导的便捷性，流量传导的作用范围不受时间和地域的限制，其既可以扩大平台在其他市场上的影响力，也能够增强平台在同一市场上的力量。以社交平台的流量传导为例，由于流量对短视频市场的发展具有必要性，封禁 API 等拒绝流量传导的行为引起了抖音与腾讯的纠纷。反观之，社交平台的流量传导行为也可以将其本身的影响力传递到短视频市场上，微信“视频号”的发展就是一个例证。另外，社交平台通过流量传导能够增强自身在同一市场上的力量。具体而言，流量传导可以助力平台转型以延续其优势地位。相反，若缺乏导流，社交网络的强锁定效应会使新的市场进入者难以挑战之前平台的地位。

（一）借助流量传导行为增强自身在其他市场的力量

积聚海量用户、掌握流量入口的社交平台具有天然的流量优势。中国社会科学院大学互联网法治研究中心在《互联网平台与数据竞争规制问题研究报告》中提出，社交软件的影响力已超越了单纯的私人社交属性，而带有商业交易上的“交往”属性。目前，各行业的经营者正越来越将社交平台作为经营、推广、引流的工具。以腾讯为例，鉴于其旗下的微信和 QQ 几乎独占了国内社交软件平台的流量，诸多企业选择与腾讯合作换取更大的发展机会。基于自身的流量优势，腾讯对其“合作伙伴”的控制度也逐渐加深，以其为中心的新型互联网垄断正在形成。〔30〕

区别于传统企业在实体经济中的垄断，“流量垄断”成为数字经济时代屡见不鲜的现象，与其相关的纠纷也随之显现。2021 年 2 月 2 日，字节跳动旗下的抖音在北京知识产权法院向腾讯提起反垄断诉讼。其提出，微信、QQ 以“短视频整治”为由，对抖音等产品进行了长达三年的持续封禁和分享限制。这一行为构成《反垄断法》所禁止的“滥用市场支配地位排除、限制竞争的垄断行为”。〔31〕腾讯则发布声明回应称，字节跳动公司的相关指控纯属失实，系恶意诬陷，且字

〔27〕 参见杨东：《“共票”：区块链治理新维度》，载《东方法学》2019 年第 3 期。

〔28〕 See Hovenkamp，Herbert J，*Antitrust and Platform Monopoly*，Legal Scholarship Repository：Faculty Scholarship at Penn Law，2020，p. 1924.

〔29〕 参见杨东：《后疫情时代数字经济理论和规制体系的重构——以竞争法为核心》，载《人民论坛·学术前沿》2020 年第 17 期。

〔30〕 参见朱邦凌：《微信收费的“底气”在于“新流量垄断”》，载《新京报》2018 年 7 月 3 日，第 B02 版。

〔31〕 参见《关于抖音起诉腾讯垄断的声明》，载微信公众号“抖音”，2021 年 2 月 2 日。

节跳动及相关公司存在诸多侵害平台生态和用户权益的违法违规行为。〔32〕

“头腾大战”的争议主体抖音属于短视频平台，微信和 QQ 则属于社交平台。二者固然处于两个不同的市场，但“流量”如同一个管道，可以将两个市场连通起来。流量对致力于吸引大量用户积极创作、分享和交流的短视频市场来说，具有重要意义。甚至可以认为，流量是短视频应用发展的基础。腾讯关闭 API 接口导致某些抖音用户无法通过社交平台网络授权登陆，或无法通过直接跳转分享链接等内容到社交平台，实际上是拒绝为抖音提供流量传输途径，切断了流量传导的管道。这将会使抖音用户登录、分享的步骤复杂化，影响到抖音用户的分享积极性。从反垄断法的视角来看，腾讯是否构成垄断还需经进一步分析。但就其行为本身而言，“拒绝向竞争者开放数据入口”已被认为是具有数字经济特征的新型垄断行为。〔33〕 关闭 API 接口作为一种平台封禁行为，可能会涉嫌违反反垄断法关于排他性交易、拒绝交易、差别待遇等的规定。〔34〕

社交平台的流量封禁会影响短视频应用的发展，反观之，社交平台的流量传导行为也可以将其本身的影响力传递到短视频市场上。实际上，腾讯自身也关注到了短视频市场的潜力，早已将短视频作为自己的主要进攻方向之一。据三言财经统计，腾讯至少上线了微视、企鹅看看、闪咖、QIM、DOV、MOKA 魔咔、猫饼等约 16 款短视频相关 APP，再加上依托微信平台的时刻视频，短视频产品的总数约 17 个。2020 年 1 月 19 日微信的视频号上线，2020 年 6 月，微信官方宣布视频号日活已破两亿。方正证券预测在没有开启商业化的情况下，视频号目前的日活基准水平是 3 亿，长期空间预估 6 亿，最终会接近微信本身的日活水平。〔35〕

数字平台通过对流量入口的垄断，将自己变成了行业和社会的中心，并借助流量合作加深对其他经营者的控制。可以认为，平台利用自身海量、高黏性的流量调控和分配，在与其紧密合作的经营者之间构建起了基于流量的卡特尔，〔36〕 通过导流行为增强了自身在其他市场上的力量。

（二）借助流量传导行为增强自身在同一市场的力量

2021 年 1 月，米聊发布公告称，其将于 2021 年 2 月 19 日停止服务。而与其发布时间相近、功能相似的竞争对手微信，如今已成为国民级的社交通信产品。2021 年 3 月 24 日，腾讯发布 2020 年第四季度业绩报告。宣布微信用户已逾 12 亿，每天超过 1.2 亿用户在朋友圈发表内容，3.6 亿用户阅读公众号文章，4 亿用户使用小程序。〔37〕 回顾历史可以发现，微信的成功并非一帆风顺。其上线半年后，用户数还未达到 100 万。而当时，腾讯 QQ 注册用户已超过 6 亿，成为腾讯在移动社交领域的护城河。〔38〕 为支持微信的发展，腾讯作出决定通过 QQ 为微信导流。一方面，QQ 在其主页和 QQ 邮箱的首页打出了微信的广告，吸引用户关注这一新产品；另一方面，QQ 为微信提供了互操作性，方便用户从 QQ 转移至微信。相比通过通讯录添加好友的米聊，微信用户可以通过 QQ 账号注册，且微信可读取 QQ 好友的信息，并将他们添加至好友列表。正是

〔32〕 参见《字节跳动恶意构陷，腾讯将起诉》，载微信公众号“鹅厂黑板报”，2021 年 2 月 2 日。

〔33〕 参见刘云：《互联网平台反垄断的国际趋势及中国应对》，载《社会科学文摘》2021 年第 2 期。

〔34〕 参见张江莉、张镭：《互联网“平台封禁”的反垄断法规制》，载《竞争政策研究》2020 年第 5 期。

〔35〕 参见《微信的生态与野望：大音希声，大象无形》，载微信公众号“方正证券研究”，2021 年 1 月 20 日。

〔36〕 参见前引〔23〕，杨东、臧俊恒文。

〔37〕 参见《腾讯发布 2020 年业绩报告，全年净利润 1598.5 亿元人民币》，载 https：//www.chinaz.com/news/1231338.shtml，最后访问时间：2021 年 4 月 27 日。

〔38〕 参见《微信十年，“熬死”一个又一个对手》，载 http：//www.chinanews.com/cj/2021/01-26/9396867.shtml，最后访问时间：2021 年 4 月 27 日。

通过 QQ 一系列的导流措施，微信才能在短期内获取大量用户，上线 433 天即实现了用户数突破 1 亿，在同时期推出的同类社交产品中脱颖而出。

不同网络间的高转换成本所带来的锁定效应，在社交网络中表现得更为明显。这意味着，在缺乏外因干涉的情况下，用户大量从一个已成熟的社交平台向另一个平台转移的可能性较低。相反，如果用户关系链上的相当一部分用户选择了另一个平台，则该用户也有很大可能向该平台转移。有学者曾指出，用户使用移动 SNS 的行为意愿强烈依赖于社会影响、群聚效应。〔39〕还有学者归纳出了三段式社交媒体用户转移行为路径，指出用户在过渡阶段的转移，大部分是由于受到了周围环境的影响和带动。〔40〕从这一理论出发看 QQ 为微信导流事件，可以发现，QQ 实施流量传导的行为，特别是为微信提供互操作性，可以有效地降低用户转移成本，弱化 QQ 本身的锁定效应。又由于 QQ 导流对象的唯一和确定性，弱化 QQ 锁定效应带来的流量红利只能由微信享有，这为微信的早期发展提供了机遇。

从深层意义上看，QQ 的流量传导不仅助力了微信的发展，更重要的是，其帮助腾讯实现了在社交应用领域的成功转型。QQ 的设计是基于 PC 时代的用户体验，由于当时的技术水平有限，PC 端的 QQ 移植到手机端时，无法复制全部功能，且数据无法做到同步。另外，QQ 的用户定位在年轻人群体，功能上更偏向娱乐化，受众有限，且由于每个用户可以注册的 QQ 号数量缺乏限制，导致有些 QQ 号实际上长期处于无人使用的低活跃度状态，不利于 QQ 进一步发展用户。在米聊等竞争对手纷纷推出竞争性产品之际，为了在手机端占据市场、实现自身在社交应用领域的转型，腾讯选择利用 QQ 导流微信，借此占据了更大的市场份额，增强了自身在同一市场上的力量。

流量传导行为可以助力平台转型以保持优势地位，反之，在缺乏导流的情况下，网络特别是社交网络的强锁定效应会凸显出来。这意味着，在同一个市场已存在基本成熟的平台时，与其功能互补性不强的平台将很难争取用户的关注，也因此无力挑战之前平台的优势地位。当前微信几乎独占了国内社交软件平台的流量。由于用户在微信上的好友、聊天记录、朋友圈等无法打包转移到其他社交软件平台，社交应用领域用户的低迁移度制约了同类社交软件的发展，遑论与微信相抗衡。实际上，在社交应用市场上，若缺乏腾讯系的导流，锁定效应会将网络访问变成竞争性武器。〔41〕如快播的马桶 MT、字节跳动的多闪、锤子科技的聊天宝，虽都定位于社交，想要挑战微信的地位，但在发布伊始，三个 APP 就都遭到了微信的屏蔽，其流量巅峰也只出现在刚推出之时。

四、余　论

数字经济平台实施的流量传导行为能够增强平台的市场力量，而且其作用范围不受时间和地域的限制。平台市场力量的增强无疑会引发人们关于垄断风险的担忧，鉴于预防和制止垄断行为是语

〔39〕 See Shahrokh Nikou，Harry Bouwman，Ubiquitous use of mobile social network services，31 *Telematics and Informatics*，422－433 (2014).

〔40〕 参见贾若男、王晰巍：《基于扎根理论的社交媒体用户转移行为特征研究》，载《图书馆学研究》2018 年第 17 期。

〔41〕 参见李勇坚、夏杰长：《数字经济背景下超级平台双轮垄断的潜在风险与防范策略》，载《改革》2020 年第 8 期。

序逻辑下《反垄断法》的首要立法目的，〔42〕因此流量传导行为有必要受到《反垄断法》的审视。

规制平台流量传导行为的路径有两条。其一是将其作为垄断行为的一种规制。但流量传导服务协议不能被认为是一种“垄断协议”，其如果配合流量垄断行为实施，固然可能会加剧“流量垄断”的反竞争效果，如腾讯封禁抖音的同时大力推广其自身的“视频号”功能，有效抢占了短视频市场，但仅凭流量传导行为，很难达到垄断协议所要求的排除、限制竞争的效果。且流量传导行为也不符合《反垄断法》中“滥用市场支配地位”的行为样态。第二种选择是将其作为认定平台“市场支配地位”之有无的考虑因素。认定互联网平台经营者具有市场支配地位，应同时考虑平台的经营模式、网络效应、经营者掌握和处理相关数据的能力、经营者在关联市场的力量等因素。流量传导行为在很大程度上反映了平台的经营模式，且能够增强网络效应、为经营者提供持续的数据流，通过杠杆效应增强经营者在关联市场的力量。因此在认定平台市场支配地位时，有必要考虑到其流量传导行为的实施情况。

总而言之，流量传导的价值不可低估，有必要对其进行规范，正确引导流量价值的实现。在规范流量传导行为时，应注意避免引发垄断风险，保持互联网的开放共享性。在判断平台企业是否具有市场支配地位时，应将其进行流量传导的能力、流量传导行为的有无以及效果纳入考量因素。

Abstract：Flow conduction behavior is not equivalent to purely data transmission or agglomeration，and it is significant to discuss this behavior separately from data. Because the forms of flow conduction behavior on the platform are different with various business models of platforms，it should be analyzed in diverse scenarios. From the macro level，the flow conduction behavior makes the leverage effect easier to achieve，and raises the market entry barriers. As a result，there is a conclusion that the flow conduction behavior can enhance the market power of the platform. From the perspective of specific implementation path，the direct impact of flow conduction behavior on the platform is to bring flow，that is，users’ attention. The accurate matching algorithm greatly enhances the conversion rate of flow value and strengthens the certainty of flow utilization. Moreover，the process of flow conduction is also the process of data accumulation. By improving the update speed of data，it helps the platform transform the advantage of flow into advantage of data，and intensifies the “winner takes all” phenomenon in the platforms of digital economy.

Key Words：flow conduction behavior，platform，market power，monopoly

（责任编辑：殷秋实　赵建蕊）

〔42〕 参见刘乃梁：《“预防垄断行为”的理论逻辑及其制度展开》，载《社会科学》2020 年第 12 期。

财经法学 No. 2，2021
pp. 79 - 97

虚拟货币的国际监管：以反洗钱为起点走出自发秩序

吴　云　朱　玮*

内容提要：虚拟货币诞生已逾十年，其并未对现有法定货币体系造成冲击，因此，主要国家货币当局并未对个人持有并使用虚拟货币进行禁止。同时，由于虚拟货币是否适合普通投资者并没有定论，主要国家证券监管当局也并未正面注册或审批任何一种面向公众投资者发行的虚拟货币或与其挂钩的金融产品。但是，投机、欺诈和严重的洗钱问题促使各国当局不得不以实质性手段回应关切，在金融行动特别工作组（FATF）推动下，2019 年各国当局首先就虚拟货币反洗钱监管达成了共识，全球范围内的虚拟货币的监管框架正式形成，从根本上改变了行业自发生态。但反洗钱监管规则仅限于区块链外部活动时的洗钱预防问题，虚拟货币的链上治理将是下一个阶段监管的核心问题，也是挑战性最大的问题。

关键词：虚拟货币　反洗钱监管　区块链治理

一、引论：背景、主要作品回顾和本文的贡献

2009 年 1 月，中本聪设计的比特币（bitcoin）诞生，标志着虚拟货币作为一种现象级事件正式登上了历史舞台。中本聪设计比特币的目的在于创造一种点对点的支付系统，这个系统不依赖于任何第三方信任，使比特币成为一种开源的、基于网络的、点对点的匿名电子货币。〔1〕比特币

* 吴云，中国人民银行反洗钱局制度处副处长，金融风险分析师（FRM）；朱玮，北京无知智慧人工智能科技有限责任公司区块链工程师。

衷心感谢中国人民银行反洗钱局的领导和同事给予笔者在相关课题中的研究和参与机会。本文为作者个人学术思考，不代表所在机构观点。

〔1〕 See Satoshi Nakamoto，Bitcoin：A Peer-to-Peer Electronic Cash System 1，8（2008），available at https://bitcoin.org/bitcoin.pdf，last visited on Jun. 10，2020.

很大程度上受哈耶克私人货币思想的影响，从一开始就怀有实践私人货币实验的宏大理想。〔2〕但哈耶克所挑战的是国家对货币发行的垄断权力。〔3〕中本聪所挑战的是传统社会对第三方的信任，包括哈耶克所支持的商业银行，哪怕这些商业银行是在充分竞争的市场中。哈耶克要解决的问题是政治和经济问题，即如何实现货币的市场化和自由竞争；而中本聪要解决的问题是技术问题，即如何让虚拟货币摆脱对第三方可信服务器的依赖（即对中心化服务器的依赖）。〔4〕因此，比特币的创新不仅体现在技术层面，也体现在社群生态的设计上，开启了用区块链技术实现“去中心化”的生态治理模式，一切都是自发的，无需一个中心节点的组织、管理和裁决。

“虚拟货币”一词随着比特币的产生而有了新的内涵。在比特币产生之前，“虚拟货币”仅指在特定网络世界使用的代币，典型例子是游戏币；而比特币则可以实现广泛的交易和兑换功能，可在一定程度上承担货币的职能。为区分这两种情况，国际组织和主要监管当局将前者称为“不可转换式”（non-convertible）或“封闭式”（closed）虚拟货币，将后者称为“可转换式”（convertible）或“开放式”（open）虚拟货币。不可转换式虚拟货币被设定为特定社群内的单项用途，典型的如“Q 币”，持有者仅能在腾讯游戏世界使用，不能转移交付给第三方，是特定用途的电子化商品。可转换式虚拟货币可在不同用户之间转移，可以实现与法定货币、其他虚拟货币的双向兑换。〔5〕本文所讨论的虚拟货币仅指可转换式虚拟货币。

我们承认，虚拟货币这一场私人货币实验运动中，诞生了一系列影响经济模式和社会格局的技术创新，这些技术创新一般被总称为“区块链技术”，在价值流转、权利证明、商业模式等方面都有广泛的运用空间。〔6〕但是，从货币职能的角度，这场私人自发运动并不成功，反而产生了巨大的负面效果。徐忠和邹传伟指出了比特币的支付容量过小成为制约其作为支付手段的瓶颈，但限于主题需要并未展开进行详细论证和说明。〔7〕吴云和朱玮结合技术分析，从货币职能的角度，全面分析了虚拟货币的社会实验是一场失败的运动，指出内在技术缺陷导致其无法成为公众广泛使用的交易媒介，在无监管状态下比特币价格被严重操纵，不仅未能展示普惠金融的优势，相反，比特币的匿名性和跨国性被犯罪活动滥用为洗钱工具。〔8〕

〔2〕 关于哈耶克思想对虚拟货币的影响，可参见 Luca Fantacci，Cryptocurrencies and the Denationalization of Money，48 (2) *Int'l J. Pol. Economy*，105，105－112 (2019).

〔3〕 哈耶克认为政府并不值得相信，历史一再证明政府如果垄断某种商品一定会导致无效率，政府发行货币的历史，无一不以政府失信、货币贬值终结。私人货币发行者之间的竞争要优于政府的垄断。（See F. A. Hayek，*Denationalization of Money*：*The Argument Refined* ，Hobart Paper，1978，p. 9.）

〔4〕 参见朱玮、吴云、杨波：《区块链简史》，中国金融出版社 2020 年版，第 3 页。

〔5〕 欧洲中央银行较早提出了通过“可转换性”对虚拟货币进行监管分类，并提出只有可转换式虚拟货币才具有金融监管意义。这种分类方法被国际监管界和主要国家监管当局所普遍接受。[See European Central Bank，Virtual Currency Schemes，p. 5 (October 2012).] 另可参见〔德〕伦纳·库尔姆斯：《比特币：自我监管与强制法律之间的数字货币》，廖凡、魏娜译，载《国际法研究》2015 年第 4 期。这是中文作品中少有的深入讨论虚拟货币可转换性的可信佳作。

〔6〕 参见前引〔4〕，朱玮、吴云、杨波书，第 179－226 页。

〔7〕 参见徐忠、邹传伟：《区块链能做什么、不能做什么?》，载《金融研究》2018 年第 11 期。该文在论述虚拟货币的社科类文章中堪称技术严谨的典范。

〔8〕 参见吴云、朱玮：《虚拟货币：一场失败的私人货币社会实验?》，载《金融监管研究》2020 年第 6 期。

沃巴赫的《信任，但需要验证：论区块链为何需要法律》〔9〕是跨学科的佳作，其法律论证建立在技术的真实背景之上。该文从区块链治理的角度分析监管的必要性，而本文则是立足虚拟货币的职能和社会效果来分析监管的必要性，两者角度不同，可以相互补充和验证。在具体的论证上，两者也可以相互补充验证。例如，沃巴赫文指出信任区块链的分布式记账技术“不可与信任特定个人和机构混为一谈”，而本文关于虚拟货币价格操纵的论述则是对这个判断的恰当注解。

中外学者虽然对虚拟货币是否构成“货币”有所争议，但至少都肯定其可以或者部分可以执行货币的三大职能（交易媒介、价值储藏、计价单位）。〔10〕2017 年以来，随着“代币首次发行”（ICO）在中国监管文件中出现，〔11〕一些学者援引美国等法例，论证虚拟货币属于证券。〔12〕一些文献也开始跟踪国际反洗钱规则的变化，并梳理了虚拟货币的国际反洗钱监管动态。〔13〕

但是，有些文献在论证某种属性时，往往带着非此即彼的基本假设，在论证一种性质时会否定另外一种性质。例如，杨东提出虚拟货币的性质是众筹〔14〕（美国法上可以豁免监管的一类证券），杨延超认为虚拟货币应该属于“货币”〔15〕。这些作品的共同不足在于，试图论证出“唯一”的属性，忽视了从金融监管的角度看，虚拟货币可以同时具有多重属性。

在国内文献中，综合视角的尝试不多，仅见孙国峰和陈实的短评文章从综合的视角分析了美国对虚拟货币的多重监管，〔16〕朱玮、吴云和杨波初步提出了“虚拟货币三重属性”，即货币（或者执行货币职能）、证券和价值转移手段（反洗钱的监管对象）〔17〕。多重监管是很常见的现象，以中国证券行业为例，证监会作为行业主管部门要对证券机构（准入、内部治理等）和证券行为（发行、交易等）实施监管，中国人民银行作为反洗钱主管机关实施监管。

本文分析了虚拟货币三个金融属性的监管框架，并结合工作经验对监管框架内在逻辑进行了分析；回答了为什么国际上首先就虚拟货币反洗钱问题形成了成熟的监管规则和共识，而证券监管和货币监管尚处在起步阶段；同时，对虚拟货币反洗钱监管及其对整个金融监管框架的影响进行了分析。

〔9〕 参见〔美〕凯文·沃巴赫：《信任，但需要验证：论区块链为何需要法律》，林少伟译，载《东方法学》2018 年第 4 期。

〔10〕 例如，贾丽平：《比特币的理论、实践与影响》，载《国际金融研究》2013 年 12 期。该文认为，虽然虚拟货币还没有成为真正的货币，但可以执行货币的职能。该文是国内较早就虚拟货币的货币性质进行研究的论文，论证比较中肯，结论也广为接受。

〔11〕 2017 年，中国人民银行等七部委颁布了《防范代币发行融资风险的公告》，这是官方对外规范性文件中第一次出现“代币首次发行”。

〔12〕 例如，孙国峰、陈实：《论 ICO 的证券属性与法律规制》，载《管理世界》2019 年第 12 期。该文比较娴熟地运用美国证券监管规则分析了虚拟货币的证券属性。

〔13〕 参见蔡制宏：《数字货币发展状况、可能影响及监管进展》，载《金融发展评论》2015 年第 3 期。

〔14〕 参见杨东：《“共票”：区块链治理新维度》，载《东方法学》2019 年第 3 期。

〔15〕 参见杨延超：《论数字货币的法律属性》，载《中国社会科学》2020 年第 1 期。该文提出了“数字货币新货币说”，但从其表述来看，应仅限于“虚拟货币”（私人发行的数字货币）中的加密货币（非中心化、分布式的虚拟货币）。

〔16〕 参见孙国峰、陈实：《美国虚拟货币监管借鉴》，载《中国金融》2017 年第 19 期。该文虽然仅是一篇非学术的简短评论，但比较全面讲解了美国对虚拟货币的金融监管框架，是国内文献中少有的多维度讲解虚拟货币的文章。但限于篇幅和期刊性质，该文仅讲解了监管框架，尚未深入分析虚拟货币的性质。

〔17〕 参见前引〔4〕，朱玮、吴云、杨波书，第 271－283 页。

尤其值得注意的是，反洗钱监管在国际上早已是“大热门”，但在中国尚属“偏门”，《反洗钱法》通过仅 15 年时间，法学界研究还多限于刑法学界，罕有真正从“金融监管”角度进行的研究。〔18〕学界很多作品强调虚拟货币的洗钱风险，但罕有专业性分析（内在洗钱风险等）。

本文在这些方面填补了空白。本文的基本逻辑是：虚拟货币作为一场货币实验的失败反证了国家干涉的必要性；由于虚拟货币并未对现今货币体系形成冲击，且虚拟货币是否适合普通投资者参与也存在很大争议，而虚拟货币价格操纵、通过虚拟货币洗钱则是现实紧迫的问题，因此，各国首先就虚拟货币反洗钱监管达成了共识，迈出了虚拟货币监管的关键性一步。

本文的主要贡献在于：按照虚拟货币三重属性的观点，提出虚拟货币监管的框架和内在逻辑，对强制性国际反洗钱标准及其影响进行分析，并就如何对区块链治理实施监管这样深层次的问题进行了展望。

二、虚拟货币的失败：监管的必要性前提

虽然学界对“什么是货币”有多种学术观点，〔19〕但是，对于货币的职能却有高度共识，即货币具有价值储藏、交易媒介和计价单位三大职能〔20〕。同理，对虚拟货币是否构成“货币”争论很多，〔21〕但是，虚拟货币已经可以执行货币职能已经是不争的事实〔22〕。吴云、朱玮曾指出，在虚拟货币这一场私人货币实验运动中，虽然诞生了一系列影响经济模式和社会格局的技术创新，在价值流转、权利证明、商业模式等方面都有广泛的运用空间，但是，从货币职能的角度，这场私人自发运动并不成功，而且产生了巨大的负面效果。〔23〕总结起来，主要有以下几个方面：

（一）虚拟货币执行货币职能存在根本缺陷：以比特币为例

法定货币与比特币的对比可参见表 1，以下分别详细阐述。

---

〔18〕 我国 2006 年通过的《反洗钱法》是参照国际标准制定的金融监管性法律，其基本逻辑是通过对金融机构等义务机构实施监管构筑反洗钱预防体系，而如何惩治洗钱行为则由《刑法》规定。“洗钱”是一个不断发展的概念。本文对“洗钱”采用广义的概念，“洗钱”包括“狭义的洗钱”“恐怖融资”两个方面。“洗钱”在更广义的情况下还包括 FATF 框架下的“扩散融资”，指的是向联合国安理会所制裁的朝鲜、伊朗个人或实体提供资金、资产或与其进行交易的行为。

〔19〕 例如，商品货币学派认为货币是商品中衍生出的一般等价物，信用货币学派认为货币仅是计量“信用—债务”关系的会计工具。(See Thomas H. Greco, JR., *Money: Understanding and Creating Alternatives to Legal Tender*, Chelsea Green Publishing, 2001, p. 22.)

〔20〕 这是中外主流教科书中对货币基本功能的界定。例如，N. Gregory Mankiw, *Principles of Economics*, Cengage Learning, 2018, p. 605；逄锦聚等主编：《政治经济学》，高等教育出版社 2014 年版，第 50－52 页。该《政治经济学》教科书中还列举了延期支付（书中称为“支付手段”）和世界货币两个职能，延期支付职能可被认为是交易媒介职能的延伸，两者具有包含关系，世界货币职能是前几个货币职能的国际化延伸。

〔21〕 王信、骆雄武提出货币从民间到官方是一个历史趋势，虚拟货币由于缺乏国家信用支撑，很难获得认可，并且进一步提出央行数字货币的推出将在吸收虚拟货币技术优势的基础上进一步强化国家法定货币的地位。(参见王信、骆雄武：《数字时代货币竞争的研判及应对》，载《国际经济评论》，2020 年第 2 期，第 25－35 页。) 本文赞同该文的论证和观点，并进一步认为，应当从正当性和功能两个角度来理解虚拟货币的货币属性，而且要考虑获到社会共识是一个动态和演化的过程。

〔22〕 See Mark Carney, The Future of Money, Speech by the Governor of the Bank of England to the inaugural Scottish Economics Conference , Edinburgh University (March 2, 2018). 该演讲很大程度上代表了国际金融监管界的共识。国内学术文献可参见前引〔10〕，贾丽平文。

〔23〕 参见前引〔8〕，吴云、朱玮文。

表 1　　**法定货币和比特币的对比**

	法定货币	比特币	后果
系统容量	现有电子支付系统理论上可以无限扩容	系统容量有理论上限	比特币无法成为公众大规模使用的支付手段
支付速度	几秒（现有电子支付）	平均 10 分钟	
币值波动率	相对稳定（主要货币）	超过主要货币 10 倍	比特币无法成为价值储藏手段和可信计价单位
支付成本	中国国内银行转账：0 中国国际电汇：200～300 元	0.58～224 元 （2017 年）	比特币并未展现普惠金融的优势
技术安全性	高	低	

1. 系统承载容量有限无法用于大规模支付

比特币特殊的技术安排导致其交易容量有限，不能承载社会大规模使用。比特币的技术设计限定了平均每秒 7 笔的交易容量，而支付宝可承载的峰值交易记录是每秒 25.6 万笔（2017 年 11 月 11 日）。截至 2019 年 11 月 23 日，比特币共有约 60.5 万个区块，理论上目前的比特币系统仅能承载约 24.78 亿笔交易，不及中国第三方支付的三天清算量。相反，现有的中心化电子支付系统（银行电子支付系统、第三方支付系统）可以通过系统的软硬件升级做到无限扩大容量。

尽管后续的虚拟货币试图对比特币进行改进，但技术缺陷仍未有根本突破。例如，根据以太坊白皮书推算，以太币（ETH）的理论最高承载量仅为每秒 15 笔交易。柚子币（EOS）声称每秒承载容量可达到 3996 笔交易，〔24〕这一容量使其至多作为小的国家、地区或者行业的支付方式。最近提出的“闪电网络”寄希望于通过离线技术（以比特币作为“抵押”在闪电网络进行交易，通过比特币系统作最后“结算”）实现比特币无延迟、低成本交易，但目前仅有 895 个比特币的支付容量，〔25〕且存在一系列技术性不足〔26〕。

2. 交易速度极慢导致虚拟货币无法用于日常支付

从单笔处理速度看，比特币比现有普遍使用的电子支付方式落后了几个数量级，无法用于公众日常使用。实践中比特币每笔交易的平均确认时间为 10 分钟（大额交易需要的确认时间更长），相反，支付宝每笔交易时间为 3 秒，而常用的非接触卡交易时间少于 1 秒。2017 年 12 月，比特币价格上涨导致比特币交易暴增，比特币系统开始拥堵，当月一笔交易平均等待时间是 2 天 2 夜。〔27〕

因此，从交易媒介的角度，比特币及后续出现的多种虚拟货币由于容量过小、交易速度过慢，无法作为公众大规模使用的支付手段，只能用于对时限要求不高的大宗交易。

〔24〕 参见其官方网站，载 https://eosnetworkmonitor.io/，最后访问时间：2020 年 3 月 6 日。

〔25〕 2018 年 1 月闪电网络系统在比特币主网上线，目前闪电网络有节点 11624 个，支付通道 36289 个，整体支付容量为 895 个比特币。数据来源于 1ml 网站，载 https://1ml.com/statistics，最后访问时间：2020 年 3 月 6 日。

〔26〕 如闪电网络结构趋向中心化，网络运行效率依赖大型中心节点的支付容量，而非点对点网络的规模扩张。

〔27〕 数据来源：https://www.blockchain.com/charts，最后访问时间：2020 年 3 月 6 日。

3. 币值波动过大导致虚拟货币不能承担价值储藏手段和计价单位职能

比特币在其发展初期的 2011 年曾经在两个月内价格从 0. 75 美元上涨 40 倍，达到 30 美元，随之 2012 年 2 月跌破 2 美元，跌幅超过 93%。最近一次较大波动发生在 2019 年 11 月 21 日，24 小时内比特币价格下跌 7%。〔28〕 相反，主要国家货币日涨跌幅达到 1%、主要股票指数的日涨跌幅达到 2%～3%已经属于较大价格波动。

吴云和朱玮通过统计长期以来不同资产价格变化率发现，比特币的波动率是主要货币波动率的 10 倍，是贵金属波动率的 3～5 倍，是股票市场波动率的 3～5 倍，是原油波动率的 3 倍。〔29〕比特币极高的波动率超过了现有主要货币波动率一个数量级，远高于主要风险资产的波动率，无法成为价值储藏的手段，交易各方无法约定比特币计价的未来商品和服务。

因此，从货币职能角度看，由于交易媒介和价值储藏两个核心职能存在缺陷，以虚拟货币标价（计价单位）的体系难以稳定和有效，虚拟货币难以成为可信的计价单位。

4. 容量有限、速度慢导致交易费用过高

比特币的支持者一再宣扬：对于无法从现有金融体系中获得服务的人们（如偏远地区没有银行网点，民众难以获得金融服务），虚拟货币的去中心化可以增强金融的包容性。然而，这仅仅是一种理论上的推演，完全不符合实际情况。虚拟货币虽然可以脱离金融中介在点对点网络中流转，但是，这种虚拟货币的流转需要消耗系统算力，用户支付转账时必须要给提供算力的矿机支付一定比例的虚拟货币以补偿其提供的算力。〔30〕

当用户转移比特币时，首先要在钱包上构造交易，然后提出一个手续费报价，交易广播出去到达矿机后，矿机一般会按照手续费由高到低进行“接单”，形成一个众多钱包各自分散报价和众多矿机自主选择交易的撮合体系。也就是说，比特币的交易费用由用户和矿机间的自由市场所确定，并无固定比例和规则约束。随着虚拟货币币值的升高和交易活跃程度增加，转账手续费也会越来越高。其中，虚拟货币币值升高，意味着等量手续费对法定货币的相对价格上升；交易活跃程度增加，则大量交易在矿机中形成基于手续费高低的竞争。用户若希望矿机更早验证和打包自己的交易，则需要支付更高的手续费。

2016 年每笔比特币交易费折合人民币平均为 0. 58 元，2017 年 12 月由于交易拥堵和比特币价格暴涨则高达 224 元。〔31〕 相比而言，我国内银行国内网络转账已经实现零手续费，几大银行对境外汇款每笔手续费一般在 200～300 元之间，比特币转账在成本上并无任何优势。

5. 安全性较差

比特币私钥一旦丢失将无法追回。〔32〕 例如，2013 年虚拟货币交易所 Mt. Gox 价值 4. 5 亿美

〔28〕 关于比特币的历史价格来源：http://www. blockchain. com/charts，最后访问时间：2020 年 3 月 6 日。

〔29〕 参见前引〔8〕，吴云、朱玮文。

〔30〕 矿机为系统提供算力可以获得两部分利润，一是系统提供挖矿收益，二是用户提供的转账手续费。按照比特币的算法设计，2140 年之后，比特币总量不再增加，矿机的收益将只有用户的转账手续费。（参见前引〔4〕，朱玮、吴云、杨波书，第 86 页。）

〔31〕 数据来源：https://www.blockchain.com/charts，最后访问时间：2020 年 3 月 6 日。

〔32〕 See Christian Beer，Beat Weber，Bitcoin-The Promise and Limits of Private Innovation in Monetary and Payment Systems，Q4 *Monetary Pol'y and the Economy*，53，53－66 (2015).

元比特币丢失，2016 年虚拟货币交易所 Bitfinex 价值 7000 万美元的比特币丢失。虚拟货币对使用者的技术水平提出了很高的要求，往往超出了普通人的技术能力。相反，现有的电子支付体系经过反复调试已经兼具较高的安全性和便捷性。

这也提出了普惠金融的悖论：若使用者能够安全使用虚拟货币进行支付，那么他一定拥有电子设备和相应的技术能力，可这样的人往往有充分的渠道获得现有金融体系的服务。

（二）比特币价格被人为操纵，刺激了虚拟货币泡沫

信任区块链的分布式记账技术不可与信任特定个人和机构混为一谈。〔33〕一些大交易所利用独特地位操纵虚拟货币价格。

第一次是 2013 年 10 月 3 日至 11 月 30 日，每枚比特币的价格由 116 美元涨至 1150 美元，两个月内暴涨 10 倍。一则学术研究用严谨的数据和逻辑证明，当时全球最大的交易平台 Mt. Gox（注册地在日本）虚增几个特定账户中的美元资金和比特币，然后通过几个账户之间的交易人为拉高比特币价格。〔34〕2019 年 3 月，东京地方法院判决 Mt. Gox 的 CEO 篡改记录虚增资产罪名成立。〔35〕

第二次是 2017 年 3 月 27 日至 12 月 17 日，每枚比特币价格由 1046 美元上涨至日间最高 20089 美元，九个月之内暴涨 20 倍。一则学术研究揭露，Tether 公司通过发行没有实际支持资产的稳定币 USDT 在其旗下的 Bitfinex 交易所操纵比特币价格。〔36〕由于该研究的巨大影响力，2018 年 11 月美国司法部和美国期货交易委员会（CFTC）联合对比特币背后可能存在的价格操纵进行了调查。〔37〕

比特币价格的暴涨，引起了对虚拟货币投资的跟风效应，刺激了“山寨币”的大量出现，代币首次发行（ICO）变成了热门话题，各种“币”价格暴涨。

早期的山寨币运营，需要一定的技术和成本投入，如早期的万事达币（Mastercoin）就是比特币二层协议的经典。2015 年以太坊的出现彻底消除了山寨币的技术门槛。以太坊的智能合约使用 Solidity 语言，开发者可以极为便捷地使用 Solidity 开发出新的虚拟货币，只需部署一个标

〔33〕 参见前引〔9〕，凯文·沃巴赫文。

〔34〕 See Neil Gandal et al.，Price Manipulation in the Bitcoin Ecosystem，95 *J. Monetary Econ.*，86，86－96（2018）.

〔35〕 有关案件的情况参见 Yuki Furukawa，Former Mt. Gox CEO Mark Karpeles Gets Suspended Jail Term，March 15，2019，载 https：//www. bloomberg. com/news/articles/2019－03－15/former-bitcoin-baron-mark-karpeles-gets-suspended-jail-term，最后访问时间：2020 年 6 月 10 日。

〔36〕 See John M. Griffin，Amin Shams，Is bitcoin really un-tethered? October 28，2019，available at SSRN：https：//ssrn.com/abstract＝3195066，last visited on Jun. 10，2020. 此论文更新版本将发表于权威期刊《金融学期刊》（The Journal of Finance）。作者通过对 200G 的交易数据的研究，证明了几个主要假设：（1）当比特币价格下跌时，大量 USDT 被用来购买比特币；（2）当比特币价格在整数关口附近时，大量 USDT 被用来购买比特币；（3）存在明显的“月底效应”。每个月月底会计师事务所要审计 USDT 在该时点是否有充足的美元作为支持资产，审计前存在明显的卖出比特币换回 USDT 的情况，这在一定程度上验证了 Tether 所发行的 USDT 并没有足额支持资产的传闻。在更新的版本中，作者增加了一个新的发现，一个账户的交易者展现了“未卜先知”（clairvoyant）的把握交易时点的能力，对比特币价格施加了“极端大的”（extremely large）影响力。

〔37〕 See Matt Robinson，Tom Schoenberg，Bitcoin-Rigging Criminal Probe Focused on Tie to Tether，Bloomberg，November 20，2018，at Markets；Kate Rooney，As Bitcoin Nosedives，Regulators Said to be Investigating Whether It Was Propped Up Illegally，CNBC，November 20，2018，available at https：//www. cnbc. com/2018/11/20/regulators-investigate-whether-bitcoin-price-was-propped-up-illegally. html，last visited on Jun. 10，2020.

准的 ERC20 代码即可完成，其简易程度如同注册一个域名，用时不超过 10 分钟。据 etherscan.io 网站的统计，在 2018 年 6 月 12 日以太坊上的 ERC 20 代币智能合约共计 90738 种，到 2020 年 3 月 5 日已经增加到 245504 种。其中真正有技术含量或价值的，凤毛麟角。

根据 Coinmarketcap 按照市值排名对 5164 种虚拟货币的回溯性统计，2014 年 1 月 1 日，虚拟货币市场总市值为 106 亿美元（其中比特币 94 亿美元），而到了 2017 年 12 月 17 日，虚拟货币总市值为 8003 亿美元（其中比特币 3200 亿美元）。比特币在虚拟货币市值中的比重由约 90% 降为约 40%，虚拟货币领域由比特币一枝独大变成了遍地开花。

从 2013 年起，美国证券交易委员会（SEC）通过风险提示公布了大量以虚拟货币为幌子的欺诈案例。〔38〕在中国，大量山寨币沦为空气币，完全成为投机和诈骗的工具。如“太空链”诈骗金额高达 10 亿元；〔39〕“GGP 共赢积分”以虚拟货币为噱头进行传销，涉案金额 10 亿元；〔40〕“PlusToken”席卷全球 170 个国家，涉及受害人 300 万，涉案金额 200 亿元〔41〕。

（三）被洗钱和犯罪滥用

虚拟货币由于其匿名性、无国界性，具有被洗钱利用的很高内在风险（inherent risk），容易被洗钱和犯罪活动所利用。〔42〕几乎所有的“暗网”市场都通过虚拟货币进行交易。至少一半左右的暗网活动是违法犯罪活动。〔43〕暗网也被恐怖主义活动利用，伊斯兰国（ISIS）曾经广泛使用暗网进行信息分享、招募、宣传，并通过虚拟货币筹集资金。〔44〕

虚拟货币也出现在各类网络犯罪活动中，越来越多的犯罪活动不再通过传统的金融系统进行支付，而是通过虚拟货币收取勒索的赎金等，从而逃避监管和执法机关的追踪。〔45〕

虚拟货币至少一半用于违法犯罪活动。根据 2018 年的研究推算，四分之一的比特币用户、二分之一的比特币交易与非法活动有关，2015 年至 2017 年每年大约有 720 亿美元的规模，相

〔38〕 例如，SEC，Investor Alert：Ponzi Schemes Using Virtual Currencies（July 23，2013）；再比如 SEC，Investor Alert：Bitcoin and Other Virtual Currency-Related Investments（May 7，2014）。

〔39〕 参见冯樱子、金微：《太空链破发 90% 大佬纷纷撇清关系》，载《华夏时报》2018 年 4 月 9 日，第 13 版。

〔40〕 2019 年该案已经二审宣判，并被最高人民检察院列为 2019 年典型案例。（参见最高人民检察院官方网站，载 https://www.spp.gov.cn/xwfbh/wsfbh/201912/t20191203_440338.shtml，最后访问时间：2020 年 3 月 6 日。）

〔41〕 关于 PlusToken 的相关报道参见毕丹丹：《警惕“虚拟货币”“区块链”骗局：勿让非法集资钻空子》，载《上海金融报》2019 年 11 月 8 日，第 10 版；《涉案 200 亿 币圈最大的资金盘崩了》，载《知识经济》2019 年第 20 期。

〔42〕 内在风险（inherent risk），也译为“固有风险”，是反洗钱专业术语，指在不考虑任何风险控制措施的情况下所暴露的洗钱风险。例如，在我国，由于股票采取公开集中竞价交易，在没有任何控制措施的情况下，股票交易比银行转账交易的洗钱风险要低，可以认为前者比后者的洗钱内在风险更低。[See The Wolfsberg Group，Wolfsberg FAQs on Risk Assessments for ML，Sanctions and Bribery & Corruption，p. 7（2015）.]

〔43〕 See Gollnick，Clare，Emily Wilson，*Separating Fact from Fiction*：*The Truth about the Dark Web*，Terbium Labs，2016，pp. 5 - 6.

〔44〕 万维网（the World Wide Web）分为“表层网”（surface web）和“深网”（deep web）两个部分。我们日常能够使用的仅是表层网，能够通过搜索引擎索引，可以通过普通浏览器直接登录；不能被搜索引擎索引的被称为“深网”，也叫“不可见网”（invisible web），日常常见的包括电子邮件、网络银行、付费数据库、公司的内网等。根据估计，“深网”的规模至少是“表层网”的 4000～5000 倍。“暗网”（dark net，dark web）是“深网”的一部分，通过加密技术刻意将内容、网址等隐藏起来，需要通过特殊的软件、授权或设置才可以接入。（See Kristin Finklea，Dark Web 2 - 3，9 - 12，Congressional Research Service：R44101，2017.）

〔45〕 See ECC Europol，The Internet Organised Crime Threat Assessment（IOCTA）2015 at 11（Sept. 30，2015）.

当于美国和欧洲每年毒品犯罪额的总和。〔46〕无论是相对数量还是绝对数量都是非常惊人的。〔47〕

三、为什么虚拟货币监管从反洗钱开始

虚拟货币严重的价格操纵、投机以及被洗钱和犯罪滥用风险，反证了国家对货币秩序进行干涉的必要性。但国家对虚拟货币不同维度干涉的急迫性和必要性是不同的。

由于虚拟货币对法定货币体系的冲击并未显现，衍生出的审慎问题也尚在讨论之中，因此，货币相关当局对虚拟货币基本处于观察之中。同时，由于投资者适当性问题的困扰，美国等主要国家尚未允许任何一种虚拟货币对公众发行，国际社会也没有就如何向普通投资者发行虚拟货币形成大范围的共识，注册或审批的正面案例不多。相反，目前在投资领域虚拟货币暴露的更多是价格操纵、欺诈等问题，因此，主要国家对虚拟货币的监管以采取行政处罚、司法调查等方式为主。同时，由于通过虚拟货币洗钱的问题日益严重，各国反洗钱当局已经共同认识到监管虚拟货币的现实必要性和急迫性。

（一）金融监管的基本框架和问题

传统的金融监管包括审慎监管和行为监管两个目标。审慎监管包括宏观审慎监管和微观审慎监管。前者的目的是维持金融体系的稳定，一般由作为货币当局的中央银行负责；后者的目标是单个金融机构的稳健性，由中央银行或者单独的审慎监管机构负责。行为监管以金融消费者保护为目的创造并维护金融市场秩序的公平性、透明性（如证券市场的强制信息披露）。在现有的法定货币体系中，由于货币会通过金融中介（典型的是商业银行）进行信用放大，进而衍生出审慎监管问题，为简化讨论，我们将中央银行和审慎监管当局统称为“货币监管相关当局”。

反洗钱监管并非传统意义上的金融监管，最初是20世纪70年代美国为应对日益严重的毒品犯罪而对银行设定反洗钱义务，其目的在于预防和发现利用金融体系的犯罪活动。〔48〕

我们根据美国对虚拟货币的多重监管的事实，〔49〕参照前述朱玮、吴云和杨波的结论，认为虚拟货币具有三种属性：从货币的角度，虚拟货币可以执行货币作为价值储藏手段、交易媒介和计价单位的职能；从投资的角度，虚拟货币是证券投资（或者至少是一种需要被监管的投资）；

〔46〕 See Sean Foley，Jonathan R. Karlsen，Talis J. Putnins，Sex，Drugs，and Bitcoin：How Much Illegal Activity Is Financed Through Cryptocurrencies? 32（5）*Rev. Financial Stud.*，1798，1798－1853（2019）.

〔47〕 也有研究认为比特币从事非法活动数量可能不多。美国麻省理工学院IBM沃森人工智能实验室利用人工智能对20万个比特币节点的23万个支付流和166种特征进行了深度学习，只发现其中2%从事非法活动、21%从事合法活动。但由于对其余77%无法进行有效识别，该研究说服力不强。（See Mark Weber et al.，Anti-Money Laundering in Bitcoin：Experimenting with Graph Convolutional Networks for Financial Forensics，arXiv：1908. 02591，Submitted on July 31，2019，available at https://arxiv.org/abs/1908. 02591，last visited on Jun. 10，2020.）

〔48〕 在不同国家，可能由不同的部门对金融机构实施反洗钱监管，包括：中央银行（如中国）、财政部（如美国）、警察部门（如澳大利亚）、金融行为监管部门（如英国）、单设专门部门（如俄罗斯）等。

〔49〕 参见前引〔16〕，孙国峰、陈实文。

从反洗钱角度，虚拟货币是价值转移的手段。〔50〕

虚拟货币执行货币职能与价值转移手段职能二者紧密联系，虚拟货币正是因为可以充当交易媒介，所以可以替代法定货币进行价值转移。按照实质优于形式的原则，2013 年美国财政部就将虚拟货币纳入了反洗钱监管。〔51〕这个原则被 FATF 制定的国际反洗钱标准所吸收。

虚拟货币可以执行货币职能、可以作为价值转移的手段较为容易理解，但是，在直觉上虚拟货币与通常的证券（股票、债券）相差极大。美国 SEC 在阐述监管政策时指出，传统的证券确实是基于企业或公司利益的，但这并不是证券的本质所在，SEC 仍然坚持用“豪威标准”（Howey test）四要件判断是否属于证券。〔52〕由于虚拟货币性质讨论并非本文重点，本文在此仅作一般说明，国内有大量关于 ICO 研究的论文可以参考。〔53〕

虚拟货币所面临的金融监管问题的汇总可参见表 2。

表 2　　虚拟货币面临的金融监管问题

性质	监管内容	监管当局	具体监管者举例	虚拟货币有关的监管问题
货币〔54〕	支付和清算，法定清偿手段	中央银行	中国人民银行，英格兰银行	尚未对法定货币体系形成冲击
	金融稳健性	审慎监管当局	中国人民银行（宏观）、中国银保监会（微观）；英格兰银行	对金融审慎的问题尚处在概念讨论阶段
证券〔55〕	投资者保护、市场秩序	金融行为监管当局	中国证监会；英国金融行为监管局（FCA）；美国证券交易委员会（SEC）	是否适合普通投资者存在巨大争议；主要面临的问题是欺诈、价格操纵
价值转移手段	反洗钱	反洗钱监管当局	中国人民银行；美国财政部；英国金融行为监管局（FCA）	被洗钱和犯罪活动利用已经相当严重，具有监管的迫切性

（二）反洗钱先行的内在逻辑

对虚拟货币货币属性、证券属性和价值转移手段属性的三种监管在现阶段面临的急迫性和必

〔50〕 参见前引〔4〕，朱玮、吴云、杨波书，第 271－283 页。

〔51〕 See Financial Crimes Enforcement Network，Application of FinCEN's Regulations to Persons Administering，Exchanging，or Using Virtual Currencies，United States Department of the Treasury（March 2013）. 美国财政部认为，提供虚拟货币价值转移服务在性质上和已有的货币服务业务（money service businesses，MSBs）没有本质区别，因此要适用相同的反洗钱监管标准。

〔52〕 See SEC Chairman Jay Clayton，Statement on Cryptocurrencies and Initial Coin Offerings（Dec. 11，2017）. 豪威规则四要件的具体运用可参见 SEC，Framework for“Investment Contract”Analysis of Digital Assets（April 3，2019）。

〔53〕 如前引〔12〕，孙国峰、陈实文；张美慧：《境外市场证券法视野下的代币发行监管——基于美国、新加坡、澳大利亚和中国香港地区的监管实践》，载《财经法学》2019 年第 3 期，该文深入运用多个国家和地区的监管规则分析了虚拟货币的证券属性。

〔54〕 美国银行业的监管体系较为复杂，涉及审慎监管职能的包括美联储、财政部下设货币监理署（OCC）、联邦存款保险公司（FDIC），为简化问题，表中略去有关内容。

〔55〕 证券行业通常被认为是“资本中介”，自身并不经营风险，风险由投资人承担，证券行业仅在自己作为交易对手方等少数情况下存在审慎监管的问题。金融监管对审慎问题关注的焦点是银行和保险，实践中证券业的行为监管和审慎监管一般由同一个监管者负责。（参见吴云、张涛：《危机后的金融监管改革：二元结构的“双峰监管”模式》，载《华东政法大学学报》2016 年第 3 期。）

要性是不同的。

1. 虚拟货币并未对法定货币体系形成冲击：货币相关当局的容忍

在作为价值储藏手段和交易媒介时存在的天然缺陷，导致虚拟货币并未对现有货币体系形成值得关注的冲击或影响。各国在坚持法定货币作为唯一法定清偿手段的前提下，基本采取了容忍态度（除少数绝对禁止的国家）。

同时，数字货币（包括私人发行的虚拟货币和中央银行发行的“央行数字货币”）出现后，传统的金融中介（如银行）是否还有存在价值、社会信用如何放大等完全处在概念讨论阶段，〔56〕因此，审慎监管也并非本阶段的问题。

总之，目前货币主权和相关的金融稳定问题并不突出，也没有监管的必要性和急迫性。

2. 虚拟货币并不适合普通投资者：公开发行的暂缓

证券监管的核心目标是保护公众投资者，只有适合公众投资风险承受能力的产品才可以公开募集和发行，才需要进行监管（否则可以豁免）。虚拟货币究竟在多大程度上适合普通投资者是始终使各国监管者困惑的根本问题，因为专业投资者对虚拟货币的内在价值也存在巨大的分歧和争议。美国尚未登记或批准任何一种面向大众的虚拟货币或虚拟货币金融产品。〔57〕2018 年 SEC 在驳回 Winklevoss 申请比特币金融产品的官方意见中指出：按照美国证券法，是否具有内在价值由投资者自己判断，但是，SEC 有权审查基础资产（比特币）市场是否可以内在地抵御欺诈和操纵（inherently resistant to fraud and manipulation）或者有充分的预防性手段抑制欺诈和操纵。比特币（基础资产）市场并不能“内在地抵御欺诈和操纵”，也没有充分的预防性手段抑制欺诈和操纵，因此，比特币为基础资产的金融产品不适合普通投资者参与。〔58〕

虚拟货币由于没有任何支持资产，〔59〕“是否具有内在价值”“如何判断内在价值”在专业投

〔56〕 See BIS, Central Bank Digital Currencies 6, CPMI Papers No. 174, March 2018, available at https://www.bis.org/cpmi/publ/d174.pdf, last visited on Jun. 10, 2020. 中文作品中对此比较通俗的介绍，可参见〔德〕约翰内斯·比尔曼：《中央银行视角下的现金与数字货币》，载《金融市场研究》2019 年第 12 期。

〔57〕 2017 年美国芝加哥商品交易所挂牌了比特币期货，但是，期货参与者是合格投资者或专业投资者。

〔58〕 See Securities Exchange Act Release No. 83723 (July 26, 2018), 83 FR 37579 (Aug. 1, 2018). 在证券发行审批制的国家，监管当局要替代投资者进行实质性判断。但是，即使美国这样的证券注册制国家，监管当局也并非完全放弃对证券的实质性审查。SEC 多次驳回以比特币为基础资产公开发行金融产品的申请。

〔59〕 这里讨论的虚拟货币内在价值问题仅限于比特币这样没有支持资产的非稳定币。以法定货币或实物资产为储备的“稳定币”（stablecoin），也叫“资产支持型稳定币”（asset-linked stablecoin）。USDT 以美元为储备资产，是最典型也是最广泛使用的稳定币。此外，脸书（Facebook）对外公布的“天秤币”（Libra）曾打算以“一篮子”货币作为储备资产；还有以商品为支持资产的虚拟货币，如 DGX（DIGIX GOLD TOKENS）以黄金作为储备资产。但是，这种稳定币需要对支持资产进行托管，一些研究对这种稳定币发行者是否有足额资产提出怀疑，如前文所引 Griffin 等（2019）。“资产支持型稳定币”稳定币值的效果取决于支持资产的币值稳定性。在广义上，“算法基础型稳定币”（algorithm-based stablecoins）也被归为稳定币，通过算法调节代币总量来保持币值稳定。当币值价格下跌时，销毁部分代币，从而维持价格稳定；反之则增加代币数量。但是，这种稳定币在实践中并未取得稳定币值的效果，典型的例子是 NuBits。当然，对“算法基础型稳定币”的定义和范围还存在一定争议，此处不赘述。［See FSB, Regulation, Supervision and Oversight of “Global Stablecoin” Arrangements: Final Report and High-Level Recommendations, 9－10 (2020); Dirk Bullmann, Jonas Klemm, Andrea Pinna, In Search for Stability in Crypto-assets: are Stablecoins the Solution? ECB Occasional Paper No. 230, 23 (2019).］

资者当中尚有巨大的分歧。著名投资家沃伦·巴菲特认为比特币是“赌博的工具”“老鼠药”。〔60〕巴菲特的理解不一定正确，但至少说明全球顶级的专业投资者群体中对比特币的内在价值也存在巨大的争议。国际社会没有就如何向普通投资者发行虚拟货币形成大范围的共识，注册或审批的正面案例不多。

3. 反洗钱监管先行

时任 FATF 主席在 2018 年公开撰文呼吁各国重视虚拟货币被犯罪活动所利用的严重性，因为“虚拟货币已经与金融犯罪手牵手”〔61〕。虚拟货币由于匿名性，欺诈和价格操纵很难被发现。反洗钱监管能够为遏制虚拟货币市场的严重欺诈和操纵创造良好的前提，从而减少普通投资者的进入障碍。反洗钱监管将在很大程度上建立一个交易的可追踪体系，可以从根本上提高识别和遏制通过虚拟货币进行的违法犯罪活动的能力，从而净化市场和交易。因此，打击虚拟货币价格操纵、欺诈和打击通过虚拟货币洗钱的两个诉求汇聚到了反洗钱监管。

（三）国际社会以反洗钱为起点的监管尝试

金融行动特别工作组（Financial Action Task Force，简称“FATF”）是国际反洗钱标准的制定者，〔62〕从 2013 年起，FATF 着手对虚拟货币的洗钱风险进行研究。2014 年 6 月 FATF 发布了《虚拟货币：关键定义和潜在反洗钱、反恐怖融资风险》（Virtual Currencies：Key Definitions and Potential AML/CTF Risks）的报告，梳理了相关定义并结合刑事案例对虚拟货币洗钱进行了研究。2015 年 6 月 FATF 发布了《以风险为基础的虚拟货币指引》（Guidance for a Risk-based Approach to Virtual Currencies），对 FATF 标准如何适用于虚拟货币进行了探讨。

经过长期研究和讨论，在 FATF 框架下各国当局就虚拟货币反洗钱监管达成了共识。2019 年 6 月 FATF 全体会议通过了虚拟货币监管标准和配套监管指引《以风险为基础的虚拟资产和虚拟资产服务提供商指引》（Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers，以下简称《FATF2019 虚拟货币指引》），并且着手对各国执行情况进行评估。这是所有国际组织中，制定并通过的第一个针对虚拟货币的监管标准，形成了虚拟货币反洗钱监管的国际共识。

---

〔60〕 See Yun Li，Warren Buffett Says Bitcoin is a “Gambling Device” with “a lot of Frauds Connected with It”，CNBC，May 4 2019，at Market，available at https：//www. cnbc. com/2019/05/04/warren-buffett-says-bitcoin-is-a-gambling-device-with-a-lot-of-frauds-connected-with-it. html，last visited on Jun. 10，2020.

〔61〕 Marshall Billingslea，Virtual Assets and Financial Crime Now Go Hand in Hand，Financial Times，Oct. 28，2018，at Opinion.

〔62〕 FATF 成立于 1989 年，最初是“七国集团”峰会为应对洗钱危害、预防并协调反洗钱国际行动而发起设立的政府间国际组织。经过长期演变，其已经成为国际反洗钱标准的制定机构。目前，FATF 有 39 个正式成员（含两个国际组织），全球共超过 200 个国家和地区加入了 FATF 或 FATF 框架下的区域反洗钱组织。FATF 秘书处设在经济合作与发展组织（OECD）巴黎总部。参见 FATF 官方网站的介绍，载 https://www.fatf-gafi.org/about/，最后访问时间：2020 年 6 月 10 日。中国是 FATF 成员，同时是 FATF 框架下区域性反洗钱组织“欧亚反洗钱组织”（EAG）和“亚太反洗钱组织”（APG）的成员。FATF 已经组织完成三轮世界范围内的反洗钱评估，目前正在进行第四轮反洗钱评估。中国分别于 2007 年和 2019 年通过 FATF 第三轮和第四轮反洗钱评估。

四、虚拟货币反洗钱国际监管标准及其影响

（一）反洗钱监管的国际标准概述：带有“牙齿”的强制性规则

FATF 标准由“四十项建议”组成，每项建议及其释义具有同等效力。〔63〕为了评估各国执行“四十项建议”的情况，FATF 发展了一套完整严密的“评估方法”，包含四十个合规性指标（对应“四十项建议”），十一个有效性指标（从“四十项建议”中整合而出），每个指标下一般有十几个分项指标。〔64〕

FATF“四十项建议”的特点是围绕反洗钱设定一系列的要求，包括刑事司法、反洗钱监管、国际合作、执行联合国定向金融制裁四个方面，涵盖了从司法、执法、监管到外交的各个领域。

FATF“四十项建议”对全球 200 多个经济体均有约束力。与以往国际组织不同，FATF 通过成员之间相互评估的方式督促成员履行标准，对于不能达标的成员，将采取金融抵制和反制措施，实同金融制裁。由于 FATF 的核心发起国家掌握了全球主要的可自由兑换货币和跨国支付结算系统，这些国家联合起来实施金融制裁，足以将任何经济体隔绝在世界金融体系之外，威力远超过传统的经济制裁或贸易制裁。这一整套带有“牙齿”的评估机制，使得 FATF 的反洗钱标准成为具有实质性强制约束力的国际标准。

2019 年 6 月，FATF 通过在“建议 15（新技术）”中新增“释义”的方式，具体规定了虚拟货币监管的要求。标准采用一种“连锁”（cascading）影响的方式，具体列举现有哪些“建议”适用于虚拟货币以及如何适用虚拟货币。2019 年 10 月，FATF 根据修订后的“四十项建议”修改了“评估方法”。根据 FATF 全会的决定，FATF 首先在 2020 年 6 月完成对各国（地区）执行情况的初步审查，在此基础上再组织针对性全面评估。

FATF 新通过的虚拟货币反洗钱监管标准，涉及行业准入、反洗钱监管要求、国际合作等，对虚拟货币的运行模式和行业发展具有直接的革命性影响。

（二）虚拟货币反洗钱监管的具体要求

1. 尊重各国对于虚拟货币合法性的态度

为防止外界对虚拟货币合法性的误解，FATF 将“虚拟货币”改称“虚拟资产”，并发表了声明澄清不对虚拟货币合法性进行背书。〔65〕

类似于 FATF 对赌场的监管要求，如果一国能够有效禁止虚拟货币，则不需要进行监管，反

〔63〕“四十项建议”的全称是《打击洗钱、恐怖融资和扩散融资的国际标准》［International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation（amended June 2019）］，业内一般将其称为“FATF Recommendations 2012”“四十项建议”。

〔64〕“评估方法”的全称是《评估 FATF 建议技术性合规和反洗钱、反恐怖融资体系有效性的方法》［Methodology for assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems（amended October 2019）］，业内一般将其称为“Methodology 2013”“评估方法”。

〔65〕 See FATF Statement，Regulation of Virtual Assets（Paris，France，Oct. 19，2018）.

之，则需要设立监管规则并有效监管。〔66〕

2. 适用对金融活动和金融机构的监管标准对虚拟货币活动及其服务提供商进行监管

现有的反洗钱监管规则的基本框架是，通过给义务机构（包括金融机构和“特定非金融机构”〔67〕）设定反洗钱预防义务构建反洗钱体系，反洗钱监管当局的主要目标是督促义务机构履行反洗钱义务。FATF 在原有的两类义务机构的基础上，创设了第三类义务机构：虚拟资产服务提供商（Virtual Assets Service Provider，VASP）。从技术中立的立场出发，FATF 的监管基本原则是，适用金融机构和金融活动的标准都适用于虚拟资产服务提供商和虚拟资产活动。〔68〕

虚拟资产服务提供商承担与银行一样的反洗钱义务（“建议 10”至“建议 21”共 12 条标准），其核心的三项义务包括：客户尽职调查，〔69〕保存客户资料和交易资料，向国家指定的金融情报中心提交可疑交易报告。虚拟资产服务提供商与银行关于活动性质、活动内容、反洗钱义务的对比请参见表 3。

表 3　　虚拟资产服务提供商与银行对比

	银行（典型反洗钱义务主体）	虚拟资产服务提供商（VASP）
活动性质	价值转移	
活动内容	法定货币保管、控制	虚拟货币的保管和控制
反洗钱义务	反洗钱三项核心义务等	

3. 监管的范围包括所有虚拟资产活动

FATF 监管规则通过活动的实质来定义机构，虚拟资产服务提供商是为虚拟资产活动提供服务且作为营业（as a business conduct）的机构或个人。为便于理解，《FATF2019 虚拟货币指引》中列举了主要的“虚拟资产活动”，包括：（1）法定货币和虚拟货币之间兑换；（2）不同种类虚拟货币之间兑换；（3）虚拟货币转移；（4）保存、管理虚拟货币；（5）参与虚拟货币发行和销售，或者为其提供服务。在此之前，一些国家仅对虚拟货币和法定货币直接兑换过程进行反洗钱监管，FATF 标准将所有虚拟货币转移活动纳入了监管范围，尤其是虚拟货币之间的转移活动。

〔66〕 See FATF, Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, paras. 32, 67 (June 2019).

〔67〕 FATF 框架下的非金融机构被称为“特定的非金融行业和职业”（Designated Non-Financial Businesses or Professions），缩写为“DNFBPs”，中文官方标准译法为“特定非金融机构”，通常包括律师、会计师、房地产经纪等。

〔68〕 讨论过程中，秘书处提出的方案是：直接将虚拟资产活动纳入金融活动范畴，将虚拟资产服务提供商纳入“金融机构”的范畴，这样，原有的规则将自动适用。与会代表同意这个监管思路，但是，有代表提出这种安排在技术上过于笼统，不能解决虚拟货币的特殊问题和关切。因此，最后达成的方案是在“建议 15”中增加“释义”，具体列明现有的哪些规则适用，哪些规则按照更高的要求适用。

〔69〕 根据“建议 10”的规定，客户尽职调查（customer due diligence）比我们通常所说的“客户实名制”要求更加广泛，不仅包括核实客户身份准确性，还包括穿透识别法人客户背后的最终控制自然人或最终拥有自然人，了解客户业务的目的和性质等。

理解虚拟资产活动的关键是理解“托管钱包”，“托管钱包”是 FATF 设置规则的“假象典型”。FATF 在列举上述虚拟资产活动范围时，已经推定了上述活动中，服务提供商通过“托管钱包”获得了虚拟货币的控制权。“托管钱包”类似于银行账户，用户将虚拟货币的私钥储存在“托管钱包”中，服务商获得了私钥的控制权，用户通过指令可以要求服务商对“托管钱包”中的虚拟货币进行转移。

如果用户不通过第三方保管和使用虚拟货币，那么他使用的是“非托管钱包”，“非托管钱包”可以理解为存放现金的保险柜，是由个人自己控制的存储手段。提供“非托管钱包”服务类似于提供现金保险柜，提供的是技术服务，不属于反洗钱监管范围。

现有货币体系和虚拟货币体系下，是否通过第三方保管和使用法定货币或虚拟货币，带来的反洗钱义务范围对比，请参见表 4。

表 4　　典型反洗钱义务范围对比

	现有货币体系	虚拟货币体系	说明
自我保管和使用	使用者自己持有现金（保险箱）	使用者自己持有私钥（非托管钱包）	提供现金保存手段的机构（如保险箱制造商）不是反洗钱义务机构；类似地，仅提供个人保管和使用虚拟货币有关技术服务的机构也不是反洗钱义务机构
通过第三方保管和使用	使用者通过银行（银行账户）	使用者通过虚拟货币服务商（托管钱包）	银行是价值转移执行者，是反洗钱义务机构；类似地，虚拟货币服务商属于反洗钱义务机构

虚拟货币托管钱包与银行账户、证券账户的对比请参见表 5，将有利于理解“托管钱包”。

表 5　　虚拟货币托管钱包与银行账户、证券账户的对比

	银行账户	证券账户	虚拟货币托管钱包
保管对象	法定货币	证券	虚拟货币
保管控制方式	银行对账户中资金进行保管、控制	证券经纪商对账户中证券进行保管、控制	钱包提供商对托管钱包中资产进行保管、控制
交易方式	根据用户指令	根据用户指令	根据用户指令
政府公权力行使	监管机关可以通过银行账户对资金流向实施监控，政府可以依法指令银行冻结账户资产	监管机关可以通过证券账户对证券资产流向实施监控，政府可以依法指令证券经纪商冻结账户资产	监管机关可以通过托管钱包对资金流向实施监控，政府可以依法指令虚拟货币服务商冻结账户资产

我们常说的“虚拟货币交易平台”就是典型的虚拟资产服务提供商。〔70〕

4. 设置行业准入门槛，防止游离监管之外

FATF 对行业准入设置了门槛要求，一国要根据情况采取注册制或审批制，虚拟资产服务提

〔70〕 另外，还出现了物理形态的电子终端（physical electronic terminals），如比特币自动取款机（bitcoin ATMs）等，对于通过这些物理终端机器购买、转移虚拟货币的活动，也适用 FATF 关于虚拟货币监管的规则。平台如果仅发布价格信息，不从事任何交易活动，则不属于受监管活动。关于监管范围，可参见前引〔66〕，FATF 文，第 33－54 段。

供商必须获得注册或许可后方可提供服务。具体而言，成立地、运营地、客户所在地都可以要求服务商向其申请注册或许可。服务商是非自然人时，其成立地必须要求其申请注册或许可；服务商是自然人时，其营业地须要求其申请注册或许可。对于服务商注册地提出强制性要求的动议，由中国等发起，针对的是防止离岸服务（在一个辖区注册，但为另一个辖区提供服务）游离于监管之外，防止形成“监管天堂”或“监管洼地”。〔71〕

5. 强化国际合作，防止监管套利

“建议 37”至“建议 40”分别规定了司法协助、跨境资产冻结和没收、引渡、其他形式的国际合作。其中，“建议 37”“建议 38”“建议 39”规定的是刑事司法协助，“建议 40”是正式的刑事司法协助以外的其他合作，主要是双边反洗钱监管合作和双边反洗钱金融情报交换。FATF 为了全面加强在虚拟货币领域的国际合作，将相关要求扩大化到所有监管领域（不限于反洗钱领域）。其规则指出，对虚拟货币监管机关不同，对虚拟货币性质、称谓不同，都不应影响各国进行监管信息交换，〔72〕从而防止监管套利。

6. 监管标准更为严格的适用

FATF 认可虚拟资产更高的内在风险，因此，按照风险为本的要求对某些标准适用更为严格，主要在两个方面：

一是 FATF 标准要求对于金融机构必须由政府机构实施监管，对于非金融机构可以由自律组织进行监管。鉴于虚拟资产服务的特殊风险状况，FATF 要求只能由政府机构对其实施监管。

二是鉴于虚拟货币具有跨国性特点和较高的洗钱内在风险，将虚拟资产的价值转移统一推定为跨国交易，并实施比现有跨国交易更加严格的反洗钱要求。根据 FATF 标准，对于偶发性（occasional）交易，当交易额（无论国内或跨国）达到 1.5 万美元或欧元（孰低）时金融机构必须实施客户尽职调查，当跨国交易达到 1000 美元或欧元（孰低）时金融机构必须核实客户身份的准确性（客户尽职调查的一个方面）。新的标准进一步要求，涉及虚拟货币的偶发性交易，只要达到 1000 美元或欧元（孰低）就必须实施客户尽职调查。

（三）反洗钱国际标准对行业生态的革命性影响

只有个人之间通过“非托管钱包”（完全是个人之间的点对点交易，不借助任何外部服务）的交易在监管之外，任何交易通过第三方服务进行，都将纳入监管体系之内。这符合基本的监管逻辑和行业技术特点。“非托管钱包”对使用者有很高的技术要求，如果缺乏相应技术，不仅很难正确交易，而且容易丢失虚拟货币，因此，其仅限于少数人使用。监管主要关注的是营业性活动，而不是个人之间的行为。个人不借助任何外部服务的点对点交易很难被发现，类似于大众的现金交易，对于这些行为的监管不符合监管的成本收益原则。

〔71〕 中国在建议中提出，成立地有首要的（primary）监管义务。秘书处在吸收各个成员意见基础上，将表述改为“at a minimum”（作为最低要求）。

〔72〕 FATF“建议 15 释义”第 8 段第 2 句话规定：“尤其是，虚拟资产服务商的监管机关应当立即和建设性地与外国对应机关交换信息，不应受制于双方监管机关的性质、地位以及对服务商的不同称谓和地位。”

FATF 规则设置了基本的准入门槛，防止了行业“裸奔”状态。而且，为了防止跨辖区的监管套利，FATF 要求成立地必须实施行业准入，而且强化了国际合作要求。

根据 FATF 规则，服务商要对所有客户进行实名制登记，对交易背景和目的进行审查，将可疑交易信息报告给政府，反洗钱监控全面植入虚拟货币交易服务，国家“追踪资金”的范围延伸到虚拟世界。

监管对于虚拟货币在投资者适当性方面的担忧，很大一部分来源于虚拟货币缺乏可追踪性。随着反洗钱基础设施的建立，各国证券当局可能会允许虚拟货币在一定条件下成为公众可投资的金融产品。

五、监管的展望：从“外部活动”到“内部治理”

（一）“外部活动”与“内部治理”：反洗钱规则的局限性

我们可以将一个虚拟货币自我运转的社群类比于一个上市公司，“链上治理”指的是这个社群的内部的治理，包括代码修改的规则、增加虚拟货币总量规则、“分叉”（部分矿机用脚投票，在原有链的基础上形成新的链）等，这些内部的投票活动很大程度上和公司内部治理具有相似性。“链上交易”活动相当于上市公司的股票在公司之外的发行和流通。上市公司与虚拟货币社群有关活动的对比，请参见表 6。

表 6　　上市公司和虚拟货币社群有关活动的对比

	上市公司	虚拟货币社群	现有监管规则
内部治理（链上治理）	章程修改	代码规则修改	实践空白
	股票增发	增加虚拟货币总量	实践空白
	公司分立	“分叉”	实践空白
外部活动（链上交易）	股票发行	ICO	仅有反面实践
	交易规则（防止价格操纵等）	交易规则（防止价格操纵等）	仅有反面实践
	作为价值转移手段	作为价值转移手段	完整监管规则

我们现有的反洗钱监管规则仅限于作为价值转移手段时的外部活动。主要国家监管当局并未正面审批或注册通过任何一种虚拟货币作为公开发行的金融产品，因此，对虚拟货币内部治理的实践完全空白。目前已有的实践，仅有对操纵市场和未经审批或注册发行虚拟货币两种行为的打击。

比特币创造了“代码即法律”的社群治理模式。菲利皮（Filippi）和洛夫拉克（Loveluck）以比特币治理为例将区块链治理分为两个层次，“以基础设施进行治理”和“对基础设施进行治

理”，两者是相互作用的，最终的体现在于“对基础设施进行治理”，也即对代码的修改。〔73〕对代码规则的修改类似于上市公司章程的修改，是治理中最高的权力/权利，是其他权力/权利的基础。

对于内部治理，只有当虚拟货币通过监管当局审批或注册时，才可能将现有的证券监管规则运用到区块链治理中去。非中心化的治理秩序在多大程度上能够实现良好的治理，需要在现有法律框架下继续尝试。

（二）“内部治理”：未来的根本性挑战

对于监管者而言，链上的内部治理将是全新的议题，至少面临以下三个根本性挑战：

首先，从应然性的角度，“什么是良好的治理”？公司治理的标准在多大程度上适用于自治社群？监管在多大程度上允许不同治理模式的探索？区块链自治社群的时间远短于公司存在的时间，已有的经验和案例相当少，这注定是一个反复探索的过程。

其次，从责任承担的角度，自治社群本身不存在有形实体和组织架构，监管者如何找到监管对象和义务主体？公有链的参与者是可以匿名的（上述反洗钱规则并不要求区块链参与者实名制，只是参与者通过第三方对外发生交易时才需要在服务商进行实名制登记），而且自治社群并不存在有形的组织架构，究竟谁来履行监管规定的义务？如何识别义务履行者？“道”（Dao）平台尝试了“非中心化自治组织”的理想，尽管其发行“道币”行为被美国 SEC 认定为未经注册发行证券行为而叫停，但是引发了如何界定区块链自治社群中新型组织的法律性质和责任承担这两个根本性问题。〔74〕

最后，从法律执行的角度，区块链社群是依据代码的治理，监管者如何强制自治社群修改代码？法律应当赋予监管者“超级代码控制者”的权力吗？“超级代码控制者”修改代码后，社群参与者会选择用脚投票吗？

（三）展望：相信试错的力量

从系统自发维持的角度，比特币的社群自治实验无疑是成功的，在一个没有暴力维持运营、没有第三方权威的社群中，比特币、以太币社群自发形成全球性的、千亿美元规模的金融体系。但是，从普通参与者的角度，尽管比特币的理想是建立一种非中心化秩序，然而比特币，及其后来的以太币、“非中心化自治组织”尝试的“道”在治理结构上都是一种中心化结构，虚拟货币社群还存在严重的决策权力集中、普通用户难以发声的治理缺陷。

中心化和非中心化治理的平衡点，表面上看是公司治理、社群治理的问题，但背后是人类政

---

〔73〕 See Primavera De Filippi，Benjamin Loveluck，The Invisible Politics of Bitcoin：Governance Crisis of a Decentralized Infrastructure，5（4）*Internet Pol'y Rev.*，（2016），available at https://policyreview.info/articles/analysis/invisible-politics-bitcoin-governance-crisis-decentralised-infrastructure，last visited on Jun. 10，2020.

〔74〕 如果从既有法律中推导，这种组织的法律性质应当是普通合伙。法人、有限合伙的设立在绝大部分国家以登记为前提，“道”没有登记，因此不能构成法律上的法人、有限合伙；普通合伙不以登记为前提，可以基于共同的合同行为而产生，所有参与者要承担无限连带责任。至少在美国法框架下，认定该组织为合伙，并不影响其 ICO 行为构成证券发行。［See Laila Metjahic，Deconstructing the DAO：The Need for Legal Recognition and the Application of Securities Laws to Decentralized Organizations，39 *Cardozo L. Rev*，1533，1533－1568（2017）.］国内学者普遍认为，普通参与者不应当承担无限连带责任，因此比较适合将其认定为“有限合伙”。（参见汪青松：《区块链系统内部关系的性质界定与归责路径》，载《法学》2019 年第 5 期。）

治哲学的永恒难点，自古希腊以来西方政治哲学对此问题一直没有固定不变的最优解。从动态的角度看，也许十年时间还太短，我们不能以一时的治理困局就否定竞争和进化的力量，毕竟虚拟货币的用户掌握了用脚投票的权利，私人竞争的长期存在，给反复试错提供了可能性。

对虚拟货币的反洗钱监管，可以提高虚拟市场预防和抵御欺诈、操纵的能力，为虚拟货币公开发行提供良好的市场前提。如果虚拟货币发行可以得到国家的认可，那么国家监管的规则也将会随之强行植入虚拟货币社群，现有的证券投资者保护规则在多大程度上适用于区块链社群以及监管的边界、容忍度、手段都将是全新的挑战。我们相信，国家监管所代表的现实世界的法律和虚拟世界的技术规则在动态的博弈中可能会最终产生意想不到的成功治理模式。

Abstract：Ten years after the birth of virtual currencies（VCs），they still have not introduced significant impact over the fiat currency systems，then the major monetary authorities do not prohibit individuals from holding or using VCs. At the same time，the major securities authorities also do not register or license to the public any virtual currencies or financial products based on VCs，because the investment suitability of VCs is still unclear. However，the authorities must address the serious speculations，frauds and money laundering in a substantial way. Under the promoting and leading of the Financial Action Task Force（FATF），the global society finally reached consensus on anti-money laundering（AML）regulation over VCs in 2019. The new regulatory framework will fundamentally change the autonomy of VCs communities in the world. While the AML rules only cover the regulation over the activities out of blockchain to prevent ML，and the governance of blockchain will be the core issue and biggest challenge for further regulation in the next stage.

Key Words：virtual currencies，anti-money laundering regulation，governance of blockchain

（责任编辑：缪因知　赵建蕊）

财经法学 No. 1，2020
pp. 13 - 24

论政府数据开放与政府信息公开的关系

王万华*

内容提要：政府数据开放与政府信息公开关系的基本定位为“承继但不取代”。兴起于20世纪60年代的政府信息公开确立了公民的知情权，建构了开放政府的理念和制度，为21世纪大数据时代来临兴起的政府数据开放奠定了基础。政府数据开放在承继政府信息公开的基础上，回应开放数据的基本要求，拓展了开放政府的内涵，形成独立于政府信息公开的制度体系。政府数据开放与政府信息公开的主要差异体现为：制度基础及立法进路不同；政府角色及政府与公众关系结构不同。我国应当进行政府数据开放专门立法，主要设想包括：尽快制定《开放政府数据法》，以提升数字时代政府治理能力为立法目标，重视内部体制机制完善，建构多元机制解决开放范围难题。

关键词：政府数据开放　政府信息公开　开放政府　开放政府数据法

一、问题的提出

政府数据开放与政府信息公开同为开放政府的组成部分，形式上二者均体现为政府将信息或数据公开给社会知悉、利用，因此，探讨政府数据开放立法绕不开已有的政府信息公开立法。在《政府信息公开条例》修订过程中，学者提出通过修改条例，或将政府数据开放机制纳入其中以打造政务公开的3.0版本，〔1〕或为未来制定专门政府数据开放立法预留制度空间。〔2〕但是，2019年4月3日发布的新《政府信息公开条例》仅完善了政府信息公开制度本身，并未涉及政府数据

* 王万华，中国政法大学诉讼法学研究院教授。

〔1〕 如周汉华教授提出，“在公开内容方面，除政府信息公开外，升级版政务公开制度要尝试推进诸如决策会议公开、政府数据开放、电子参与、执法过程公开、政府绩效公开、专家咨询论证意见与过程公开等，以丰富公开的内容与形式”。周汉华：《打造升级版政务公开制度——论〈政府信息公开条例〉修改的基本定位》，载《行政法学研究》2016年第3期，第11页。

〔2〕 如肖卫兵教授提出，应当充分利用《政府信息公开条例》修改的有利契机，为政府数据开放预留或者提供涉及政府数据定义、开放方式和开放例外等方面的基本制度接口和制度支撑。参见肖卫兵：《论我国政府数据开放的立法模式》，载《当代法学》2017年第3期。

开放制度。《政府信息公开条例》刚刚修订完成，近期内不可能再次启动修订程序，那么，我国是否需要进行专门的政府数据开放立法？还是借助政府信息公开制度框架，辅之以政策对政府数据开放予以推进？如果制定专门立法，又如何定位其内容，如何与《政府信息公开条例》相衔接？这一系列问题的探讨，均离不开对政府数据开放与政府信息公开的关系的认识和讨论。

对政府数据开放与政府信息公开的关系，学界目前尚存在不同认识，一种观点认为应将政府数据开放从政府信息公开中剥离出来；〔3〕另一种观点认为数据开放无论从概念、法律、价值和管理上都是信息公开的一部分，主张在制度上建构统一的政府数据资源管理体系。〔4〕目前关于政府数据开放与政府信息公开关系的研究主要从厘清“信息”与“数据”的关系的角度切入。〔5〕然而，一方面，信息与数据的区分只具有相对性，且在有关开放政府的政策和立法中，二者经常被混用；另一方面，在立法工作和法律实施过程中，信息与数据作为技术概念存在的认识分歧所产生的影响并不大。对政府数据开放与政府信息公开关系定位影响更大的是回应大数据时代特征的“开放数据”中“开放”一词所必须满足的特定要求，有必要进一步拓宽对政府数据开放与政府信息公开关系影响因素及二者关系定位的研究。

海量政府数据开放过程中价值与风险并存。立法是政府数据有序开放给社会再利用的制度保障，也为有效防范开放所可能产生的个体权利损害及社会风险所必需。开放政府数据无论是在域外，还是在国内，兴起的时间都不长，政府数据开放立法均面临诸多难题需要深入研究。当前，学界已对政府数据开放立法模式、立法框架、立法内容等涉及立法的一系列问题展开了初步研究，〔6〕这些问题尚有进一步深入研究的必要。2019 年 8 月 29 日，历经七年努力之后，上海市正式出台我国首部关于政府数据开放的专门立法《上海市公共数据开放暂行办法》，开启了政府数据开放专门立法的地方尝试。可以预见，随着国家大数据战略的实施，政府数据开放实践的持续推进，将会有更多地方加入专门立法的探索。《上海市公共数据开放暂行办法》的出台，为进一步探讨政府数据开放专门立法提供了分析样本。本文拟对政府数据开放与政府信息公开关系进行研究，并结合《上海市公共数据开放暂行办法》，就有关我国政府数据开放立法相关问题提出初步设想。

二、二者关系的基本定位为“承继但不取代”

“政府数据开放”与“政府信息公开”这一组概念形式上具有对应性，内容上具有相关性，

〔3〕 参见季统凯、刘甜甜、伍小强：《政府数据开放：概念辨析、价值与现状分析》，载《北京工业大学学报》2017 年第 3 期。

〔4〕 参见黄璜、赵倩、张锐昕：《论政府数据开放与信息公开——对现有观点的反思与重构》，载《中国行政管理》2016 年第 11 期。

〔5〕 这两个概念的关系在不同学科中都进行过广泛讨论，形成了“数据大于信息说”“信息大于数据说”“数据与信息等同说”“数据与信息相对说”等不同认识。参见叶继元、陈铭、谢欢、华薇娜：《数据与信息之间逻辑关系的探讨——兼及 DIKW 概念链模式》，载《中国图书馆学报》2017 年第 3 期。纪海龙教授将数据按照物理层、符号层和内容层三个层面进行划分，相应地将大数据时代背景的“数据”分为存储介质层、数据文件层和信息内容层，能够比较好地解释“数据”和“信息”在开放数据立法和政策中被混用的现象。参见纪海龙：《数据的私法定位与保护》，载《法学研究》2018 年第 6 期。

〔6〕 参见前引〔2〕，肖卫兵文；何渊：《政府数据开放的整体法律框架》，载《行政法学研究》2017 年第 6 期；宋华琳：《中国政府数据开放法制的发展与建构》，载《行政法学研究》2018 年第 2 期。

这使得“政府数据开放”易被认为是“政府信息公开”在大数据时代的升级版。然而，二者之间并非简单的升级替代关系，政府数据开放的出现并没有取代政府信息公开，而是与政府信息公开一起完善和丰富了开放政府的结构与内容，构成二元并立的开放机制体系。如美国1966年出台《信息自由法》，2009年1月，奥巴马总统签署《透明与开放政府备忘录》，2019年1月14日，特朗普总统签署《开放政府数据法》。韩国于1996年制定了《公共机构信息披露法》，2013年通过了《促进公共数据的提供和使用法》，2016年通过了《开放公共数据指令和社会使用原则》。

我国于2007年4月5日发布《政府信息公开条例》，地方层面由上海于2019年出台了首部政府数据开放专门立法《上海市公共数据开放暂行办法》。政府数据开放为“开放数据”与“开放政府”相交集部分，“开放政府”与“开放数据”均对政府数据开放制度建构产生影响。但是，在“开放政府”与“开放数据”这两个影响因素中，“开放数据”对政府数据开放制度建构的影响更大，是“开放数据”对“开放”的一系列要求形塑了政府数据开放制度的基本面向。这使得政府数据开放与作为早期开放政府同义语的政府信息公开之间虽存在承继关系，但是，并没有作为其升级版取代后者，而是发展出独立于政府信息公开的制度体系，并与之共同构成了大数据时代的开放政府制度体系。

（一）政府数据开放以政府信息公开为基础得以落地

1766年的瑞典《出版自由法》尽管被认为是第一部关于政府信息公开的立法，但是，这部法律与政府信息公开的关联有限。现代意义的政府信息公开始于20世纪60年代，并在之后的数十年间于世界范围形成立法浪潮。正是有了政府信息公开立法对公民获取政府信息的权利的确立和制度化，当大数据时代来临时，公民获取政府的数据才成为可能。在此意义上，政府信息公开构成政府数据开放的基础。

2018年12月31日，美国国会通过了《开放政府数据法》，特朗普总统于2019年1月14日签署该法，该部法律名称的完整表述为Open，Public，Electronic and Necessary（OPEN）Government Data Act。根据该法规定，也可将这部法律名称表述为OPEN Government Data Act，一般将之翻译为《开放政府数据法》。该法律名称中同时出现了Open和OPEN，前一个Open为“公开、透明”之意，后一个缩写词OPEN为“开放”之意。“开放”中包含了“公开、透明”的内涵。没有公开，就失去开放的基础，但是，开放又不仅限于公开、透明。这部法律的名称很好阐释了政府数据开放如何承继和发展了政府信息公开制度所建立的开放政府理念。开放政府的概念由Wallace Parks于1957年提出，〔7〕但是没有对开放政府内涵做出明确解释，而是主张开放政府与信息公开等同，与民主问责直接相关，是良好行政的题中之意。1966年，美国制定了《信息自由法》，根据该法规定，任何人都有权申请行政部门公开政府记录，从而确立了普遍性的知情权。个人不需要具备特定利益，只要申请公开的信息不属于豁免公开的范围，即可申请获得政府信息。《信息自由法》所建构的政府信息公开制度由此成为开放政府的基石，“在接下来的几

〔7〕 See Wallace Parks，The Open Government Principle：Applying the Right to Know Under the Constitution，26 *GEO. WASH. L. REV.*，1，4（1957）.

十年里，开放政府主要作为公众获取此前未公开的政府信息的同义词”〔8〕。

20 世纪 60 年代至 21 世纪初，政府信息公开立法在世界范围获得长足发展，开放政府理念和制度在全球范围得以确立，为大数据时代来临之后公众获取政府数据奠定了基础。当开放政府数据成为大数据时代的现实需求时，受益于政府信息公开所建构的开放政府理念和对知情权的确立，开放政府数据没有遭遇理念上的障碍，被视为数字时代政府治理的应有之义。

基于政府数据开放面临的诸多风险，各国政府在政府数据开放的早期，基本采用了在政府信息公开制度框架内以政策方式逐步推进的路径。如美国奥巴马总统上任伊始于 2009 年 1 月发布的《透明与开放政府备忘录》中，要求由政府首席技术官牵头，与管理与预算办公室一起协调其他部门根据《信息自由法》制定《开放政府指令》，之后，美国颁布了一系列行政文件。〔9〕英国 2012 年新修订的《信息自由法》第 102 条规定，当申请者向政府部门申请的信息是该部门拥有的数据集时，只要合理可行，部门应当提供这些信息的电子版本。同年，英国政府发布《开放数据白皮书——释放数据潜能》。在我国，政府数据开放也主要通过中央、地方出台政策的方式予以推进。〔10〕实际操作中，有的地方政府主要依托政府信息公开平台和制度开展这项工作。〔11〕

（二）政府数据开放拓展了开放政府的内涵

开放政府早期等同于政府信息公开，政府数据开放的出现拓展了开放政府的内涵。开放政府不再仅限于信息或数据的公开，而是作为数字时代的一种治理方式出现。进入 21 世纪之后，伴随信息与通信技术的极大发展，开放政府获得两方面的发展：一方面，传统以文本文件为核心的信息公开实现公开电子化，信息公开申请和处理均可以通过在线方式办理。美国《透明与开放政府备忘录》中要求利用新技术将联邦政府掌握的信息在线提供给公众利用。另一方面，信息技术的发展与开放政府相结合催生了政府数据开放机制。Silvana Fumega 在对政府信息公开与政府数据开放两种制度进行对比时，将 Freedom of Information（FOI），Open Government Data（OGD），Information and Communication Technology（ICT）列为理解二者关系的三个核心概念，并认为这三个概念之间的关系体现为：信息与通信技术的发展为开放政府数据提供技术条

〔8〕 Harlan Yu，David G. Robinson，The New Ambiguity of Open Government，59 *UCLA L. Rev. Discourse*，178，186（2011）.

〔9〕 行政文件主要包括：2009 年《开放政府指令》，2012 年《数字政府：构建更好服务美国人民的 21 世纪平台》，2013 年《开放数据政策——管理信息资产备忘录》等。

〔10〕 如 2015 年 8 月，国务院印发的《促进大数据发展行动纲要》中提出“要稳步推进公共资源开放，加快建设国家政府数据统一开放平台”。2017 年 2 月，中央全面深化改革领导小组第三十二次会议审议通过《关于推进公共信息资源开放的若干意见》，要求着力推进重点领域公共信息资源开放，释放经济价值和社会效应。2018 年 4 月，《国务院办公厅关于印发 2018 年政务公开工作要点的通知》中提出依托政府网站集中统一开放政府数据。2018 年，中央网信办、发展改革委、工业和信息化部联合印发《公共信息资源开放试点工作方案》，确定在北京、上海、浙江、福建、贵州开展公共信息资源开放试点，要求试点地区制定公共信息资源开放管理办法。2019 年 8 月，《国务院办公厅关于促进平台经济规范健康发展的指导意见》中提出畅通政企数据双向流通机制，制定发布政府数据开放清单，探索建立数据资源确权、流通、交易、应用开发规则和流程，加强数据隐私保护和安全管理。

〔11〕 参见晴青、赵荣：《北京市政府数据开放现状研究》，载《情报杂志》2016 年第 4 期；郑磊：《开放不等于公开、共享和交易：政府数据开放与相近概念的界定与辨析》，载《南京社会科学》2018 年第 9 期。

件，信息公开制度使得开放政府数据成为现实。〔12〕

大数据时代，政府收集、储存、使用、公开信息的方式均出现重大变化，海量数据出现在政府运作系统中，这些数据与社会、经济发展密切相关，蕴含无限商业机会和创新潜能，获得政府所掌握的原始数字数据成为社会的强烈现实需求。在此背景下，各国政府在政府信息公开基础上，尝试向社会开放政府数据。

在与开放数据相交集的过程中，开放政府的内涵也得以扩展。大数据的出现除对政府与数据相关的活动产生影响外，还对政府的政策制定方式、决定作出方式、公共服务的提供等均产生深刻影响。政府在数字时代的社会治理不仅仅是获得技术上的提升，更重要的是改变了治理结构。正如英国学者维克托·迈尔-舍恩伯格在《大数据时代》一书中提到的“大数据是人们获得新的认知，创造新的价值的源泉；大数据还是改变市场、组织机构，以及政府与公民关系的方法”〔13〕。大数据在深刻改变商业模式的同时，也在深刻改变政府管理模式和重塑政府与公民之间的关系。

政府开放数据的出现，在推动政府透明度建设的同时，还促进了政府与社会之间的合作治理。美国预算与管理办公室发布的《开放政府指令》（Open Government Directive）中详细解释了“开放政府”的含义：透明、参与和合作三项原则构成开放政府的基石。透明指通过向公众提供有关政府在做什么的信息来促进问责制；参与让公众贡献思想和技能帮助政府决策；合作通过鼓励联邦政府、各级政府之间以及政府和私人机构之间合作来提高政府效能。参与和合作与透明一起构成开放政府的内容，丰富和发展了大数据时代开放政府的内容。我国学者也将数据开放作为大数据时代开放政府的重要内容，从一种全新治理理念视角理解开放政府，认为“开放政府是一种治理理念，它旨在通过信息公开、数据开放、政府与公众之间的互动和对话，以及政府与企业和非营利性社会组织之间的合作，提升政府的治理能力。当然，其最终的目标是通过提供完善的公共产品和服务实现公共价值和社会价值”〔14〕。

（三）政府数据开放形成了不同于政府信息公开的制度体系

尽管政府信息公开制度在一开始为政府数据开放成为现实提供了制度框架，但是，由于大数据对“开放数据”提出的特定要求很难在政府信息公开制度框架内完全得到实现，政府数据开放在发展进程中逐渐形成不同于政府信息公开的制度体系。如美国自 2009 年启动开放政府数据以来，发布了大量行政文件，引导联邦政府向社会开放数据，最终于 2018 年底由国会通过了专门的《开放政府数据法》。

1. “开放数据”的基本要求

大数据的价值在于利用及再利用。围绕数据利用，“开放数据”形成一系列特定要求。2007

〔12〕 See Silvana Fumega, Understanding Two Mechanisms for Acecessing Government Information and Data Around the World, November 5, 2019, available at https://webfoundation.org/docs/2015/08/UnderstandingTwoMechanisms forAccessing GovernmentInformationandData.pdf, last visited on Nov. 10, 2019.

〔13〕〔英〕维克托·迈尔-舍恩伯格、肯尼思·库克耶：《大数据时代》，盛杨燕、周涛译，浙江人民出版社 2013 年版，第 9 页。

〔14〕 王本刚、马海群：《开放政府理论分析框架：概念、政策与治理》，载《情报资料工作》2015 年第 6 期，第 36 页。

年，30 位开放数据倡导者在美国加州首次对开放政府数据提出了八项基本原则，数据只有符合这八项要求，才能被认为是“开放的”：完整性、原始性、及时性、可获得、可机读、非歧视性、非专属、免授权。〔15〕 2012 年，英国政府发布的《开放数据白皮书——释放数据潜能》中对开放数据提出三项标准：一是可获取，即不超过复制成本，不限制用户身份或意图的获取；二是数字化的、机器可读的，即采用与其他数据可互操作的数字的、机器可读的格式；三是无限制再利用和再分发，即在许可条件下不受限制地使用或重新分发。

美国 2013 年《开放政策——管理信息资产备忘录》附件中将开放数据界定为：开放数据这一概念是指以能够被终端用户完全发现和使用的方式公开的可用数据。一般而言，开放数据应符合以下原则：公开、可获取、描述性、可再利用、完整、及时、开放后管理。2015 年《开放数据宪章》将开放数据界定为具备必要的技术和法律特性，从而能被任何人在任何时间和地点进行自由利用、再利用和分发的电子数据。开放数据的基本要求涉及数据的质量、开放范围、用户获得数据方式等，这已为各国政策和立法所吸收和体现。

2.“开放数据”的特定要求影响了政府数据开放制度基本面向

大数据对政府数据活动乃至治理活动产生的重大影响是政府数据开放得以兴起的直接现实因素，后续的制度建构必然需要回应大数据对数据“开放”提出的要求。无论域外学者，〔16〕 还是国内学者，〔17〕 均认为政府数据开放制度以新技术驱动为基础建构，侧重数据的利用及再利用，旨在挖掘数据的潜在价值，为政府和社会有效解决各种问题提供新的路径和资源。〔18〕 政府信息公开为政府数据开放提供了基础，但是，原始、完整、及时、可机读、可再利用等一系列围绕数据利用而形成的要求，均难以在以个人知情权保障为基础建构的政府信息公开制度中完全得以实现。

信息公开制度以实现民主和问责为目标，强调的是通过个人对政府信息的知悉（Right to Know），推动政府透明度建设，更好监督政府，对政府进行问责。在《信息自由法》所规定的信息公开机制中，公开的信息往往是经过行政机关加工处理过的文本文件、统计报告等非原始信息，公开方式则以公民提出申请为主要方式，具有被动公开、碎片化等特征，难以满足政府数据开放面临的一系列要求。因此，尽管政府数据开放在初始阶段主要借助信息自由立法所建构的开放政府理念和制度框架得以进入实际操作层面，但在推进过程中，回应“开放”特定要求的制度建构需求使其发展形成了不同于政府信息公开的制度体系，并与政府信息公开一起，在大数据时代共同完善和丰富了开放政府的结构与内容。

---

〔15〕 国际组织对开放数据或开放政府数据也作出界定。如开放知识基金会认为，“开放数据是一类可以被任何人免费使用、再利用、再分发的数据——在其限制上，顶多是要求署名和使用类似的协议再分发”；世界银行提出“开放数据指的是非专有的、机器可读的数据，可能来自任何地方，任何人都不能施加法律或技术的限制，可以被任何人自由使用、重复使用、操作和传播”。

〔16〕 See Beth Simone Noveck, Rights-Based and Tech-Driven: Open Data, Freedom of Information, and the Future of Government Transparency, 19 *Yale Human Rights and Development Law Journal*, 1 (2017); Beth Simone Noveck, Is Open Data the Death of FOIA, Yale Law Journal Forum 126 (2016—2017): 273 - 286; Katleen Janssen, Open Government Data: Right to Information 2.0 or its Rollback Version? ICRI Working Paper 8/2012.

〔17〕 参见前引〔11〕，郑磊文。

〔18〕 即使主张在制度上建构统一的政府数据资源管理体系的学者也赞成这一结论。参见前引〔4〕，黄璜、赵倩、张锐昕文。

三、政府数据开放与政府信息公开的差异

在明确政府数据开放与政府信息公开关系的基本定位基础上，为探讨政府数据开放立法的基本定位，有必要进一步比较政府数据开放与政府信息公开两种开放机制的具体差异。作为两种独立的开放机制，政府信息公开与政府数据开放的差异体现在多个方面，中外学者均对此展开了比较研究。〔19〕在二者诸多差异中，尚有一些问题未得到充分研究，如二者各自的立法进路和政府在二种机制中的角色等问题，这些问题对政府数据立法定位均有直接影响。此外，目前学界关于二者差异的研究，主要以域外政府信息公开立法为对象展开，而我国《政府信息公开条例》与域外相比较，有其独特之处，这使得二者的差异在我国呈现出一些不同于域外的特点。

（一）制度基础及立法进路不同

美国《信息自由法》规定立法目的为“确立和保护公众获得政府信息的权利”，《开放政府数据法》规定立法目的为“扩展政府数据的使用和管理，促进公开透明，促进政府有效治理，促进创新”。美国学者 Beth Simone Noveck 将政府信息公开制度和政府数据开放制度的特征分别提炼为“基于权利的信息公开制度”和“基于技术驱动的政府数据开放制度”。〔20〕这一区分揭示了政府信息公开与政府数据开放的最大差别在于前者以知情权为逻辑起点架构制度，后者并不以个人权利保障为其制度建构的基础。制度基础决定了制度基本方向，作为知情权的实现和保障机制，政府信息公开的制度架构围绕公众知情权（信息自由）和政府公开义务这一组法律关系展开，公开范围以公开为原则，公开方式以依申请公开为主要方式，个人知情权受到损害可以通过诉讼方式获得救济。尽管信息自由立法通过赋予个人无差别的知情权的方式，赋予了该制度监督行政机关和促进行政民主问责的公共性质功能，但是，制度的基础和体系仍建立在个人主观请求权的确立、实现、救济之上。

基于信息技术发展兴起的政府数据开放没有沿着公民知情权由信息向数据自然延伸的进路展开制度建构，而是离开了权利保障机制这一传统行政法治建构轨道，走向寻求更优数字治理效果的功能主义制度建构思路。有学者分析美国联邦和部分州政府发布的政府数据开放政策文本之后，指出“美国开放政府数据的价值观是实现并创造公共价值”，“就是要通过政府向公众开放政府数据，使公众能免费获取政府数据，从而实现和创造公共价值”〔21〕。政府数据开放通常被视为

〔19〕 如美国学者 Beth Simone Noveck 认为二者的差异体现在三个方面：其一为公开的时间不同。根据《信息自由法》公开信息属于信息的事后公开，政府数据开放是一种事前公开。其二为公开的信息类型不同。根据《信息自由法》所公开的信息类型比较窄，主要集中在与行政问责相关的信息；政府数据开放所公开的信息类型要宽泛很多。其三为受众不同。《信息自由法》最主要的利用者是各类公司，政府数据开放的受众则更为宽泛，所有的主体都可以再利用政府开放的数据。参见前引〔16〕，Beth Simone Noveck 文，第 1 页。郑磊教授认为二者的区别体现在三个方面：其一为内容上，政府信息公开的对象主要是文本形式的文件或经过归总分析后的统计报告，政府数据开放将开放层面推进到数据层。其二为目的上，政府信息公开的首要目标是保障公众的知情权，政府数据开放强调赋予社会利用政府数据的权利。政府信息公开是政府的一种责任，开放数据本质上是一项公共服务。其三为方式上，政府信息公开的中心在于政府，政府数据开放则要同时关注政府和利用者两方。参见前引〔11〕，郑磊文。

〔20〕 参见前引〔16〕，Beth Simone Noveck 文，第 1 页。

〔21〕 赵润娣：《美国开放政府数据范围研究》，载《中国行政管理》2018 年第 3 期，第 33－34 页。

政府向社会提供的公共服务，而非对公众获得数据权利的确立和保障，如郑磊认为，“政府数据开放强调赋予社会利用政府数据的权利，更侧重于其经济与社会价值，开放数据本质上是政府提供的一项公共服务”〔22〕。《上海市公共数据开放暂行办法》第 3 条第 2 款体现了这一观点，明确将公共数据开放的性质定性为公共服务。〔23〕美国《开放政府数据法》第 2 条（a）（1）中指出：联邦政府的数据为价值巨大的国家资源，将政府数据开放给一般公众、科研、商业、新闻媒体等，可以提高政府治理效率，创造商业机会，促进科学研究，更重要的是能够使民主更为强大。

从这些立法中我们可以看到，政府数据开放立法进路带有很强的功能主义色彩，立法的目的是促进政府数据价值最大限度发挥，而非确立个人权利，显现出不同于传统行政法治的规范思路。美国《开放政府数据法》在开篇即指出“联邦政府数据为价值巨大的国家资源”，这一定位构成了建构制度的基础和前提，具有很强的大数据时代烙印。政府数据开放是为了最大限度挖掘政府数据经济、社会价值而作出的法律制度安排，具有明显的客观法律制度属性。

以功能主义而非传统行政法治之下的控权理念建构政府数据开放制度，既回应了大数据的时代特色，也能够很好解决立法面临的诸多难题。海量数据开放过程中需要解决个人信息、商业秘密、国家安全等法益保护问题，而传统政府信息公开框架下对这些法益的保障机制难以适应大数据时代面临的新问题。如个人信息保护并非大数据时代产生的新问题，但是，大数据时代的来临给个人信息保护提出前所未有的巨大挑战，匿名化、模糊化、知情同意规则等传统隐私权保护机制在大数据环境下均失去作用。因此，放弃传统的权利保护机制建构思路，根据政府数据管理和开放的实际情况，在坚持开放数据基本要求的前提下，采用更为灵活的制度安排，通过多元机制，并在立法之外辅以政策，分类别、有重点推进政府数据开放进程，有利于平衡数据开放的价值和潜在的风险，防止因其他法益保护不足造成整个制度无法落地的情况。

在我国《政府信息公开条例》框架之下，政府信息公开与政府数据开放之间的差异并不如此明晰。《政府信息公开条例》虽没有明确规定知情权这一权利类型，也没有以明示方式规定公开原则，但是，原《政府信息公开条例》的立法目的中就包含了域外立法所没有的“充分发挥政府信息对人民群众生产、生活和经济社会活动的服务作用”，这一规定在新修订的条例中得到保留。〔24〕该项立法目的与政府数据开放的公共服务性质定位是一致的。此外，在公开方式上，我国政府信息公开方式以主动公开为主，修订后的条例更是进一步加大了政府主动公开的信息范围和公开力度。这些特点使得我国政府信息公开制度与政府数据开放制度之间的差异并不如域外那样突出，为政府数据开放的推行打下了很好的基础。

（二）政府角色及政府与公众关系结构不同

无论政府信息公开还是政府数据开放，形式上均体现为政府将其保管的信息或数据向公众开放，但是，两种机制中，政府的角色及政府与公众关系结构完全不同。在政府信息公开中，政府

〔22〕 前引〔11〕，郑磊文，第 87 页。

〔23〕《上海市公共数据开放暂行办法》第 3 条第 2 款规定：“本办法所称公共数据开放，是指公共管理和服务机构在公共数据范围内，面向社会提供具备原始性、可机器读取、可供社会化再利用的数据集的公共服务。”

〔24〕 关于知情权主观权利客观化问题的探讨可以参见蒋红珍：《面向“知情权”的主观权利客观化体系建构：解读〈政府信息公开条例〉修改》，载《行政法学研究》2019 年第 4 期。

为信息提供者和被监督对象，政府负有公开信息的义务，向公众单向输出信息。在依申请公开中，如果行政机关没有履行公开义务，申请人可以向法院提起司法审查请求，政府与公众之间形成一种对抗关系。在我国政府信息公开实践中，就出现了非正常申请公开大量政府信息的现象，有的行政机关工作人员将政府信息公开工作视为负担和畏途。以陆红霞案件为代表的这一类申请及案件折射出政府与公众之间因政府信息公开而形成的对抗关系和对立情绪。

基于公共服务的制度性质定位，在政府数据开放中，政府的角色及其与公众的关系不同于政府信息公开。主动开放是政府数据的基本开放方式，较之信息公开，政府透明度得到进一步提升，更容易在政府与公众之间建立起信任关系，缓和双方之间的对立关系。就政府的角色而言，政府不再是单纯的信息提供者，同时也是数据的开发利用者，还是数据开放的受益者。如《上海市公共数据开放暂行办法》第 24 条第 2 款规定："本市鼓励数据利用主体与市经济信息化部门、市大数据中心以及数据开放主体开展合作，将利用公共数据形成的各类成果用于行政监管和公共服务，提升公共管理的科学性和有效性。"

就政府与公众的关系而言，政府数据开放建立了一种双方合作共赢而非对抗的关系。在数据的开发利用过程中，政府往往需要寻求私人及私人机构、社会组织的合作，如寻求互联网企业的合作完成平台开发利用。因此，开放政府数据的过程也是政府与私人机构、社会组织合作的过程，是私人参与政府治理的过程，双方由此形成合作治理的非对抗关系。很多城市治理的经验表明，通过开放交通、天气等与民生相关的数据，企业、组织、公民既可以挖掘政府开放的数据的商业价值，也可以利用数据帮助政府解决交通管理、公共事件预测与应对等问题，与政府共同解决城市治理面临的大城市病，借由数据开发实现公私合作治理。

四、二者关系定位对政府数据开放立法定位的影响

政府数据开放以政府信息公开为基础发展而来，承继并拓展了开放政府的内涵。政府数据开放立法一方面应当坚持公开、透明的原则，另一方面应当回应开放数据的基本要求，通过开放政府数据，提升政府在数字时代的治理能力。《政府信息公开条例》修订过程中，学界强烈呼吁通过修订条例回应政府数据开放的现实需求，在条例中作出相应的制度安排，但是，修法最终仅完善了政府信息公开制度，不涉及政府数据开放的问题。那么，关于政府数据开放的立法未来应当如何安排？有必要从政府数据开放与政府信息公开关系视角对有关立法的基本问题展开探讨。

（一）宜在国家层面尽快制定《开放政府数据法》

在我国《政府信息公开条例》立法目的和制度框架之下，政府信息公开与政府数据开放之间的差异较之域外并不十分突出。这一特点为政府数据开放的推行奠定了更好的基础，但是，也易形成认识上的混乱和模糊。实践中一些地方将政府信息公开与政府数据开放混同，原因固然是多方面的，欠缺统一立法也是影响因素之一。立法的缺失，既影响对政府数据开放工作的认识，更重要的是在依法行政的严格要求和严格的问责机制之下，潜在的法律风险使得地方政府难以实质性地推进。

按照政府数据开放与政府信息公开"承继但不取代"的基本定位，立法需求很难通过修改《政府信息公开条例》满足，需要建构独立于政府信息公开的政府数据开放制度体系。我国目前

采用了中央政策引导、地方立法先行先试的立法路径，但是，由于数据开放涉及其他法益保护的问题，《政府信息公开条例》关于豁免公开范围的规定，直接影响数据开放的范围，而这一问题是地方立法难以解决的。此外，政府数据开放涉及统一平台建设等行政内部机制完善问题，也难以通过地方立法予以解决。从已有关于地方政府数据开放平台建设、数据开放效果的文献来看，〔25〕我国政府数据开放实践仍存在很多问题，制定完善专门立法解决目前的诸多问题已有相当程度的共识。

政府数据开放立法为关于政府权力透明、开放运行的法律，就其性质而言，属于程序法范畴。程序规则应当统一，也易于统一，不同部门、不同地方政府遵循的政府数据开放规则具有高度相似性，在国家层面统一立法更为适宜。目前，与政府数据开放立法相关的《个人信息保护法》已于 2018 年被列为第十三届全国人大常委会立法规划的第一类立法项目，要对之进行统筹协调考虑，政府数据开放立法宜采用制定《开放政府数据法》的立法形式。

（二）以提升数字时代政府治理能力为立法目标

政府数据开放的兴起使得开放政府的内涵在公开政府信息基础上进一步扩展，政府数据开放成为数字时代政府与私人合作治理的新形式。如《上海市公共数据开放暂行办法》将“提升政府治理能力和公共服务水平”作为立法目的之一。〔26〕如以提升数字时代政府治理能力为立法目标，立法定位应当：

第一，政府数据以开放为原则、不开放为例外。获得数据是利用数据的基础，也是开放政府最基本的要求。虽然政府数据开放立法没有沿着知情权保障的路径展开制度建构，但是，公开、透明本身是开放政府的基本要求，也是开放的基础。此外，在技术层面，数据完整性也要求数据的公开应尽可能完整、充分。

第二，立法要全面回应开放数据的基本要求，明确开放政府数据应当遵循的基本原则，〔27〕完善开放、保护、利用等各环节的相关制度。开放数据的基本要求是对建构政府数据开放制度提出的最低限度要求，需要立法全面予以回应。在数据开放过程中，面临的法益保护等问题较之政府信息公开要复杂得多，面临的法律风险也更大，回应开放数据基本要求也为立法提供了具有操作性、可供把握的基本底线。

第三，硬法软法规范并重。以知情权保障和民主问责为目标的政府信息公开立法围绕公众知情权和政府公开义务这一组法律关系展开制度建构，立法明确了政府承担的公开义务及不履行公开义务所应承担的法律责任，基本为硬法性质的规范。政府数据开放不仅是将数据开放给私人部门利用，同时也通过私人部门利用政府数据帮助政府解决治理中存在的问题，这一目标的达成，需要借助柔性工具才能实现。如《上海市公共数据开放暂行办法》第四章“数据利用”规定了大量软法性质的条款，其中第 23 条第 1 款规定：“本市鼓励数据利用主体利用公共数据开展科技研究、

〔25〕 参见刘畅、刘璇：《天津政府数据开放：现状、问题与政策建议》，载《图书馆学研究》2018 年第 11 期；前引〔11〕，晴青、赵荣文；杨瑞仙等：《我国政府数据开放平台建设现状与发展对策研究》，载《情报理论与实践》2016 年第 6 期；曹雨佳：《政府数据开放生存状态：来自我国 19 个地方政府的调查报告》，载《图书情报工作》2016 年第 14 期。

〔26〕《上海市公共数据开放暂行办法》第 1 条规定：“为了促进和规范本市公共数据开放和利用，提升政府治理能力和公共服务水平，推动数字经济发展，根据相关法律法规，结合本市实际，制定本办法。”

〔27〕《上海市公共数据开放暂行办法》第 4 条仅规定了政府数据开放工作遵循的基本要求：本市公共数据开放工作，遵循“需求导向、安全可控、分级分类、统一标准、便捷高效”的基本原则。

咨询服务、产品开发、数据加工等活动。”再如第30条“多元主体参与”规定：“市经济信息化部门应当会同市大数据中心、相关行业主管部门建立多元化的数据合作交流机制，引导企业、行业协会等单位依法开放自有数据，促进公共数据和非公共数据的多维度开放和融合应用。”

（三）宜重视内部体制机制的完善

传统行政法治以外部行政法律关系为核心，将内部行政关系设定为行政自我调整的场域和空间，主要依靠行政内部规则予以调整，立法很少直接调整。从涉及的法律关系来看，政府信息公开以调整外部法律关系为主，内部关系涉及不多。但是，在政府数据开放中，内部体制安排和内部运行机制就十分重要。如数据质量的保障机制和数据完整性原则，要打破部门之间的信息壁垒，不通过立法而依靠政策很难解决。《上海市公共数据开放暂行办法》中涉及内部法律关系的条文比重很大，如总则条款中的第5条明确了“职责分工”，第7条规定了“协调机制”，第8条引入外部平衡机制“专家委员会”；各章条款中，第二章开放机制中明确了开放主体的确定规则，第三章平台建设中明确了统一开放平台等。完善的内部体制机制安排是政府数据得以顺利对外开放和达成开放目标的重要保障，在政府数据开放立法中，需要突破传统行政法治以外部法律关系为主的规范思路，重视内部体制机制的完善。

（四）建构多元机制解决开放范围难题

开放范围是政府数据开放制度建构中的难题，开放范围如果过窄，开放政府数据的目标难以达成。与政府信息公开制度建构一样，法益平衡是确定开放范围必须考量的因素，且在政府数据开放中难度更大，因为传统信息环境下的个人权益保障机制在大数据时代面临失灵的问题，而新的保护机制又尚未成熟。《上海市公共数据开放暂行办法》中采用了对数据进行分级分类，同时辅之以开放清单、定期动态调整等机制来解决这一问题。分级分类是其核心机制，根据该法第11条的规定，综合考量公共数据安全要求、个人信息保护要求、应用要求等因素，将数据分为非开放类、有条件开放类、无条件开放类三种类型。其中，非开放类包括涉及商业秘密、个人隐私，或者法律法规规定不得开放的公共数据。商业秘密和个人隐私在《政府信息公开条例》中属于相对不公开的信息，但在该办法中被列为非开放类数据。尽管第11条第3款补充规定“非开放类公共数据依法进行脱密、脱敏处理，或者相关权利人同意开放的，可以列入无条件开放类或者有条件开放类”，但是，原则上该类数据属于非开放类数据。《上海市公共数据开放暂行办法》对于这类数据较之《政府信息公开条例》实际给予了更严格的保护。

《上海市公共数据开放暂行办法》在分级分类这一核心机制之外，辅之以开放清单、定期动态调整等机制，形成多元综合机制解决开放范围确定难度大的问题。这一灵活的规范思路契合了政府数据开放实现数字治理效果的立法目的，也体现了政府数据开放立法所秉持的功能主义立法思路。在法益保护尚存在相当难度时，可遵循如下立法思路解决此问题：总则中对数据等核心概念的内涵作出明确规定，并明确规定政府数据开放以开放为原则，不开放为例外；开放范围部分列举不属于开放范围的情形；开放机制中规定开放清单和动态调整等多种机制。政府数据开放以实现数据公共价值为制度取向，在坚持政府数据以开放为原则的前提下，也要看到在海量政府数据中，存在高质量数据和一般数据的区分，尽管在如何确定什么数据是“高质量数据”这个问题上，存在一定争议。通过清单机制确定年度开放重点，通过定期评估调整开放范围，可以回应、契合社会当下的实际需求，使得法律规范层面的开放范围模糊性问题，通过具体机制予以调整。

五、结　论

政府数据开放不仅仅是政府信息公开向大数据时代的自然延伸，更是代表着一种全新的政府治理模式。政府数据开放承继了政府信息公开所建构的开放政府理念，并通过原始数据的开放让政府更透明。政府数据开放还拓展了开放政府的内涵，不仅将蕴含巨大价值的政府数据开放给社会利用，也通过社会挖掘政府所开放的数据反哺政府的公共治理。政府信息公开中的权利义务对抗在政府数据开放中转型为公共部门与私人的合作，公私得以携手开发数据的价值，创造更大的经济财富，共同有效解决社会问题。然而，这一美好图景中也隐藏着巨大的法益冲突和潜在的国家安全、社会稳定风险。立法无疑是解决开放与冲突并存问题的必要路径。

政府数据开放与政府信息公开虽然有着共同的理念和制度上的承继和衔接关系，但是，不同的制度取向决定了无法在现有的政府信息公开框架下解决政府数据开放的问题。现有的中央出政策、地方立法先行先试立法路径又难以克服地方政府立法权限的局限性。国家层面加快制定《开放政府数据法》无疑才是回应大数据时代政府治理模式变革的法治保障。

Abstract: The basic orientation of the relationship between government data opening and government information disclosure is "inherited but not replaced". The government information disclosure that emerged in the 1960s established citizens' right to know, constructed the concept and system of open government, and laid the foundation for the opening of government data in the 21st century big data era. On the basis of inheriting government information disclosure, the government data is open to respond to the basic requirements of open data, expands the connotation of open government, and forms an institutional system that is independent of government information disclosure. The main differences between government data opening and government information disclosure are as follows: institutional basis and legislative approach are different; government role and government-public relations structure are different. China should carry out special legislation on government data opening. The main ideas include formulating the Open Government Data Law as soon as possible to improve the governance capability in the digital age, attach importance to the improvement of internal institutional mechanisms, and construct a multi-disciplinary mechanism to solve the problem of open scope.

Key Words: government data open, government information disclosure, open government, open government data law

（责任编辑：刘　权　赵建蕊）

财经法学 No. 1，2020
pp. 25 - 34

网络爬虫行为对数据资产确权的影响

李　帅*

内容提要：数字经济模式下，商业竞争手段日趋多样。通过爬虫行为获取同业经营者线上数据并作营利用途，除有不正当竞争之嫌外，还构成对传统市场机制的严峻挑战。依据不同标准，可将技术爬取的数据划分为多种类型。受到爬虫不当行为影响的权利在边界范围、主体身份以及法律属性等方面呈现复合特征。从本源看，受损事实的发生多是因相关数据性质不明，从而使其衍生权利的界定面临障碍。以“数据资产”概念的提出为基础，结合公私法域多维视角分析其“权利性”，并最终提出网络数据资产的确权建议，是通过法律途径规制不当数据爬取行为的关键一环。

关键词：网络爬虫　数据资产　不正当竞争　数据安全

数字经济时代，数据作为一种新的生产要素，在预判市场走向、调控交易行为、影响各主体权利义务等方面发挥着重要作用。市场参与者特别是互联网企业，通过收集、存储、挖掘、加密、交易等一系列行为，充分发挥数据作为生产性资源的经济价值，更有企业直接将数据视为一种资产。与传统财产性资产不同，线上数据不具备明显的有体性，而以无形、可共享及可传输为主要特点，[1]这也就导致商业竞争向新的方向发展，并以争夺数据占有状态为主要形式。以下两则典型案例的核心内容均是一方主体通过线上行为获取另一方数据，但法院却作出截然不同的判决，其原因不仅关涉市场竞争与交易秩序的规范化，更与数据获取行为本身的合法性、数据的法律属性等问题密切相关。

案例一为 hiQ vs. LinkedIn。2017 年，同为职业类信息网站运营者的 hiQ Labs 公司（以下简称“hiQ”）将 LinkedIn 公司诉至法院，起因是后者通过后台程序阻止前者获取其客户数据。据调查，hiQ 将其商业模式基本建立在对 LinkedIn 用户数据的分析上，所依托的技术也以数据的爬取和挖掘为主，直至 LinkedIn 采取反爬措施。对此，法院判决 LinkedIn 不得阻止 hiQ 进入、

* 李帅，北京外国语大学法学院讲师。

〔1〕 参见刘金瑞：《数据财产保护的权利进路初探》，载《中国信息安全》2017 年第 12 期。

复制并使用其网站的公开信息，亦不得采用技术措施进行阻碍。〔2〕2019 年 9 月，美国第九巡回上诉法院对该案作出二审判决，认定 hiQ 公司从 LinkedIn 上抓取公开数据的行为不构成违法。案例二为“酷米客”vs.“车来了”。2013 年起，深圳市谷米科技有限公司（以下简称“谷米公司”）发布并运营一款名为“酷米客”的实时公交 App，通过与公交集团协议安装的定位系统获取公交车辆的位置信息。2015 至 2016 年间，武汉元光科技有限公司（以下简称“元光公司”）为提高其 App“车来了”的信息查询准确度，利用爬虫软件获取“酷米客”服务器中的实时数据，日均达到 300 万至 400 万条。基于此，“酷米客”将“车来了”诉至法院，法庭经审理认为被告“车来了”运营方构成不正当竞争，应立即停止侵权行为并依法进行赔偿。〔3〕

两则案例相反的认定结果，除了因为不同经济体制下法律功能与目标的差异之外，最关键的原因还是爬虫行为在本质、细节等方面存在区别从而使行为外部性的实质不同。以此为背景探讨网络爬虫行为，分析其引发的权利义务变动，能够有效深入问题核心——网络数据的法律属性。

一、何为“网络爬虫行为”

网络爬虫是一种自动获取互联网信息的程序或脚本。可以说在大数据时代，除直接通过用户采集之外，另一大数据来源就是使用网络爬虫采集公开信息。常见的爬虫手段包括有构造合理的 Http 请求头、设置 Cookie、使用代理等。作为一项互联网技术，爬虫行为本身并不违法，甚至很多信息类网站的基础技术就是爬虫程序。然而，当技术中立受到商业偏好的影响时，诸如“同业爬虫”等非正当行为则对存储在云空间中的各类数据形成安全性冲击。实践中，爬虫行为正当性的判定，要在企业竞争保护和数据权利保护的双重思想指导下展开，从而全面实现数据关联利益。

（一）两则案例中的爬虫行为定性

在案例一中，一方面，hiQ 通过爬虫程序获取的数据为 LinkedIn 对外公开的内容，且大部分系由用户直接输入、未经平台加工，所以 LinkedIn 在本质上仅是数据收集者和占有者。此外，hiQ 实施的数据访问行为与一般用户无异，仅在获取的数量上多于后者，但也不足以构成限制其爬虫行为的理由。另一方面，LinkedIn 的主要经营业务是提供职业社交服务，为业内公认的绝对支配者，掌握丰富的职业关系信息；相比之下，hiQ 从事的主要是企业员工行为测评工作，并依托员工职业生涯中的自评或他评信息为雇主及人力资源部门提供“员工离职风险分析”服务，在经营项目和目标群体上与 LinkedIn 均无冲突，不属于同业竞争者，所以除有正当理由外，不应限制 hiQ 作为市场活动参与者的正当数据行为。

在案例二中，“车来了”运营商爬取“酷米客”数据，虽然获取的也是后者实时公开的内容，但与案例一却有着本质上的区别。其一，两款手机 App 的运营商均为用户提供实时公交定位服

〔2〕 See hiQ Labs，Inc. v. LinkedIn Corp.，273 F. Supp. 3d 1099（N. D. Cal. 2017）.

〔3〕 参见深圳市中级人民法院（2017）粤 03 民初字 822 号民事判决书。

务，商业模式基本相同，存在明显的竞争关系。本案中，元光公司爬取数据的目的就是得到更精准的信息，扩大市场占有份额，可以判定其实施了不正当竞争行为。其二，在数据性质方面，虽然公交车辆运行路线、运行时间等信息仅系客观事实，但经人工收集、分析、编辑与整合之后，就可为 App 的商业运行带来可观效益，所以实际上已具备无形财产的特征。谷米公司系“酷米客”App 设计者，对相应数据除了享有这种特殊的所有权外还是其著作权权利人，因而对于软件所包含的核心数据，未经权利人同意不得私自爬取并用于经营行为。

（二）网络爬虫不当行为的判定标准

数字经济时代，爬虫行为的存在已是普遍现象。在不违背交易秩序和竞争规则的前提下，市场主体对爬虫基本持默许态度，亦有经营者之间通过内部协议允许互相爬取数据的先例。〔4〕此外，《电子商务法》第 31 条规定平台经营者应当“记录、保存商品和服务信息、交易信息，并确保信息的完整性、保密性、可用性”，亦是通过强调“保密”与“可用”并不矛盾的精神，侧面反映出监管的目标既在于维护网络数据安全，又关注数据多维价值的实现。因此，以“爬虫行为正当性高度依赖数据价值属性”这一特征为基础，可将判定网络爬虫不当行为的考量因素总结为以下两个方面：

1. 数据来源及目标用途

基于商业目的，爬虫技术的应用不仅局限在获取已公开的数据，更多是为了得到对方未开放的内部数据或后台数据，在数字经济过程中则是爬取企业运营所依赖的基础信息。例如，金融爬虫重点获取用户的真实姓名、消费金额记录、信用借贷记录等既关涉个人隐私、又属于商业秘密的信息内容，这与搜索引擎爬取网站界面数据的行为完全不同，其负面性根源在于信息渠道的非正当。

但是，并非所有未涉及内部数据的爬虫行为都是正当的，亦即，合理来源要与合理用途相结合。具体到实践中，判断爬虫行为正当与否，应当考虑以下因素：第一，爬虫获取的数据被用于同业竞争还是非同业经营。实践案例除了前文提及的“酷米客”与“车来了”纠纷之外，还有商业银行信用卡中心之间、互联网现金贷 App 之间相互爬取后台数据，基于对方的放款额度或授信额度，确定本商业实体对自身用户的信贷金额，这些都属于利用同业经营者的数据资源从事相同经营活动，且客观上未履行自身作为金融机构对用户的资格审查职责，故应当被定性为爬虫不当行为。第二，爬虫行为的社会效果是利大于弊，还是弊大于利。当前，大量互联网抢票软件利用爬虫程序在铁路购票及航空购票网站持续点击，实时抢购平台余票。这一操作虽然可以实现加价抢票效果，但实际却影响到网站使用流畅度和所有消费者公平购票的权利，因而属于爬虫不当行为。

2. 授权获取方式及数据使用范围

《网络安全法》第 41 条规定：“网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同

〔4〕 例如，诸多互联网平台与百度、Google 等搜索引擎运营公司签订内部协议，允许后者爬取其数据作为用户搜索结果，并链接至原网站平台。

意。”基于法律对数据来源主体的权利保护规则，虽然网络爬虫并非直接从用户手中获取数据，但理论上同样应在事前取得授权。

当前共享经济与电子商务协同发展，互联网实时线上数据体量巨大，用户关注的重心往往与购买商品、享受服务以及获取资讯相关，而对平台上的消费者协议内容一带而过，并通过勾选的方式将“同意”与“授权”一次性作出。实践中，有网络运营商采用各种方式扩大用户信息的获取和使用范围，很大程度上侵害了用户个人信息安全。常规互联网平台在获取授权过程中尚如此，爬虫程序获取用户授权则更具“表述模糊性”与“方式隐蔽性”。例如在商业竞争中，有经营者希望获得更多同业商家持有的用户信息，则要求自己平台上的用户提供在其他同类平台注册时的用户名和密码，以便获得更好的服务。这种做法虽然得到了用户授权，但大部分授权人并不知晓实际获取信息的主体是爬虫程序，被爬数据的真实范围远大于用户知情范围，且数据的最终用途也与获取授权时告知的内容不符，这就使得数据来源主体的知情权和依托数据产生的其他权利受到严重侵害。

二、数据权利内涵新解及其与爬虫行为的相互关系

在网络爬虫行为中，线上数据作为一系列活动的标的，其所承载的内涵与传统数据相比实现了量级化突破。这种行为对象上的拓展，直接导致相应权利客体发生变化，受爬虫行为影响的权利种类和性质亦有一定改变。因此，对数据权利属性进行研究，既有利于厘清爬虫行为中受损的权利内容，为相关制度的完善提供依据，同时更是制定数据资源确权、开放、流通、交易相关制度的起点和基石，有利于完善数据产权保护制度。〔5〕

（一）以网络为媒介的数据种类界分

传统经济时代，数据的分类标准主要包括产生时间、涵盖范围、权利主体等，相应地，其类别有当前数据与历史数据、宏观数据与微观数据、个体数据与群体数据等。而现今，网络技术丰富了数据的产生、流转、利用与交易途径，数据分类方式和分类标准不再局限于二维层面，其复合属性日益明显。

首先，以数据的生成是否需要网络平台加工为标准，可以将线上数据分为用户个人信息、实时位置信息等原始数据，以及交易记录信息、活动轨迹信息等加工数据。其中，加工数据涉及多重主体的贡献迭代问题，与原始数据相比附加了更多的社会价值，因而利用规则也相对复杂。具体而言，实践中对加工数据的获取与应用，要额外考量数据处理的经济成本，并以加工主体的意愿为决定因素之一。

其次，以数据的存在形式为标准，可分为文本数据、状态数据与新模态数据。文本数据指的是可经记载、描摹或复制，将内容以有形形式存储的信息，包括但不限于各种文字、符号、图像及其组合。状态数据是以非文本形态生成并存储，具有较强时效性的信息，例如实时地理位置信息等。人工智能技术背景下，电子身份识别所需的指纹、瞳孔、声音等信息具备了高度代码化特

〔5〕 参见李爱君：《数据权利属性与法律特征》，载《东方法学》2018 年第 3 期。

征，可独立成类，即为新模态数据。实践中，数据的特殊形态常被用作不当获取行为的抗辩理由，其原因主要就是信息类型化的不甚完善。所以，扩展数据的传统认知范畴，能够有效划定爬虫行为的对象领域。

再次，以数据内容的重要性程度和生成环节为标准，可分为核心数据与周边数据。此分类标准下，数据子类包含的具体内容并不确定，需要结合实际情况，分析相关数据是否体现核心权利义务关系，以及该数据是否系数据生成、流转或存储行为的附属产物。具体言之，作为数据行为的目标产物，且蕴含社会、经济价值的数据通常被认定为核心数据，爬取时需要得到数据主体的知情同意和授权；除此之外，数据流通过程中产生的程序信息、档案信息或其他信息，不具有明确的使用价值或对行为人权益无实质性影响，通常在确认不涉密之后则可供爬取。

最后，以数据主体的身份差别为标准，可以分为用户数据与商家数据。前者系网络用户基于自愿，主动向平台提供的有关个人身份、行为习惯等方面的信息；后者为平台经营者实施商业运营行为产生的新信息，或者从事数据加工行为产生的增值信息等。因为与主体权益密切相关，所以规制此类数据时需要以主体身份的明确为前提，在此基础上深入分析权利种类，将主体与权利相匹配，最终为数据爬取行为的实施者提供意见征询对象及征询内容。

（二）数据权利内涵的时代性拓展

伴随数据形态和内容的丰富，依托其生成的数据权利也面临着因应性变革，主要趋势就是权利内涵的进一步充实，以及多种属性权利的并行存在。理论研究进程中，邻接权客体与财产权客体的争议至今尚存，〔6〕而蕴含着人格权内涵的“资产权客体说”作为新生理论，在网络社会中日益显现更适于保障数据主体权益的能力。

当前实践中，立法对数据权利的定性尚未明确，世界范围内亦不存在一部调整各类数据行为的法律规范，仅在个人信息或隐私保护的维度上有所突破。以 2018 年欧盟出台的《一般数据保护条例》（GDPR）为例，该法案以强化数据主体对个人数据控制为导向，但未能明确划分数据权利项下人格权与财产权的边界，一定程度上掣肘了立法目标的实现。因此有学者认为保护公民的隐私权益，应当更多采取公法风险规制与消费者法保护的框架，而不是寻求一种具有确定性边界的隐私权或个人信息权。〔7〕推及互联网背景下的所有数据范畴，这一理念同样具有其合理性：其一，大量互联网数据系从用户个人处收集所得，且主要来源于用户的消费行为，可界定为消费数据的组成部分，因而以消费者法的思路对相关信息进行保护具有客体的适格性。其二，存储在网络数据库中的信息并不局限于原始的用户信息，还有因流转和加工而不断充实的信息，所以坚持以一种确定的权利名称界定互联网数据，不论对权利属性的全面认知还是合法权利的有效保障而言，都缺乏科学合理的指导意义。

综上，选择具有综合意义的“资产权”概念诠释新时代的数据权利，赋予其人格、身份、财

〔6〕 持“邻接权客体说”的学者主要有林华、秦珂等，参见林华：《大数据的法律保护》，载《电子知识产权》2014 年第 8 期；秦珂：《大数据法律保护摭谈》，载《图书馆学研究》2015 年第 12 期。持“财产权客体说”的学者主要有高富平、齐爱民等，参见高富平：《信息财产——数字内容产业的法律基础》，法律出版社 2009 年版；齐爱民：《捍卫信息社会的财产——信息财产法原理》，北京大学出版社 2009 年版。

〔7〕 参见丁晓东：《什么是数据权利？——从欧洲〈一般数据保护条例〉看数据隐私的保护》，载《华东政法大学学报》2018 年第 4 期。

产乃至知识产权等多重内涵，将是数据时代规范爬虫行为的权利设定基础。正如龙卫球教授所言，一旦承认了用户具有数据财产权，那么就会迫使数据使用者主动与数据主体进行商议，如此则改变了用户在数据市场被忽视的境地，使得用户获得了一定的议价能力。〔8〕这在互联网商家竞相爬取用户数据的当下，可以说为最核心的数据主体——个人用户——提供了权益保障的良性思路：既关注了用户在互联网数据活动中的数据来源者地位，认可其对自身数据享有一定的决定权与处分权，又洞悉了用户参与互联网活动的关键意图是成为消费者，所以承认并保障其包括知情权、选择权等在内的消费者权益，将进一步拓展数据权利的内涵和外延。

（三）受爬虫行为影响的具体数据权利

以爬虫时代为背景，当数据获取行为日渐成为互联网主体的常规活动时，窃取他人数据谋取经济利益的行为就可能混同于其他数据获取行为中，给用户、商家、平台的数据权益造成不利影响。

从不同主体在数据来源、应用及流转中的身份差异来看，可将受到网络爬虫不当行为影响的具体数据权益做如下划分：第一，对互联网平台经营者而言，商家之间的数据爬虫不当行为破坏了平台正常的运行规则，在影响数据安全的同时，还可能使用户对平台本身的中立地位产生质疑，从而侵害到平台运营方的经营权，给其商业信誉带来负面影响。当然，如果利用爬虫程序不当获取数据的行为系平台方所为，则前述不当后果应由平台自行承担。第二，对在平台上从事经济活动的商家来说，如果是被爬取方，则其依托相关数据而享有的商业秘密、知识产权将会因此受到侵害；如果是爬取方，则在利用爬取数据进行后续经营活动时，极易因资质欠缺或使用不当而造成用户损失，从而违反现行法律的相关规定、影响自身商誉，严重者还可能构成犯罪。第三，对于互联网用户群体而言，爬虫不当行为的直接对象就是其个人数据，即使这些数据关涉的内容主要是商业活动，但通过大数据技术深入挖掘，很容易精确定位个人身份并形成专属于个体的消费习惯信息，对隐私权、自主选择权等权利造成损害。

以上提及的“合法权益”，其界定思路仍然以传统部门法学视角下的分类标准为主，即在民事权利项下划分具体的权利种类，并按照不同部门法的规定对侵权行为进行处理。这种方式在实践领域沿用已久，虽具备较强的可操作性，但在处理实效和便捷度方面却存在不可否认的缺陷。因此，以互联网爬虫不当行为的频繁出现为背景，法学实践和理论研究都开始寻求一种更为简捷的权益保障路径，这也对一种更具概括性的权利种类提出了明确需求。综上，传统法学研究开始从单纯的“原理型”转向同时侧重原理和对策的多重价值型，并以切实解决当前数据时代的新型问题为主要任务。这在应对爬虫不当行为时，主要表现为对已有权利种类的丰富和对传统法律保护方式的更新。

三、数据“资产型保护”路径的确立

（一）从“泛资产”到“大资产”的概念演变

在金融领域，“泛资产”概念的出现基本始于 2010 年前后，标志性事件即投资基金逃离传统

〔8〕 参见龙卫球：《数据新型财产权构建及其体系研究》，载《政法论坛》2017 年第 4 期。

实体经济，流向农产品、艺术品等具有资产性质的实物或者影视一类具有资产意义的行业，从而使这些非典型财产获得了资产的属性，被称为“泛资产”。伴随互联网布局的扩大和大数据技术的发展，泛资产的概念亦无法与实践的发展保持完全同步，诸如信息、数据以及由此衍生出的各类电子资料，以及表现为声音、图像、指纹、虹膜等多种模态的生物档案也日益呈现出可供挖掘与利用的经济价值。因此，以泛资产时代的出现为参考和借鉴，笔者提出“大资产”概念，用以指称上文提及的信息和数据等新型财产客体。

之所以称其为“大资产”，而没有在“泛资产”的概念上进行外延扩充，一方面是因为“泛资产”的用法源自金融领域，并且在一定程度上已经成为具有特指意义的术语，所以法学研究需要结合社会需求和学科特征，创设相对新型的术语。另一方面则是基于当前“大健康”“大文娱”等概念的出现，社会公众对此类表述已形成一定的认知和理解，因此用“大资产”一词来统摄现存具有资产性质的事物、行业或产业，具有现实基础。在法学研究中，因大资产而派生出的权利主要是与其相对应的“资产权”，当然，与传统法学研究中学者曾提出的“资产权”概念相比，其在权利的主体、客体、权利义务关系等方面均呈现出较大差异。

传统研究中，资产权主体多为企业或国家，因而问题的探讨较多集中于国有土地使用权以及PPP项目中的权利转让等领域，〔9〕并未将其视为公民个体法定权利的一种。因而本节提出构建“资产型”的权利保护路径，首先就要突破现有的理论认知，将资产权主体范围拓展至个人，并赋予其综合性权利的属性，具体来说，综合的主要是物权、知识产权的特性，并且在特定情况下还可能包括人格权属性。

（二）爬虫时代Robots协议的失灵现象

Robots协议，又称“爬虫协议”或“机器人协议”，〔10〕是技术界为了实现爬取方和被爬取方之间的意愿沟通而设定的一种计算机程序。〔11〕根据中国互联网协会《互联网搜索引擎服务自律公约》〔12〕第7条的定义，Robots协议是指互联网站所有者使用robots. txt文件，向网络机器人（Web Robots）给出网站指令的协议。具体而言，Robots协议的关键内涵在于提示网络机器人哪些网页不应被抓取，而哪些网页可以抓取。〔13〕关于此处Robots协议的法律属性，我国目前尚无立法明确规定，可供适用的调整型规范仅有前文述及的《互联网搜索引擎服务自律公约》。〔14〕鉴于该公约的非强制性特征，实践中商业主体为获取经济利益而违背协议的现象频频

〔9〕 相关研究例如：占一熙、陈芬辉：《农村集体资产权属的几点思考》，载《农村经济管理》2016年第8期；赵琰：《PPP项目资产权属及会计核算方法》，载《财会学习》2017年第22期；郭滨辉：《PPP项目的资产权属、会计核算及税务处理》，载《财会月刊》2019年第3期。

〔10〕 Robots协议诞生于1994年2月，由荷兰软件工程师Martijn Koster创建，据称起因是Koster的服务器遭受到不良爬虫的爬取而致使服务堵塞。不久该协议即成为现存及未来的网络爬虫都被期望遵守的行业惯例。参见瞿森、杜承彦、谭晓明：《数据之争：网络爬虫涉及的法律问题（二）》，载微信公众号“知产力”。

〔11〕 参见罗刚：《网络爬虫全解析：技术、原理与实践》，电子工业出版社2017年版，第45页。

〔12〕《互联网搜索引擎服务自律公约》系2012年11月由百度、即刻搜索、盘古搜索、奇虎360、盛大文学、搜狗、腾讯、网易、新浪、宜搜、易查无限、中搜12家企业联合发起并签署的行业自律公约。该公约共4章22条，适用于中国互联网协会会员单位和自愿加入的互联网从业单位，并且倡议其他从业单位积极遵守。

〔13〕 参见瞿森、焦晨恩：《数据之争：网络爬虫涉及的法律问题（一）》，载微信公众号“金杜研究院”。

〔14〕《互联网搜索引擎服务自律公约》第7条第1款规定：“遵循国际通行的行业惯例与商业规则，遵守机器人协议（Robots协议）。”

发生。

在日趋强烈的经济利益导向下，仅有的行业性规范很容易被突破，Robots 协议面临严重的失灵问题：爬虫行为不仅大批量获取其他商业主体的后台信息，还会强行突破对方网站设置的技术措施以实时、无限制地抓取信息。形成这一现象的原因，除了经济效益的驱使之外，主要还在于 Robots 协议并不构成具有法律效力的协议，当前在我国仅被视为业内普遍遵守的“公认的商业道德”，缺乏国家强制力约束，对 Robots 协议性质的界定和详细论述可参见 2013 年百度诉奇虎 360 案判决书。〔15〕但需要注意的是，即使协议不具备强制约束力，上述行为同样可能违反其他现行法律的规定，例如构成《反不正当竞争法》第 12 条中“利用技术手段，实施妨碍、破坏其他经营者合法提供的网络产品或者服务正常运行的行为”。此外，对于强行突破某些特定被爬取方技术措施的，还可能构成刑事犯罪。这里对违法抑或犯罪行为的处理思路，仍然是将被侵犯的权利进行分离，结合上文所述两则案例来看，即司法机关在裁判过程中并未明确界定受损数据的权利性质，只是通过所有权或著作权模式进行保障，尚不存在一个相对复杂、综合的保障方式。

（三）新型数据保护思路的确立

从目前已发生的数据纠纷情况来看，其化解方案主要还是从既有法律体系中寻求解决办法，最多援引的法律规范即为《合同法》《反不正当竞争法》《侵权责任法》以及知识产权法律。例如，数据合同法路径救济的前提是争议主体之间存在预先的合同安排，但是我们发现这种合同安排无论如何周密也只是一种债的保护，本身不具有排他性，无法对抗来自第三人的数据加害，而在现实中数据加害往往就是来自企业数据合同关系之外的第三人侵入或者非法利用。〔16〕与此同时，相对松散的 Robots 协议无法起到绝对的约束作用，这就更加呼吁一种具有排他性，且在权利保护顺位上占据优先级别的保护方式。

在法学领域确立“大资产”概念并通过资产权路径保护互联网用户、商家及平台的数据权利，成为当下新型权利保护的可行思路。具体而言，就是应当同时关注社会的风险规制和消费者的选择与预期，〔17〕综合运用公法和私法理念。落实到实践中，即需要设计一种兼具物权与知识产权属性，并同时体现人格权与财产权价值的权益，建议采用“资产权”的表述，其保护路径应适当借鉴欧盟和日本等国家（地区）的“放松收集环节，加强使用监管”的数据处理规则及相应立法例，强化数据加工处理阶段的保护要求。

四、数据资产确权背景下相应法律保护措施的展开

（一）推进统一的综合性数据资产保护立法进程

互联网数字经济时代，爬虫不当行为对数据安全造成的负面影响实际上只是冰山一角，更多行为诸如数据交易、数据不当应用等也对存储于网络数据库中的海量信息产生安全性威胁。因

〔15〕 参见北京市第一中级人民法院（2013）一中民初字第 2668 号民事判决书。

〔16〕 参见龙卫球：《再论企业数据保护的财产权化路径》，载《东方法学》2018 年第 3 期。

〔17〕 参见前引〔7〕，丁晓东文。

此，在国家层面制定统一的数据保护类立法，并以各类个人数据、商业数据等为主要保护对象，成为当前该领域内的立法发展趋势。在 2018 年 9 月公布的“十三届全国人大常委会立法规划”中，《数据安全法》已被列为“条件比较成熟、任期内拟提请审议的法律草案”，标志着具有一般性法律规范性质的数据法制定工作已经提上日程。

从法律名称来看，《数据安全法》仅调整与数据安全有关的法律关系，对数据的财产权益等其他法律关系并不涉及，〔18〕但结合实践需求分析，此次立法除了应对社会公共层面的数据安全问题外，还应着力解决网络数据权属不明、保障措施不力的现状。因此，制定中的《数据安全法》应充分考虑不同主体对数据立法的差异化需求，明确在“资产权”概念下保护数据资产的方式：第一，清晰界定受本法保护的“数据”范畴，明确用户、商家及平台享有的数据资产权在范围、时限上的差异；第二，规定各数据主体的责任和数据处理、利用规则；第三，授权设立专门的数据保护监管机构，监督数据的收集、使用与流转；第四，明确侵犯数据资产权所应承担的责任。

（二）区别不同阶段的数据保护和处理规则

数字经济下，大数据的多维度、多层次应用给传统网络法中的同意原则、自主可控原则、透明度原则、匿名原则、最小化原则等法律原则带来严重挑战。首先，在数据收集环节，如今基本可以做到只要接触网络就会留有痕迹，即凡是“触网”的数据必然遭到收集。所以，要求数据的收集必须经权利人同意，甚至必须通过特定程序获取同意，已然不适应于当前社会的发展。在此建议适当放松对数据收集环节的管控和限制，规定只要经合理的明示方式履行了告知义务，即可收集与法定经营权限相关的用户信息。其次，在数据加工处理阶段，商家或平台通常会利用各种分析工具对数据进行挖掘，获取成倍于数据表层含义的信息量。对此，应当严格规范数据的加工、处理与应用环节，本着权利人同意为前提的基本原则，在获得授权的范围内实施数据处理行为，并将数据加工后所得形态、数据流转的去向以及未来可能适用的场域均告知权利人。

可见，在数据行为的不同阶段，法律的保护力度和限制条件应当有所差别，这既是法治发展适应社会需求的基本要求，也反映了法律制度在变革中不断趋于科学、理性的过程。

（三）强化侵犯数据保护的责任追究

数据资产权保护模式下，电子化的个人信息、商业信息具备了产权性质，排他地从属于权利主体，具有直接支配性。换言之，用户、商家的个人数据、消费数据或经营数据等内容，不再只是受到非法侵犯后才能获得救济式的保障，而是在日常生活中就享有与所有权相似的“第一性”或“充分性”，通过法律文本对权利的确认而获得主动式的保障。

在这一变化背景下，应当合理配置数据保护责任体系，强化侵犯数据保护的责任追究机制。一方面，建议以我国现行《物权法》第一编的立法体例为蓝本制定《数据安全法》总则部分，转变传统数据保护的侵权法思路，明确规定数据资产权的实现与保护路径。另一方面，划分数据违法行为的类型与损害程度，规定不同的法定责任承担方式及担责范围，并加强对违法提供、使用

〔18〕 参见史宇航：《今年将推进立法的〈数据安全法〉，有哪些看点?》，载 https://baijiahao.baidu.com/s?id=1627780949714211002&wfr=spider&for=pc，最后访问时间：2019 年 8 月 20 日。

或侵犯个人信息和商业数据者的责任追究。

五、结　语

网络爬虫不当行为的日益泛滥，给数字经济的发展和互联网整体环境的优化都带来严重的负面影响。传统侵权保护模式只能起到有限的私权恢复作用，而无法实现公法意义上的行为规制与风险防范目标。以《数据安全法》的立法推进为契机，确立数据资产权概念并开拓资产权保护路径，是行政法与民法的一次交流与合作，亦是大数据时代法治不断成熟与完备的必然进路。

Abstract: In internet economy era, the means of commercial competition have become increasingly diverse. Obtaining online data from peer operators through the crawler program and using it for profit-making purposes, are largely suspected of unfair competition, meanwhile constitute a serious challenge to traditional market mechanisms. According to different standards, the content of technology crawling can be divided into raw data and processing data, text data and status data, core data and peripheral data, as well as merchant data and user data, etc., which makes the rights affected by crawler misconduct shows composited features in boundary scope dependent subject and legal attribute. From the root cause, the facts of damage happening are mostly due to the unclear nature of the corresponding data, which leads to the obstacles in the definition of derivative rights. Therefore, based on the concept of data assets, combined with the multi-dimensional perspective of public and private jurisdictions to analyze its rights' status, and finally put forward the recommendations for the determination of online data assets, is a key link to regulate improper data crawling behavior through legal channels.

Key Words: web crawler, data assets, unfair competition, data security

(责任编辑：刘　权　赵建蕊)

财经法学 No. 2，2020
pp. 94 - 109

数据产品保护路径探究
——基于数据产品利益格局分析

毛立琦*

内容提要：数据产品是运营商对信息主体的原始数据进行生产加工后形成的产品。根据数据处理形式的不同，数据产品可以分为汇集型数据产品和演绎型数据产品。基于对各类数据产品依附的利益格局分析，汇集型数据产品的权益应由运营商行使，但应注意对信息主体权益的保护；不同于此，信息主体对演绎型数据产品已无法确定权益，所以运营商可以独立自主行使产品权益。运营商对数据产品的利益位阶越低，其利益受财产法律调整保护的力度相应越弱。基于对运营商利益与公共利益之间的权衡，数据产品适用权利保护模式时，必须满足权利授予的相关条件。对于无法达到权利保护模式的数据产品，行为规制模式提供基础性保护。针对数据产品的保护，两种模式相互独立，相辅相成。

关键词：数据产品　权利　利益　权利保护模式　行为规制模式

一、问题的提出

随着科学技术和互联网的不断发展，数据日益成为企业谋求经济转型和创新发展的突破点。在大数据时代，单个个人信息不具备商业化的条件，大数据的商业化利用才是促进社会经济发展的基石。〔1〕网络运营商基于用户个人信息的原始数据进行收集、处理、加工、利用，形成数据产品，其对于企业自身发展与社会公共利益具有巨大价值。因此，如何有效对数据产品进行保护，就成为一个亟待解决的问题。

* 毛立琦，南京大学法学院博士研究生。

本文为2019年度南京大学博士研究生创新创意研究计划“证券行业的反垄断默示豁免制度研究”（CXCY19 - 21）的阶段性成果。

〔1〕 参见李媛：《大数据时代个人信息保护研究》，华中科技大学出版社2018年版，第195页。

在淘宝（中国）软件有限公司（以下简称“淘宝公司”）与安徽美景信息科技有限公司（以下简称“美景公司”）不正当竞争纠纷案中，杭州市中级人民法院认为，美景公司利用其平台，共享淘宝公司开发的数据产品，涉案行为构成不正当竞争。〔2〕但杭州互联网法院首先对用户个人信息、原始数据及数据产品进行了界分，认定淘宝公司对数据产品享有独立的竞争性财产权益，但是囿于“物权法定”原则的约束，并未认可淘宝公司对该数据产品享有财产权，而在《反不正当竞争法》一般条款下对涉案数据产品权益进行保护。〔3〕

法律框架下调整对象不同的法律性质意味着不同的保护模式，也就意味着不同的交易成本与制度效率。〔4〕李友根教授将法律视野中的利益分为以下四种不同形态：否定利益、放任利益、法益以及权利。〔5〕对数据产品保护路径的探析，不仅是为了确定网络运营商对数据产品享有何种利益，更旨在构建一个平衡信息主体、运营商与社会公共利益的法律框架。数据产品肇始于运营商收集的个人信息，所以本文拟追本溯源，首先分析数据产品依附的利益格局，进而确定运营商对数据产品的利益性质，最终探究数据产品的保护路径。

二、数据产品的界定

目前，相关数据立法主要集中在个人信息保护方面，尚无法律法规对数据产品进行标准化定义，相关立法几乎为零。〔6〕相较于立法的空白，理论界已经开始关注企业数据产品的保护，但是，对于何为数据产品，现有文献并未予以明确界定，多是将其作为现有概念直接使用。〔7〕

在淘宝公司与美景公司不正当竞争纠纷案中，杭州市中级人民法院认为，数据产品所提供数据内容不再是原始网络数据，而是在巨量原始网络数据基础上通过一定的算法，经过深度分析过滤、提炼整合以及匿名化脱敏处理后而形成的预测型、指数型、统计型的衍生数据，其所呈现方式是趋势图、排行榜、占比图等图形，提供的是可视化的数据内容。〔8〕

有的学者即是基于司法实践对数据产品进行界定。〔9〕相较于此狭义的界定，《中国电子商务立法研究报告》认为数据产品是运营商基于自身业务需求，对用户个人信息进行收集、整理、分析及加工后得到的产品。〔10〕有的学者指出数据库、数据平台以及数据决策等均属于数据产

〔2〕 参见杭州市中级人民法院（2018）浙 01 民终 7312 号民事判决书。

〔3〕 参见杭州互联网法院（2017）浙 8601 民初 4034 号民事判决书。

〔4〕 参见周林彬、马恩斯：《大数据确权的法律经济学分析》，载《东北师大学报》（哲学社会科学版）2018 年第 2 期。

〔5〕 参见李友根：《经营者公平竞争权初论——基于判例的整理与研究》，载《南京大学学报》（哲学·人文科学·社会科学版）2009 年第 4 期。

〔6〕 截至 2019 年 4 月 10 日，笔者在北大法宝数据库（http://www.pkulaw.cn/）以“数据产品”为关键词进行全文搜索，结果显示的 108 篇“中央法规司法解释”中没有专门涉及数据产品的文件。

〔7〕 有学者将“大数据”作为数据产品予以论述，如涂燕辉：《大数据的法律确权研究》，载《佛山科学技术学院学报》（社会科学版）2016 年第 5 期；有学者将数据产品表述为数据财产，如郝思洋：《知识产权视角下数据财产的制度选项》，载《电子知识产权》2019 年第 9 期；有学者在论述企业数据时，也有涉及数据产品，如李扬、李晓宇：《大数据时代企业数据权益的性质界定及其保护模式建构》，载《学海》2019 年第 4 期。

〔8〕 参见前引〔2〕。

〔9〕 参见王江桥：《数据产品的权益归属及司法保护》，载《人民司法》2019 年第 8 期。

〔10〕 参见全国人大财政经济委员会编：《中国电子商务立法研究报告》，中国财政经济出版社 2016 年版，第 98 页。

品。〔11〕有的学者将数据的处理行为进一步划分为简单加工的汇集性处理和经过演算的分析性处理。〔12〕

基于上文分析，本文对数据产品采取广义界定，即数据产品是运营商对于信息主体的原始数据进行生产加工处理后形成的产品，其不仅可以包含数据“质”的改变，也可以仅是数据“量”的集聚。〔13〕数据产品既可以是可视化数据内容，也可表现为数据加工处理形成的计算机软件或者技术方案等。运营商对数据的处理环节不同，形成的数据产品利益格局亦有所不同。本文根据数据处理形式的不同，借鉴《著作权法》对作品的分类，将数据产品分为汇集型数据产品和演绎型数据产品，下文将具体展开论述。

数据产品涉及多方主体关系，依附着不同种类的利益，对于利益的选择与衡量标准，终究是价值判断问题。对于数据保护的利益衡量，以欧盟为代表的大陆法系优先保护信息主体的隐私利益，以美国为代表的英美法系则更注重数据开发成果的利用价值。〔14〕随着数据经济的发展，建构在信息主体权益保护基础之上的莱斯格信息财产理论的单向性不足越来越明显，运营商的重心地位日渐凸显。〔15〕数据经济逐渐体现为一种围绕数据经营和利用而展开的复杂关系，以一种运营商为重心的双向动态结构显示出来。〔16〕

在信息主体利益与产业利益之间，本文认为，应以激励信息资源流通为首要价值目标。信息资源流通不仅是实现数据产品“赋值”和“增值”的基础，信息主体的数据安全也镶嵌在整个数据产业的发展之中。〔17〕然而，目前对于信息资源流通激励的呼声远少于对信息主体赋权的呼声，因此本文将激励信息资源流通作为数据产品利益格局衡量的首要价值目标，以期提升社会总福利。

三、汇集型数据产品的利益格局

（一）信息主体的利益

汇集型数据产品是指网络运营商对于原始数据进行简单汇集加工形成的产品。其已经具有区别于信息主体原始数据的形态、价值等，具有产品的属性。〔18〕虽然该类数据产品可能开发程度较低，但网络运营商也对其付出了劳动。在大数据时代，汇集型数据产品具有非常重要的价值，是支撑数据产业发展的基石。

---

〔11〕 参见龙卫球：《数据新型财产权构建及其体系研究》，载《政法论坛》2017 年第 4 期。

〔12〕 参见高富平：《数据生产理论——数据资源权利配置的基础理论》，载《交大法学》2019 年第 4 期。

〔13〕 在实践中，原始数据不仅可能来源于信息主体，也可能来源于公共领域，而原始数据的加工处理也可能有多方主体参与。为聚焦核心问题，本文将围绕数据产品的法律关系限定为最基础的法律主体之间，将数据产品的关涉主体简化成两大类，一类是提供原始数据的信息主体，一类是对原始数据进行生产、加工、分析、利用的网络运营商。

〔14〕 参见宋亚辉：《个人信息的私法保护模式研究——〈民法总则〉第 111 条解释论》，载《比较法研究》2019 年第2 期。

〔15〕 参见前引〔11〕，龙卫球文。

〔16〕 See Jerry Kang，Information Privacy in Cyberspace Transactions，50 *Stanford Law Review*，1193（1998）.

〔17〕 参见前引〔7〕，郝思洋文。

〔18〕 参见前引〔12〕，高富平文。

1. 信息主体主动创制信息

在大众点评软件中，用户点评聚合形成的用户平台，即为典型的汇集型数据产品。大众点评运营商并未对用户的点评数据进行分析处理，仅是使其按照一定顺序排列展示。信息主体通过录制、拍摄、汇编、制作等创制、创作形成的各类数据，构成这类汇集型数据产品的核心内容。这类信息不属于个人信息范畴，多是信息主体自愿的表达，其创作过程反映了信息主体的思想。为了保护信息主体的权益，鼓励信息的创作和传播，当其创作成果满足《著作权法》要求的构成要件时，其可以享有著作权。

然而，信息主体主动创制的信息能否成为“作品”，较难判定。以大众点评网中的用户点评为例，对上海汉涛信息咨询有限公司与爱帮聚信（北京）科技有限公司的系列纠纷，2008 年北京市海淀区人民法院一审认为，针对一个餐厅的点评内容即使存在感受、评价等方面的重复，但是因表达方式和能力不同，具有一定的独创性，属于作品范畴。〔19〕2009 年北京市第一中级人民法院二审认为，非常简单的用户点评难以达到法定的独创性要求，不构成作品；较为详细的用户点评，其中用于简单描述客观事实或观点的表达方式也非常有限，若给其著作权保护，会导致相关事实或观点被垄断。因此，其不必然构成作品。即使构成作品，因其包含大量对客观事实的简单描述，受《著作权法》保护的范围也非常有限。〔20〕在第二轮诉讼中，2011 年北京市海淀区人民法院再次重申其之前观点，认为因表达能力、角度、方式不同，在表现形式上体现作者的个性、情感、体验的评论，具有独创性，属于《著作权法》保护的作品。〔21〕

即使信息主体主动创制的信息不构成作品，其也属于言论表达范畴，信息主体也付出了一定的劳动，基于洛克劳动价值理论，显然信息主体对其享有法益。〔22〕但是，主动创制信息的商业价值离不开用户对数据的共享和企业的整合。企业并不是将收集到的数据简单相加，而是需要投入资金、技术，对数据进行进一步的分析、应用、共享、交换才能实现增值。从博客到微博再到大众点评，互联网时代人人都是数据的生产者，都在随时随地地共享信息，但是如果对其不能上升到著作权保护的高度，则这些数据单独仍不具备商业化条件，需要依赖企业的平台效用。因此，信息主体对其创制的信息享有的法益是其表达自由的积极自主利益以及不被整合滥用的消极利益。

2. 信息主体被动提供信息

除上述信息主体主动创制的信息外，汇集型数据产品涉及的信息也可能是信息主体为了从事某项活动或者接受某项服务而提供的个人相关信息，如身份、联系方式等。学界基本已达成共识，个人信息之上承载有人格利益、财产利益和公共利益。〔23〕这类信息显然与人格利益紧密相关。百度、腾讯、阿里巴巴、新浪等大型互联网公司的《隐私权政策》均表明，如果收集的个人

〔19〕 参见北京市海淀区人民法院（2008）海民初字第 16204 号民事判决书。

〔20〕 参见北京市第一中级人民法院（2009）一中民终字第 5031 号民事判决书。

〔21〕 参见北京市第一中级人民法院（2011）一中民终字第 7512 号民事判决书。

〔22〕 有学者基于自然权利理论和法律经济学理论证成个人信息财产权。参见邢会强：《大数据交易背景下个人信息财产权的分配与实现机制》，载《法学评论》2019 年第 6 期。由于个人信息财产权的生成仍然存在争议，因此本文在此仍使用“法益”的表达。

〔23〕 如高富平：《个人信息使用的合法性基础——数据上利益分析视角》，载《比较法研究》2019 年第 2 期；刘金瑞：《个人信息与权利配置——个人信息自决权的反思和出路》，法律出版社 2017 年版，第 138－139 页；杨惟钦：《价值维度中的个人信息权属模式考察——以利益属性分析切入》，载《法学评论》2016 年第 4 期。

信息包含个人特征信息或者结合后具有可识别性，均会进行匿名化处理。这同时也是法律的要求。〔24〕换言之，如果运营商收集的是人格紧密型个人信息，在开发汇集型数据产品时，会进行匿名化处理。如果不通过特别的技术处理，将无法通过数据产品识别出信息主体本人，信息的人格利益一般不会被触及，因商业性开发人格利益产生的财产利益也将无从谈起。

根据美国合理隐私期待理论的发展，在 United States v. Miller 一案中，美国联邦最高法院确立了“第三方原则”，即个人在自愿的情况下，将自己的信息和资料告知第三方，就已丧失合理的隐私期待了。因为信息主体对其信息可能被第三方以外的人知晓是可以预判的，其应该承担外人知晓的风险，从而失去了合理的隐私期待。〔25〕同理，在汇集型数据产品形成过程中，信息主体将其个人信息提供给运营商时，就已经丧失了合理的隐私期待，后续运营商在不违背法律和合同约定的情况下，如何开发利用和使用个人信息，已经不在信息主体的可控范围内。简而言之，被数据产品收集处理的个人信息背后承载的利益，仅是信息主体对其个人数据被他人收集、开发、利用的被动防御利益，以及不被整合滥用的消极利益。

（二）运营商的利益

互联网时代，运营商可以基于原始数据进行个性化业务定制、产品智能创新等。原始数据被视为竞争资源、企业的新资产。〔26〕本文认为，运营商基于合法方式，公开获悉收集信息主体的原始数据，并对其进行汇集性加工，形成的汇集型数据产品，网络运营商应该对其享有利益。

首先，根据法律规定，运营商按照规定的目的和方式收集个人信息，且被收集者对此知情同意，该行为不具有违法性。〔27〕基于合法方式收集并利用个人信息，网络运营商对于个人信息的取得不具有违法性。正如淘宝公司《隐私权政策》所宣示的，用户信息收集、使用的规则符合法律规定的“合法、正当、必要”的原则要求。〔28〕

其次，根据洛克的劳动价值理论，〔29〕劳动可以作为财产获得正当性的基础。个人信息是一种流动性资源，网络运营商收集这些个人信息，并对其进行汇集性加工，付出了大量的人力、物力、财力，最终形成的数据产品也并非自然领域的产物，而属于劳动创造的内容，因此赋予运营商对数据产品的利益符合劳动价值理论。但是囿于洛克但书规定，〔30〕运营商通过劳动获取权益的前提是，使原始数据脱离原始状态，即匿名化处理，同时其不能从中取出超出其能充分利用的部分，即不能侵占公共领域，确保其他企业也可以获得“足够多”和“足够好”的数据资源。

---

〔24〕 有学者对平台和应用的用户服务协议相关条款进行了汇总。参见侯媛：《反不正当竞争法视野下用户数据获取行为解读》，载《经济法学评论》2018 年第 1 期。

〔25〕 See United States v. Miller, 425 U. S. 435, 443 (1976).

〔26〕 参见前引〔23〕，高富平文。

〔27〕 参见《网络安全法》第 41 条之规定。

〔28〕 参见淘宝网：《隐私权政策》，载 https://terms.alicdn.com/legal-agreement/terms/suit_bu1_taobao/suit_bu1_taobao201703241622_61002.html?spm=a21bo.2017.1997523009.37.5af911d9cYf5SB，最后访问时间：2019 年 4 月 20 日。

〔29〕 参见〔英〕约翰·洛克：《政府论》（下篇），叶启芳、瞿菊农译，商务印书馆 1964 年版，第 20 页。

〔30〕 参见易继明：《评财产权劳动学说》，载《法学研究》2000 年第 3 期。

再次，由于数据的非排他性和非竞争性特征，数据产品的开发利用可能会陷入“公地悲剧”，运营商也会因此丧失继续参与数据产品开发的动力。根据激励理论，数据财产制度可以实现外部价值内部化，将非排他部分转化为排他部分。〔31〕因此，赋予运营商对数据产品一定的权益，运营商可以更有动力实施数据产品开发，推动企业研发大数据产品，从而促进社会经济发展。

最后，在大数据时代，运营商依靠数据创新发展俨然是一套完整的商业模式。尤其是，对于某些网络产品或服务，用户个人信息的提供有时是其功能实现所必不可少的。比如 Facebook 即可以控制信息主体从注册登录到在线发表，再到删除退出期间产生的所有信息，基于这些信息，运营商就可以进行定向营销或推送，以获取广告收入。

基于互联网企业的一般运营模式，数据已然成为运营商的一种商业资本。运营商依托该种商业模式实现自己收益的同时，也会增加消费者福利，促进国家经济结构转型。因此，为了更好运营该种商业模式，承认运营商对汇集型数据产品的法益是前提，也是必要条件。囿于本文研究框架，运营商对于数据产品是否享有权利等相关研究，在后文予以展开。

（三）平衡视角下的利益格局

基于上文分析，信息主体与运营商对于汇集型数据产品均享有利益。由于被汇集的信息种类不同，信息主体对汇集型数据产品的利益亦有所分别。当被汇集的数据构成“作品”时，信息主体对其享有著作权。但是，无论被汇集的数据是否构成“作品”，运营商都对汇集型数据产品享有利益。汇集型数据产品之上不同的利益格局，影响了产品的利益归属，进而决定了产品权益的行使主体和方式。

当信息主体主动创制的信息构成“作品”时，信息主体享有著作权，运营商对于数据产品仍享有积极自主的法益。类比“汇编作品”，汇编作品著作权人的权利行使，不能影响被汇编作品著作权人的权利。举重以明轻，根据利益位阶的衡量，运营商对数据产品的利益，不能影响信息主体的权益。当被汇集的数据是“作品”时，运营商需事先征得信息主体的同意，也即“知情同意原则”的适用。目前在运营商提供给信息主体的格式合同中，可能会包含一揽子授权协议，即信息主体将数据可能关涉的权利均授权或转移给运营商。〔32〕关于此类格式合同及知情同意原则适用的讨论已有很多，本文在此不再赘述。〔33〕

当信息主体主动创制的信息不构成“作品”时，信息主体享有表达自由的积极自主利益以及不被整合滥用的消极利益，其与运营商享有的积极自主利益如何衡平，则需考虑对公共利益的影响。正如上文的分析，主动创制的信息需要借助运营商平台，才能具有商业价值。并且，信息主体作为个体，其力量有限，难以与运营商或者第三方企业抗衡，很难维护自己的权益。因此，基于经济要素考量，在保护信息主体表达利益的前提下，应该更加重视对运营商和公共利益的维

〔31〕 参见石丹：《企业数据财产权利的法律保护与制度构建》，载《电子知识产权》2019 年第 6 期。

〔32〕 参见《美团点评平台用户服务协议》，载 https://rules-center.meituan.com/rules-detail/4，最后访问时间：2019 年 12 月 4 日。

〔33〕 如江帆、常宇豪：《个人信息保护中“知情同意”适用的困境与出路》，载《经济法论坛》2018 年第 2 期；田野：《大数据时代知情同意原则的困境与出路——以生物资料库的个人信息保护为例》，载《法制与社会发展》2018 年第 6 期；王文祥：《知情同意作为个人信息处理正当性基础的局限与出路》，载《东南大学学报》（哲学社会科学版）2018 年第 S1 期。

护。通过运营商开发的数据产品，公众有更多的机会和渠道接触和使用信息主体发布的信息，数据产品的运营流量也会因此增加，运营商也会更加注重数据产品的投资，保护信息主体的权益。简而言之，赋予运营商更多的运营利益，既有助于维护信息主体的权益，也可以促进信息资源的流动共享，实现数据产品的利益最大化。

当信息主体被动提供个人信息时，信息主体对其个人数据享有被他人收集、开发、利用的被动防御利益以及不被整合滥用的消极利益，相较于运营商的积极自主利益，处于利益位阶的下位。此时对于数据产品权益的行使，则可以由运营商主导。在实践中，运营商基本是通过格式条款来获取个人信息。国外很多学者运用社会交换理论阐释信息主体和运营商之间的营销互动。在电子商务环境下，信息主体将运营商对个人信息的收集看作一种交换投入，换取的回报则是运营商提供的服务、产品或者其他有价值的东西。〔34〕根据社会交换理论，信息主体会在提供个人信息之前进行成本—收益评估，预计信息的后续使用状况，并决定是否提供相应信息。根据调查，一般信息主体都会提供个人信息。〔35〕理论界对格式合同最主要的抨击在于无法有效保障信息主体权益，但事实上信息主体的人格权益和自我决定利益可以在个人信息及侵权法等相关法律体系下得到充分保护。〔36〕《合同法》对格式合同中双方交易能力的矫正实际上是对信息主体权益保护的锦上添花。

四、演绎型数据产品的利益格局

演绎型数据产品是指网络运营商对原始数据进行深度加工、演算分析后形成的数据产品。淘宝公司与美景公司纠纷中系争标的“生意参谋”即为典型的演绎型数据产品。相较于汇集型数据产品，演绎型数据产品已经识别不出原始数据，其是从数据中得出新知识、新发现，以做出预测性判断或者解决方案。〔37〕汇集型数据产品只涉及原始数据的“量”的积累，在演绎型数据产品中，原始数据的“质”已发生改变。

演绎型数据产品一般旨在发现分析对象的规律或预测未来趋势，因此其涉及的信息主体数据多是个人数字足迹信息，即特定个人使用计算机和网络的行为过程被网络服务记录下来而形成的行为轨迹或过程数据。〔38〕因为不具有“可识别性”，这类信息不属于个人信息范畴，并不直接关涉信息主体人格利益，更谈不上人格利益商业化利用产生财产利益。因此，参照上文的分析，信息主体对个人足迹信息不享有积极自主利益，只享有消极防御性利益。演绎型数据产品在经过深度加工演算后，已经无法识别出信息主体的原始数据，因此信息主体对于个人足迹信息的消极防御利益无法延伸至演绎型数据产品。此时信息主体对数据产品的利益，属于法律放任的

〔34〕 See Laurence Ashworth，Clinton Free，Marketing Dataveillance and Digital Privacy：Using Theories of Justice to Understand Consumers，67 *Online Privacy Concerns Journal of Business Ethics*，107，123（2006）.

〔35〕 参见刘金瑞：《个人信息与权利配置——个人信息自决权的反思和出路》，法律出版社 2017 年版，第 39－50 页。

〔36〕 Vgl. Thouvenin，Wem gehören meine Daten? Zu Sinn und Nutzen einer Erweiterung des Eigentumsbegriffs，SJZ 113/2017，S. 21，S. 25.

〔37〕 参见前引〔12〕，高富平文。

〔38〕 参见前引〔12〕，高富平文。

生活资源。〔39〕

当汇集型数据产品是演绎型数据产品的原材料时，本文认为，信息主体对汇集型数据产品的利益无法传递到演绎型数据产品层面。如果信息主体对被汇集的数据享有著作权时，在经过对原汇集型数据产品深度加工后，已形成全新的数据产品，无法从中识别出信息主体的独创性表达，信息主体不再享有著作权。另外，基于财产权客体自由让与的特征，信息主体行使支配权只能一次性用尽，在其个人数据以被他人收集或被转让的方式脱离自己的支配之后，数据主体无法控制其个人数据的后续使用和后续转让，也无法施加任何限制。〔40〕因此为了维护数据产品市场的有效运行，信息主体的权益不能追及于演绎型数据产品。如果信息主体对汇集型数据产品只享有法益时，经过多环节加工后，信息主体的利益已经被显著淡化。由于演绎型数据产品依附的是海量原始数据，产品加工转化后，信息主体难以在其中识别出自身利益。因此信息主体的利益仅及于汇集型数据产品这一环节，相关权益主张可以在该环节得以解决，其利益无须扩张至演绎型数据产品环节。言而总之，信息主体对演绎型数据产品的利益，属于法律放任的生活资源。

相较于汇集型数据产品，运营商生产开发演绎型数据产品需要付出更多的劳动，演绎型数据产品也因此具备很高的商业价值。黑庭格曾指出，劳动者只能得到其中劳动增值的部分，且劳动付出需要与劳动成果相匹配。〔41〕因此，基于洛克劳动价值理论，运营商付出的增值性劳动可以获得相应的权益保护，增值性劳动越多，享有的利益权能越高。因而相较于汇集型数据产品，运营商对演绎型数据产品享有的利益位阶更高。

简而言之，就演绎型数据产品而言，运营商享有积极自主利益，信息主体的利益则属于法律放任的生活资源。根据利益位阶衡量，运营商对演绎型数据产品享有独立自主利益，可以自行决定行使方式。

然而，在淘宝公司与美景公司不正当竞争纠纷案中，杭州互联网法院仍坚持“用户授权＋平台授权＋用户授权”的三重授权原则。〔42〕立法上也呈现出该趋势，《网络交易监督管理办法（征求意见稿）》规定，个人信息在流通过程中，需逐次同意。对于“三重授权”原则，学者莫衷一是。〔43〕本文并不认可“三重授权”原则。首先，“三重授权”原则源于信息主体的个人信息权利，但是目前关于个人信息的性质仍有争议，从中延伸出的授权内容，也无法令人信服。该原则仍困于个人信息权的窠臼之中，强调对信息主体权利的保护，而没有深入分析数据产品之上的利益格局。另外，“三重授权”原则受“知情同意”原则影响深刻，但合意虚化问题严重，立法不去矫正“知情同意”原则背后的交易能力不对称，而是一味深化甚至增加同意环节，无

〔39〕 我国台湾地区学者曾世雄教授根据生活资源本位的观点，将民法所涵盖之生活资源分为权利、法益及自由资源。参见曾世雄：《民法总则之现在与未来》，中国政法大学出版社 2001 年版，第 53－69 页。

〔40〕 See Julie E. Cohen, Examined Lives: Informational Privacy and the Subject as Object, 52 *Stanford Law Review*, 1373, 1391－1392 (2000).

〔41〕 See Edwin C. Hettinger, Justifying Intellectual Property, 18 *Philosophy & Public Affairs*, 52 (1989).

〔42〕 参见前引〔3〕。

〔43〕 如许可：《数据保护的三重进路——评新浪微博诉脉脉不正当竞争案》，载《上海大学学报》（社会科学版）2017 年第 6 期；徐伟：《企业数据获取“三重授权原则”反思及类型化构建》，载《交大法学》2019 年第 4 期。

疑是徒劳无功。

五、数据产品保护路径的类型化

法律对数据产品背后的利益进行调整已无争议。利益保护可采权利保护模式或行为规制模式，前者通过设定具体权利类型以涵盖相应利益，并将相应利益划归权利人享有，赋予权利人一般性的排他可能性，后者则是从他人行为控制的角度来构建利益空间，通过他人特定行为的控制来维护利益享有者的利益。〔44〕理论界多主张对数据产品采取权利保护模式。〔45〕然而，在司法实践中，针对数据产品产生的纠纷一般适用行为规制模式，即在《反不正当竞争法》下予以解决。如果对某一种类的数据产品利益格局的分析，主要考虑信息主体与运营商的利益平衡，那么对于数据产品的具体利益类型及其行使限制，则主要关涉运营商利益与公共利益之间的平衡。

在淘宝公司与美景公司不正当竞争纠纷案中，杭州互联网法院认为，由于我国目前未对数据产品的权利保护做出具体规定，基于“物权法定”原则，不能给予其财产所有权保护。〔46〕当利益并非法律已经规定的权利时，可以基于事物本质的相似性理论，考察能否将该项利益解释归入某种法律规定的权利类别。如果无法走通，则可以考虑私法或者公法上有无保护该种利益的规范。基于此种路径，可以打通权利保护模式和行为规制模式的界限，从而在一个更加广阔的背景上处理利益的保护问题，同时也可避免动辄在司法实践中创设新权利的风险。〔47〕本文即基于上述思路，在现有法律框架下探讨数据产品的保护路径。

（一）权利保护模式

当运营商对其生产开发的数据产品付出了很多投资时，运营商当然可以享有利益。是否给予这种利益以权利的保护模式，除了内在正当性外，还需考虑外在必要性，即需考虑对公共利益的影响。在现行法律体系下，财产权不仅包括物权，还包括知识产权等。〔48〕法律调整对象的性质决定法律制度的类别。由于数据产品与知识产权客体在性质上存在内在相似性，〔49〕对数据产品法律制度的选择，可以借鉴知识产权制度。运营商对数据产品付出的创造性劳动越多，对数据产品权益的独占性越高，越易受到权利法保护。根据法律对数据产品的权利保护程度高低，下文将依次介绍专利权保护模式、著作权保护模式及数据库特殊保护模式。

---

〔44〕 参见叶金强：《〈民法总则〉“民事权利章”的得与失》，载《中外法学》2017 年第 3 期。

〔45〕 有学者认为立法对数据产品规定了一种新型的财产权利，如程啸：《论大数据时代的个人数据权利》，载《中国社会科学》2018 年第 3 期；有学者主张数据产品类似数据库或汇编作品，对企业数据权益采取邻接权保护模式更为合理，如林华：《大数据的法律保护》，载《电子知识产权》2014 年第 8 期。

〔46〕 参见前引〔3〕。

〔47〕 参见方新军：《一项权利如何成为可能？——以隐私权的演进为中心》，载《法学评论》2017 年第 6 期。

〔48〕 目前很多学者撰文建议对企业数据财产赋权，如高富平：《信息财产——数字内容产业的法律基础》，法律出版社 2009 年版；但是同时也有很多争议，有学者认为，数据不应纳入民事客体范围，不宜作为独立财产，如梅夏英：《数据的法律属性及其民法定位》，载《中国社会科学》2016 年第 9 期。因此本文仅在现行法律体系下对数据产品的权利属性进行分析，并不涉及数据产品上新型权利的生成。

〔49〕 参见郑成思：《知识产权法》，法律出版社 2003 年版，第 127 页。

1. 专利权保护模式

当数据产品表现为数据加工处理形成的计算机软件或者技术方案时，可以考虑用专利权进行保护。对数据产品的专利权保护主要表现为计算机程序的专利保护。国家知识产权局在《大数据及其知识产权保护》报告中展示，我国大数据领域的专利包括：特别适用于特定功能的数字计算机设备或数据处理设备或数据处理方法；单个组中不包含的装备、设置、电路和系统等；专门适用特定经营的系统或方法等等。〔50〕

不同于著作权“思想、表达二分”的权利限制，专利权既可以保护计算机程序的算法，也可以保护依据该算法编写的程序代码。专利权赋予权利人的独占使用权，较之著作权更为强烈。然而，根据专利权“以公开换垄断”的思想，专利权仅保护权利人对专利信息的独占性使用，并不限制他人对信息内容的获取，他人可以对专利信息内容自由访问。

计算机程序的专利权保护需要满足相应的申请条件，即其需具有“新颖性、创造性、实用性”。互联网技术的高速发展导致现在代码开源盛行，反向工程接连不断，这些都给计算机软件的“三性”审查带来很大阻力。专利的审查流程复杂，审查周期长，并不利于计算机软件的实践应用，无法适应信息资源的快速流通诉求。

同时，计算机程序很容易与“智力活动的规则和方法”混淆。美国在司法实践中经常将作为数据产品的计算机程序认为是“在机器上运作的抽象概念和算法”，从而否认数据产品的“可专利性”。〔51〕我国《专利法》也规定，智力活动的规则和方法不授予专利权。在实践中数据产品所涉及并应用的特定算法或者计算机软件，其属性往往属于此种形式，不具备专利性。实践中对于获得专利的大数据相关技术的类型和应用目的的统计结果也印证了这一观点。〔52〕

2. 著作权保护模式

（1）演绎型数据产品

运营商开发的演绎型数据产品，一般表现为偏好分析等类似研究报告的可视化数据内容。此时，数据产品完全脱离于原始数据，以期适应市场需求和用户体验，当其符合《著作权法》要求的“独创性”时，运营商可以对其享有著作权。

如果演绎型数据产品背后的数据代码的表达方式达到“独创性”标准，则可成为著作权的保护客体，即计算机软件。计算机软件指计算机程序及有关文档，其可以是具体的程序作品，也可以是特定问题的技术解决方案。计算机软件程序实质是算法设计思想代码化的过程，软件思想与表达此时混合在一起，难以区分。《著作权法》强调“思想、表达二分”，即只保护计算机软件的表达方式。然而，运营商构思的算法，作为计算机软件的核心，却不能被《著作权法》保护。显然，根据《著作权法》对计算机软件进行保护，范围过窄，保护程度太低。

如果演绎型数据产品是运营商应用特定计算机软件生成的产物，则需讨论计算机软件生成物

〔50〕 参见国家知识产权局：《大数据及其知识产权保护》，载 http://www.sipo.gov.cn/gwyzscqzlssgzbjlxkybgs/zlyj_zlbgs/1062627.htm. 最后访问时间：2019 年 12 月 4 日。

〔51〕 See Mayo Collaborative Service v. Prometheus Laboratories Inc.，132 S. Ct. 1289（2012）；Alice Corp. v. CLS Bank Int'l.，134 S. Ct. 2347（2014）.

〔52〕 参见徐实：《企业数据保护的知识产权路径及其突破》，载《东方法学》2018 年第 5 期。

的可“作品”性。《著作权法》仅保护人类的智力创作成果，机器或者程序产生的产品，并非由人类直接创造。在司法实践中，已有案例回应计算机软件智能生成内容的著作权问题。

在北京菲林律师事务所与北京百度网讯科技有限公司著作权侵权纠纷案中，北京互联网法院认为，作品应由自然人创作完成。在相关内容的生成过程中，软件研发者（所有者）和使用者的行为并非创作行为，相关内容并未传递二者的独创性表达，因此该内容不能构成作品。〔53〕

无论计算机软件本身是否能成立著作权，使用功能性应用软件开发的生成物都不能作为汇编作品进行保护，因为存在思想与表达的混同。相反，如果不同的运营商就相同范围的数据使用该软件无法获得基本相同的生成物，则说明该计算机软件掺杂有人的个性化主观判断，存在个体差异，思想与表达并未混同，该生成物可以作为作品加以保护。〔54〕当然，如果计算机软件具有深度学习等类人工智能的功能，并基于此生成产物，则落入人工智能生成物的研究范畴。本文在此不再展开论述。〔55〕

（2）汇集型数据产品

相较于演绎型数据产品，运营商对于汇集型数据产品付出的劳动相对较少，且其权益的行使，仍需顾及信息主体的权益，所以其对汇集型数据产品享有的权能不如对演绎型数据产品享有的权能完整。但是，无论被汇集的数据是否构成“作品”，当汇集型数据产品对于数据的选择、编排具有“独创性”时，其可构成《著作权法》中的“汇编作品”。此时受《著作权法》保护的是独创性编排表达，并不是构成数据产品的数据本身。〔56〕运营商仅有权排除他人对汇集型数据产品整体结构的复制、传播，不能禁止其他主体对汇集型数据产品中的信息或数据的利用。

另外，汇集型数据产品的“独创性”认定标准尚无定论，存在争议，在上海汉涛信息咨询有限公司与爱帮聚信（北京）科技有限公司的系列纠纷中，2008 年北京市海淀区人民法院一审认为大众点评通过收集、选择和编排，将点评内容汇集成一个整体信息，大众点评对其享有汇编作品的著作权。〔57〕2009 年北京市第一中级人民法院认为，网友点评内容系按照时间顺序排列，此种排列方式不具有独创性，大众点评不享有汇编作品著作权。因此，对于汇集型数据产品“独创性”的认定还需考察被汇集的数据在选择、编排上的特殊性。〔58〕

3. 数据库的特殊保护模式

《欧盟数据库指令》给予非独创性数据库以“特殊权利”（sui-generis right）保护，只要数据库制作人在数据库要素的选取、审核、呈现上进行了实质性投入，就可获得特殊权利的保护。〔59〕实际上，非独创性数据库的特殊权利保护模式还是对早期“额头流汗原则”的继承，只要作品中

〔53〕 参见北京互联网法院（2018）京 0491 民初 239 号民事判决书。

〔54〕 参见王迁：《论汇编作品的著作权保护》，载《法学》2015 年第 2 期。

〔55〕 相关研究如孙山：《人工智能生成内容著作权法保护的困境与出路》，载《知识产权》2018 年第 11 期；孙建丽：《人工智能生成物著作权法保护研究》，载《电子知识产权》2018 年第 9 期；李晓宇：《人工智能生成物的可版权性与权利分配刍议》，载《电子知识产权》2018 年第 6 期。

〔56〕 Lothar Determann，No One Owns Data，70 UC Hastings Research Paper，19（2018）.

〔57〕 参见前引〔19〕。

〔58〕 参见前引〔20〕。

〔59〕 参见王镭：《“拷问”数据财产权——以信息与数据的层面划分为视角》，载《华中科技大学学报》（社会科学版）2019 年第 4 期。

体现了作者的“劳动”，就应当认为该作品具有独创性。〔60〕

依据该制度，权利人拥有对数据库全部或实质部分的提取权和再利用权。2004 年欧盟法院在 British Horseracing Board v. William Hill 一案中明确特殊权利只保护为了自己业务需要创作数据库而进行的数据选择、编排等，对于某一具体数据的生产投入并不受保护。〔61〕欧盟法院通过适用副产品理论（spin-off theory）区分运营商对数据选编的投入和对数据库创造的投入。〔62〕因此，特殊权利的保护模式仍然不能及于作为构成要素的每个数据本身。从利益衡量的角度，特殊权利制度依然旨在维护信息资源的流动，防止数据垄断。

目前我国没有专门的权利立法规定对于数据库投资的保护。在司法实践中，法院通过适用《反不正当竞争法》对非独创性数据库进行保护。如北京阳光数据公司与上海霸才数据信息有限公司技术合同纠纷案。〔63〕因此，我国仍坚持传统的《著作权法》的立法目的，对于不满足独创性要求的数据库，没有采用权利保护模式，而是采用行为规制模式，对此下文将展开论述。

4. 权利保护模式评析

信息的实质在于流动，自由流通的信息是科技发展、经济进步的动力，相比于有形财产而言，对基于无形数据发展而来的数据产品赋予财产权，需要权衡对信息自由流通及其他公共利益的影响。因此，如果运营商想对数据产品享有相关权利，必须满足权利授予的严苛条件，如著作权的“独创性”等。即使被赋予相关权利，在数据产品保护和防止数据垄断之间，运营商对数据产品权利的行使也会受到诸多限制。如囿于著作权“思想、表达二分”，无法给予数据产品以完整保护。简而言之，正如田村善之教授认为的知识产权制度是“行为规制物权化”的方法，〔64〕知识产权不强调对客体的圆满控制，而是在对客体的特定使用行为上架构利益空间。〔65〕

通常认为，权利保护模式可以提供更周全的保护力度，然而技术规范并非如此。对于数据产品的侵权很难举证，所以容易应用到法定赔偿制度。《著作权法》的法定赔偿额度最高为 50 万元，而修订后的《反不正当竞争法》规定的法定赔偿额度则是最高为 300 万元。就此而言，反而是行为规制法提供的保护力度更大。

（二）行为规制模式

正如上文所述，数据产品的权利保护模式在某些情况下存在一些局限性。同时，运营商对某些其生产开发的数据产品的利益可能由于客体不确定、支配性不强或者排他性不足等原因并不适宜权利化，或者由于价值位阶不高而无法得到权利化，〔66〕因而此时运营商对数据产品的利益更适宜采取行为规制模式，包括一般侵权行为制度和类型化的《反不正当竞争法》。数据产品的开

〔60〕 参见郑成思：《知识产权论》，社会科学文献出版社 2007 年版，第 208 页。

〔61〕 See British Horseracing Board v. William Hill, case C－203/02 (2005).

〔62〕 Malte Grützmacher, Dateneigentum-ein Flickenteppich, 8 Computer und Recht, 485, 495 (2016). 转引自前引〔59〕，王镭文。

〔63〕 参见北京市高级人民法院（1997）高知终字第 66 号民事判决书。

〔64〕 参见〔日〕田村善之：《知识产权法的理论》，李道道译，载吴汉东主编：《知识产权年刊》（创刊号），北京大学出版社 2005 年版，第 32 页。

〔65〕 参见吕炳斌：《个人信息权作为民事权利之证成：以知识产权为参照》，载《中国法学》2019 年第 4 期。

〔66〕 参见王镭：《电子数据财产利益的侵权法保护——以侵害数据完整性为视角》，载《法律科学》2019 年第 1 期。

发与应用日益成为当前互联网行业的主要商业模式，是运营商获取市场竞争优势的重要方法。运营商基于数据产品开发产生的财产利益是产生纠纷的根本原因，也是阻却其他企业不当攫取数据的正当性基础。因此，本文仅在此讨论《反不正当竞争法》对数据产品利益的调整。

数据产品俨然已成为运营商的重要经营资源，无论其权利属性如何，均承载着重要的财产利益属性。在司法实践中，法院没有因数据权属不明和权利类型不清晰影响判断，而是灵活地避开权属认定难题，承认运营商对其开发的数据产品享有财产权益，在《反不正当竞争法》项下进行调整。〔67〕

竞争法的立法目标在于保护自由竞争和维护消费者利益。〔68〕根据运营商与信息主体之间的相关协议，运营商不仅要合法获取用户信息，同时还要妥善保存并使用它们。因此在《反正当竞争法》项下对数据产品进行保护，同样可以实现信息主体利益、运营商利益和公共利益之间的平衡。

1. 一般条款规制模式

虽然法院目前普遍运用一般条款进行裁判，但是学界多认为广泛适用原则性条款会有一些问题，比如一般条款调整模糊、适用不稳定，法院无法统一认定诚实信用原则和商业道德等内容。〔69〕法院适用《反不正当竞争法》第 2 条，不仅是对《反不正当竞争法》立法宗旨和一般条款核心意旨的诠释过程，亦是在包容性、开放性和不确定性之间寻求平衡的过程。〔70〕换言之，一般条款由于具有模糊性，才更易根据个案进行利益平衡。同时，有的法院根据互联网行业中数据产品技术形态和市场竞争模式与传统行业存在的显著差别，为保障新技术和市场竞争模式的发展空间，创新提出一般条款的适用条件。

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，北京知识产权法院认为，除了最高人民法院在（2009）民申字第 1065 号民事判决书中提出的适用《反不正当竞争法》第 2 条的认定条件外，还应满足以下三个条件：第一，该竞争行为所采用的技术手段确实损害了消费者的利益；第二，该竞争行为破坏了互联网环境中的公开、公平、公正的市场竞争秩序，从而引发恶性竞争或者具备这样的可能性；第三，对于互联网中利用新技术手段或者新商业模式的竞争行为，应首先推定其具有正当性，不正当性需要证据加以证明。〔71〕

诚然，原则性的一般条款更具灵活性，可以方便法院于个案中在数据产品权益保护和信息自由流动之间进行利益权衡。但是，为保障新技术和市场竞争模式的发展空间，法院在互联网大数据行业中适用一般条款时应秉承谦抑的司法态度。

2. 商业秘密条款规制模式

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，新

〔67〕 参见曾雄：《数据不正当竞争纠纷的司法实践——现存问题与解决路径》，载《信息安全与通信保密》2018 年第 11 期。

〔68〕 参见陈兵：《反垄断法实施与消费者保护的协同发展》，载《法学》2013 年第 9 期。

〔69〕 参见刘继峰：《论用户数据的竞争法保护路径》，载《价格理论与实践》2018 年第 3 期。

〔70〕 参见郑友德、伍春艳：《论反不正当竞争法的一般条款——兼论〈反不正当竞争法〉（修订草案送审稿）第二条的完善》，载《电子知识产权》2016 年第 6 期。

〔71〕 参见北京知识产权法院（2016）京 73 民终 588 号民事判决书。

浪微博提出的诉讼观点之一是用户数据属于商业秘密。但是法院对此没有给予正面回应。〔72〕在衢州万联网络技术有限公司与周慧民等侵害商业秘密纠纷案中，法院认为，网站数据库中的用户信息，能为运营商带来经济利益且具有实用性，不易为相关领域人员普遍知悉和容易获得，且已采取了保密措施，故上述信息符合商业秘密的构成要件。〔73〕

数据产品作为商业秘密被保护，应符合其构成要件。商业秘密要求的“不为公众所知悉”与信息资源的流动开放特性可能存在不兼容。例如，在汇集型产品中，被汇集的事实类数据多来自公有领域，任何人均可以从公开渠道获悉。但是，数据产品作为整体，不应该将其人为割裂分析，“商业秘密”是要求数据产品作为整体具有秘密性。

2019 年《反不正当竞争法》修订时，将该要件的举证责任转移给了侵权人。同时，在司法实践中，也出现了一系列数据库表、存储过程、源代码文件等被认定为商业秘密的案例。〔74〕随着司法实践对商业秘密认定不断倾向作宽泛解释，通过主张商业秘密保护数据产品具有可行性。

3. 互联网专条规制模式

在 2017 年《反不正当竞争法》修订时，新增的第 12 条被称为“互联网专条”，拟将互联网领域的纠纷类型化纳入不正当竞争视野中。该条第 2 款的前三项都是从典型案件中抽象出来的规则。兜底条款的规定是为了给未来出现的新型不正当竞争案件留下适用空间。但是目前尚无适用互联网专条裁判数据产品纠纷的案件。有学者认为法院没有适用《反不正当竞争法》第 12 条，而是适用第 2 条的原因是，原告希望依据第 2 条认定被告行为违法，并以此确认相关数据权益，从而获得相应补偿。〔75〕

但是，与《反不正当竞争法》一般条款类似，互联网专条的兜底条款也具有适用标准不清晰等问题。有学者认为，互联网专条的兜底条款更具有针对性，与数据产品纠纷更契合，适用该条款可以防止一般条款范围的不断扩大，分解一般条款的适用压力。〔76〕但是，本文认为，并未被直接列举规定的数据产品纠纷同样存在兜底条款适用模糊的问题，而且，兜底条款并不能适用于所有数据产品纠纷，具体的司法适用条件仍需要在个案中予以明确提炼。

4. 行为规制模式评析

相较于权利保护模式，行为规制模式无法提供完整排他的数据产品权益保护。《反不正当竞争法》只能提供法益层面保护和消极保护，运营商无法基于数据产品正面设计权利，如设定抵押等。另外，《反不正当竞争法》只能调整经营者之间因为不正当竞争而产生的数据产品纠纷，相应地，对于行为人的约束也限定为立法列举的类型。

但是，通过行为规制法调整，更有利于数据产品各方利益的平衡。《反不正当竞争法》的制度价值并不在于保护某个经营者的具体利益，而在于通过对不正当竞争行为的认定和规制实现保

〔72〕 参见前引〔71〕。

〔73〕 参见上海市高级人民法院（2011）沪高民三（知）终字第 100 号民事判决书。

〔74〕 如“北京何晨亮等人侵犯商业秘密案”，参见北京市海淀区人民法院（2013）海民初字第 15447 号民事判决书。转引自前引〔17〕，郝思洋文。

〔75〕 参见前引〔67〕，曾雄文。

〔76〕 参见前引〔69〕，刘继峰文。

护市场经济发展的目标。因此，《反不正当竞争法》必须落实多元利益保护的立法目的，在经营者利益、竞争利益、消费者利益之间寻求平衡保护。利益的冲突根源于制度的价值取向，而这又是一个随社会发展而不断变化的过程。因此，更具灵活性的行为规制法更具活力。法院通过合理解释行为规制法的原则性条款和类型化条款可以权衡各方利益冲突，实现利益之间的和谐共生，顺应社会的发展方向。这一点对于发展中国家尤其重要。行为规制法的能动性不仅体现在对利益的权衡上，还可以体现在对其他法律的不足予以弥补上。因为行为法提供“宽保护”，所以其可以成为各个法律之间协调联系的纽带，促使整个法律体系的和谐发展。

六、结　论

《国家信息化发展战略纲要》指明：“信息资源日益成为重要的生产要素和社会财富。”在信息时代，大数据持续激发商业模式创新，不断催生新业态，已成为互联网等新兴领域促进业务创新增值、提升企业核心价值的重要驱动力。单个数据不具备商业化条件，被运营商开发利用形成的数据产品才会产生巨大的经济价值。

本文对数据产品采取广义界定，即数据产品是网络运营商对于信息主体的原始数据进行生产加工处理后形成的产品，根据数据处理形式的不同，数据产品可以分为汇集型数据产品和演绎型数据产品，不同种类的数据产品依附的利益格局有所不同。

信息主体和运营商对汇集型数据产品均有利益，但根据不同利益的位阶衡量，汇集型数据产品的权益仍应由运营商行使，但其应注意对信息主体权益的保护；不同于此，信息主体对演绎型数据产品已无法定权益，所以运营商可以独立自主使用演绎型数据产品。

对具体某种数据产品的利益格局分析，主要考虑信息主体和运营商的利益平衡。但是，针对运营商对数据产品享有利益类型的判断及其行使，则主要关涉运营商利益与公共利益之间的平衡。运营商对数据产品的利益支配性越弱、利益位阶越低，其利益受财产法律调整保护的力度相应越弱。

由于数据产品与知识产权客体在性质上存在内在相似性，因此对数据产品法律制度的选择，可以借鉴知识产权制度。当数据产品满足《专利法》规定的“新颖性、创造性、实用性”时，运营商可以对其享有专利权。当数据产品符合《著作权法》要求的“独创性”时，运营商可以对其享有著作权。目前我国没有专门立法规定对数据库投资的保护。在司法实践中，法院通过适用《反不正当竞争法》对非独创性数据库进行保护。

相较于权利保护模式的严苛条件，行为规制模式更为灵活。数据产品的《反不正当竞争法》适用存在三种可能路径：第 2 条一般条款、第 9 条商业秘密条款、第 12 条第 2 款第 4 项（互联网专条的兜底条款）。在司法实践中，具体的类型化条款，应优先于一般条款予以适用。

我国没有对数据产品提供全方位的财产权保护，而是根据不同类型的数据产品，提供不同程度的保护，多头并举。权利保护模式和行为规制模式并不矛盾，二者相互独立的同时，对于无法达到权利保护模式要求的数据产品，行为规制模式提供基础保护。正如郑成思教授引述的国外学者的经典比喻，“专利法、商标法、版权法是浮在海面的冰山，反不正当竞争法是下面托着这三

座山的海水”〔77〕，面对数据产品这一新型事物，在探究法律对其合适的保护路径时，根据制度选择原理，应优先遵循已有法律框架的制度设计。

Abstract：Data products are products formed by the operator's production and processing of the original data of the information subject. According to different data processing forms, data products can be divided into collective data products and deductive data products. Based on the analysis of the interest pattern of various data products, the interests of collective data products should be exercised by operators, but attention should be paid to the protection of the interests of information subjects. Unlike this, the information subject can no longer determine the interests in deductive data products, so operators can exercise product interests independently. The lower the operator's interest level in data products, the weaker their interest is protected by property law adjustments. Based on the trade-offs between the operator's interests and the public interest, when data products apply the right protection model, they must meet the relevant conditions for granting rights. For data products that fail to meet the right protection model, the behavior regulation model provides basic protection. For the protection of data products, the two models are independent of each other and complement each other.

Key Words：data products, rights, interests, rights protection mode, behavior regulation mode

（责任编辑：武　腾　赵建蕊）

〔77〕 前引〔49〕，郑成思书，第479页。

财经法学 No. 3，2020
pp. 150 - 160

大数据时代日本个人信息保护法探究

张　红*

内容提要：个人信息本来是极其隐私的事物，在大数据时代却时刻处于“裸奔”状态，时刻面临被侵犯的风险。特别在新冠肺炎疫情防控中，大数据技术发挥了重要作用，个人信息保护再次引起关注。整体而言，日本个人信息保护法以“个人优先”与“公共优先”的宗旨博弈为出发点，以“个人信息”的概念界定为基础，以个人信息权的保护为核心，以个人信息保护机构的独立设置为落脚点，为个人信息的保护奠定了基础。我国应当积极行动起来，尽快颁布《个人信息保护法》，助力大数据时代个人信息保护和数字经济的发展。

关键词：个人信息　《个人信息保护法》　大数据时代　新冠肺炎疫情

当今社会，大数据以及与之相关的互联网、云计算、区块链等接踵而来，谓之大数据时代，它改变着社会生活的方方面面。大数据的价值在于对包括个人信息在内的海量数据的整合提升、宏观把控。现实中，个人信息侵权严重，如过度收集个人信息、擅自披露个人信息、非法买卖个人信息。在日本如此，在我国也如此。在2020年新冠肺炎疫情中，大数据技术被充分运用，诸如有效治疗药物的统计、人员流动的统计与分析。与此同时，个人信息保护也出现一些新问题，亟待法学界和立法者的关注。可以说，解决大数据时代的个人信息侵权问题迫在眉睫，个人信息保护的法律制度要随之革新并不断完善。

长期以来，日本社会逐渐形成三元法律体系。一是公法，其中实体法如宪法、行政法、刑事法等，程序法如民事诉讼法、行政诉讼法、刑事诉讼法等。二是私法，如民法典、商法典、公司法、金融商品交易法等。三是社会法，如劳动法、社会保障法、经济法、健康保险法等，也包括个人信息保护法。亦即，日本个人信息保护法突破了传统公法与私法的界限，属于社会法的范畴。本文将在大数据时代背景下，结合新冠肺炎疫情应对状况，围绕日本《个人信息保护法》（Act on the Protection of Personal Information，APPI），探讨2020年日本内阁批准修改的新法案，相应考察个人信息保护的立法体系、当代学术研究、焦点问题及典型判例，为我国立法提供有益参考。

* 张红，日本国立冈山大学法学部教授。

本文为2018年国家社科基金重大项目“大数据法制立法方案研究”（18ZDA136）的阶段性成果。

一、日本个人信息保护立法体系考察

2003年日本参议院通过了《个人信息保护法》，同年又通过了《独立行政法人等个人信息保护法》。2017年，日本大幅度修改了《个人信息保护法》，并于2020年3月由内阁批准新的修正案，如日本议会批准则将在2021年生效。2019年，日本还修改了《独立行政法人等个人信息保护法》。〔1〕在此之前，日本在1999年还曾通过了《行政机关个人信息保护法》。这意味着日本构筑了一个相对完整的以《个人信息保护法》为基本法，各部门单行法补充的法律体系。亦即，对国家机关、地方公共团体、行政机关、独立行政法人等分别制定了不同的法律法规。

日本《个人信息保护法》（日语名称为：個人情報の保護に関する法律）以个人信息的有效利用及其保护为对象，确立了个人信息保护的基本理念和原则，明确了国家和地方公共团体的职责以及使用个人信息的企事业单位应履行的义务，目的在于协调个人信息的有效利用和个人权益保护之间的平衡。该法共88条，分为：总则（目的和基本理念）、国家及地方公共团体的责任和义务、保护个人信息的措施、个人信息处理业者的义务、个人信息保护委员会的职责、杂则（适用范围）、罚则（违法责任）等内容。

日本个人信息保护立法体系请见图1。

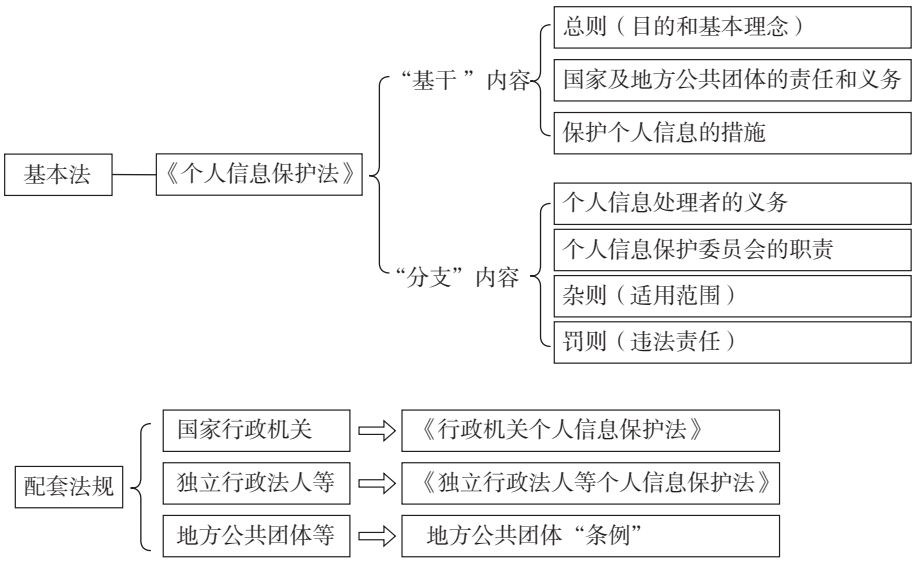

图1　日本个人信息保护立法体系概要示意图

（一）日本《个人信息保护法》的立法宗旨

日本《个人信息保护法》的立法宗旨可从以下四个层面加以论证。一是适应信息社会的高速发展。大数据时代下信息社会的高度发展，难免引发个人信息侵权问题。单纯保护个人信息安全，难免阻碍信息社会的高速发展；单独推进信息社会的高速发展，又难免牺牲个人信息安全。2020年新冠肺炎疫情，日本也比较严重，相关个人信息保护与披露存在着一些新问题，更加证

〔1〕参见日本法务省专员，「情報公開・公文書管理・個人情報保護」，载http://www.moj.go.jp/disclose_index.html，最后访问时间：2020年3月26日。

明日本《个人信息保护法》与其相关配套措施是正确的，可以适应信息社会的高速发展。

二是个人信息的适当处理、有效利用。“适当处理”强调个人信息处理的适当性，既非故步自封、自我屏蔽，也非毫不节制、肆无忌惮。在应对新冠肺炎疫情背景下，如何才是“适当”，众说纷纭，有待进一步判定。“有效利用”强调个人信息利用的有效性，体现利用的效果。有效也同样难以量化，如何才是“有效”，有待进一步判定。

三是对新兴产业、经济社会、国民生活的促进。新冠肺炎疫情中的个人信息保护与披露，有助于国民健康、社会发展。这是从“个人”走向“公共”的过程。强调“新兴产业”，说明了与大数据相关产业的重要性。强调“经济社会”，说明了个人信息保护与经济社会发展密切相关。强调“国民生活”，说明了个人信息保护对整个国民生活权益都有至关重要的影响。

四是充分保护个人合法权益。不得假借类似新冠肺炎疫情的名义，非法披露个人信息。具体而言，个人信息是个人合法权益的基本组成部分，保护个人信息就是为了保护个人合法权益。

（二）日本个人信息保护的立法动态

2017 年日本为确保信息流通的可追溯性，〔2〕加强国家监管部门对个人信息一元化的管理，大幅度修改了《个人信息保护法》。

一是增加“敏感信息”概念。所谓“敏感信息”是指有关政治观点、宗教（宗教思想和信仰）、工会会员、种族和民族以及出生地和住所、医疗保健、性生活、犯罪记录信息等信息。〔3〕二是新增加“个人信息保护委员会”一章，即第 59－74 条。该章主要规定个人信息保护委员会的设置、任务、职权行使的独立性、委员长、专门委员、任期、身份保障、罢免、事务局、会议、保密义务、规则制定等事项。三是增加“非法提供信息数据库罪”。所谓“非法提供信息数据库罪”是指从事个人信息处理业者或从事与其相关数据库业务的法人（包括高管人员、管理人员在内的非法人团体），为自己或第三人谋求不正当利益，而提供或盗用其业务处理过的个人信息数据库（包括对其部分或全部信息的复制、加工）的，处一年以下有期徒刑或 50 万日元以下罚款。〔4〕

2020 年《个人信息保护法》修正案为迎合大数据时代技术创新的要求，防范和化解未来个人信息保护中潜在的各类风险，扩充了很多内容，如：保障个人权利；信息使用推广；扩大企业责任；强化法律处罚；增加域外适用等。其中，保障个人权利涉及权利范围、个人信息范围、第三方限制等；信息使用推广如引入“假名化信息”，但仅限于经营者内部使用，并禁止向第三方提供假名化信息；扩大企业责任如信息泄露报告、限制不正当使用；强化法律责任如增加罚款；域外适用如赋予个人信息保护委员会（PPC）更多权力、加强国际传输监管。

日本《独立行政法人等个人信息保护法》（日语名称为：独立行政法人等の保有する個人情報の保護に関する法律）是在独立行政机构对个人信息的使用日益增加的背景下制定的。该法明确了有关独立行政机构等对个人信息处理的基本事项及独立行政机构等未识别加工处理的信息，以确保独立行政机构等的正常运行。该法共 54 条，分为：总则；独立行政机构等个人信息处理；个人信息文档；公示、更正、停止利用；独立行政机构等非识别加工处理的信息提供；杂则；罚

〔2〕 曽我部真裕「個人情報保護法とメディア」マスコミ倫理 695 号（2017 年）2 頁参照。

〔3〕 渡邉雅之『これ一冊で即対応平成 29 年施行改正個人情報保護法 Q&Aと誰でもつくれる規程集』第一法規（2016 年）80 頁参照。

〔4〕 ITメディア「改正個人情報保護法案が閣議決定データベース提供罪創設『ビッグデータ』活用へ規定整備」，载 https://www.itmedia.co.jp/news/articles/1503/10/news143.html，最后访问时间：2020 年 4 月 12 日。

则；附则。

日本《行政机关个人信息保护法》（日语名称为：行政機関の保有する個人情報の保護に関する法律）主要是考虑到行政机关越来越多地使用个人信息，对如何安全准确处理个人信息（包括未识别正处理的信息）做出了明确规定，目的在于保护个人信息的同时，还要保护个人信息权益。该法共57条，分为：总则；行政机关持有的个人信息处理；个人信息文档；公示、更正、停止利用；行政机关非识别加工信息的提供；杂则；罚则；附则。

二、日本学者对个人信息保护法的研究

日本学者很早以前就以个人信息保护法为对象进行了深入调查和研究，并且已经取得了一定的成果。

关于“个人信息”的界定。一种观点认为，“个人信息”是指生存人的姓名、性别、出生日期等基本信息，即可识别出特定个人的基本信息。〔5〕另一种观点认为，“个人信息”除了个人基本信息以外，还包括文件、图纸或电磁记录、语音、动作或其他方法等便于识别特定个人的信息〔6〕。

关于企业对个人信息的保护。日本有学者认为，企业掌握着大量的客户个人信息包括个人隐私，如何正确使用相关信息，〔7〕特别是在企业的国际化趋势之下，如何防止非法泄露，是一个极为重要的课题。

关于医学需要特别注意的个人信息。2004年，日本文部科学省、厚生劳动省、经济产业省三家政府机构，专门制定了医学研究领域个人信息的指导方针。此指导方针（日语名称为：医学研究等における個人情報の取り扱いの在り方等について2004年）遵循言论自由、尊重人权、个人信息有效利用三大原则，要求特别注意保护最前沿技术方面医学研究的相关个人信息。日本学者指出，如利用基因治疗特殊病种的有关病人信息、记录等，未经同意不能泄露给第三方，如在不得已交付第三方的情况下，要保证第三方给予适当保密管理。〔8〕

关于个人信息保护立法革新的建议。日本学者认为，在个人信息充分利用的同时，需要注意不经本人同意不得提供给第三方。特别是要探讨协调个人信息的一般处理与行政处理之间的信息统一、国家行政机关与地方公共团体的信息统一、个人信息处理的内涵和外延、未成年人信息的处理、基于医疗需要对个人信息的特别保护、欧美等国际其他地区有关个人信息的新动向研究、课税导入、法律执行的强化等方面的问题。〔9〕

关于个人信息保护立法的配套法律修改。日本学者认为，2017年《个人信息保护法》的修

〔5〕佐藤一郎「ビックデータと個人情報保護法データシェアリングにおけるパーソナルデータの取り扱い」情報管理58号（2016年）828－834頁参照。

〔6〕Ikuko Komachiya「ぼちぼち改正個人情報保護法を読む2条（定義：個人に関する情報・個人識別性）」Information Law（2017年）10頁参照。

〔7〕川口嘉奈子「個人情報保護法で保護されないプライバシーに対する企業による配慮の重要性」（人）概念の再検討（2015年）25－36頁参照。

〔8〕米村滋人「医学研究における個人情報保護の概要と法改正の影響」NBL 1103号（2017年）6－15頁参照。

〔9〕関啓一郎「特集：いよいよ本格化するパーソナルデータの利活用———個人情報保護法とその10年ぶりの改正について」知的資産創造（2015年）6－29頁参照。

改，要求其他法律也随之进行配套修改。如《个人信息保护法》第 15 条规定，个人信息处理业者在处理个人信息时，必须尽可能将其利用目的加以特定（第 1 项）。在个人信息处理业者变更其利用目的时，不得超出（被合理地认定为）变更前的利用目的（具有相当关联性的）和范围（第 2 项）。而日本《民法》第 548 条规定：（1）就解除权的行使没有规定期限时，有关人员可以在规定期间内，催告该人行使解除权。如在规定期间内没有接到解除通知的，则放弃解除权。（2）因自己的行为或过失，显著毁损合同标的物或致不能返还其物时，或因加工、改造将其物变为他种物时，其解除权消灭。（3）合同标的物，非因解除权人的行为或过失而消灭或毁损时，解除权不消灭。因此，《个人信息保护法》要求个人信息处理业者变更其利用目的时，不得超出变更前的利用目的（具有相当关联性的）和范围。《民法》要求在相对期间，相对人可以催告解除权人在该期间内作出是否解除的确认。两法相互矛盾，需要加以配套修改。〔10〕

笔者认为，日本现有研究依然存在着三大不足需要解决：一是现有研究遍及个人信息保护法的方方面面，但没有内部的逻辑牵引，本文将从出发点、基础、核心、落脚点逐层递进加以探讨。二是由于不同国家的政治经济等背景不同，需要加强分析、探讨，但还是有很多不足。因而本文在对日本个人信息保护法论证的基础上，提出对我国的立法期许，以供参考。三是极其缺乏在大数据时代和重大疫情背景下全新思考个人信息保护的法律问题，这是世界各国（包括中日两国）都面临的问题，正是本文研究的立足点。

三、日本个人信息保护法的焦点思考

（一）以“个人优先”与“公共优先”的宗旨博弈为出发点

日本个人信息保护法有四个基本宗旨，但归根到底是“个人优先”与“公共优先”的宗旨博弈问题，在《个人信息保护法》2020 年修正案拟定过程中也有很多讨论。目前日本存在两种倾向，即“个人优先”与“公共优先”。其中，个人优先论注重个人权益保护，在个人利益与公共利益发生冲突时，以个人权益保护为要。公共优先论有利于公共发展需要，在个人利益与公共利益发生冲突时，以公共利益为要，尤其注重保护新兴产业（包括与大数据相关的产业）发展。

从个人优先出发，需要考虑特定的个人信息，日本称为“敏感信息”。这是 2017 年修改《个人信息保护法》时增加的新概念，即需要事先取得用户同意。这里可以列举很多种情形，如种族、信仰、社会身份、病历、犯罪经历、受害事实、对本人的不当歧视、偏见等。上述情形很多属于个人隐私，却容易为人窥探。对具体个人而言，上述情形既不方便向社会透露，也不愿意向社会披露。如果相关信息泄露，对个人的身体和精神都将造成极大的创伤。2020 年《个人信息保护法》修正案有严格限制向第三方进行信息披露的倾向，体现了个人优先。

从公共优先出发，一般个人信息则以限制滥用为原则。2020 年《个人信息保护法》修正案加大罚款力度，如法人团体违反 PPC 命令则处以最高罚款 1 亿日元，体现公共优先。另外，公共优先存

〔10〕 板仓阳一郎、寺田麻佑「個人情報保護法改正案及び民法（債権法）改正案の利用規約及びプライバシーポリシーにおける個人情報取扱条項への影響」IPSJ SIG Technical Report（情報処理学会研究報告）14 号（2015 年）68 頁参照。

在特殊规定。一是基于法律的明确要求，必须如实提供，如行政人员查询等。二是充分保护人身、财产安全，不能存在丝毫懈怠，如受灾信息等。三是考虑公共卫生、儿童健康等。2020 年新冠肺炎疫情相关的个人信息披露中，从考虑公共卫生出发，充分运用大数据技术，坚持“公共优先”，全面提高疫情防控的整体效能。四是加强行政事务合作，履行公民义务，如政府调查等。

（二）以“个人信息”的概念界定为基础

大数据时代的呼唤，聚焦于信息的删除、管理、共享、披露，考虑是否可检索、检索便捷性等要素，必须保护好个人信息。这就要界定好“个人信息”这一基本概念。“个人信息”的概念界定，基于日本《个人信息保护法》的第 2 条。“个人信息”是能够识别出个人特征的信息，如山田太郎户口本（日语名称为：居民票）公开的姓名、生日、住址等基本信息，还有以身体特征为标识、以个人号码为标识等个人信息，以及与其他信息结合形成的个人信息。2020 年《个人信息保护法》修正案又引入“假名化信息”概念，禁止非法向第三方提供假名化信息。“个人数据”是由个人信息构成的数据，如名片的姓名、公司名称、公司地址、电话号码等印刷出来的信息。用特定软件保存、读取个人信息，即用某种检索方法得到的个人信息，称为“个人信息数据库”。从“个人信息”到“个人信息数据库”示意图请见图 2。

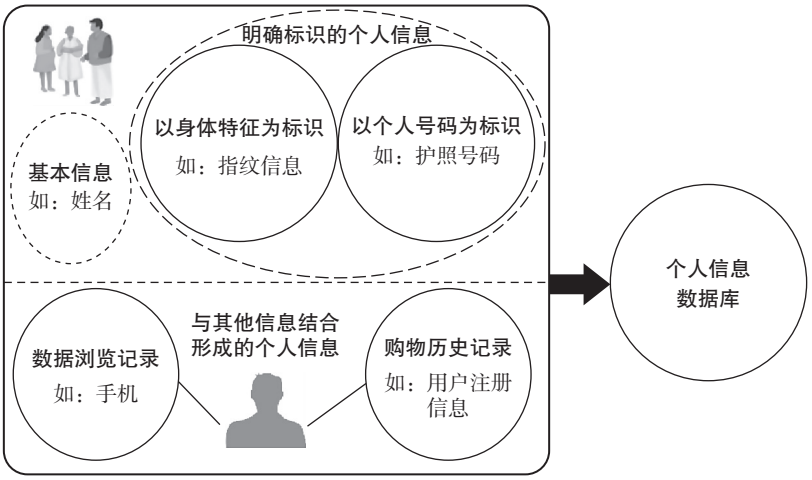

图 2　从“个人信息”到“个人信息数据库”示意图

目前，大数据技术很发达，容易将个人信息数据化。例如，使用“人脸识别软件”识别到的人脸信息，或经过加工的个人数据，不能轻易提供给第三方。又如，监控摄像头虽然不是个人数据，但是录有个人的影像信息，不经有关方同意，不能轻易检索当天的录像内容。监控摄像头一定时间内拍摄到的影像信息，很快就会自动导入数据库，缺少个人隐私保护。换句话说，这很容易违反个人信息保护法。再如，医疗方面的“个人信息”，如残疾、智力（精神）障碍等检查结果在什么时候需要披露到哪个程度，都是值得研究的。

另外，基于疫情防控需要，对外披露的不同主体的“个人信息”的范围存在明显区别，如正在接受治疗的确诊患者、疑似患者、已治愈者，相关人员需要提供之前的行踪、生活地点、接触者信息等。因而，由此集成的“个人信息数据库”一般是有目的地在一定范围内加以使用或保护。日本《个人信息保护法》尤其强调要保护“个人信息数据库”，不能轻易“提供给收集个人

信息的第三方”，一旦“第三方”要求提供某种数据时，一定要经过当事人同意，否则就违反个人信息保护法。事实上，向第三方提供个人信息，涉及“识别”这一概念，这在 2020 年《个人信息保护法》修正案中得到体现。

（三）以个人信息权的保护为核心

日本个人信息保护法需要确立一种基本权利，从新冠肺炎疫情防控也可以看出，个人信息保护与披露必须明确规定，从维护个人权益的高度加以认知，所以个人信息权的确立迫在眉睫。无论《个人信息保护法》是否明确表达，个人信息权始终应当从应有权利走向实有权利。个人信息权不是一般的财产权、物权，因为其具备一般财产权、物权没有的人身属性。个人信息权也不是一般的人身权，因为其具备一般人身权没有的财产属性。个人信息权也不是知识产权可以涵括的，它超出智力成果的直接权利范畴。因而，个人信息权必须独立，且能够独立成为一种明文规定的权利。

大数据时代之下，个人信息权的独立，必须有独立的主体。与前文对应，在新冠肺炎疫情防控之中，个人信息权的主体要考虑正在接受治疗的患者、疑似患者、治愈者等不同情况。个人信息权的主体是个人，“个人”意味着个人信息权本身并非集体所有、国家所有，而是个人所有。“个人”并非单方面凸显个人本位，也非自私自利，只是主体的特定化而已。“个人”的信息权最终要落实到具体人，不能是抽象的、模糊不定的。

大数据时代，个人信息权的独立，必须具有相应的权利内容，包括：一是个人信息收集，即“个人”有权利决定个人信息的收集，因新冠肺炎疫情防控需要利用大数据技术收集个人信息则属法定允许情形。二是个人信息查询，即“个人”有权利决定个人信息的查询。三是个人信息利用，即“个人”有权利决定个人信息的利用。新冠肺炎疫情防控中，对于相关个人信息的利用必须是为了疫情防控本身，不得用于商业目的。四是个人信息更正，即“个人”有权利决定个人信息的更正。五是个人信息传输，即“个人”有权利决定个人信息的私密传输，尤其是大数据时代下惊人的传输量，提出相应的权利诉求。个人信息的传输请见图 3。六是个人信息披露，即“个人”有权利决定个人信息的公开披露，在大数据时代尤其要考虑披露方式（2020 年《个人信息保护法》修正案全面引入电子方式）、披露范围，因 2020 年新冠肺炎疫情防控需要而披露某些个人信息则属法定允许情形。七是个人信息删除，即“个人”有权利决定个人信息的删除。八是个人信息被遗忘，新近又延伸出“被遗忘权”的概念，但事实上“被遗忘权”应当是个人信息权下面的子权利。总之，上述内容只是不完全列举，在大数据时代是远远不足的。个人信息权的权利内容将越来越广泛，《个人信息保护法》应当充分考虑这些崭新诉求并有所回应。

（四）以个人信息保护机构的独立设置为落脚点

考虑到个人信息的有效利用，日本专门设置一个确保正确处理个人信息的最高机构，即个人信息保护委员会。个人信息保护委员会的设立目的与个人信息保护法的立法宗旨一致，即：适应信息社会的高速发展，个人信息的适当处理、合理有效利用，对新兴产业、经济社会、国民生活的促进，充分保护个人合法权益。个人信息保护委员会行使职权具有独立性，包括基本方针政策及其宣传推广、国际交流合作、监督管理、上访处理等职能。个人信息保护委员会工作概要请见图 4。

个人信息保护委员会设立委员长 1 名、常务委员 4 名、非常务委员 9 名。其中，常务委员分别主管如下事务：制定个人信息保护的有关政策及监督、指导、宣传，个人信息技术处理（如

AI、信息处理技术），本国公民的个人信息保护与处理、监管，国际信息交流（如与欧美国家保护隐私机构的沟通）。对相关成员的具体要求包括保护个人信息、保障消费者相关权益、信息处理技术知识、行政领域相关知识、民间企业相关实务经验等。

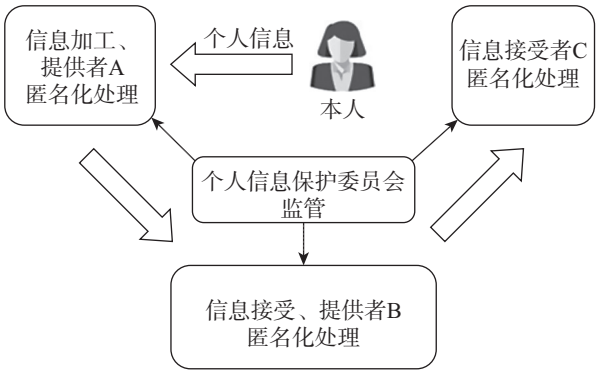

图 3　个人信息传输示意图

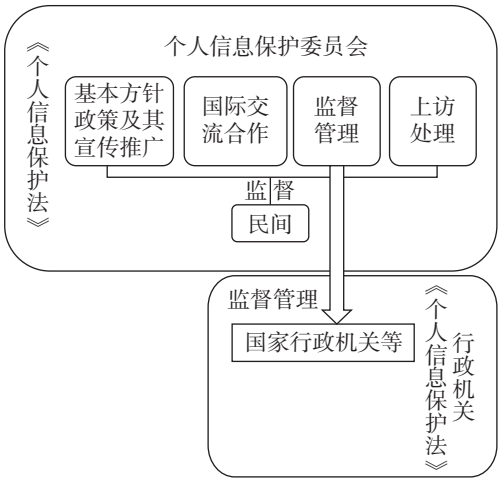

图 4　日本个人信息保护委员会工作概要示意图

可以预见，在大数据时代和新冠肺炎疫情防控的背景下，2020 年《个人信息保护法》修正案将赋予个人信息保护委员会更多的职责，使其在个人信息保护中发挥更为重要的监管作用。

四、日本个人信息保护相关典型判例的类型化适用

（一）有公开披露义务的必须依法披露

1. 借贷案

以下以借贷案［日语为：貸金業者の取引履歴開示義務違反が認められた例（損害賠償控訴事件）］为例探讨特定披露问题。〔11〕原告委托律师作为代理人，以整理财务为理由，向借贷从业者 X 股份有限公司提出了公开交易信息的要求。X 股份有限公司要求代理人提供委任状和印章注册证明书或者身份证明，最终拒绝了提供交易信息。因此，原告认为 X 股份有限公司行为构成违法行为，向其受托人提出了损害赔偿。一审中，法院判决 X 股份有限公司违反了公开交易信息义务，X 股份有限公司不服进行上诉。二审驳回上诉，认定被告公司存在违反公开交易信息义务的行为。最高法院判决，除了出现特别情形以外，借贷从业者根据借贷从业法中相关合同的规定，负有公开交易信息义务。而被告公司拒绝提供交易信息的行为，违反了公开交易信息义务。

本案的焦点在于如何认定“特别情形”的具体内容，X 股份有限公司以《个人信息保护法》和相关从业守则（正在修改）为依据拒绝提供公开信息。法院认定 X 股份有限公司违反交易信息公开义务的根据是，《个人信息保护法》第 29 条中，个人信息处理业者在接到本人请求后，除其他法令规定的特别情形之外，处理业者应立即在必要的范围内展开调查。但是，原告委托代理律师请求的

〔11〕 松井智予「貸金業者の取引履歴開示義務違反が認められた例」ジュリスト1404 号（2010 年）132 頁参照。

行为依照相关行业实务惯例，并不属于上述特别情形之内，对于代理律师相关手续的改变是没有必要的。对于特别情形，该条规定除了滥用的情形之外，还有在短时间内反复要求公开的情形。

总之，关于“特别情形”的例外认定，是大数据时代个人信息特定披露亟需关注的问题。

2. 交通事故案

以交通事故案（日语为：損害賠償等請求控訴事件）为例探讨依据法定程序披露。〔12〕A（原告）在发生交通事故后，在医生 B 所开设的诊所（被告）接受了治疗。此后，被告向负责调停该交通事故的简易仲裁所提供了相关诊断书，原告主张被告侵害了其个人隐私，构成了违法行为，要求被告对其进行精神损失补偿。在第一审中，法院驳回了原告的请求。在二审中，法院仍然驳回了上诉人的请求。

判决理由如下，被告的行为属于《个人信息保护法》第 23 条（向第三者提供个人数据的限制）规定的特殊情形中的“为执行法令规定的事务而提供必要协助”。被告向有关机构提供相关带有个人隐私信息的文件书类，也是根据文书递交嘱托制度的法令而进行的，递交嘱托行为，属于公共社会责任，目的在于正确和有效地解决民事纠纷，具有公益性，是一种正当行为。

总之，何为“法定机构”，何为“法定程序”，解答这一问题在大数据时代必须以“公益性”为依托。

（二）不属于公开披露的不得披露

1. 教育开发公司案

以教育开发公司案［日语为：業務委託先の従業員の不法行為と委託元の責任（ベネッセ個人情報流出事件）（損害賠償請求事件）］为例探讨的是：内部人员违法披露个人信息，应由所属单位对外承担管理责任。〔13〕从事教育开发的公司 Y1（被告 1）于 2012 年 4 月，为了汇总分析顾客所授权使用的个人信息，委托关联公司 Y2（被告 2）进行系统开发、运用和维护等业务。Y2 公司又将其中一部分业务委托给其他多家公司进行再委托。Y2 委托的公司又委托公司中的员工 A，于 2012 年 4 月左右开始，在 Y2 公司（东京分公司办公室）获取了上述个人信息系统数据库的访问账号，并使用 Y2 提供的工作用电脑从事该系统的开发等工作。

2013 年 7 月左右开始至 2014 年 6 月 27 日为止，员工 A 在上述东京分公司办公室将本案件的个人信息数据窃取出来，不仅将该数据存储在上述工作用电脑上，还通过安卓手机的 MTP（媒体传输协议）传输方式，保存进自己的个人手机的内置存储器中。然后，A 将通过不正当方式获取的个人信息数据的全部或部分卖给了三家个人信息收集公司。鉴于员工 A 这一系列的行为造成了个人信息（姓名、性别、生日、住所、电话号码、邮件地址、预产期、未成年人抚养者的信息等）的泄露，原告 X（462 人）向 Y1 和 Y2 提出了诉讼，要求赔偿损失以及承担律师费。

综上所述，Y2 公司对于员工 A 的故意违法行为负有管理责任。根据员工 A 的业务状态，确定 Y2 公司和员工 A 是实质性的领导监督关系，本案件里的个人信息受法律保护，个人信息贩卖行为与其取得信息的契机有紧密的关联。Y2 公司让员工 A 签署了信息保密的同意书，进行了上岗前信

〔12〕 柳井圭子「裁判所の文書送付嘱託と個人情報保護法」年報医事法学 24 号（2009 年）126 頁参照。

〔13〕 石橋秀起「業務委託先の従業員の不法行為と委託元の責任（ベネッセ個人情報流出事件）」新・判例解釈 Watch 25 号（2019 年）73 頁参照。

息安全研修以及上岗一年后的信息安全复训，因此虽然满足了《个人信息保护法》第20条（安全管理措施），但违反了第22条（对被委托人的监督），构成公司对员工A在工作上监督的失职。

总之，对“管理责任”的界定与适用，必须持续关注，才能有助于大数据时代对外披露禁止的研究。

2. 医院案

以医院案［HIV感染不告知を理由とする採用内定取消しと当該情報の目的外使用の違法性：北海道社会事業協会事件（損害賠償事件）］为例探讨违法公开披露。〔14〕

HIV感染者（原告）在一家北海道内的医院（被告）获得了应聘的内定资格，但此后被告被取消了内定的资格。取消内定资格属于违法行为，被告主张上述医院在治疗范围以外使用原告相关的个人信息，属于侵权行为。

判决认为：第一，社会上对HIV感染的偏见和歧视仍然根深蒂固，HIV感染者的个人信息应具有极高的保密度，在处理时需要非常谨慎。原告在通过HIV抗病毒药检的情况下，免疫机能维持良好。主治医师诊断原告不影响本职工作，无须担心在工作场所感染他人，原告并没有义务向被告报告HIV感染的事实。第二，被告医院违反了《个人信息保护法》第16条，在未经原告同意的情况下在超出原有特定医疗目的范围，擅自使用并泄露原告的个人信息，构成违法行为。第三，被告医院的一系列行为，可能导致患者质疑医疗机构的使命，助长对HIV感染者的歧视和偏见，这将导致患者对医疗机构失去信任。

总之，偏见歧视、超过特定利用目的、不当履行社会使命等是构成大数据时代违反个人信息保护法的重要元素，值得深思。

五、结语：对中国的立法期待

2020年新冠肺炎疫情发生之后，大数据技术在中国疫情防控过程中发挥了重要作用，其中包括个人信息的合法收集和披露。与此同时，大数据运用在疫情防控中也会造成对个人信息的某些非法侵犯。因而，在妥善处理新冠肺炎疫情之后，个人信息保护立法问题必将得到更为广泛的关注和期待。大数据时代，中国必须积极行动起来，早日颁布《个人信息保护法》。

其一，关于体例设计。参考日本立法，结合目前大数据发展状况，中国《个人信息保护法》可分为总则、个人信息权保护措施、个人信息保护特别组织、个人信息保护监督管理、法律责任、附则。在此基础上，有必要制定完善配套的法律法规，如《民法典》的相关篇章之中详细规定个人信息保护问题，加强现有《刑法》的严格规制（如侵犯公民个人信息罪）并制定明细的司法解释。

其二，关于立法宗旨。参考日本立法，结合目前大数据发展状况和疫情防控实践，中国《个人信息保护法》的立法宗旨应当以维护个人合法权益为要，体现个人利益与集体利益、社会公共利益、政府利益、国家利益的有机统一，在“个人优先”与“公共优先”之间实现动态平衡。基

〔14〕 小西康之「HIV感染不告知を理由とする採用内定取消しと当該情報の目的外使用の違法性：北海道社会事業協会事件」ジュリスト1538号（2019年）4頁参照。

于此，必须明确规定例外情形，如国家安全、政府管理（如征税）、公共安全（如公共疾病）、学术研究、涉及违法犯罪。

其三，关于基本概念。与日本立法类似，结合目前大数据发展状况和疫情防控实践，中国《个人信息保护法》必须明确“个人信息”的概念，并在相关配套的法律法规之中同样适用。“个人信息”的概念可以采用归纳法与列举法并行的方式。归纳法是强调能够识别个人身份的各类信息，列举法则在归纳法的基础上具体列举，如姓名、出生日期、证件号码、电话号码、个人生物识别信息等。

其四，关于法律原则。参考日本立法，结合目前大数据发展状况和疫情防控实践，中国《个人信息保护法》必须在总则之中规定个人信息保护的法律原则。一是知情同意原则。与之对应，必须在具体条文之中详细规定何为“情”。二是目的明确原则。目的主要指使用目的，即使用个人信息的目的要明确。三是安全使用原则。“安全”既要考虑个人安全，也要考虑公共安全。

其五，关于个人信息权。考虑全世界的立法潮流，结合目前大数据发展状况和疫情防控实践，中国《个人信息保护法》必须明确规定“个人信息权”，作为该法的基本权利。个人信息权包括信息收集、信息查询、信息利用、信息更正、信息传输、信息披露、信息删除、信息被遗忘等诸多内容。

重视个人信息保护是大数据时代的全球趋势，无论中国或日本，皆如此。法律是保护个人信息的基本手段，制定具有本国特色的《个人信息保护法》势在必行。在新冠肺炎疫情防控的背景下加强个人信息保护研究，更具有深远的理论价值和实践意义。保护个人信息，是为了更好地保障公共卫生、促进社会福利。从本质上讲，个人信息保护和疫情防控、公共卫生、社会福利是高度统一的。本文从日本个人信息保护法着眼，为中国立法提供某些启迪。基于当今社会的大数据趋势，个人信息保护是恒久话题，无疑提供了中日学术交流的巨大空间。

Abstract：Personal information is an extremely private thing，but in the era of big data，it is always in a state of “streaking”，and is facing the risk of being violated. Especially in the prevention and control of new crown pneumonia，big data technology has played an important role. The protection of personal information again aroused concern. As a whole，Personal Information Protection Law in Japan is based on the purpose of “individual first” and “industry first” game，taking the definition of personal information as basis，the protection of personal information right as the core and the independent setting of personal information protection institution as the foothold. China should take active steps to enact the Personal Information Protection Law as soon as possible to promote the development of personal information protection and digital economy in the era of big data.

Key Words：personal information，Act on the Protection of Personal Information，the age of big data，new crown pneumonia outbreak

（责任编辑：刘　权　赵建蕊）

财经法学 No. 4，2020
pp. 108 - 120

“数据抗疫”中个人信息利用的法律因应

李晓楠*

内容提要：大数据在疫情态势研判、传播路径分析、精准防控及后续治理中都扮演着重要角色，有利于及时追溯疫情根源，有效切断疫情传播。但不当的数据处理行为可能导致个人信息的泄露，侵犯个人隐私，损害个人权益。为此，在重大疫情防控中，必须遵循法治路径，处理好公共利益维护与个人隐私保障之间的平衡关系。原则上，疫情防控可以作为豁免数据控制主体部分义务、克减信息主体部分权利的合法事由。但数据控制主体仍应承担起必要的个人信息安全保障责任，遵循“目的限制”和“必要性”等数据处理的基本原则。此外，基于公共利益和比例原则在概念上的抽象特质，应进一步完善公共利益下个人信息处理的具体法律安排，从数据利用规制和私权救济两个面向，共同促进个人信息在重大疫情防控中的规范化利用。

关键词：重大疫情防控　个人信息　规范利用

一、引　言

2019 年 12 底开始，新型冠状病毒逐步呈现出全国传播的严重态势。在证实病毒“人传人”的性质后，实现患者及疑似患者的有效隔离就成为了阻断传播的重要管理举措。在追踪确诊患者和疑似患者的过程中，从政府部门到基层自治组织再到企事业单位，均收集了大量的个人信息。一方面应当看到，个人信息的有效运用有助于实现疫情防控目的，各地充分运用“大数据＋”等手段，为“抗疫”配上“最强大脑”。通过建立疫情防控专题数据库，加强疫情防控数据汇聚和共享应用，及时发挥大数据在服务决策、精准防控方面的作用。〔1〕另一方面也应看到，个人信息收集行为不规范甚至随意收集个人信息的行为导致了侵害个人隐私权等情形的发生，如云南文山

* 李晓楠，对外经济贸易大学法学院博士研究生。

〔1〕 参见《湖北宜昌：大数据为抗疫配上“最强大脑”》，载 https://baijiahao.baidu.com/s?id=1660404050154520788&wfr=spider&for=pc，最后访问时间：2020 年 3 月 10 日。

州5名医务人员利用工作便利，偷拍、散布患者信息，引发了隐私保护的担忧，反映了疫情防控下个人信息保护的短板。〔2〕

这一方面是因为我国个人信息保护规范还不健全，缺乏明确的数据利用行为指引；另一方面也在于公共利益优先、私利服务公益的思维惯性容易导致对个人数据权利的忽视。从我国的法律规定来看，《传染病防治法》第12条、第20条、第38条以及《突发公共卫生事件应急条例》第40条，均赋予了疾病预防控制机构、医疗机构及县级以上政府和乡镇基层自治组织收集个人信息的权利，但是上述法律法规缺少个人信息收集、管理、利用、存储、共享等数据生命周期全流程的具体操作规范。我国《网络安全法》虽然对个人信息保护作出了较为全面和广泛的要求，在个人信息更正与删除权、数据泄露通知、个人信息转让等方面有更为具体的规定，但《网络安全法》主要旨在保护国家的“网络主权”和落实网络安全要求，且规制的主体为网络运营者，〔3〕难以辐射疫情管控下多个主体的个人信息收集和利用行为。

但是，应当看到，在疫情防控的背景下，个人信息保护容易让位于公共安全维护，引发公共利益与个人权利的紧张冲突。为了处理好公共安全与个人隐私保护之间的平衡关系，在我国法律规范缺位的情况下，有必要进一步完善疫情防控下个人信息利用全流程的行为规范；明确个人数据的认定标准、范围和数据权能；构建专门的个人信息安全监督机构，从数据控制主体行为规制和数据主体权利救济两个方面，并行推进个人信息在疫情管控中的规范利用。

二、个人信息保护及重大疫情应对中收集利用个人信息的正当性证成

（一）个人信息及个人信息权利保护

数据是信息的形式，信息是数据的内容，没有个人信息的数据不是个人数据，个人信息的权利也即个人数据的权利。〔4〕依据我国《民法典》第1034条第2款规定，所谓个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。围绕个人数据权利的性质和内容，有学者认为，个人数据权利不同于人格权或财产权，而是一种“自决利益”，具体来说，表现为：数据控制主体未经数据主体同意不得收集、转让；数据主体有权知悉其个人数据使用的目的、方式、范围；数据主体有权查询个人数据并主张更正、删除等权利。〔5〕有学者认为，根据数据本身“指向性”的程度，可以将个人数据分为原始数据、信息和隐私，并对应数据权、信息权与隐私权，但总体上属于防御性权利，应以防止损害为中心，而不能主动援引。〔6〕还有学者认为，个人数据保护的人格权与财产权路径均存在难

〔2〕 参见《云南5名医务人员偷拍散布患者信息被罚》，载 https://www.sohu.com/a/371387254_162645，最后访问时间：2020年3月10日。

〔3〕 See Asia Business Law Institute, Regulation of Cross-Border Transfers of Personal Data in Asia, available at https://www.abli.asia/UploadPDF/DP_Compendium_May_2018.pdf, last visited on Mar. 10, 2020.

〔4〕 参见程啸：《论大数据时代的个人数据权利》，载《中国社会科学》2018年第3期。

〔5〕 参见姚岳绒：《论信息自决权作为一项基本权利在我国的证成》，载《政治与法律》2012年第4期。

〔6〕 参见李勇坚：《个人数据权利体系的理论建构》，载《中国社会科学院研究生院学报》2019年第5期。

以克服的弊端，对于个人数据保护来说，应当借鉴欧盟《一般数据保护条例》（以下简称 GDPR）的规定，构建起消费者预期与风险规制相结合的路径。〔7〕

个人信息本身可能蕴含着数据主体的人格利益和财产利益，前者如个人隐私，后者如以个人数据为标的的商业交易。但是基于数据共享和流动对经济社会的重要意义，个人数据财产利益不应具有物权排他性的绝对效力。〔8〕而隐私权本身主要是一种被动性的人格权，通常在遭受侵害时，权利人才可援引，难以满足数据主体对个人数据积极管理的需要。〔9〕尽管针对个人数据权利有不同的表达，但为回应数据主体利益同时兼顾数字经济社会发展需要，我国也逐步形成了以“数据自主”为重要内容的个人信息保护和数据主体权利体系规则，包括“知情—同意”“数据可携带”“被遗忘权”等。〔10〕

从欧盟的 GDPR、美国《加州消费者隐私法案》（California Consumer Privacy Act，CCPA）和澳大利亚《竞争与消费者（消费者数据权）规则 2020》（Consumer Data Right，CDR）等个人信息保护实践看，个人数据权利不排除数据的共享利用，但数据控制主体、处理主体等需要履行数据主体保护义务，既包括提供安全可靠的技术防护手段以防止个人信息泄露，又包括数据利用全流程的安全管理义务，并需要满足数据主体的信息自主权。总之，尽管学界对个人数据权利的保护形式和具体行使方式还存在争议，但个人信息主体享有个人数据自主利益，数据控制主体具有配合数据主体自主利益实现的义务已经成为共识，并成为个人数据保护规范的重要内容。

（二）个人信息作为重大疫情防控中政府决策的基础

信息技术的高速发展，使政府利用海量数据进行公共决策成为可能。习近平总书记在北京市调研指导新型冠状病毒肺炎疫情防控工作时强调，要运用大数据等手段，加强疫情溯源和监测。〔11〕大量个人信息被收集，既包括公权力部门为履行法定职能或执行应急方案依职权收集个人信息，又包括非公主体依据法律法规或行政命令亦或出于自我防护需要而收集个人信息，并汇聚至政府大数据分析平台，辅助政府部门应急决策。例如，疫情暴发之初，浙江省当即启动重大突发公共卫生事件一级响应，并运用“大数据＋网格化”手段，精准滚动摸排所有相关人员，寻找“隐性传染源”。依托新型城市治理平台“城市大脑”搭建的“卫健警务—新型冠状病毒防控系统”，共享、比对卫健委、公安机关等各部门数据，有关部门可以了解每天从疫情重点区域到杭人员信息，实现了对过境车辆和人员“从哪里来、到哪里去、来干什么”的轨迹动态跟踪，便于早期介入、动态管理，并实现各区县市共享，提升防疫实效，避免防疫盲区。〔12〕总之，在疫情防控中，个人信息的大数据利用发挥了重要作用，成为疫情管控中不可或缺的一环。

〔7〕 参见丁晓东：《什么是数据权利？——从欧洲〈一般数据保护条例〉看数据隐私的保护》，载《华东政法大学学报》2018 年第 4 期。

〔8〕 参见梅夏英：《在分享和控制之间：数据保护的私法局限和公共秩序构建》，载《中外法学》2019 年第 4 期。

〔9〕 参见王利明：《论个人信息权的法律保护——以个人信息权和隐私权的界分为中心》，载《现代法学》2013 年第 4 期。

〔10〕 参见《网络安全法》第 40－44 条；《信息安全技术 个人信息安全规范》（GB/T 35273—2020）第 8 条。

〔11〕 参见济兼：《防控疫情要用好大数据》，载 http://opinion.people.com.cn/n1/2020/0217/c1003－31589986.html，最后访问时间：2020 年 3 月 10 日。

〔12〕 参见《浙江：让大数据成为“战疫”利剑》，载 https://baijiahao.baidu.com/s?id＝1658231498659116892&wfr＝spider&for＝pc，最后访问时间：2020 年 3 月 10 日。

（三）重大疫情防控作为克减个人信息权利的正当事由

基于数据权利自主性的特征，个人有权拒绝他人收集信息的行为。换句话来说，收集利用个人信息应当经过数据主体的同意，这也被称为数据管理中的“知情—同意”原则。〔13〕然而，拒绝权本身不是绝对的，在特定情况下，无须获得数据主体同意即可收集、使用其个人信息。之所以存在“同意”原则例外，是因为存在其他权利和合法事由在价值保护顺位上高于信息自决权。从个人信息保护实践看，国内外普遍将维护公共利益需要置于信息自决权之上，而不受“知情—同意”原则的约束。

如前所述，我国《传染病防治法》《突发事件应对法》《突发公共卫生事件应急条例》已经赋予了相关主体基于疫情防控收集个人数据的权能。我国《信息安全技术 个人信息安全规范》（GB/T 35273—2020）就规定了“同意”原则的几种例外事由，主要包括数据收集和使用与国家安全、国防安全直接相关的，与公共安全、公共卫生、重大公共利益直接相关的，出于维护个人信息主体或其他个人的生命、财产等重大合法权益的等。此外，根据我国《民法典》第1036条第3项之规定，为维护公共利益可以不经信息主体或其监护人同意直接处理自然人个人信息。从现有法律规定上看，公序良俗已经成为民法基本原则之一，公共利益维护本身就是限制私权的合法理由。〔14〕为此，即便个人享有信息权利，也不得违反法律，不得违背公序良俗原则。反过来说，为维护公共利益而合理收集、使用或者公开自然人个人信息时，无须承担侵害个人信息的民事责任。

欧盟GDPR序言第（46）条明确规定，传染病监测构成公共利益，处理个人数据时可不征得数据主体的同意，并在序言第（65）（73）条明确针对涉及公共卫生的公共利益，允许欧盟或成员国通过立法对数据主体权利、数据保护基本原则加以限制。第6条亦将为履行涉及公共利益的职责所必要的数据处理排除在“知情—同意”原则的约束外。此外，GDPR通过多个具体条文对公共利益下个人数据权利同时也是数据控制主体的义务进行了相应的克减。如GDPR第14条有条件豁免了出于公共利益目的而间接获得个人数据的主体的告知义务；第17条、第18条规定，当数据控制者为公共利益而履行义务或者为行使其职务权限进行数据处理时，数据主体不得行使删除权（被遗忘权）或限制处理权；第89条规定，当个人数据因公共利益存档的目的被处理时，欧盟法律或成员国法律可以针对个人数据权利和相关的安全保护措施设定克减条款等。

在新冠肺炎疫情期间，美国卫生部门通过发布公报的方式明确规定，出于公共卫生目的和“防止严重和迫在眉睫的威胁”，可以公开个人健康信息而豁免《健康保险可携带与责任法案隐私权规则》（HIPAA）患者健康信息的隐私期待。〔15〕在实践当中，美国卫生部门通过发出“迫在眉睫危险令”（an imminent danger order），可以直接调取个人信息。以密歇根州为例，如果密歇根州卫生服务部门（MDHHS）认定存在“迫在眉睫的危险”，则有权立刻发出“迫在眉睫危险令”，命令相关人员作出降低或消除危险所必要的动作，这其中自然包括要求个人汇报与疾病相

〔13〕 参见张新宝：《个人信息收集：告知同意原则适用的限制》，载《比较法研究》2019第6期。

〔14〕 参见程啸：《民法典编纂视野下的个人信息保护》，载《中国法学》2019年第4期。

〔15〕 See U. S. Department of Health and Human Services，Office for Civil Rights（2020），COVID-19 and HIPAA：Disclosures to Law Enforcement，Paramedics，Other First Responders and Public Health Authorities，available at https://www.hhs.gov/sites/default/files/covid-19-hipaa-and-first-responders-508.pdf，last visited on Mar. 10，2020.

关的情况。〔16〕

三、重大疫情下个人信息利用的法律限制

在利益衡量的基础上，个人信息自决权需部分让位于公共利益，但重大疫情下利用个人信息的行为也并非没有法律限制。基于个人信息收集的主体和具体场景，可将个人信息利用的法律限制分为对公权力主体和对非公主体的不同面向，同时亦应受到个人信息保护规范的一体限制。

（一）公权力主体收集利用个人数据的法律限制

《传染病防治法》《突发事件应对法》《突发公共卫生事件应急条例》均明确了公权力机关，包括县级以上人民政府及其有关部门，各级疾病预防控制机构，街道、乡镇以及居民委员会、村民委员会等疫情信息的收集职能，以供疫情的防控分析，传染病监测、预测和通报。个人应当配合公权力机关有关传染病的调查，如实提供有关信息，否则可能承担不利后果。如在本次疫情中，有地方明令所有通过公路、机场、铁路等方式进入本市的外来人员，在进入本市时应如实填写健康登记表。对于拒绝履行的人员，执法部门将依法协助卫生健康行政部门、医疗机构和疾病预防控制机构采取相应的强制措施。〔17〕从行为类型上看，公权力机关收集个人信息的行为，实质上为相对人创设了如实上报个人信息的义务，应当属于具体行政行为，受到行政法基本原则的限制。

尽管基于应急管理的需要，可以赋予公权力机关直接收集、处理个人信息的权力，个人信息自主权应当受到一定程度的限缩、克减，但对个人信息的处理仍需遵循法律的基本原则，并妥当平衡公权力和私权利之间的关系。〔18〕一方面，要通过法律明确授权，赋予公权力机关紧急行政权等应对紧急事件的必要职权；另一方面，要防止公权力滥用，避免对公民数据权利的过分限缩，克服极端倾向，防范应急状态下出现社会冲突，维护社会正常管理秩序。〔19〕

从行政法基本原则的具体内容看，合理行政原则中的比例原则可以作为规范行政机关收集、利用个人信息行为和维护个人信息权利的有益工具。在确认疫情应对中收集个人信息具有正当性的前提下，比例原则要求个人信息收集应当具有合目的性、适当性，并做到损失最小。具体而言，行政合目的性要求收集个人信息的目的必须是为了防控疫情需要；适当性原则要求收集个人信息时选择的具体措施和手段应为防控疫情所必须；损失最小原则要求收集个人信息应当采用对当事人权益损害最小的方式。总之，公权力机关在收集、利用个人信息的过程中，应当接受行政合理性原则的指导，妥当处理公权力行使与个人信息权利之间的协调关系。

（二）非公权力主体收集、利用个人信息的法律限制

从当前疫情防控的实践看，也存在非公权力主体收集个人信息的行为。如疫情期间，私营企业、小区物业、商场超市等要求进出人员登记个人信息；APP 如“航班管家”基于自有以及收

〔16〕 See Public Health Law Bench Book for Michigan Courts, available at https://www.michigan.gov/documents/ag/PHLBB_2016_Edition_532659_7.pdf, last visited on Mar. 10, 2020.

〔17〕 参见《郑州市新型冠状病毒感染的肺炎疫情防控领导小组办公室通告》（第 5 号），载 http://www.zhengzhou.gov.cn/html/www/news6/20200202/2343414.html，最后访问时间：2020 年 3 月 10 日。

〔18〕 参见江必新：《用法治思维和法治方式推进疫情防控工作》，载《求是》2020 年第 5 期。

〔19〕 参见王万华：《略论我国社会预警和应急管理法律体系的现状及其完善》，载《行政法学研究》2009 年第 2 期。

集的航班、铁路行程、确诊患者信息等数据，匹配新型肺炎确诊患者的行程信息。〔20〕非公权力主体收集、利用个人信息存在多元化的动机。比如，为了遵守公权力机关的行政要求。例如，各地方一般要求企业复工复产应提交《企业疫情防控工作承诺书》，承担疫情防控主体责任，并配合有关部门的流行病调查等工作。〔21〕比如，基于新冠肺炎的强传染性，有关主体为了实现自我防护目的，通过获取出入人员的个人信息，可以及时采取禁止入内等措施避免交叉感染。再如，为了扩大企业的影响力，如航班管家 APP 上线的“新型肺炎确诊患者同乘旅客查询工具”，在为用户提供便利的同时，也起到了吸引流量的效果。当然，非公权力主体收集、利用个人信息的各动机之间并不互相排斥，甚至可以互相包容，也就是说，既可能是为了遵从行政机关要求，同时又可能是为了自我防护并提供他人查询。

在依据行政机关的要求处理个人信息时，非公权力主体应当严格遵循行政机关确立的个人信息收集范围和利用方式，否则将失去个人信息收集、利用的合法性。在防控疫情实践中，非公权力主体用于收集个人信息的登记簿的条目一般由行政机关统一确定，主要包括个人身份信息、是否发热、是否去过特定地区等行程信息；并按照行政机关要求上报来访人员等的涉疫信息。为此，出于履行行政机关要求而收集利用个人信息时，非公权力主体不得超越行政机关确定的数据处理范围和方式。

在基于维护重大合法权益如自我防护等收集利用个人信息时，应受到民法基本原则的约束。民法基本原则要求权利不得滥用，此外，还有学者将公法领域的比例原则引入私法领域，介入难以充分协商或体现意思自治的民事行为。〔22〕非公权力主体以维护重大利益为由收集、利用个人信息，可以不经数据主体同意，形成了事实上的单方强制，有以比例原则进行必要矫正的余地。例如，在疫情下，有些企业在入口处安装体温采集装置，自动收集进出人员包括员工的体温信息，如体温异常则自动报警。体温对新冠肺炎具有重要指标作用，非公权力主体出于自我保护的目的可以越过数据主体同意直接收集，具有合理性。但是，对于对疫情自我防控并不必要的信息，如血型、民族等信息，则不得随意采集，否则有滥用权利之嫌，也不符合比例原则的要求。总之，无论是禁止权利滥用原则抑或是将比例原则引入私法领域，从法理根源出发，均是为了防止私权利主体间权利的过分失衡，使优势主体的权利得到限制，被动接受主体的权利和自由不被过度干预。〔23〕

（三）个人信息权利对数据控制主体行为的限制

因为原则的概括性和模糊性，通过个人数据保护专门立法细化和完善个人数据权利，同时实现对数据控制主体行为的有效指引和规范成为了必要选择。例如，我国已经将《个人信息保护法》和《数据安全法》列入了 2020 年立法规划；欧盟早在 2018 年 5 月就出台了 GDPR；澳大利亚发布了《竞争与消费者（消费者数据权）规则 2020》；美国加州制定了《加州消费者隐私法案》

〔20〕 参见《航班管家“新型肺炎确诊患者同乘旅客查询工具”上线》，载 http://www.caacnews.com.cn/1/4/202002/t20200212_1292673.html，最后访问时间：2020 年 3 月 10 日。

〔21〕 参见《郑州市新型冠状病毒感染的肺炎疫情防控领导小组办公室通告》（第 20 号），载 http://www.zhengzhou.gov.cn/html/www/news6/20200219/2367004.html，最后访问时间：2020 年 3 月 10 日。

〔22〕 参见郑晓剑：《比例原则在民法上的适用及展开》，载《中国法学》2016 年第 2 期。

〔23〕 参见李敏：《我国民法上的禁止权利滥用规范——兼评〈民法总则〉第 132 条》，载《法律科学（西北政法大学学报）》2018 年第 5 期；李海平：《比例原则在民法中适用的条件和路径——以民事审判实践为中心》，载《法制与社会发展》2018 年第 5 期。

等等。而其中 GDPR 以其对个人数据保护的周延性和严格性受到全球范围的关注，并成为个人数据保护的标杆。〔24〕

已有的数据管理实践基本都通过对数据控制主体义务的明确规定，达成对公共利益下的个人信息利用行为的规制。从具体义务内容看，主要包括安全技术义务与安全管理义务两大类。〔25〕我国《民法典》第 1035 条就明确规定，处理个人信息应当遵循合法、正当、必要原则，包括公开处理信息的规则；明示处理信息的目的、方式和范围。第 1038 条又进一步明确信息处理者不得泄露、篡改个人信息，并应当采取技术措施和其他必要措施保障个人信息安全。又如，GDPR 第 5 条规定了与个人数据处理相关的原则，实际上也是数据控制主体的义务要求，包括合法性、公平性、透明性原则，目的限制原则，数据最小化原则，准确性原则，存储限制原则，完整性和保密性原则等。澳大利亚 CDR 在第一部分前言中也强调了消费者个人数据处理上的最小化等原则。

即使在紧急卫生情况下出于公共利益目的处理数据，数据控制主体也要提供适当且具体的措施以保障数据主体的基本权利与利益，履行特定数据保护义务，而不能随意处理个人数据。我国有学者认为，即便公共利益可作为限制个人信息权利的合法事由，也并不意味着在任何情况下，为了公共利益等诉求，就必须共享个人信息。基于公共利益收集、使用和共享个人信息，也应当遵循必要性、最小化适用等个人信息利用的基本原则。〔26〕

此外，从域外经验看，鉴于公共利益概念的模糊性和扩张性，GDPR 第 6 条明确要求，当与公共利益目的相关时，各成员国应当对处理行为设立更为精细的具体要求和其他措施，或者成员国法律可以要求数据控制者向监管机构咨询并且征得其事先授权，以确保数据处理的合法与公平。又如，GDPR 第 13 条、第 23 条规定的透明性要求（针对直接从个人处获得数据的主体），包括明确被处理的数据类型，个人数据可能被披露的对象，处理数据的目的，可能的数据权利限制；GDPR 第 89 条规定了目的限制规则，即对个人数据权利的克减是实现特定公共利益目的所必须；GDPR 第 9 条、第 23－25 条、第 32 条等规定，为了保护数据主体的权利和自由，基于公共利益目的而进行的个人数据处理行为应当采取适当的技术和组织保护措施，如可能的匿名机制、数据最小化机制（个人数据的数量、处理规模、存储期限、可访问性）和保密措施等。西班牙数据保护局（AEPD）发布有关新冠肺炎的个人数据处理报告又进一步指出，在应对疫情过程中处理个人数据应当符合合法性、安全性、透明度、目的限制、准确性和数据最小化等原则。〔27〕

四、重大疫情下收集利用个人数据行为的规范化路径

如前所述，不管是基于应急管理的需要，还是个人数据管理的实践，均承认疫情防控目的下处理个人信息的必要性。但基于“比例原则”及“权利不得滥用”的基本法理和国内外个人信息

〔24〕 See EU，General Data Protection Regulation，available at https://gdpr-info.eu/，last visted on Jan. 10，2020.

〔25〕 参见丁晓东：《个人信息私法保护的困境与出路》，载《法学研究》2018 年第 6 期。

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

〔27〕 See AEPD，Report on Processing Activities Relating to the Obligation for Controllers from Private Companies and Public Administrations to Report on Workers Suffering from COVID-19，available at https://www.aepd.es/es/documento/2020－0017－en. pdf，last visited on Mar. 10，2020.

保护的法律实践，重大疫情下处理个人信息应遵循法治路径。具体来讲，结合疫情防控的实践，首先，在疫情中应坚持以比例原则作为判断个人信息处理是否妥当的指导。例如，各地疫情防控指挥部门应在制定涉及个人信息处理的防控措施时考虑比例原则的要求；各类防控主体在进行数据处理时应满足比例原则的要求等。其次，在设定疫情下个人信息处理的具体法律规范时，应细化疫情中信息主体权利的内容，从私权救济出发强化疫情中的个人信息保护；应明确数据控制主体在疫情防控中的个人信息安全保障义务，规制数据控制主体的数据处理行为；应健全疫情中个人信息不当处理的问责机制，倒逼疫情下防控措施和数据处理行为的审慎实施。

（一）坚持疫情下个人信息处理的比例原则

重大疫情防控需要处理好公共利益和个人信息权利之间的平衡关系，比例原则可以成为平衡利益的有益工具。欧盟《个人数据保护比例原则指南》指出，应在适当的数据处理与合法目的间进行平衡，无论是公共或私人领域，都应在所有阶段实现公共利益、个人权利和自由之间的利害关系的平衡，保证对个人数据权利干预的强度与在特定情况下需要达到的目标之间的必要平衡关系。〔28〕比例原则以“手段—目的”的二元均衡结构作为思考和分析工具，〔29〕可使社会公共利益之判断更为具体，进而更好地约束疫情防控中涉及个人信息的防控措施和各类收集利用主体的个人信息处理行为。

在比例原则的指导下，可分步判断处理个人信息的措施是否正当。首先要判断数据处理的适当性，在防控措施的设定和个人信息的处理上，用于防控和处理的个人信息类型应当可以实现防疫目的。目前个人上报信息种类主要包括姓名、身份证号、居住地、行程信息、通行人员、目的地、所乘交通工具及身体健康情况等，各地疫情防控指挥部在制定涉及个人信息处理的防控措施时以及数据控制主体在处理个人信息时，必须具有合理依据证明上述个人信息能够实现防疫目的，对于不为防疫所需要的个人信息，不能纳入防疫措施的范围和数据处理的范围。其次，判断数据处理手段是否可以实现防疫目的。根据 GDPR 的规定，数据处理的手段除了收集外，还包括记录、存储、改编或修改，查询、使用、传播、披露、删除或销毁等操作。各地疫情防控指挥部决定采取的防控措施以及数据控制主体决定采取的处理措施应能实现防疫目的，如果无需共享、披露等即可满足防疫需求，则个人信息不能被共享或披露，否则不符合比例原则要求。再次，要判断疫情防控措施及数据处理的必要性，也即在疫情防控措施的设定及处理的个人信息类型和处理方式的选择上，应采取最为和缓的干预手段，以影响最少的个人信息量和使用最简短的数据处理流程，尽可能使公民权益遭受最小损害。最后，还要进一步在疫情防控措施及个人信息处理方式与所欲实现的公共利益目的之间进行权衡，确定疫情防控措施或数据处理行为对于相对人所造成的负担是否超过维护公共利益带来的效益。

（二）完善重大疫情下收集个人信息的法律规范

1. 进一步细化个人信息类型，提供梯度保护

以可识别性程度及对个人权益的重要程度，可将个人信息进一步划分为一般个人信息和敏感

〔28〕 See European Data Protection Supervisor, Assessing the Proportionality of Measures that Limit the Fundamental Rights to Privacy and to the Protection of Personal Data, available at https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf, last visited on Mar. 10, 2020.

〔29〕 参见前引〔22〕，郑晓剑文。

个人信息。通常来讲，对个人敏感信息的保护力度要强于一般信息，对个人敏感信息要提供更强的权利救济，对数据控制主体采取更严格的规制措施。就疫情防控中收集的个人数据而言，健康数据、家庭住址等可以被认定为敏感信息。因为个人健康数据尤其是病毒感染信息及家庭住址等如果发生泄露，将可能严重损害个人尊严和正常的生活安宁，引发歧视和社会的不公正对待，且难以通过有效的救济手段恢复至未受侵害的状态。实际上，在本次疫情暴发过程中，针对未及时自我隔离和如实报告个人信息又被确诊的新冠肺炎患者，出现了被“人肉”、谩骂攻击这样的违法行为；武汉籍的个人即便未被确诊，也会引起其他人的恐慌，出现了“谈鄂色变”的自保式歧视，侵害了数据主体的权益。另外，部分携疫人群或密切接触者由于惧怕群体歧视而选择隐匿瞒报个人信息，带来公共关系中的一系列“次生问题”，不利于抗疫工作的开展。相较而言，个人行程信息包括乘坐交通工具信息、出发地和目的地信息、同行人员等，即便泄露，对个人的人身权益影响也较小，可以被认定为一般数据。然而，在大数据技术下，可能很难对某些数据进行准确的定性分类，如在此次疫情防控中已经开始利用的个人位置信息而言，短时间的个人位置信息不至于严重侵害个人隐私，可以认定为一般个人数据，而较长时间的个人位置信息就可能认定为敏感个人数据。例如，美国最高法院在 Carpenter 案中就认为，较长时间范围内的手机位置将暴露个人行踪的全部记录，与 GPS 信息一样，带有时间标记的数据提供了一个关于人们生活的私密窗口，可能揭露了“家庭、政治、专业、宗教和性关系”。〔30〕

通过立法的形式进一步明晰个人信息可能体现的不同权益，并提供分层保护，有利于防疫工作的规范化和对个人权益的保障。具体而言，疫情防控指挥部在制定涉及个人敏感信息的防控措施时应当采取更为审慎的态度，数据控制主体在处理个人敏感信息时也应采取更周全的安全保障措施。但信息本身表现为复杂的利益纠缠，如前所述有些种类的信息如健康数据、基因数据等，单独就构成了敏感信息，而有些数据如个人位置信息、网页浏览记录等，还需要具备一定的时间跨度条件才可能构成敏感信息，想要进行准确定性，不但考验立法技术，同时也需要在信息保护的实践中不断进行总结。

2. 进一步明确疫情防控下个人信息的权利内容

尽管国家市场监督管理总局、国家标准化管理委员会发布了《信息安全技术 个人信息安全规范》（GB/T 35273—2020），对公共利益下个人数据的处理作出了规定，但该规范作为行业标准，仅具有推荐参考意义，并不具法律强制力。此外，该规范的有关规定过于原则，缺乏灵活性，“一刀切”地将公共利益保护作为“知情—同意”原则的例外（包括数据收集、使用、共享、转让、公开披露的告知义务），难以满足个人信息保护的多样化需求。如前所述，即便基于公共利益目的，数据主体也不能随意处理个人信息，而应符合比例原则和保护信息主体权利的要求。GDPR 第 21 条第 1 款就规定，数据主体有权反对控制者为了执行公共利益领域的任务或行使控制者既定的公务职权之必要，对其个人数据进行的处理，包括根据这些条款进行的用户数据画像。除非控制者能够证明其合法利益高于数据主体的利益、权利和自由，或者法定请求权的确

〔30〕 参见楼恺毅：《Carpenter v. United States——论卡彭特诉美国案带来的重要变革》，载微信公众号“清华大学智能法治研究院”，2019 年 11 月 22 日。

立、行使和抗辩有强有力的法律依据。

然而原则本身具有抽象性特质，在疫情防控中要求疫情防控指挥部门和数据处理主体反复以比例原则对涉及个人信息的防控措施和数据处理过程进行审视，难免会增加疫情防控主体和数据控制主体的负担，影响疫情防控的效率，减损疫情信息共享带来的效益，即会引发对疫情防控措施和数据处理行为的合法性质疑，也不利于数据主体依法主张合法权益。为此，应当通过立法的形式进一步完善疫情防控下个人信息权利的具体内容。具体来讲，如果信息主体行使个人信息权利不会严重阻碍防疫目的实现，或是不必要地增加疫情防控主体或数据控制主体的负担，那么就应当赋予信息主体疫情防控背景下的数据权利。例如，个人信息主体查询、更正权利和数据控制主体的告知义务本身不会影响防疫目的实现，且对数据的及时更正反而有利于防疫措施的精准实施。当然，信息主体在行使数据权利时应当秉持诚实信用原则，不得通过反复查询、要求重复告知和故意上报虚假个人信息，不当增加数据控制主体的合规负担。对于删除权应视个人信息可能的作用而区别对待：如果个人信息可以持续用以防疫及相关公共利益目的，如确诊患者的健康数据可用于疫苗的研发、医学研究、传染病持续追踪调查等，则不应允许信息主体行使删除权；如果个人信息如个人行动轨迹信息在疫情消除后没有继续存储的必要，则应当及时删除或应信息主体的要求删除。特别是非公权力主体对其收集的个人信息，原则上在疫情结束后应主动销毁，除非存在其他合法继续存储个人信息的理由。而数据可携带权主要是为了便利数据主体对个人信息的进一步使用或者转移给其他控制者，丰富供给数据主体的服务内容，提升用户体验。〔31〕我国《信息安全技术 个人信息安全规范》（GB/T 35273—2020）通过规定数据主体有权获得个人信息副本来表征数据可携带权。数据可携带权服务于个人信息在不同控制者间的重复利用，对商业主体而言，由于其已经从个人信息的处理中获得了商业利益，要求其满足数据可携带请求具有利益衡平上的合理性。而在疫情防控下，基于公共利益目的收集个人信息的控制者，额外要求其提供结构化、通用化和可机读的个人信息，难免不当增加其负担，不符合比例原则的衡量基准。在疫情防控的背景下，随着个人数据信息内容的不断完善，对于其他各种类型的个人信息权利如拒绝权、限制处理权等，能否以及在多大程度上得到回应，应当结合数据对信息主体的重要程度、对防疫目的实现的关键作用等，在比例原则的指导下进行情景化确定。

（三）完善疫情中个人信息安全管理的组织与技术保障

1. 设立专门机构监督疫情中个人信息的处理行为

目前我国对于个人信息的保护偏重于司法救济（民事诉讼或刑事追责），而欠缺有效的行政救济。〔32〕这一方面是因为，我国没有专门细致的个人信息安全管理规定，行政追责的可操作性不强；另一方面，我国并无专门的个人信息保护机构，而主要由各行业主管部门负责本领域的个人信息保护工作，但不同部门的执法资源、执法手段相差巨大，容易产生监管漏洞。为此，在完善疫情中个人信息保护规范的同时，还应确立专门的个人信息保护机构，从法律层面及时、有效指引和规范疫情中个人信息的利用行为。我国的网信办在个人信息保护执法领域已经积累了一定

〔31〕 参见卓力雄：《数据携带权：基本概念，问题与中国应对》，载《行政法学研究》2019 年第 6 期。

〔32〕 参见郭春镇、马磊：《大数据时代个人信息问题的回应型治理》，载《法制与社会发展》2020 年第 2 期。

经验，可以考虑通过立法的形式确立其在疫情中保护个人信息专门机构的地位，负责保护个人隐私，限制个人信息的收集、披露、处理和共享等数据处理行为，授予其制定配套细则的权力及必要的执法手段包括调查、行政强制和行政处罚等，以及时制止或限制疫情中数据控制主体的不当个人信息处理行为。

除了行政执法外，个人信息保护机构还应向疫情防控指挥部门和数据控制主体提供政策咨询、指导；制定疫情中有关隐私、数据保护的指南；推广隐私增强技术并监督和评估疫情防控措施和数据控制主体的合规性。此外，个人信息保护机构还应承担起受理疫情中个人投诉的职责，并可以要求数据控制主体做出相应回应；在必要时支持并指导个人提起民事诉讼，如果存在潜在犯罪的证据，应将相关情况通报至公安机关进行刑事追责；对于疫情防控指挥部门和公权力数据控制主体，还应当赋予个人信息保护机构向有关机关发出监督建议的权力，督促其及时纠正不当的疫情防控措施和个人信息处理行为，必要时启动行政追责。

2. 引导疫情防控指挥部门和数据控制主体开展内部评估和外部咨询

基于风险控制的考量，不论是疫情防控指挥部门制定涉及个人信息的防控措施，还是数据控制主体处理个人信息，都应履行个人信息保护风险的自我评估和必要时的咨询义务。具体而言，疫情防控指挥部门在制定疫情防控措施时，应当考虑到个人信息保护的要求，防控措施应符合比例原则的要求；数据控制主体要明确个人信息处理生命周期各环节的具体操作规范，加强内部监控，避免不当操作；建立定期测试、评估、评价技术和管理措施是否有效的体系，进一步落实数字控制主体的个人信息保护自查责任。从国际经验看，澳大利亚采取了“创始人”（生成数据的人）的制度，利用数据保护性标识督促数据控制主体履行数据保护义务。当数据生成时，创始人需要评估未经许可访问或不当使用数据所带来的损害及后续影响。〔33〕欧盟采用数据保护影响评估（DPIA）机制，内容包括：个人数据处理行为的性质、范围、内容和目的可能会对自然人的权利和自由产生的风险；基于处理目的对处理行为的必要性和相称性的评估；处理这些风险的预想方案，包括安全和保障措施是否充分；考量个人信息主体尤其是敏感信息主体的权利和合法利益的实现。在疫情中制定防控措施或收集、利用个人信息尤其是个人敏感信息，应当进行充分的合法性和适当性评估，确保个人信息权利的实现。

此外，鉴于公共利益对个人信息权利的克减，尤其是公共利益本身在概念上具有抽象的特质，在防疫工作中不可避免地要进行敏感信息的处理，不当的处理行为难免会造成公共利益与个人信息权利的失衡。为此，当疫情防控指挥部门制定的防控措施涉及个人敏感信息或数据控制者进行个人敏感信息处理时，或者经自我评估发现可能已经造成不相称的后果时，就应当采取更为审慎的态度，及时向个人信息保护监管机构咨询防控措施或个人信息处理行为的妥当性并征得其事先授权。世界范围内，如欧盟数据保护主管部门（European Data Protection Supervisor，EDPS）和新加坡个人数据保护委员会（Personal Data Protection Commission，PDPC），就相关个人信息保护规范的执行已经接受过多次的咨询，并发布了一系列指南，以协助有关机构和个人

〔33〕 See Asia Business Law Institute，Regulation of Cross-Border Transfers of Personal Data in Asia，available at https://www.abli.asia/UploadPDF/DP_Compendium_May_2018.pdf，last visited on Mar. 10，2020.

了解及遵守数据保护法令。〔34〕为此，在疫情防控中，除了数据控制主体应积极向个人信息保护机构咨询以满足个人信息处理的合法性要求外，还应要求疫情防控指挥部门等应急管理责任主体在制定涉及个人信息处理的疫情防控措施的过程中，充分征求个人信息保护机构的意见，实现依法行政与个人信息保护的有机结合。

3. 对疫情中的个人信息采取加密和脱敏措施

基于疫情防控需要，已经形成了公路、铁路、民航、通讯、医疗等疫情相关方多源数据监测、交换、汇聚、反馈机制。〔35〕个人信息需要在公权力主体内部不同部门间以及公权力主体和非公权力主体之间存储、传输、共享，容易导致个人信息的泄露，为此，数据控制主体应当加强个人信息的保密措施。尤其是线下收集及共享个人信息的过程中，应当建立周密的保密组织安排，如：确定专门保密人员负责个人信息的管理，尽可能减少个人信息的不必要接触主体范围；采取合理的保密措施，包括个人信息记录的集中保存等；组织开展个人信息安全培训等。此外，对于广泛利用扫码等进行线上个人信息收集以及利用“重大疫情联防联控网格化管理信息系统”进行不同部门间的个人信息共享、传输，有必要强化数据安全的技术安排，通过数据加密如哈希加密或设定特定访问权限等技术手段，限制个人信息的随意获取，从源头确保个人信息安全。此外，针对疫情预警的需要确需向公众披露个人信息时，应当事先做好屏蔽（或截词）等脱敏处理，包括通过隐藏局部信息令个人信息无法完整显示，或者使用匿名、差分隐私等技术对真实信息等进行处理，以避免个人信息直接暴露于外，进一步落实个人信息收集、利用的安全保障制度。

（四）健全个人信息不当处理的问责机制

数据防疫下，合理的问责机制是确保数据控制主体落实个人信息保护主体责任，维护个人合法权益，实现防疫法治化的重要内容。从责任主体类别上看，主要涉及数据控制主体、数据处理主体等。根据 GDPR 的定义，数据控制者（controller）是指单独或与他人共同确定个人数据处理的目的和方式的自然人、法人、公共权力机关、代理机构或其他机构；数据处理者（processor）是指代表数据控制者处理个人数据的自然人、法人、公共权力机关、代理机构或其他机构。不同身份的主体需要承担不同的数据管理义务。

对于数据控制主体来说，应严格落实疫情中个人信息保护的第一责任人义务，采取合理和必要的措施保障个人信息安全和个人信息权利的实现。如前所述，数据控制主体可以进一步划分为公权力主体和非公权力主体两大类。对于公权力主体，主要是指行政部门，由于疫情应急管理工作面对的是灵活、多变、难以预期的传染病突发事件，为了有效处理危机、防害降损，数据控制主体可能会选择在相对僵化的规则之外行事，如果以此追究其违规的法律责任，不利于应急管理工作的顺利进行。〔36〕为了实现防疫目的，对于法律规范明确规定的数据合规要求，数据控制主体应当严格遵守，否则应承担过错责任；而对于法律规范授予数据控制主体数据处理中自由裁量的事项，固然应当要求数据控制主体遵照比例原则的要求实施具体行为，但在法律评价上不应过

〔34〕 参见刘秀丽：《新加坡〈个人数据保护法〉立法研究综述》，载微信公众号“互联网法治研究”，2020 年 3 月 10 日。

〔35〕 参见李张光：《为打赢疫情防控阻击战提供大数据支撑》，载 http://www.ccdi.gov.cn/yaowen/202002/t20200211_211194.html，最后访问时间：2020 年 3 月 10 日。

〔36〕 参见林鸿潮：《公共危机管理问责制中的归责原则》，载《中国法学》2014 年第 4 期。

分苛责，只要有利于疫情的防控且未严重侵害个人的权利（包括信息自主权和隐私权等），即便存在违反比例原则的不当行为，亦可免责。对于非公权力主体而言，应严格按照行政机关的要求，落实个人信息的收集处理义务，限定个人信息的收集范围，采取适当的信息安全保障措施等，否则应当承担过错责任。如果非公权力主体自行决定以其他合法事由收集利用个人信息（如出于维护个人信息主体或其他个人的生命、财产等重大合法权益等），〔37〕该非公权力主体除了应当履行相应的数据技术和组织安全保障外，还应当进一步举证证明处理个人信息的合法性，否则应当承担过错责任。

对于数据处理主体来说，如在疫情下为数据控制者提供个人信息采集接口的软件运营商，除了应当采取必要的安全技术和组织措施外，如假名化或加密，保障处理系统和服务具备风险应对能力，制定安全措施有效性的测试、评估和评价流程等，还应当严格按照数据控制主体的指示处理个人信息，不得超出数据控制主体委托或授权处理个人信息的内容、性质和目的处理个人数据，否则应当承担相应的过错责任。此外，如果数据处理者超出授权范围自行决定疫情中个人信息的处理目的和方式，则其应当被视为数据控制者，并履行疫情中数据控制者的合规要求并承担相应责任。

Abstract：Big data plays an important role in epidemic situation analysis，transmission path analysis，precise prevention and control and follow-up management，which is conducive to tracing the root of the epidemic in time and effectively cutting off the spread of the epidemic. However，improper data processing may lead to the disclosure of personal information，invasion of personal privacy and damage of personal rights and interests. Therefore，we must follow the path of rule of law in the prevention and control of major epidemics，and deal with the balance between the maintenance of public interests and the protection of personal privacy. In principle，epidemic prevention and control can be used as a legal reason to exempt the obligations of data control subjects and reduce the rights of information subjects. However，the data control subject should still bear the necessary responsibility of personal information security，and follow the basic principles of data processing such as “purpose limitation” and “necessity”. In addition，based on the abstract characteristics of the concept of public interest and the principle of “proportion”，we should further improve the specific legal arrangement of personal information processing in the public interest，and jointly promote the standardized use of personal information in the prevention and control of major epidemics from two aspects of data utilization regulation and private right relief.
Key Words：major epidemic prevention and control，personal information，standardized utilization

（责任编辑：王叶刚　赵建蕊）

〔37〕 参见《信息安全技术 个人信息安全规范》（GB/T 35273—2020）第 5.6 条。