□ 元宇宙规制

□ 个人信息保护法治

□ 人工智能与算法治理

□ 数据治理

财经法学 No. 5，2022
pp. 35 - 53

元宇宙金融规制理论

邓建鹏*

内容提要：元宇宙金融以基于公共区块链的去中心化金融为核心。这种新型金融开创了低成本、高效率的运营方式，但因其无准入门槛，全球参与主体身份不明确、防篡改、抗审查、自我创制规则及自动运行等特点，冲击着金融监管法律体系。然而，元宇宙金融并非绝对不可规制，其历经“去中心化”到“再中心化”的演进，监管机构以“再中心化”的主体为重要抓手，通过非正式指引，出台区块链技术与代码安全的国家标准及正式法规、推动传统金融和元宇宙金融融合等方式，影响基于代码的规则体系、提升金融安全与形塑社区自治规范。不过，元宇宙金融“再去中心化”的演变决定了其在较长时期不能完全被法律规制。

关键词：元宇宙金融　区块链　再中心化

一、导　论

（一）被忽视的核心内容

元宇宙（metaverse）概念起源于尼尔·斯蒂芬森的科幻小说《雪崩》（Snow Crash）。作为3D数字化虚拟共享空间，元宇宙以高速通信网络为基础，支持虚拟时空的大量应用创新，以高性能的虚拟现实（VR）或增强现实（AR）等技术设备及软件带给用户高沉浸、低延迟、多样性和即时参与的感受，借助人工智能驱动的虚拟数字人将元宇宙的内容有组织地呈现给用户。2021年下半年以来，元宇宙概念在学术界被万众瞩目，相关论文如过江之鲫。这些研究主要从传播、文化或哲学思考等领域入手。比如《探索与争鸣》等杂志于2022年2月主办“认识元宇宙：文化、社会与人类的未来”论坛，与会学者就“元宇宙”的哲学基础、道德伦理、媒介实践、社会

* 邓建鹏，中央财经大学法学院教授。
本文为中央财经大学新兴交叉学科建设项目“金融系统安全与区块链监管科技”（批准时间：2021—03）阶段性成果。

特征、主体特征等方面开展交流和反思。〔1〕其他一些核心期刊发表的“元宇宙”论文亦着重从社会传播、哲学思考或政治风险角度切入。〔2〕法学“元宇宙”主题论文有的从宏观或抽象层面论述，〔3〕有的则尝试分析其铸币权等细分问题。〔4〕

然而，元宇宙最引人注目的莫过于数字创造等经济活动。有学者认为元宇宙能够提供各种数字产品和服务，其成败取决于其能否具有实质性的丰富活动，使人们接入元宇宙是一件既具有经济价值又具有学习、社会、娱乐等价值的活动。〔5〕业界专业人士把数字资产创造、交换、消费等所有在元宇宙进行的经济活动统称为元宇宙经济。数字经济是以数字要素作为关键生产资料的经济活动，传统经济升级的方向是数字经济，元宇宙经济是数字经济的一个子集，是其最活跃、最彻底、最具革命性的部分。〔6〕元宇宙经济要素规模无限大，消费频率大幅提高，边际成本趋零化，因此元宇宙经济规模将是现实世界的数倍。〔7〕这样一种由实际生产和消费支撑的高效虚拟经济系统将超越现实世界大多数传统经济体的规模。〔8〕

2022 年 3 月，花旗银行的“全球视野与解决方案”部门（Global Perspectives & Solutions，GPS）发布长达 184 页的深度报告《元宇宙与货币：解密未来》，该报告指出：“到 2030 年，元宇宙经济潜在市场规模将达 8 万亿美元到 13 万亿美元之间，潜在用户将高达 50 亿户。”报告着重指出：“随着元宇宙发展，将需要一系列金融服务支持其活动。元宇宙金融（MetaFi）融合了当今两大技术趋势：元宇宙和去中心化金融（DeFi），即‘元宇宙的去中心化金融工具’，将推动去中心化金融快速增长。从最初的资本形成到支持元宇宙内的商业，金融服务可以在其演变中发挥重要作用。”〔9〕该报告是笔者迄今所见元宇宙领域最详细、最专业的研究。

根据底层技术架构和治理权力的特征，元宇宙分为封闭式（中心化）与开放式（去中心化）两种结构。〔10〕封闭式元宇宙由特定法律主体（公司或个人）掌控，如美国 Epic 公司旗下游戏《堡垒之夜》（Fortnite）及元宇宙上市第一股“罗布乐思”（Roblox）等，其借助相对封闭、分割的特征，由所属公司获取大部分收入与利润。以“罗布乐思”为例，首先，其允许用户以平台自主发行

〔1〕 参见屠毅力、张蕾等：《认识元宇宙：文化、社会与人类的未来》，载《探索与争鸣》2022 年第 4 期。

〔2〕 参见喻国明、耿晓梦：《何以“元宇宙”：媒介化社会的未来生态图景》，《新疆师范大学学报（哲学社会科学版）》2022 年第 3 期，等等。

〔3〕 参见程金华：《元宇宙治理的法治原则》，载《东方法学》2022 年第 2 期；张钦昱：《元宇宙的规则之治》，载《东方法学》2022 年第 2 期。

〔4〕 参见袁曾：《元宇宙空间铸币权论》，载《东方法学》2022 年第 2 期。在国外，个别学者分析元宇宙化身（虚拟人）的法律问题。See B. C. Cheong，Avatars in the Metaverse：Potential Legal Issues and Remedies，International Cybersecurity Law Review（2022），available at https://link. springer. com/article/10. 1365/s43439 - 022 - 00056 - 9 # citeas，last visited on Aug. 8，2022.

〔5〕 参见何哲：《元宇宙新经济的裂变及可能趋势》，载《人民论坛》2022 年第 7 期。

〔6〕 参见赵国栋、易欢欢、徐远重：《元宇宙》，中译出版社 2021 年版，第 30、86 - 87 页。

〔7〕 参见邢杰、赵国栋等：《元宇宙通证》，中译出版社 2021 年版，第 32 页。

〔8〕 参见长铗、刘秋杉：《元宇宙》，中信出版社 2022 年版，第 58 页。

〔9〕 See Metaverse and Money：Decrypting the Future，available at https://www. citivelocity. com/citigps/metaverse-and-money/，last visited on May 22，2022.

〔10〕 有学者将元宇宙分为中心化元宇宙和去中心化元宇宙。参见王德夫：《论“去中心化元宇宙”的风险识别与法律治理——以“元宇宙使馆”事件为观察》，载《荆楚法学》2022 年第 3 期。但极少有法学研究者指出这一重大区分并作差异化研究。在前区块链时代，少量开创性研究停留于对中心化元宇宙的论述。See Cory Ondrejka，Escaping the Gilded Cage：User Created Content and Building the Metaverse，49 *New York Law School Law Review* 81（2004）.

的虚拟货币“罗布币”（Robux）购买平台内用户生成内容（user generated content，UGC）或平台增值服务；其次，用户只能按平台设定价格向平台以美元购买罗布币，并限于平台内使用；最后，“罗布乐思”允许开发者通过开发者交换计划（DevEx）将赚取的罗布币兑换成法定货币。

开放式元宇宙并无特定法律主体掌控，如部署在以太坊等区块链的 The Sandbox 或 Decentraland 等。开放式元宇宙被认为是下一代互联网，即 Web3.0，由区块链、智能合约与非同质化通证（NFT）等构成。〔11〕这种元宇宙主要由用户构建并拥有，用户生成内容，允许内容创建者控制其内容，享有数字作品的权利。与 Web2.0 时代超级平台垄断用户数据和大部分收益不同，Web3.0 是用户和建设者共同拥有网络与数据，这在区块链技术条件下方能实现。开放式元宇宙是“利益相关者机制”，逐渐形成用户和建设者自治的组织形式（DAO），组织规则由程序代码执行，建设和维护元宇宙的社区成员分享利益，共有和共治虚拟空间，这需要应用区块链的共识机制及数字通证作为经济激励机制。综上，开放式元宇宙将与区块链深度融合，释放用户数字创造动力，代表未来的行业发展方向。

区块链为元宇宙金融提供必要基础架构、NFT（非同质化通证）和数字通证（以太币等同质化通证），为数字创造实现价值标识（确权）与价值转移（交易）。2004 年，学者指出自由市场与财产权利的界定是创新的先决条件。元宇宙要取得成功，则要求虚拟财产必须能够转换成现实世界的财产。这个自由市场要求创造者对财产拥有相应权利，方有创造财富的动力，以促进增长。〔12〕但在前区块链时代，个人拥有数字作品的财产权利缺乏技术支持，多停留于设想中。与封闭式元宇宙由所属公司掌控数字资产所有权（如游戏平台控制各类游戏道具与装备）不同，开放式元宇宙需要独立于特定应用项目的数字资产所有权，以太坊等技术标准允许元宇宙用户以可控方式拥有数字资产。用户拥有数字资产的所有权，开辟资产金融化的途径——质押、借贷、交易和衍生品等，这些业务在去中心化金融应用中已比较成熟，构成元宇宙金融主要内涵。

区块链原生数字通证或私人加密货币是激励手段，也可能成为价值储藏的载体，与稳定币构成元宇宙的支付工具。〔13〕去中心化金融降低了人们进入金融的门槛，为人们通过加密资产获利创造机会。〔14〕在这个开放系统上创建钱包、转账与交易均无需提供个人身份等关键信息，应用无需许可，无需中介机构（如券商、银行或第三方支付机构），所有业务通过区块链智能合约自动执行；无需昂贵办公场所和庞大合规团队，交易费用低于传统金融机构；各类应用程序像“金钱乐高积木”一样搭建与分工协作，允许用户创建、修改、混合、匹配或链接任何现有的去中心化金融产品；智能合约应用程序相互叠加，生成可互操作和组合的金融业务。去中心化金融的一些理念富有积极意义，如消除中间环节的暗箱操作，降低中介风险，个人掌控加密资产，交易记

〔11〕 See Paul P. Momtaz, Some Very Simple Economics of Web3 and the Metaverse" (April 17, 2022), available at SSRN: https://ssrn.com/abstract=4085937, last visited on Jun. 1, 2022.

〔12〕 参见前引〔10〕，Cory Ondrejka 文，第 100－101 页。

〔13〕 稳定币通常与美元一比一挂钩，近年成为加密资产交易的主流支付工具，其功能与风险，参见邓建鹏、张夏明：《稳定币的内涵、风险与监管应对》，载《陕西师范大学学报（哲学社会科学版）》2021 年第 5 期；邓建鹏、张夏明：《稳定币 USDT 的风险及其规制对策》，载《经济社会体制比较》2021 年第 6 期；Douglas Arner, Raphael Auer & Jon Frost, Stablecoins: Risks, Potential and Regulation, BIS Working Papers No 905, November 2020.

〔14〕 本文探讨的加密资产是区块链上发行的虚拟货币/私人加密货币/数字通证，如比特币、以太币和稳定币等同质化通证（FT）及非同质化通证（NFT），加密资产是数字资产的一个子集。

录公开透明，受公众监督等。在元宇宙中，可组合性和互操作性使不同加密资产能够应用去中心化金融协议进行传输和交换。用户在去中心化的交易所兑换不同私人加密货币，将私人加密货币存入借贷协议赚取收益，或用“跨链桥”将私人加密货币转入其他区块链系统，这些特征与元宇宙金融业态融合。

（二）法学研究的偏差

元宇宙金融以分布式自治机制（DAO）和数字通证（token）作为组织模式和激励方式，分布式自治机制建立在区块链和智能合约基础上，数字通证是激励参与者完成交易的驱动机制。元宇宙金融是以区块链技术、智能合约和分布式自治机制等为基础的第三代互联网在金融领域的重组。近年去中心化金融应用主要有三种：一是借贷，用户可基于以太坊的借贷协议（如 compound）在其借贷池中存入资产，赚取利息，或利用该协议质押加密资产以借出稳定币。如质押资产市值下跌或到期用户还款困难，协议将执行清算程序，拍卖质押品以避免损失。二是基于去中心化交易所（DEX）的加密资产交易，去中心化交易所（如 Uniswap）允许人们不经审核即在该应用协议上直接交易，允许人们交易新的加密资产。三是衍生品交易，衍生品平台（如 Synthetix）允许用户杠杆交易，或创建模仿传统股票和商品的“合成资产”，作为交易标的。〔15〕

去中心化金融成为元宇宙金融核心，其发展突飞猛进，至 2022 年 6 月 5 日，据 DeFi Pulse 统计，区块链上借贷、交易及衍生品等加密资产锁仓市值达 540 亿美元以上。〔16〕去中心化金融应用由以太坊拓展到其他区块链系统（如 Solana 等），引起业内人士与各国金融监管机构高度关注，诸如美国证券交易委员会（SEC）表态要监管去中心化金融。〔17〕去中心化金融是近年“破坏式”创新的代表，引发了显著法律风险——去中心化金融衍生品的匿名性和去中心化交易，使监管机构收集信息受阻，可能助长洗钱、恐怖融资及网络诈骗等犯罪，增加取证、侦查难度。〔18〕

然而，近年相关法学研究对加密资产法律属性或反洗钱等细分问题的探讨居多，〔19〕整合性研究较为有限。比如，有学者提出区块链金融的智慧型监管及自我规制、行业规制和监管沙箱等；〔20〕或分析去中心化自治组织的法律属性，提出去中心化自治组织适宜界定为有限合伙，发起人承担无限责任，乃普通合伙人，投资者承担有限责任，乃有限合伙人。〔21〕但这些研究忽视了对重要规制对象的深入分析，难以实现预期目的。有学者提出区块链规制的几个层面，即自主

〔15〕 See Matt Hussey, Ki Chong Tran & Jeff Benson, What is DeFi? A 3-minute guide to decentralized finance—Decrypt, available at https://decrypt.co/resources/defi-decentralized-finance-explained-guide-learn, last visited on Dec. 27, 2021. 有学者将去中心化金融应用概括为开放借贷、去中心化交易所、去中心化自治组织、聚合收益理财、稳定币、非同质化通证（NFT）等。参见郑磊：《去中心化金融和数字金融的创新与监管》，载《财经问题研究》2022 年第 4 期。

〔16〕 参见 https://defipulse.com，最后访问时间：2022 年 6 月 5 日。

〔17〕 See Scott Chipolina, SEC Chair Gary Gensler Wants To Regulate DeFi—Decrypt, available at https://decrypt.co/78933/sec-chair-gary-gensler-wants-to-regulate-defi, last visited on Dec. 27, 2021.

〔18〕 研究者系统指出，去中心化金融存在高杠杆、抵押品不足、无反洗钱机制、无用户身份识别、交易匿名与市场操纵等风险。See Sirio Aramonte, Wenqian Huang & Andreas Schrimpf, DeFi Risks and the Decentralization Illusion, *BIS Quarterly Review*, 32 (2021).

〔19〕 比如，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。

〔20〕 参见朱娟：《我国区块链金融的法律规制——基于智慧监管的视角》，载《法学》2018 年第 11 期。

〔21〕 参见郭少飞：《“去中心化自治组织”的法律性质探析》，载《社会科学》2020 年第 3 期。

规制、多方利益相关者共同规制、基于代码的规制等，〔22〕论述多为宏观抽象视野，具体在去中心化金融领域，这些方式的可行性有待观察。有学者认为区块链金融需要在沙箱式监管下实现创新，由监管部门主导完成风险的跟踪测试，金融监管的必要性决定了完全去中心化的公有链不宜适用于金融领域，该领域应淡化“去中心化”，强调分布式、弱中心特征。〔23〕这种应然层面的探索无法回应实然层面去中心化金融及元宇宙蓬勃发展所引发的现实问题。有学者认为区块链治理中驯化“去中心”是历史必然，〔24〕然而如何驯服“去中心化”尚需深思熟虑。

元宇宙虚实结合，将兼容去中心化金融与中心化金融（传统金融），但中心化金融或传统金融多由特定法人主体控制，承担法律责任的主体明确，在现有金融监管法律框架内基本可得到规制。开放式元宇宙监管环境远未成熟，去中心化金融业态将是元宇宙最具活力、革命性，甚至“破坏力”的部分，但其在现有法律与监管框架内几乎完全空白，引发巨大的规制难题，尚未引起各国监管机构普遍重视。元宇宙与去中心化金融结合带来的风险与挑战，〔25〕亟需法学研究者针对其“去中心化”表象，分析法律风险，重点思考“规制谁、如何规制、规则原则及规则方式可能的局限”等系列理论问题。综上，本文以提升元宇宙金融可规制性（regulability）作为研究核心：首先，分析开放式元宇宙金融的底层技术，即区块链对现行法律构成挑战的原因；其次，讨论元宇宙金融可规制的主要对象；再次，探索规制方式与规制重点阶段；复次，剖析规制局限及原因；最后是结语。

二、“去中心化”与“中心化”的对立

（一）元宇宙金融“去中心化”的法制挑战

元宇宙金融实为区块链去中心化金融的应用，与法律中心化特征之间存在矛盾，这是元宇宙金融挑战法律与监管规则的主因。传统法律关系由权威的中心化机构（如立法、执法和司法机关）确立、宣示和保证执行。诸如各类权益证书由中心化机构（如房产管理部门、车辆管理部门）登记、确权并受法律保护，权利和义务主体的特定化是明确法律关系的前提。参与和运维区块链系统的网络节点分布于全球，交易无需识别用户真实身份，义务承担者分散化或无法确定，权利人的请求权可能失去特定对象。法律体系是中心化社会的产物，去中心化意味着区块链系统缺乏明确法律主体，法律规制缺乏特定对象，为不特定参与者规避法律责任提供便利，甚至导致“法不责众”的局面。

区块链部署去中心化应用为交易者提供未经监管者许可的期权、借贷等各类金融产品与服务。在基于以太坊自动做市（automated market maker，AMM）交易协议的 Uniswap 上交易，不需要做市商、上币费及撮合模式下超大规模的运算资源，为元宇宙和区块链项目融资及加密资

〔22〕 参见〔英〕罗伯特·赫里安：《批判区块链》，王延川、郭明龙译，上海人民出版社 2019 年版，第 54－80 页。

〔23〕 参见崔志伟：《区块链金融：创新、风险及其法律规制》，载《东方法学》2019 年第 3 期。

〔24〕 参见李佳伦：《区块链信任危机及其法律治理》，载《法学评论》2021 年第 3 期。

〔25〕 学者认为去中心化金融风险种类比传统金融多，在智能合约代码安全、治理风险、流动性、操作、信用、监管等方面都存在风险点。参见前引〔15〕，郑磊文。

产价格发现提供便利。Uniswap 基于以太坊协议，允许用户以去中心化和无需许可的方式促进以太币和其他任意加密资产（要遵循以太坊 ERC-20 协议发行）之间自动兑换。如某种代币不在 Uniswap 上，只需复制和粘贴该代币的智能合约地址就可添加。有学者认为 ERC-20 协议是至今以太坊上发行的受认可程度最高、使用最为广泛的加密资产协议，旨在为以太坊上通证合约提供一个特征与接口的共同标准。但其并未考虑监管方面对加密资产发行的要求，或者说是为避免对生成于公有区块链的加密资产监管而诞生的一种通用的、简单的标准化协议。〔26〕任何用户可在 Uniswap 自由存入代币进行兑换，自由提取，〔27〕没有中心化交易所（CEX）进行用户注册、身份验证和充提币限制，智能合约自动运行，无需像中心化交易所那样，必须核实用户身份信息。很多项目开发团队原来只能先向中心化交易所付费（业界称“上币费”），通过中心化交易所严格审核或社区投票后才能上市交易某种加密资产（IEO）。〔28〕

去中心化金融业务近年来飞速发展，据以太坊市场分析平台 Dune Analytics 的数据，即使在 2022 年 6 月 15 日“币圈”熊市期间，以 Uniswap 为代表的去中心化交易所在一周内仍创下了 230 亿美元的交易量。〔29〕多数国家针对中心化交易所设有严格牌照管制和相应法律与监管。然而，这种商业模式不用验证交易者身份，无人审核特定加密资产是否存在代码漏洞，不必验证资金合法性来源。诸如 Uniswap 仅是一段代码，部署于以太坊上。区块链防删改的特性使上述项目一旦启动，创始人亦无法停止其运行。当前尚无有效法律与监管机制应对之。

（二）元宇宙金融自生规则与法制的分立

元宇宙金融多无明确控制主体，责任承担主体模糊化，无用户真实身份或地理位置信息，增加监管与合法性审查难度。如学者所述：“现有法律体制的监管重点，是负责和协调在线活动的各种中心化中介机构，而部署在区块链上的系统，如果主要或完全借助密码法运作，就难以受到现有法律体制的控制和监管。”〔30〕法律规制对象主要是中心化社会特定的、可承担义务的主体，这是法律规制的前提。元宇宙金融破除现实中心主义的过程中创生新机制，以分布式架构与不确定主体随时参与或退出为特点，这个时空的规则由元宇宙金融社区自生秩序演化而来，影响现实社会人的行为及法律机制。

元宇宙金融的规则自我创生，自我发展，以系统自身商业目的为准则，不以现实世界监管机构的意图为内涵。当法律试图工具主义地对待元宇宙，使之更好地服务于监管者意图时，双方不可避免地会产生对立。公共区块链系统假名或匿名及免授权许可的方式，使其无任何准入门槛。如比特币系统创建全球分布式价值传输网络体系，交易者可低成本跨境转移巨额资产。比特币在传统金融账户体系之外实现了价值传输，客观上规避现行法律与监管要求。比特币系统基于代码的规则与金融监管法律体系不一致。私钥是持有人控制比特币的唯一途径，多保存在每个持有者

〔26〕 参见姚前、林华等：《区块链与资产证券化》，中信出版社 2020 年版，第 201 页。

〔27〕 参见 https://www.feixiaohao.com/coindetails/uniswap/，最后访问时间：2021 年 2 月 26 日。

〔28〕 IEO 即“Initial Exchange Offerings”，一个区块链项目除早期私募由机构参与外，之后的公募和上线交易都是基于某交易所（Exchange）完成。该模式的核心是知名交易所用自身信用为项目方背书。

〔29〕 参见 https://dune.com/hagaetc/dex-metrics，最后访问时间：2022 年 6 月 15 日。

〔30〕〔法〕普里马韦拉·德·菲利皮、〔美〕亚伦·赖特：《监管区块链：代码之治》，卫东亮译，中信出版社 2019 年版，“导论”第 XIII 页。

的本地终端，持有者控制存储或转移价值不用借助金融中介机构。这种去中心化的价值管控方式，使司法机构查封、扣押、冻结违法者财产的传统方式难以执行。〔31〕

网络信息管理部门曾指出“区块链作为一项新兴技术，具有不可篡改、匿名性等特性”〔32〕，但其在《区块链信息服务管理规定》第16条却规定：“区块链信息服务提供者应当对违反法律、行政法规规定和服务协议的区块链信息服务使用者，依法依约采取警示、限制功能、关闭账号等处置措施。”诸如在以太坊系统，单方面修改已记录在区块上的信息（包括限制功能、关闭账号等措施）难度极大，因此前述法规要求如缘木求鱼。有学者认为，某些严格遵循去中心化构想的区块链系统在实质上没有能力对系统上的活动开展实质性审查。对此，一个重要的平台责任确定原则是，必须结合履行能力来确定平台义务。这就意味着，对于区块链平台无法履行的行为，不能为其施加义务。〔33〕

由于区块链分布式账本跨越国界，元宇宙金融全球化应用场景产生的风险难以受到单一国家监管规则约束。各国对加密资产及智能合约监管等存在不同态度又催生了规则空白。链上行为跨越不同司法辖区，而各国法律规制意图并不相同。元宇宙金融中的博彩游戏、跨境资产转移或敏感信息上链等行为在特定国家或地区受法律保护，在另外一些国家或地区则是打击对象，不同国家对同一行为的合法性评判存在显著差异。如何处理不同国家或地区的法律冲突，哪些国家或地区的法律能够得到执行？这带来不同国家或地区监管执法与司法难题。元宇宙金融难以同时满足所有国家或地区规制的差异化内涵。

代码规则允许加密资产、稳定币和智能合约在未受监管机构审批的前提下组成丰富多样的金融业务与产品，这些新生业态的法律地位或法律属性在现有法律与监管体系中多不明朗，使元宇宙金融在现有法律框架下呈现高度不确定状态，其代码规则可能背离现实社会金融监管法律体系。受代码规则约束的各类加密资产的功能及法律性质差异甚大，对法律产生不同影响、冲击或挑战。具体而言，有的加密资产是功能性或消耗性的，比特币则在事实上逐渐成为价值存储的载体，日益成为欧美众多传统投资机构的重要投资标的。以太坊发行的以太币更像是一种“加密燃料”（crypto-fuel）形式的激励，支付程序运行所需要的费用。去中心化组织无法律实体，通过代码规则与数字通证界定成员的贡献量，从而分配相应权益。去中心化金融创造金融工具，也创造金融资产。比如MakerDAO系统既创造借贷协议，也创造稳定币DAI及治理代币MKR。治理代币持有者可对协议参数的更改（例如稳定费或最低质押比率等）投票。MKR根据DAI价格波动而创建或销毁，使DAI价格尽可能接近1美元。MKR还用于在MakerDAO系统上支付交易费用，并为持有人提供MakerDAO批准的投票系统内的投票权。

（三）基于代码治理的元宇宙金融

元宇宙金融借助区块链系统，其代码规则客观上排斥现实社会的中心化权威，加剧了元宇宙

〔31〕 参见《最高人民法院关于人民法院民事执行中查封、扣押、冻结财产的规定》（法释〔2004〕15号）。

〔32〕《区块链信息服务管理规定》，载 http://www.cac.gov.cn/2019-01/10/c_1123971138.htm，最后访问时间：2021年6月5日。

〔33〕 参见马永强：《区块链金融的刑法风险与规则之治》，载《重庆大学学报（社会科学版）》，转引自 https://kns-cnki-net.webvpn.cufe.edu.cn/kcms/detail/50.1023.C.20210610.1109.002.html，最后访问时间：2022年8月8日。

金融与金融监管法律体系的紧张关系。元宇宙各类金融应用搭建在公共区块链系统之上，需要遵守底层协议，随着应用普及，世俗社会的权力由立法、执法与司法等中心化机构部分转移到区块链核心技术开发人员手中。程序员编写的代码成为另一种“法律”，形塑加密资产创造、资产转移、融资借贷和资产交易等行为。在区块链系统，代码确立的规则等同于刚性法律，不遵守其架构，无法处理包括支付、交易、“挖矿”（竞争区块链账本信息记录权以获取加密资产奖励）和数字签名等行为。这个刚性规则排斥违背代码协议的行为，元宇宙金融可在现实社会执法机构、仲裁机构或司法机构等第三方缺失情况下运行自如。

元宇宙金融是自由开放体系，现实社会金融产品可上链交易，元宇宙金融也可向传统金融体系反向渗透。前者如以美元储备支撑的稳定币 USDC 在以太坊上发行和流通，后者如区块链应用项目 Mirror Protocol 和 Synthetix 创造特斯拉公司等知名公司股票的复制版本。项目开发者在区块链上创建“镜像”协议，激励交易者套利价格差异和管理代币实际供应量，使合成股票价格与真实股票基本保持一致。这些代币在 Uniswap 等去中心化交易所交易，被设计成无需购买真实股票，就可反映它们所追踪的股票价格。〔34〕但这些合成产品未受监管，也没有在特定国家证券交易所交易。这些代币化股票发行和交易可能违反证券法。阻止“镜像”股票交易，就必须关闭该应用的实施基础，即遍布全球的以太坊网络节点和开源代码，关停所有“矿机”，这存在现实困难。

在元宇宙金融系统，中央银行法、商业银行法、证券法、货币管理法和外汇管制法等法律被代码置换。现实社会的规则在区块链及元宇宙中的价值转移、支付或交易过程中并非必选项。元宇宙金融依托区块链自治组织机制，其社区投票结果而非法院裁决具有决策权威。比如在 2016 年，“DAO 项目”由于智能合约漏洞，约 1.5 亿美元的以太币（当时价格）被黑客攻击，对此，以太坊社区大部分网络节点投票决定同意“硬分叉”，取回被盗以太币，原以太坊最后被分叉为以太坊（ETH，即“新链”）和以太坊经典（ETC，即“旧链”）。〔35〕在这起涉及巨额资产的重大争议中，其决策过程无监管机构、仲裁机构或司法机构介入，完全由以太坊社区投票表决。传统金融创新产品上市须经监管机构审批，产品背后有明确责任主体，面向合格投资者销售。元宇宙金融产品和服务无需审批，交易通过合约自动执行，实现代码治理与社区“私法自治”。智能合约是对双方合意的特别执行程序，也是权利义务的代码化表述，通常排除合同变更、合同条款重新解释与特殊情况下不履行合同等情况。在传统合同法视野下，发生欺诈、胁迫或显失公平等事由时，合同可撤销或可变更。在智能合约中，执行代码发送到所有系统的节点分布式处理，只有多数节点代码同步修订才能更改原智能合约。因此，元宇宙金融实行代码规则的自我治理，社区规范与内部自治取代法律。

三、“去中心化”与“再中心化”之悖论

综上，元宇宙金融“去中心化”冲击与挑战金融监管法律体系。有学者认为，去中心化结构

〔34〕 See Fake Tesla，Apple Stocks Have Started Trading on Blockchains，available at https://medium.com/bloomberg/fake-tesla-apple-stocks-have-started-trading-on-blockchains-ed3addaf99e，last visited on Jul.8，2021.

〔35〕 参见井底望天、武源文等主编：《区块链世界》，中信出版社 2016 年版，第 74－80 页。

由许多不同参与者管理，有效管控需要努力识别许多不同相关行为者，但这些行为者匿名、难以找到或位于国外时，就很难做到这一点。去中心化还带来法律执行问题，当系统被设计成其运行的责任分散到许多不同参与者时，分配责任和惩罚违规行为会变得很困难。〔36〕对此，从捍卫一国金融监管主权、防范金融风险及推动金融创新角度而言，在借鉴固有互联网规制模式的同时，应着重思考规制元宇宙（及区块链）与规制传统互联网存在什么差异，可规制的对象（法律责任承担主体）是谁。

（一）元宇宙与传统互联网规制差异

元宇宙被视作下一代互联网，讨论元宇宙金融或区块链规制问题时，人们易沿用传统互联网（Web2.0）规则的固有思维。对后者，美国宪法与互联网法专家劳伦斯·莱斯格的《代码 2.0：网络空间中的法律》为本领域经典著作。〔37〕但 Web2.0 时代互联网产业最终被法律规制，关键原因是互联网产业均依托中心化商业机构或法人实体。如亚马逊等商业机构总部均位于特定主权国家范围，背后有明确的高管、实际控制人和投资机构。通过以下层次的制约，平台及用户逐渐被严密规制：一是平台实行内部控制规则，对违背平台规则的交易者施以惩治，如交易者被禁用淘宝账号；二是平台规则正当性不断受法律评价和审查，平台规则逐渐与正式法规融合甚至一致；三是公权力机构通过监管执法与司法，将平台间冲突、平台上发生的交易行为置于规制范围内，比如处罚违背反不正当竞争法或反垄断法的平台。

有学者认为，网络平台经营活动主要依靠消费者权益保护法、反垄断法、反不正当竞争法、电子商务法等法律制度从外部加以规范；平台制定的大量规则对其用户的权利义务起到实质影响；法律也有必要回应平台内部的权力关系与民主诉求。〔38〕基于商业模式便利，诸如淘宝或二手书交易中介商“孔夫子网”等平台事先引导交易者实名化，明确交易者收件地址，鼓励交易者对每次买卖行为互相评分。诸如微信支付及支付宝用户实名制则来自商业机构精准营销及遵照金融监管法律体系关于用户识别、反洗钱等已有规则的要求。总之，平台基本实现法律规制，很大程度是商业机构利益驱动与政府监管合力的结果。此如有学者认为，无论是商业利用还是政治控制的需要，都将不断推动那些增强互联网可规制性的技术——身份验证、数据标识和物理定位——被广泛采用。〔39〕

有学者认为，互联网真实权力机制由三个要素构成：账户、数据和评分。商业和政府力量使互联网控制权重新变得集中，互联网出现独特的中心化控制机制，即少数平台通过“账户—数据—评分”机制加强网络治理。〔40〕互联网规制方式为区块链或元宇宙金融的法律规制似乎提供了参考，但鉴于两者中心化信息互联网和去中心化价值互联网的本质差异，元宇宙金融注定无法照搬固有的规制模式。在 Web3.0 时代，区块链架构有全新的设计和调整，通过分布式记账、密码学原理和共识算法等技术集成解决陌生人主体间信任问题，实现价值可编程，新的构建模块打开

〔36〕 参见〔美〕威廉·马格努森：《区块链与大众之治》，高奇琦等译，上海人民出版社 2021 年版，第 230－231 页。

〔37〕 参见〔美〕劳伦斯·莱斯格：《代码 2.0：网络空间中的法律》（第 2 版），李旭、沈伟伟译，清华大学出版社 2018 年版。

〔38〕 参见刘权：《网络平台的公共性及其实现——以电商平台的法律规制为视角》，载《法学研究》2020 年第 2 期。

〔39〕 参见戴昕：《犀利还是无力？——重读〈代码 2.0〉及其法律理论》，载《师大法学》2018 年第 1 辑。

〔40〕 参见胡凌：《超越代码：从赛博空间到物理世界的控制/生产机制》，载《华东政法大学学报》2018 年第 1 期。

了新型金融业态的大门。其中多数构建超越了劳伦斯·莱斯格代码 2.0 时代的设想。去中心化的元宇宙金融有自身特质，“无须信任”的架构允许不同参与方无须互相信任就能完成复杂金融交易，实现价值转移，传统互联网则需要诸如评分机制来加强网络治理；传统金融业围绕银行账户展开，元宇宙金融借助区块链用公私钥体系取而代之。综此，元宇宙金融的特殊性要求监管者调整其旧有思维。

区块链账户模式各有千秋，但账户均无需绑定用户身份、识别用户真实性或提供用户通讯地址等任何个人信息，这些特征内嵌于元宇宙金融，使传统互联网账户关键要素被区块链消解。通过不对称加密与共识算法等“技术信任”，区块链无需以评分模式让用户增信。有学者认为互联网平台的社会规范是以诸如身份认证、行为追踪和记录评分等核心内容的权力结果为基础，〔41〕这在区块链中均非必备要素。综上，元宇宙金融规范相较于传统网络规范存在显著差异。固有金融监管模式中，金融机构（确定运营主体）、金融账户（确定用户主体）及牌照管理（确定运营主体合法性）是实现监管意图的关键，但这些因素被元宇宙金融逐一化解。

国外专家认为，与互联网一样，法律总是能适应监管、约束和影响区块链技术的发展。毕竟，区块链只不过是一个去中心化网络，这和互联网并无本质不同。区块链系统必须依赖为底层区块链网络提供支持的新型中介机构，而这些机构易受到监管。此外，这些系统必须依赖代码（或体系结构），它们的运作方式最终取决于市场力量，并受制于社会规范。〔42〕这为区块链及元宇宙的规制提供一些启示，但研究者忽略了两者的重大差异，并未提出有效思路。

（二）元宇宙金融的“再中心化”

有效规制元宇宙金融，应明确其技术底层——区块链的“权力架构”，即在区块链系统发挥关键影响力的私权力主体，确定可规制的重要对象（法律责任承担主体），这是元宇宙金融被金融监管法律规则塑造的前提。如前所述，这个关键性问题在近年研究中多被忽略。有学者认为，应完善区块链相关法律法规及配套制度，加大区块链在金融领域应用的治理。〔43〕然而，法律并非万能，技术总在变异，过度宽泛的建议与有效规制区块链（及元宇宙）存在遥远距离。为常人忽略的是，元宇宙金融虽借助区块链“去中心化”，同时却在若隐若现地“再中心化”。个别研究者断言，“完全去中心化”是种幻觉，去中心化金融平台有一群利益相关者，他们执行决策、实施经营或拥有所有者利益。他们的互动以这个群体及治理协议为基础，对政策制定者而言是个自然的监管入口。〔44〕本文认为，当前影响主流区块链及元宇宙金融的“权力架构”主要由四个关键私主体构成，即核心技术开发团队、大型“矿工”、主流加密资产交易所、投资机构。这是元宇宙金融“再中心化”的重要主体。

元宇宙金融中，技术掌控权力，权力决定规则，规则塑造行为，行为产生结果。核心技术开发团队（通常以非营利基金会形式注册于瑞士等国）塑造元宇宙底层架构、业务本质和激励模

〔41〕 参见戴昕：《重新发现社会规范：中国网络法的经济社会学视角》，载《学术月刊》2019 年第 2 期。

〔42〕 参见前引〔30〕，普里马韦拉·德·菲利皮、亚伦·赖特书，第 192 页。

〔43〕 参见马治国、刘慧：《中国区块链法律治理规则体系化研究》，载《西安交通大学学报（社会科学版）》2020 第 3 期。

〔44〕 参见前引〔18〕，Sirio Aramonte、Wenqian Huang、Andreas Schrimpf 文，第 33 页。另一研究者亦指出实践中存在破坏区块链系统去中心化设计初衷的因素。参见前引〔36〕，威廉·马格努森书，第 298－301 页。上述研究指出去中心化金融存在“中心化主体”，但未系统思考如何规制之。

型。核心技术开发团队拥有元宇宙及区块链系统的“立法权”，奠定其“法律世界”——基于代码的规则体系，形塑交易行为。这些规则确立区块链系统行为模式和交易结构，是区块链系统的“宪法”，独立于现实世界的法律，依托日益增长的全球分布式算力而愈发稳定。元宇宙受益于区块链开发者推陈出新的技术迭代，最后构造独立于现实世界和开发团队自身的“平行宇宙”，即由代码规范的“元宇宙世界”。

与之相关，“矿工”是运维区块链系统的主体，遍布全球。拥有算力优势的大型“矿工”负责把特定时间段系统发生的交易信息记载到区块。为激励“矿工”竞争参与“挖矿”，提升区块链系统安全性，核心技术开发团队设定加密资产（数字通证）激励机制，让“矿工”利益得到保证，并吸引足够多“矿工”参与，技术开发团队预设挖矿难度动态调整，设定诸如比特币每四年发行量减半的规则，参与越早，获利可能越大。“矿机”算力越强，“挖矿”难度越大，区块链系统稳定性越高。〔45〕研究者指出，诸如以太币等加密货币和建于其上的去中心化金融协议依赖验证者或矿工作为中介机构，以验证每笔交易、更新区块信息。这些中介机构可选择添加到账本的交易及交易顺序，因此他们可以采用一些在传统市场可能属于违法的行为，比如抢先交易（front-running），这种获利结果被称为“矿工榨取价值”。就这种市场操纵行为需要针对这类中介机构采取新的监管方式。〔46〕

加密资产交易所决定哪个区块链系统发行的加密资产可在其平台交易。头部中心化交易所（如 Coinbase）及主流 NFT 交易平台（如 OpenSea）巨大的交易体量和交易深度为特定加密资产带来了价格发现、流动性、变现能力、投资价值和财富效应，从而吸引更多投资者投资区块链和元宇宙项目，持有或使用特定加密资产。财富效应直接影响区块链及元宇宙系统技术开发团队的后续积极性和用户人数，影响其成长和生命力。典型事例是原以太坊因“DAO 事件”硬分叉后，大部分矿工切换到新链时，部分矿工维持着旧链，他们在旧链挖出的币（ETC）在交易所无法交易，几乎没有任何价值，矿工无经济来源。在旧链即将消失时，当年全球最大的以太币交易平台 Poloniex（业界称“P 网”）宣布开始交易 ETC，ETC 因此具有流通价值，矿工们的生计得以为继，旧链算力迅速增强。〔47〕

公共区块链需要某种资源驱动，如以太坊需要类似于燃料性质的以太币驱动智能合约执行或每一步链上交易行为。一些加密资产长期成为投资或炒作对象，成为一些高风险投资者储藏价值或法币替代性支付的途径。人们获取此类加密资产的主要途径，一是“挖矿”激励所得，二是在各类交易场所购入。因此，主流加密资产交易所与大型“矿工”作为特定机构，可成为法律规制的有效“抓手”。元宇宙金融表面上高度去中心化，但大型“矿工”与主流加密资产交易所导致

〔45〕 以太坊 2.0 阶段将采用“权益证明机制”（POS），这一阶段质押巨额以太币作为验证节点的个体或机构拥有话语权，成为“再中心化”主体之一。研究者认为这类大型“矿工”为了金融利益，拥有足够权力，可能改变记载上链的信息。参见前引〔18〕，Sirio Aramonte、Wenqian Huang、Andreas Schrimpf 文，第 28 页。

〔46〕 See Raphael Auer，Jon Frost & Jose Maria Vidal Pastor，Miners as Intermediaries：Extractable Value and Market Manipulation in Crypto and DeFi，BIS Bulletin，16 June 2022. 研究者称，“挖矿业”集中对公共区块链去中心化的前提提出质疑，在以太坊权益证明（POS）机制下，以太币巨额拥有者促进不同程度的集中。此外以太坊基金会在以太坊生态系统中具有较强地位。参见〔美〕凯文·韦巴赫：《区块链与信任新架构》，杨东等译，机械工业出版社 2020 年版，第 95－96 页。

〔47〕 参见前引〔35〕，井底望天、武源文等主编书，第 80－81 页。

其“再中心化”。监管机构对交易所和“矿工”备案、登记、核准或管制，要求其提供大额加密资产流向信息登记，交易对手采取实名制，防止拥有算力优势的“矿工”发动“双花”攻击。对加密资产交易所的规制可参照金融监管法律体系，形塑交易所规则。如要求交易所比对与识别交易者身份，充提币身份验证、限时限额提币、提币黑地址（可能被黑客使用过的公钥地址）识别并拒绝服务等。

投资机构资金参与量直接影响区块链系统及元宇宙项目的研发、使用热度、知名度、系统迭代进度，加密资产（如元宇宙售卖的虚拟地块）价格上涨吸引“矿工”投入更多资金购买专用计算机设备“挖矿”，或投资人竞相购买加密资产，使区块链和元宇宙金融运行愈加安全稳健。多数知名区块链项目背后都有行业投资机构作为推手。通常，核心代码开发者决定元宇宙底层结构、激励机制与商业模式，但商业利益方面的诉求使得投资机构的意图必然形塑代码开发者的理念，影响元宇宙商业模式和应用。

通过规制行业头部投资机构（中心化实体），监管者有可能将元宇宙金融置于法律规制之下，借由中心化机构实施对元宇宙金融的规制。比如，自 2021 年以来，美国世可（Circle）公司发行受美国监管的中心化稳定币 USDC，其作为 DAI（去中心化稳定币）的质押比例不断上升。世可公司跟美联储充分合作，它的美元资产在美联储监管下，资产形态是美元和美国国债。在 USDC 份额占 DAI 的质押品一半以上时，DAI 事实上已被中心化的公司潜在支配。USDC 作为连接传统金融（中心化金融）与去中心化金融的媒介，提升传统金融机构对稳定币的采用率，帮助传统资金以合规方式获得元宇宙金融服务。在这一进程中，去中心化的稳定币主要由中心化机构的资产支持时，美国金融监管法律体系实际上经由受监管的稳定币向元宇宙金融渗透。与此类似，加密资产交易另一主流稳定币 USDT 由中心化的法律实体 Tether 公司经营。当元宇宙金融高度依赖这些稳定币时，也将受中心化金融与传统金融支配。

此外，还有一些边缘性私主体拥有小部分“权力”，并发挥着一定的影响力，比如主流区块链资讯媒体、区块链数据与安全分析公司及知名区块链浏览器等。综上，有效规制元宇宙金融，政府及法律应将核心技术开发团队、大型“矿工”、主流加密资产交易所和投资机构作为重点被规制对象，助推现实世界的权力以规训元宇宙系统。

（三）重点规制阶段的配置

加密资产与法币兑换是加密资产流通中至关重要的环节，也是加密资产及元宇宙各类数字创造（如在元宇宙的虚拟地块建造别致的虚拟建筑物并以 NFT 形式确权）完成价格发现的渠道。作为这一渠道的关键载体，加密资产交易所以及 NFT 交易平台已成为元宇宙金融的基础设施。这些载体承担加密资产变现和融资的功能，为元宇宙带来资金和创新动力，是投资人的变现途径。因此，政府规制元宇宙金融的重点阶段可置于元宇宙金融与现实世界的链接点——交易者以加密资产兑换法定货币（或现实世界的产品与服务）这一过程。监管机构难以监管元宇宙金融本身，但可对法币（现实世界）与元宇宙（虚拟空间）交互过程施加有效监管。监管机构通过授权合规、严格管控的中心化交易所或平台，创新探索实施特定加密资产“上市”和“退市”制度试点，间接将元宇宙金融纳入规制范围。在监管机构指导下制定交易所业务和技术标准通用规范、职业道德规范，强化各类审查制度，包括严格的用户身份识别机制、反洗钱机制、交易所网络安

全标准及交易资金合法性来源审查等，〔48〕处罚违法的交易平台。规制中心化交易所或平台，监管机构推动金融监管法律体系与元宇宙金融链接，使现实世界的法律向虚拟时空传递。对初始意图即为明确对抗审查与监管而生的加密资产（比如零币、门罗币等隐私币），〔49〕监管机构可直接要求交易所不得交易此类资产，限制元宇宙金融潜在风险（如洗钱）。

去中心化交易所无特定法律主体，允许用户保持匿名状态和抗审查，不必将现实世界真实身份与交易或账号联系，为元宇宙金融用户借机进行违法犯罪行为（洗钱等）提供便利。不过目前去中心化交易所影响力较为有限，交易量不可与中心化交易所同日而语，〔50〕但其运行特点挑战监管者能力，将成为监管者下一步规制的对象。在去中心化交易所发展壮大前，大力鼓励受监管的中心化交易所吸引大部分投资者，使现实社会的法律与元宇宙金融链接，不失为规制路径的首选。

综上，为提高效率，各类去中心化应用在治理机制方面不可避免地有“再中心化”特色，并非绝对“不可规制”。近年多数去中心化应用表层采取“去中心化”治理模式，项目迭代、参数变动及项目“财库”的代币调用等倚靠社区投票表决。持有去中心化项目发行的治理代币数量决定了投票权权重，然而，大量治理代币主要集中在核心代码开发团队、早期投资机构或应用项目重要参与者手中。〔51〕寡头式治理比大众共治具有更高效率，尤其是应对金融风险及时作出决策是去中心化项目存活的关键。这些因素决定了中心化治理色彩将是常态。因此，元宇宙的“去中心化”金融实质上多以“中心化”方式治理，这个悖论为元宇宙金融被有效规制提供了良途。

四、规制原则、方式和局限

（一）规制的基本原则

元宇宙金融尚在发展形成中，应对创新者与监管者间可能产生的对立情绪和立场予以警醒，其间应设定合理创新与监管博弈的空间。正常创新与监管博弈有益于理性地发展元宇宙金融。如专家所述，在比特币行业快速发展的地区，监管机构不可避免地面临两难选择。他们过早行动，在没有正当理由的情况下会使新技术受到旧规则的约束，就有可能扼杀创新或将其推行至其他司法辖区。但若监管者观望时间过长，公众将受到损害，到时候对现实存在且影响重大的行业提出监管要求的成本将会更高。〔52〕此外，有学者亦称，区块链开发活动激发在全球范围内分布与管

〔48〕 对此可参考日本与美国纽约州的监管经验。参见邓建鹏、孙朋磊：《区块链国际监管与合规应对》，机械工业出版社2019年版，第63－70页、第89－94页。

〔49〕 研究者指出门罗币隐藏所有交易信息，为洗钱犯罪活动提供便利。参见前引〔36〕，威廉·马格努森书，第243页。

〔50〕 研究者统计去中心化交易所交易量占加密资产总交易量的10％以内。参见前引〔18〕，Sirio Aramonte、Wenqian Huang、Andreas Schrimpf文，第26页。

〔51〕 比如在2019年10月举行的决定去中心化银行MakerDAO发行的稳定币DAI利率是从12％提升到13.5％还是降到5.5％的投票中，本来只有两千四百多张投票，随后一个持有人提交四万多张投票，占总投票数的97％。参见前引〔15〕，郑磊文。Uniswap在2021年6月就旨在为监管政策制定者普及、推动DeFi而筹款的基金，以投票方式通过由Uniswap财库拨款100万枚UNI以运作该基金的提案。该提案投票过于集中，有明显中心化倾向。参见https://www.8btc.com/article/6660705，最后访问时间：2021年7月14日。

〔52〕 参见前引〔46〕，凯文·韦巴赫书，第138页。

辖权竞争。美国在早期互联网行业的主导地位为美国带来了重大利益，包括经济利益和全球软实力。〔53〕区块链技术、虚拟货币在金融科技领域深受关注。各国展开的制度竞争越发突显。2022 年 3 月，美国公布《数字资产行政命令》，其强调将在数字资产创新和治理中继续发挥领导作用，首先将保护美国消费者、投资者和企业的政策目标放在首位，然后强调维护美国和全球金融稳定，降低非法金融和国家安全风险，负责任地引领创新，强化美国在全球金融体系、技术和经济竞争力方面的领导地位。〔54〕2022 年 4 月，英国财政部经济部长约翰·格兰（John Glen）在金融科技周的创新金融全球峰会上发表演讲，表示会对加密资产市场给予充分的政策和法律支持。〔55〕

这表明世界经济体大国希望通过有效监管实践，在虚拟货币全球治理中发挥领导作用。晚清对外贸易史及公司制度史的经典研究充分表明，国与国间竞争的核心是制度间竞争。〔56〕在当前国际竞争背景下，发挥政策与制度优势，提升我国在元宇宙金融乃至金融科技领域国际竞争力，具有紧迫性和必要性。规制的内涵不只是约束和禁止，也包括激励与促进。政府不应仅考虑为抑制风险而行使监管的权力，还应考虑如何利用适当的法律与政策促进元宇宙玩家的创造力，推动虚拟空间数字财富增长。近十年来，金融科技等领域的中国监管政策存在“一抓就死，一放就乱”治乱循环，易增加社会成本，打破市场主体预期。作为金融科技与数字经济时代的创新代表之一，中国对元宇宙金融应设定包容的规制原则，对元宇宙金融创新及难免招致的风险予以适度包容，在控制风险底线、保障用户合法权益的前提下，鼓励元宇宙金融创新。

（二）规制的几种途径

网络法专家论述了规制互联网的四种方式，即国家法律、市场、社群规范和架构。〔57〕这为元宇宙金融规制方式提供部分启示。区块链技术及元宇宙金融应用仍处高速发展中，远未定型。研究者谓，面向公众的区块链网络必须满足哪些内部治理要求，现有法律并无规定，因此使用者只能任凭网络创始人和开发者随意制定内部治理框架并选择通过技术代码实施。〔58〕一些区块链项目创始人和开发者的任性和随意性令人触目惊心。比如，Sushiswap 匿名创始人糯米（Chef Nomi）于 2020 年 9 月 5 日从 Sushiswap 的流动资金池中提取 Sushi（Sushiswap 项目的数字通证）套现成价值约 1300 万美元的以太币，导致 Sushi 市场价格 18 小时内暴跌 73%以上。第二天糯米突然宣布将自己的项目控制权（即私钥）交给加密资产交易所 FTX 的 CEO 萨姆（Sam Bankman-Fried）。〔59〕

〔53〕 参见前引〔46〕，凯文·韦巴赫书，第 151 页。

〔54〕 See The White House, Executive Order on Ensuring Responsible Development of Digital Assets, 2022-03-09, available at https://www.whitehouse.gov/briefing-room/presidential-actions/2022/03/09/executive-order-on-ensuring-responsible-development-of-digital-assets/, last visited on May 29, 2021.

〔55〕 See John Glen, Keynote Speech by John Glen, Economic Secretary to the Treasury, at the Innovate Finance Global Summit during Fintech Week 2022, 2022-04-04, available at https://www.gov.uk/government/speeches/keynote-speech-by-john-glen-economic-secretary-to-the-treasury-at-the-innovate-finance-global-summit, last visited on May 29, 2021.

〔56〕 参见方流芳：《公司词义考：解读语词的制度信息——“公司”一词在中英早期交往中的用法和所指》，载《中外法学》2000 年第 3 期。

〔57〕 参见前引〔37〕，劳伦斯·莱斯格书，第 360-366 页。

〔58〕 参见〔英〕凯伦·杨：《区块链监管：“法律”与“自律”之争》，林少伟译，载《东方法学》2019 年第 3 期。

〔59〕 See Fishy Business: What Happened to $1.2B DeFi Protocol SushiSwap Over the Weekend, available at https://www.coindesk.com/sushiswap-liquidation-weekend, last visited on Jun. 5, 2021.

有学者认为，在创新初生期，行政机关承担主导性规制，大多以指导性规制方式展开；在创新成熟期，创新本身的规制问题点充分发酵，可能需要将部分规制内容上升为立法；司法机关则在创新各个阶段承担裁判性规制，作为以上两种规制方式的辅助。随着信息革命到来，复杂变动的社会事实令指导性规制在整个规制框架内扮演着重要角色。〔60〕首先，元宇宙金融处于创新初生期，针对行业风险与问题，监管机构通常处于规制的主导地位，在具体方法上，以非正式指导或正式法令、指引影响区块链代码规则、技术安全标准与社区自治规范，前者如发布技术白皮书，会议讨论和风险提示等方式，后者如与技术、代码安全等相关的国家标准。这些方式有助于引导元宇宙社区自治规范以程序正义的方式制定规则和决策，把上述规则和决策转换成代码，然后将这些代码部署到区块链系统和智能合约中，同时监管者应鼓励行业进行事前专业的智能合约安全审计，排查各类漏洞。

政府部门引导企业制定区块链与元宇宙的技术标准，通过规制技术，间接规制元宇宙的业务与行为。如在2020年7月，中国人民银行印发《关于发布金融行业标准推动区块链技术规范应用通知》和《区块链技术金融应用评估规则》（JR/T 0193—2020）。该标准规定了区块链技术在金融领域应用的实现要求、评估方法、判定准则等，适用于金融机构开展区块链技术金融应用的产品设计、软件开发和系统评估。该标准从基本要求、性能、安全性等方面为去中心化金融应用提供客观、公正、可实施的评估规则，保障去中心化金融设施与应用的安全稳定运行，促进去中心化金融应用健康有序发展。〔61〕不过，中国已有规则主要针对持牌金融机构开发联盟链而设定，表达监管者规制区块链的初步尝试，对公有链影响力较有限。

其次，通过修订法律、提升监管技术，推动元宇宙金融与监管科技结合，推动主权国家逐渐将元宇宙置于法律规制之下。元宇宙金融稳健发展，需为加密资产和智能合约构建合适的法制框架，包括加密资产及稳定币的法律属性，智能合约的法律地位及其法律救济等。在监管技术方面，多数区块链上的信息透明可查询、可追踪。监管机构在一些区块链安全与数据分析技术公司的协助下，解析诸如比特币或以太坊等的账本数据，追溯定位特定公钥地址与使用者的对应关系，最后揭示当事人的真实身份，打击从事洗钱、传销、违禁品交易及通过病毒软件勒索比特币等行为的罪犯。〔62〕监管机构在区块链安全技术公司帮助下，给一些攻击者（黑客）的相关公钥地址打上标签，一旦这些被“标签”的地址开始转账，系统会自动标记相关交易地址，追踪和监控资金流向，监控目标地址交易，追踪主体信息，锁定犯罪分子。尤其是当用户由虚拟空间进入现实世界时，如将加密资产兑换为法币，或用加密资产购买现实世界的商品与服务，其真实身份将显露出来。加密资产在区块链系统中的发送与接收，与传统的网络IP地址类似。理论上而言，监管机构可以跟踪这些IP地址，将加密资产流向置于规制范围之中。

最后，信息科技巨头基于其强大的技术研发力量，为元宇宙构建提供各种硬件和软件，必然

〔60〕 参见王首杰：《创新规制的时间逻辑》，载《华东政法大学学报》2022年第3期。

〔61〕 参见《〈区块链技术金融应用 评估规则〉金融行业标准正式发布》，载https://www.cfstc.org/jinbiaowei/2929436/2976686/index.html，最后访问时间：2020年8月27日。

〔62〕 美国执法机构曾在2021年通过技术手段，将黑客以勒索病毒获取的比特币赎金成功“夺取”回来。See Eric Tucker, US Recovers Most of Ransom Paid after Colonial Pipeline Hack, available at https://apnews.com/article/technology-business-government-and-politics-8e7f5b297012333480d5e9153f40bd52, last visited on Jun. 8, 2021.

影响元宇宙金融规则制定，这为现实世界的法律与监管政策规制元宇宙金融提供了路径。相关部门可鼓励商业机构进军元宇宙，探索商业应用，在技术标准与代码规则等领域发挥影响力；推动中心化商业机构（封闭式元宇宙）与开放式元宇宙融合，影响元宇宙“再中心化主体”，以现实世界的法规塑造开放式元宇宙规则框架；监管机构推动封闭式元宇宙在整个元宇宙规则制定中的话语权，使元宇宙金融与现实世界法规协调。比如，鼓励元宇宙去中心化金融与传统金融融合，使传统金融合规业务向元宇宙渗透。有研究者称，去中心化金融可利用传统金融的资产以合规方式实现扩张，打造虚实结合的数字金融环境。在一些国家，去中心化金融服务已打通虚拟与现实世界。一些加密货币模仿现实金融体系要求，建立资产储备制度，将加密货币等对应一定比例的现实资产与商品。〔63〕

（三）规制局限性的思索

头部加密资产交易所是规制的重要抓手，但也存在局限性。反洗钱金融行动特别工作组（FATF）建议监管机构记录加密资产用户的资料，使他们能更好地识别犯罪活动。其在 2020 年 9 月中旬的一份报告中指出，将用户交易活动与其个人资料对比，可发现某些危险行为和特征，包括用户是否有犯罪记录，或是否活跃在与非法活动相关的网站和论坛上。监管机构也需要关注用户使用比特币或以太坊购买诸如门罗币或零币等行为，后两者会混淆第三方的交易活动。〔64〕将主流加密资产交易所、加密资产钱包提供者纳入监管范围，有助于减少上述风险。FATF 在 2020 年下半年还计划为各国政府制定关于共享虚拟资产服务提供者信息的全球框架，此类提供者包括加密资产交易平台、钱包服务提供者及稳定币发行方。〔65〕当然，多数加密资产交易所面向全球客户提供金融服务，鉴于各国监管标准差异甚大，单一国家如何有效规制境外交易所成为时代挑战。由于交易所的全球分布式办公，办公机构与金融业务跨越多个司法管辖区，容易规避特定国家的监管。更进一步，某些境外交易所可能直接注销中国境内的关联公司，从而对中国司法机关的管辖或案件执行造成困难。

有学者提出政府可监管开发区块链协议和智能合约的人。〔66〕例如，在各国监管者呼吁或压力之下，以太坊核心技术开发人员可能通过提出部分代码修订，使以太坊部分代码融合现代法律规则，但这能否完全收效，尚有待观察。元宇宙与区块链的规范是通过代码规制社群，发挥着独立于现实社会法律体系的作用。以太坊等主流区块链背后有影响力巨大的核心技术开发团队，其通常依托于非营利基金会，获取基金会资助。核心技术开发团队在元宇宙及区块链发展方面拥有很大话语权和影响力，因此，技术团队负责人可成为法律规制的对象。

不过，这种规制意图可能部分落空。其一，代码规则和智能合约内容涉及大量机器语言，内容极为复杂，难以事先审查。政府全面监管一国范围内所有代码开发人员，一是增加巨额监管成本，二是直接阻碍区块链与元宇宙技术创新。其二，一些代码开发者一开始便有意隐匿真实身份

〔63〕 参见前引〔15〕，郑磊文。

〔64〕 See User Profiling Can Help Regulators Identify Illegal Crypto Activity, Says FATF, available at https://www.coindesk.com/user-profiling-regulators-cryptocurrency-crime-fatf, last visited on Nov. 26, 2020.

〔65〕 See FATF Plans to Strengthen Global Supervisory Framework for Crypto Exchanges, available at https://www.coindesk.com/fatf-plans-to-strengthen-global-supervisory-framework-for-crypto-exchanges, last visited on Nov. 26, 2020.

〔66〕 参见前引〔30〕，普里马韦拉·德·菲利皮、亚伦·赖特书，第 199 页。

（如“中本聪”），致监管失效。其三，大多数具有世界影响力的区块链和元宇宙项目创新应用的核心代码开发者分布在欧美等发达国家。无论是主流共识算法，还是跨链、侧链等拓展技术或元宇宙金融重要生态，基本由国外技术团队主导。对中国监管机构而言，规制境外核心技术开发人员可能力不从心。其四，多数核心技术开发团队组织并非固定法律实体，而是松散组织，开发者随时可自由加入或退出团队。这种自治组织形式的运作遍布不同司法管辖区，没有董事会或经营者这样的公司管理层，而是通过民主参与、代码规则、算法与分布式共识管理，使用智能合约收集成员投票。组织成员使用代码和智能合约管理事务，智能合约设定的条款至高无上，代码规则而非法律文件被用以界定成员间权利和义务。这种自治组织作为协调全球投资和社区治理的模式，可用于包括管理区块链项目运营和资本运作等许多目的，这种运营特色对中心化的规制方式造成障碍。

如特定区块链系统大部分核心技术开发团队或系统全球算力的51％以上集中在某一国家，该国政府可以通过规制技术开发团队或“矿工”的方式，有可能部分规制元宇宙金融。比如，迫于监管者压力，技术开发团队和“矿工”同意修订某些区块链底层协议，但也可能带来巨大代价。一是此种行为成本高昂，诸如对比特币新区块的修订，要汇集比特币系统算力的51％以上，其成本或将近百亿美元；二是这将大幅度降低区块链和元宇宙极高的技术信用，直观表现就是相关币价可能暴跌，元宇宙加密资产甚至有归零风险，严重侵害全球合法持有者的权益，可能招致全球投资者国际诉讼风险，这将使监管机构对此种规制投鼠忌器。

元宇宙金融经历着“去中心化—再中心化—再去中心化”的演化，加剧“不可规制性”，导致金融监管法律体系与代码规则间的紧张关系。以 MakerDAO 为例，治理在其生态系统中有着重要角色，但代币持有者投票治理过程漫长，为此，几个核心小组的参与确保治理得到运行，再加上其质押资产近一半为中心化的美元稳定币 USDC，这为现实社会法律规制创造了机会。不过，这一中心化治理风险为更加去中心化的治理模式，即借贷协议 Liquity 提供了机遇。Liquity 系统选择无人治理的模式，Liquity 协议参数要么一成不变，要么完全由算法控制，质押资产则是极具去中心化特色的以太币。Liquity 系统的借贷费和赎回费由数学算法决定，让交易者信任代码按承诺执行，算法、代码和数学的信用取代了人的信用，因此，特定主体的人为因素在系统运行中被降到极致。

作为早期成功的风险投资机构，Andreessen Horowitz（业界简称“A16z”）持有 Compound、Uniswap 等去中心化金融项目的大量代币。A16z 建立授权计划，将这些代币半数以上的投票权委托给非营利组织、德国电信等全球企业、加密初创公司及崭露头角的社区领袖，被委托人可以合适方式独立于代币持有者投票。〔67〕 授权计划改变了 A16z 在 Compound、Uniswap 等项目中投票权过度集中的状态，在保证投资机构盈利的前提下，淡化自身在上述项目治理机制的中心化角色，这是典型的刻意“再去中心化”。有学者认为，当去中心化自治组织无中心权威，实现分布式决策后，去中心化自治组织有限合伙定性的组织基础或成员结构已然丧失，而我国现有法人形态是中心化科层式的制度设计，与其去中心、去信任等本质特点不符，无法直接套用。〔68〕 元宇

〔67〕 参见《A16z DeFi 委托“开源”计划详解》，载 https://www.jinse.com/blockchain/1149655.html，最后访问时间：2021 年 9 月 5 日。

〔68〕 参见郭少飞：《再论区块链去中心化自治组织的法律性质——兼论作为法人的制度设计》，载《苏州大学学报（哲学社会科学版）》2021 年第 3 期。

宙金融“再去中心化”，本质是“可规制性”向“不可规制性”转型。

近年一些诉讼表明，一些区块链系统私权力主体试图规避或抵制在现实社会承担法律责任的要求。比如，美国证券交易委员会（SEC）认为瑞波（Ripple Labs）公司未证券注册，擅自发行加密资产，向当地法院提起诉讼，〔69〕要求瑞波公司承担证券法上的相关责任。针对 SEC 的起诉，瑞波公司认为瑞波币价格波动主要由二级交易市场决定，投资者并非依赖瑞波公司（中心化主体）的努力获益，因此瑞波币不符合“豪威测试”第四项要求。〔70〕瑞波公司声称在瑞波币价格影响方面居于边缘角色，这与事实并不符。区块链项目开发者精心构建代币系统，力图向法院证明其发行的代币不符合“豪威测试”标准，以规避证券法约束。〔71〕

权力即责任，权力越大，责任越大。元宇宙中心化主体“再去中心化”，试图规避现实社会责任，形式上避免成为中心化权力来源。知名区块链系统创始人及近年一些知名去中心化金融应用创始人保持匿名，加剧了区块链和元宇宙的“不可规制”。综上，元宇宙金融将大部分被规制，但难以完全驯服。

五、结　论

区块链为元宇宙提供去中心化金融业务的技术基础，元宇宙金融逐渐成长为与传统金融平行的新体系，各种应用组合形成高度创新的生态，客观上出现元宇宙与政府争夺虚实空间的控制权和治理权的状况，固有金融监管法律体系难以完全适用。现实社会法律与监管规则尝试规制这种新业态时，需从金融包容角度进行思考。如有学者认为，对区块链金融衍生品法律评价应多元，不能因其可能诱发犯罪就拒绝赋予其合法地位，对其评价要考虑未来技术发展需要，要考虑对我国实体经济是否能产生促进作用，要考虑相关行为是否具有严重的社会危害性等诸多因素。虽然政府曾多次出台相关文件规范加密资产，禁止金融机构开展与比特币相关的业务，但是政府的这种政策性叫停并未从本质上解决问题，只有良好的法律才能为其发展提供强有力的保障。〔72〕我国当下在虚拟货币领域采取的“禁令型”监管是暂时的政策选择与监管观望，后续有必要持续探索更加符合金融科技风险特征的治理机制。〔73〕元宇宙金融犹如空气般弥散于世界，打破市场、企业、社会和国家的界线，自生代码体系和法律制度相对独立，但其并非不可规制，原因是元宇宙金融“再中心化”，即核心代码开发者、头部加密资产交易所、大型“矿工”和主流投资机构等私权力主体掌控元宇宙。

元宇宙金融突破传统金融业态，使金融监管法律体系不得不回应和重构。元宇宙金融底层技术

〔69〕 See SEC, Complaint: Ripple Labs, Inc. (“Ripple”), Bradley Garlinghouse and Christian A. Larsen, available at https://www.sec.gov/litigation/complaints/2020/comp-pr2020-338.pdf, last visited on Jan. 5, 2021.

〔70〕 See Ripple, Our Statement on Recent Market Participant Activity, available at https://ripple.com/ripple-press/our-statement-on-recent-market-participant-activity/, last visited on Jan. 5, 2021.

〔71〕 See Neil Tiwari, The Commodification of Cryptocurrency, 117 *Michigan Law Review*, 615-617 (2018).

〔72〕 参见杨玉晓：《区块链金融衍生品刑法规制研究》，载《重庆大学学报（社会科学版）》2020 年第 6 期。

〔73〕 参见邓建鹏、马文洁：《虚拟货币整治的法治思考与优化进路——兼论对金融科技的“禁令型”监管》，载《陕西师范大学学报（哲学社会科学版）》2022 年第 3 期。

架构决定特定国家法律规制存在困难，需要监管者重点厘清可规制对象，提升监管科技水平和规制能力，依托国际间政府组织，推动金融监管国际协作，同时应充分理解当前规制方式的限度。元宇宙金融可能将传统金融业务边界拓展至无限，出现元宇宙世界与现实世界双重构造，二者行为模式与治理规则交互形塑人们的社会关系。固有金融监管法律体系并非应对元宇宙而生，很难应对其风险，因此有必要全面思考这一领域的技术特点和商业模式。有学者认为，信息革命的加速到来，中国法学的自主不足和数字时代的重大挑战，为当下法学研究带来了双重压力，同时也带来了独特机遇，适时转换研究理念就成为一种必然抉择。〔74〕元宇宙金融正在生成新型财产权利关系，奠定前所未有的权利义务结构、复杂法律属性和金融业态，与现实社会有不一致的构造、规则生成与行为模式，经历“再中心化”与“再去中心化”的动态演化。“一刀切”式的固有整治思维并不管用，法学家需要极为精细的研究，紧密跟踪和研判元宇宙金融发展趋势，加强对区块链技术的知识储备，深化法学（及金融监管）意义的研究视角，从而贡献更为有效的规制理论体系。

Abstract：The core of metaverse finance is decentralized finance based on blockchain technology. This new type of finance has created a low-cost and high-efficiency operation method，and it has characteristics such as no access threshold，unclear identity of the global participants，tamper-proof，anti-censorship，self-creation of rules and automatically running，etc.，which have impacted the financial supervision legal system. However，metaverse finance is not absolutely unregulated. It is undergoing an evolution process from “decentralization” to “recentralization”. Regulators should take the “recentralized” organizations of metaverse finance into regulation，through informal guidance，promulgate national standards and formal legislation on blockchain technology and code security，promote the integration of traditional finance and metaverse finance，to which affect code rules，improve technical security and shape community autonomy norms. At the same time，the technical characteristics of the blockchain and the “re-decentralization” evolution of metaverse finance determine that it cannot be completely regulated by law in a long time.

Key Words：metaverse finance，blockchain，recentralization

（责任编辑：李　敏　赵建蕊）

〔74〕 参见马长山：《迈向数字社会的法律》，法律出版社 2021 年版，第 19 页。

财经法学 No. 5，2022
pp. 3 - 19

规范元宇宙：可能性、难题与基本思路

丁　玮　於兴中*

内容提要：虽然当下热议的“元宇宙”是一个缺乏明确定义的概念，但是“数字化生存”的愿景和想象启示了人类进入数字化社会形态的各种可能性。元宇宙本身不是一种方法，也不是一种技术，而是一个集人的游戏（玩）、好赌及趋利性三种主要特性于一身的商业概念。人的这三种特性构成了元宇宙的核心。元宇宙发展的方向取决于人类自身的选择和建构，虚拟世界与现实世界在法律关系上具有同一性、关联性和相似性，虚拟世界的规范秩序建构依赖于现实世界的法律概念、原则和制度。未来元宇宙是以法律规则为核心的组织化、规则化和秩序化的秩序建构过程。法律规制和政府监管对虚拟世界来说是必需的，谁来管控元宇宙是重要的议题，在宪法层面对元宇宙的私权力进行有效规制，对于塑造更美好的未来具有结构性的基础作用。

关键词：元宇宙　再中心化　虚拟世界

一、引言

进入信息社会后，互联网、移动通信、云计算、大数据和人工智能等技术发展的速度远超人类文明的任何阶段。在数字化和智能化的大背景下，人类的生存空间逐渐从物理空间拓展到虚拟空间，“数字化生存”的愿景和想象启示了人类进入数字化社会形态的各种可能性，元宇宙（metaverse）概念的横空出世看似颠覆了人类的想象，又好似技术发展和进步的水到渠成。这是一个人人皆知的术语，但仍然是一个缺乏明确定义的概念。这是一个吸引了最大的科技公司——苹果、Meta、微软——最聪明的头脑的想法，但没有人真正知道它将会是什么。

* 丁玮，哈尔滨工程大学人文社会科学学院副教授；於兴中，澳门大学法学院讲座教授、西安交通大学法学院海外讲座教授。

本文为2021年度国家社会科学基金项目“数字社会私权力宪法规制研究”（21BFX043）、中央高校基本科研业务费专项资金资助项目“数字法学视域下公民数字素养培育研究”（HEU3072022WK1313）的阶段性成果。

元宇宙的概念对不同的人来说显然意味着非常不同的东西。现存的是一系列雏形的数字空间，如脸书（Facebook）的 Horizon、Epic Games 的 Fortnite、罗布乐思（Roblox）的游戏和游戏创作数字空间，以及基于区块链的数字世界 Decentraland。所有这些都有明确的边界、不同的规则和目标以及不同的增长速度。

尽管如此，比较清楚的是，元宇宙正在到来。它将把今天的互联网与虚拟现实（VR）、增强现实（AR）和区块链技术相结合。它将是一个人们相互交流的地方，在那里购买和销售商品和服务，在那里围绕教育、文化、娱乐和信仰形成社区，而个人数据、财产和隐私的传统边界将会被弃之不顾。在某些方面，它将与我们已经知道的数字世界相似，而在其他方面，它将完全不同。

元宇宙是否能够真正成为引领未来数字技术发展的方向，成为人类文明进化历史中的奇点，取决于人类自身的选择和建构。在当下关于元宇宙的热议和评论中，基本问题仍然如赫拉利在《人类简史》中的灵魂拷问："我们人类究竟想要什么？"在元宇宙中智人历史是飞跃还是终幕？元宇宙已在哲学、传播学、文学、社会学、经济学等众多人文社会科学领域引起较大关注。目前，最重要的是人们开始初步探索元宇宙的监管问题。尽管人们很清楚监管一个尚未成型的对象并非易事，但这并不妨碍对元宇宙监管问题进行探索。元宇宙是否有必要监管？元宇宙有哪些可能的风险？法律如何面对未来元宇宙的秩序建构？本文试图对这些问题进行探讨。

二、元宇宙概念的理想与现实

目前尚没有一个关于元宇宙本身的科学定义。一般的定义往往是对数字技术所驱动和连接的信息空间的一种概括性描述。〔1〕元宇宙是一个连接使用者所有生活方面的线上、3D 和虚拟空间概念。这个概念将引导多个平台连接在一起，就像今天的互联网一样，通过一个单一的浏览器进入多个网页。本质上，元宇宙的概念可以理解为一个由相互连接的，并且可由公共界面进入的，融合 2D 和 3D 要素的深度互联网虚拟世界组成的大规模基础设施。因此，没有单一的实体可以被称为元宇宙，元宇宙是通过数字化和 3D 网络工具的多个实体的共同合作进入我们的环境，成为我们生活的一部分。〔2〕

（一）文学叙事中的想象

元宇宙或许被认为是互联网发展的终局，但其并不是互联网发展的产物。众所周知，元宇宙的概念由尼尔·斯蒂芬森在 1992 年出版的恶托邦（Distopia）科幻小说《雪崩》（Snow Crash）发展而来。〔3〕这一概念的流行夸大了小说《雪崩》在赛博朋克科幻史上的地位。美国学者吉尔·莱波雷（Jill Lepore）认为元宇宙"马斯克主义"是一种奢侈的资本主义形式，其来源正是批判资本主义的科幻故事。〔4〕元宇宙并不是人们向往的地方，而是逃避丑恶现实的地方。

〔1〕 参见段伟文：《探寻元宇宙治理的价值锚点——基于技术与伦理关系视角的考察》，载《国家治理》2022 年第 2 期。

〔2〕 See Kevin W. Allen, *Metaverse*, Copyright by Kevin W. Allen, 2022, p. 7.

〔3〕 参见〔美〕尼尔·斯蒂芬森：《雪崩》，郭泽译，四川科学技术出版社 2017 年版。

〔4〕 参见〔美〕吉尔·莱波雷：《元宇宙、马斯克主义？科技富翁们的外星资本主义》，载 https://www.sohu.com/a/500614847_115479，最后访问时间：2022 年 7 月 1 日。

西方科幻文学的基调是科技悲观主义。人们发现科技进步总是带来种种问题，人的生存处境似乎比工业革命前更加艰难，第一部科幻小说《弗兰肯斯坦》讲述的就是技术伦理悲剧。20 世纪 60、70 年代的科技悲观主义与流行的朋克文化结合形成的赛博朋克文学范式，具有向权威和旧秩序抗争的进步意义。但是，赛博朋克追求感官享受，缺乏对科技走向反人类、技术资本垄断等问题更深层次的思考，使得这一文学形式像一股风一样很快就刮过去了。《雪崩》开启了“后赛博朋克”阶段，小说没有赛博朋克故事中常见的压抑的世界秩序和悲壮的反抗运动，只剩下荒诞的元宇宙喜剧。换言之，这里只有赛博，没有朋克。〔5〕在面对技术利维坦的巨大压迫和垄断下，人们无法形成有效反抗，转而投身其所批判的科技愿景中，成为臣服于感官享乐的数字奴隶，这反映了文学对现实批判力的减弱甚至丧失。《雪崩》文学叙事中的元宇宙是一种隐喻，它隐喻了当前对元宇宙概念的热炒，资本和大众对科技寡头的拥抱，以及未来的技术、社会与人类的关系。

（二）游戏中的现实

《雪崩》之后最先将元宇宙想象应用于虚拟世界的就是虚拟游戏。1995 年的虚拟世界 Active World，2003 年的开放式游戏《第二人生》（ Second Life）都受到了斯蒂芬森小说的影响。在虚拟游戏发展分期中，第一阶段是 20 世纪 70 年代文本互动游戏，《龙与地下城》（Dungeons and Dragons1974）和《洞穴探险》（ Colossal Cave Adventure1975），被视为元宇宙的史前叙述；第二阶段为 20 世纪 90 年代 3D 图像和开放式社交的虚拟世界，包括 1994 年的多人社交游戏 Web World 和 1995 年的内容创作虚拟世界 Active World；第三阶段为 21 世纪以后大规模多人在线数字游戏和开放式游戏，以《第二人生》和《机器砖块》（ Roblox）为代表。〔6〕

有学者认为，虚拟游戏是虚拟美学的一大领域。它采用虚拟现实技术构建高度仿真的虚拟存在世界，具有技术、动作、意境、内涵等方面的审美特征，可以产生虚实相生的独特审美效应。〔7〕例如，我国《古剑奇谭》是虚拟游戏艺术的一个代表，这种艺术形式充分运用了虚拟现实技术，通过角色设计、场景设计和光影效果设计，构建出一个高度仿真的虚拟世界，产生独特的审美效应，让玩家在其中获得感官的“沉浸”，补充和延展了现实世界的不足，从而有效调节人们在现实世界中的失衡心态，也折射出深厚的美学思想。〔8〕笔者认为，与其说虚拟游戏属于虚拟美学的范畴，莫不如说虚拟游戏使虚拟幻想以更逼近梦境的样态带给人避世和快感。元宇宙创生出一种“叙事的永远现实态”，它更巧妙地掩盖了市场垄断、利润剥夺和价值操控的存在，人们不必用“规训或惩罚”的条令来管理自己，元宇宙轻松实现人们的“平等感”“自由感”，取代社会平等和政治自由本身。快感已经可以成为财产。我们为了快感而在游戏中储币，更会“氪金”。元宇宙叙事正是完全鼓励这种快感或者说享乐实体化的形式，让文学艺术和社会生活越来越趋于快感化。只要给身体制造相应的感知设备、提供快感场景，人就会被机器制造出来的快感

〔5〕 参见陈韬：《面对“元宇宙”，科幻文艺怎样保持批判力》，载《中国文艺评论》2022 年第 2 期。

〔6〕 参见胡泳、刘纯懿：《“元宇宙社会”：话语之外的内在潜能与变革影响》，载《南京社会科学》2022 年第 1 期。

〔7〕 参见夏洁：《虚拟游戏的审美特征及价值》，载《美与时代（上）》2016 年第 12 期。

〔8〕 参见夏洁：《论虚拟游戏的审美特征——以〈古剑奇谭〉为例》，载《参花（下）》2014 年第 10 期。

直接支配。〔9〕虚拟游戏的发展受到元宇宙文学想象的影响，而虚拟游戏的进一步发展反过来又加深和拓展了未来元宇宙的构想，也就是说，文学和游戏在勾画元宇宙概念和未来愿景中起到引领作用。

（三）商业上的资本运作

“元宇宙”并非“新概念”，2021 年之所以能被冠以元宇宙元年，皆因资本的入场。2021 年是人们开始认真谈论元宇宙的一年，这可能并非偶然。在新冠疫情大流行期间，许多事情，从社交到购物到工作，都因为需求而数字化了，以至于有时感觉我们似乎已经进入了元宇宙的一半。事实上，我们还没有进入甚至还没有接近元宇宙。随着脸书（Facebook）调整商业布局，资本市场随之起舞，元宇宙成为业界和投资者的热门概念。2021 年 3 月，元宇宙概念第一股罗布乐思（Roblox）在美国纽约证券交易所正式上市，招股书里面直接提到了元宇宙；2021 年 5 月，脸书宣布将在 5 年内转型成一家元宇宙公司，并于 10 月 28 日更名为“Meta”；2021 年 8 月，字节跳动斥巨资收购 VR 创业公司 Pico.；2021 年 11 月 23 日，在虚拟世界平台 Decentraland 里，一块数字土地被卖出 243 万美元。

2022 年以来，元宇宙已经超越了斯蒂芬森 1992 年首创这个词汇时所赋予的沉浸式 3D 虚拟世界的内涵，拓展至物理世界中的物体、行动者、界面以及构建起虚拟环境并与之交互的网络等。〔10〕虽然元宇宙在过去只是一个文学中的科幻概念，但现在它看起来会在未来成为现实。元宇宙将利用增强现实技术，使每个用户都能够控制一个角色或者化身，参加混合现实会议，在虚拟办公室使用 Oculus VR 完成工作，用以区块链为基础的游戏来放松，然后管理数字加密货币钱包和金融，所有这一切都发生在元宇宙中。

支持者认为，除了支持游戏、社交媒体，元宇宙将连接经济、数字身份、去中心化治理以及其他应用。即使在今天，用户创造结合有价值的所有权和金钱将帮助发展独特的元宇宙。所有这些能力将赋予区块链在未来技术中巨大的潜在权力。而批评者则认为，科技渐进式的进步才是常态。当前在技术突破、新的需求、主体功能等方面没有任何新的东西，元宇宙更像是一个概念炒作，而且它也符合概念炒作的基本特点，目前业界和学界都没有将虚拟现实、虚拟游戏、静态三维建模、数字孪生、传感器与元宇宙相区别，而是混同使用。〔11〕

通过以上三个方面对元宇宙由来的梳理可以看出，元宇宙与当前互联网的区别主要是被称为“共同在场”（co-presence）的维度，即在同一个数字空间感受他人在场的能力。它不同于当前技术和平台应用的 2D 平面数字空间，是一种具有三维深度的数字传感器空间。已经问世的虚拟游戏世界已经具有一些元宇宙的因素，这些应用接近元宇宙，但还不是元宇宙。现在，元宇宙并不存在。在元宇宙概念的背后是已然渗透到人类社会生活方方面面的数字资本主义，人们生活在数字资本主义所构造的域之中，遵循着被定义的规则，自由时间被占用和填充，元宇宙似乎并没有

〔9〕 参见周志强：《元宇宙、叙事革命与某物的创生》，载《探索与争鸣》2021 年第 12 期。

〔10〕 参见前引〔1〕，段伟文文。

〔11〕 参见贾韬：《“元宇宙热的冷思考”笔谈（上）》之《概念先行后的一地鸡毛：元宇宙会是例外?》，载《科学经济社会》2022 年第 1 期。

带来什么不同。〔12〕未来，元宇宙能否给人类社会带来全方位的变革，并塑造出一个全新的社会形态，除了交给时间没有人能说得清楚。但是，对可能世界的可能问题展开前瞻性研究仍然是值得的。

三、元宇宙的实质

从2021年下半年开始，元宇宙逐渐进入媒体世界，成为一个使用率较高的词汇。然而，频繁使用该词的，也就是为元宇宙鼓与呼的，基本上是游戏公司和投资公司的代理人。2022年7月18日，《时代》杂志发表了一篇题为《元宇宙将重塑我们的生活，让我们确保它变得更好》的文章。作者马修·鲍尔是知名的元宇宙支持者，也是控股公司Epyllion的CEO，风险投资公司Makers Fund的风险合伙人。他在文中指出，直到现在人们还没有一个比较清晰的元宇宙的概念，而元宇宙的产品也尚未问世，关于它的计划也没有落地，尽管对元宇宙的投资已经超过1200亿美元。〔13〕

不过，重要的是鲍尔使用了定冠词来形容元宇宙（The Metaverse），这意味着元宇宙是一个独一无二的存在。事实上，苹果公司、微软、Meta、罗布乐思等公司都在开发自己的元宇宙。这就是说，很可能有若干个而不是一个独一无二的元宇宙。与此相关的是，有一种说法认为元宇宙是和我们的现实世界平行的另一个世界。〔14〕与我们的世界平行的，会是一个什么样的世界？如果说是网络世界，即虚拟/拟真世界是和现实世界平行的世界，那倒也说得通。然而，元宇宙仅仅是网络世界中的若干个场域，或者是游乐场，或者是赌场，或者是办公场所。它不是一个特定的世界，而是一个特定的世界中的若干个组成部分。所谓元宇宙是我们的平行世界的说法是站不住脚的。

众所周知，任何事物都有它内在的规定性，不管我们如何称呼它，本质、基本特点或者基本规定性，这样一种内核是存在的。尽管我们今天已经不太强调本质主义，但我们可以用其他的词汇来形容这种情况。从元宇宙概念的起源来看，它不是一个技术概念，不是一个科学概念，不是一个哲学概念，不是一个历史概念，也不是一个文学概念。如前所述，它是一个从科幻小说里产生出来，被游戏公司试图变为现实的商业性概念。职是之故，元宇宙并不具有研究的学术价值。

元宇宙本身不是一种方法，也不是一种技术，它只是试图将各种主要用于娱乐的尖端技术融合到一起，创造一个环境、一个场域或者一个空间的愿景。它将是一个虚拟现实空间，用户可以

〔12〕 参见高奇琦、梁兴洲：《幻境与虚无：对元宇宙现象的批判性反思》，载《学术界》2022年第2期。

〔13〕 See Mathew Ball, The Metaverse Will Reshape Our Lives. Let's Make Sure It's for the Better, Time, July 18, 2022, available at https://time.com/6197849/metaverse-future-matthew-ball/, last visited on Jul. 25, 2022.

〔14〕 参见《元宇宙已经来了，或许就是传说中的平行世界》，载https://www.kepuchina.cn/Article/articleInfo?business_type=100&classify=0&ar_id=83853，最后访问时间：2022年7月26日；小七有书：《你相信吗？在现实世界之外，真的存在另一个世界》，载https://baijiahao.baidu.com/s?id=1738050177203007894&wfr=spider&for=pc，最后访问时间：2022年7月26日；柳浪闻莺眺西子：《“元宇宙”到底是什么？一个跟现实世界平行运行的人造空间》，载http://www.360doc.com/content/20/0813/07/71135856_1004666238.shtml，最后访问时间：2022年7月26日。

在其中与计算机生成的环境和其他用户进行互动。元宇宙很可能成为一类虚拟空间的代称，而不是特指某一个大的虚拟空间。也就是说它不是跟我们的宇宙或现实世界平行的另外一个世界，而是若干个大玩场，其中有两路玩家：一路是在里面玩的小朋友，一路是在外面赚钱的商家。

游戏公司罗布乐思在招股书里提到，元宇宙有八个重要特征，即身份、朋友（社交）、沉浸感、随时随地、低延迟、内容的多元化、经济、安全。〔15〕扎克伯格认为，元宇宙就是一组相互连接的数字空间，能让你在其中做一些物理世界中无法做到的事情，而重要的是，它将以社会存在为特征，无论你碰巧在世界哪个角落，你都能感觉到与另外一个人在一起。他强调，他们不像别人那样只是讨论工具，讨论人和物，他们想要做的是联系人与人，要以人为中心。〔16〕然而，按照常人的理解，既然要以人为中心，我们本来就在现实世界中，为什么要到虚拟世界中生活？扎克伯格的元宇宙也要通过虚拟现实的头盔或者类似设备的链接，以化身进入，计划使用加密货币，支持 NFT，然后有临场感、沉浸感、即时感等。

在一定意义上，元宇宙实际上就是一种幻境，把有些人偶尔做的梦变成可以重复的梦。戴上头盔和手套，即可进入一个梦幻的自由世界，可以随意追求现实中无法实现的目标。一旦取下头盔，即刻回到现实，梦境荡然无存。而且，做梦是需要花钱的。

它很可能是网上的迪士尼，迪士尼的增强版。当然，这是比较客气的说法。《金融时报》的一位作者说，元宇宙实际上是拉斯维加斯的最新化身。〔17〕这种说法虽然夸张，但也指出了一些问题。比如，现在在元宇宙中热炒的 NFT，多少有赌博的意味，而且玩和赌往往交织在一起。

但这并不意味着元宇宙本身没有生命力。相反，元宇宙的生命力会非常强大。不过，这种强大并不是因为它的科学性或逻辑性，而是因为它集成了人的三种主要特性，即游戏（玩耍）、好赌和趋利。这三种特性构成了元宇宙的核心结构。这是一个无法打破的铁三角关系，极少有人能够抗拒它的诱惑。因此，不管元宇宙的概念有多不清楚，有多虚幻，人们还是要追捧，资本还是会进入。

正是因为元宇宙的核心是玩、赌与资本的紧密结合，所以元宇宙一旦发展，其势头猛不可挡。各行各业都会进军元宇宙。万物皆可元宇宙。元宇宙是不是伪命题，谜底尚未揭开。但是，某些产业已经将其作为一种创新的营销手端。目前，涉及元宇宙概念的上市公司比比皆是，虽然大多数公司还没有任何与元宇宙有关的产品。〔18〕

四、规范元宇宙的必要性

为了成为可行的生活和商业场所，元宇宙需要现实世界的控制，以保护用户免受滥用、欺诈

〔15〕 See veled, What is the meta universe?, Matters, available at https://matters.news/@veledaseohwv/211982-what-is-the-meta-universe-bafyreidy6kzrt2qka6ewqgvrx6f2fg6pyimkpwabsjkruwtdjltl7gwwqe, last visited on Aug. 29, 2022.

〔16〕 See Mark Zuckerberg, Founder's Letter, 2021, Meta, available at https://about.fb.com/news/2021/10/founders-letter/, last visited on Aug. 29, 2022.

〔17〕 See Izabella Kaminska, The metaverse is just the latest incarnation of Las Vegas, Financial Times, available at https://www.ft.com/content/739235bc-c418-4895-a426-3bd245ec6a00, last visited on Aug. 29, 2022.

〔18〕 参见於兴中、沈岿：《“元宇宙”：玩家的利益与知识分子的责任》，载“中国法律评论”微信公众号，2021 年 12 月 20 日。

和损失。然而，有效监管需要时间，也很难在全球范围内实施。重要的是，首先要认识到对元宇宙监管的必要性。元宇宙不再是科幻，必须要考虑它可能带来的威胁，无论是对个人消费者还是对企业。如果元宇宙真正可行，监管机构和这些虚拟空间的设计者现在就应该努力确保其用户的安全。元宇宙存在着风险。现实世界和虚拟世界的交融预示着一种大的社会转变，存在对现有法律制度、财产制度以及消费者隐私的挑战，因此我们不得不慎重对待。

（一）元宇宙中的风险

元宇宙中的交易充满风险。首先，我们在虚拟世界中交换的不是传统意义上的货币，它们要么是加密货币，要么是《堡垒之夜》（V-Bucks）中的游戏内货币。可能有账户或钱包来存储这些资产，但没有政府支持的保护措施来防止损失或欺诈。其次，我们在元宇宙中买卖东西的价值不如现实世界中那么明显。一个不可替换（非同质）的代币（NFT）或一块虚拟房地产可能看起来有价值，但情况并不一定如此，也没有退款权或其他的消费者保护。再次，还有更多的传统风险，如欺诈。我们还不知道网络犯罪分子可能利用元宇宙的所有方式。但比较清楚的是，无论是通过黑客攻击还是身份盗窃，虚拟世界并不能避免现实世界已经存在的安全问题。更重要的是，我们在心理上也面临重大风险。如果元宇宙看起来和感觉起来像现实世界一样，但却不受刑法的约束，并且有更极端的体验，那么就会有围绕创伤和负面心理健康影响的重大风险。

（二）前所未有的社会转型

元宇宙意味着从以第三人称观看的平面媒体到以第一人称体验的沉浸式媒体的巨大社会转型。用户的角色，从外部的观察者变成了内部的参与者。换句话说，现实世界和虚拟世界如何衔接、融合仍然是未知数。社会生活的方方面面都可能受到影响，但如何影响、影响多大，目前难以判断。自从互联网诞生以来，网络空间已经发生了很多变化，我们甚至可以预测未来的生活将受到影响。然而，未来可能比想象中离我们更近。元宇宙是一个三维的虚拟领域，用户可以利用先进的人机交互接口（HCI）技术与虚拟环境互动。元宇宙提供了一种虚拟现实的体验，让人们沉浸在不同类型或形式的现实中。它是物理现实和数字现实的混合体。我们正经历着生活方式的转变，如虚拟环境、增强现实应用程序、社交网络和虚拟世界。新技术将我们最疯狂的科学幻想变为现实，而这将改变我们的生活。一些人认为这是互联网的未来。我们将习惯于被限制在家里，与世隔绝，在巨大的虚拟景观中进行全球旅行。〔19〕另一方面，这种变化实际上意味着平台供应商，即管理这些大型平台的实体，将拥有更多的控制权、影响力和对人们生活的了解。消费者处于被动地位。这更充分证明了监管的必要性。

（三）对现行法律的挑战

元宇宙中的活动，包括经济活动，明显地对现行法律制度构成了挑战。

首先，虚拟身份的主体地位。元宇宙所构想的虚拟世界，是与现实世界平行和交互融合的数字化生存空间。相较于目前的平面 2D 互联网空间，其进化和发展表现在，人类可以其化身在元宇宙中生活、生产、交易、娱乐。如果元宇宙从梦想走进现实，就会形成两个世界，每个人都有自己的化身。由此引发的法律问题是，化身是否具有独立的法律主体资格，能否具有权利能力和

〔19〕 See K. Bavanaa, Privacy in the Metaverse, 2 *Jus Corpus Law Journal* 1 (2022).

行为能力，进而为其行为承担相应的法律责任。如果不具有独立的法律主体资格，而是由其“主人”承担责任，那么接下来会产生新的法律问题，比如如何界定元宇宙中化身的行为的性质。例如，当用户通过化身进行互动时，发生争吵该如何处理？如果发生在现实世界的人之间，很可能会违反侵权法（涵盖民事索赔，如疏忽或滋扰）或刑法（涉及非法行为和犯罪，如攻击、谋杀、入室盗窃或强奸）。如果一个化身袭击了另一个化身，是否可以将攻击和殴打的刑法适用于这种情况？我们怎样才能让化身为他们在元宇宙的行为负责呢？这将会很复杂，因为这意味着需要给化身赋予法律地位，让他们在法律体系中拥有权利和义务，允许他们起诉或被诉。这显然是很难做到的。此外，证明攻击或殴打也会更加困难，因为它通常需要“实际的身体伤害”。在元宇宙中，自然不会有实际的身体伤害。要证明化身所遭受的伤害、损失或损伤是很有挑战性的。〔20〕

其次，虚拟资产的确认和保护。元宇宙中的交易通常使用加密货币或 NFT（不可伪造的代币）。NFT 是一种独特的数字资产，它可以是一张图片、一段音乐、一段视频、一个三维物体，或其他类型的创意作品。很难说这是一种趋势还是一种新的和令人兴奋的资本投资形式。这些类型的交易提出了一些有意义的法律问题。〔21〕例如，在“现实”世界中，当涉及购买一件艺术品时，财产法规定，所有权针对的是实际的实物艺术品。买方可能拥有也可能不拥有艺术作品的知识产权，这取决于销售条款。但是，在数字艺术的交易中，买者所拥有的并不是实物艺术品。这种所有权究竟包括什么样的权利？是一种许可形式，还是一种服务？在这种情况下，真正的所有权可能仍然属于所有者。这可能意味着，没有真正所有者的许可，买方不能出售该物品。虚拟房地产也已成为一种 NFT，个人或者公司花费巨资在元宇宙中拥有某种“房地产”。现实世界的土地法能在这里适用吗？比如，现实世界的法律能否用于制止元宇宙中私人土地上的入侵者？这种“房地产”能办理抵押贷款吗？

再次，个人数据的隐私问题。元宇宙中另一个对法律的挑战是对数据的有效保护。元宇宙中化身间的互动将暴露出个人数据的多样性。这可能包括面部表情、手势和其他类型的反应。这些都需要有效的保护。欧盟的《通用数据保护条例》（GDPR）、英国的《数据保护法》已有相关规定。但是，鉴于元宇宙的新颖性，为了确保用户的权利得到保护，可能需要重新审视这些法律中有关数据处理的规定和程序。

最后，知识产权问题。互联网已经给音乐家、电影制片厂和软件业带来了大量的版权问题，而元宇宙也可能会有自己的一系列版权问题。根据美国法律，美国的版权保护适用于“固定在任何有形表达媒介中的原创作品”〔22〕。元宇宙的许多方面都有可能受到版权保护，如软件、图形、视频和音频记录。虽然元宇宙可能会给版权人提供保护，但也有潜在的风险和挑战。版权作品的盗版可能是一个问题，当版权作品的使用很少时，版权所有者在证明版权侵权时可能会遇到问题。

---

〔20〕 See Brandy Tricker, Taming the Wild West: Solving Virtual World Disputes Using Non-Virtual Law, 35 *Rutgers Computer and Technology Law Journal* 138 (2008).

〔21〕 See Ahad Syed, NFTs: Sharks and Shards: What Are Fractional Nonfungible Tokens and Are They Subject to Securities Regulation?, 110 *Illinois Bar Journal* 18 (2022).

〔22〕 See Copyright, LYNN University, available at https://www.lynn.edu/university-policies/volume-i-governance-and-administration/copyright-policy, last visited on Aug. 29, 2022.

商标在元宇宙中也可能是有效的。商标是一种知识产权，由文字、图形、字母、数字等要素组成，用于识别具有特定来源的产品或服务并将其与其他产品或服务区分开来。商标法防止未经授权的第三方以任何可能淡化商标的方式使用该商标。〔23〕如果有人创建了一个模拟现实世界的虚拟世界，里面有商店、餐馆和咖啡馆，并包括星巴克、Applebee's 之类的标志，这些品牌的商标所有人就有理由对创建该虚拟世界的实体提起诉讼，因为这将使一个理性的人相信商标所有人拥有或赞助这些虚拟企业。元宇宙为新形式的沉浸式娱乐提供了无限机会，包括游戏、电影、音乐、音乐会和节日。这意味着有关知识产权的法律和法规需要与时俱进，涵盖新的知识关系。

所有这些都使监管变得至关重要，尽管说到监管，人们尤其是内容创作者会感到紧张。需要监管的不仅仅是平台供应商，也包括消费者个人。

五、规范元宇宙的可能性

（一）主要研究路径

21 世纪初，随着虚拟游戏的发展，虚拟世界（virtual reality）引起了法律学者和从业者的注意，他们在各种背景下探究了虚拟世界与现实世界法律之间的关系，重点关注现实世界的法律可以或应该在多大程度上适用于虚拟世界活动，以及虚拟世界治理和争议解决的相关问题。〔24〕近年来国外出现了大量研究虚拟世界相关法律问题的文献，其研究进路包括：第一，现有“真实世界”的法律规则如何可能以及是否应该适用于虚拟世界。〔25〕这方面研究有的是描述性的，对现有“真实世界”法律是否确实适用于虚拟世界活动进行研究；有的是规范性的，探究现有“真实世界”法律是否应该适用于虚拟世界活动；有的两者兼而有之。第二，从虚拟世界的视角看待法律与虚拟世界的关系，从虚拟世界活动和争议开始，回望现有的“现实世界”法律学说或制度对虚拟世界治理〔26〕或解决虚拟世界争端的适切性。〔27〕第三，两个世界融合的视角。将虚拟世界视为“边界或边界空间”，参与者及其互动是在虚拟和现实之间来回穿梭，法律机构如何处理虚拟与真实之间的这种交叉融合，并说明两个世界的边界及其上出现的各种问题。〔28〕

另一个值得关注的研究进路，是从社会法律（socio-legal）的角度，探究虚拟世界本身和内部的合法性构建和执行，以及社会秩序的维护。研究法律与虚拟世界之间关系的最早作品之一，就是运用了社会法律/法律人类学的视角来构建虚拟世界中的合法性。〔29〕在《第二人生》中，法

〔23〕 See Theodore C. Max, Trademarks in the Veldt: Do Virtual Lawyers Dream of Electric Trademarks, 101 *The Trademark Reporter* 282 (2011).

〔24〕 See Jack M Balkin & Beth Simone Noveck eds., *State of Play: Law, Games, and Virtual Worlds*, New York University Press, 2006.

〔25〕 See Caroline Bradley & A Michael Froomkin, Virtual Worlds, Real Rules, 49 *New York Law School Law Review* 103 (2004).

〔26〕 See Michael Risch, Virtual Rule of Law, 112 *West Virginia Law Review* 1 (2009); Michael Risch, Virtual Third Parties, 25 *Santa Clara Computer and High Technology Law Journal* 415 (2009).

〔27〕 See Kevin W Saunders, Virtual Worlds—Real Courts, 52 *Villanova Law Review* 187 (2007).

〔28〕 See F Gregory Lastowka & Dan Hunter, The Laws of Virtual Worlds, 92 *California Law Review* 1 (2004).

〔29〕 See Eric M. Fink, The Virtual Construction of Legality: Griefing and Normative Order in Second Life, 21 *Journal of Law, Information and Science* 89, 90, 91 (2011).

律和社会秩序问题表现得尤为明显。这些研究关注的重点不是现实世界法律与虚拟世界之间的连接，“真实世界”法律如何适用于（或是否应该适用于）虚拟世界活动，或者“真实世界”法律理论或机构如何适应虚拟世界治理和争议解决，而是虚拟世界居民自身对合法性的构建和体验。这种方法将虚拟世界社会关系作为一种新兴属性的社会规范和非正式秩序加以考察。

（二）虚拟世界的法律关系

对虚拟世界法律问题的研究很多是以《第二人生》为案例素材的。《第二人生》是一个在线虚拟世界或多用户虚拟环境，参与者通过化身参与常规的或非常规的线上活动，在虚拟空间实时与他人互动。其开发和运营者林登实验室（Linden Lab）将其描述为一个由居民创建的三维虚拟世界，自 2003 年向公众开放以来发展迅猛，如今全球数百万居民居住在这个虚拟世界中。在这个庞大的数字大陆上，充满了人、娱乐、体验和机遇，定居者在这里建造房子，进行创作并被他人的创作所包围。在这里数字创作的知识产权受到保护，居民之间可以进行买卖和贸易。该市场支持每月通过世界贸易单位林登币（Linden dollar）进行的数百万美元的交易，林登币可以在几个繁荣的在线林登币交易所兑换成美元。虽然《第二人生》在某些方面类似于多人电脑游戏，但它的特点在于，该活动是开放式的，而不是由特定的目标和角色驱动。此外，与大多数电脑游戏不同，《第二人生》明确允许并认可“真实货币交易”。

在《第二人生》的虚拟空间中，几乎可以遇到“真实”世界的每一个可以想象的合法和非法方面，但是明显缺乏一个重要的现实世界的特征，《第二人生》没有正式的法律制度，也没有解决居民之间纠纷的法律机制。然而，缺乏正式的法律体系并不意味着在《第二人生》中不会出现“法律问题”，这也是本文所关注和研究的基本问题。居民之间的互动和争议可能引发与不动产、动产和知识产权相关的问题，合同和商业交易、诽谤和隐私、公民权利和自由、犯罪与惩罚，以及其他各法律领域的问题。〔30〕巴尔金（Balkin）提炼了虚拟世界的六种基本关系：（1）平台所有者和国家之间的关系，关于游戏空间的设计、维护以及管理问题；（2）玩家和国家之间的关系，关于玩家参与游戏空间的规则；（3）玩家和平台所有者之间的关系，关于玩家和平台所有者在游戏空间的规则；（4）玩家之间关系，关于一方的游戏空间内的活动是否侵犯了另一方的合法权利；（5）平台所有者与未玩游戏的第三方之间的关系，关于游戏空间内的活动是否损害了第三方受法律保护的利益；（6）玩家和未玩游戏的第三方之间的关系，关于玩家的游戏空间内的活动是否损害了第三方受法律保护的利益。〔31〕

姆努金（Mnookin）描述了早期基于文本的虚拟世界 LambdaMOO 中发展起来的非正式规则体系和争议解决系统。在这个虚拟空间中，新规则将由全体居民投票表决，如果获得三分之二的多数票，则予以通过。虚拟空间中发生的纠纷和争议提交给有约束力的仲裁机构，仲裁员由居民自愿担任。姆努金研究发现，大多数纠纷都与虚拟世界中的产权和言论自由有关，虚拟世界的性质受到居民理解虚拟世界活动与现实世界法律之间的关系隐喻的影响，其将虚拟世界分为四种类型，即社交俱乐部、村庄、独立的国家和角色扮演游戏。在“社交俱乐部”的隐喻中，虚拟世界

〔30〕 See Benjamin Duranske, *Virtual Law: Navigating the Legal Landscape of Virtual Worlds*, American Bar Association, 2008.

〔31〕 See Jack M. Balkin, Law & Liberty in Virtual Worlds, 49 *New York Law School Law Review* 63, 67 (2004).

的活动本质上与现实世界的法律具有相关性。在“村庄”的隐喻中，虚拟世界被视为现实世界的一个子集，居民在尝试纠纷内部解决后，仍然可以寻求现实世界的法律救济。“独立国家”的隐喻则意味着一个充分发展的治理体系，独立于现实世界的法律体系。“角色扮演”隐喻将虚拟世界的活动视为一场游戏，除非虚拟世界的行为会造成现实世界的损害，现实世界的法律将不适用于虚拟世界。〔32〕

LambdaMOO 虚拟世界的建构无论是程序性的还是实质性的社会规范，都强烈依赖于现有法律模式，这表明了将虚拟现实视为与现实生活完全不同的范式的局限性。任何虚拟世界既不是完全自主的，也不是对现实世界法律的简单模仿，它是融合了现实世界的法律概念以及制度变化和创新理念的一种法律形式。这些隐喻在《第二人生》中具有相同的效果。虽然《第二人生》的居民通常会表达与“村庄”和“独立国家”的隐喻一样的情感，试图在《第二人生》中建立相对或完全自主的正式法律制度，在虚拟世界活动和“现实世界”规则之间保持鲜明的区别，但是迄今为止没有任何一个取得成功。〔33〕虚拟世界居民在缺乏正式法律体系和官方法律机构的情况下构建非正式规范秩序的方式，〔34〕值得进一步研究和探讨。虚拟世界与现实世界在法律关系上具有同一性、关联性和相似性，虚拟世界的规范秩序建构依赖于现实世界的法律概念、原则和制度。元宇宙与虚拟世界在构成和性质上有区别吗？元宇宙有哪些特殊的问题？以上研究为我们进一步观察元宇宙能否成为法学的研究对象，现实世界的法律应否适用于元宇宙提供了研究模板和参照对象。

（三）政府监管的可能性

世界各国政府在过去几十年里，通过政策和立法加强对互联网的规制和网络空间活动的控制，监管机构尝试为数字领域起草和实施规则。虽然数字版权管理（DRMs）以及其他类似的技术解决方案的结果记录好坏参半，但不可否认的是，对网络和虚拟空间的法律规制和监管争论是近年来围绕数字科技发展的主要事件和基本特征。对 2D 互联网最有效的政府监管方式是一种对门户进行的管制，虽然这种方式的最初意图是让 ISPs 对发布的内容负责，但这也推动了一系列的立法解决方案，其中包括对平台的责任豁免。〔35〕如果互联网能够受到私人实体和政府、国际机构的合理监管，那么元宇宙是否需要完全不同的监管方式？至少从目前对元宇宙的构想来看答案是否定的，大部分适用于网络空间的法律解决方案都可以适用于元宇宙。〔36〕

以管辖权为例，近年来最重要的信息法争议问题是将国家立法适用于国际数字媒体平台。在司法领域的主要障碍是试图确定法院如何以及何时对其他国家的法人和自然人行使管辖权。另一个问题是内容提供商是否应该受制于世界上所有的司法管辖区，因为他们的作品位于那个国家。虽然要回答和解决这些问题是困难的，但目前已经出现了解决该问题的立法方案和符合法律逻辑

〔32〕 参见前引〔29〕，Eric M. Fink 文，第 95 页。

〔33〕 See Greg Lastowka, *Virtual Justice: The New Laws of Online Worlds*, Yale University Press, 2010, p. 9.

〔34〕 参见前引〔29〕，Eric M. Fink 文，第 89－111 页。

〔35〕 See Ethan Katsh, Bringing Online Dispute Resolution to Virtual Worlds: Creating Process Through Code, 49 *New York Law School Law Review* 271 (2004).

〔36〕 See Andres Guadamuz, Back to the Future: Regulation of Virtual Worlds, 4 *A Journal of Law, Technology and Society* 242 (2007).

的司法判决。〔37〕

网络空间的争论转移到虚拟世界是否具有相同的意义？《第二人生》是否能够受到法律的约束？如果出现法律纠纷，是否可以向法院起诉？答案是肯定的。虚拟世界按照区域划分有三种类型：全球、区域和国家。全球每个人只要有账户和互联网就可以访问虚拟世界，例如《星战前夜》和《第二人生》。区域虚拟世界《魔兽世界》《英雄之城》和《天堂》的居民限定在某一特定地区或管辖范围内，即有明确的不同服务器之间内容的地理分隔。目前，区域性虚拟世界存在的原因主要有：在技术性方面，区域或国家服务器往往连接较少，可以更便宜的运行和维护；在语言方面，有些游戏可能需要对客户端进行语言的修改；在社会、文化方面，游戏可能没有全球性的吸引力，但玩家可能喜欢和说母语的人一起玩；在法律方面，通过拥有符合特定法规的区域服务器来减少潜在责任。

这些区域服务器的实施本身就是很好的例证，对虚拟世界的监管不仅是可能的，而且是现实的。用户必须建立账户才能参加游戏或进入虚拟环境，这可以限制从多个国家 IP 地址连接的用户，或提供商可以采取支付限制，即你必须在某个国家拥有一个银行账户才能创建该虚拟账户。这种对潜在用户的审查有助于通过最终用户许可协议［End-User License Agreements（EULAs）］、支付方式，甚至通过他们的互联网服务提供者将用户进行潜在身份识别和捆绑。〔38〕元宇宙带来的科技进步有可能再次改变进入虚拟世界的方式，引导和改变我们生活的某些方面，如当前热烈讨论的区块链技术导致的去中心化效应。然而，让人惊叹的新技术之美不应该让我们忽视这样一个事实，即政府通过技术创新、迭代和升级实现对社会的管控，既包括现实世界也包括虚拟世界。而法律规制和政府监管对虚拟世界来说是必需的，元宇宙也不例外。未来，我们可能像谈论网络空间一样谈论元宇宙，两者之间甚至可能没有任何区别。

（四）规范元宇宙的几个议题

1. 私权力的宪法规制

对私权力进行宪法规制可以追溯至 20 世纪 60 年代巴龙（Jerome A. Barron）发表在《哈佛法律评论》上的一篇重要文章，其标志了私权力宪法规制研究的开端。他关注对个人言论进行审查的私权力，认为对美国言论自由最大的威胁不是国家，而是大众媒体对个人言论的压制。〔39〕此后，学术界的讨论主要围绕传统媒体权力与法律规制，对表达自由进行控制的新媒体私权力形式和文化实践，国会立法和政府监管以及法院宪法解释对私权力与基本权利的权衡。21 世纪以来，大科技公司主导和推动了信息和数字技术的发展，由此形成的技术权力具有私权力的基本特征，形成了新的宪法权利和权力关系。数字平台的审查是附带性审查，具有与政府合作和融入的特征，数字平台责任是促进公私合作的一种策略，而美国私人平台责任豁免将导致新的宪法权利危机。新兴技术对社会的影响不仅是市场性的，而且是非市场性的，竞争法和反垄断法已经不足以应对上述挑战，传统的私法救济在面对私权力时凸显其理论困境。巴尔金认为，数字人权的保

〔37〕 See Dow Jones v. Gutnick［2002］HCA 56.

〔38〕 See Farnaz Alemi，An Avatar's Day in Court：A Proposal for Obtaining Relief and Resolving Disputes in Virtual World Games，11 *University of California Los Angeles Journal of Law and Technology* 1（2007）.

〔39〕 See Jerome A. Barron，Access to the Press—A New First Amendment Right，80 *Harvard Law Review* 1461（1967）.

障需要对私权力进行宪法规制。〔40〕

今天的互联网是几十年来通过政府研究实验室、大学、独立技术专家和机构的工作建立起来的。这些大多为非营利性的集体组织，通常专注于建立开放标准，帮助服务器共享信息，就未来的技术、项目和想法进行协作。任何人都可以从任何设备、任何网络上访问或构建互联网，成本很低甚至没有成本。然而，“企业互联网”是当前元宇宙的期望，元宇宙正由私营企业开拓和建设。2016年早在全世界企业高管认真考虑元宇宙之前，Epic Games的斯威尼（Sweeney）告诉VentureBeat：“如果一家中央公司获得元宇宙的控制权，他们将比任何政府都强大，它将成为地球上的神。”Nvidia创始人兼首席执行官黄仁勋（Jensen Huang）认为，元宇宙的GDP最终将超过“物质世界”。元宇宙的概念意味着我们生活、劳动、休闲、时间、财富、幸福和人际关系中越来越多的部分将在虚拟世界中度过，而不仅仅是通过数字设备来辅助生活。它将位于我们的数字和物理经济之上，并将两者结合在一起。因此，控制这些虚拟世界的公司将比当今数字经济中的领导者更具有统治力。〔41〕

元宇宙将使当今数字社会存在的诸如数据权利、数据安全、虚假信息、数字人权、平台监管等难题更加尖锐。在元宇宙时代处于领先地位的大科技公司的哲学、文化和优先事项将决定我们未来的世界。从宪法的角度来看，承认或者不承认像Meta这样的大公司的宪法地位，以及它是否有可能改变我们现有政治权力的结构，是一个重大的宪法问题。扎克伯格曾经明言，Facebook事实上更像一个政府，而不是传统意义上的公司。〔42〕Facebook有自己制定规则、自己执行、自己裁决的实践。此外，元宇宙与之前的虚拟世界的区别在于区块链，区块链在元宇宙中的应用有两个主题：虚拟货币和虚拟资产。未来元宇宙将发行自己的货币或者类似的凭证，现在的美国，比特币、各种代币、加密货币等等已经形成了初具规模的市场，实际上对美元形成了一定的冲击。当前热议的是区块链技术将产生去中心化效应，但也有学者对此持怀疑观点，区块链和元宇宙是不是一个共生关系，现在没有明确答案，关于虚拟资产区块链解决的仅仅是记账的问题，不能解决虚拟资产体现出的自身使用价值问题。更核心的问题是，本质上来讲元宇宙一定是中心化的，元宇宙的构建需要规则，那么这些规则都需要中心化才能实现。〔43〕这是一个宪法上应该考虑的问题。当然，更重要的宪法问题是，由于化身的普遍化，如何来界定“现实—虚拟”这种状态下的人的身份。传统宪法和宪法学考虑到的是自然人和法人（拟制的人），但是没有考虑过虚拟的人（virtual person）。研究者应在宪法层面提前关注化身和主人，虚拟人和现实中的真人之间的互动与调节，界定一个或数个化身与真人及他人（真人或化身）之间的法律关系。

在线视频游戏以及托管和营销游戏的平台带来的教训和风险是：如果不加以控制，私人公司

〔40〕 See Jack M. Balkin, Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation, 51 *University of California Davis Law Review* 1149, 1187 (2018).

〔41〕 参见前引〔13〕，Mathew Ball文。

〔42〕 See Henry Farell, Margaret Levi & Tim O'Reilly, Mark Zuckerberg runs a nation-state, and he's the king, Vox, available at https://www.vox.com/the-big-idea/2018/4/9/17214752/zuckerberg-facebook-power-regulation-data-privacy-control-political-theory-data-breach-king, last visited on Aug. 29, 2022.

〔43〕 参见前引〔11〕，贾韬文。

和资本将以逐利为目的，把元宇宙带入危险的环境中。目前很多国家已经开始对元宇宙游戏系统进行立法规范。例如，《欧盟指令 2010/13》（Directive 2010/13 EU）修正案寻求将服务监管与线上电视视频相结合，包括特定的视频共享平台（VSP），以保护未成年人免受有害内容的影响。其他欧洲国家开始建立网络规制体系。18 岁以下儿童及青少年是新的英国《适龄设计规范》（ICO Age-Appropriate Design Code）关注的主要对象，该规范于 2021 年 9 月生效。该规范建议一定的默认程序设置，包括儿童个人数据处理服务的设计。一项新的德国法律《联邦青年保护法》（Jugendeschutzgesetz-JuSchG）于 2021 年 5 月 1 日生效，其立法目的在于保护儿童和年轻人免受新媒体消费的伤害，并且保证媒介的传播或获得是按照年龄分类而执行。各种类型的媒体和出版物涉及年龄分类，包括不道德和暴力内容、详细的暴力行为展示、大屠杀、获取正义的弱肉强食法则的建议等。法国也开始立法规范线上行为。一项待定的法国视听改革草案授予单一机构执行权力，视听和数字通信管理局［Audiovisual and Digital Communication Regulatory Authority（ARCOM）］被认为是新超级立法者，有能力规范在线平台、打击互联网有害内容、促进隐私保护。〔44〕而在所有国家的政策法律中都需要考虑的首要问题是，规范平台、开发商、投资者未能在平台上履行反线上有害内容义务时，应否承担责任以及如何承担责任。这些问题将在未来元宇宙时代继续呈现和发展。未来在很大程度上是不确定的，在建构元宇宙的过程中，谁来管控元宇宙是重要的议题，在宪法层面对元宇宙的私权力进行有效规制，对于塑造更美好的未来具有结构性的基础作用。

2. 个人数据保护

从数据保护的角度来看，未来元宇宙中 VR（virtual reality）技术进步和发展将涉及一些相关问题。VR 技术能够通过眼球追踪系统、面部识别系统和先进的传感器（如指纹、声纹、手和脸的几何形状、肌肉电活动、心率、皮肤反应、眼球运动检测、头部位置等）收集身体跟踪数据，为用户提供沉浸式和舒适的体验。尽管这项技术还没有完全投入大众市场，但已经出现了严重的隐私问题。与其他传统技术相比，VR 需要收集和处理越来越私密的个人数据，涉及欧盟 GDPR 的相关原则和规定。该类数据可被界定为生物识别数据（biometric data），即根据 GDPR 第 4（14）条，“与自然人的身体、生理或行为特征相关的特定技术处理产生的个人数据，能够确认该自然人的唯一身份，如面部图像或指纹数据”〔45〕。生物识别数据是一种特殊的个人数据类别，对它们的处理需要特别注意。GDPR 第 9 条规定除就业和社会保障法、至关重要和实质性的公共利益、预防或职业医学等某些有限目的外，禁止对生物识别数据（用于唯一识别自然人）进行处理，除非数据主体明确同意。〔46〕意大利数据保护局关于生物识别数据的一般申请令重申：处理生物识别数据需要提供信息通知；有关处理须得到数据主体的同意；生物特征数据必须通过适当的安全措施（例如加密）加以保护；含有生物特征数据的数据库必须能够访问和追踪；数据

〔44〕 See John Russel, *Metaverse For Beginners: A Complete Guide on How to Invest in the Metaverse, Copyright by John Russel*, 2022, pp. 37 - 40.

〔45〕 Art. 4 (14) GDPR, General Data Protection Regulation (GDPR), Definitions, available at https://gdpr. eu/article-4-definitions/, last visited on Jul. 22, 2022.

〔46〕 See Art. 9 GDPR, General Data Protection Regulation (GDPR), Processing of Special Categories of Personal Data, available at https://gdpr. eu/article-9-processing-special-categories-of-personal-data-prohibited/, last visited on Jul. 22, 2022.

必须保留至处理目的所需的时间。〔47〕其中，同意是生物识别数据收集处理的有效法律基础。衡量有效同意的核心是自愿原则，如果服务没有提供处理生物识别数据的有效替代办法，可以认为同意不是自愿的。值得注意的是，数据主体所谓的“虚拟隐私”在 VR 环境下可能与在非 VR 环境下不同，其隐私感知较现实世界低，事实上导致非自愿同意处理生物识别数据的情况比现实世界更为突出。因此，法律有必要严格规范 VR 处理生物识别数据，在数据主体没有任何有效的替代方案的情形下，认定该同意为非自愿，从而不能获得处理生物识别数据的许可。此外，VR 处理生物识别数据的必要性原则也应考虑在内，禁止或限制 VR 对个人生物识别数据的非必要使用和处理，对必要性原则在不同应用场景的适用规定条件和程序。根据 GDPR 第 25 条，默认/设计的隐私原则（privacy by default/design）要求产品/服务的设计和开发是为了保护用户的个人数据。特别是考虑到“处理大量生物识别数据对自然人的权利和自由造成不同风险的可能性和严重性”，VR 提供商应在处理数据时，实施适当的技术和组织措施，如匿名化和/或数据最小化，以满足 GDPR 的要求和保护数据主体的权利，并确保为特定目的处理个人数据的必要性。〔48〕根据 GDPR 第 35 条规定，VR 提供商在处理数据之前应进行数据保护影响评估［Data Protection Impact Assesement（DPIA）］。〔49〕随着数字技术的不断更新，包括 GDPR 在内的各国现有法律的有效适用必然会面临新的难题和挑战。在元宇宙背景下个人数据的跨境传输、未成年人数据的特殊保护、数据侵权责任归属及承担等与数据保护相关的一系列问题，都需要法律因应技术发展而做出跟进、改变和调整。

3. 刑法的适用问题

元宇宙中可能涉及的刑事犯罪，包括性骚扰、性侵犯、虚拟物/虚拟财产的盗窃、个人数据的盗窃、身份盗用、诈取、欺诈、洗钱和非法融资活动等。2016 年，一位名叫乔丹·贝拉迈尔的女性成为一次虚拟性侵的受害者，引发了法律界和虚拟现实界对虚拟行为造成实际伤害的可能性的思考。贝拉米尔后来写道，她对这起事件感觉是“真实的”并且遭到了“亵渎”。近日一名 21 岁女性受害者在 Meta 发行的《地平线世界》游戏中，创建了一个女性虚拟形象，遭到一位男性虚拟人物的“性侵”。另有媒体报道，一名日本游戏玩家阿基拉（Akira）在 VRchat 虚拟游戏中遭到其他虚拟玩家的性侵犯。〔50〕目前学界和实务界对此类事件如何定性尚不明确，存在争议。一种观点认为，身体未被触摸，也可以被判定为性骚扰，因为虚拟行为对人格和尊严的影响通常是确凿无疑的。另一种观点认为，“虚拟强奸”（virtual rape）目前很难被定义为真正的“强奸”。因为强奸罪一般要符合三个条件：行为违背被害人（一般指妇女）的意愿；行为人必须采取使妇女不能反抗、不敢反抗或不知反抗的手段，通常是暴力、胁迫或者其他手段；施暴人和受害人要

〔47〕 See Giangiacomo Olivi, Niccolo Anselmi & Claudio Orlando Miele, Virtual Reality: Top Data Protection Issues to Consider, 3 *The Journal of Robotics, Artificial Intelligence & Law* 141 (2020).

〔48〕 See Art. 25 GDPR, General Data Protection Regulation (GDPR), Protection by Design and by Default, available at https://gdpr.eu/article-25-data-protection-by-design/, last visited on Jul. 22, 2022.

〔49〕 See Art. 35 GDPR, General Data Protection Regulation (GDPR), Protection Impact Assessment, available at https://gdpr.eu/article-35-impact-assessment/, last visited on Jul. 22, 2022.

〔50〕 参见大千纪实：《“VR 侵害”频频发生？虚拟世界中的猥亵行为，受害者可以维权吗？》，载 https://baijiahao.baidu.com/s?id=1732160284422915432&wfr=spider&for=pc，最后访问时间：2022 年 8 月 29 日。

有实际的身体接触。就此次元宇宙“性侵”事件而言，“虚拟强奸”可能满足条件一，或可满足条件二，但是，条件三（即二者要有实际的身体接触）可能无从谈起。这是当前切实存在的现实法律困境。〔51〕从受害人的角度来看，虚拟性侵、猥亵或强奸的真实性是虚拟行为是否与现实世界刑法具有相关性的关键因素。虚拟现实的独特性在于用户的完全沉浸感，虚拟现实的目的是欺骗用户的大脑，让他们认为他们的虚拟体验是真实的。研究表明，在虚拟现实中被扇耳光的受试者会在皮肤、电导率和心率水平上有相应反应，就好像他们真的被打了一巴掌。〔52〕沉浸感（immersion）是虚拟现实与任何其他通信技术的区别，技术的发展会加强虚拟世界的沉浸感。随着现实和虚拟之间的界限变得模糊，用户对虚拟身体的感知将与真实身体攻击具有同样的心理反应。匿名、缺乏后果和游戏文化已经导致了虚拟世界中的无数性骚扰事件。相关研究数据显示，在 600 多名 VR 游戏受访者中，约有 49％的女性在虚拟空间受到过侵犯，包括语言猥亵和虚拟性侵，36％的男性受访者受到攻击和骚扰，这显然是一种新型网络暴力，其造成的创伤不亚于现实中的侵害。〔53〕

刑法对虚拟环境的干预是一项富有挑战性的法律改革。虚拟世界中的行为将不再停留在虚拟世界中，其行为后果及于现实世界。个人控制的化身在沉浸式虚拟环境中对另一个人控制的化身的行为造成了现实世界的实际损害，刑法应对此作出必要回应，考虑将现实世界刑法概念及原则与虚拟现实相结合，因为虚拟行为可以造成真正的伤害，行为人需要为其所操控的化身在虚拟世界的行为承担相应的法律责任。刑法为有效预防和惩罚这种伤害而采取的任何行动所应遵循的原则，必须能够处理将虚拟行为定为犯罪时所面临的复杂问题。归根结底，最重要的出发点是承认虚拟行为可能造成真正的伤害。这一原则可以作为未来处理元宇宙相关法律责任的法理基础。〔54〕对虚拟环境施加的任何监管都需要在政策法律上明确，沉浸式虚拟环境应该在社会中扮演角色，虚拟世界不应成为法外之地。当然，刑法干预只是规范虚拟行为可采取的众多选择之一。虚拟现实开发者也应该对惩罚违法者负责。实施了不法行为的用户可能会受到平台警告，在虚拟环境中面临处罚，或者被完全禁止进入该环境。一些平台已经引入了个人泡沫，如果一个用户干扰另一个用户的个人空间，他们就会从受害者的视线中消失。〔55〕计算机代码是一种可用于管理这些问题的规则形式。然而，平台或者元宇宙自治尚不足以规范严重违法或者犯罪行为，类似的见解可见于人工智能伦理的讨论。当虚拟世界的行为造成严重危害时，刑法的在场及出场是规范未来元宇宙有序发展的必要策略。这些原则也适用于未来可能在元宇宙中实施的其他违法或犯罪行为。

〔51〕 参见王小伟：《元宇宙“性侵”事件：如何在虚拟世界保护人的尊严》，载 https://baijiahao.baidu.com/s?id=1734239302666360393&wfr=spider&for=pc，最后访问时间：2022 年 7 月 22 日。

〔52〕 See Mark A Lemley & Eugene Volokh, Law, Virtual Reality, and Augmented Reality, 166 *University of Pennsylvania Law Review* 1051 (2018).

〔53〕 参见川味东子：《“VR”性侵事件！对于虚拟世界中的猥亵行为，受害人是否能维权?》，载 https://3g.163.com/dy/article/HADMKLFT05534KYC.html，最后访问时间：2022 年 7 月 23 日。

〔54〕 See Joshua Hansen, Virtual Indecent Assault: Time for the Criminal Law to Enter the Realm of Virtual Reality, 50 *Victoria University Wellington Law Review* 33 (2019).

〔55〕 See Katherine Cross, Sexual Assault Enters Virtual Reality, The Conversation, 10 November 2016, available at https://theconversation.com/sexual-assault-enters-virtual-reality-67971, last visited on Jul. 24, 2022.

六、结　论

约翰·佩里·巴罗曾在1996年发表了《网络空间独立宣言》，警告世界各国政府不要干预网络空间的独立性。今天，当人们讨论元宇宙议题时，可以很容易地将元宇宙与网络空间联系起来，再次重温网络自由的倡议，并构想未来元宇宙自由。未来数字新技术似乎保证了一种完全不同的监管方式，去中心化成为当下热议元宇宙的主要话题。所谓的网络自由论者的论点假设未来新技术在基本方式上是开创性的，从而需要一个完全不同于现实世界的监管方式。属于这一阵营的人倾向于看到网络空间，现在是元宇宙作为一个独立的王国，不受过时法律规则的约束和规范。本文认为，元宇宙从本质上来说，是一个虚实融合的数字空间，依附并依赖于现实世界。元宇宙无限度自由仅仅是一种乌托邦的想象，数字无政府主义最终导致的是失序与混乱，互联网的发展也验证了这一点。未来元宇宙的构建不仅是技术创新和迭代发展的过程，更是一个组织化、规则化和秩序化的过程，以法律规则为核心的秩序建构必然是再中心化而不是去中心化。法学研究的任务是从元宇宙空间的法律规范视角，提炼元宇宙的可能法律议题，深化虚拟世界和现实世界的法律概念、原则和制度的一般性与特殊性讨论，防范元宇宙可能的法律风险，探索构建元宇宙健康有序发展的社会秩序。

Abstract: Although “metaverse” is a concept that lacks a clear definition, the vision and imagination of “digital existence” reveal various possibilities for human beings to enter into digital social forms. The direction of the development of the metaverse depends on the choices and constructions of human beings themselves. The metaverse itself is not a method, nor a technology, but a commercial concept that integrates the three main characteristics in human nature: gaming (play), gambling and human tendency of pursuing interest. These three characteristics of man form the core of the metaverse. The virtual world and the real world share sameness, relevance and similarity in legal relations, and the construction of the normative order of the virtual world relies on the legal concepts, principles and institutions of the real world. The future metaverse is an order construction process of organizing, regulating and ordering with legal rules as the core. Legal and government regulation are necessary for the virtual world. Who will control the metaverse is an important issue. Effective regulation of the private power of the metaverse at the constitutional level plays a structural and fundamental role in shaping a better future.

Key Words: metaverse, recentralization, virtual world

(责任编辑：赵　真　赵建蕊)

财经法学 No. 5，2022
pp. 20 - 34

元宇宙的法律规制

丁道勤*

内容提要：元宇宙是通过虚拟现实或增强现实等数字技术形成的现实虚拟世界交融共生的数字生态系统。元宇宙放大并复杂化了现实世界的众多法律问题，如持续性非自愿的个人敏感信息综合采集所带来的隐私个人信息保护挑战、海量数据实时交互处理和加密网络技术的广泛应用冲击了数据安全保护体系、用户生成内容方式（UGC）对内容作品的确权和知识产权权益分配机制提出新挑战、跨平台一键登录和互操作的竞争反垄断等问题，以及缺乏统一可信的数字身份体系、数据资产确权利用规则不明晰、NFT 金融安全风险突出等特殊问题。元宇宙法律规制应坚持现实世界法律框架都能直接映射适用于元宇宙的基本原则，建议修订完善现有个人信息保护、网络数据安全及知识产权规则，延展制定元宇宙隐私个人信息保护的特别条款、数据全生命周期安全可信规范和 UGC 新的知识产权授权规则等。推动出台数字身份国家战略，通过数字身份专门立法建立统一分层次的数字身份体系，制定数据资产新的确权利用法律规则，从国家层面建立起统一的 NFT 监管框架。

关键词：元宇宙　数字身份　数据资产　非同质化代币（NFT）

元宇宙概念发端于《雪崩》，出圈于《头号玩家》《失控玩家》，爆火于被众多媒体称为“元宇宙元年”的 2021 年，更是在 2021 年 10 月 Facebook 更名为 Meta 后，引发全球行业追捧新热潮。元宇宙被描绘为不同于现实世界的另一个世界的蓝图，但元宇宙的内涵和外延仍是仁智互见，目前并没有统一的认知和概念。

从发展历程来看，互联网经历了三次重大变革时代。第一次是桌面互联网时代，即计算机普及带来桌面互联网，自 1971 年首款个人计算机（PC）诞生以来，其应用领域从科学研究、政府机构逐步走向家庭。到 20 世纪 90 年代互联网大发展，诞生了 IBM、微软、雅虎、谷歌、新浪、

* 丁道勤，北京航空航天大学工业和信息化法治战略与管理（工信部）重点实验室研究员。
本文仅为个人观点，不代表任何机构立场。

搜狐等大门户网站。第二次是移动互联网时代，标志是2007年第一代iPhone发布，加速智能手机普及，开启移动互联网时代。特别是2010年后，3G、4G驱动移动互联网大发展，全面颠覆人们的生活、体验以及价值认知，如网络购物、本地生活服务、手机游戏、移动社交等，诞生了Facebook、Twitter及国内的BAT等互联网公司。第三次是下一代互联网，如未来更加先进的AI、XR、大数据、云计算等都将围绕5G和6G产生变革，元宇宙正处于第三次互联网技术变革时期。

元宇宙承载了人类数字化转型的愿景，但技术变革的同时也带来了众多问题，例如，技术问题、经济问题、道德伦理问题、法律问题、社会治理问题，也引起社会各界的广泛关注。在元宇宙被热炒的当下，尤其需要冷静理性探究元宇宙本源法律问题。那么，元宇宙究竟有哪些特殊法律问题，是否为“法外之地”，又该建立怎样的法律规制体系，值得深入思考。本文尝试分析元宇宙的关键属性，探讨元宇宙带来的复杂性和特殊性法律问题，进而提出相关法律规制建议。

一、元宇宙的特性

从词源上看，metaverse有两个部分：meta源于希腊语，有“元”的意思，“元”意指最基础、最本源。verse是指universe，有“宇宙”的意思。因此，metaverse被顺理成章地翻译为了“元宇宙”。科幻小说《雪崩》中描绘了一个称为元宇宙（metaverse）的多人在线虚拟世界，用户以自定义的“化身”（avatar）在其中进行活动。〔1〕维基百科对元宇宙的描述是：通过虚拟增强的物理现实，呈现收敛性和物理持久性特征的，基于未来互联网，具有链接感知和共享特征的3D虚拟空间。元宇宙大致是生活在现实物理世界的自然人以“化身”或者“数字人”的方式，通过计算机操作系统，与其他数字人即时互动的3D数字虚拟空间，也是大部分人所认定的下一代互联网形态。〔2〕根据中纪委官网文章的定义，元宇宙是基于互联网而生、与现实世界相互打通、平行存在的虚拟世界，是一个可以映射现实世界、又独立于现实世界的虚拟空间。〔3〕综上，元宇宙是通过虚拟现实或增强现实等数字技术形成的现实虚拟世界交融共生的数字生态系统。

（一）关键特性

元宇宙的出现可能改变人类社会对于“自身存在”的主流认知，向虚拟时空的迁跃是信息技术和人类文明发展的必然趋势。作为人类社会的平行数字时空，著名分析师马特乌·波尔（Matthew Ball）认为，metaverse具有永续性、实时性、无准入限制、经济功能、可连接性、可创造性六大特征，metaverse不等同于“虚拟空间”“虚拟经济”，或仅仅是一种游戏抑或UGC平台。在元宇宙里将有一个始终在线的实时世界，有无限量的人们可以同时参与其中。它将有完整运行的经济、跨越实体和数字世界。Roblox首席执行官大卫·巴斯祖可（Dave Baszucki）认为，元

〔1〕 参见〔美〕尼尔·斯蒂芬森：《雪崩》，郭泽译，四川科学技术出版社2018年版。

〔2〕 See Haihan Duan, Zhonghao Lin, Jiaye Li, Xiao Xu, Sizheng Fan & Wei Cai, Metaverse for Social Good: A University Campus Prototype, Proceedings of the 29th ACM International Conference on Multimedia, 2021, pp. 153－161.

〔3〕 参见管筱璞、李云舒：《元宇宙如何改写人类社会生活》，载https://www.ccdi.gov.cn/toutiaon/202112/t20211223_160087.html，最后访问时间：2022年6月7日。

宇宙是一个将所有人相互关联起来的 3D 虚拟世界，人们在元宇宙拥有自己的数字身份，可以在这个世界里尽情互动，并创造任何他们想要的东西。归纳起来，元宇宙具备可靠的经济系统、强认同的虚拟身份、强社交性、开放自由创作、沉浸式体验等特点。从功能层面，元宇宙是一个承载虚拟活动的平台，用户能进行社交、娱乐、创作、展示、教育、交易等社会性、精神性活动。〔4〕综上，元宇宙的关键特征主要表现为沉浸式体验、强社交性、全息生存、自由创造、经济系统等。

（二）技术架构

元宇宙是 AI、区块链、5G、物联网、半导体、显示等技术的集大成者。业界普遍认为，元宇宙是基于 Web 3.0 技术体系和运行机制的数字空间。从科学角度，元宇宙实质上就是广义网络空间，在涵盖物理空间、社会空间、赛博空间以及思维空间的基础上，融合多种数字技术，将网络、软硬件设备和用户聚合在一个虚拟现实系统之中，形成一个既映射于、又独立于现实世界的虚拟世界。从技术角度，元宇宙不宜称为新技术，而是现有 IT 技术的综合集成运用，它是信息化发展的一个新阶段。〔5〕总之，现阶段元宇宙实则是智能化信息技术的一种集成创新应用生态。

有专家认为，元宇宙的计算基础可以用 BIGANT（“大蚂蚁”）来概括，B 是指区块链技术（blockchain），I 指交互技术（interactivity），G 指电子游戏技术（game）、A 指人工智能技术（AI），N 指网络及运算技术（network），T 指物联网技术（internet of things）。〔6〕也有专家认为，元宇宙框架为硬件入口、基础设施、底层技术、人工智能、内容、合作方六大组件，首先是提供元宇宙体验的硬件入口（VR/AR/MR/脑机接口），其次是支持元宇宙平稳运行的基础设施（5G/算力与算法/云计算/边缘计算）与底层技术（引擎/开发工具/数字孪生/区块链），再次是元宇宙中的人工智能，最终呈现为百花齐放的内容，以及元宇宙生态繁荣过程中涌现的大量提供技术与服务的合作方。〔7〕也有人认为元宇宙并不是游戏的升级版，而是 BAND（blockchain、game、network、display）各技术赛道的融合，BAND 构建了元宇宙的四大技术支柱，即区块链（blockchain）、游戏（game）、网络算力（network）和展示方式（display），分别从价值交互、内容承载、数据网络传输及沉浸式展示融合构建元宇宙。〔8〕还有专家认为，元宇宙本身的核心技术归类为两类半。一类是感知与交互技术，即“脑机接口”，现在用的 VR、AR 的设备，在某种程度上可以理解为广义的脑机接口。第二类是持久计算技术，即可以支撑持久存在的虚拟世界的技术，包括相关的计算基础设施、引擎与建模技术等。还有半类核心技术是虚拟资产，是对元宇宙有益的补充和助力，但并不是非有不可。〔9〕

（三）主要场景

元宇宙拓展了游戏娱乐行业，并与更多的实体行业进行交互延伸，最终形成虚拟现实世界的

〔4〕 参见宋嘉吉、赵丕业：《元宇宙：互联网的下一站》，国盛证券研究报告，2021 年 5 月 30 日。

〔5〕 参见王文喜等：《元宇宙技术综述》，载《工程科学学报》2022 年第 2 期。

〔6〕 参见赵国栋、易欢欢、徐远重：《元宇宙》，中信出版社 2021 年版，第 26－28 页。

〔7〕 参见焦娟：《科技巨头布局元宇宙系列报告 1：Facebook，改名为 Meta》，安信证券研究报告，2021 年 10 月 29 日。

〔8〕 详见前引〔4〕，宋嘉吉等文。

〔9〕 参见袁昱：《全球视野下的元宇宙全景与展望》，载 https://mp.weixin.qq.com/s/3aE2Yef6c2BwfBUPeb_gpQ，最后访问时间：2022 年 6 月 7 日。

交融一体，其主要应用场景有以下三大类：一是生活消费场景，主要包括游戏、虚拟社交、电竞、娱乐、智慧教育、医疗健康等，例如，Unity 和 Roblox 两大游戏制作平台让数百万创作者参与创作元宇宙游戏。二是经济生产场景，主要包括沉浸式电商、协同生产、工业数字孪生。三是协作空间场景，主要包括远程办公、全息虚拟会议、协作设计空间、虚拟地产、虚拟场馆、数字文旅等。

二、元宇宙的特殊法律问题

与桌面互联网和移动互联网时代一样，技术创新往往会推动监管创新，元宇宙相关产业在国内发展的潜在风险和法律问题，也引起相关监管部门的关注和警示。2021 年 11 月 19 日，新华社发文解码元宇宙指出，元宇宙在发展过程中，也将遇到价值伦理、虚拟空间管控等新问题，需要监管部门进一步进行规范。〔10〕2021 年 12 月 23 日，中纪委官网文章指出，目前元宇宙产业还处于发展初期，距离大规模产品化还十分遥远。元宇宙产业具有新兴产业的不成熟、不稳定等特征，还存在一些潜在风险。技术生态和内容生态尚未成熟，场景入口也有待拓宽，理想愿景和现实发展间仍存在漫长的“去泡沫化”过程。〔11〕2022 年 2 月 18 日，处置非法集资部际联席会议办公室（银保监会）发布《关于防范以“元宇宙”名义进行非法集资的风险提示》进行风险提示，一些不法分子蹭热点，以“元宇宙投资项目”“元宇宙链游”等名目吸收资金，涉嫌非法集资、诈骗等违法犯罪活动。元宇宙带来了先前未曾考虑到的新挑战和新变量，现实世界和互联网相关法律法规并不能覆盖元宇宙引发的所有问题。根据新技术新业务带来法律关系的调整、相关法律问题是否为元宇宙所特有为标准，元宇宙相关法律问题可以区分为映射延展问题和特殊性问题两个层面。

（一）映射延展问题

现实世界、桌面互联网和移动互联网现有的和众多悬而未决的法律问题，同样能映射和延展至元宇宙场景，并可能被放大而更加复杂化，例如，网络空间主权、内容安全、道德伦理、隐私个人信息保护、网络数据安全、知识产权、反垄断、刑事违法犯罪、税收等。这些问题并非元宇宙所独有，而是现实世界和互联网存在的法律问题映射到元宇宙场景之中。

其一，持续性非自愿的个人敏感信息的综合采集所带来的隐私和个人信息保护挑战。元宇宙是基于扩展现实技术向用户提供更真实的、沉浸式体验，意味着可能需要收集或导入更多的用户可识别信息，比如生物信息，这些个人敏感信息一旦泄漏或滥用，将对用户乃至整个元宇宙生态带来极大的隐患和冲击。有人甚至认为，元宇宙中无隐私，元宇宙是隐私荒地（privacy wasteland），〔12〕元宇宙将加工一些新类型的个人数据，包括面部表情、手势和其他分身在元宇

〔10〕 参见胡喆、温竞华：《什么是元宇宙？为何要关注它？——解码元宇宙》，载 http://gd.news.cn/newscenter/2021-11/20/c_1128081990.htm，最后访问时间：2022 年 5 月 24 日。

〔11〕 参见前引〔3〕，管筱璞等文。

〔12〕 See Edvardas Mikalauskas, Privacy in the Metaverse: Dead on Arrival?, available at https://cybernews.com/privacy/privacy-in-the-metaverse-dead-on-arrival/, last visited on Jun. 2, 2022.

宙交互时产生的反应。为了确保用户数据权利得到保护，关于数据处理的告知同意程序可能需要重新思考。〔13〕AR/VR 之所以带来了全新的用户隐私考量是因为：一是 AR/VR 设备由不同的信息收集技术组成，每一项技术都呈现出不同的隐私风险及相应的降低风险的方法；二是 AR/VR 设备收集的信息类型是其他一般消费者技术设备不收集的敏感信息；三是这种综合的信息收集对于 AR/VR 设备的核心功能至关重要。〔14〕因此，元宇宙场景中所使用数据的存储、处理和保护问题，以及数据被盗或滥用的责任问题，都是值得关注和亟待解决的。

其二，海量数据实时交互处理和加密网络技术的广泛应用冲击了数据安全法规的严格约束。元宇宙可能面临网络安全违规风险，如企业间谍、勒索软件攻击、国际网络战和老式黑客攻击都将转移到元宇宙。〔15〕元宇宙内不同应用之间、元宇宙和外部设备间的数据交互过程，以及外部设备采集、存储、处理、分发、利用和处置个人行为数据的过程，在技术层面上需要区块链相关的分布式网络、共识机制、智能合约、隐私计算等加以支撑，在法律层面上则需要受到数据安全相关法律法规的严格约束。〔16〕元宇宙中流通的海量数据以及这些数据的使用方式对用户构成了越来越大的安全风险，犯罪分子可以隐藏在加密及无法追踪的网络技术应用后面从而难以被识别并进行法律追踪，身份盗用、化身复制和滥用的风险为互操作性也带来了相应问题。〔17〕此外，元宇宙场景下的深度伪造内容（deepfake）带来的“非同意色情”、虚假新闻、名誉破坏、敲诈勒索、虚假证据、恶意商业竞争、负面社会消息、恐怖主义等现象引发对个人和社会两个层面的危害。〔18〕

其三，用户生成内容方式会对内容作品的确权和知产权益分配机制提出新挑战。元宇宙与桌面互联网和移动互联网很大的不同在于，元宇宙场景下的 UGC 方式，UGC 全称为 user generated content，也就是用户生成内容，即用户原创内容。UGC 的概念最早起源于互联网领域，即用户将自己原创的内容通过互联网平台进行展示或者提供给其他用户。第三方自由创造的内容，以及闭环经济体的持续激励，是元宇宙延续并扩张的核心驱动力。〔19〕元宇宙是一个交互平台，服务协议条款很可能允许用户对其个性化制作的分身和数字资产拥有知识产权。〔20〕在虚拟世界中创新是一个常态。2003 年，《第二人生》（一款游戏）没有采取行业惯例的做法，拒绝对其虚拟世界中生成的内容主张所有权，未来的游戏很有可能跟随这一做法。《第二人生》将版权所有权赋予了用户，这引发了版权法在虚拟创作上的适用问题。一方面推动传统版权法原则适用于虚拟世界引发了一系列问题，威胁创新，另一方面要求玩家转让其对虚拟作品的权利会抹杀

〔13〕 See Jerameel Kevins, Metaverse as a New Emerging Technology: An Interrogation of Opportunities and Legal Issues: Some Introspection, SSRN (March 6, 2022), available at https://ssrn.com/abstract=4050898, last visited on May 28, 2022.

〔14〕 See Pavan Duggal, *The Metaverse Law*, Kindle Edition, 2021, pp. 32 - 33.

〔15〕 See Jon M. Garon, Legal Implications of a Ubiquitous Metaverse and a Web3 Future, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4002551, last visited on Jun. 15, 2022.

〔16〕 参见董月英：《从法律视角看元宇宙发展的六个问题》，载《上海证券报》2022 年 2 月 17 日，第 8 版。

〔17〕 See European Parliamentary Research Service, Metaverse: Opportunities, Risks and Policy Implications, PE 733.557 - June 2022, available at https://www.europarl.europa.eu/at-your-service/en/stay-informed/research-and-analysis, last visited on Jun. 28, 2022.

〔18〕 参见华劼：《深度伪造内容著作权侵权问题研究》，载《电子知识产权》2022 年第 4 期。

〔19〕 参见前引〔6〕，赵国栋等书，第 103 页。

〔20〕 参见前引〔15〕，Jon M. Garon 文。

版权法所蕴含的激励机制。必须在鼓励创作和公共可获取性之间达成平衡，因为阻碍虚拟创新将威胁到虚拟世界自己的活力。〔21〕元宇宙带来了更多的挑战，即关于信息表达和虚拟创造是否受到法律保护、是否赋予所有权，在第三方信息层下方的支撑性内容是否属于修订或衍生作品的范围，引用或私人复制形式的著作权保护例外应如何适用的问题。〔22〕此外，元宇宙的知识产权问题还可能表现为擅自使用他人虚拟人形象，虚拟店铺中使用他人商标，侵犯他人受版权保护的游戏软件、角色、用户界面，数字资产是否具有《商标法》项下的商标资格，元宇宙应用的算法是否属于《专利法》保护的客体范围，以及知识产权侵权人身份不明时应向谁主张侵权责任等方面。

其四，跨平台一键登录和互操作的竞争反垄断问题。2020 年，Facebook 将其旗下的 Oculus 与 Facebook 账号绑定，要求用户用 Facebook 账户登入，连接社交和 VR 设备的数据，引发了德国联邦卡特尔办公室（FCO）的关注，FCO 主席认为，将 VR 产品和集团社交网络连接在一起可能构成滥用市场支配行为。〔23〕FIDO 联盟可通过没有密码的一键式登录、数据可自由携带、跨平台登录、互操作等方式，打破头部平台对数据账号和账户数据的控制权。延伸到业务领域，就可能出现利用垄断优势滥用信息的情况，从而产生垄断问题。此外，元宇宙很有可能出现平台经济中的自我优待问题，从 GAFA 的自我优待和反竞争行为可以看出，元宇宙平台可能优待自家产品，实施反竞争行为。〔24〕

（二）特殊问题

元宇宙的特殊问题主要表现为数字身份、数据资产、非同质化代币（NFT）。数字身份是元宇宙的起点和基石，基于数字身份及其身份行为产生的相关数据，积累于数字世界上的个人数据账户中，并进行挖掘、加工和增值利用，形成用户个人数据资产。用户再通过投资、创作、交易买卖形成数字化资产，典型的如通过记录各类数字资产权属的价值等价物的 NFT，搭建和丰富元宇宙的经济系统。

其一，缺乏统一可信的数字身份体系。元宇宙是承载人类虚拟活动的平台，是承载真人意识的数字体验，其核心在于可信地承载人的社交身份和资产权益。〔25〕Roblox 首席执行官大卫·巴斯祖奇（Dave Baszucki）指出，元宇宙的第一个关键特征是“身份”，且这种身份是可以自由设定并开发其“第二人生”的。〔26〕用户可以创建数字化身，以数字人或虚拟人身份在元宇宙进行生存、交互。数字化身代替了文本性的自我描述，个人可以在网络中通过替身的建构来获得身份，即在既定环境中形成他们的视觉形象、技能和态度以及他们的社会互动。因此，数字化身也

〔21〕 See Matthew R. Farley, Making Virtual Copyright Work, 41 (1) Golden Gate Univer Law Review 1, 1-32 (2010).

〔22〕 See Sophie Goossens, Christine Morgan, Cem Kuru, Fred Ji & DJ Cespedes, Protecting Intellectual Property in the Metaverse, 33 (9) Intellectual Property & Technology Law Journal 11, 11-16 (2021).

〔23〕 See Mason Marks, Biosupremacy: Big Data, Antitrust, and Monopolistic Power over Human Behavior, 55 UC Davis Law Review 513, 513-590 (2021).

〔24〕 参见前引〔15〕，Jon M. Garon 文。

〔25〕 参见前引〔4〕，宋嘉吉等文。

〔26〕 参见李章虎：《浅析“元宇宙”可能带来的法律挑战和解决路径》，载 https://mp.weixin.qq.com/s/czaepbduY-EY680kUKIzug，最后访问时间：2022 年 6 月 13 日。

被定义为一种用户交互式的社会表征。〔27〕元宇宙的核心在于增强“交互”，本质是用户肉身的数字化，并非用户肉身向元宇宙中“移民”。数字化身背后是元宇宙建设及其问题的起点与归宿——数字身份。〔28〕

数字身份作为数字主体的虚拟标识，关联了与该主体相关的属性信息，是其进行各种网络活动的支撑手段。数字身份管理是数字世界安全事务的核心，为鉴别、授权、访问控制、账户访问及其他各种与用户属性相关的应用提供支持。〔29〕用户的“身份”通过加密散列和时间戳记构成的分布式文件传输和存储系统，将得到前所未有的强化，甚至可以通过追溯政府颁布的出生证明、学历注册、工商登记和职业资格认证等信息，进行“盖戳”加密与固化，只能添加，不可篡改。而基于用户“身份”的一系列网络行为轨迹，例如图文与视频的发布、网购记录、大宗买卖、水电账单、商业合同、法证收集、生产供应链流程衔接等，都会通过属于每一个“身份”的资产通证（token）和智能合约运作，得到清晰的记录和戳记，甚至被智能合约自动推进。〔30〕当一个用户在元宇宙上通过化身进行交互时，如何确定所交互化身的准确性或合法性，元宇宙身份信息的可信认证研究就成为重要问题。〔31〕但是，目前我国尚没有建立起顺应数字时代发展的统一的可信数字身份体系。

其二，数据资产确权利用规则不明晰。在元宇宙里内容创作者是驱动经济发展的主要动力，元宇宙这种对现实世界底层逻辑的复制，让元宇宙成为坚实的平台，任何用户都能参与创造，且劳动成果受到保障。基于此，人们在元宇宙的劳动创作、生产、交易和在实际生活中的劳动创作、生产、交易没有区别。〔32〕用户基于个人数字身份，在数字世界中享受各类数字服务时，其在所有互联网平台上产生的本人相关的身份、行为、消费偏好、社交关系等所有数据都被关联起来，这些数据积累于各个平台的个人数据账户中。元宇宙更核心的问题可能是数据资产的确权问题，Web3.0 与 Web2.0、Web1.0 最大的不同在于，它是一个数据资产被确权的网络。〔33〕用户所产生的每个字段或轨迹信息，都可以进行定价，可以作为用户的虚拟财产进行确权。用户个人数据是数字世界的基石，以数据为生产要素的互联网服务提供者能够提升和改进现有的产品和服务，从而产生价值，也使得其所积累的数据得以变现，这就会衍生出数据流通利用的问题。因此，个人数据资产的核心问题在于个人数据如何关联、如何确权以及如何处置。

数据权属是数据利用和流通及数据产业化的逻辑起点，数据资产所有权的归属决定着数据价值利益的分配以及对数据质量、安全责任的划分。〔34〕数据确权和流通利用规则，在移动互联网

〔27〕 参见陆青：《数字时代的身份构建及其法律保障：以个人信息保护为中心的思考》，载《法学研究》2021 年第 5 期。

〔28〕 参见陈吉栋：《超越元宇宙的法律想象：数字身份、NFT 与多元规制》，载《法治研究》2022 年第 3 期。

〔29〕 参见国家质量监督检验检疫总局、中国国家标准化管理委员会：《信息安全技术 鉴别与授权 数字身份信息服务框架规范》（GB/T 31504—2015），引言。

〔30〕 参见骆轶航：《为什么 Web3.0 革命必将发生在中国?》，载 https://mp.weixin.qq.com/s/zEq6-CcyhjOb4Vyn4BngCw，最后访问时间：2022 年 6 月 14 日。

〔31〕 参见前引〔14〕，Pavan Duggal 书，第 19 页。

〔32〕 参见前引〔4〕，宋嘉吉等文。

〔33〕 此为万向区块链董事长兼 CEO 肖风先生的发言观点，有关数据资产的确权、授权和处置，笔者颇受启发，在此表示感谢。

〔34〕 参见丁道勤：《基础数据与增值数据的二元划分》，载《财经法学》2017 年第 2 期。

时代很难较好解决，但在元宇宙虚拟主体的场景下，就有可能得到解决。因为 Web3.0 商业模式的愿景和本质是在区块链上实现数据的确权，用户由此可以拥有、控制其在互联网上创造的数据并从中获利。〔35〕早在 1999 年，美国学者劳伦斯·莱斯格（Lawrence Lessig）教授系统提出数据财产化（data propertization）理论，他认为，应认识到数据的财产属性，通过赋予数据以财产权的方式，来强化数据本身的经济驱动功能，以打破传统法律思维之下依据单纯隐私或信息绝对化过度保护用户而限制、阻碍数据收集、流通等活动的僵化格局。〔36〕也有经济学者认为，在元宇宙中，用户应对其创造物享有所有权，企业应对虚拟财产享有所有权，以实现融资。例如，多角色扮演游戏（MMORPG）玩家在游戏中进行定制和创作，并将其中价值转换回现实世界。MMORPG 游戏证明，虚拟商品可以在现实世界具有相应价值，任何希望将用户引导到元宇宙的平台都必须允许用户赚钱，必须允许用户拥有其创造物，所有权是一个至关重要的问题。〔37〕现代虚拟世界运营的核心在于财产系统，这一系统具备现实世界的相同特征，如排他性的所有权、权利的存续、合同或强制条款的转让、货币系统。虚拟财产和其他无形、有时效的现实财产性权益之间几乎没有差异，不能因为虚拟财产并不“真实”而忽略虚拟财产的财产性权益。不论是边沁的功用主义，还是洛克的劳动论、黑格尔的人格论，都可以支持虚拟主体所主张的财产构成现实财产这一结论。〔38〕

其三，NFT 金融安全风险问题突出。非同质化代币（NFT）是表示数字或物理资产的所有权的数字证书，是数字资产的新形式，具有稀有和唯一性、不可篡改性、所有权可管理等特点。NFT 最早是在 2014 年为数字图像创建的，主要依赖区块链、NFT 市场平台、数字钱包等技术。〔39〕区块链是元宇宙的补天石，保障用户虚拟资产、虚拟身份的安全，实现元宇宙中的价值交换，并保障系统规则的透明执行。Web3.0 运动的领导者专注于找回因 Web2.0 而失去的财产权，通过使用 NFT 来强制执行财产、实现用户直接控制，以阻止企业过度扩张，Web3.0 可能矫正 Web2.0 的不平衡。〔40〕元宇宙独有的经济体系有可能会出现货币安全、金融诈骗等一系列问题。现阶段，除比特币外，NFT 是关键组成部分，其使得用户可以拥有、交易、购买、出售元宇宙资产和服务。NFT 记录了各类数字资产的创建和所有权，并将它们存储在区块链分布式账本中，该账本不可更改地分布在众多区块链用户之间，因此这些 NFT 记录不会发生单个结点故障。与所有权相关的这些创建和交易记录，使得每个 NFT 及相关艺术品或数字资产都是独一无二的，具有稀缺性和收藏价值。〔41〕因此，目前 NFT 主要应用于数字艺术藏品、虚拟房地产、游戏、供应链追

〔35〕 参见卢璟、夏彦、曾铮：《Web3.0 时代：数据保护法规将如何影响市场发展?》，载 https://www.toutiao.com/article/7107499463685538339/，最后访问时间：2022 年 6 月 19 日。

〔36〕 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。

〔37〕 See Cory Ondrejka, Escaping the Gilded Cage: User Created Content and Building the Metaverse, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=538362, last visited on Jun. 28, 2022.

〔38〕 See F. Gregory Lastowka & Dan Hunter, The Laws of the Virtual Worlds, 92 (1) *California Law Review* 1, 1-73 (2004).

〔39〕 参见美国政府问责局（GAO）：《NFT 概念、应用、风险、机遇和挑战》，载 https://www.gao.gov/assets/gao-22-105990.pdf，最后访问时间：2022 年 6 月 21 日。

〔40〕 参见前引〔15〕，Jon M. Garon 文。

〔41〕 See Michael D. Murray, Ready Lawyer One: Lawyering in the Metaverse, available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4082648, last visited on Jun. 28, 2002.

踪、健康医疗记录等领域。

对于 NFT 的法律性质，有“虚拟财产”和“权益凭证”等不同认识，〔42〕司法实践中多认定其为法律意义上的财产，例如，2022 年 6 月 6 日，纽约最高法院批准了一家总部位于美国的律师事务所“Holland & Knight”的申请，空投了 NFT 作为“服务通证”用于向被指控为黑客的被告发出临时限制令。在本案中，如果钱包所有者即被告未能在 30 天内对通知作出答复，案件将继续进行，法院可能将视为钱包所有者承认有罪，允许冻结被盗的数字资产。〔43〕2022 年 3 月，英国英格兰和威尔士高等法院裁定，NFT 构成法律意义上的财产，遭遇 NFT 被盗的权利人可向法院申请禁令，要求冻结相关账户，并强迫披露账户持有者信息。〔44〕新加坡法院与英国法院观点一致。2022 年 5 月 13 日，新加坡高等法院将 NFT 视为法律意义上的财产加以保护，发布禁令，在所有权争议纠纷解决之前，冻结以太坊链上的 Bored Ape Yacht Club NFT 作品的销售。〔45〕我国杭州互联网法院判决认为，NFT 交易的数字作品属于法律意义上的财产，NFT 数字作品交易行为受信息网络传播权控制，NFT 数字作品交易平台负有知识产权初步审查义务。〔46〕

NFT 交易可能引发以下特殊问题：一是 NFT 艺术作品的权属问题。NFT 所有者对其持有内容的权利范围有多大？在涉及知识产权的情况下，NFT 所有权是否本质上属于一种许可，作品所有权仍然归属主人，卖家在未取得主人同意的情况下不得销售作品？〔47〕如果艺术作品由多个匿名用户的分身完成，确定创作者的身份很难，在此情况下，法院如何认定合理使用？二是 NFT 房地产资产的权属。当虚拟房地产成为 NFT，用户和公司可花钱购买、享有一定财产权益，现实世界的土地法是否适用，现实世界的法律是否适用于入侵元宇宙私人领地的用户，是否可通过虚拟房地产获得抵押、进行融资？〔48〕三是隐私保护问题。如果没有进行适当的安全保护，分布式数字账本和数字钱包中的 NFT 信息可能会被公开访问，其中涉及的个人可识别信息会被其他用户看到。与垃圾邮件类似，用户可能会收到并不想要或非法的 NFT，比如包含网络淫秽内容的 NFT，因为有些交易是不需要接收者同意的。〔49〕四是金融安全问题。近期炒作 NFT 的现象显示，NFT 具有金融属性，可能受到证券、银行、货币等金融法律法规监管，尤其是 NFT 项目涉及利用分布式自治组织（decentralized autonomous organization，DAO）集资投资、分利润

〔42〕 参见前引〔28〕，陈吉栋文。

〔43〕 See LCX AG v. John Doe Nos. 1－25，Index No. 154644/2022（N. Y. Supreme，Ct.，2022).

〔44〕 See Lavinia Deborah Osbourne v. （1） Persons Unknown （2） Ozone Networks Inc. trading as Opensea，available at https://www. signaturelitigation. com/nfts-recognised-as-property-lavinia-deborah-osbourne-v-1-persons-unknown-2-ozone-networks-inc-trading-as-opensea/，last visited on May. 28，2022.

〔45〕 See Shaun Leong，Withers Obtains Worldwide Injunction for Singaporean to Freeze Sale of Rare Bored Ape Yacht Club NFT，Withers Khattar Wong （May 18，2022），available at https://www. withersworldwide. com/en-gb/insight/withers-obtains-asia-s-first-nft-freezing-injunction，last visited on Jul. 5，2022.

〔46〕 参见曲忠芳、李正豪：《“NFT 侵权第一案”镜鉴：元宇宙平台担责 三大安全风险待解》，载《中国经营报》2022 年 5 月 9 日，第 21 版。

〔47〕 See Sophie Goossens & Nick Breen，Ownership in the metaverse-the great illusion of NFTs，in Reed Smith，Guide to the Metaverse，2021，pp. 55－58.

〔48〕 参见前引〔13〕，Jerameel Kevins 文。

〔49〕 参见前引〔39〕，美国政府问责局文。

的情况。〔50〕2022 年 4 月 13 日，中国互联网金融协会等三协会发布《关于防范 NFT 相关金融风险的倡议》指出，NFT 作为一项区块链技术创新应用，存在炒作、洗钱、非法金融活动等风险隐患。2022 年 5 月 19 日，由新华社主办的《半月谈》官方公众号发布题为《别让“NFT”成炒作新宠》的文章，对国内 NFT 行业存在的金融化倾向、炒作倾向及产品竞争同质化等问题进行点评，认为一些数字藏品被拆分交易，打破了 NFT 的非同质化特性，可能促使 NFT 相关业务演变成非法集资、非法发行证券等非法、金融活动。同时，国内 NFT 发行方和交易平台尚未被强制要求对发行、售卖、购买主体进行实名认证，为 NFT 领域洗钱问题埋下隐患。〔51〕五是税收问题。在购买和出售 NFT 资产时，是否需要缴纳相关的所得税和销售税？例如，印度税务部门将于 2022 年 7 月 1 日起对虚拟数字资产（VDA）征税，包括加密货币和非同质化代币（NFT）。

三、元宇宙的法律规制建议

元宇宙治理问题是影响元宇宙发展的一个关键因素。从元宇宙整个行业来看，治理决定了未来元宇宙的行业格局。元宇宙相关的监管规则不仅复杂，而且已经成为摆在我们面前的现实问题。〔52〕基于元宇宙的构造，程金华教授认为元宇宙的基本治理逻辑在于：现实世界为元宇宙发展提供法治、现实世界与元宇宙交互时进行共治以及元宇宙内部生态系统建设和运行的自治。〔53〕结合上述元宇宙的法律问题，笔者进一步阐释认为，元宇宙的法律规制主要有三个层次：首先，现实世界的法律法规基本都能适用于元宇宙空间，是一种映射直接适用；其次，针对元宇宙放大而复杂化特定领域的法律问题，需要对现实世界法律法规做相应修改完善后，再进行延展适用；最后，就元宇宙特殊问题，有待制定新的规则，进行专门立法规制。

（一）映射直接适用

元宇宙并非“法外之地”。历史证明现实世界的政府完全有能力控制线上活动。3D 空间并没有什么独一无二的地方需要我们采取全然不同的监管路径，适用于网络空间的法律规则能够直接或间接地适用于元宇宙。〔54〕现实世界的法律是元宇宙治理的主要规则形式，这是毫无疑问的。毕竟，现实世界才是元宇宙的“母体”，而不是相反。〔55〕因此，现实世界的法律规则，基本都能同样映射延展适用于元宇宙空间。例如，欧洲议会强调，隐私和数据保护框架确实适用于元宇宙，其呼吁欧盟委员会确保在元宇宙中的公司和实体遵守现有法律框架。〔56〕再如，元宇宙空间里，发生的名誉权、名称权、姓名权、肖像权等民事侵权甚至是刑事犯罪行为，都能将现实世界

〔50〕 参见前引〔15〕，Jon M. Garon 文。

〔51〕 参见兰天鸣：《别让“NFT”成为炒作新宠》，载 http://m.banyuetan.org/jrt/detail/20220523/1000200033134991653012333494625312_1.html，最后访问时间：2022 年 6 月 8 日。

〔52〕 参见张晓添：《元宇宙有五大长期价值，大型互联网公司具备天然优势——对话德勤管理咨询中国元宇宙卓越中心领导合伙人王嘉华》，载《证券市场红周刊》2022 年第 20 期。

〔53〕 参见程金华：《元宇宙治理的法治原则》，载《东方法学》2022 年第 2 期。

〔54〕 See Andrés Guadamuz, Back to the Future: Regulation of Virtual Worlds, 4 SCRIPTed 242 (2007).

〔55〕 参见前引〔53〕，程金华文。

〔56〕 参见前引〔17〕，European Parliamentary Research Service 文。

的法律法规直接予以适用。

（二）延展修正适用

首先，完善制定元宇宙隐私和个人信息保护的特别条款。基于元宇宙具有的一些独特性质，当前一些个人信息保护规则可能并不能直接适用于元宇宙。据此，有人呼吁修订和更新欧盟《一般数据保护条例》（GDPR），GDPR 对由元宇宙带来的一些挑战和复杂性问题未作出相关规定，例如需要监管在无意识行为中收集的数据，或者与人工智能互动产生的数据。〔57〕因此，有必要修订完善现有个人信息保护规则，延展制定元宇宙隐私个人信息保护的特别条款，应强调隐私保护的基本原则，充分利用数据混淆（data obfuscation）、加密和聚合（aggregation）等数据技术，注意个人数据的存储，并探索契合元宇宙的个人数据使用规则。〔58〕

其次，完善网络数据安全配套法规。2015 年《国家安全法》对“数据的安全可控”作出原则性规定，2021 年颁行的《数据安全法》作为我国数据领域的基础性法律，确立了数据分类分级管理、数据安全审查、数据安全风险评估、监测预警和应急处置等基本制度。国家网信办发布的《互联网信息服务算法推荐管理规定》《网络音视频信息服务管理规定》《网络信息内容生态治理规定》《区块链信息服务管理规定》等规定，涉及元宇宙相关的算法推荐、内容治理、深度合成和数据出境等内容，初步建立起相关的监管规则。但是，在元宇宙内兼顾隐私保护和数据合规利用，系统至少应满足数据的全生命周期安全可信、用户自主控制数据、支持各方进行分布式协同治理这三个基本要求，元宇宙场景下数据都存储在用户自己或者受委托信任的节点上，各个节点构成一个“分布式自组织”（DAO）。〔59〕因此，有待进一步完善网络数据安全相关配套法规，加快制定多层次的数据安全相关技术标准规范，对元宇宙场景下数据的全生命周期安全可信、数据可携带自主可控、DAO 数据安全、内容治理、数据跨境等方面进行有效法律规制。

最后，修正形成新的知识产权授权和权益分配机制。虚拟世界中的创造大多具有衍生属性，虚拟创作者不太可能享有强的知识产权保护，因此，在版权法适用于虚拟世界之前，必须进行修订。版权法不适应虚拟世界中常见的合作型原创，很难将这种原创方式放进版权法的传统定义之中，只有改革规则才能促进有意义的分析。在版权法适用于虚拟世界的前提下，扩大合理使用在虚拟世界中的适用范围、推行虚拟衍生作品的强制许可将促进创新，更有效地实现版权法的目标。〔60〕总之，需要修正完善现有知识产权法律，顺应用户生成内容（UGC）方式的发展，形成新的知识产权授权和权益分配机制。

（三）专门立法规制

其一，构建统一的分层次的数字身份体系。身份认证成为用户访问元宇宙的“护照”。身份是 NFT 的基础，借由数字身份的建构，加之 NFT 作为流通工具，用户能够在虚拟空间与现实社会之间保持高度同步和互通。〔61〕数字身份被广泛认为是下一代身份认证手段系统，很多国家和

〔57〕 参见前引〔17〕，European Parliamentary Research Service 文。

〔58〕 See Rocio de la Cruz，Privacy Laws in the Blockchain Environment，SSRN（Mar. 19，2020），available at https://papers. ssrn. com/sol3/papers. cfm?abstract_id=3543901，last visited on Jun. 30，2022.

〔59〕 参见徐磊、赵扬：《元宇宙的隐私保护：技术与监管》，中金研究院研究报告，2022 年 6 月 20 日。

〔60〕 参见前引〔21〕，Matthew R. Farley 文，第 1－32 页。

〔61〕 参见前引〔28〕，陈吉栋文。

地区都已经陆续通过公共部门或私有部门采取行动来应对数字身份问题。例如美国积极实施可信数字身份战略，数字身份立法呈现出系统化趋势，并已在技术标准规范层面形成系统化指南，建立数字身份标准框架，美国商务部下属国家标准与技术研究院（NIST）发布经修订的第三版《数字身份指南》（Digital Identity Guidelines），美国比尔·弗斯特（Bill Foster）等议员提出了《2020年改善数字身份法案》和《2021年改善数字身份法案》。欧盟层面，欧洲议会和理事会2014年发布的《内部市场用于电子交易的电子识别（eID）和信任服务条例》（第910/2014号条例）是欧盟第一个数字身份立法，旨在为跨境电子识别、验证和网站认证提供基础。在第910/2014号条例的基础上，2021年6月，欧盟委员会发布《欧盟议会和欧盟理事会修订欧盟第910/2014号条例、建立欧盟数字身份框架的提议》，提出建立一个值得信赖、安全的数字身份框架，敦促成员国为公民设立数字身份档案系统。2020年3月，G7反洗钱金融行动特别工作组（Financial Action Task Force）发布《数字身份监管指引》（Digital identity Guidance），适用对象主要是政府、金融机构、虚拟资产服务提供商和其他受监管实体，主要规范因数字身份引起的洗钱风险。2022年3月，英国政府宣布启动数字身份立法，设立一个新的数字身份和属性办公室，旨在建立稳健安全的认可和认证流程和信任标识，确认数字形式的身份的有效性等同于实体形式的身份（如实体护照）。2018年9月11日，泰国通过《数字身份验证法案》（The Proofing and Authentication of Digital Identity Bill），旨在为成立数字身份验证监督管理委员会做准备，以落实提高泰国数字身份验证水平，并使之能够全面通过数字渠道进行的计划。

我国也出台了《居民身份证法》《反洗钱法》《网络安全法》《个人信息保护法》及其配套法规、技术标准等相关法律法规，规范真实身份认证等问题，但是还主要是单一应用账户模式，尚缺乏对更高阶段的联盟式和分布式数字身份模式的法律回应，更缺乏统一和专门的身份认证管理法律法规。从国外经验和相关行业实践来看，建议从以下三个层面构建我国可信数字身份法律体系：一是推动出台数字身份国家战略，构建一套包括专门立法、基础设施建设、技术标准规范和行业最佳实践等在内的数字身份战略体系。二是通过数字身份专门立法，建立统一的分层次的数字身份体系。数字身份体系包括身份层、验证层、应用层和数据层四个层次，身份层又可分为法定身份（基础身份）和商业身份（应用身份）。明确规定基于用户个人身份证号码建立起国家法定的、唯一的、权威的用户数字身份体系，商业机构等其他主体基于统一的法定的基础数字身份凭证，构建可信的商业数字身份，并基于基础身份凭证，实现可信数字身份在多个生态圈中的互联互通，打通法定身份和商业身份的互联互通，推动商业领域数字身份的跨平台登陆和互操作。三是推动国家数字身份基础设施建设，积极推进数字身份新技术研究，制定数字身份技术标准规范（国家标准、行业标准、团体标准、企业标准等），推动数字身份基本服务和商业模式创新的落地。

其二，建立数据资产确权利用规则。数据新型财产权从体系上说，应该在区分个人信息和数据资产的基础上，进行两个阶段的权利建构：首先，对于用户，应在个人信息或者说初始数据的层面，同时配置人格权益和财产权益；其次，对于数据经营者（企业），在数据资产化背景下，基于数据经营和利益驱动的机制需求，应分别配置数据经营权和数据资产权。〔62〕如前文所述，

〔62〕 参见前引〔36〕，龙卫球文。

基于数字身份及其身份行为，产生了大量各类的个人数据，应对其进行定价和确权，通过法定基础身份和商业应用身份的互联互通，将分散各处、各种数字服务提供者自行管理的身份信息进行连接和交互，积累汇聚于用户跨平台的个人数据账户，经用户授权后，其他机构或平台可以访问和应用相关数据，在不调走数据的基础上经过安全、协同计算，实现数据账户的跨机构共享使用，为用户量身定做如金融产品等各类数字增值服务产品。通过包括本人数据管理模式（my data）在内的方式，让消费者可以去获取和携带自己的消费数据，促进数据的分享、流通利用。个人基础数据的占有权、使用权、获益权都可以在授权访问数据时，通过与数据需求方签订相应的合同来解决。

同时，平台对用户在其应用上产生的各类数据提供记录、检索、整理、挖掘、加工和处理等增值服务，经过匿名化脱敏处理后，产生各类数据服务产品，可以与第三方共享，甚至进行数据交易。因此，应当允许数据处理者享有经个人数据主体同意基于基础数据进行加工编辑分析而产生的增值数据所有权。〔63〕通过数据资产相关立法和统一的基础数据技术标准规范，建立数据产权制度，完善数据资产确权、利益分配机制和流通利用规则，激发个人数据中的资产基因，促进各类数据更便捷地流通利用。

其三，建立统一的 NFT 监管框架。针对前文所述的 NFT 挑战问题，在美国，2022 年 3 月，美国总统拜登签署《关于确保负责任地发展数字资产》的 14067 号行政命令（Executive Order on Ensuring Responsible Development of Digital Assets），详解美国数字资产监管行动框架，旨在解决数字资产及其底层技术的潜在风险。2022 年 3 月，司法部审理了一起利用 NFT 进行投资诈骗的案件。2022 年 4 月，全球税务执法主席联盟发布了如何识别利用 NFT 进行洗钱和其他非法用途的公告。但美国没有针对性的规制 NFT，NFT 在美国法下的法律地位和监管分类尚不明确，其取决于 NFT 的特征及销售方式，NFT 可能落入证券、反洗钱、制裁等监管框架内。目前美国已出现主张 NFT 构成投资合同、进而应受证券法管辖的案例。〔64〕2022 年 6 月 7 日，美国参议院农业委员会成员柯尔斯滕·吉利布兰德（Kirsten Gillibrand）和参议院银行委员会成员辛西娅·卢未斯（Cynthia Lummis）提出了《金融创新责任法案》（Responsible Financial Innovation Act），旨在为数字资产创建一个完整的监管框架，鼓励负责任的金融创新、灵活性、透明度和消费者保护，同时将数字资产纳入现有法律，提高不断增长的数字资产和区块链行业的确定性和清晰度。〔65〕

欧盟也没有专门针对 NFT 出台具体法规，但 NFT 发行的特征可能触发证券领域加密资产市场法规等法规。2020 年《加密资产市场条例（草案）》可能规制 NFT 相关的一部分市场活动；NFT 可能落入欧盟反洗钱指令的规制范围中，欧洲议会成员在 2022 年 7 月 5 日公布的拟议修正案中表示，NFT 交易平台应遵守欧盟反洗钱（AML）法律，因此，市场经营者需要就 NFT 销

〔63〕 参见前引〔34〕，丁道勤文。

〔64〕 See Friel v. Dapper Labs，Inc. et al.，No. 1：21-cv-05837（S. D. N. Y.）.

〔65〕 See Lummis，Gillibrand Introduce Landmark Legislation to Create Regulatory Framework for Digital Assets，avalilable at https://www.lummis.senate.gov/press-releases/lummis-gillibrand-introduce-landmark-legislation-to-create-regulatory-framework-for-digital-assets/，last visited on Jun. 19，2022.

售进行反洗钱合规。英国没有针对性的规制 NFT，其可能落入特定加密资产的范围，进而受到监管。在个案中将根据 NFT 的结构、性质（是否具有电子货币或证券代币的特征）来判断 NFT 的分类及是否属于现有监管范围。新加坡没有针对性监管 NFT，监管一般考察代币的标签和特征，如果 NFT 是受到监管的，那么就需要遵守合规要求。2022 年 5 月 13 日，新加坡最高法院有史以来第一次发布了禁止出售 NFT 的禁令，法院承认 NFT 是有价值、需要承认、可以保护的财产。5 月 27 日，新加坡中央公积金局（CPFB）建议将 NFT 作为多元化投资组合的一部分，代币同行分为安全代币、支付代币和使用代币，对应不同的监管框架。在德国，NFT 可以被用于投资，可能构成《德国银行法案》项下的加密资产。NFT 也可能构成《德国资本投资法案》项下的投资产品。在意大利，NFT 可能构成“虚拟货币”，落入欧盟《反洗钱指令》的范围，触发反洗钱义务。一些 NFT 也可能构成投资产品，受《意大利合并金融法案》监管，需要得到额外的许可。在日本，NFT 不是代币，不具有结算功能，因此不会被作为加密资产进行监管。大部分 NFT 不受任何监管，卡片或游戏内物品的 NFT 交易现在在日本非常普遍。若在游戏内发行 NFT，可能触发《反不合理溢价及误导性说明条例》和刑法典中的赌博条款。日本加密货币商业协会出台了 NFT 指南。〔66〕

在中国，虽然对于 NFT 没有统一的监管框架，但金融监管部门发布并实施了一些限制性政策，严格限制加密货币和加密资产活动。2012 年 7 月，《国务院办公厅关于清理整顿各类交易场所的实施意见》明确要求，交易场所及其分支机构不得将任何权益拆分为均等份额公开发行。中国互联网金融协会等三协会发布《关于防范 NFT 相关金融风险的倡议》，强调 NFT 去金融化，要求“不在 NFT 底层商品中包含证券、保险、信贷、贵金属等金融资产，变相发行交易金融产品”。2022 年 6 月 10 日，福建省地方金融监督管理局披露《福建省清理整顿各类交易场所工作小组关于防范 NFT 违规风险的提示函》，明确要求“福建省交易场所不得开展 NFT 交易相关活动”。

为了维护好元宇宙内的经济体系，防止不法分子通过元宇宙内的经济体系进行洗钱、诈骗等违法活动是需要解决的重点难题之一，因此，建议从国家层面建立起统一的 NFT 监管框架，严格监管加密货币和加密资产市场。现阶段，坚持“去金融化”理念，监管重点聚焦平台，要明确 NFT 交易的多方法律关系，压实主体责任。〔67〕解决好 NFT 的权属、金融风险、个人隐私信息保护等问题，才能让 NFT 这一区块链技术创新应用，持续健康丰富数字经济模式、促进文创产业大发展。

四、结　语

互联网信息技术发展“一日千里”，元宇宙技术和应用仍在不断迭代创新，在未来很长的一段时间里，仍将处于弱元宇宙阶段。在向强元宇宙阶段发展的进程中，未知远大于已知，元宇宙

〔66〕 See Diego Ballon Ossio & James Cranston et al., *Non-Fungible Tokens: The Global Legal Impact*, Clifford Chance, 2021, pp. 2 - 13.

〔67〕 参见程啸、王苑：《透视“元宇宙侵权第一案”数字艺术品法律风险如何规制》，载《光明日报》2022 年 6 月 11 日，第 5 版。

将持续放大和复杂化一些法律问题，同时元宇宙的特殊性法律问题也在不断变化中。不宜高估和热炒元宇宙概念，也不应过度放大甚至妖魔化元宇宙的各种问题。元宇宙并非“法外之地”，现实世界相关法律法规基本都能直接映射适用于元宇宙空间，这是元宇宙法律规制的基本原则。针对那些放大而复杂化特定领域的法律问题，相关法律法规需要做相应修改完善后再进行延展适用，而就元宇宙带来的特殊问题，有待制定新的规则，进行专门规制。

Abstract：The metaverse is a digital ecosystem in which the real and virtual world blend and coexist through digital technologies such as virtual reality or augmented reality. A number of legal issues in the real world will likely be amplified and become more complicated in the metaverse. For example, protection of user privacy and personal information may be challenged as the metaverse involves comprehensive collection of personal sensitive information in a constant and involuntary manner. Data security systems could be greatly impacted by real-time interactive processing of massive data and the widespread application of encryption network technology. The model of user generated content (UGC) may pose new challenges to the right confirmation of content and the distribution mechanism of benefits with regard to intellectual property rights. Competition concerns may arise when users are free to login in with one account across all platforms with interoperability realized. Other unique issues concerning the metaverse include a lack of unified and credible system of digital identity, uncertainty in the rules governing right confirmation and use of data assets, and prominent financial risks associated with NFT. Therefore, to regulate the metaverse and address legal issues concerned, the following principles should be observed. Firstly, the existing legal framework in the real world can directly apply to the metaverse. Secondly, the existing rules with respect to protection of personal information and cybersecurity, data security, as well as intellectual property, may be subject to revision and improvement. Thirdly, new rules could be formulated, such as special provisions governing user privacy and protection of personal information in the metaverse, trusted norms on full-lifecycle data security, and new intellectual property authorization rules for the UGC. In conclusion, this article proposes to develop national strategies for digital identity, establish a unified and hierarchical system of digital identity by introducing specific legislation, formulate new legal rules for the right confirmation and use of data assets, and build a unified regulatory framework for NFT at the state level.

Key Words：metaverse, digital identities, data assets, non-fungible tokens (NFTs)

（责任编辑：刘　权　赵建蕊）

财经法学 No. 5，2022
pp. 54 - 69

元宇宙对著作权法的挑战与回应

张金平*

内容提要：元宇宙是跨多个司法管辖区的去中心化虚拟现实世界，供来自全球的用户利用元宇宙平台提供的工具自由创建和交易虚拟现实物品，因而可为人们提供与现实世界无异的创作环境。然而，元宇宙跨境去中心化运营会对著作权法的地域性带来一系列的挑战，导致元宇宙中作品著作权的归属、著作权具体权利内容和保护程度、著作权的利用以及侵权救济都会出现不确定性，但通过科学解释著作权基本原理和国际私法规则，并结合技术解决方案仍可以妥善应对。

关键词：元宇宙　著作权　NFT

一、元宇宙提出的著作权问题

元宇宙（metaverse）并非2021年才凭空提出。早在1992年，尼尔·斯蒂芬森在小说《雪崩》中就首次提出这个概念。在该小说中，尼尔将元宇宙描绘成一个由计算机协会全球多媒体协议组织管理的虚拟空间，当用户进入元宇宙时看到的是一条大街，楼宇和电子标志牌延伸到黑暗之中，消失在星球弯曲的地平线之外，用户实际看到的是一幕幕电脑图形表象，即一个个出自各大公司设计的软件用户界面。若想把这些东西放置在元宇宙大街上，各家大公司必须征得全球多媒体协议组织的批准，还要购买临街的门面土地，得到分区规划许可、获得相关执照；有关土地购买的资金全部流入由该组织拥有和运营的一项信托基金，用于开发和扩充机器设备，维持大街继续存在。在元宇宙中，每个用户都是编程高手，所以这片乐园显得品味不凡。〔1〕

* 张金平，中央财经大学法学院副教授。

本文为中央财经大学青年教师发展基金资助项目“人工智能时代著作权制度的挑战与应对”（QJJ2003）、国家社科基金重大研究专项“社会主义核心价值观视角下个人信息保护立法研究”（20VHJ008）的阶段性成果。

〔1〕 参见〔美〕尼尔·斯蒂芬森：《雪崩》，郭泽译，四川科学技术出版社2009年版，第29－32页。

虽然元宇宙目前尚未完全构建出来，但已经有三次重大尝试。第一次突破性的尝试是林登实验室2003年创建的虚拟现实空间《第二人生》。〔2〕林登实验室突破了传统游戏开发商对游戏内容和故事完全掌控的做法，仅为用户提供可购买的虚拟土地、可自由创建三维内容的工具，以及可自由交易创建内容的平台和可兑换现实货币的林登币，从而让用户充分根据自己的意愿去创建内容并与他人交互。根据林登实验室2022年的数据，《第二人生》全球拥有5000万用户，用户自创20亿个虚拟物品，这些虚拟物品年交易额达到6.5亿美元。〔3〕不过，这个元宇宙雏形仍然是中心化的大型在线虚拟现实空间，用户仍然要遵守林登实验室制定的平台规则，而且用户创建的内容无法在其他平台共享使用。第二次尝试是2017年开发的Decentraland。不同于基于中心化管理的《第二人生》，Decentraland基于区块链以太坊而创建，采用“去中心化自主组织”（decentralized autonomous organization，DAO）来管理，用户可以利用NFT技术交易自主创建的虚拟物品，〔4〕还可以成为Decentraland的成员来参与管理。〔5〕Decentraland使用以太坊钱包作为用户在元宇宙中的账号，为与其他同样使用以太坊创建元宇宙的平台进行跨平台交互提供了可能。第三次尝试则是扎克伯格2021年10月对元宇宙虚拟现实的设想。他通过长达77分钟的视频阐述了更为贴近尼尔·斯蒂芬森在《雪崩》中所要构建的元宇宙，即元宇宙有且只有一个，是由多平台共建、可互联互通的虚拟现实世界，而且用户在任一个元宇宙平台创建的内容都可以直接在另一个元宇宙平台使用。〔6〕

基于上述有关元宇宙的设定，我们可以结合作品创作、管理、利用和保护四大制度归纳元宇宙的特点。〔7〕一是提供用户自我创作的充分自由度，即用户利用元宇宙平台提供的物品编辑器可以编辑三维虚拟物品。只要满足独创性，这些物品可以构成作品。二是具备社交属性，用户通过作品在多个元宇宙平台之间无缝传播自己的思想表达，并在好友或者粉丝中建立声誉。〔8〕三是提供用户对其创设内容变现的环境和机会，即用户利用元宇宙平台提供的数字货币可以自主对虚拟物品标价并与其他用户交易，这些数字货币可以与现实货币兑换。〔9〕从作品交易的角度而言，用户可以通过作品著作权许可或转让的形式获得版税收入。四是可以实现去中心化管理。通过成为去中心化组织成员的形式，用户可以享有对元宇宙尤其是用户自建内容的运营和管理的决定权。从作品保护的角度而言，用户作为去中心化管理的成员更有可能形成有利于作品在元宇宙中的创作、管理、利用和保护的平台规则共识，例如将作品交易中介费降低到让这个交易系统可

〔2〕 See Cory Ondrejka，Escaping the Gilded Cage：User Created Content and Building the Metaverse，49 *New York Law School Law Review* 81，87 (2004).

〔3〕 See Linden Lab，Tilia Partners With Unity to Power Virtual Economies for Game and Metaverse Developers，available at https://www.lindenlab.com/releases/tilia-unity-partnership，last visited on Jul. 11，2022.

〔4〕 See Decentraland，White Paper，2017，pp. 5－14.

〔5〕 See Decentraland，DAO，available at http://dao.decentraland.org/en/，last visited on Jul. 11，2022.

〔6〕 不过扎克伯格希望用户在元宇宙的化身也采用真实世界的身份和外形，而且也更倾向于通过新成立的Meta公司来主导元宇宙内容的构建。See Meta，The Metaverse and How We'll Build It Together，Connect 2021，available at http://www.facebook.com/facebookrealitylabs/videos/561535698440683/，last visited on Jul. 11，2022.

〔7〕 这里借鉴了韩国李林福先生提出的元宇宙三大要素，即自由度、社交、收益化，但他并未从著作权法的角度加以解读。参见〔韩〕李林福：《极简元宇宙》，黄艳涛、孔军译，中译出版社2022年版，第36－39页。

〔8〕 创作者声誉需要在社交的环境下才能形成，如果作品仅对自己可见那么难以形成规模化创作的内驱力。

〔9〕 在国内目前尚不允许数字货币与现实货币兑换，但国家已经开发和采用数字货币，未来数字货币可作为交易货币。

以持续运转的程度即可。

不过，元宇宙的去中心化跨境运营与著作权法的地域性会产生一定冲突。这些冲突至少可以归纳为三大方面：〔10〕一是每个国家对作品的归属安排不尽相同，为了元宇宙全球同步运营，可能需要作品著作权统一归属的安排；二是作品的全球跨平台展示和传播涉及的具体著作权有所不同，例如各国采用不同的著作财产权来控制作品交互式传播，这对作品全球统一许可或转让带来一定的难度；三是元宇宙中散布全球的用户发生著作权侵权如何确定管辖和准据法，一旦确定侵权，元宇宙采用的交易记录不可篡改的区块链技术可能会对停止侵权等侵权责任的承担造成障碍。考虑到多平台互联互通并去中心化管理的元宇宙尚未完全建成，本文在对上述问题进行讨论时，将围绕中心化的《第二人生》和去中心化的 Decentraland 两个代表性元宇宙模型展开交叉分析，希望能够发掘元宇宙开发不同阶段上述著作权问题的不同解决方案，求教于各位方家。

二、作品著作权归属的挑战

基于著作权的绝对权属性，元宇宙中的作品创作完成即产生著作权，不因平台规则而消灭，但对这些作品在全球的统一著作权归属仍要基于《伯尔尼公约》相关规则来解决。〔11〕

（一）用户创作行为的决定性

《伯尔尼公约》规定只要作品创作完成，作者就对其作品享有著作权，不需要通过任何登记或审批等行政程序。〔12〕因此，在现实世界中，著作权始于作品创作这一事实行为。对于元宇宙，我们假定包括我国政府在内的各国政府都承认元宇宙的物品可以获得现实世界的价值，〔13〕那么用户创作的虚拟物品就不仅仅停留在虚拟空间，进而可通过赋予著作权的形式激励更多作品在元宇宙空间内的创作，打破过去由游戏开发商集中开发和控制的单一局面。

在元宇宙中，用户的哪些行为构成著作权法意义上的创作行为？在传统大型网络游戏构建的虚拟现实空间中，用户只能根据游戏开发商设计的内容和故事，进行竞技或者升级打怪，但这些行为都不是对游戏内容的创作。相比之下，元宇宙开发平台突破传统游戏开发商单方集中式创设内容的局限性，提供用户创制虚拟物品的工具或者编辑器，让用户创作更为丰富和复杂的虚拟现实世界。例如，林登实验室开发的《第二人生》直接提供游戏内的 3D 实时编辑器和脚本编辑工具，用户注册后就可以实时创制虚拟物品，并可以通过脚本程序设置指令让这些虚拟物品动起来。而且，林登实验室也不对用户创制内容设置单独的提交和审批程序。〔14〕相比之下，Decentraland 在提供创制物品的编辑器和脚本程序的同时，〔15〕还提供了建造虚拟物品的 3D 模型和材

〔10〕 元宇宙中可能涉及人工智能生成物的著作权问题，但这个问题脱离元宇宙也同样成立，所以不再单独分析。

〔11〕《与贸易有关的知识产权协定》（TRIPs）要求成员国遵守《伯尔尼公约》规定的义务，所以在作品归属、权利保护程度、准据法等方面的规则都取决于《伯尔尼公约》。

〔12〕 参见《伯尔尼公约》第 5 条。

〔13〕 该问题超出本文有关著作权的探讨范围。

〔14〕 参见前引〔2〕，Cory Ondrejka 文，第 87－93 页。

〔15〕 参见前引〔4〕，Decentraland 书，第 10 页。

料的在线内容库，并兼容外部 3D 模型和材料内容库，〔16〕让用户创建内容的门槛进一步降低，同时还可以借助 NFT 技术让创建内容变得可特定化。〔17〕因此，在元宇宙平台中，用户的创作行为可以是完全自我创作原始作品的事实行为，也可以是在他人创制的 3D 模块基础之上创作演绎作品的演绎行为。世界各国著作权法都普遍承认这两类产生作品著作权的创作行为，只是演绎作者在行使演绎作品著作权时必须尊重被演绎作品的著作权。

创作者对具备独创性的虚拟物品享有著作权。一般而言，用户在元宇宙中创作的虚拟物品主要包括化身的造型及其装饰品、虚拟土地上的建筑物和建筑物内部和周边可以展示的任何跟真实世界物品外观类似的物品，包括墙上的广告和其他 2D 画面、地面上静态或动态的 3D 物品。〔18〕其中，化身造型及装饰品是以线条、色彩或其他方式构成的有审美意义的立体造型艺术，可以作为美术作品得到保护。〔19〕虚拟建筑物因表现出审美意义而可构成建筑作品得到保护。〔20〕静态物品如以一定比例仿照现实物品的形状和结构则可以构成模型作品。〔21〕动态物品涉及脚本程序，可作为计算机软件得到保护。〔22〕在这些虚拟物品是否具备作品独创性的判断中，各国著作权法虽有差异，但随着《伯尔尼公约》和《与贸易有关的知识产权协定》（TRIPs）对各国著作权法的融合，这种差异基本可以忽略，只要能够体现出作者在创作素材的选择和安排中的个性化即可。〔23〕当然，仅仅复制他人 3D 模块不构成演绎，简单组合他人 3D 模块也因不具有独创性而无法产生著作权。

（二）平台规则不影响用户著作权的产生

著作权作为财产权具有绝对性，其权利的产生、权利的类型和保护期等不因私人的意志而变化，所以平台一旦提供用户创作作品的工具并允许这些作品可与现实世界交互，那么用户因创作而产生和享有的著作权就不因平台规则而消灭或者剥夺。在传统游戏中，游戏运营商为了绝对控制游戏，往往在平台规则中禁止玩家交易游戏装备，一旦玩家被发现通过第三方交易平台或者线下交易游戏装备就可以封号，剥夺用户参与游戏的权利，法院也普遍承认传统游戏运营商通过格式合同作出的这种限制。〔24〕相比之下，元宇宙开发平台如果赋予用户创制内容的工具，同时又在其平台规则中不承认用户对其创制内容享有著作权，那么该服务协议的相关条款可以根据格式条款的相关规则判定为无效，即因构成排除和限制用户主要权利而无效。〔25〕

有鉴于此，目前致力于打造元宇宙的《第二人生》和 Decentraland 的平台规则都承认用户对

〔16〕 例如 Sketchfab 的 3D 材料库。

〔17〕 NFT 技术在第三部分再展开介绍。

〔18〕 元宇宙中的音乐往往是从现实世界中创作的音乐嵌入，因而这些音乐脱离元宇宙可以单独保护。元宇宙中用户在其虚拟土地上创作的连续动态画面也可以构成视听作品获得保护。

〔19〕 参见《著作权法实施条例》第 4 条对美术作品的定义。

〔20〕 参见《著作权法实施条例》第 4 条对建筑作品的定义。

〔21〕 参见《著作权法实施条例》第 4 条对模型作品的定义。

〔22〕 参见《计算机软件保护条例》第 3 条。

〔23〕 不过，李明德教授认为作者权体系国家在提供著作权和相关权二分保护的框架下，作品的独创性要求显然要高于版权体系下作品的独创性。参见李明德：《体育赛事直播画面的作品属性认定》，载管育鹰主编：《知识产权审判逻辑与案例：著作权卷》，法律出版社 2022 年版，第 18－20 页。

〔24〕 参见“李宏晨与北京北极冰科技发展有限公司娱乐合同纠纷案”，北京市第二中级人民法院（2004）二中民终字第 02877 号民事判决书。

〔25〕 参见《民法典》第 497 条。

其创作内容的著作权。其中，《第二人生》最新的平台规则并未直接强调用户对其内容享有著作权或其他知识产权，而是仅仅规定“您通过您的账号或使用 Tilia（《第二人生》开发商林登实验室的下属子公司）服务而提交的细节、信息或者其他数据享有所有权”〔26〕。相比较而言，Decentraland 作为新兴元宇宙代表则在其平台规则中比较详细而明确地承认用户对其创制内容享有著作权等知识产权，即“用户对其创造的内容享有其上的所有权利、所有权和知识产权”〔27〕。

（三）元宇宙用户作品著作权归属的确定

《伯尔尼公约》的国民待遇原则足以确保元宇宙用户对其作品享有著作权。〔28〕世界上已经有 179 个国家加入《伯尔尼公约》，根据国民待遇原则，如果元宇宙用户属于成员国国民，其作品著作权自动在另一成员国获得同等保护；即使元宇宙用户不属于公约成员的国民或者属于无国籍人，只要在元宇宙上创作并发布作品，基于元宇宙的全球跨国同步运行的原理，该行为同样符合作品首次在成员国出版或者在一个非成员国和一个成员国同时出版的条件，其著作权也可以在该公约成员国获得同等保护。

在著作权归属上，世界各国的著作权法普遍提供两种规则：一般规则和特定作品的特殊规则。其中，《伯尔尼公约》明确了作品归属的一般规则，即作品著作权归属于作者，在作品之上署名的自然人推定为作者，但有相反证明的除外；即使作者采用假名，只要根据该假名可以准确识别作者身份，该推定同样成立。〔29〕在元宇宙中，用户通过元宇宙平台的账号创造的作品都会直接附属在这个账号之上，而且 Decentraland 等元宇宙平台本身是建立在区块链之上的，用户创制作品的著作权归属也可以借助区块链记载这一证据推定该用户所有人是作者，并借助区块链技术不可篡改的优点强化这一推定。不过，由于区块链只是将作品的哈希值而非作品本身记录在区块链之上，而且区块链平台并不审查作品上链前是否属于该特定区块链账户原始创作的作品，所以区块链记载也仅仅起到作品登记的证据效力，任何人有相反证据时，仍可以推翻前述权属推定。

相比之下，《伯尔尼公约》对于法人作品、职务作品、合作作品、委托作品、视听作品和演绎作品等特殊作品的著作权归属并未设定统一规则，留给成员国自行规定，〔30〕元宇宙的同一作品可能因不同国家对其归属的不同规定导致出现不同的著作权人，给该作品在元宇宙的跨国统一许可或转让等带来障碍。以其中最为复杂的视听作品为例，视听作品指的是一系列有伴音或无伴音的连续画面，包括电影、电视剧、短视频等形式，各国在规定其著作权归属时可能授予参与创作的自然人所有、制片人所有，或者自然人和制片人共同所有，也可以是自然人所有（即原始所有人）但默示转让给制片人（继受所有人），还可以是自然人所有但推定（可被推翻）转让给制片人。而且，各国的规定可能在不同时期出现变动，例如我国《著作权法》2020 年修订前采用电影作品和类电影作品概念，其著作权归属于制片人，编剧、导演、摄影、作词、作曲等作者享有署名权，但 2020 年修法时采用了视听作品的概念，其中电影作品、电视剧作品的著作权由制

〔26〕 Tilia Inc. User Terms of Service，available at https://www.tilia.io/legal/tos，last visited on Jul. 11，2022.

〔27〕 Decentraland Terms of Use，available at https://decentraland.org/terms/，last visited on Jul. 11，2022.

〔28〕 参见《伯尔尼公约》第 3 条、第 4 条。

〔29〕 参见《伯尔尼公约》第 15 条第 1 款。

〔30〕 参见《伯尔尼公约》第 14 条。

作者享有，可以单独决定电影作品的利用，编剧、导演、摄影、作词、作曲等作者享有署名权，但短视频等其他类型视听作品则由参与创作的主体约定其著作权归属。〔31〕

有鉴于此，《伯尔尼公约》第 14 条之二专门协调电影作品的著作权归属及著作权人的权利边界。首先，电影作品著作权归属原则上由被要求保护国的著作权法来决定归属，并且在该国内的电影作品利用则按照该国的规则确定；其次，如果被要求保护国著作权法承认参加电影作品制作的剧本作者、配乐作者、台词作者、电影主要导演之外的自然人（如摄影、副导演）属于著作权人，该国法律除非另有特别规定，应当默示承认这些作者不能反对对电影作品的复制、发行、公开表演、演奏、向公众有线传播、广播、公开传播、配制字幕和配音。尽管做了这样的协调，成员国的这些规定仅适用于成员国内部，仍然会出现同一电影作品在不同成员国有不同权利人的局面，仍然无法解决全球统一许可和转让的问题。一种可能的解决方案是，以最密切联系国的著作权法来确定这些特殊作品的著作权归属并由该权利人统一决定后续的利用，其中的最密切联系点可以体现为主要决定这些特殊作品的内容创作行为或者投资行为的实施地。

三、作品跨境同步利用的挑战

基于元宇宙在全球去中心化的同步运营，元宇宙中作品的利用因为涉及不同国家的不同著作权法，除了前述不同著作权归属带来的难题外，同一利用行为也可能涉及不同国家的不同具体著作权，这些权利的许可和转让都会给元宇宙作品全球跨境跨平台利用制造障碍。

（一）元宇宙利用涉及的具体著作权

元宇宙的全球去中心化运营表明它是一个公众中不特定成员可以自由访问并受现实法律规制的空间，那么，元宇宙用户创作完作品之后的利用行为都可以落入著作权法框架下具体权利控制范围，作品的许可和转让合同要协调不同国家的不同规定。

著作权主要分为人身权利和财产权利，人身权主要包括署名权、发表权、保护作品完整权，财产权利主要包括广义上的复制权、传播权和演绎权。在元宇宙中利用作品都要受到这些权利的控制。例如，用户利用元宇宙平台提供的工具创作完成作品之后，选择对外发布即公众可见，相当于行使了著作人身权中的发表权，而且发表权一经行使就用尽。又如，虚拟物品发布后向公众展示，让公众中的成员可以访问该作品，那么该行为就受传播权的控制。如果将虚拟物品铸造成 NFT 进行出售，其中铸造和发行可能涉及复制权、传播权。如果允许他人在自己作品之上继续创作可能涉及演绎权。值得注意的是，如果将不在元宇宙中创作的作品以 NFT 画框的形式展示在元宇宙空间内，〔32〕同样涉及作品的传播权。

然而，每个国家著作权法对人身权、复制权、传播权和演绎权的具体规定并不相同。例如，对公众可以在选定时间和地点获得作品的控制，在我国法规定为信息网络传播权，但在美国法则

〔31〕 参见《著作权法》（2010）第 15 条；《著作权法》（2020）第 17 条。

〔32〕 Decentraland 就允许注册用户这样做。用户只需要在虚拟土地上设置一道墙，在墙上就可以装一个展示 NFT 数字藏品的画框。然后就可以将 Decentraland 之外的 NFT 的 ID 和 NFT 合同地址复制到这个 NFT 画框中，这个 NFT 就可以在这个虚拟空间中展示出来。

可能受制于公开展示权（针对作品单个复制品或者视听作品中图片的单独展示）或者公开表演权（针对视听作品图片的连续性表演）。这就造成对全球同一行为的控制到底应当通过许可或者转让哪一个权利来实现的技术性问题。

（二）对元宇宙平台作品利用的全球授权模式

在元宇宙中作品的统一许可或转让更有利于著作权人进行作品管理和收益。一方面，虽然元宇宙未改变著作权法的地域性以及著作权的私权属性，著作权人对作品的利用可以选择各国的单独许可和转让，但著作权人这样做的同时也要背负根据单一国家著作权法确定交易的合同条款和价格所带来交易成本。这种单独授权模式很大程度上贬损了元宇宙去中心化全球运行的价值。另一方面，元宇宙全球统一实时运行意味着作者的版权市场是全球市场，所有潜在买家都可以同时参与交易甚至是竞价，从而让作者以最低成本实现利益最大化。在这里，有两大技术帮助著作权人实现作品全球统一管理，并以最低的成本实现利益最大化。一是智能合约，它是合约（交易规则）的代码（即计算机程序），可在区块链上运行，一旦触发合同生效的条件即可自动执行。因此，著作权人可以通过智能合约自动执行作品的交易和营收分配，省去了各国层层中间商或者著作权集体管理组织的代理环节和利益分流。二是谷歌浏览器等语言自动翻译技术，传统环境下的作品传播和交易可能存在不同国别有不同的语言和传播范围的局限，但是目前很多采用 NFT 形式开展的作品交易可以通过谷歌等浏览器实时进行作品内容和交易条件的翻译，〔33〕从而破除了过去的语言障碍。

实践中，元宇宙作品利用的主体主要有两大类，元宇宙平台和元宇宙用户。对于元宇宙平台的利用，著作权人往往不得不同意元宇宙平台制定的格式合同条款。其中，元宇宙平台根据其是否利用区块链技术可以分为中心化运营元宇宙和去中心化元宇宙，而中心化运营元宇宙是元宇宙的过渡形式。因此，《第二人生》这类中心化平台的平台规则往往要求用户对其创造作品的著作权提供宽泛的全球免费许可，“您同意授予一个全球、免费、可再许可、可再转让的，有关您上传、存储、发送、接收或者通过本服务而提供的任何内容的使用、复制、发行、演绎、展示等许可”〔34〕。在这里我们可以发现，该平台选择的许可规则已经超出了一国对作品利用应当明确具体许可的权利类型和一国地域范围之内的通常规则。〔35〕同时，考虑到元宇宙的全球运营以及各国著作权法对著作权具体权利的不同规定，该许可条款直接规定许可针对的是任何使用（并列举主要的利用形式，如复制、展示），而不指向具体权利的许可。此外，可再许可的要求也对未来多平台互联互通的利用预留了空间。

相比之下，利用区块链技术的去中心化元宇宙平台则遵守区块链尤其是公链的去中心化运行的特性，不对用户创制作品进行集中存储、审核和事前管理，也不直接调用用户的作品。〔36〕例如，基于以太坊区块链运作的 Decentraland 在其平台规则中规定，用户在该平台购买虚拟土地后可以在该土地之上自主创设任何内容（包括符合作品条件的内容），并且对其拥有绝对的控制权，

〔33〕 Decentraland 默认要求通过谷歌浏览器来进行翻译。

〔34〕 Art. 6. 3 of Tilia Inc. User Terms of Service.

〔35〕 例如我国《著作权法》第 26 条规定著作权许可使用合同应当包括许可使用的权利种类、许可使用的地域范围的形式要求等内容。

〔36〕 例如，Decentraland 对用户内容采用去中心化存储方式，用户计算机自行存储其创设的虚拟物品，平台服务器上仅仅存储可以调用该作品的区块链地址。参见前引〔4〕，Decentraland 书，第 9 页。

而未规定平台对用户作品的利用。〔37〕

（三）NFT 形式的作品利用授权

元宇宙中作品利用的主要市场来自其他用户的交易和后续使用，具体交易对象主要有两种，用于装扮化身的可穿戴虚拟装备和其他虚拟现实物品（包括外形上与现实世界物品类似或一致的虚拟物品和数字化的传统艺术品）。这两种交易主要通过 NFT 技术来实现交易对象的确认、跟踪和流转。〔38〕NFT 即不可替代代币或者非同质化代币（Non-Fungible-Tokens），指的是一种基于智能合约管理的具有不可分割、不可替代、可验证、可流通等特性的数据单元（合同地址，unit256代币标识），每一个代币标识都对应一个合同地址而可以代表对数字或者实物资产的所有权。〔39〕目前，NFT 主要指的是通过以太坊《ERC-721：NFT 智能合约标准》发行的 NFT，该标准定义了在以太坊智能合约上跟踪、流转 NFT 的应用接口规范。〔40〕每个 NFT 在 ERC-721 智能合约中都通过 unit256 数据（即元数据）而获得唯一标识（简称 Token ID），该标识在合同有效期内不得更改，并以“合同地址，unit256 代币标识”的形式成为特定资产在以太坊链上的全球唯一的标识符，用于指示该合同地址所有者对代表数字资产的标识拥有所有权，可以决定对该资产是否进行交易以及交易的条件。〔41〕

在 ERC-721 标准下铸造 NFT 时通常会涉及著作权控制的有关作品利用行为。第一步：将数字内容上传至网络服务器（可以是集中或者分散的服务器）可能涉及作品的复制。拥有以太坊钱包（钱包地址就是合同地址）的用户，通过某个以太坊应用平台（如 Opensea）将特定数字内容（如图片、视频、3D 模型等）上传至该平台的服务器，从而在该服务器上形成了有关该数字内容的复制品，并生成有关该内容的网络地址。如果数字内容构成作品，那么该上传行为构成作品复制行为，〔42〕至于是否会演变为传播行为则取决于 NFT 铸造者的下一步行为。

第二步：用户在设定该 NFT 交易规则时可能涉及提出有关作品许可或转让的要约或者创设事实上的追续权规则。在创制 NFT 时，铸造者可以选择在智能合约用户界面上描述该数字内容，如著作权人是谁，购买者获得该 NFT 的意义（如可以获赠一张带有创作者签名的作品复制品），以及转售该 NFT 时创作者可以获得的利益分成（不高于交易费的 10%），用户也可以选择不对这些内容进行描述，而只描述该数字内容是什么。这一步骤可能发生两个关键著作权行为。一是提出有关 NFT 交易的著作权许可或转让条件，只要该条件非常明确则可以构成要约（如包括了交易标的、交易价格和附带的著作权许可或转让约定），一旦买方同意该交易条件并点击确认交易则构成承诺，交易双方根据智能合约的自动执行即可达成有法律约束力的著作权许可或转让合

〔37〕 参见前引〔27〕。

〔38〕 See Decentraland Content Policy，available at https://decentraland.org/content/，last visited on Jul. 11，2022. 当然，在不依赖区块链技术的早期元宇宙平台如《第二人生》，则不必依赖 NFT 进行交易，而如同传统中心化组织管理下的交易。在该技术下的交易，玩家购买可穿戴等虚拟物品，如这些虚拟物品具有著作权，玩家仅仅获得了一份作品复制品的使用权，也未获得该复制品的所有权。

〔39〕 See EIP-721：Non-Fungible Token Standard，available at https://eips.ethereum.org/EIPS/eip-721，last visited on Jul. 11，2022.

〔40〕 参见前引〔39〕。

〔41〕 参见前引〔39〕。通常合同地址也就是创制该 NFT 的用户，即 NFT 原始所有人。

〔42〕 参见陶乾：《论数字作品非同质代币化交易的法律意涵》，载《东方法学》2022 年第 2 期。

同。不过，ERC-721 标准并不要求 NFT 铸造者作出有关作品著作权许可或转让方面的描述或约定，因为一旦描述就构成智能合约的一部分并在条件成就时自动执行合同条款。一方面，ERC-721 标准制定者并不想干预铸造者在这方面的自由，另一方面智能合约只保障计算机环境下合约的自动执行，而不保证现实世界作品的许可和转让的自动执行。

第二步的第二个关键行为是 NFT 铸造者一旦设定了 NFT 二次交易时交易费用返回给 NFT 铸造者的比例，则构成通过智能合约设定事实上的作品追续权规则。为了吸引艺术家采用以太坊上 NFT 这种新型应用，形成良好生态，部分 NFT 平台允许艺术家选择在智能合约中设定 NFT 二次交易利益分享比例（例如 Opensea 平台要求不超过 10%），在 NFT 二次交易时基于智能合约的自动执行产生类似法定追续权的效果。然而，这种做法并不满足法定追续权的三大要件。追续权指的是作家和作曲家对其艺术原作和原稿在二次交易时对二次交易价格享有一定比例的利益分配权。对此权利《伯尔尼公约》并未硬性规定，目前法国等 80 多个国家已有规定，我国不在此列。〔43〕 追续权的第一要件是作品类型及载体限制，仅限于艺术作品的原作和原稿。NFT 涉及的往往是上传至 NFT 平台的作品复制件。第二个要件是对作品原件和原稿首次交易后二次公开商业化交易，私下交易不受该权的限制。NFT 二次交易会记录在区块链上，满足公开交易要求，因而可以满足该要件。三是二次交易利益分配的对象和比例由成员国法律确定，不能由当事人自行确定。〔44〕 NFT 二次交易的利益分成则在平台最高限框架下由作者自行决定，不能代表国家意志。

第三步：发布 NFT 可能涉及作品的传播行为。完成前面两步，该 NFT 尚未对外发布也未被写入区块链。区块链上记录内容的算力成本和燃费（gas）都非常高，因此所记录的仅仅是交易摘要的哈希值和时间戳。铸造 NFT 本身只是对上传到网络服务器上的数字内容复制品的所在网址根据特定算法生成了唯一标识码，只有其他用户购买该 NFT 时才能完成交易，这时形成的交易摘要的哈希值才会上链记录。同时，考虑到防止恶意交易和激励矿工耗费算力对交易进行上链，NFT 铸造者在发布前往往被要求预付 NFT 交易上链的燃费。〔45〕 只有支付足额燃费后，该 NFT 才会正式在 NFT 交易平台上发布，并在未来交易完成时上链。在 NFT 平台发布后，公众即可在选定时间和地点，通过 NFT 附带的网络地址或者哈希值全网搜索的形式，访问存储在网络服务器的作品。因此，发布 NFT 受传播权的控制，具体到我国则是信息网络传播权。〔46〕

第四步：交易 NFT 可能涉及作品利用的正式授权，但通常购买者仅通过交易获得了代表数字内容的唯一标识码，并未获得著作权法意义上的著作所有权。NFT 在 NFT 平台发布后，任何公众只要用其数字签名确认接受该 NFT 的出售价格和附带的智能合约并完成支付，双方就通过要约和承诺形成了交易合同，区块链则根据智能合约自动记载此次交易摘要的哈希值，相应地该 NFT 的数据单元（合同地址，unit256 代币标识）中的卖家合同地址就会替换为买家合同地址，买家据此持有了该 NFT。然而，购买者实际上仍然没有获得作品本身，而仅仅持有该作品在

〔43〕 参见李雨峰：《论追续权制度在我国的构建》，载《法律科学》2014 年第 1 期。

〔44〕 参见世界知识产权组织：《世界知识产权组织管理的版权及相关权条约指南以及版权及相关权术语汇编》，世界知识产权组织 2004 年版，第 67 页。

〔45〕 参见邹军等：《区块链技术指南》，机械工业出版社 2018 年版，第 44 页。

〔46〕 参见杭州互联网法院（2022）浙 0192 民初 1008 号民事判决书。

NFT 平台上对应的唯一标识码，也没有获得独家访问上链前存储在网络服务器上对应作品复制品的权利，因为该复制品为了后续 NFT 二次交易而仍存储在网络服务器上并供公众公开访问。〔47〕值得注意的是，鉴于发行权必须涉及作品有形载体所有权的转移，〔48〕卖家或者作者通过 NFT 交易也并非在行使发行权：一是因为 NFT 交易仅涉及作品数字化复制品的元数据（unit256代币标识）的持有者改变（合同地址发生变化），而并非作品原件或复制件所有权的改变；二是《ERC-721：NFT 智能合约标准》并不要求 NFT 平台或者 NFT 铸造者必须在智能合约中约定交易完成即将存储在 NFT 平台上的作品复制品发送一份给买方，买方因而不必然获得作品原件或者复制件，而通常获得访问 NFT 平台上作品复制件的权利。〔49〕

因此，元宇宙用户利用以太坊《ERC-721：NFT 智能合约标准》铸造 NFT 与其他用户交易时，假设这些 NFT 所指向的数字内容构成受著作权法保护的作品，用户通过 NFT 平台发布 NFT 相当于默示授予该平台在全球范围内的作品使用许可，〔50〕以供其存储一份复制品并在全球范围内公开展示该复制品；〔51〕同时默示授予购买 NFT 的用户个人在全球范围内的非商业性使用许可，以供购买者在全球根据自己选定的时间和地点访问该复制品，甚至使用该复制品（如将可穿戴物品穿搭在化身上），但购买者持有该作品复制品的全球唯一标识码本身跟著作权没有任何关系。不过，作者如果在铸造 NFT 时在标准智能合约之外作出其他著作权许可或者转让要约，〔52〕在购买者作出承诺并支付更大对价时，则与购买者达成相应的著作权许可或者转让合同。只要这类超出智能合约自动执行的合约部分符合法律的要求，完全可以通过法院加以强制执行。〔53〕

四、作品侵权救济的挑战

元宇宙用户在自行创制作品的过程中可能有三个场景会发生著作权侵权：一是将他人现实世界的作品复制到元宇宙中，如将他人的名画数字化后制作成元宇宙内的虚拟物品进行售卖；二是在元宇宙中对他人在元宇宙创作的作品进行复制，例如将他人在元宇宙创造的 3D 作品超出其著作权许可范围进行演绎或者商业性使用；三是将他人在元宇宙中的作品复制到现实世界，例如将他人的 3D 虚拟物品打印成平面图片印制在 T 恤上出售。在无授权的情况下使用他人作品即构成

〔47〕 当然，这里并不排除卖家通过智能合约对作品复制品作出其他专门安排，也不排除该 NFT 平台因为服务器故障或其他原因导致公众无法再次访问该作品复制品。

〔48〕 参见前引〔44〕，世界知识产权组织书，第 165 页；李明德、管育鹰、唐广良：《〈著作权法〉专家建议稿说明》，法律出版社 2012 年版，第 226 页。

〔49〕 在这个交易中，不排除卖家为买家提供其他承诺，如线下提供作品有形载体并附上签名，只有买家线下获得该作品有形载体时才会涉及发行权问题。对发行权的讨论，可参见前引〔42〕，陶乾文；杭州互联网法院（2022）浙 0192 民初 1008 号民事判决书。

〔50〕 国内一些公司为了满足国内的监管需求采用联盟链或者私链供用户铸造 NFT，此时的许可通常限于国内。参见杭州互联网法院（2022）浙 0192 民初 1008 号民事判决书。

〔51〕 参见前引〔42〕，陶乾文。

〔52〕 See Megan E. Noh，Sarah C. Odenkirk & Yayoi Shionoiri，GM! Time to Wake Up and Address Copyright and Other Legal Issues Impacting Visual Art NFTs，45（4）Columbia Journal of Law & the Arts，7（2022），available at SSRN：https://ssrn.com/abstract=4028116，last visited on Aug. 8，2022.

〔53〕 有关实践可以参见耐克公司旗下的 RTFKT 公司的 NFT 许可协议。See RTFKT，Digital Collectible Limited Commercial Use License Terms，available at https://rtfkt.com/legal-2A，last visited on Jul. 11，2022.

侵权，因而这些场景下的著作权侵权在侵权判断标准上跟现实世界没有差异，即首先确认原告是否享有著作权，然后判断被告行为是否落入著作权人专有权控制的范围。然而，元宇宙的去中心化运营却可能给著作权人维权带来挑战：一是司法管辖权的确定；二是准据法的确定；三是著作权停止侵权在区块链技术下的实现。

（一）司法管辖权的确定

基于元宇宙的全球去中心化运行，用户的账户采用区块链钱包（即私钥管理软件），用户的身份是匿名并且对平台而言通常也是匿名的，况且利用区块链的元宇宙平台管理者往往是去中心化组织（例如 DAO）。那么，一旦发生著作权侵权，著作权人应当向哪里的法院起诉这些侵权人，法院又是否有权审理发生在他国的侵权行为？例如，拥有 A 国国籍的张三复制了拥有 B 国国籍的李四的作品，并利用王五在 C 国运营的 NFT 平台铸造了 NFT，并利用在 D 国设立运营的元宇宙平台 Decentraland 中的 NFT 画框将该 NFT 植入 Decentraland，那么全球公众可以通过上述 NFT 平台或者 Decentraland 访问到上述作品。这时，李四作为著作权人面对这种涉外侵权纠纷是选择在 ABCD 四个国家同时起诉，还是选择在某个国家起诉张三要求对在全球范围内造成的损害结果承担责任，上述主张又能否得到法院的支持，就成为问题。

《伯尔尼公约》第 5 条规定，作者享有的具体著作权、保护的程度以及为保护作者权利而向其提供的救济方法完全由被要求给予保护的国家的法律规定。WIPO 在解释该条款时只强调被要求给予保护国著作权法的决定事项并不延及著作权的许可和转让等合同问题，并未明确涉外著作权案件的管辖权。〔54〕 对此，国际著名版权法学家山姆·里基森、简·金斯伯格指出，涉外著作权侵权案件的司法管辖权由各国自行规定。〔55〕 然而，各国对涉外案件的司法管辖权规定并不统一，可能采取属人管辖权或者对事管辖权，或者二者兼有。其中，前者的联结点是被告所在地，包括了国籍地和经常居住地。后者的联结点多是侵权行为地、侵权结果地、被告可供扣押财产所在地。例如，我国《民事诉讼法》第 272 条规定，因财产权益造成的涉外纠纷，对在中华人民共和国领域内没有住所的被告提起的诉讼，可以由诉讼标的物所在地、可供扣押财产所在地、侵权行为地或者代表机构住所地人民法院管辖。〔56〕

各国不同的司法管辖权规定可能带来的重要影响除了诉讼的成本之外，还有法院有权对原告提出的哪些诉求进行审理，最终影响原告能否通过单一诉讼获得充分救济。通常而言，限于著作权法的地域性，如果法院实施管辖的联结点是侵权结果发生地，那么法院的审理权限也限于该国境内的损害，无权审理发生在他国的损害；当实施管辖的联结点是侵权行为地或者被告所在地时，法院仍不能通盘考虑发生在其他国家的侵权，原告需对在其他国家产生的损害结果发起单独诉讼。〔57〕 对

〔54〕 参见前引〔44〕，世界知识产权组织书，第 31 页。

〔55〕 参见〔澳〕山姆·里基森、〔美〕简·金斯伯格：《国际版权与邻接权——伯尔尼公约及公约以外的新发展》，郭寿康等译，中国人民大学出版社 2016 年版，第 1145 页。

〔56〕 对于其中涉及信息网络传播权的侵权行为地，《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》第 15 条规定，侵权行为地包括实施被诉侵权行为的网络服务器、计算机终端等设备所在地，但侵权行为地和被告住所地均难以确定或者在境外的，原告发现侵权内容的计算机终端等设备所在地可以视为侵权行为地。

〔57〕 例如，在普通法系国家，这一规则被称为属地诉讼而不是追身诉讼。See Paul Goldstein & Bernt Hugenholtz, International Copyright: Principles, Law, and Practice, Oxford University Press, 2013, pp. 118 - 120.

· 64 ·

此问题，欧盟《布鲁塞尔条例》允许侵权实施地或者被告住所地法院审理跨越多国的著作权侵权案件。〔58〕然而，我国对此问题尚未明确规定，未来我国法院在审理元宇宙著作权侵权案件时就要对此作出选择。目前而言，我国采用类似欧盟的做法更为可取，一方面国际上有这样的先例，另一方面能最大化保护著作权人的合法利益。

此外，如果多国法院依据本国法都有权管辖时，而且原被告就同一侵权行为在多国起诉时，那么各国诉讼之间应当如何处理，是最先受理法院先行审理、其他国家法院应等待先行审理判决后才能审理，还是不受先行审理法院的影响？对此，各国做法也不统一，目前中国法院〔59〕和美国法院认为不受影响，欧盟国家遵守《布鲁塞尔条约》则要等待先行审理法院的结果。〔60〕因此，元宇宙案件中原告在A国提起侵权之诉，而被告在B国提起确认不侵权之诉时，两诉之间的关系受制于这两个国家之间是否存在管辖权的条约，如果缺少则完全取决于这两个国家的各自规定。〔61〕对此，可能的理想解决方案是鼓励当事人在双方协商确定的法院进行诉讼，从而避免陷入多国竞争诉讼的泥潭。

（二）准据法的确定

按照《伯尔尼公约》第5条规定，一旦著作权人选择在某国提起著作权侵权之诉，那么其作品著作权的具体权利内容、保护的程度以及救济方法都归该国法律来确定。同时，《伯尔尼公约》仅规定了著作权保护的最低要求，各国在作者享有的著作权、保护的期限、行政救济或司法救济的单轨保护还是双规保护、损害赔偿是否包括惩罚性赔偿及其计算方法等方面都各不相同。例如，德国法规定公开提供权控制作品的网络交互式传播，作品保护期持续到自然人作者死后七十年，但并未规定著作权侵权的惩罚性赔偿。相比之下，中国法规定信息网络传播权控制作品的交互式传播，作品保护期仅持续到自然人作者死后五十年，但提供了一至五倍的惩罚性赔偿。

由此，各国的规定可能导致著作权人获得的保护在结果上有违国民待遇原则，于是《伯尔尼公约》对第5条又做出了例外规定。〔62〕首先，各国可以自主决定对实用艺术品以及工业品平面和立体设计提供专门法保护或者著作权法保护（但保护期不得少于25年），如果起源国和被要求保护国都仅提供专门法保护，则按照被要求保护国的专门法保护，如果被要求保护国仅提供著作权法保护，则按照作品提供保护。〔63〕因此，如果元宇宙用户将现实世界的实用艺术品及工业品平面和立体设计复制到元宇宙中，要遵守这一例外规定。

其次，被要求保护国对作品的保护期限如果超过作品起源国，仍以起源国的保护期限为准。〔64〕其中，关于何为作品起源国：对于首次在《伯尔尼公约》成员国出版的作品，以该国家

〔58〕 参见前引〔55〕，山姆·里基森、简·金斯伯格书，第1146－1148页。

〔59〕 参见《最高人民法院关于适用〈中华人民共和国民事诉讼法〉的解释》第533条；张鹏：《跨境知识产权侵权纠纷的民事诉讼管辖规则研究》，载《知识产权》2022年第1期。

〔60〕 参见前引〔57〕，Paul Goldstein、Bernt Hugenholtz书，第125页。

〔61〕 类似问题在标准必要专利全球诉讼中尤为明显，各国对标准必要专利的FRAND许可原则的解释不一，而且还可能通过禁诉令的形式要求当事人不得在全球其他法院就同一问题进行起诉。参见前引〔59〕，张鹏文。

〔62〕 参见前引〔55〕，山姆·里基森、简·金斯伯格书，第1150页。

〔63〕 参见《伯尔尼公约》第2条第7款。

〔64〕 参见《伯尔尼公约》第7条第8款。

为起源国；对于在分别给予不同保护期的几个本同盟成员国同时出版的作品，以立法给予最短保护期的国家为起源国。〔65〕在元宇宙全球同步运行的情况下，元宇宙内创作的作品的保护期往往以《伯尔尼公约》成员国中给予最短保护期的国家为起源国。不过，在涉外诉讼中其保护期仍然可以按被要求保护国提供的更长保护期计算。

最后，对于追续权的保护，被要求保护国不提供追续权保护的，或者被要求保护国提供追续权保护但作者国籍国不提供追续权保护的，那么该追续权主张无法得到被要求保护国法院的支持；作者国籍国和被要求保护国同时提供追续权保护的，以被要求保护国为准提供保护。〔66〕因此，元宇宙用户如果选用 NFT 来出售作品，并且在智能合约中设定了二次销售的利益分享比例，那么借助智能合约的自动执行，铸造 NFT 的用户可以获得这些分成，不论被要求保护国和作者国籍国是否提供追续权保护。然而，如果该用户并非著作权人，著作权人起诉时，在被要求保护国提供追续权保护但作者国籍国不提供追续权保护的情况下，法院不保护著作权人的追续权诉求，但这里不排除法院将其作为侵权人获利计入其他侵权的损害赔偿额。此外，在被要求保护国提供的追续权二次交易利益分享比例高于作者国籍国保护程度且高于侵权人在智能合约中设定的比例时，著作权人应当获得的追续权利益要比智能合约自动执行的还要高。

因此，元宇宙本身对著作权侵权的准据法确定本身并未提出挑战，但对当事人维权设置了难题：当事人不仅要考虑哪国是否有管辖权、是否最适合管辖等程序问题，更要结合具体侵权情况考虑该国实体法是否更有利于保护自己的利益。

（三）共同侵权的被告问题

在元宇宙环境下的著作权侵权涉及元宇宙平台和侵权用户的责任问题，然而元宇宙依靠区块链去中心化运行会带来两个问题：一是缺乏内容集中存储和统一控制的中心化平台，平台的管理组织通常是去中心化运行的 DAO 组织；二是在区块链上开发元宇宙并不要求用户在平台中提供身份信息注册才能登录元宇宙，相反该元宇宙平台往往允许拥有相应区块链账户的用户直接登录，此时元宇宙平台也不直接掌握用户的身份信息。那么，著作权人维权时应当如何确定和选择所要起诉的被告？

对此，我们仍然需要结合被要求保护国有关共同侵权或者间接侵权规则来确定起诉的主体。各国这些实体法通常直接适用于著作权领域，各国在具体规则上仍然存在差异。例如，美国的间接侵权规则主要是法院形成的判例法，包括了帮助侵权、替代侵权和引诱侵权，并在一系列涉及作品 P2P 共享的案件中引入著作权侵权领域，这些判例的特点是原告著作权人可以仅仅起诉提供共享技术的平台并要求其承担间接侵权责任，而无须起诉直接侵权人。那么，著作权人选择在美国起诉著作权侵权时，就可以不再单独考虑起诉直接侵权的用户，而可以选择起诉 DAO 组织承担间接侵权责任。虽然 DAO 组织不实际存储所有用户上传的内容，但它仍然是这个平台运行规则的实际制定者（可以通过成员投票改变平台运行规则，如加入作品上传的审查要求）并拥有财产（通常是信托财产）。〔67〕

〔65〕 参见《伯尔尼公约》第 5 条第 4 款。

〔66〕 参见《伯尔尼公约》第 14 条之三。

〔67〕 参见前引〔4〕，Decentraland 书，第 5－14 页。

相比之下，我国法下共同侵权规则有三个特点：一是起初《民法通则》虽然规定了帮助侵权条款，但法院在适用时往往要求原告同时起诉直接侵权人和帮助侵权的平台，否则以不能查明案件事实为由不予受理或者驳回起诉，〔68〕后来《侵权责任法》和《民法典》的网络侵权条款都直接规定了帮助侵权的平台因为自己的行为要独立承担侵权扩大责任，所以元宇宙平台也可以作为帮助侵权人被单独起诉；〔69〕二是我国没有对应的替代侵权，最高人民法院在相关著作权侵权司法解释中指出平台直接从直接侵权中获利的要承担更高的注意义务；〔70〕三是我国最高人民法院在相关著作权司法实践中也明确了引诱侵权，元宇宙平台以言语、推介技术支持、奖励积分等方式诱导、鼓励用户实施侵害信息网络传播权行为的，也可以被单独起诉要求承担责任。〔71〕由此可见，各国的共同侵权规则不仅存在差异，而且各自可能还在不断发展变化，著作权人在维权时要进一步考虑准据法中的共同侵权或者间接侵权规则，最终确定所要起诉的被告及其承担的具体侵权责任。

（四）停止侵权责任的承担方式

元宇宙的去中心化运行往往依赖区块链技术，该技术的分布式记账导致当事人无法篡改有关作品的交易记录，因而可以通过交易价格与区块链交易记账的燃费和中介费的差价来计算出交易的获利，以此确定损害赔偿的数额，从而让著作权人更容易获得准确的损害赔偿。

然而，区块链技术导致交易记录不可篡改和智能合约的自动执行也给著作权的停止侵权带来了一定的挑战，如可能导致侵权状态自动持续下去。对此，为了防止 NFT 交易的持续，国内法院在第一起 NFT 案件中认为，“（NFT）平台可将该侵权 NFT 数字作品在区块链上予以断开并打入地址黑洞以达到停止侵权的法律效果”〔72〕。其中，黑洞地址指的是丢了私钥或者无法确定其私钥的地址，〔73〕而地址就是用户账户，即用户在区块链所用加密技术中分配的公钥，缺少了对应的唯一私钥用户就无法再操控该账户，由此 NFT 交易到这些地址后就像进入黑洞一样无法逃逸，尽管该 NFT 仍然存在但无法进行后续交易。〔74〕同时，由于用户在铸造 NFT 时将作品复制品上传于 NFT 平台并形成了该复制品的网络地址，任何人全网搜索该地址即可访问到该复制品。因此，法院认为在区块链上对数字作品的网络地址予以断开并将该 NFT 打入黑洞地址可以实现停止侵权的效果。〔75〕

对于法院的上述做法，我们应当回归到停止侵权的责任形式来评价。我国《著作权法》第 52 条规定停止侵权的责任形式是停止侵害，针对的是侵权人实施的侵害行为已经发生并且仍在继续的，〔76〕内容上不包括《民法典》第 1167 条规定的排除妨碍和消除危险这两种预防性责任形式。其中，排除妨碍适用的前提是侵权人实施的行为使他人无法行使或者不能正常行使人身、财产权

〔68〕 参见郑成思：《侵权责任、损害赔偿责任与知识产权保护》，载《环球法律评论》2003 年冬季号。

〔69〕 在国内第一起 NFT 案中，原告就仅起诉了 NFT 平台，而未起诉铸建涉案 NFT 的用户。参见杭州互联网法院（2022）浙 0192 民初 1008 号民事判决书。

〔70〕 参见《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》第 11 条。

〔71〕 参见《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》第 7 条。

〔72〕 杭州互联网法院（2022）浙 0192 民初 1008 号民事判决书。

〔73〕 以太坊官方黑洞地址为：0x0000000000000000000000000000000000000000dEaD。See Christian Heidorn，How to Burn NFT on OpenSea in 4 Easy Steps，available at https://tokenizedhq.com/how-to-burn-nft-on-opensea/，last visited on Jul. 11，2022.

〔74〕 参见前引〔52〕，Megan E. Noh 文，第 14 页。

〔75〕 参见杭州互联网法院（2022）浙 0192 民初 1008 号民事判决书。

〔76〕 参见王利明主编：《中国民法典评注：侵权责任编》，人民法院出版社 2021 年版，第 39－41 页。

· 67 ·

益，〔77〕然而著作权的客体作品是非物质性或者非竞争性的，侵权人占有或以其他方式利用作品复制品并不妨碍著作权人行使著作权（如将作品许可他人使用），故著作权侵权不适用排除妨碍。消除危险是指负有责任的人支配下的物对他人人身和财产安全构成威胁，或者存在侵害他人人身或财产现实可能性的情况下，受到威胁的人有权请求消除这种危险，〔78〕然而如果他人仅仅持有一份作品复制品但未公开传播往往受隐私权或者著作权合理使用制度（如个人使用）的保护，并不必然威胁到著作权人的利益。在 NFT 侵权场景下，侵权行为首先表现为 NFT 平台用户未经许可将他人作品上传至 NFT 平台并生成一份复制品，这构成侵害复制权；其次，借助 NFT 平台的服务自动生成有关该作品复制品可公开访问的网络地址，该地址转化为 NFT 智能合约下的 unit256 代币标识并在后续交易完成时被写入区块链，而且任何人知悉或者持有作品复制件的网络地址或者其对应代币标识都可以访问该作品，这构成侵害我国法下的信息网络传播权。在这个过程中，用户是复制权和信息网络传播权直接侵权人，NFT 平台是帮助侵权人，但在该案中权利人仅向平台主张停止侵害，因此法院只要判令平台删除用户上传的侵权内容或者断开侵权链接即可。侵权用户持有 NFT 仅仅持有了侵权作品的网络访问地址并不等同于向公众提供侵权内容，一旦 NFT 平台断开了侵权链接，任何人持有的网络地址将不再能够访问涉案作品，著作权人停止侵害的诉求就可以满足，至于侵权用户继续交易 NFT，本质上并不会侵害著作权，〔79〕似乎造成了未来可能侵害著作权人的危险而需要请求消除危险，但著作权侵权不适用消除危险。况且，在以太坊等公链技术之下，NFT 平台通常无权操纵用户账户使涉案 NFT 与黑洞地址发生交易。当然，在该案中，NFT 平台刚好利用的是联盟链，平台在技术上仍能够操纵用户，但这对联盟链的声誉实质上是一种伤害。

回归到元宇宙中 NFT 的停止侵权问题，元宇宙平台理论上采用公链技术，平台无法直接操纵用户账户使之与黑洞地址发生交易。而且，元宇宙平台中的用户内容往往存储在用户自己的电脑终端或者其他分散的节点，只有用户删除该终端上的侵权内容或者将侵权内容移出共享文件才可以实现停止侵害，即侵权内容不再被访问。因此，著作权人主张停止侵害的应当起诉侵权的元宇宙用户。值得注意的是，采用公链技术的元宇宙平台往往不要求用户使用真名，也不要求注册时提供真实身份信息，甚至可能不要求用户注册而直接使用其公链钱包账户登录元宇宙平台，因此用户真实身份往往难以确定。〔80〕如果该侵权用户不主动表明身份就很可能逍遥法外，〔81〕这时的停止侵害可能得通过改变区块链共识机制来实现。然而，共识机制是区块链运行的重大机制，需要大多数节点同意才能修改共识机制，因此修改共识机制的成本与某个作品著作权侵权损失相比完全不合比例，采用这种方法来实现停止侵权不具有操作性。〔82〕例如，在以太坊 the DAO 事件中，黑客攻击 the DAO 项目将价值 6000 万美元的 360 多万以太币转走，为了解决这次危

〔77〕 参见前引〔76〕，王利明主编书，第 41－42 页。

〔78〕 参见前引〔76〕，王利明主编书，第 42－44 页。

〔79〕 这时可能构成欺诈。

〔80〕 扎克伯格希望建立的元宇宙就主张用户采用与真实身份相一致的化身，包括化身的名字和外形。这就容易将用户的行为纳入法律的监管。此外，我国《区块链信息服务管理规定》第 8 条也要求区块链服务提供商对用户进行身份认证。

〔81〕 参见前引〔52〕，Megan E. Noh 文，第 14 页。

〔82〕 这种技术上的无解或者高成本解决方案，法律上也很难处理，除非从一开始就禁止使用公链或者强制要求公链进行实名化，但这相当于因噎废食。

机，以太坊创始人维塔利（Vitalik）通过改变共识机制的形式来追回部分被盗资金。〔83〕通常情况下著作权侵权损失达不到这个数额，而且修改共识机制也会对区块链的声誉造成重大损失。

五、结　论

打造元宇宙的目的不是平台集权式开发内容让用户娱乐，而是解放人们的创造力，让用户可以自由在虚拟现实空间中自由创作，并通过作品的分享与交易获得其他用户认可的声誉乃至经济回报，从而进一步激发用户在元宇宙中创作更多作品，〔84〕推进人类“向内”发展。〔85〕要实现这样的目的，元宇宙开发平台通过区块链提供用户创作的工具、社交的媒介和作品交易变现的经济体。鉴于这种虚拟与现实的交互，现实世界的法律应当适用于元宇宙，且不因元宇宙开发者意志而转移，包括元宇宙中的作品创作完成自动产生著作权，作品的利用应当获得著作权人的授权，未获得授权的使用构成著作权侵权等。而且，元宇宙借助区块链这种去中心化的分布式记账技术得到了前所未有的发展。借助区块链上运行的智能合约和 NFT 技术，用户可以对创作的作品在不依靠中间商的前提下完成交易并获得经济回报，实现了著作权制度设计者们梦寐以求的愿景——作品目标受众与作者的直接市场化连接。〔86〕不过，元宇宙的去中心化全球运行，也为作品的著作权归属、全球跨国许可或转让、著作权侵权救济带来一定的挑战，但通过对著作权的基本原理、《伯尔尼公约》等规则的适当解释以及技术解决方案，仍然可以妥当解决这些新型问题，尚不至于说元宇宙会颠覆传统著作权法。

Abstract：Metaverse is a decentralized virtual reality world that spans multiple jurisdictions. It provides users around the world tools to create copyrightable virtual objects and to trade them, thus build an environment for them to live a life by creating. However, the decentralized and cross-border operation of metaverse will bring a series of challenges to the territoriality of copyright legal system, creating legal uncertainty to the works' copyright ownership, specific copyright and degree of protection, utilization and tort relief. Anyway, by combining the scientific explanation of the basic principle of copyright rules, private international law, and technical solutions, those challenges could still be properly solved.

Key Words：metaverse, copyright, NFT

（责任编辑：殷秋实　赵建蕊）

〔83〕 参见伍旭川、刘学：《The DAO 被攻击事件分析与思考》，载《金融纵横》2016 年第 7 期。

〔84〕 参见邓建鹏：《元宇宙及其未来的规则治理》，载《人民论坛》2022 年第 7 期。

〔85〕 即向虚拟现实世界发展，相对于人类向外太空的发展而言。

〔86〕 参见〔美〕保罗·戈斯汀：《著作权之道》，金海军译，北京大学出版社 2008 年版，第 28 页。

财经法学 No. 5，2022
pp. 70 - 80

NFT 交易模式下的著作权保护及平台责任

王江桥*

内容提要：近年来，NFT 交易作为一种新兴的商业模式在快速发展的同时，亦对当前法律秩序带来挑战，产生了一系列新型法律问题。如何规制 NFT 市场，明确相关主体责任边界，依法保护各方主体的合法权益，从而引导 NFT 市场健康有序发展亦具有紧迫性。有必要从司法案例中反映的著作权问题出发，针对 NFT 模式下行为法律属性、NFT 交易平台的责任边界、数字作品是否适用权利用尽原则、侵权责任承担方式等新型法律问题进行分析研究。NFT 数字作品交易并非著作权法上的发行，应纳入信息网络传播权控制范畴；NFT 交易平台属于一种新型网络服务提供者，综合 NFT 数字作品的法律属性、NFT 交易模式、技术特点、平台控制能力、营利模式等多种因素，其应当承担较高的注意义务；NFT 侵权责任承担方式应当结合区块链技术特点予以合理确定。

关键词：NFT　信息网络传播　平台责任　侵权不停止

一、问题提出

近年来，NFT 交易作为一种新兴的商业模式得以快速发展，特别是 2021 年以来，我国相关行业对 NFT 的关注度急速升温。据不完全统计，腾讯、蚂蚁金服等一百多家企业纷纷推出各自的 NFT 发行平台。头豹研究院以阿里蚂蚁链销售额为基础，结合腾讯科技、Nonfungible 数据分析认为我国 NFT 市场在未来 5 年增长率约为 150%，市值有望达到近三十亿元。国外仅 Opensea 平台 2021 年的交易额就达到了 140 亿美元。〔1〕NFT 交易快速发展的同时亦带来了一系列新的法律问题，比如 NFT 模式下行为法律属性、NFT 交易平台的责任边界、数字作品是否适用权利穷

* 王江桥，杭州互联网法院副院长、三级高级法官。

〔1〕 参见头豹研究院：《2021 年中国 NFT 平台研究院报告》，第 19 页，载 https://pdf.dfcfw.com/pdf/H3_AP202202081545653782_1.pdf?1644314982000.pdf，最后访问时间：2022 年 8 月 5 日。

竭原则以及侵权责任承担方式等等，这无疑对当前法律秩序带来了新的挑战。目前相关法律规定尚属空白，相关理论界也鲜有深入研究。面对 NFT 交易引发的纠纷案件，司法并不能拒绝裁判，即使法律没有规定也不例外。法官或者运用法律解释方法，或者运用类推适用、目的性扩张等法律漏洞填补方法以及不确定性概念的价值补充方法、利益衡量方法来“发展”规则，为新的社会行为提供规则引导。〔2〕正如丹宁勋爵所言“法官不可以改变法律织物的编制材料，但是他可以也应该把皱熨熨平”〔3〕。2022 年 4 月 20 日，杭州互联网法院宣判了“NFT 侵权第一案”（以下简称 NFT 案），首次对 NFT 交易模式下的相关法律问题进行了分析和探索。〔4〕作为此案审理的参与者，现结合该案涉及的法律问题，从著作权保护角度就如何确定 NFT 交易模式下的行为属性、NFT 交易平台的责任边界以及侵权责任承担三个方面做一梳理和分析。

二、NFT 交易模式下的行为性质

（一）NFT 与 NFT 数字作品

NFT，是英文 non-fungible token 的简称，中文翻译包括“非同质化代币”“非同质化通证”“非同质化权益凭证”，是一种基于区块链技术而产生的不可复制、篡改、分割的加密数字权益证明。NFT 具体表现为通过区块链、智能合约等技术手段将数字内容确定为特定的交易对象，形成唯一对应关系，从而使其具有一定的交易价值，并作为特定客体实现在 NFT 交易平台进行交易流转。从外在表现形式来看，NFT 表现为区块链上一组加盖时间戳的元数据，〔5〕其与存储在 NFT 交易平台上的某个数字文件具有唯一的指向性，对应为一串独一无二的元数据库。该组元数据显示为存储特定数字内容的具体网址链接或者一组哈希值，点击链接或使用哈希值进行检索，就能够访问被存储的特定数字内容。〔6〕NFT 作为区块链下的一个新兴应用场景，一旦 NFT 被铸造，它就已经在区块链上以加密方式发布，使得 NFT 无法更改。同时，智能合约代码定义了 NFT 购买条件等规则，将促使并记录发生的所有 NFT 交易，并在满足其条件时自行执行 NFT 所有权转让。NFT 利用区块链技术记录并验证真实性，能够记录 NFT 数字内容的初始发行者、发行日期以及未来的每一次流转信息，做到全流程记录，区块链上所有节点同步予以见证，可确保数字内容公开透明、安全可信。NFT 本质是权利凭证而非权利，是一种特殊的具有稀缺性的链上数字资产，通过智能合约来实现其权利的转移，并通过区块链来记录权利转让的整个过程。〔7〕

NFT 数字作品属于典型的 NFT 数字资产，系将数字作品上传 NFT 交易平台并铸造 NFT 后再进行流通的数字内容。笔者认为，当一件数字作品以 NFT 形式存在于交易平台上时，由于数字作品数量的限量性和区块链节点之间的信任和共识机制，从而产生“特定性”“稀缺性”“价值

〔2〕 参见李占国：《网络社会司法治理的实践探索与前景展望》，载《中国法学》2020 年第 6 期。

〔3〕 丹宁勋爵：《法官绝不可以改变法律织物的纺织材料，但是他可以也应该把皱折烫平》，载 http://oppo.yidianzixun.com/article/0KUm3sQh？appid=oppobrowser&s=oppobrowser，最后访问时间：2022 年 8 月 5 日。

〔4〕 参见杭州互联网法院（2022）浙 0192 民初 1008 号民事判决书。

〔5〕 参见陶乾：《论数字作品非同质化代币化交易的法律内涵》，载《东方法学》2022 年第 2 期。

〔6〕 参见前引〔5〕，陶乾文。

〔7〕 参见陈吉栋：《超越元宇宙的法律想象：数字身份、NFT 与多元规制》，载《法治研究》2022 年第 3 期。

· 71 ·

性”等效果。NFT 数字作品以数据代码形式存在于虚拟空间且具备价值属性时，已具有数字商品属性；同时其亦具备一定的独立性、特定性和支配性，符合虚拟财产的基本特征，应属于虚拟财产范畴。当然，虽然 NFT 数字作品交易双方形式上呈现的是所有权人的变更，但我国《民法典》中物权编在定义所有权时，将其规定为“所有权人对自己的不动产或者动产，依法享有占有、使用、收益和处分的权利”。可见，虚拟财产并不属于上述法律规定的动产或不动产范畴，自然不存在所有权一说。

因此，NFT 数字作品交易并非实质意义上的所有权转让，而是一种数字资产（虚拟财产）转让。我国《民法典》第 127 条首次对虚拟财产的保护作出了规定，但对其法律性质并未予以明确，只是进行了宣示性或指引性规定。对于虚拟财产的法律属性，当前理论界与司法界存在物权说、债权说、知识产权说、新型财产权利等不同观点，但主流观点认为虚拟财产具有财产性利益，可以作为一种财产性权益予以保护。故此，NFT 数字作品交易中转让的对象本质上是一种受法律保护的财产性权益而非财产权利。换言之，NFT 数字作品被特定化为一个具体的“数字商品（资产）”后，呈现出一定的投资和收藏价值属性，并具有受法律保护的财产权益。NFT 交易本质上属于以数字化内容为交易对象的转让关系，购买者所获得的并非对一项数字财产的使用许可，亦非知识产权的转让或许可，而是一项财产性权益。因 NFT 数字作品购买者无法直接获得该数字作品，其享有的权利实际上主要表现为“所有权身份”和二次交易时的支配权。诚如“澎湃新闻社”专栏作家李奥尼德·波尔席斯基所言，NFT 购买方在多数情况下不过“是实施一个令人厌烦的摆显权”〔8〕。

（二）NFT 数字作品交易的行为属性

NFT 数字作品交易流程通常涉及铸造、上链、出售等环节。首先，从 NFT 数字作品的铸造流程来看，须将作品上传到 NFT 交易平台，故此时上传者终端设备中存储的数字作品被同步复制到网络服务器。其次，从 NFT 数字作品的上链环节来看，系在 NFT 交易平台上以出售为目的呈现该 NFT 数字作品，在作品被呈现的情况下，该展示行为使公众可以在选定的时间和地点获得作品。再次，从 NFT 数字作品的出售环节来看，由于 NFT 数字作品的交易条件及交易过程采用了智能合约技术，整个交易过程由智能合约中嵌入的“自动执行”代码触发完成。故当 NFT 交易平台注册用户通过数字钱包支付对价和服务费后，即刻成为平台上公开显示的该 NFT 数字作品的所有者。下面就 NFT 交易模式下的上述行为是否属于著作权法上的“复制”“信息网络传播”“发行”，以及是否适用“权利穷竭原则”等问题进行分析。

1. 是否属于著作权法上的“复制”

复制行为包括广义上的“复制”和狭义上的“复制”，前者可以理解为“再现作品”的行为，包括表演、广播、放映、改编等行为都可以被称为对作品的“复制”；后者仅指以特定方式对作品“再现”才是复制行为。〔9〕当前大多数国家的著作权法采用的是狭义上的复制行为定义。《中华人民共和国著作权法》（以下简称《著作权法》）第 10 条第 1 款第 5 项规定：“复制权，即以

〔8〕 Leonid Bershidsky, NFT Art Is All About the Hype, March 4, 2021, available at https://www.Bloomberg.com/opinion/articles/2021-03-04/the-nft-phenomenon-is-for-real, last visited on Aug. 5, 2022.

〔9〕 参见王迁：《知识产权法教程》，中国人民大学出版社 2021 年版，第 163 页。

印刷、复印、拓印、录音、录像、翻录、翻拍、数字化等方式将作品制作成一份或者多份的权利。”可见，我国著作权法上的复制权所控制的复制行为应当满足以下两个要件：一是该行为应当在有形物质载体（有体物）之上再现作品；二是该行为应当使作品被相对稳定和持久地“固定”在有形物质载体上之上，形成作品的有形复制件。〔10〕这里所指的复制件应当是产生新的复制件，即增加复制件的数量。当一件作品开始铸造 NFT 时，铸造者首先须按照平台要求上传作品，此时该作品的复制件已同步保存于平台网络服务器中。这种以数字化等方式将作品制作成一份的形式，一方面可以形成稳定的存储作品信息，另一方面亦形成了一个可以相对稳定、持久固定作品信息的有形物质载体，同时也具备作为信息源向其他载体进行信息传播的能力。因此，一件作品的铸造行为包含了著作权法所规制的复制行为。虽然上述复制行为的目的并非向他人提供作品复制件，但该复制件中的作品并未被后来的作品所替代，而是一种永久性的固定，因此，该行为亦并非临时复制。笔者认为，数字作品的铸造行为应属于复制权所控制范畴，其行为亦侵害了复制权。但因该复制是网络传播的一个必备步骤，其目的在于以互联网方式向社会公众提供作品，故复制本身给权利人造成的损害已经被信息网络传播给权利人造成的损害后果所吸收，〔11〕理应无需单独对此予以评价。当前司法实务中亦普遍采取此种做法，在认定构成信息网络传播权侵权的同时不再就复制行为进行评判。

2. 是否属于著作权法中的“信息网络传播”

信息网络传播权是随着互联网的迅速发展而产生，其目的是为了加强作品在互联网交互式传播中的著作权保护。《著作权法》第 10 条第 1 款第 12 项规定：“信息网络传播权，即以有线或者无线方式向公众提供作品，使公众可以在选定的时间和地点获得作品的权利。”据此，我国著作权法上的信息网络传播权所控制的信息网络传播行为应当具备以下条件：一是从作品使用的方式来看，该行为应当通过信息网络向公众提供作品；二是从效果来看，能够使公众在其选定的时间和地点获得作品。由于 NFT 数字作品通过铸造上链后，该数字作品系直接置于开放的网络服务器上进行交易，交易对象为不特定公众，且公众可以在选定的时间和地点获得 NFT 数字作品，故 NFT 数字作品上链交易行为符合信息网络传播行为的特征。铸造者未经许可通过 NFT 交易平台上链交易 NFT 数字作品的行为，应认定为侵害作品的信息网络传播权。需要强调的是，当前大多数 NFT 交易平台采用的是全网可见或者平台用户可见，个别平台采用“盲盒”销售模式，仅在购买者支付对价后方能看到其所购买的数字作品。因任何愿意购买的公众依然可以在个人选定的时间和地点进行购买从而获得该作品，故仍然属于信息网络传播权控制范畴。

3. 是否属于著作权法上的“发行”

著作权法上的发行是指权利人通过销售或赠送等转移作品所有权的方式提供作品原件或复制件。随着数字技术的进一步发展，传统权利也扩展到数字领域，以至于对数字作品是否适用于发行权存在不同的认识。尤其针对发行权中的作品原件或复制件是否包含有形和无形产生了诸多分歧。有观点认为，我国著作权法中的发行权定义中的“以出售或者赠与方式向公众提供作品的原

〔10〕 参见前引〔9〕，王迁书，第 164 页。

〔11〕 参见王迁：《复制权与信息网络传播权的关系》，载《湖南师范大学社会科学学报》2022 年第 2 期。

· 73 ·

件或复制件”就是指将固定了的作品有形物质载体面向公众进行出售或赠与，即转移物质载体的所有权。〔12〕另一种观点认为，发行权应扩展至网络环境，以出售的方式向公众提供数字作品的复制件，应当落入发行权控制范围。发行权的核心特征在于作品原件或复制件的所有权转让，无关作品载体是有形还是无形。〔13〕我国加入的《世界知识产权组织版权条约》（WIPO Copyright Treat，简称 WCT）明确规定“发行权”是指作者、表演者和录音制作者享有的授权通过销售或其他所有权转让形式向公众提供其作品、录音制品和录制的表演原件或复制件的权利。同时在《通过条约的外交会议的议定声明》中指出，发行权条款中的“复制件”和“原件和复制件”是专指可作为有形物品投放流通的规定的复制件，“原件”是指首次被固定在有形物质载体之上形成的。WCT《基础提案》中亦指出，向公众提供权是指“除了发行复制件之外，使公众能够通过任何的方法和过程获取的权利”。欧盟立法亦采取与 WCT 一样的标准，其在《信息社会版权指令提案》明确发行权的复制件必须固定在有形载体之上，向公众传播权为“除了发行物质复制件之外”的权利。

《著作权法》第 10 条第 1 款第 6 项规定：“发行权，即以出售或者赠与方式向公众提供作品的原件或者复制件的权利。”虽然我国《著作权法》对发行权的载体并未做出明确的规定，但当前理论和实务界主流观点认为应理解为“有形物质载体”，也就是说构成著作权法上的发行行为应当符合以下要件：一是该行为应当面向“公众”提供作品的原件或复制件；二是该行为应当以转移作品有形物质载体所有权的方式提供作品的原件或复制件。笔者同意当前主流观点，理由如下：一是我国作为《世界知识产权组织版权条约》成员国，理应与其保持一致，遵守相应的规定。我国《著作权法》相关内容基本上移植于《世界知识产权组织版权条约》。《著作权法》对“发行权”“信息网络传播权”分别作出了规定，且两者之间的区别是非常清晰的。二是数字作品并没有原件或复制件一说，且数字作品的“发行”表现为“向公众提供作品”而非“向公众提供作品的原件或复制件”，此种情形下的存储作品的物质载体并没有发生转移。三是无论有形载体还是无形载体，发行权一定涉及作品原件或复制件所有权转让，而当前数字作品的“发行”并不产生一种作品原件或复制件所有权的转移。

基于上述分析，笔者认为，在 NFT 交易模式下，虽然 NFT 数字作品交易对象是作为“数字商品”的数字作品本身，交易产生的法律效果亦表现为所谓的“所有权”转移，但因发行权的核心特征在于作品原件或复制件的所有权转让，即当前著作权法中的发行仅限定为有形载体上的作品原件或复制件的所有权转让或赠与，且我国当前法律尚未将“数字商品（虚拟财产）”纳入财产权利范畴予以保护，NFT 数字作品出售并非实质意义上的所有权转让，故 NFT 数字作品出售并不属于发行行为，未经权利人许可将 NFT 数字作品在第三方交易平台的出售行为尚无法落入发行权控制范畴。也即，NFT 数字作品的首次销售以及二次销售等均未侵害著作权人的发行权。需要指出的是，本文将 NFT 数字作品交易排除在发行权控制之外，是基于当前我国《民法典》《著作权法》的相关规定得出的结论。随着数字经济的快速发展，“数字商品”“数字资产”作为交易对象将成为一种常态。中央全面深化改革委员会第二十六次会议强调，要积极推进数据要素

〔12〕 参见前引〔9〕，王迁书，第 175 页。

〔13〕 参见何怀文：《网络环境下的发行权》，载《浙江大学学报（人文社会科学版）》2013 年第 5 期。

市场化，加快构建以数据为关键要素的数字经济，建立数据产权制度，健全数据要素权益保护制度。为此，立法理应及时修改相关法律，对“数字商品”这种虚拟财产的性质给出一个明确的法律身份。一旦“数字商品”纳入财产权利范畴，赋予其所有权法律地位，笔者亦赞同将《著作权法》中的发行权范围进行适当的扩大，将 NFT 数字作品出售纳入发行权控制范畴。

4. 权利穷竭原则在 NFT 数字作品交易中是否适用

权利穷竭原则又称“首次销售原则”或“发行权用尽原则”，〔14〕是指合法获得该作品原件或复印件所有权人可以不经著作权人许可将其再次出售或赠与。权利穷竭原则是著作权法为平衡著作权人与所有权人利益而对发行权进行的限制，目的在于防止著作权人对他人所有权和有形财产的合法流通加以干涉，从而损害合法商品自由流通这一市场经济出现后存在的基本规则。我国《著作权法》虽然并没有明确规定这一原则，且在有形载体发行领域适用权利穷竭原则并无争议。然而，网络环境下数字作品是否适用该原则则产生了三种观点。其中，王迁教授认为，“权利穷竭原则”的价值在于澄清“发行权”与“信网权”之间的界限，数字作品的转售或网络传播属于信息流动，并不发生有形物的转移，发行权用尽当然是失去了存在的基础。也有学者认为，数字作品发行与传统有形作品发行均是以转移作品所有权的方式向公众提供作品，只要以转移所有权的方式向公众提供作品，就应该认定其为发行行为，从而适用“权利穷竭原则”。〔15〕还有观点认为应采用折中路径：权利穷竭原则有条件适用于数字作品发行中，即数字发行权有限用尽。具体而言，根据数字作品的不同类别、不同特性以及不同创作成本等，允许著作权人在一定次数或范围内继续控制数字作品的二次传播，发行权在一定次数或范围内暂时不用尽，超过次数或范围的限制，从而实现著作权人私益与社会公共利益之间的平衡。〔16〕

笔者同意第一种观点。我国著作权法采用了发行权和信息网络传播权分开规定的二元结构。发行权适用于作品的有形载体发生所有权转移的情形，而数字传播行为则全部由信息网络传播权控制，这也是当前司法实践中的通用做法。我国法院表明“复制权和发行权控制的行为需以作品存在于有形载体之上为必要要件，而将作品置于互联网之中系信息网络传播权的保护范围”〔17〕。基于此，笔者认为，NFT 数字作品交易同样亦不能适用权利穷竭原则。其一，如前所述，WCT 第 8 条将数字传输归入向公众传播权，并明确向公众提供权是指“除了发行复制件之外，使公众能够通过任何的方法和过程获取的权利”；WCT《基础提案》中亦指出，初始提供或二次提供均被纳入向公众提供权之中。由此可见，向公众二次提供行为必须经过权利人授权，即上述条约明确将数字作品排除在“权利穷竭原则”之外。而我国作为 WCT 成员国，自然应当与条约规定保持一致。其二，在著作权领域，权利穷竭原则主要适用于发行权权利限制，该原则主要目的是为了防止他人出售作品的非法复制件，而非限制合法售出的作品原件或复制件的使用、处置权利。但著作权领域的“权利穷竭原则”的适用基础是作品与其有形载体的不可分性，是对作品有形载体的使用权利作出规制，具有物理空间和现实操作的可控性。但网络改变了作品的传播方式，公

〔14〕“首次销售原则”是英美法系国家的提法，“权利穷竭原则”“发行权用尽原则”是大陆法系国家的提法。

〔15〕参见前引〔5〕，陶乾文。

〔16〕参见陈全真：《数字作品发行权用尽的解释立场即制度协调》，载《出版发行研究》2021 第 9 期。

〔17〕丁靖文：《论数字作品转售不适用首次销售原则》，载《学术研究》2021 年第 4 期，第 74 页。

众无需转移有形载体就可以获得作品的复制件。这一过程与传统传播途径的根本区别是不会导致作品有形载体在物理意义上的转移。其三，在当前法律框架下，NFT 数字作品虽然可以作为特定化的“数字商品”进行交易，但法律并未赋予其一项财产性权利地位，这意味着 NFT 数字作品交易并非以作品载体所有权的方式提供作品原件或复制件，亦就缺乏了适用“权利穷竭”的前提和基础。同时，在 NFT 交易模式下，不特定公众可以在选定的时间和地点获得 NFT 数字作品，属于典型的信息网络传播行为。这种以信息网络途径传播作品属于信息流动，亦并不导致作品有形载体所有权或占有权的转移，自然不受发行权的控制。当然，本文之所以认为数字作品（含 NFT 数字作品）不适用“权利穷竭原则”，同样是基于当前的立法规定。

三、NFT 交易平台性质及责任边界

根据《信息网络传播权保护条例》及相关司法解释规定，网络服务提供者一般提供自动接入、自动传输、信息存储空间、搜索、链接、文件分享技术等网络服务。由于网络服务提供者不直接向网络用户提供信息或对信息进行组织、筛选和审查，只提供传输通道或者展示平台，相关内容由网络用户提供，故其责任认定时应遵循“避风港规则”和“应知标准（红旗标准）”，适用过错归责原则。然而，随着互联网技术的不断发展，商业模式的不断更新，网络服务提供者逐渐更深度地参与到信息的发布、传播当中，出现了明显不属于上述法律规定情形的“云服务平台”“小程序”“视频分享平台”等一系列新型网络服务提供者。同时，当前大量互联网技术发展，特别是人工智能、算法等技术的普遍使用，二十多年前从美国引进的“避风港规则”所设计的利益平衡和适用环境、技术内容等已经完全不同，亟需构建一套与目前技术状况相匹配的关于网络服务提供者注意义务的机制，以实现动态变化中的利益再平衡。当前，虽然存在不同的意见，但主流观点认为应当给网络服务提供者设置更高的注意义务。对此，笔者认为，对于互联网新技术带来的新类型互联网行为，司法理应秉持谦抑的司法理念，通常情况下不宜轻易做出肯定或否定评价。但是，在当前法律存在空白且亟需明确这些新型网络服务提供者责任边界时，司法应当及时通过个案裁判明确各方主体权利义务，合理界定平台责任，厘清责任边界，规范该新型商业模式市场秩序，发挥司法指引作用，从而引导其依法有序健康发展。对于新型网络服务提供者的责任确定，不能简单地适用现有法律规定予以裁判，而是应当根据网络服务提供者的具体服务方式、经营模式、控制能力、技术特点等因素，综合运用比例原则、利益平衡原则和权利义务一致原则等予以综合认定。

根据经营方式不同，NFT 平台主要分为自营和他营两种模式；根据入驻方式不同，NFT 平台主要分为邀请制和注册制；而根据是否允许二次交易可分为 NFT 交易平台和 NFT 非交易平台。本文仅针对采取他营模式和注册制的 NFT 交易平台进行探讨。从 NFT 交易平台提供的交易模式和服务内容来看，其系专门提供 NFT 交易服务平台，交易的 NFT 数字作品由平台注册用户提供，且不存在与用户以分工合作等方式参与 NFT 数字作品交易，故此，根据当前法律的相关规定，NFT 交易平台应属于网络服务提供者而非内容提供平台。NFT 交易平台作为一种为注册用户提供 NFT 数字商品交易服务的平台，明显不属于“提供自动接入、自动传输、信息存储空

间、搜索、链接、文件分享技术等网络服务”中的任何一种网络服务平台。NFT 数字作品交易系伴随着互联网技术发展，并结合区块链、智能合约技术衍生出现的网络空间“数字商品”交易模式创新，属于新型商业模式。有学者称其“在国内外的数字版权交易活动中，在有效解决确权难、实现去中心化交易方面发挥了显著作用”〔18〕。对于像本 NFT 案所涉 Bigverse 平台这种提供 NFT 数字作品交易服务的网络平台的责任边界，应结合 NFT 数字作品的特殊性及 NFT 数字作品交易模式、技术特点、平台控制能力、经营模式等方面综合认定。〔19〕

首先，从 NFT 数字作品交易模式来看，NFT 数字作品作为交易客体时表现为特定的“数字商品”，既涉及作为数字作品的著作权，也涉及作为“数字商品”的“所有权”。如前所述，NFT 交易模式下产生的法律后果将包括“所有权”的转移。因此，NFT 数字作品的铸造者（出售者）应当是作品原件或复制件的所有者。同时，根据《著作权法》的相关规定，所有权发生转移，但作品著作权并未发生改变。在 NFT 交易模式下，NFT 数字作品的铸造者（出售者）将 NFT 数字作品复制、上传至平台进行交易的行为，分别为《著作权法》中的复制权、信息网络传播权所控制，因此，NFT 数字作品的铸造者（出售者）不仅应当是作品复制件的所有者，而且应当系该数字作品的著作权人或授权人，否则该 NFT 数字作品属于明显侵害他人著作权的侵权商品。对此，Bigverse 平台作为专门从事 NFT 数字作品交易服务平台知道也应当知道，且理应采取合理措施防止侵权发生，审查 NFT 数字作品来源的合法性和真实性，以及确认 NFT 铸造者获得适当权利或许可来从事这一行为。换言之，Bigverse 平台对用户上传用于铸造 NFT 的数字作品相关权利应当进行合理的事先审查，以防止该 NFT 数字作品存在权利瑕疵，侵害他人著作权。

其次，从 NFT 数字作品交易采用的技术来看，整个交易模式采用的是区块链和智能合约技术。作为区块链技术下的一个新兴应用场景，NFT 不仅解决了数字作品作为商品时的可流通性和稀缺性（非同质化），而且能够解决交易主体之间的信任缺乏和安全顾虑，构建了一种全新的互联网新业态之诚信体系。其中，NFT 数字作品之所以具有投资价值和收藏价值，最核心原因之一是基于区块链中的信任机制，智能合约是承载交易双方合意的载体，Bigverse 平台上的每一次交易因智能合约中已嵌入了“自动执行”代码将自动触发完成。因此，如果 NFT 数字作品存在权利瑕疵，不仅将破坏交易主体以及 NFT 交易平台业已建立的信任机制，而且将严重损害整个交易秩序的确定性，进而损害交易相对人的合法权益以及著作权人的权益。同时，因整个交易系通过智能合约由代码自动执行，交易次数将无法人为控制，且 NFT 数字作品交易属于信息网络传播行为，并不适用权利用尽原则。因此，一旦 NFT 数字作品构成侵权，往往会损害数个甚至几十个善意交易相对方的合法利益，导致交易双方纠纷频发，动摇 NFT 商业模式下的信任生态，将严重妨碍整个 NFT 行业的有序发展。

再次，从 Bigverse 平台控制能力来看，一是，所有 NFT 交易形成的数据均保存于 Bigverse 平台网络服务器中，特别是用户上传作品后至完成 NFT“铸造”前，均是由 Bigverse 平台控制整个流程以及所有内容，因此，Bigverse 平台具有较强的控制能力。二是，从 Bigverse 平台 NFT 数字作品铸造流程来看，用户按照平台要求，完成上传作品并提交后即进入平台审核环节，

〔18〕 薛晗：《基于区块链技术的数字版权交易机制完善路径》，载《出版发行研究》2020 年第 6 期，第 51 页。

〔19〕 参见杭州互联网法院（2022）浙 0192 民初 1008 号民事判决书。

· 77 ·

只有审核通过的才能上架，最终作为 NFT 数字作品在 Bigverse 平台上进行交易。可见，对 NFT 数字作品进行一定形式上的审查原本就是 Bigverse 平台所设置的必备流程之一。因此，赋予 Bigverse 平台一定的审查义务，并没有直接增加平台义务。三是，从 Bigverse 平台审查的对象来看，每个用户每次提交审查的均为单个作品，并不存在海量的数据内容，不会出现平台无法一一审查的情形。故此，Bigverse 平台对其平台上交易的 NFT 数字作品不仅具有较强的控制能力，而且也具备相应的审核能力和条件，同时亦并没有额外增加其审查内容和控制成本。

最后，从 Bigverse 平台的经营模式来看，其不同于电子商务平台和提供存储、链接服务等网络服务平台，并非免费或者采取会员费等方式获取经济利益，而是系直接通过佣金等方式从 NFT 数字作品交易中获得利益。从 NFT 数字作品交易流程来看，Bigverse 平台不但在铸造时收取作品燃费，而且在每次作品交易成功后收取一定比例的佣金及燃费。笔者认为，平台获得的经济利益应与其注意义务相适用，在平台用户的权利与著作权保护之间保持一种平衡。既要从兼顾行业利益格局、主体利益分配和成本效率权衡三个维度进行考量，以实现各方主体的利益平衡，又应充分发挥司法引导作用，避免各方利益失衡的情况发生。《最高人民法院关于审理侵害信息网络传播权民事纠纷案件适用法律若干问题的规定》第 11 条第 1 款规定："网络服务提供者从网络用户提供的作品、表演、录音录像制品中直接获得经济利益的，人民法院应当认定其对该网络用户侵害信息网络传播权的行为负有较高的注意义务。"Bigverse 平台这种营利模式明显属于上述法律规定范畴，即在 NFT 数字作品中直接获得经济利益，其自然应承担较高的注意义务。

综上，笔者认为，NFT 交易平台不仅需要履行一般网络服务提供者的责任，还应当承担较高的注意义务，包括但不限于对 NFT 数字作品权利的事先审查、明知或应知侵权时的主动下架删除等义务，否则应承担相应的法律责任。NFT 案中，Bigverse 平台正因为其未履行相应的审查义务，最终被法院认定构成帮助侵权。NFT 交易平台在履行上述注意义务时，理应建立一套有效的知识产权审查机制，对平台上交易的 NFT 作品的著作权做初步审查，如审查申请 NFT 铸造的用户是否提供了涉及著作权底稿、原件、合法出版物、著作权登记证书、认证机构出具的证明等初步证据证明其为著作权、与著作权有关权益的权利人。当然，这种审查应当是基于网络服务提供者具有的善良管理者义务角度进行评价，并且应赋予网络服务提供者一定的自主决策权和审查空间，可以在法律规定的框架内，根据自身审查需要、知识产权权利类型、产业发展等实际情况等因素，对具体要求进行明确和细化。从判断标准来看，应当采用"一般可能性"标准。也就是说，该初步证据应当排除明显不能证明是著作权、与著作权有关权益权利人的证据，并具有使得一般理性人相信存在权利的可能性即可。同时，NFT 交易平台还应构建相应的侵权预防机制，形成有效的筛查、甄别体系，从源头上防止侵权发生，必要时可要求铸造用户提供担保机制，最大限度防止 NFT 数字作品存在瑕疵，以防止侵权发生。

四、侵权责任承担方式的探索

按照侵权责任法的相关原理，"停止侵害"是侵权责任中最主要也是最重要的责任承担形式。我国《著作权法》亦秉持侵权责任法一般规定精神，明确著作权侵权人应当承担停止侵权责任。

也就是说，在 NFT 案中，Bigverse 理应立即删除侵权 NFT 数字作品等侵权内容，停止侵权。然而，根据 Bigverse 平台服务协议，Bigverse 平台对侵权的“NFT 数字作品”可以采取的措施仅为删除、屏蔽、断开侵权链接，无法将该“数字作品”对应的非同质化通证（NFT）及其他上链侵权内容予以删除。因 NFT 系采用区块链技术进行同步保存数据的，NFT 数字作品及其交易的相关数据均保存于区块链服务器和各节点服务器中。区块链中各节点均为匿名，且“共识机制”是区块链中各节点之间必须遵守的处理机制。故此，通常而言，各区块链节点之间无法形成共识，进而无法删除以哈希值形式存在的侵权数字作品所对应的“NFT”以及交易的相关数据。因该“NFT”及其交易的相关数据仍然保留在 NFT 交易平台服务器中，侵权内容并没有删除，理论上仍存在侵权的可能性，显然并没有达到“停止侵害”之法律效果。因此，NFT 案中最终采用 Bigverse 平台将该侵权 NFT 数字作品在区块链上予以断开并打入地址黑洞之方式以达到停止侵权的法律效果。笔者认为，NFT 案中对停止侵权的责任承担方式的处理无疑是一种契合区块链等互联网技术而创新的探索，一方面可以实现停止侵权的效果，另一方面又兼顾了 NFT 交易模式的技术特点，妥善平衡了 NFT 数字作品侵权中各方主体的利益，较好地解决了 NFT 交易模式下“停止侵权”这一棘手的问题，亦为今后类似案件的处理提供了新的思路和参考。

同时，笔者认为，除了 NFT 案所探索的责任承担方式之外，也可以探索“著作权侵权不停止制度”在 NFT 侵权责任承担中的适用。在知识产权领域，“侵权不停止”最早出现在美国司法判例中，其实质属于对权利人行使权利的一种限制，系关于知识产权保护的例外规定和利益平衡的有效手段。这种平衡机制不仅对知识产权人专有权给予保护，而且应当保护其他私权利、公共利益以及公平竞争等。〔20〕也就是说，通过适当限定知识产权人的专有权利，调整知识产权人与公众、利益关系人的关系，合理兼顾各方利益，使之处于利益平衡状态，以彰显立法的灵活性和司法的能动性和智慧性。〔21〕侵权不停止制度主要适用于对私人与公共利益、私人与私人利益平衡之情形。“侵权不停止”制度在我国最早出现在司法政策中。2009 年《最高人民法院关于当前经济形势下知识产权审判服务大局若干问题的意见》第 15 条指出，如果停止有关行为会造成当事人之间的重大利益失衡，或者有悖社会公共利益，或者实际上无法执行，可以根据案件具体情况进行利益衡量，不判决停止行为，而采取更充分的赔偿或经济补偿等替代性措施了断纠纷。之后，2016 年颁布的《最高人民法院关于审理侵犯专利权纠纷案件应用法律若干问题的解释（二）》第 26 条规定：“被告构成对专利权的侵犯，权利人请求判令其停止侵权行为的，人民法院应予支持，但基于国家利益、公共利益的考量，人民法院可以不判令被告停止被诉行为，而判令其支付相应的合理费用。”这是我国知识产权立法首次对这一制度作出规定。虽然我国《著作权法》及相关司法解释并没有明确规定侵权不停止制度，但其现已成为立法和司法的新趋势，尤其是被不断适用在著作权侵权案件中。比如“大头儿子”著作权纠纷案、〔22〕中国音乐著作权协会与长安影视公司等著作权侵权纠纷案、〔23〕正东公司与东上海分公司等著作权侵权纠纷案〔24〕等。可见，“著

〔20〕 参见田小军、刘洋：《“侵权不停止”在知识产权案件中的适用问题》，载《中国版权》2016 年第 6 期。

〔21〕 参见徐清云、张波：《著作权侵权不停止的利益平衡理论》，载《四川职业技术学院学报》2018 年第 4 期。

〔22〕 参见杭州市中级人民法院（2015）浙杭知终字第 356 号民事判决书。

〔23〕 参见北京市第一中级人民法院（2003）一中民初字第 2336 号民事判决书。

〔24〕 参见北京市朝阳区人民法院（2012）朝民初字第 12869 号民事判决书。

• 79 •

作权侵权不停止”可以适用于著作权侵权纠纷中已经成为一种共识。正如有学者所言，《著作权法》第 53 条中的“应当根据情况”可理解为法律不要求停止侵害责任一律适用，即法院可以根据个案的具体情况自由裁量做出判决，通过以赔偿方式替代侵权责任的司法指导意见同样适用。〔25〕

笔者认为，作品的价值在于传播，著作权本身具有一定的社会公共属性。从这一角度上讲，“著作权侵权不停止制度”既符合我国著作权法所提倡的促进科学和文化事业发展与繁荣的根本目的，亦符合著作权法的基本原理。在 NFT 数字作品著作权侵权纠纷中，一方面因 NFT 采用了区块链技术来保障交易，实际上无法真正完全执行“停止侵权”之责任承担；另一方面，NFT 交易是通过智能合约执行的，整个交易次数无法人为控制，因此一旦停止侵权往往会涉及多个善意交易主体的合法利益，既不利于整个 NFT 商业模式的发展，也会动摇 NFT 交易中的整个信任机制。同时，NFT 交易模式下的著作权侵权大多数针对侵害著作财产权，这也为用经济补偿（类似于支付许可使用费）替代停止侵权提供了可能。因此，在 NFT 数字作品著作权侵权纠纷处理中，为了调整著作权人、NFT 数字作品交易相对人与社会公众的利益关系，使之处于利益相对平衡状态，可用更充分的赔偿或经济补偿来替代“停止侵权”之责任承担，在充分保障著作权人合法权益的基础上，实现 NFT 交易主体之间的利益平衡，从而推动 NFT 交易这种新型商业模式有序健康发展。

Abstract: In recent years, NFT transaction, as a new business model, has developed rapidly, and it also brings challenges to the current legal order and produces a series of new problems. It is also urgent to regulate the NFT market, clarify the boundary of responsibility of relevant subjects, protect the legitimate rights and interests of all parties according to law, so as to guide the healthy and orderly development of the NFT market. It is necessary to analyze and study new legal issues such as the nature of behavior under the NFT mode, the boundary of liability of NFT trading platform, whether the exhaustion of rights principle applies to digital works, and the way of bearing tort liability, based from the copyright issues reflected in judicial cases. NFT digital works trading is not the distribution of copyright law, and should be included in the control of information network transmission rights. NFT trading platform is a new type of network service provider. Considering the legal attributes of NFT trading mode, technical characteristics, platform control ability, profit mode and other factors, it should assume a high duty of care. The mode of NFT tort liability shall be reasonably determined based on the characteristics of blockchain technology.

Key Words: NFT, information network dissemination, platform responsibility, infringement does not stop

（责任编辑：张金平　赵建蕊）

〔25〕 参见前引〔21〕，徐清云、张波文。

· 80 ·

财经法学 No. 6，2022
pp. 125 - 136

元宇宙的法律难题

［印尼］萨法里·卡西亚安托　［德］穆斯塔法·基林茨　著
郑志峰　罗有成　译*

内容提要：在社交媒体巨头的首席执行官宣称元宇宙将成为继互联网之后的下一个大事件后，元宇宙获得了良好的发展势头。虽然目前还没有统一、共识性的元宇宙定义，但对元宇宙的共同理解是该概念结合了 IoT、AR、VR、XR 和 3D 技术。元宇宙蕴含巨大的市场资本和经济潜力，因此，讨论元宇宙的法律含义至关重要。本文是第一篇以恰当的方式阐述元宇宙的法律难题的文章。它包括对一般物权法和知识产权法的讨论，以及是否已经到了需要制定“虚拟财产法”的时候。它还讨论了隐私和数据保护、合同法、网络安全和网络攻击、货币和支付系统法、虚拟资产法规、税法、反洗钱法和了解客户规则，以及刑法等其他法律问题。元宇宙创造了一个现实世界法律可能难以适用的新空间。因此，元宇宙破坏了法律权威的“传统主张”、扰乱了尊重法治的需求。然而，将现实世界的法律适用于元宇宙仍然是可能的，但有局限性。当在元宇宙实施现实世界的法律时，这种局限性就会具体地表现出来。

关键词：元宇宙　法律难题　虚拟世界　货币法　支付系统法

一、引　言

自从 2019 年新冠肺炎疫情暴发后，全球经济的增长势头开始放缓。在新冠肺炎疫情暴发之

* 萨法里·卡西亚安托，蒂尔堡大学经济与法律研究中心研究员；穆斯塔法·基林茨，德国奥托贝森商学院助理研究员；郑志峰，西南政法大学民商法学院副教授、网络空间治理研究院副院长；罗有成，西南政法大学网络空间治理研究院助理研究员、博士研究生。

本文为 2020 年国家社科基金青年项目“人工智能与《民法典》双重背景下个人信息保护研究”（20CFX041）、2020 年国家社科基金重大项目“数字社会的法律治理体系与立法变革研究”（20&ZD177）的阶段性成果。

原文发表于《中央银行法律与制度杂志》（Journal of Central Banking Law and Institutions），感谢作者和期刊的慷慨授权。经作者同意，译者在此省略了引文。

前，全球经济增长达到了 2.8%，其中，发展中国家增长了 3.7%，发达经济体仅增长 1.7%。在新冠肺炎疫情暴发期间，全球经济增长大幅收缩，在 2020 年下降了 3.1%，伴随着大多数经济行业的人均产出的普遍下降。这是自 19 世纪 70 年代长期经济大萧条以来的最大降幅。尽管预计 2021 年全球经济增长将会触底反弹至 5.7%，但这场疫情对于经济的损害已经造成，并且留下了不可磨灭的创伤。新冠肺炎疫情造成人员流动严重受阻、城市封锁、各个经济体国边界关闭，人们进入防疫或者隔离状态。大多数经济行业的市场规模急剧下降。〔1〕以受疫情影响最严重的行业之一——旅游业——为例，2020 年市值同比下降了 70%，几乎是一夜之间回到了 30 年前。由此可见，世界的经济正面临着前所未有的危机。

然而，在新冠肺炎疫情重创经济并引发各种社会危机的同时，数字化（digitalisation）却迎来了蓬勃发展。伴随着所谓的“新常态”，使用数字技术和创新已经成为公众的一种新的生活方式。居家远程办公变得无处不在，〔2〕虚拟会议非常普遍，〔3〕在线和远程学习增加，数字交易也创下了历史最高记录。为了克服旅游业的下滑，政府和企业开始使用虚拟现实（VR）等数字活动来吸引游客。在印度尼西亚，2022 年第一季度使用电子货币的交易额同比增长了 42.06%，而使用数字银行平台的交易额同比增长了 34.9%。预计到 2022 年，整体电子交易将同比增长 18.03%，电子货币将达到 360 万亿卢比，数字银行将同比增长 26.72%，达到 51729 万亿卢比。

在新冠肺炎疫情后，数字化的势头继续增强。2021 年 10 月，社交媒体巨头 Facebook 的首席执行官马克·扎克伯格（Mark Zuckerberg）宣布，元宇宙是下一个大事件（the next big thing），是互联网从当前 Web 2.0 迈向未来 Web 3.0 的一场革命。扎克伯格甚至将公司的名称更改为 Meta，并承诺将投入 100 亿美元用于元宇宙的开发。在这个新的虚拟世界——元宇宙——中，人们可以像在现实世界中一样，使用化身（avatars）来行动、互动以及进行商业活动。2021 年 12 月，有人支付了 45 万美元购买虚拟土地。〔4〕无独有偶，Token.com 的首席执行官安德鲁·克里格尔（Andrew Kriggel）花了 240 万美元的高价在元宇宙时尚区买了一块虚拟土地，〔5〕与公众人物史努比·道格（Snoop Dogg）做起了邻居。元宇宙创造的世界可能是虚拟的，但围绕它们的经济交易却是真实的，对现实世界的影响也是实实在在的。因此，元宇宙中的交互可以在关联的各方主体之间产生权利和义务。这种权利和义务可以是基于社会、伦理或者法律规范而产生的，就像现实世界那样，因为虚拟世界的居民实际上是现实世界中真实的人。随着虚拟（线上）世界和现实（线下）世界的碰撞，法律规则在元宇宙场景下的适用就出现了一系列难题。这些难题主

〔1〕以印度尼西亚为例，其大部分经济行业在 2020 年大幅下滑，其中，最严重的行业是交通和物流行业（下降了 15.04%）以及住宿服务和食品饮料行业（下降了 10.22%）。只有少数行业，如卫生和社会服务行业、信息通信技术（ICT）行业保持着高效的增长率，分别为 11.6%和 10.58%。总体而言，印度尼西亚的经济在 2020 年下降了 2.07%。

〔2〕元宇宙中的远程办公可以促使人们远离大城市。也许，元宇宙可以成为政府更好地将居民安置在城市和郊区之间的工具。

〔3〕据研究统计，在线平台 Zoom 的日常会议参与者从 2019 年 12 月的 1000 万人激增至 2020 年 3 月的 2 亿人。尽管 Zoom 平台存在安全问题和网络攻击，但在线平台会议的使用量增加了 2000%，其原因就是新冠肺炎疫情的暴发。

〔4〕在涉及虚拟房地产这一商业活动时，Sandbox（沙盒）被认为是最大的元宇宙平台，其拥有大约 62%的可用元宇宙土地。2012 年，Sandbox 还是一款在线视频游戏。2021 年 11 月，Sandbox 已经转变为元宇宙。

〔5〕这个元宇宙平台名为 Decentraland。2015 年，Decentraland 作为开源 3D 世界建立。与沙盒不同的是，Decentraland 的土地是有限的，其元宇宙土地只能由社区成员获得。

要包括现实世界中的法律如何在元宇宙中适用、谁将颁布元宇宙独有的法律、谁将在元宇宙中执法，以及谁将保护元宇宙社会并维持其秩序。

本文详细阐述了元宇宙引发的一系列法律难题。为了更好地进行分析，本文考察了技术进步是如何冲击法律权威，又是如何违背法治要求的。罗杰·布朗斯沃德（Roger Brownsword）指出，技术对于法律的冲击可以分为三种：第一种技术冲击挑战了国家法律权威机构的主张，即作出决策的权力、决策或者法令获得遵守的法律约束力。当智能技术创造出传统法律难以适用的新空间时，这种情况就会发生。例如，网络空间的互动涉及多个司法管辖区、多个国家的公民、复杂而新颖的行为，以及使用虚拟货币或财产的跨境支付。第二种技术冲击破坏了法律原理，即法律应该受到尊重仅仅因为它是法律。当人类的行为不再需要由人类来统治，而是全面受制于技术时，这种情况就会出现。第三种技术冲击对于法律的破坏更为深远。因为它侵蚀的是我们对于权威和尊重法律的概念性思维。当智能技术支配了所有人类行为（当然是在某些领域）的时候，我们所熟悉的关于法律权威的传统思维以及尊重法律的要求，都会变得过时。

本文认为，元宇宙对法律产生的冲击属于第一种。元宇宙破坏了法律权威的“传统主张”和尊重法律的要求。因此，元宇宙的法律和治理就成为一个亟待解决的难题。本文试图通过将元宇宙中的法律、治理和伦理问题作为在现实世界中发生的问题来讨论，进而尝试解决这些问题。尽管这种方法并不完美，但作为解决这一难题的首次尝试，它还是有用的。

本文是第一篇以恰当的方式系统阐述元宇宙的法律难题的文章。此前关于元宇宙的研究主要包括元宇宙的开发方法、元宇宙的技术方面、元宇宙的治理和伦理方面，以及元宇宙法律方面的一些具体问题，尤其是隐私和数据保护。本文的独特价值在于，对元宇宙的法律问题进行了较为全面的分析，包括物权法、知识产权法、合同法和智能合约、货币和支付系统法、加密资产法规、税法、反洗钱法和了解客户（know your customer）规则，以及刑法。根据我们的了解，现有的研究都还没有讨论元宇宙中有关货币和支付系统法或税法的问题。

本文结构安排如下：第二部分概述了元宇宙的理论和实践，作为我们认识元宇宙中行为的基础；第三部分讨论了元宇宙中行为引发的法律和伦理问题，首先包括物权法和知识产权法（以及当下是否需要制定“虚拟财产法”）、隐私和数据保护、合同法和智能合约、货币和支付系统法，另外，本文讨论的其他法律问题还包括诸如证券和大宗商品法等虚拟资产法规、税法、反洗钱法和了解客户规则、刑法；第四部分提供了一个结论。

二、元宇宙：理论与实践

在这一部分中，我们将讨论元宇宙的理论及其实践。在这些元宇宙实践中，出现了独特的法律和伦理问题。在理论维度，我们将概述元宇宙的概念、经济和技术性细节，以及元宇宙中使用的货币和支付系统。在实践维度，我们将解释元宇宙的应用，因为它们是元宇宙用户之间法律关系的来源。这两个维度的讨论，将作为元宇宙法律分析的基础。

（一）元宇宙的概念

目前没有一个统一、共识性的元宇宙概念。“元宇宙”一词最早由尼尔·斯蒂芬森（Noel

Stephenson）在 1992 年的科幻小说《雪崩》（Snow Crash）中提出。在《雪崩》中，斯蒂芬森用“元宇宙”来描述一个乌托邦，以避免现实生活中的反乌托邦。如今，“元宇宙”这一概念已经扩展到包括虚拟世界中的真实活动。这样的虚拟世界通常配备了增强现实（AR）、虚拟现实（VR）、扩展现实（XR）、3D 技术以及物联网（IoT）技术。元宇宙也被称为 Web3.0，是当前 Web2.0 状态的下一代互联网。

从词源上讲，“元宇宙”一词来源于 meta 和 universe 这两个词。meta 的意思是“之后”“在……之后”“转变”或“超越”。帕克和金（Park & Kim）的一项研究很好地提炼了元宇宙的许多定义。在该项研究中，他们提供了从 54 项研究汇总而来的元宇宙的广泛定义。然而，元宇宙最常见的概念，是指用户使用化身来行动/交互的虚拟世界，以及作为一种媒介、通过用户的化身去连接用户的扩展现实技术（XR）。元宇宙的最新概念与其早期版本（例如游戏《第二人生》的版本）的不同之处在于，它是第一个使用 Z 世代的社会价值观开发的，Z 世代认为线下世界和线上世界根本没有什么区别。

（二）元宇宙的经济

2021 年 10 月，元宇宙公司总市值为 14.8 万亿美元。其中，包括市值 155 亿美元的 Roblox、市值 19.3 亿美元的 Sandbox 和市值 19 亿美元的 Decentraland。图 1 展示了元宇宙的市场参与者。

图 1　元宇宙的市场图（6.1 版本，2021 年 11 月 24 日更新）

值得注意的是，虽然目前的元宇宙状态尚未发挥其全部的潜力，但它已经展示了巨大的经济潜力。早期的研究表明，元宇宙的市场潜力在 3.75 万亿美元到 12.46 万亿美元之间。这或多或少受到了元宇宙狂热者的最近推动，特别是加密货币和非同质通证（non-fungible tokens，又译“非同质代币”，简写为 NFTs）用户的推动。如图 2 所示，2022 年 5 月，通过元宇宙应用程序进行的销售的全球日销售额飙升到了 6 亿美元。

元宇宙的经济问题包括初创企业和现有企业之间的竞争问题，以及运营元宇宙对社会福利的

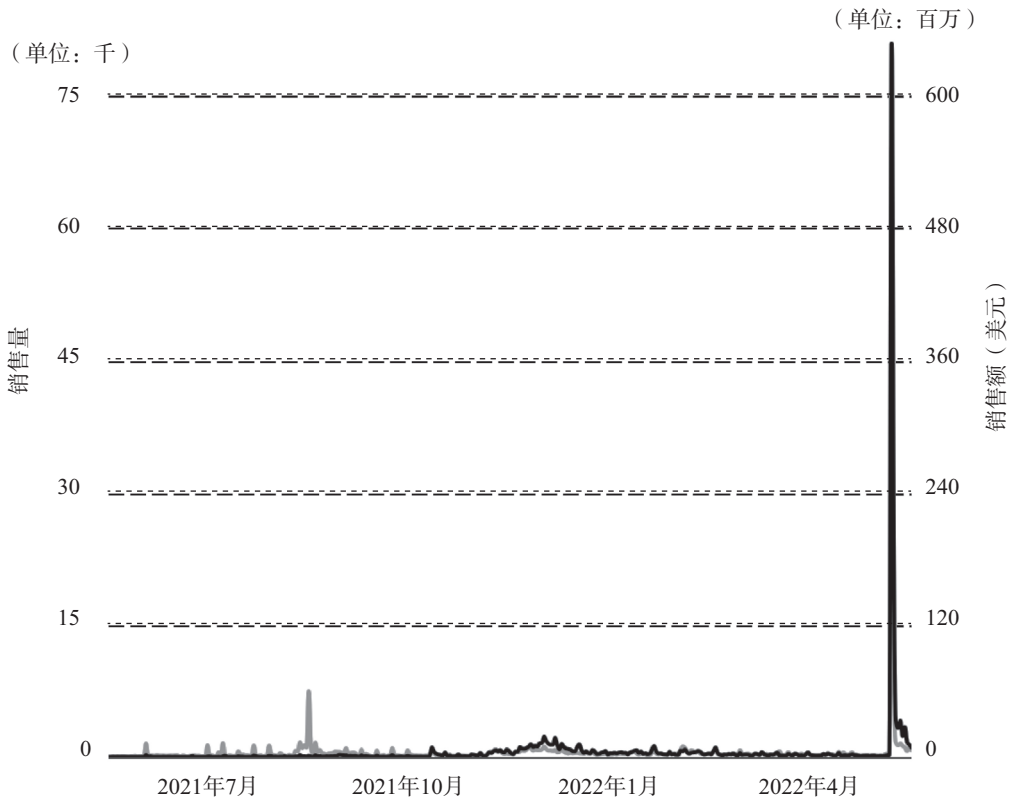

图 2 过去一年通过元宇宙应用程序的每日销售额〔6〕

影响。元宇宙是凯恩斯主义的需求驱动型创新，因此内嵌在元宇宙中的“按需”（on-demand）产品/服务将成为其优势。正如我们所知，这可能会导致元宇宙对传统商业的破坏，或者元宇宙仍然停留在一个乌托邦的设想上。

（三）元宇宙的分类

由于元宇宙目前仍处于早期阶段，许多研究都提出了不同的分类方法，以便我们更好地理解元宇宙这个概念。其中，一项突出的研究是帕克和金提供的元宇宙分类。他们提出了实现元宇宙概念的三大构成和三种方法：三大构成是物理设备和传感器（硬件）、识别和渲染（软件）以及场景生成（内容）；而三种方法则包括用户交互、实施的技术方法和元宇宙应用。图 3 显示了用于实现元宇宙概念的每个构成部分和方法的详细信息。

在这项研究中，值得注意的是元宇宙应用程序的关键作用，因为它们将作为法律权利和义务的基础。这些应用程序包括模拟、游戏、办公、社交、营销、教育和经济交易。

（四）元宇宙使用的货币和支付系统

元宇宙中的活动都通过加密货币、非同质通证或代币等支付手段而绑定起来。这些虚拟资产充当了元宇宙联通现实世界的经济桥梁。有人可能会说，这些虚拟资产确实赋予了元宇宙更深的

〔6〕 数据来自 https：//nonfungible. com/market-tracker.

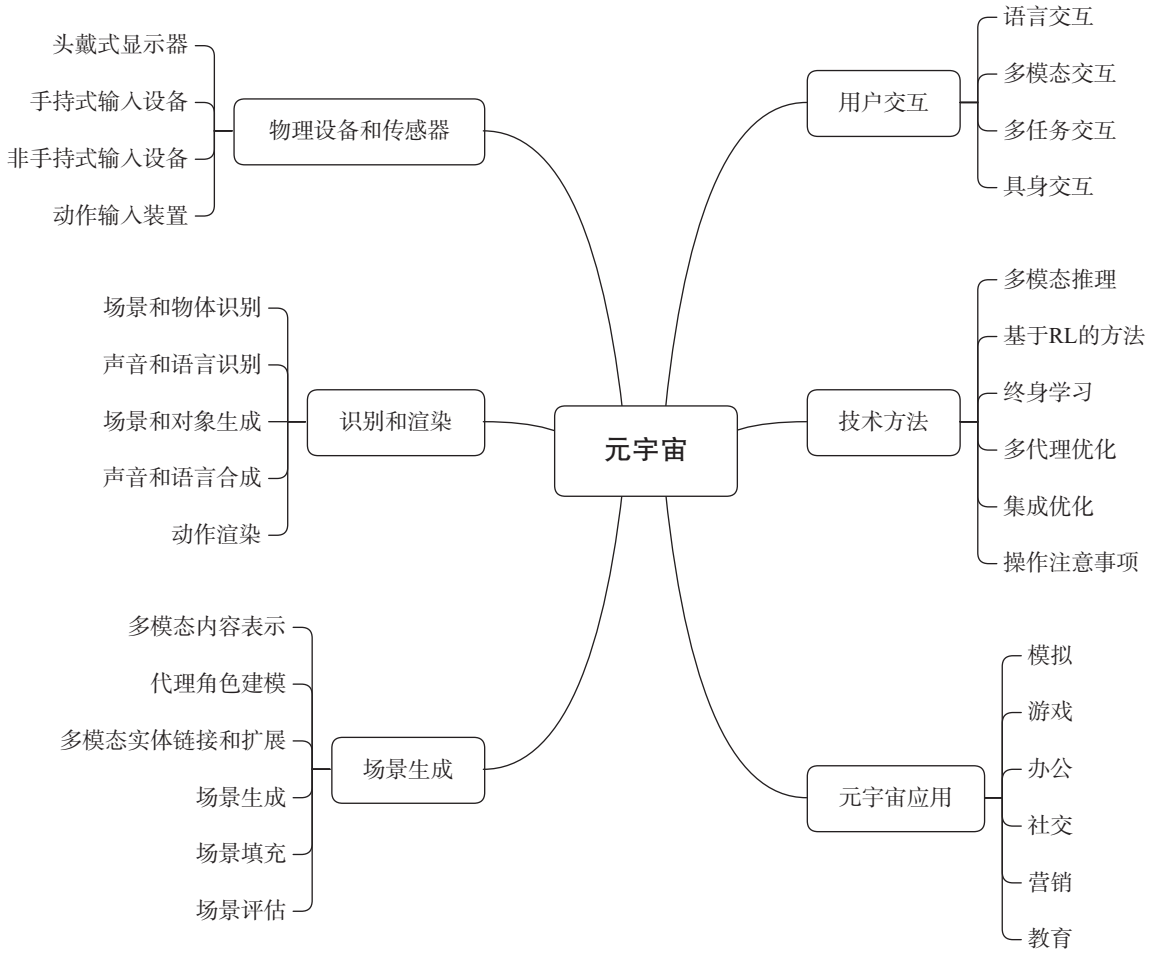

图 3　帕克和金的元宇宙分类

社会和经济意义。例如，Decentraland 使用 Polygon Mana 这种加密货币，而 Sandbox 使用的加密货币是 Sand Crypto。在加入元宇宙之前，用户必须为自己创设数字钱包，用户可以在数字钱包中存放如 Mana 和 Sand 之类的加密货币、非同质通证或代币。

三、元宇宙的法律难题

本部分主要围绕元宇宙有关的法律问题展开讨论，涉及元宇宙的各种应用和各方主体。根据上述元宇宙的理论和实践，我们归纳了元宇宙中的七种行为类型，包括模拟、游戏、办公、社交、营销、教育和经济交易。当然，所有这些行为都是以虚拟形式进行的。从这些类型化的行为出发，我们分析了相关的法律问题，并在以下各小节中进行讨论。

（一）物权法和知识产权法：需要一部“虚拟财产法”吗？

第一个也是最关键的法律问题，即物权法和/或知识产权法是否可以在元宇宙中适用。或者说，一个明显的问题是，制定一部“虚拟财产法”的时机是否成熟。

通常来说，物权法调整使用物并排除他人使用该物的权利。它回答了两个常见的难题：（1）谁

有权使用该物；（2）他们如何获得这项权利。物权法的常见例子是土地或个人物品（例如自行车或椅子）的使用。物权法的目标是为各种利益、使用权之间的分配提供一种公正、可预测、透明的手段。

在元宇宙中，所有的物都是虚拟的，且使用和存储方式同样是虚拟化的。它们不同于物权法中的有体物，有体物在物理上可以位于特定位置。虽然物权法制度可以用于解决无体物的使用问题，但不能解决权利使用的分配问题。因此，物权法基本无法适用于元宇宙。

知识产权法可能在本质上更适用于元宇宙。与传统的物权法不同，知识产权法调整的客体不一定是可以在物理上放置的有体物。知识产权法调整无体物的权属、享有的权利以及其衍生的权利形式。这些权利包括专利权、版权和商标权。

研究知识产权如何在元宇宙中发挥作用至关重要。按照一种非常传统的方式，元宇宙中的权属可以分为两种不同的类型。第一种是虚拟世界中一切财产的权利属于平台提供商（platform provider）。在这种情况下，用户只能从平台提供商处获得使用此类物的许可。游戏《魔兽世界》（World of Warcraft）〔7〕就是一个例子。根据《魔兽世界》的《服务条款》，平台内的所有权利、资格和利益均属于平台提供商。这包括用户账户、数据、计算机代码、虚拟商品（如货币和数字卡）、所有角色，甚至角色的名字。〔8〕第二种是允许用户拥有某些财产。游戏《第二人生》就是一个很好的例子。根据《第二人生》的《服务条款》，用户将保留任何法律上承认的权利，包括版权等知识产权。〔9〕

然而，第一种权利模式无法适用于元宇宙。对于元宇宙来说，只有第二种权利模式是可能的，其中用户有权拥有某些财产。这是因为，在元宇宙中，用户的行为模仿了现实世界，包括拥有土地和/或房屋（当然是虚拟的）的权利、拥有进行交易的货币（当然还有加密货币），或者创造、购买和出售非同质通证或代币。〔10〕如果在元宇宙中适用第一种权利模式，元宇宙就无法发挥其最大潜力。也许，这样的平台根本就不能被称为元宇宙。

如果允许元宇宙中的任何用户拥有某些财产，那么下一个问题将是，现有的知识产权法是否足以保护用户知识产权免受他人的侵犯。与规制有体物的物权法不同，知识产权法乍一看似乎是完美的。但是，知识产权法在法律实施方面会显现出局限性。由于元宇宙的行为跨越了不同司法管辖区并涉及不同国家的主体，法律管辖权、法律选择和执法权等问题就导致现有知识产权法在元宇宙中的适用具有不确定性。

（二）隐私和数据保护

当我们从公开透明原则来考虑元宇宙时，隐私问题就会出现。然而，人们加入元宇宙的动机

〔7〕《魔兽世界》是暴雪娱乐在2004年发行的一款最受欢迎的大型多人在线角色扮演游戏。根据Statista数据平台统计，《魔兽世界》现在拥有大约475万活跃用户。

〔8〕参见暴雪最终用户许可协议的第2条。

〔9〕例如，《服务条款》第1.2条第1款规定的“……你（用户）保留你在你的用户内容中拥有的任何法律上承认的权利、资格和利益”，以及第2.3条第1款规定的“你在你上传、发布和提交的内容中保留你法律上拥有的任何和所有知识产权……”。

〔10〕与此同时，有学者针对这一问题也提供了类似的分析，但使用了不同的术语。例如，有学者［迈克尔·周（Zhou）、马克·林德斯（Leenders）、凌美聪（Cong）］指出，元宇宙中有两种不同的权利框架，即平台所有权和内容所有权。这两个所有权框架对元宇宙来说至关重要。

始终是享受社交互动，包括与他人共享个人数据与信息。由于元宇宙是为开放和透明而设计的，因此信息共享是无条件的。在现实世界中，人们在与他人互动时完全掌控着自己的个人信息。然而，这显然不符合元宇宙的实际情况。因此，监管机构需要对元宇宙平台提供商进行监管，以优先考虑元宇宙用户的隐私。

第二个隐私问题涉及侵犯隐私权。就像在现实世界中一样，人们在元宇宙中同样爱管闲事和充满好奇。在元宇宙中的社交互动中，用户与用户之间往往有更多的接触，因为元宇宙中的“生活”对他们来说更加奇幻。这种动机和行为可能会使隐私处于危险之中。一旦发生隐私泄露，元宇宙平台提供商只有非常有限的机制来降低隐私泄露的负面影响。

另一个问题与用户的数据保护有关。元宇宙存储和管理着用户的大量数据，包括个人数据。元宇宙的数据流量非常巨大，从而导致了一些数据控制问题。这还没有考虑与跨境数据流动相关的问题，因为元宇宙的用户通常来自数百个国家。[11] 下面这些棘手的问题已经显现出来：（1）元宇宙平台提供商在多大程度上有义务遵守隐私和数据保护法，例如遵守严格的欧盟数据保护方面的法律法规；（2）数据保护机构是否有权对其管辖范围以外的元宇宙平台提供商执法。

（三）合同法和智能合约

元宇宙中的合同法问题是双重的。第一类合同关系调整的是诸如林登实验室（Linden Labs）和动视暴雪（Activision Blizzard）等平台提供商和其用户之间的法律关系。此类合同出现在平台提供商提供的服务或使用条款（terms of services or uses）和最终用户许可协议（end users licensing agreement）中。不幸的是，这些合同中没有最低限度的条款来保护元宇宙用户。例如，法院对用户能否保留其合法权利的裁判不一，这会使事情变得复杂化，尤其是在发生争议时。如此一来，对于同时横跨多个元宇宙平台的用户来说，不存在一致性待遇。

第二类合同关系调整平台用户之间的交互关系。由于元宇宙对任何个人（包括企业）同样开放，因此该类合同可能是 C2C、C2B 或 B2B。与此同时，虽然某项法律能够适用于现实世界的情形，但它在元宇宙中适用的结果可能是不确定的。消费者保护法就是这样的一个例子。因此，元宇宙用户之间的合同关系是独特的，需要在适用特定法律之前逐案分解。

进一步的问题涉及智能合约。元宇宙本质上是一个计算机程序，因此，它通过计算机代码的使用而获得发展，也就必然鼓励智能合约的应用。在元宇宙中使用智能合约可以提升整个元宇宙运行的实用性、效率性和敏捷性，因此，没有必要将传统合同照搬适用于元宇宙中的每一个行为。

（四）网络安全和网络攻击

最近，越来越多的网络攻击发生在虚拟世界中。网络安全的风险随着下一互联网——元宇宙——的展开而有所增加。此类风险各不相同，从身份盗窃到安全漏洞造成的经济损失，不一而足。元宇宙安全问题的关键点包括：（1）身份管理，元宇宙平台提供商如何设计和加强元宇宙用户身份管理的安全性；（2）DDoS 攻击；（3）设备漏洞，这更多的是在用户端；（4）数据外溢和数据开发。一旦发生违规行为，由于有限的补救程序以及管辖范围/地区问题，元宇宙用户是最

〔11〕 例如，游戏《第二人生》平均每天有 20 万的活跃用户，他们来自 200 多个国家和地区。

为脆弱的。

（五）货币和支付系统法

货币和支付系统法的主要法律渊源是两大类法律：货币法和中央银行法。第一类法律为货币作为法定货币的使用奠定了基础，第二类法律赋予了中央银行在其管辖范围内采取货币政策并规范、监督支付系统的权力。〔12〕

大多数国家的货币法将自己的货币定义为法定货币。公民必须使用和接受这种货币来履行金融义务，包括清偿债务。一些国家限制使用其他货币或资产来履行这些义务，而另一些国家则在明确规定使用其他货币或资产方面处于真空状态。这就是为什么当加密货币的使用出现时，各国政府采取了截然不同的方法。美国和中国政府从一开始就明确限制在其管辖范围内使用加密货币。同样的，印度尼西亚政府也禁止使用加密货币作为支付手段。

现代中央银行法更加标准化。它们主要包括中央银行的目标以及法律赋予中央银行实现这些目标的职能或权力。然而，这些目标可以是单一的、双重的，甚至是多重的，具体取决于国家在建立中央银行时的经济、社会和政治条件。无论出于什么样的条件，世界上每一部中央银行法都将维持物价稳定的目标反映在稳定的通货膨胀和汇率上。

由于中央银行的主要目标与维持物价稳定有关，加密货币的兴起就对中央银行的有效性构成了威胁。这是因为，加密货币是由中央银行管辖范围以外的各方或团体发行、流通的私人货币。加密货币的广泛使用将使中央银行的工作变得困难，尤其是在控制货币供应方面。不幸的是，元宇宙中的行为与加密货币、非同质通证以及中央银行以外的私人发行的代币紧密相关。因此，元宇宙的兴起可能会对中央银行履行职责构成更大的威胁。

（六）虚拟资产法规

在货币和支付系统法律的相关问题之后，讨论虚拟资产法规也是很重要的。不同的经济体在监管虚拟资产方面采取了不同的方法。相关的法规包括对加密货币交易要求获得政府许可的证券法、将加密资产视为大宗商品的大宗商品法，〔13〕以及反洗钱法和了解客户规则，〔14〕其要求虚拟财产交易所履行某些义务，如提交可疑交易报告。由于元宇宙仅将加密资产用于其交易，因此不同法律的适用可能导致元宇宙的发展变得复杂。

（七）税法

对虚拟商品和服务以及虚拟世界中的行为进行征税的问题，一直是G20经济体领导人关注的重点。〔15〕事实上，十年前就已经出现了这一问题，即政府是否可以对虚拟世界中的商品、服务和商业交易行为征税。因此，政府需要制定履行此类义务的框架和标准，从而避免双重征税，加重公民、企业的负担。这场运动的主要背景是，虚拟世界一直被视为避税天堂。此外，元宇宙与

〔12〕 对于中央银行法，国际货币基金组织（IMF）有一个由世界上大多数国家的中央银行法组成的数据库，即中央银行法数据库（CBLD）。该数据库可以通过预先查询和注册获取。

〔13〕 例如，印度尼西亚是将加密货币等虚拟资产视为商品的国家之一。

〔14〕 适用此类规则的司法管辖区包括美国、英国、加拿大和德国。

〔15〕 现在，它甚至已经成为G20峰会的主要优先议程之一。G20是一个由20个主要国家和地区组成的合作小组，其中包括美国、加拿大、欧盟、澳大利亚、德国、法国、意大利、沙特阿拉伯和印度尼西亚。今年，在印度尼西亚担任轮值主席国期间，G20峰会进一步讨论了将税收义务适用于虚拟世界中的行为的标准和框架。

区块链紧密相关，而区块链的支付系统是加密货币，这种加密货币以逃税而闻名。元宇宙中的经济交易量不断增加，各方继续享受虚拟世界中的商品和服务，而政府却难以征税。税务机关一直无法触及价值数万亿美元的虚拟市场。

（八）赌博监管

当美国政府禁止《第二人生》这款游戏的赌博功能时，《第二人生》就失去了名气和大量用户。最受欢迎的早期元宇宙版本的用户量减少了近一半，《第二人生》游戏的人气开始下降。最近，《第二人生》的日活跃用户平均为 20 万，来自约 200 个国家和地区。〔16〕

从游戏《第二人生》的案例来看，政府对赌博的监管显然与元宇宙的发展有关。尽管元宇宙声称是一个使用化身进行交互的纯粹虚拟世界，但事实证明，政府在现实世界中的执法会影响元宇宙的存续。因此，元宇宙的倡导者在制定这方面的规则时需要更加谨慎。

（九）刑法

从更加科学的方式出发，我们可以从劳埃·克里斯汀（Laue Christian）提出的三种不同观点来理解元宇宙。第一种观点考虑虚拟世界平台是否会为已有互联网犯罪带来新的维度。也就是说，目前互联网上的犯罪类型有增加的潜在危险，但对于一种全新犯罪类型的发展来说，可能性仍很低。第二种观点将虚拟世界视为一个独立的社会。在这种观点的理解下，犯罪行为的影响可以通过犯罪学来评估。然而，应用这种观点存在一个关键问题，即现实世界中犯罪学的结论往往难以应用于元宇宙的独特条件。第三种观点认为，元宇宙的使用可以触发现实世界用户的反馈效应。这种观点认为长期沉溺于元宇宙会对现实世界用户的行为产生不利影响。然而，这种观点目前来看相当荒谬，因此还需要进一步研究。

有观点认为，元宇宙中的潜在犯罪活动包括跟踪、攻击和虐待行为、儿童色情、绑架、侵犯知识产权以及庞氏骗局等金融欺诈和各种诈骗。运用上述劳埃·克里斯汀的理论，是很难评估这些潜在的犯罪行为的。元宇宙中的这些犯罪是完全新型的犯罪，还是与现实世界的犯罪相似但又独立的类型，可以适用现有的犯罪学理论吗？对此，主张适用现有犯罪学的观点似乎更为便利。如此一来，执法机构就能够简单地使用既有的完备程序来履行其职责。然而，简单粗暴地应用这种观点而不接受任何其他可能的观点是危险的。未来是未知的，元宇宙的发展仍处于早期阶段。因此，元宇宙鼓励思想的开放。

（十）其他问题：治理和伦理

长期以来，人们一直认为虚拟世界缺乏治理。当然，元宇宙也不例外。适用于此类虚拟世界的规则，主要包括使用条款和平台提供商制定的社区标准/规范。事实上，虚拟世界中没有任何民主可言。这是因为，平台掌控者就像独裁者一样统治他们的元宇宙。一些案例已经充分证明，这些平台掌控者往往无法将“社会福利”作为一项优先考虑的事项，因为他们有着私人的商业利益。正因如此，对元宇宙进行标准化的全球治理的呼声应运而生。

另一方面，元宇宙中的伦理问题并不比治理问题更为简单。自从使用 Web 2.0 以来，元宇宙中的伦理问题就被提了出来，然后随着物联网的普遍使用而进一步扩展。在元宇宙中，至少有五

〔16〕 这一数据是由林登实验室（Linden Labs）在 2021 年 6 月 23 日庆祝《第二人生》上线十八周年时公布的。

种与伦理问题相关的场景。它们包括身份问题、不同用户或用户群体的不同伦理和价值观、剥削风险、骚扰和破坏以及犯罪问题。

尽管有人可能会提出元宇宙伦理问题是否重要的问题，但如果我们希望元宇宙得到蓬勃发展，就必须解决这些伦理问题。例如，与身份相关的问题就与元宇宙用户的动机密切相关。接近43%的用户加入元宇宙，是为了通过了解真实的自我来帮助自己。曾经有一项调查显示，75%使用男性头像的用户实际上是女性，而80%使用女性头像的用户竟然是男性。尽管元宇宙是模仿现实世界中的活动，但事实证明，元宇宙中的化身并不是100%代表现实世界中的真人。当然，这种情况会使事情复杂化，尤其是在涉及法律权利和义务时。

四、结 论

虚拟世界、元宇宙的兴起似乎是不可避免的。许多人支持元宇宙的发展，因为它蕴含着巨大的潜力。他们认为元宇宙是继互联网之后的下一个大事件，并将其称为Web 3.0。然而，也有不少人对元宇宙不抱有太乐观的看法，主要原因有以下两个：（1）元宇宙的想法并不是全新的；（2）元宇宙的早期版本（例如游戏《第二人生》）并没有很成功，而它当前的版本（例如Sandbox和Decentraland）仍在开发中。因此，这些反对者认为元宇宙的兴起只不过是人为炒作而已。

从法律的角度来看，元宇宙引发了一系列法律难题。关于技术对于法律权威和尊重法律的要求的三种冲击的理论观点表明，元宇宙属于技术冲击的第一种。元宇宙创造了一个现实世界中的法律可能难以适用的空间。因此，元宇宙破坏了法律权威的“传统主张”，以及仅仅因为它是法律而尊重法律的要求。然而，将现实世界的法律适用于元宇宙中的行为是最简单的方法，尽管这种方法并非没有挑战。尽管元宇宙中的行为被认为是在模仿现实世界的行为，但将现实世界的法律适用于元宇宙中存在很多局限性。

第一个局限涉及元宇宙的财产及其所应适用的所有权框架。物权法很难在元宇宙中适用，因为元宇宙中的财产不是物权法所调整的具有物理性存在的有体物。知识产权法可能更适合在元宇宙中适用，但法律管辖、法律选择和法律执行等问题也会出现。这样的法律在纸面上对于元宇宙来说可能是完美的，但在具体实施中将是有缺陷的或者不完整的。进一步的难题涉及：（1）元宇宙存储和管理大量数据（包括用户的个人数据）所带来的数据保护问题，以及跨界数据流动问题，因为元宇宙中的用户通常来自数百个国家；（2）如何在元宇宙中适用“传统”合同法，因为元宇宙主要使用智能合约来实现其整体运作的实用性、效率性和敏捷性；（3）网络安全问题，因为越来越多的网络攻击发生在虚拟世界中；（4）各国政府对虚拟商品、服务和商业行为征税的共同努力；（5）政府限制元宇宙中的赌博活动，对元宇宙的发展产生了不利影响；（6）将刑法适用于虚拟犯罪的问题；（7）元宇宙被指责缺乏治理和民主，并且元宇宙的一些用户在行为上缺乏道德感。

此外，需要特别强调的是将货币和支付系统法适用于元宇宙的局限性。货币和支付系统法的法律渊源是货币法和中央银行法。这两类法律都倾向于限制加密货币在元宇宙中的使用，因为加

密货币给中央银行实现维持物价稳定的目标带来了困难。美国、中国和土耳其等国家都采取了在管辖区范围内限制使用加密货币的方法。此外，加密资产的法规因不同司法管辖区而异，这也对元宇宙的繁荣构成了障碍。此类法规包括美国的证券法、印度尼西亚的大宗商品法以及英国、加拿大和德国适用的反洗钱法和了解客户规则。

Abstract: The metaverse has gained momentum after the CEO of the biggest social media organization made a statement that the metaverse would be the next big thing after the Internet. Although there is no single, agreed upon definition of the metaverse, the common understanding of the metaverse is that the concept combines IoT, AR, VR, XR, and 3D technologies. The market capital and other economic potential of the metaverse is enormous. Hence, it is of importance to discuss the legal implications of the metaverse. This article is the first to elaborate the legal conundrums of the metaverse in a proper manner. It includes discussion of general and property law and intellectual property law, and whether the time has come to have "a virtual property law". It also discusses some other legal issues such as privacy and data protection, contract law, cybersecurity and cyberattacks, monetary and payment systems laws, and regulation of virtual assets, tax law, anti-money laundering laws and KYC, and criminal law. The metaverse creates a space where the law of the real world may be difficult to apply. Therefore, the metaverse disrupts the "traditional claims" from the legal authority and the demand for respect for the rule of law just because it is the law. However, applying this subset of the real-world laws to the metaverse turns out to be possible, but with limitations. Such limitations arise specifically when it comes to the operation of the law.

Key Words: metaverse, legal conundrums, virtual world, monetary law, payment system law

（责任编辑：张金平　赵建蕊）

财经法学 No. 1，2022
pp. 3 - 17

信息主体同意的适用边界

李群涛　高富平*

内容提要：在欠缺其他合法性基础情形下，信息主体同意是否适用，关键在于处理的个人信息是否含直接标识符。直接标识符能单独表征信息主体身份，从而使信息处理风险与信息主体身份精准连结。因此，出于尊重陌生人社会信息主体隐匿身份的自由、尊重信息主体对处理风险的自主决策，信息主体可以通过同意控制含直接标识符的个人信息，即“单独识别个人信息”。但同意不适用于“结合识别个人信息”。首先，结合识别个人信息具有模糊性，个人信息处理者难以就此直接识别信息主体身份进而征求同意。其次，《个人信息保护法》确立了处理结合识别个人信息不需告知规则，逻辑上也要求有相应的不需同意规则。最后，结合识别个人信息不适用同意规则也是实现“促进个人信息合理利用”这一立法目的的可行路径。

关键词：单独识别个人信息　结合识别个人信息　同意　直接标识符　个人信息保护法

一、引　言

《民法典》与《个人信息保护法》已经相继出台，作为个人信息保护制度重要内容的同意规则，其框架已经建构完成。无论《民法典》第1035条第1款第1项还是《个人信息保护法》第13条第1款第1项，都确认“信息主体同意”这一合法性基础的重要地位。然而在解释上尚未明确之问题为：当不具备《个人信息保护法》第13条第1款第2至7项所列举的合法性基础时，[1]信息主体同意是否适用于对各类个人信息的处理行为。此即本文尝试回答的信息主体同意之适用边界问题。

针对信息主体同意之适用边界问题，学界已有讨论，并形成四种学说。按照各学说主张的适

* 李群涛，华东政法大学法律学院博士研究生；高富平，华东政法大学法律学院教授。

〔1〕 关于《个人信息保护法》第13条所列七项合法性基础的研究，参见程啸、王苑：《论个人信息处理中无需取得个人同意的情形》，载《人民司法》2021年第22期。

用范围从小到大排列，分别为“无适用空间说”“敏感个人信息说”“全部个人信息说”和“全部个人信息＋匿名信息说”。笔者逐一简要述评。

“无适用空间说”认为，同意规则不能适用于任何个人信息之上，甚至不宜作为个人信息处理的合法性基础。〔2〕然而，《民法典》和《个人信息保护法》仍然坚守同意规则，故该说不为现行法所接纳。

“敏感个人信息说”认为，同意规则仅适用于敏感个人信息。〔3〕然而目前同意规则位于《个人信息保护法》“个人信息处理规则”章的“一般规定”中，该制度的体系位置至少表明一般个人信息并非一概不适用同意规则。故该说亦不为现行法所接纳。

“全部个人信息说”认为，同意规则适用于全部个人信息。〔4〕当然该说亦承认应当针对不同类别个人信息建构一套宽严有别的梯度保护体系。〔5〕该说似符合法条文义，但不利于实现《个人信息保护法》所确立的“促进个人信息合理利用”的立法目的。笔者将于本文第三、四部分详细论证，此处不赘。

“全部个人信息＋匿名信息说”认为，同意规则适用于现行《个人信息保护法》中规定的个人信息与匿名信息。〔6〕然而无论《网络安全法》第 42 条第 1 款但书，还是《民法典》第 1038 条第 1 款但书，抑或《个人信息保护法》第 4 条第 1 款皆明定匿名信息不适用同意规则。因此，该说亦不为现行法所采。

综上，关于信息主体同意的适用边界问题，上述四说均难谓妥当。

个人信息是与个人有关的各种信息，同意是个人信息处理的合法性基础，个人信息处理者为取得同意，在收集个人信息之前即需判断信息主体身份。然而个人信息范围无边无界，大量个人信息在信息主体身份判断方面具有模糊性，这对个人信息处理者于处理前履行“取得同意义务”造成障碍。

于是，本文提出，按照是否含直接标识符的标准将个人信息划分为“单独识别个人信息”与“结合识别个人信息”，同意规则仅适用于单独识别个人信息。事实上此种对个人信息的分类方法在学界的讨论中并不少见，〔7〕甚至已经为现行法所接纳（《民法典》第 1034 条第 2 款），但是鲜有观点将此种分类与同意规则的适用边界相联系并进行证成。〔8〕本文首先勾勒该边界的轮廓，

〔2〕 参见任龙龙：《论同意不是个人信息处理的正当性基础》，载《政治与法律》2016 年第 1 期。

〔3〕 参见汤敏：《论同意在个人信息处理中的作用——基于个人敏感信息和个人一般信息二维视角》，载《天府新论》2018 年第 2 期。

〔4〕 参见陆青：《个人信息保护中“同意”规则的规范构造》，载《武汉大学学报（哲学社会科学版）》2019 年第 5 期；徐丽枝：《个人信息处理中同意原则适用的困境与破解思路》，载《图书情报知识》2017 年第 1 期。

〔5〕 参见丁晓强：《个人数据保护中同意规则的“扬”与“抑”——卡－梅框架视域下的规则配置研究》，载《法学评论》2020 年第 4 期。

〔6〕 参见林洹民：《个人信息保护中知情同意原则的困境与出路》，载《北京航空航天大学学报（社会科学版）》2018 年第 3 期。有必要指出，该说否认存在匿名信息，因为技术界人士已经明确表示不存在绝对不可复原的匿名信息。在此基础上，按照该说，仅当法律规定了不准复原义务时，现行法所述的匿名信息才豁免适用同意规则。

〔7〕 参见陶盈：《我国网络信息化进程中新型个人信息的合理利用与法律规制》，载《山东大学学报（哲学社会科学版）》2016 年第 2 期。

〔8〕 有学者曾提及此方面，但并未展开。参见胡文华、黄道丽、孔华锋：《个人数据保护“同意规则”的检视及修正》，载《计算机应用与软件》2018 年第 9 期。

进而分别论证同意适用于单独识别个人信息，而不适用于结合识别个人信息。

二、信息主体同意规则适用的判断标准：含直接标识符

信息主体同意是否适用，其判断标准就在于个人信息是否含有直接标识符。在重视和重新界定直接标识符概念的基础上，个人信息分为单独识别个人信息与结合识别个人信息。

（一）直接标识符概念的重视与重新界定

直接标识符是指能够单独识别特定自然人身份的信息。〔9〕直接标识符的典型特征在于具有唯一性〔10〕和身份指向性，例如身份证号、社会保险号码、人脸信息等。需要注意的是，直接标识符与特定自然人是单向唯一对应关系。具言之，一直接标识符只对应唯一特定自然人，但一特定自然人将有许多直接标识符。所谓身份指向性意味着存在直接标识符即足以识别信息主体真实身份。正如学者所言，信息的人格属性集中体现在其可识别特定自然人身份的性质。〔11〕

我国立法已经接纳了直接标识符概念。我国个人信息概念借鉴欧美，而这一来源于欧美的概念恰恰无法脱离直接标识符。例如，欧盟《一般数据保护条例》（GDPR）第 4 条 a 项后半句中的身份证号等系本文所述直接标识符。同样地，美国立法一直强调直接识别符（direct-identifier）概念作为个人可识别信息（PII）的重要判断标准。与这一国际趋势相一致，我国实质上已经接受直接标识符概念，《网络安全法》第 76 条第 5 项以及《民法典》第 1034 条第 2 款，都具体列举了不少直接标识符，如身份证号码、生物识别信息等。

直接标识符可谓信息主体风险的重要来源。现代社会是风险社会，技术应用确实会给人类带来一定风险。同样地，在个人信息领域，大数据技术应用可能导致风险产生。然而，如果风险产生无法对应特定身份、不会影响到特定自然人，那么对于该自然人而言这或许并非风险，即使是也不必过于关注和担忧。但如前所述，直接标识符的本质特征在于其唯一性和身份指向性，直接标识符恰恰使个人信息处理者可知晓特定自然人身份。直接标识符在个人信息中具有重要地位，个人信息与个人身份的勾连往往依赖直接标识符。个人信息处理风险主要在于风险能通过个人信息直接传导至具有特定身份的自然人，此中起桥梁作用者正是直接标识符。

随着时代发展，直接标识符的范围已日渐扩张。目前，直接标识符包括社会身份标识符和生物身份标识符，后者是对传统直接标识符概念的扩张。〔12〕以前，直接标识符主要指身份证号、驾照号码、护照号码、社会保险号码、军官证号、工作证号、出入证号、社保卡号、居住证号码等社会身份标识符。〔13〕生物身份标识符后来也成为直接标识符的重要来源。例如，随着人脸识别技术发展，人脸信息等与特定信息主体之间也形成了唯一对应和身份指向关系。总之，某符号

〔9〕 参见《中国互联网定向广告用户信息保护行业框架标准》。

〔10〕 参见范姜真媺：《大数据时代下个人资料范围之再检讨——以日本为借镜》，载《东吴法律学报》2017 年第 2 期。

〔11〕 参见刘士国：《信息控制权法理与我国个人信息保护立法》，载《政法论坛》2021 年第 6 期。

〔12〕 参见《信息安全技术个人信息安全规范》（GB/T 35273—2020），附录 A，第 23 页；上海市地方标准《数据去标识化共享指南》（DB31/T 1311—2021）。

〔13〕 参见《信息安全技术个人信息安全规范》（GB/T 35273—2020）之附录。

具有唯一性和身份指向性，即可被认定为直接标识符。

直接标识符与间接标识符、准标识符均非同一概念。一方面，直接标识符与间接标识符并非同一概念。如果仅就“唯一性”而言，手机等智能设备序列号（又称“国际移动设备识别码”，简称 IMEI）也具有唯一性。仅依此虽能触及个人但不能识别个人身份，因此不具有前述直接标识符的“身份指向性”特征。于是，本文称之为“间接标识符”。另一方面，直接标识符与准标识符亦非同一概念，两者差异为是否具有唯一性。美欧都有实质意义上的准标识符概念。美国的准标识符（quasi-identifier）〔14〕对应欧盟 GDPR 第 4 条 a 项中的“个人属性”（factors），包括民族、种族、婚姻状况、身体、心理、基因、精神状态、经济、文化、社会因素等。准标识符中的“准”（quasi）字表明其本质上并非标识符。一个准标识符可能会对应多位自然人，不具有唯一性。例如，“研究生”是准标识符，能够对应千千万万研究生，无法指向特定自然人身份。

（二）基于直接标识符对个人信息的区分

以是否含有直接标识符为标准可将个人信息周延地分为单独识别个人信息和结合识别个人信息。

1. 单独识别个人信息

以前对个人信息相当部分的讨论恰以单独识别个人信息为基本思考模型。事实上 20 世纪即已经产生个人信息保护问题，当时个人信息即以单独识别个人信息为主。例如：“姓名张三，性别男，年龄 65 岁，身份证号 123456789012345678，电话号码 12345678901，家庭住址青海省西宁市湟源县胜利镇未来街道幸福小区 1 栋 1 单元 1025 号，银行卡号……”此为含有直接标识符个人信息（即单独识别个人信息）的典型样态。个人信息处理者据此能直接了解此个人信息对应的信息主体身份。单独识别个人信息的典型特征即在于含直接标识符。就此而言，《民法典》第 1034 条第 2 款中的“能够单独识别特定自然人的信息”与《个人信息保护法》第 4 条第 1 款中的“与已识别的自然人有关的各种信息”可表达同一含义。正因如此，本文一律用“单独识别个人信息”指代含直接标识符的个人信息。

单独识别个人信息，强调信息“含”直接标识符，而非除直接标识符之外没有其他信息。换言之，一旦数据集中含有直接标识符，直接标识符与其后跟随的购物记录、行踪轨迹等结合组成单独识别个人信息。如上所述，随着时代发展，直接标识符的概念有所扩张，生物身份标识符即为直接标识符的最新内容。因此，单独识别个人信息之范围亦相应扩张，兹不赘述。另外，是否“含”直接标识符，应当以数据集为单位全面审视，而非割裂个别数据项而单独看待。就此而言，直接标识符有可能是由一个数据集中多个数据项共同组成的，例如，在一个含有姓名、性别、学校、班级、行踪轨迹等数据项的数据集中，姓名、性别、学校、班级将共同构成直接标识符。

〔14〕 也有译为“间接标识符”，但须指出，此间接标识符与本文所谓间接标识符并非同一含义。参见刘颖、谷佳琪：《个人信息去身份化及其制度构建》，载《学术研究》2020 年第 12 期；程海玲：《个人信息匿名化处理法律标准探究》，载《科技与法律》2021 年第 3 期。

2. 结合识别个人信息

与单独识别个人信息相对的是结合识别个人信息，即不含直接标识符的个人信息。《民法典》第1034条第2款中“能够与其他信息结合识别特定自然人的各种信息”以及《个人信息保护法》第4条第1款中“与可识别的自然人有关的各种信息”，描述的均为不含直接标识符的个人信息。为表统一，本文一律用“结合识别个人信息”的概念。

结合识别个人信息也属于个人信息的范畴，但在未与直接标识符相结合的情况下，仅凭结合识别个人信息难以识别身份。换言之，信息主体以外的人仅通过结合识别个人信息来识别个人身份是需要成本的。目前个人信息定义无限扩张，这几乎成为国际社会的共识。欧盟第29条工作组出台的关于个人信息概念的意见对个人信息概念明显采广义理解，强调与其他信息结合能识别自然人身份或者特征，以及综合考虑内容、目的和影响三因素的情况下与个人有关系。〔15〕甚至按照欧洲学者分析，天气信息有时也能成为个人信息。〔16〕经扩张后的个人信息概念，其判断标准已经从能识别身份变为相关处理行为对人（不一定为特定自然人）有风险的信息。〔17〕按照《个人信息保护法》第4条第1款对个人信息的定义，我国接受了此种扩张标准。此标准非以信息当下状态为观察视角，而是要求立足当下预测充满无限可能之未来，即以未来看现在，这使得个人信息边界显著扩张且趋于模糊。从此角度而言，信息即使不含直接标识符，亦不妨碍被认定为个人信息从而适用个人信息保护相关规则。

结合识别个人信息大致有两类来源：一是各类传感器设备所收集的个人信息；二是从原始处理者或其他处理者处间接获取的经去标识化处理的信息。一方面，随着传感器的广泛布设，智能穿戴设备、网络设备的普及以及物联网技术的飞速发展与充分应用，海量的个人相关信息被快速采集供给、实时加工分析。但是相应地，部分传感器等设备能做到的只是实时记录个人有关情况而无法提供个人直接标识符等信息（信息主体主动提供的除外）。另一方面，随着信息实践不断开展，部分主体所控制的信息已经是经去标识化处理的信息。

需要注意结合识别个人信息与匿名信息的关系。所谓匿名信息是指经处理无法识别个人且不能复原的信息（《个人信息保护法》第73条第4项）。匿名信息制度通行于欧美而非我国独创。欧盟GDPR“鉴于条款”（recital）第26段明确指出，匿名信息（anonymous information）不适用于该法。该段同时指出，为了确定自然人是否可识别，应当考虑个人信息处理者或其他人（by another person）的识别能力，因此，匿名信息意味着任何人都无法通过匿名信息识别自然人身份。简言之，欧盟规定的匿名信息客观上不具有识别可能性。不过有专家已经声明，技术方面“匿名化是一种幻想”，只能达到识别可能性比较低的水平。〔18〕美国法学会2020年公布《数据隐私法律原则重述》，并在第2条中指出，无法识别个人的（non-identifiable）信息不适用数据隐私

〔15〕 See Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data, 01248/07/EN WP 136.

〔16〕 See Nadezhda Purtova, The Law of Everything. Broad Concept of Personal Data and Future of EU Data Protection Law, 10 *Law, Innovation and Technology*, 40 (2018).

〔17〕 参见范为：《大数据时代个人信息保护的路径重构》，载《环球法律评论》2016年第5期。

〔18〕 See Ohm, Paul, Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization, 57 *UCLA Law Review*, 1701 (2010). 当然，由此观之欧盟规定的匿名信息认定标准并不合理，对此本文不再详述。

保护原则。〔19〕不同的是，欧盟匿名信息指客观上无识别可能性，而美国“无法识别的个人信息”是指识别可能性极低。然而此种无法识别的个人信息仍具有一定的识别可能性，如果不使其受制于个人信息保护规范，那么将使该部分信息暴露于风险之中。为了弥补这一点，美国的匿名信息制度有其预设前提，即禁止再识别。〔20〕或许是受欧美影响，我国《个人信息保护法》第 4 条第 1 款规定匿名信息不属于个人信息。然而借鉴比较法的重要前提是我国与借鉴对象有相同的制度环境。〔21〕我国《个人信息保护法》第 73 条第 4 项没有明确规定禁止再识别要求，且在难存此解释空间的情况下，一旦将我国匿名信息等同于美国无法识别的个人信息，将导致对匿名信息的处理失去控制。而且从笔者梳理的 50 多个法域的法律文本来看，极少有对个人信息定义作如此限制的先例。但《个人信息保护法》既已作如此规定，只能认为应对匿名信息进行严格把握，当无法确定是否满足客观“不能复原”要件时，应当认定该信息为结合识别个人信息而非匿名信息。

三、同意规则适用于单独识别个人信息

信息主体能够以同意来控制个人信息的处理行为，其正当性基础在于由宪法上的个人尊严、自由以及主体地位推演而得的个人事务自决。〔22〕笔者以下欲指出，在个人信息领域，个人事务自决主要体现为尊重陌生人社会个人隐匿身份的选择和自由，以及尊重信息主体对处理风险的决策。此二理由均仅指向单独识别个人信息。

（一）尊重陌生人社会个人隐匿身份的自由

现代社会是陌生人社会，〔23〕隐匿身份是陌生人社会中的个人选择和自由。〔24〕人口增加、人口流动性增大和社会不安全因素混杂，导致公众轻易不愿意暴露身份。虽然社会交往要求社会中每个人必须允许其他人了解自己，但是此种要求也应仅限于与个人有交往关系之人。例如，一个人的亲朋好友、同事、老师、同学、交易对手，甚至欲与其缔结合同者。但不应无限扩展到千里之外与个人毫无瓜葛的陌生人。逐渐地，是否隐匿身份成为个人自主决定的事项，受到社会认可和法律保护。

〔19〕 See The American Law Institute, Principles of the law-Data Privacy (2020), available at https://1.next.westlaw.com/Document/I0f02ee65145811eb8a02f30620293de0/View/FullText.html?ppcid=1c4fd268d6b54fc98b7f1ebff22c23f3&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=%28sc.Search%29, last visited on Dec. 3. 2021.

〔20〕 按照美国《数据隐私法律原则重述》(2020) 的总结，其所谓不适用数据隐私法律原则的匿名信息条件有三：第一，采用合理方法去掉个人信息上的标识符；第二，使去标识符后的个人数据处于较低风险水平；第三，个人信息处理者不再重新识别个人。

〔21〕 参见〔德〕茨威格特、克茨：《比较法总论》(上)，潘汉典等译，中国法制出版社 2014 年版，第 30 页。

〔22〕 参见田野：《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；王雪乔：《论欧盟 GDPR 中个人数据保护与“同意”细分》，载《政法论丛》2019 年第 4 期；高富平：《同意≠授权——个人信息处理的核心问题辨析》，载《探索与争鸣》2021 年第 4 期。

〔23〕 近年来已经有相关文件关注到陌生人社会这一社会转型现象。参见《东莞市人民政府办公室关于印发〈东莞市深化“二标四实”工作总体方案〉的通知》(东府办〔2018〕44 号)；《江苏省民政厅对省十三届人大一次会议第 5015 号建议的答复》。学理上的讨论，参见张清、王露：《陌生人社会与法治构建论略》，载《法商研究》2008 年第 5 期；龚长宇、郑杭生：《陌生人社会秩序的价值基础》，载《科学社会主义》2011 年第 1 期；何绍辉：《论陌生人社会的治理：中国经验的表达》，载《求索》2012 年第 12 期。

〔24〕 参见龚长宇：《陌生人社会：价值基础与社会治理》，中国人民大学出版社 2021 年版，第 105 页。

然而，处理单独识别个人信息，将侵犯个人自主决定是否隐匿身份的自由。单独识别个人信息处理强调获得个人同意，其背后价值观与陌生人社会伦理基础不可分割。有学者称，“个体对于个人隐私和个人信息的身份识别的保护就是基于传统熟人环境社会下的潜在人格尊严和人格自由意识，而人们对于识别性的风险和恐惧多来自于传统观念下的身份泄露”〔25〕。显然，这种保护身份意识蔓延到了陌生人社会，成为个人典型的自由。如果毫不相干的主体欲全面了解一陌生人的单独识别个人信息（事实上就是了解身份），那么实在无任何正当性可言。虽然许多学者提及将分散的个人信息汇聚成大数据对于发挥数据经济价值、促进公共福利具有重大意义，但是直接标识符并非达致该目标所利用的大数据之必需。难以想象无任何交往关系的陌生私主体为了促进公共利益，需要利用他人之个人信息而且非含直接标识符不可。笔者强调，本文讨论的前提是不存在《个人信息保护法》第 13 条第 1 款第 2—7 项合法性基础，故为紧急救助而处理个人信息的情形不在本文讨论范围。正因如此，有学者指出，二次利用个人信息的首要条件是脱敏，即除去直接标识符。〔26〕简言之，陌生人可以收集他人的个人信息甚至进行个性特征分析，但是不允许其擅自知晓该“他人”的真实身份。社会学学者将这种秩序称为对陌生人“冷漠的尊重”。〔27〕

只有获得特定信息主体同意，才能使个人信息处理者与特定信息主体之间的显名交往正当化。在陌生人社会中，应然社会秩序是尊重他人的不同观念和不同选择。每个人相对于他人皆为“道德异乡人”，抱有不同信念、恪守不同行为规范；仅当取得他人“允许”“同意”“包容”时才能达成双方间新的共同行为规范。〔28〕陌生人社会的价值观在于每个人仅允许与其有关系的人了解其个人身份（当然随着关系远近了解程度会有不同），没有社会关系的陌生人不能了解其个人身份。与此相对应，允许与特定个人没有社会关系的人收集、使用该特定个人的个人信息，但仅限于收集、使用结合识别个人信息且不得在分析特征的过程中分析出真实身份。这便是个人信息领域陌生人的行为规范。如果处理单独识别个人信息，则等同于突破陌生人之间行为规范，因此，只有获得信息主体的同意以形成双方间新共同行为规范时，处理单独识别个人信息才被允许。或许出于类似考虑，有学者也指出信息主体能够支配自己的姓名、身份证号码、相貌特征等等。〔29〕此观点值得赞同。

（二）尊重信息主体对处理风险的决策

直接标识符的存在使得信息处理风险得以精准传导至具有特定身份的自然人。“风险可以被界定为系统地处理现代化自身引致的危险和不安全感的方式。”〔30〕如直接标识符定义所阐释，其最大特征为与特定自然人身份具有唯一对应性。个人信息处理者通过其所控制的单独识别个人信

〔25〕 苏今：《〈民法总则〉中个人信息的“可识别性”特征及其规范路径》，载《大连理工大学学报（社会科学版）》2020 年第 1 期，第 86 页。

〔26〕 参见姬蕾蕾：《论个人信息利用中同意要件的规范重塑》，载《图书馆》2018 年第 12 期。

〔27〕 参见前引〔24〕，龚长宇书，第 19 页。

〔28〕 参见前引〔24〕，龚长宇书，第 115－116 页。

〔29〕 参见郭明龙：《论个人信息之商品化》，载《法学论坛》2012 年第 6 期；韩强：《人格权确认与构造的法律依据》，载《中国法学》2015 年第 3 期。

〔30〕〔德〕乌尔里希·贝克：《风险社会》，何博闻译，译林出版社 2004 年版，第 19 页。

息便能直接识别信息主体而不需要进行任何处理行为（识别行为）。对此类单独识别个人信息进行分析，其决策结果可以通过直接标识符的桥梁作用精准配置于特定自然人。此种结果对于特定自然人而言可能有好有坏。例如，银行处理特定自然人单独识别个人信息用以评估该特定自然人信用情况，当处理结果符合信用要求时对该自然人而言有正向反馈，但当处理结果不符合信贷政策所要求的信用等级时，对于该自然人而言具有不利影响，因为这将关系到信息主体是否能顺利申请贷款。但算法不同以及其他因素，导致处理分析行为结果是好是坏无确定性甚至不可预期，这本身对于信息主体而言即为一种风险。除此之外，此类个人信息的滥用以及被篡改、毁损、丢失等都是对信息主体的风险。从《居民身份证法》《统计法》《刑法》等条文来看，我国个人信息立法的重要目的恰是为维护自然人人身、财产安全免受威胁。〔31〕

既然直接标识符的存在客观上产生了个人信息处理的风险与信息主体身份连结的效果，那么出于个人事务自决，应当允许个人对其未来风险进行自主判断和决定。尤其是当个人信息处理者从信息主体处直接收集个人信息时，双方处于直接交互状态，同意机制落实也较为简单。〔32〕如果立法者倾向于剥夺个人判断决策资格而一律允许个人信息处理者处理此类个人信息，那么即剥夺了个人自主决定、自主判断空间，此为典型的法律父爱主义，〔33〕将使信息主体暴露于个人信息处理的风险之中。即使法律对个人信息处理者行为进行规范和要求，也不能保证个人信息处理者必然严格遵守规则，此即禁止性规定会配套法律责任条款的重要原因。不仅如此，即便个人信息处理者遵守各类规定，也不见得处理行为不产生任何风险。当然，允许信息主体自行决策，原理在于允许个人对于精准连结身份的未来风险进行判断和决策，而非出于个人对其个人信息的完全控制。〔34〕关于该点，有学者通过细致考究已经指出，目前广为流传的个人信息自决权是对德国人口普查案的以讹传讹，〔35〕所以此处信息主体同意是个人自治的具体体现，是个人事务自决的应有之义。

事实上，避免存在直接标识符而导致信息处理风险精准传导至个人，亦符合国际个人信息保护制度的基本逻辑。以下以具有代表性的美国和欧盟的制度分别说明。

美国的信息主体同意规则重点关注可识别个人信息（personally identifiable information，简称 PII），即本文所述单独识别个人信息。起初按照美国的隐私控制理论，信息主体有资格决定个人信息在何时、以何种程度和方式进行流动。〔36〕但是隐私控制理论与美国人的信息自由信仰背道而驰。此种情况下，为了缓和信息控制和流动之间的张力，美国通过《儿童网络隐私法》等一系列法案将信息主体对个人信息的控制限制在 PII 范围内，即处理 PII 要经过信息主体同意，而 PII 恰恰相当于本文的单独识别个人信息。虽然美国分散式个人信息保护立法使 PII 的边界动态变化，但美国人的信息主体仅控制 PII 的立场却始终坚定。甚至根据美国最新出台的《统一个人

〔31〕 参见高富平：《个人信息保护立法研究》，光明日报出版社 2021 年版，第 195 页。

〔32〕 参见前引〔8〕，胡文华等文。

〔33〕 参见孙笑侠、郭春镇：《法律父爱主义在中国的适用》，载《中国社会科学》2006 年第 1 期。

〔34〕 关于该问题的讨论，参见前引〔22〕，王雪乔文；张勇：《APP 个人信息的刑法保护：以知情同意为视角》，载《法学》2020 年第 8 期；前引〔11〕，刘士国文。

〔35〕 参见杨芳：《个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体》，载《比较法研究》2015 年第6 期。

〔36〕 See Alan F. Westin，Privacy and Freedom，25 *Washington and Lee Law Review*，166（1968）.

数据保护法》（The Uniform Personal Data Protection Act，简称 UPDPA）〔37〕第 7 条第 b 款第 5 项结合同条第 a 款第 1 句，可以得出结论：针对去直接标识符的个人信息进行处理不需要获得信息主体的同意。〔38〕例如，在针对群体的医学研究中，为了研究某种疾病的地域分布关系，在收集各地患者数据时，至多同时收集患者所在省、市、县即可，没有必要得知患者姓名、身份证号等数据项，甚至患者的精确地址亦不具有必要性。此时个人信息处理者便不需要取得信息主体的同意。由是观之，美国人基本认为若无 PII 则不存在权益威胁。

欧盟的制度也体现了类似的思路。欧盟 2016 年制定了 GDPR，2018 年正式生效执行。部分关于 GDPR 的研究表明同意规则将赋予信息主体对其个人信息的超强控制力。〔39〕但在 GDPR 尚未生效执行的 2017 年，欧盟第 108 号公约协商委员会就出台了《大数据社会个人数据处理中的个人保护指南》。〔40〕其中指出，“大数据应用的复杂性和模糊性应该促使规则制定者不再将控制概念局限于个人控制（个人信息）。他们应该（将控制个人信息概念）理解为更广义的控制个人信息使用”〔41〕。显然欧盟欲澄清，信息主体同意对其个人信息的控制范围远不及研究者所言之广泛。

因此，为尊重陌生人社会个人隐匿身份的自由，尊重信息主体对处理风险的决策，信息主体同意适用于单独识别个人信息。

四、同意规则不适用于结合识别个人信息

基于尊重信息主体对处理风险的决策，以及尊重陌生人社会个人隐匿身份的自由，可以得出同意适用于单独识别个人信息的结论。基于此二者，同样能够从反面佐证同意不适用于结合识别个人信息。不仅如此，本部分另从避免《个人信息保护法》两套识别标准的“基因缺陷”、避免同意规则与不需告知规则衔接不畅，以及避免“促进个人信息合理利用”的立法目的不达三个角度证明，同意规则不适用于结合识别个人信息。

---

〔37〕《统一个人数据保护法》系由美国统一法律委员会制定，于 2021 年 7 月通过的示范法案，拟于 2022 年 1 月前后实施，该法案载于 https://uniformlaws.org/committees/community-home/librarydocuments/viewdocument?DocumentKey=afdb7812-a7c6-4468-92f6-fac09416c0ac。

〔38〕根据 UPDPA 第 7 条第 b 款第 5 项，对于创建假名或匿名化数据具有合理必要性的处理行为，是兼容的数据处理行为。根据 UPDPA 第 7 条第 a 款第 1 句，控制者或处理者可以在未经数据主体同意的情况下从事兼容的数据处理行为。因此，根据 UPDPA 第 7 条第 b 款第 5 项结合同条第 a 款第 1 句，对于创建假名或匿名化数据具有合理必要性的处理行为，不需要取得数据主体的同意。以举重以明轻的法学原理对该项规定深入研究可得出以下结论：创建假名化数据的行为针对的是能单独、直接识别数据主体的个人数据，该行为尚且不需要取得数据主体的同意，则假名化完成后的数据不能单独、直接识别数据主体，对该类数据的处理行为更不需要获得数据主体的同意。UPDPA 中的假名化数据为去除直接标识符的个人数据，大致相当于本文所指“结合识别个人信息”。

〔39〕参见王成：《个人信息民法保护的模式选择》，载《中国社会科学》2019 年第 6 期。

〔40〕Guidelines on the Protection of Individuals With Regard to the Processing of Personal Data in a World of Big Data, available at https://ccdcoe.org/uploads/2019/09/CoE-170123_Guidelines-on-protection-of-individuals-with-regard-to-processing-of-personal-data-in-a-world-f-big-data.pd, last visited on Dec. 3, 2021.

〔41〕《大数据社会个人数据处理中的个人保护指南》，李群涛译，高富平校，载 http://www.dataprotection.cn/news/126.html，最后访问时间：2021 年 8 月 30 日。

（一）避免个保法两套识别标准的“基因缺陷”

认定个人信息时，采较为宽松的识别可能性标准，个人信息处理者本身是否具有直接识别能力，在所不问；然而取得同意却恰以个人信息处理者本身具有直接识别能力为前提。两者所持标准差异导致同意规则不能及于全部个人信息，特别是不适用于结合识别个人信息。〔42〕

个人信息认定环节的判断标准是客观识别标准，其要求“个人信息处理者或者其他任何人”有能力根据信息识别信息主体身份，不仅限于个人信息处理者自身有此识别能力。单独识别个人信息是个人信息中最为典型的一类。然而，随着世界各国认识到个人信息处理活动涉及信息主体利益甚巨，出于加强信息主体权益保护目的，个人信息保护法适用范围相应扩张。〔43〕作为个人信息保护法适用门槛，个人信息范围也需随之扩张。于是国际上普遍认可，若个人信息处理者不能通过信息单独识别信息主体，而是结合其他信息可以间接识别，那么该信息（结合识别个人信息）亦属于个人信息。不仅如此，在欧盟 GDPR 影响下，国际社会进一步认同：即使个人信息处理者不能通过信息识别个人，而其他任何人（by another person）具有此种识别能力，那么该信息也属于个人信息。至此，作为个人信息判断重要标准的识别，已经从特定个人信息处理者能够识别，扩张到世界上（至少是个人信息处理者活动范围内）任何其他人能够识别。此观点被欧盟第 29 条工作组严格贯彻，〔44〕欧洲法院也在相应判决中落实这一标准。〔45〕以至于欧洲学者嗟叹，个人信息保护法某种程度上已成为“万物之法”。〔46〕简言之，为了保护个人权益，已经以当前世界上先进识别技术和丰富信息量为标准（客观识别标准）判断特定信息是否为个人信息。

然而就同意规则而言，履行“取得同意”义务必然以主观识别标准——特定个人信息处理者的实际识别能力（甚至是直接识别能力）——为限。取得同意义务是个人信息处理者自身需要履行的义务，依照“法律不强人所难”的基本法理，个人信息处理者履行某义务必然要以有履行此义务的能力为限。个人信息处理者履行取得同意义务要以信息中含有直接标识符为限，此系同意的时间要求所致。按照《个人信息保护法》第 13 条第 1 款第 1 项规定，取得信息主体同意的，个人信息处理者方可处理个人信息。易言之，原则上取得同意应当先于处理行为进行方为合法。而结合其他信息进行间接身份识别也是处理行为，因此，同意也应当先于间接识别行为而进行，否则违法。同意这一时间要求，迫使个人信息处理者在取得同意之前不得以处

〔42〕 See Christopher Kuner, Lee A. Bygrave, Christopher Docksey, *The EU General Data Protection Regulation (GDPR) A Commentary*, Oxford University Press, 2020, p. 395.

〔43〕 两份个人信息保护领域的重要文件引领了对信息主体的强保护，分别是世界经济合作与发展组织发布的《隐私保护与个人数据跨境流通指南》和欧洲理事会发布的《个人数据自动化处理中的个人保护公约》。此二文件成为之后各国立法的重要参照文件。

〔44〕 参见前引〔15〕，Article 29 Data Protection Working Party 文。

〔45〕 See Case T－670/16, Digital Rights Ireland v. European Commission, GC, order of 22 November 2017 (ECLI: EU: T: 2017: 838); Case C－434/16, Peter Nowak v. Data Protection Commissioner, judgment of 20 December 2017 (ECLI: EU: C: 2017: 994); Case C－345/17, Proceedings brought by Sergejs Buivids, judgment of 14 February 2019 (ECLI: EU: C: 2019: 122); Case C－40/17, Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV., judgment of 29 July 2019 (ECLI: EU: C: 2019: 629).

〔46〕 参见前引〔16〕，Nadezhda Purtova 文，第 78 页。

理的方式进行识别。因此，同意方面的合规，要求个人信息处理者必须在取得同意之前能单独、直接识别信息主体的身份。个人信息认定环节的客观识别标准与同意规则中的主观识别标准间的差距，使得同意控制范围注定无法及于各类个人信息上的处理行为。有学者将客观标准概括为“识别可能性”（identifiability），而将主观识别标准概括为“识别本身”（identification），并指出同意规则仅关注后者，即识别本身。〔47〕两种识别标准只有在面对单独识别个人信息时才重合。揣测普遍漠视这一差距的原因，或许是个人信息保护制度研究基本以 APP 从信息主体处直接采集个人信息的场景作为典型思考模型。于是，收集、存储、分析个人信息，当然不存在不知信息主体身份的情形。此亦从侧面说明，同意规则适用范围的限缩，往往起因于个人信息处理者非从信息主体处直接收集个人信息情形（即俗称的“个人信息二手利用”）的广泛存在。总之，个人信息的外延比同意规则所能适用的个人信息外延大得多，超出的部分包括特定个人信息处理者能够结合识别出身份的个人信息以及特定个人信息处理者本身不能结合识别出身份的个人信息。

两标准范围的不完全重合，恰恰是由于个人信息认定环节“识别”标准的极大扩张为个人信息保护制度创设的“基因缺陷”。由此观之，对个人信息范围采广义理解的国家，只要其采选进机制（opt-in），即取得同意应先于处理行为进行，则其个人信息保护体系中的同意规则亦需限缩于单独识别个人信息。欧盟发现了这一基因缺陷，并通过设置 GDPR 第 11 条试图进行解决。根据该条，个人信息处理者〔48〕有时不必仅为了合规而获取信息主体同意。也正因如此，欧洲学者赞扬 GDPR 第 11 条称，该条“弥合了（至少是试图弥合）由个人信息概念引发的鸿沟”〔49〕。

（二）避免同意规则与不需告知规则衔接不畅

同意不适用于结合识别个人信息，即要求针对结合识别个人信息建立“不需同意”制度。此系对《个人信息保护法》“不需告知”制度的必要呼应。

《个人信息保护法》设立了不需告知规则。《个人信息保护法》第 18 条第 1 款为“不需告知”制度提供了依据。“不需告知”制度主要适用于三种情形：第一，信息主体已经知情，不再需要告知；第二，已经公开的个人信息，不再需要告知；〔50〕第三，当个人信息处理者客观不识别身份或基于合规要求不被允许识别身份时，基于法律不强人所难的基本法理，也应当作为前述不需要告知情形之一。GDPR 有类似制度，其第 13、14 条分别针对从信息主体处收集个人信息、非从信息主体处收集个人信息两种情形规定了告知义务的例外情形。尤其是第 14 条第 5 款 b 项提出，个人信息处理者提供相应信息被证明是不可能或者需要投入过多不必要精力时，个人信息处理者不需要告知。不过，GDPR 亦非完美：根据 GDPR 第 11 条第 2 款，当个人信息处理者的处

〔47〕 参见前引〔42〕，Christopher Kuner 等书，第 395 页。

〔48〕 GDPR 与我国《个人信息保护法》在术语使用上略有不同。GDPR 的数据控制者对应我国的个人信息处理者。GDPR 的数据主体，对应我国的个人，即本文所谓信息主体。术语上的不统一将导致文本阅读上的障碍，为避免这一问题，本文在介绍 GDPR 条文时一律使用我国的术语。

〔49〕 前引〔42〕，Christopher Kuner 等书，第 395 页。

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

理目的不要求识别信息主体身份，且个人信息处理者能够证明自己无法识别信息主体时，如果个人信息处理者可以（if possible），则需要履行告知义务。然而当个人信息处理者不能识别信息主体时，个人信息处理者如何能够履行告知义务。于是，欧洲学者亦无奈表示，只能依赖“如果可能的话”（if possible）这一条件弥补第 11 条第 2 款的缺憾。〔51〕换言之，一般宜认为此种情况下告知义务无履行可能。

因为告知是取得同意的前提和要求，所以不需告知规则应配以不需同意制度。按照《个人信息保护法》第 14 条第 1 款第 1 句，同意应当在信息主体充分知情的前提下作出。但当信息主体不知情时（此为常态），个人信息处理者必然需通过告知使其充分知情。是故，在逻辑上告知、知情、同意依次发生，通常情况下告知是同意的逻辑前提。“告知同意”或者“知情同意”这一学界和实务界通用且公认的提法事实上已经表明告知是同意的逻辑前提。〔52〕既然如此，那么由于客观或者合规等原因不能告知信息主体时，当然也就无法取得信息主体的同意。这就要求《个人信息保护法》有对应不需告知规则的不需同意制度。

然而《个人信息保护法》没有同步设计不需同意制度。我国虽然设计了不需告知规则，但显然同意规则与此不相适应，因为按照第 13 条规定的文义，当无其他合法性基础时，各类个人信息的处理都需要以获得信息主体同意为前提，其他因素在所不问（此亦为本文引言中“全部个人信息说”的依据）。从全国人大相关机构在立法过程中形成的一系列有关欧盟个人信息保护制度和美国隐私保护制度的研究材料，以及《个人信息保护法》众多条文的表述观之，我国《个人信息保护法》立法明显有参考 GDPR 的现象。然而仅就告知同意规则来看，我国并未做到全面、完整、正确地进行制度参考。上文已经提及，我国不需告知规则学习了 GDPR 第 13、14 条，但对应此种情形，GDPR 配套设置了第 11 条第 1 款不需同意规则，即如果个人信息处理者处理个人信息的目的不要求或不再要求识别信息主体身份，则不应强制个人信息处理者仅为合规而保留、获取或处理额外信息以识别信息主体身份。言下之意，当个人信息处理者不需识别身份时，其处理不需要取得同意。但是我国只吸收了不需告知规则，没有同步建立作为其逻辑后果的不需同意制度。

当然，GDPR 第 11 条第 1 款并非我国不需同意制度的最佳选择。相反，GDPR 第 11 条第 1 款本身存在严重的逻辑漏洞，此处简要分析。根据欧盟 GDPR 第 11 条第 1 款可推知，若处理之目的不要求识别信息主体身份，则以识别身份为前提的同意也不需要获得。简言之，根据该条，是否要求获得同意系以“是否需要识别身份”为根本判断标准。需要识别信息主体身份，则需要获得同意，反之则不需要。看似周延的结论掩盖了逻辑上的漏洞，此处逻辑上的漏洞主要是指遗漏考虑一种情形，即处理结合识别个人信息（即不含直接标识符的个人信息）且处理目的要求识别信息主体身份。根据 GDPR 第 11 条第 1 款，此种情形，由于“需要识别”所以需要获得同意。

〔51〕 参见前引〔42〕，Christopher Kuner 等书，第 396 页。

〔52〕 参见前引〔17〕，范为文；叶名怡：《论个人信息权的基本范畴》，载《清华法学》2018 年第 5 期；前引〔22〕，田野文；王利明：《数据共享与个人信息保护》，载《现代法学》2019 年第 1 期；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 年第 6 期；万方：《隐私政策中的告知同意原则及其异化》，载《法律科学（西北政法大学学报）》2019 年第 2 期；吕炳斌：《个人信息保护的“同意”困境及其出路》，载《法商研究》2021 年第 2 期。

然而只有通过“识别身份”这一处理行为识别出信息主体身份才能得到其同意，而同意只能为同意之后的处理行为提供合法性基础，不能为同意之前的识别身份行为及其之前行为提供合法性基础。因此笔者指出的这种情况，根据 GDPR 第 11 条第 1 款，识别出身份之前阶段的处理行为必然将因无合法性基础而违法。法律不强人所难，所以识别身份及其之前的行为也不应当要求获得个人同意。因此，GDPR 以“是否需要识别”作为划分同意适用边界的标准并不合理，应当以是否含有直接标识符（无需进行处理即可识别身份）作为划分标准。我国没有移植 GDPR 第 11 条第 1 款，一定意义上避免了陷入前述逻辑漏洞，但这不能表明我国不应该设立不需同意制度。

于是，我国应建立的不需同意制度，不能盲目追随 GDPR，而是应基于《个人信息保护法》条文，在解释上将单独识别个人信息作为同意规则的适用范围，而将结合识别个人信息排除于同意规则适用范围之外。如前所述，我国应当存在不需同意制度。但显然，我国法缺失这一制度，导致同意规则与告知规则衔接不畅。而《个人信息保护法》生效后，必须从解释论层面寻找新出路。此即需在现行法框架下基于解释论提出具有相同功能的替代方案。而本文所提出的同意适用边界限缩恰恰是解释论下的一种有效解决方案。同意适用边界限于单独识别个人信息，并非意味着结合识别个人信息将不受控制，只是说明结合识别个人信息将不受信息主体的事前控制。但基于法律规定产生的个人信息处理者义务仍然继续适用，《个人信息保护法》规定的事前个人信息保护影响评估等措施仍然应当落实，以保护信息主体权益。并且，此时应当对个人信息处理者课以更高要求。〔53〕

（三）避免个人信息流通利用的立法目的不达

确认结合识别个人信息的处理不需要同意，恰恰能激励个人信息处理者将个人信息处理活动维持于低风险状态。个人信息保护的本意是平衡个人信息处理利用与个人信息处理利用过程中信息主体权益维护。当个人信息已经为结合识别个人信息时，已经使个人信息处理活动处于低风险水平。如果仍然认为结合识别个人信息之处理亦须取得信息主体的同意，那么必然以重新识别信息主体身份为前提，则反而因为合规要求使得个人信息重新被暴露于高风险环境。〔54〕最终与个人信息保护法立法目的相悖。正是因为单独识别个人信息与结合识别个人信息的风险水平有异，所以对两者不应采相同保护水平。结合识别个人信息之处理不需要个人同意，是对此类信息处理的制度激励，有利于鼓励个人信息处理者积极主动地对个人信息进行去标识化处理。事实上，《个人信息保护法》本身也将去标识化作为安全技术措施（第 51 条第 3 项）。

《个人信息保护法》的重要目的之一在于“促进个人信息合理利用”。信息是自由的，个人信息亦未完全脱离自由的本质，只是因为个人信息以个人为主题，所以属于特殊信息类型，需要一定程度的特殊对待。而结合识别个人信息，多属于用以分析个性特征的信息，这些信息只

〔53〕 参见前引〔42〕，Christopher Kuner 等书，第 447 页。

〔54〕 See Paul M. Schwartz，Daniel J. Solove，The PII Problem：Privacy and a New Concept of Personally Identifiable Information，86 *New York University Law Review*，1814（2011）.

有与特定个人身份关联起来，可以直接通过该信息识别信息主体身份时，才涉及隐私等人格利益问题，这意味着鼓励在不危及信息主体权益情形下对结合识别个人信息进行分析利用。当然，若导致不利后果，那么可以通过民事侵权救济而非事前控制机制，保证信息主体权益得到保护。现行法已经建立起这样的事后救济机制。当信息主体权益遭受侵害或有受侵害之虞但尚未造成损害时，《民法典》第 1037 条等已经提供了各类防御性人格权益请求权。〔55〕当信息主体权益遭受侵害并造成损害时，《个人信息保护法》第 69 条第 1 款确立了专门的损害赔偿制度。

不过，需要强调，结合识别个人信息与单独识别个人信息可能互相转换，一旦结合识别个人信息转化为单独识别个人信息，则又需要适用同意规则。处理结合识别个人信息不必获得同意，甚至连分析行为也不必获得同意。但是一旦通过处理行为识别到信息主体身份，结合识别个人信息瞬间转换为单独识别个人信息，于是应当立即寻求信息主体的同意。此时一旦同意没有取得，那么根据《个人信息保护法》第 47 条第 1 款，个人信息处理者应当删除所涉个人信息。某种意义上，结合识别个人信息转换为单独识别个人信息的时刻，很可能是个人信息处理者删除个人信息的时刻。

五、结　语

“保护个人信息权益”与“促进个人信息合理利用”是《个人信息保护法》第 1 条确立的同等重要的立法目的。该法给法律解释适用者提出的艰巨任务是实现两个目的的和谐与平衡。然而，若认为缺失《个人信息保护法》第 13 条第 1 款第 2 至 7 项的合法性基础时，对各类个人信息的处理都要经过同意，那么天平上的砝码已经过于向保护个人信息权益一侧倾斜。划定同意规则的适用范围正是“瞻前顾后”地通盘考虑两种目标的平衡之后在同意规则上的体现。本文主张信息主体的同意只能适用于对单独识别个人信息的处理行为。此结论在法律解释上体现为应当对《民法典》第 1035 条第 1 款第 1 项主文中的“自然人”以及《个人信息保护法》第 13 条第 1 款第 1 项中“个人”概念进行限缩，限缩至“个人信息中以直接标识符直接体现其身份的个人”。当然，个人信息处理的合法性须从目的合法、具有合法性基础，以及处理行为规范三个方面综合甄别。本文讨论的同意边界问题仅是合法性基础方面判断的问题，不涉及目的是否合法和处理行为是否规范两方面。

使结合识别个人信息摆脱信息主体同意的控制，也正是在法律上为目前国家提倡的数据流通机制提供法律基础。2020 年 3 月公布的《中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见》提出加快数据要素市场建设，其内含的要求便是为数据流通创造法律上的途径。个人信息是数据中的重要类别，当然应该考虑其流通利用的合法性问题。但目前个人信息流通机制于法律方面的困境在于逐一获取信息主体的同意，合规成本极大。本文试图为结合识别个

〔55〕 参见高富平、李群涛：《个人信息主体权利的性质和行使规范——〈民法典〉第 1037 条的解释论展开》，载《上海政法学院学报（法治论丛）》2020 年第 6 期。

人信息未经信息主体同意而流通利用的可行性提供法理支撑，以便在一定程度上为个人信息的流通利用松绑。

Abstract：In the absence of other legal basis，the key to the applicability of personal information subject's consent lies in whether the personal information contains a direct identifier. The direct identifier can directly represent the identity of the personal information subject，so as to accurately link the information processing risk with the personal identity. In addition，in the stranger society，the choice and freedom of individual hiding identity should be respected. Therefore，the direct identifier representing identity information should be controlled by the personal information subject，that is，applicable boundary of personal information subject's consent is individually identifiable personal information. However，consent does not apply to personal information without direct identifier. Firstly，as the fuzziness of this kind of personal information，it is difficult for personal information processors to directly identify the subject of personal information and ask for consent. Secondly，logically，the non disclosure system established by the personal information protection law needs the non consent system. Finally，the non application of consent system is also the important way to achieve the legislative purpose of personal information circulation and utilization.

Key Words：individually identifiable personal information，personal information without direct identifier，agree，direct identifier，personal information protection law

（责任编辑：武　腾　赵建蕊）

财经法学 No. 2，2022
pp. 54 - 68

数字防疫中个人信息治理的“链”“法”协同机制研究

胡元聪　龚家锋*

内容提要：在本次疫情防控中，人工智能、大数据等数字技术在降低疫情传播风险的同时使个人信息治理面临新的风险。联盟链近年来在诸多领域得到广泛应用，成为化解数字防疫中个人信息治理风险的可行工具。但在应用联盟链治理风险的同时，还需要对相应制度予以优化，从而在技术迭代与制度优化的作用下实现联盟链与法律的“携手共治”。对此，应当消除联盟链与法律之间的张力，进而构建以法律治理为主、以联盟链治理为辅的“链”“法”协同机制。具体而言，通过构建与法律相匹配的联盟链治理机制及与联盟链相适应的法律治理机制，融合区块链技术和法律各自的优势，以此来提升“链”“法”协同机制在数字防疫中个人信息治理方面的能力，从而提高国家治理现代化水平。

关键词：数字防疫　个人信息治理　风险治理　联盟链　“链”“法”协同

一、研究背景与问题的提出

新型冠状病毒肺炎疫情（以下简称“疫情”）自暴发以来，即在全球迅速蔓延。预计到世界范围内的新冠肺炎疫苗普遍接种前，我国仍将长期处于“外防输入，内防扩散”的常态化疫情防控中。与之前历次突发重大公共卫生事件相比，本次疫情防控的最大特点是“将云计算、大数据、人工智能等新兴技术应用于疫情监测分析、人员流动和社区管理等联防联控的各个方面”〔1〕进

* 胡元聪，西南政法大学经济法学院教授、西南政法大学中国市场经济法治研究中心主任；龚家锋，西南政法大学人工智能法律研究院助理研究员。

本文为国家社科基金重点项目“人工智能研发与应用风险治理的财税法协同机制研究”（21AFX021）、重庆市研究生科研创新项目“疫情防控中个人信息保护的区块链技术进路研究”（CYS20152）的阶段性成果。

〔1〕《工业和信息化部办公厅关于运用新一代信息技术支撑服务数字防疫和复工复产工作的通知》，载 http://www.gov.cn/zhengce/zhengceku/2020-02/19/content_5480843.htm，最后访问时间：2021年1月17日。

行数字防疫。〔2〕但数字技术的不确定性和规制数字技术制度的不确定性导致疫情防控“危”“机”并存：通过对公民个人信息〔3〕的治理〔4〕进行数字防疫，一方面有效地降低了疫情传播风险，另一方面却使公民个人信息面临治理风险。易言之，数字技术为降低疫情传播风险而应用，但数字技术的应用又使个人信息治理产生了新的风险。如何消除数字防疫和个人信息治理之间的冲突龃龉问题以化解个人信息治理之“危”进而利用数字进行防疫之“机”，是数字防疫亟须解决的问题。

具体来讲，随着数字技术的不断应用，越来越多的部门开始大规模搜集和使用个人信息进行分析，与此同时，一些“不当利用个人信息的侵权行为愈发普遍”〔5〕。部分防疫部门实行“地毯式”搜查却可能疏于管理，一些有关疫情的图片、视频和数据等充斥于社交平台，部分确诊或疑似患者的个人信息在网络上广泛流传。在各地推出健康码、行程卡等应用程序和基层登记办法后，大量个人信息既留存于网页、应用程序等数字代码中，也广泛暴露在商超、银行等公共场所入口的纸质登记簿上。这使得为数字防疫而搜集的个人信息产生了治理风险。不同于传统商业领域的个人信息侵害行为，数字防疫搜集的个人信息搜集面广、覆盖人群多。不当利用行为不仅“侵犯了公民的个人隐私权益，可能成为下游犯罪的预备条件”〔6〕，而且增添社会恐慌情绪，给数字防疫增加阻力，甚至“可能危害国家政治安全与社会安全”〔7〕。

区块链技术具有去中心化、可溯源的特点，经过数年的研发创新，已针对不同的应用领域衍化出公有链、联盟链等多种类型。其在业界担忧的去中心化、总量、算力、跨链方面不断改进，〔8〕可能在全球范围内引起新的技术和产业变革〔9〕。我国已逐渐成为区块链技术大国，区块链专利数量位居世界前列。联盟链成为我国区块链技术应用的趋势，其在金融、政府治理、产品溯源等方面多有实践。习近平总书记强调，要发挥区块链技术在促进信息共享、提升协同效率等方面的作用，推进区块链和经济社会融合发展。〔10〕我国《“十四五”规划和2035年远景目标纲要》也提出要以联盟链为重点发展区块链服务平台和应用方案。具体在数字防疫的个人信息治理方面，联盟链在疫情防控和个人信息治理中均已有相关应用：如济南的“区块链＋疫情防控”〔11〕系统、

〔2〕本文所称“数字防疫”是云计算防疫、大数据防疫和人工智能防疫的总称。

〔3〕本文所称“个人信息”是指《中华人民共和国民法典》第1034条规定的个人信息，即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。

〔4〕依照《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）第4条的规定，个人信息的处理包括个人信息的收集、储存、使用、加工、传输、公开等活动。本文所称“个人信息治理”主要是指对个人信息处理行为进行规范的活动。

〔5〕孙莹：《大规模侵害个人信息高额罚款研究》，载《中国法学》2020年第5期，第106页。

〔6〕叶名怡：《个人信息的侵权法保护》，载《法学研究》2018年第4期，第88页。

〔7〕《总体国家安全观视角下个人信息保护机制研究》，载http://www.gjbmj.gov.cn/n1/2020/0509/c411145-31702913.html，最后访问时间：2021年1月19日。

〔8〕参见《利用区块链促进税收管理现代化的研究》课题组、张国钧等：《基于区块链的“互联网＋税务”创新探索——以深圳市税务局的实践为例》，载《税务研究》2019年第1期。

〔9〕参见中国区块链技术和产业发展论坛：《中国区块链技术和应用发展白皮书（2016）》。

〔10〕参见《习近平主持中央政治局第十八次集体学习并讲话》，载http://www.gov.cn/xinwen/2019-10/25/content_5444957.htm，最后访问时间：2021年1月19日。

〔11〕《济南全国首发“区块链＋疫情防控”标准》，载http://www.jinan.gov.cn/art/2020/4/10/art_1861_4197790.html，最后访问时间：2021年1月19日。

广州南沙的“疫情防控协同系统”〔12〕等，积极利用联盟链防控疫情；再如中国人民银行主导的“征信链”，利用联盟链确保包括个人信息在内的信用信息安全并推动信息共享〔13〕。此外，联盟链的技术特征与《个人信息保护法》的“信息保护义务”以及数字防疫中政府部门居中管理调度的要求相契合。基于此，本文拟探讨以下四方面的问题：数字防疫对个人信息治理产生了哪些风险，联盟链能否成为化解这些风险的工具，如何处理联盟链和法律在数字防疫中个人信息治理的关系，怎样构建全方位的数字防疫中个人信息治理“链”“法”协同机制。

二、数字防疫中个人信息治理面临的风险

在本次疫情防控中，大数据、人工智能等数字技术筑起了一道道防疫“数字长城”。但受技术特性和应用实践的限制，数字技术给个人信息治理带来了技术风险和制度风险。具体表现在以下三个维度：

（一）个人信息数量激增，挑战防控信息真实性

在本次疫情防控中，政府利用电信企业的通信信息配合其他实名制信息建立了健康码、行程卡等防疫工具。这些工具可以动态跟踪人员流向，从而有效降低疫情传播风险。与此同时，需要处理的个人信息迎来“数据核爆”。以北京“健康宝”为例，其以个人信息和通信信息为基础，出入公共场所必须校验个人“健康宝”信息。这一特殊工具为有效防控疫情、排查人员流向发挥了巨大作用，同时在短时间内产生了海量信息。其自上线以来，使用人数和查询次数激增，后台所需存储的对应信息量持续增高。截至 2021 年 8 月 13 日，其累计查询、使用次数达 79 亿次。〔14〕信息的真实性是数字防疫中个人信息治理的前提。如果不能及时处理激增的个人信息，便会出现挑战防控信息真实性的风险，从而动摇防控信息的真实性基础。“个人信息是大数据和人工智能的原料。”〔15〕激增的海量个人信息具有多样性、价值性和快速性的特点，这就要求防疫部门具备高水平的信息治理能力，以保障数字防疫基础信息的真实性。这对于习惯传统治理模式的各级防疫部门而言可能是一个不小的挑战。部分防疫部门因为防控压力激增，忙于落实防控要求，可能来不及处理激增的海量涉疫信息，进而会影响到防控信息的真实性。同时，个别防疫部门出于政绩考虑或防控压力，主观上可能有漏报、瞒报行为，或者选择性收集对自己有利的信息，这也容易挑战防控信息真实性进而影响到数字防疫的准确性。

（二）个人信息安全危殆，影响防控信息公信力

个人信息安全受到威胁的主要原因在于第三方的处理：若信息只在两个主体间传输，二者对信息的加工、处理涉及的安全问题通常有相关的合意，此时一般不易出现安全风险。但如果不能

〔12〕《打通防疫“数据烟囱”，广州南沙防疫信息化系统上线》，载 http://zfsg.gd.gov.cn/xxfb/dsdt/content/post_2883625.html，最后访问时间：2021 年 1 月 19 日。

〔13〕参见《科技赋能金融，“链”上无限可能》，载 https://www.thepaper.cn/newsDetail_forward_14441734，最后访问时间：2021 年 10 月 10 日。

〔14〕参见《北京市新型冠状病毒肺炎疫情防控工作新闻发布会（第 240 场）》，载 http://www.beijing.gov.cn/shipin/Interviewlive/514.html，最后访问时间：2021 年 11 月 7 日。

〔15〕王成：《个人信息民法保护的模式选择》，载《中国社会科学》2019 年第 6 期，第 125 页。

在涉及第三方处理时实现可溯源，信息就容易被进一步转手并泄露。如在数字防疫中，个人信息往往辗转于多个防控主体之手。频繁的转移为恶意攻击提供了难得的机会，〔16〕出现安全风险在所难免。同时，数字防疫搜集的海量个人信息储存在传统中心化服务器中，通过开放的互联网传输和整合。信息可能没有时间标识，复制成本低，存在较大的泄漏及篡改风险。而常规信息加密方法只能在一定程度上缓解安全风险，并不能彻底防范外部攻击，无法根本解决个人信息的安全问题。信息的安全性及公信力是数字防疫中个人信息治理的根基。如果不能保证数字防疫中个人信息安全，便会出现影响防控信息公信力的风险，进而可能影响到数字防疫的权威。涉疫个人信息一旦被泄漏或篡改，配合防疫的公民隐私便暴露在公众的视线下，将使公民承受巨大的心理和舆论压力。这将影响公民填报信息的积极性并降低其对防控的信任度，进而影响到防控的效率、精度以及防控信息的公信力。以北京“健康宝”为例，其由公权力机关负责运营并受到多重技术保护和严格监管，却也出现了个人信息泄露事件：不法分子在网络上低价售卖大量明星的“健康宝”照片、身份证号码、核酸检测结果等相关个人信息。〔17〕不同于涉疫信息表格、截图、流调报告等泄露事件，该事件源自公共防疫应用程序。即使事故由技术服务商的程序漏洞而非政府的原因引起，也可能使防控信息的公信力受损。

（三）个人信息孤岛阻隔，降低防控信息共享度

“信息孤岛”是指信息被不同的主体储存，因储存、传输标准不统一或缺乏交流渠道等原因成为相互独立的数据集，而无法分享、整合的情形。在数字防疫中，个人信息控制主体众多，仅笔者就接触到三类：其一是基于法律法规授权的主体，如政府、医院等；其二是基于日常业务而成为信息控制者的主体，如电信企业、航空公司等；其三是处于模糊地带的主体，如商场、银行等需要统计人员流向的公共场所。每个信息控制主体都有各自的信息管理系统，信息控制主体之间相互独立，无法共享各自控制的信息。虽然近年来各界对破解“信息孤岛”提出了诸多观点并付诸实践，但受硬件设备和沟通渠道的限制，数字防疫中的“信息孤岛”现象仍然存在。信息的共享度是数字防疫中个人信息治理效率的衡量标准之一。如果不能解决“信息孤岛”问题，便会出现降低防控信息共享度的风险，从而降低防疫协同效率。个人信息控制主体本应相互配合，实现多向信息共享，减少不必要的重复步骤以提升效率。但实践中部分防疫部门仍在一定程度上各自为政，一些信息可能没有及时共享。以 2021 年春节地方政府为落实“就地过年”而排查外地返乡人员为例，部分相同的个人信息因缺乏共享而被多次重复统计。〔18〕在冬季部分地区疫情发散的背景下，各地面临严峻的防控形势。多次重复统计个人信息符合防控形势需要。但相同的个人信息因缺乏共享而被不同的防疫部门多次重复统计，一定程度上提高了防控成本并降低了防控效率。如果防疫部门之间加强信息共享，减少不必要的重复步骤，起码不再要求已经排查过的人员重复填报其他部门已经登记过的信息，则可以在一定程度上加快排查速度，提高信息的利用

〔16〕 参见邢会强：《论数据可携权在我国的引入——以开放银行为视角》，载《政法论丛》2020 年第 2 期。

〔17〕 参见《多名艺人“健康宝照片”遭泄露》，载 https://mp.weixin.qq.com/s/D198CIQsh_R5jaNdFiXeJQ，最后访问时间：2021 年 1 月 19 日。

〔18〕 仅笔者春节返乡就接触到五次统计，其中部分统计内容相同：其一是公民主动上报及相互检举；其二是社区等基层人员逐户排查上报；其三是教育部门统计学生返乡信息；其四是公安部门利用交通实名信息统计；其五是电信、互联网公司等对其用户流向进行分析。

效率。

三、数字防疫中联盟链应用于个人信息治理的可能性

个人信息的处理是数字防疫的必然要求，但数字防疫又给个人信息治理带来了新的风险。联盟链可以为数字防疫中的个人信息治理提供新的思路。联盟链存在多个中心，由多主体共同运行，〔19〕强调效率与秩序的共存〔20〕。联盟链是在克服传统区块链弊端的基础上发展而成的新形态：其不需要引入算力竞争确定写入权，可以节省计算资源和耗能；其节点数量和区块信息存量较少，有效地提高了数据吞吐能力、系统运行速度，并相应扩展了储存空间；多中心化的特征使其更容易完成特定的任务和目标，有利于提升系统的可控性并实现规范、良性监管。联盟链融合了业务去中心化和管理中心化的双重特点，〔21〕既可以解决信息不对称和隐私保护问题，又便于政府实现特定政策目标。因此，联盟链更适合在由政府主导的场景中应用，是各国政府普遍接受的区块链模式。具体在数字防疫的个人信息治理中，联盟链能够缓解当前数字防疫给个人信息治理带来的风险，且符合我国区块链政策推广和疫情防控的要求。因此，可以利用联盟链缓解数字防疫与个人信息治理之间的冲突龃龉问题。

（一）联盟链可以确保信息真实，创建防控优良信息基础

一方面，联盟链可以激励相关主体提供真实信息。“区块链技术创设的激励机制类似于制度机制，是区块链技术的核心机制之一。”〔22〕联盟链属于“无币区块链”〔23〕，一般不涉及节点争夺记账权问题，但也可根据实际需要设置激励层用来部署激励机制〔24〕。对于个人信息的真实性问题，联盟链可以以积分的方式激励防疫主体上传真实信息并激励有权限的部门积极验证信息的真实性。积分可以用于享有获取信息时的优先权或读取其他地域、部门信息的权限等。链上信息的真实性受到上传和验证的双重激励保证，虚假信息在上传或验证的过程中会被淘汰而不会被记录在系统中，从而保障信息的真实性以创建防控优良信息基础。

另一方面，联盟链可以保证信息真实不被篡改。联盟链具有区块链技术的基本链式结构，能够让链上信息一经储存就无法篡改。〔25〕联盟链系统中的每个区块都包含相连区块的哈希值并相互对应，其中任何一个数值的改变都会导致该区块无法与相邻区块对应，进而不被系统承认。因主观原因上传的虚假信息将永久保存至系统中，无法通过先上传后篡改的方式瞒报、漏报。信息的上传和使用数据同样被记录至系统中。一旦发现不实信息，可以通过系统溯源定位责任主体和使用主体，以尽可能减少损失。对于误记、错记信息的更正和变动，如核酸检测结果变化等，可以通过

〔19〕 参见卜学民：《区块链下证券结算的变革、应用与法律回应》，载《财经法学》2019 年第 3 期。

〔20〕 参见高奇琦：《智能革命与国家治理现代化初探》，载《中国社会科学》2020 年第 7 期。

〔21〕 参见马理、朱硕：《区块链技术在支付结算领域的应用与风险》，载《金融评论》2018 年第 4 期。

〔22〕 胡元聪：《正外部性的经济法激励机制研究》，人民出版社 2021 年版，第 15 页。

〔23〕 邓建鹏：《区块链的规范监管：困境和出路》，载《财经法学》2019 年第 3 期，第 36 页。

〔24〕 参见张楠迪扬：《区块链政务服务：技术赋能与行政权力重构》，载《中国行政管理》2020 年第 1 期。

〔25〕 参见徐琳、袁光：《区块链：大数据时代破解政府治理数字难题之有效工具》，载《上海大学学报（社会科学版）》2020 年第 2 期。

覆盖原有信息以完成，但原有信息不能被删除。此外，“联盟链上的节点采用了实名制的方式”〔26〕，身份相对透明。如果某一节点尝试篡改链上信息，破坏诚信的成本高昂也会使其有所忌惮。

（二）联盟链能够保障信息安全，增强防控信息公信力

一方面，联盟链可以保障信息系统内部安全。优化加密技术是个人信息和隐私保护领域的常用方案。而联盟链的非对称加密技术可以保障联盟链系统内部的信息使用和传输安全。在非对称加密技术的支持下，联盟链上的节点在其权限范围内读写信息。虽然各节点均储存全量账本，但在被系统授权之前，并不意味着该节点自动具备阅读全部账本的权限。这刚好契合防疫部门拥有的信息处理权限差异，即不同节点拥有不同的读写权限。如图 1 所示，可以通过哈希算法将防疫主体 A 上传的个人信息去标识化处理后储存，并借助非对称加密技术对读写权限进行限制，即权限不同的防疫主体对去标识化信息复原程度不同。防疫主体 B 根据其权限对信息复原后使用。这种根据权限非对称加密的有限共享方式，可以有效防控个人信息被泄漏的风险。这就确保了个人信息不会从系统内部泄漏从而增强防控信息公信力。

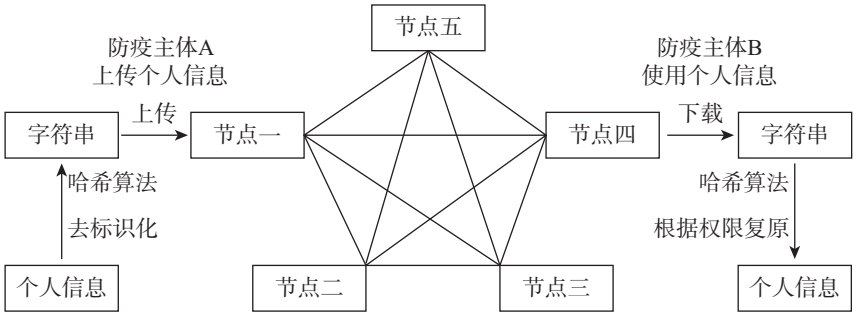

图 1　联盟链去标识化、复原个人信息示意图

另一方面，联盟链可以保证信息系统外部安全。哈希算法可以将储存的个人信息转化为无法破解的 256 位字符串。同时，系统仅保存由算法随机计算得来的字符串，系统外的其他主体无法获得系统内储存的字符串。而系统内的链上节点（即防疫主体）则可以通过匹配私钥和公钥的方式获取个人信息。即使系统因后门漏洞或外部攻击等原因泄露了字符串，也会因为私钥与公钥不匹配、没有签名等原因无法破解其代表的个人信息，不法分子也难以将有限的字符串用于其他用途。此外，联盟链的节点更容易达成新共识，便于进行系统的维护与升级，其算法、协议和加密技术都可以通过中心节点进行更新和审查，相较于其他区块链系统更利于抵抗黑客的外部攻击。〔27〕

（三）联盟链可以促进信息共享，提升防控合作协同效率

一方面，联盟链可以破解信息共享壁垒。联盟链的分布式记账本实质上是一种在节点之间共享、复制和同步的数据库，可以破解信息壁垒，〔28〕进而提高防控合作协同程度及信息治理效率。

〔26〕 翟晨曦、徐伟等：《区块链在我国证券市场的应用与监管研究》，载《金融监管研究》2018 年第 7 期，第 35 页。

〔27〕 参见王延川：《“除魅”区块链：去中心化、新中心化与再中心化》，载《西安交通大学学报（社会科学版）》2020 年第 3 期。

〔28〕 参见胡元聪、谢凤：《智慧司法下数据保护困境突破的区块链技术进路》，载《科技与法律（中英文）》2021 年第 6 期。

通过分布式记账本，防疫主体储存的信息、上传使用记录等储存在系统的每一个节点上。每个节点都是一个信息单元，系统储存的信息在每个单元上记录并共享。只要信息发生变动，就会自动同步记录至所有节点，其他节点则可以根据权限实时读取。同时联盟链只针对特定成员开放，成员需经准入才可参与。这就要求各节点统一信息的上传、储存和传输标准，否则便不能加入系统。这种准入机制一定程度上提高了系统交易性能，可以避免因成员的参差不齐而产生新问题，也在一定程度上缓解了信息不对称问题。〔29〕由此实现链上主体间的信息共享，有效打破“信息孤岛”以提升防控合作协同效率。

另一方面，联盟链可以提高信息共享程度。“代码即信任，是区块链技术的精髓。”〔30〕区块链技术通过算法加持信任以创造良性的去信任化环境，〔31〕利用计算机程序构建新型信任关系，实现点对点交流。联盟链中的节点均通过一定程序获得入链许可和准入，节点所代表的防疫主体资格有一定的保障。且上链信息已经过验证，原本并无合作关系、互不认识的防疫主体之间也无须担心信息的真实性与来源的可靠性，无须经过第三方认证或公证便可直接获取并使用。由此提升了防疫主体的信息共享程度进而提升防控合作效率。此外，可以通过智能合约技术确定信息共享程序，明确防疫主体获取信息的条件以及紧急情况下临时读取信息的处理规则，用代码的方式规范信息共享程序进而提高防控合作协同效率。

联盟链对于化解数字防疫给个人信息治理带来的风险具有天然的优势，在本次数字防疫中也已有相关实践。如广州市南沙区基于“南沙城市大脑”建立了“疫情防控协同系统”，将公安部门、卫生部门、工信部门加入联盟链中。通过联盟链汇总整合了涉疫人员相关个人信息、物资信息等防疫信息，在确保信息真实性、安全性的同时打通了各部门的“信息壁垒”。该系统利用联盟链的不可篡改特征实现企业登记备案的防疫信息不可篡改，保证了信息治理的真实性基础；利用非对称加密机制和哈希算法保障防控重点区域人员涉疫信息安全，提升了防控信息公信力；利用分布式记账本等实现区域内各部门的相关信息实时共享，提高了信息治理效率；利用智能合约技术为相关企业疫情防控承诺提高可信度。“南沙疫情防控协同系统”利用联盟链构建了传播过程不可逆、可有效溯源追踪且有约束力的信息治理系统，为数字防疫中个人信息的治理联盟链的应用提供了一定的经验。

四、数字防疫中“链”“法”协同机制的理论基础

联盟链因其特殊的技术架构对于化解数字防疫给个人信息治理带来的风险具有积极作用，但联盟链的技术特征与传统法律模式也存在天然的矛盾。联盟链虽然经过多中心化改造，对于政府实现特定政策目标和监管具有积极意义，但联盟链毕竟采用了区块链技术的基本架构，其应用将导致传统技术逻辑和业务逻辑发生较大变化，使传统法律法规的适用产生新问题。因此，应当妥善处理二者之间的关系。下面将对区块链技术与法律，即“链”“法”的关系模式进行分析，以

〔29〕 参见张礼卿、吴桐：《区块链在金融领域的应用：理论依据、现实困境与破解策略》，载《改革》2019 年第 12 期。
〔30〕 任仲平：《区块链领导干部读本》，人民日报出版社 2018 年版，第 10 页。
〔31〕 参见赵增奎：《以区块链技术推动互联网金融稳健发展研究》，载《经济纵横》2017 年第 11 期。

求得在数字防疫的个人信息治理中，联盟链与法律之间的最优“相处模式”，通过消除联盟链和法律之间的张力，使二者相互“磨合”，构建“链”“法”协同机制以提升其在数字防疫中个人信息治理方面的能力。

（一）“链”“法”的关系模式类型及评析

1.“链”“法”的关系模式类型

自科技革命以来，如何协调法律与新兴技术之间的关系成为人类社会发展面临的重要议题。新兴技术在基因改造、生物克隆、自动驾驶、信息交流等方面带来了空前的福利，也对现有法律产生了严峻的挑战。“技术一旦进入社会领域，必然会被社会制度、社会组织和社会群体的各种利益、诉求和价值判断所塑造和限制。”〔32〕目前，“链”“法”之间的关系主要有三种类型：管制模式、替代模式和互补模式。管制模式表现为国家通过法律对区块链技术进行严格管制，其坚持较为传统与保守的理念。如果区块链技术可以实现特定社会目标，就通过法律对区块链技术进行保护和激励；如果区块链技术不能实现目标，就要通过法律进行压制。〔33〕源于金融危机等历史原因，一些国家对虚拟货币和区块链技术采取非常谨慎的态度，因为担心技术创新和应用会对社会产生负面影响，所以对区块链技术进行严格管制。替代模式与管制模式截然相反，其是处理“链”“法”关系的前卫观点，认为区块链技术可以完全替代法律，即“政府可以利用区块链技术建立自己的规则系统，通过自动执行的代码系统以带来规则执行效果和效率的革命性提升”〔34〕。这种“代码即法律”的观点在国外已有诸多探讨。与前两种模式不同，互补模式介于管制模式和替代模式之间，其认为“链”“法”各有优势，应当发挥二者各自优势从而构建“链”“法”的共同应用模式。即应当在现有法律制度较为完备的情况下，应将区块链技术作为技术手段，补充现有法律以提高效率并降低交易成本。如“区块链＋发票”，通过应用区块链技术加强税收征管，促进了税收管理制度的完善。

2.“链”“法”的关系模式评析

管制模式和替代模式都是“链”“法”“分立”并相互“对抗”的结果。在管制模式中，法律占据了上风：面对区块链技术应用带来的挑战，法律拒绝做出大的调整，其强势要求区块链技术为符合社会利益而调整。这种模式可以最大程度上防范风险，对区块链技术应用暴露的安全性问题可以及时制止，但是其也会导致诸多负面影响：一方面简单将法律作为压制技术的工具，既否定了法律独特的治理价值，也破坏了法律实践的自主性及法律自身所具有的教义学结构；另一方面也否定了区块链技术的社会建构价值，最终破坏区块链技术的社会效用。在替代模式中，区块链技术获得了胜利：法律顺应区块链技术的价值进行自我调整和革新。但用区块链技术和代码完全替代法律未免过于极端。区块链技术是近年出现的新型信息技术，在智能合约、自动执行等方面迅猛发展。其作为一种去中心化的、安全的、难以破坏的数据簿，虽有自身的价值，但也有固

〔32〕 郑玉双：《破解技术中立难题——法律与科技之关系的法理学再思》，载《华东政法大学学报》2018 年第 1 期，第 87 页。

〔33〕 参见赵小勇：《法律与技术如何相处：区块链时代犯罪治理模式的双重重构》，载《探索与争鸣》2020 年第 9 期。

〔34〕〔法〕普里马韦拉·德·菲利皮、〔美〕亚伦·赖特：《监管区块链——代码之治》，卫东亮译，中信出版集团 2019 年版，第 211 页。

有的缺陷。用代码完全取代法律规则并不可行，也不合常理。法律作为带有国家意志的强制性社会规范，有其自身的优势并可持续修改完善，仍将长期作为规制社会信任的规则。在互补模式中，区块链技术与法律非但不会相互“对抗”，还可能“携手共进”，呈现相辅相成的关系。易言之，法律展现了对区块链技术的宽容，在现有法律框架内对区块链技术的应用进行回应。事实上，法律和区块链技术各有优势，区块链技术可以利用代码更好地实现事前预防和事中规范，法律凭借其强制力、规范性等可以实施有力的事后追责救济和监管。总之，区块链技术和法律各具优势，可以取长补短，通过区块链技术的应用补充和保障法律的实施。

（二）“链”“法”协同机制的选择原因及思路构想

1.“链”“法”协同机制的选择原因

联盟链对于化解数字防疫给个人信息治理带来的风险具有独特的优势，但是联盟链并不能完全替代法律，因为联盟链同样具有区块链技术自身的局限性。联盟链虽然经过多中心化改造，但同样具备分布式记账本的特征，其诞生之初就可能带有除实现特定目标之外的其他主观目的。〔35〕同时，“代码并不比制度更中立，其也受制于垄断和商业利益”〔36〕。此外，区块链技术虽然建立了特殊的信任系统，但信任系统并非完美无缺：其以现代密码技术为基础，仍存在被攻破的可能性；系统的安全和稳定还在不断地发展和变化之中，选择最优的运营模式还需一定时间；智能合约和其他软件代码一样也存在误差和安全漏洞，加之系统直接运作信息价值或财产权利，智能合约误差和漏洞的存在就显得极其危险；现有智能合约技术距离支撑法律的自动执行还有一定的差距。〔37〕因此，存在的悖论是：区块链技术为降低风险而应用，但区块链技术的应用带来了新的风险，其应用带来的外部性问题仍需要法律进行解决。

在数字防疫中，联盟链也无法全部取代法律在个人信息治理方面的作用。法律规范由人类语言构成，具有灵活性和模糊性，“具备通过不断的调试和进化来妥善处理新生事物的能力”〔38〕，可以适应立法者立法时不能预见到的各种偶然性。联盟链由代码语言构成，具有机械性和确定性，只能适用于可以客观验证并已经在底层代码中预先定义的规则。将人类语言构成的开放式法律转化为代码，容易产生歪曲法律含义的风险。这里存在的悖论是：虽然区块链技术是面向未来的技术，但其也无法适应编写时不可预见的未来。由于代码语言的确定性，用严格和正式语言编写的技术治理规则通常无法适用于处于法律灰色地带的意外案件，也很难提前充分考虑并在基础代码中写入即将出现的所有可能性。在出现更先进的“强人工智能系统”之前，代码对于数字防疫中个人信息治理方面可能出现的不可预见情况缺乏适应和解释能力。此外，法律可以通过强制力处罚公民财产、限制人身自由甚至剥夺公民生命，且有一定程度的纠错可能，而代码却无法承担如此重负：一旦代码误判、错判，当事人就会面临人身和财产被代码自动执行而受到严重侵害并无法纠错的巨大风险。因此，技术的迭代并不能完全代替制度的作用，联盟链也不能完全代替

〔35〕 参见赵蕾、曹建峰：《从“代码即法律”到“法律即代码”——以区块链作为一种互联网监管技术为切入点》，载《科技与法律》2018 年第 5 期。

〔36〕〔英〕罗伯特·赫里安：《批判区块链》，王延川、郭明龙译，上海人民出版社 2019 年版，第 32 页。

〔37〕 参见〔美〕凯文·沃巴赫：《链之以法——区块链值得信任吗?》，林少伟译，上海人民出版社 2019 年版，第 47 页。

〔38〕 殷秋实：《智能汽车的侵权法问题与应对》，载《法律科学（西北政法大学学报）》2018 年第 5 期，第 48 页。

法律。在应用联盟链治理风险的同时还需要对相应制度进行优化，从而在技术迭代与制度优化的作用下实现联盟链与法律的“携手共治”。基于此，我们认为，“技制共治”开辟了提升国家治理能力的新路径。

2.“链”“法”协同机制的思路构想

在数字防疫的个人信息治理中，可以采用互补模式，融合“链”“法”的优势构建协同治理机制。“如果现有法律信任结构仍可以普遍适用，按照现有的法律规则能够进行一定程度上的规制，那么区块链技术应该成为法律的补充和保障，其主要价值在于提升信息记录的效率和安全。”〔39〕管制模式和替代模式都有其不足，二者代表的区块链技术与法律分立的观点会带来各种弊端并增加区块链技术创新和传统法律之间的冲突龃龉问题。此外，联盟链和法律在数字防疫的个人信息治理中均有规范、保护个人信息的功能，只是实施方式和手段有所不同。联盟链通过技术手段，利用代码建立自动执行模式，规范个人信息的储存、利用程序，从技术角度实现对个人信息的技术治理。而法律通过制度手段，利用强制力规范各方权利、义务和责任，从制度角度实现对个人信息的法律治理。技术治理与法律治理尽管在治理逻辑上存在差异，但二者也存在巨大的互补性。正确处理技术治理与法律治理的关系，形成共治结构，是提升我国治理水平和能力的前提。〔40〕基于此，可以采用“链”“法”的互补模式。在数字防疫中，可以利用联盟链和法律各自的优势，采取联盟链和法律协同作用的个人信息综合治理模式，构建以法律为主体、以联盟链为辅助的“链”“法”协同治理机制。

具体而言，在“链”“法”协同治理机制中，联盟链和法律的分工有所不同。一方面，法律是数字防疫中个人信息治理的基础和前提。法律在此主要起到明确联盟链的法律地位和效力、实现追责救济、实现全程动态监管的作用。首先，法律可以明确联盟链在数字防疫中个人信息治理方面的法律地位和效力。法律具有普遍性的特征，可以根据数字技术的特征、个人信息的治理需求及疫情防控形势，明确联盟链的法律地位以及分布式记账本、智能合约等技术的法律效力，做到有法可依。其次，法律可以实现事后的追责与救济。法律具有国家强制力的特点，可以配合联盟链的溯源机制确定相关案件的事实问题，对相关案件起到定分止争的作用，对责任主体和损害主体进行强有力的追责和救济。最后，法律可以实现全程动态监管。法律具有规范性的特点，可以配合联盟链的多中心化特征进行实时监管，转变原有事前准入、事后监督的传统监管模式为实时发现风险、及时处理并加以预防的全程动态监管模式。

另一方面，联盟链是数字防疫中个人信息治理的保障和补充。联盟链在此主要起到降低个人信息治理风险、帮助法律进行追责和监管、一定程度上替代规则的作用。首先，联盟链可以降低数字技术对个人信息治理产生的风险。如前文所述，面对数字技术对个人信息治理可能产生的风险，联盟链可以提升个人信息治理的真实性以创建优良信息基础，能够保障个人信息的安全性以提升信息公信力，可以促进个人信息的共享程度以提升协同效率。其次，联盟链可以助力法律进行追责和监管。联盟链作为一种技术解决方案，有其自身的优势，从而帮助法律提升实施效果。

〔39〕〔美〕凯文·沃巴赫、林少伟：《信任，但需要验证：论区块链为何需要法律》，载《东方法学》2018 年第 4 期，第 107 页。

〔40〕参见郑智航：《网络社会法律治理与技术治理的二元共治》，载《中国法学》2018 年第 2 期。

如联盟链多中心化的特征可以帮助法律进行监管从而实现疫情的精准防控。再如数字时代个人信息保护的重点应当由传统的事前保护转移到事中、事后的保护，〔41〕而联盟链可以配合法律在数字防疫中规范个人信息的事前收集、事中处理的程序，以及在事后救济的取证方面提供助力。最后，联盟链可以实现一定程度上代替规则自动运行的作用。利用代码创设的自动化应用程序可以在一定程度上代替相关制度规则。如监管部门可以利用代码在监管节点创设自动执行的监管程序。当系统达到特定要求即可能产生风险时，自动发出警示以要求相关节点说明情况，甚至暂缓传输信息，以此代替原有规范性文件规定的相关程序性风险防范规则。

五、数字防疫中“链”“法”协同机制的构建思路

（一）构建与法律相匹配的联盟链治理机制

如前所述，联盟链是数字防疫中个人信息治理的保障和补充。在“链”“法”协同治理机制中，首先需要构建与法律相匹配的个人信息联盟链治理机制，即建立个人信息联盟链治理系统。这一过程既要动态认识联盟链的优势与法律的相对劣势，也要考虑我国数字防疫的现实，具体可以从以下三个方面展开：

1. 制定联盟链底层技术标准

联盟链作为新兴技术，其在数字防疫中的应用应当首先明确其使用的底层技术标准。建设数字防疫中个人信息治理的联盟链系统将是一个复杂的系统性工程，“链”与“非链”信息系统将长期共存。如果不能采用统一的信息格式和标准，则“容易引发系统错误、混乱等风险”〔42〕，也无法实现不同信息系统之间的信息互通。信息只能在联盟链系统内流通，使联盟链系统成为更大的“信息孤岛”，即“区块链孤岛”〔43〕，从而不能实现本质上的信息共享。制定统一的联盟链底层技术标准，可以彻底打破“信息孤岛”现象，使个人信息在“链”与“非链”中有序共享，从而提升信息治理效率；也可以为联盟链在其他领域的应用提供标准和参考，从而推动区块链产业协同发展。当前区块链产业仍处于发展初期，存在一定程度的行业乱象，各区块链服务商的技术水平和研发能力均有待加强。制定统一的联盟链底层技术标准，可以为区块链技术服务商提供标准指导，从而推进防疫主体控制的个人信息持续上链存储；也可以为数字防疫中的个人信息治理提供相关决策和监督尺度参考，从而提升监管能力和安全保障水平。本文建议：应当由防疫主管部门和工信部门负责，会同科研机构、专家学者立足现有联盟链成果，参考现有技术规范，制定数字防疫中个人信息治理联盟链系统底层技术标准，明确数据接口、共识机制、分布式记账、智能合约等代码标准和加密程度、算力空间、登录 IP 地址限制等运行规则；应当围绕数字防疫的紧迫性、个人信息的安全性需求和联盟链的优势提出此联盟链系统的底层技术要求，明确该系统的建设及运行标准；确保数字防疫中个人信息治理联盟链系统规范建立并良性运行，保证其和其他“链”与“非链”信息系统协同发展。

〔41〕 参见邢会强：《大数据时代个人金融信息的保护与利用》，载《东方法学》2021 年第 1 期。

〔42〕 杨东：《链金有法——区块链商业实践与法律指南》，北京航空航天大学出版社 2017 年版，第 309 页。

〔43〕 胡元聪：《区块链技术激励机制的制度价值考察》，载《现代法学》2021 年第 2 期，第 153 页。

2. 构建联盟链应用平台框架

联盟链对于化解数字防疫给个人信息治理带来的风险具有天然的优势，其多中心化的特征也有利于政府统一管理，从而实现精准防控。可以利用联盟链搭建数字防疫中个人信息治理的应用平台框架，建立包括监管部门、防疫主体（包括公权力防疫部门和社会防疫主体）在内的多中心联盟链系统。疫情防控需要社会各界共同参与，在国家的统一管理下实现联防联控。因此，新系统既要强化国家的中心管理作用，也要注重各行各业的参与。〔44〕在联盟链治理系统中，应当由各级政府和监管部门成为中心节点，强化国家的中心管理作用；并采用政府主导、法律政策推动的形式，将数字防疫中涉及的其他公权力防疫部门、相关社会防疫主体作为普通节点纳入系统中，使涉及疫情防控和个人信息治理的部门、企业一起联防联控，形成“共治”〔45〕机制。并根据数字防疫和个人信息治理的特点，在系统存储总量、响应速度等方面优化改进。对此，可以通过规范性文件明确各级政府和监管部门的中心节点资格，并明确其他公权力防疫部门、相关社会防疫主体的普通节点资格，并排除其他主体的节点资格。此外，可以在系统中设立没有写入权限的访问节点，供其他没有成为系统节点的主体获取信息。在数字防疫中，自然人作为信息的被处理者具有随机性，而个别社会防疫主体如社区、村委会等不容易满足加入联盟链的设备条件和制度要求，因而这些主体不被纳入联盟链系统中。但是，可以通过联盟链上没有写入权限的统一访问节点，使自然人访问其在系统中储存的本人和亲属的个人信息供其他防疫主体校验，从而使社区、村委会等个别没有成为节点的社会防疫主体也可以通过联盟链获取其权限范围内的相关防疫信息，由此在保障联盟链技术性能的前提下提升联盟链的覆盖范围，使更多主体分享技术迭代带来的“红利”。

3. 建立联盟链技术处理规则

具有规范、安全的技术处理规则是联盟链系统有序运行的前提。在联盟链系统的建设及运行过程中，应当依托现有地方联盟链防疫系统，建立信息上传、利用的技术处理规则，保证数字防疫中个人信息的安全利用。

首先，应当建立信息上传的技术处理规则，结合实践分批上传个人信息。数字防疫中涉及的个人信息数量众多，信息入链的先后顺序需要得到规范。因此，应当建立信息上传的技术处理规则，结合当前我国疫情防控实际和联盟链发展现实，根据地域分批建立联盟链系统，依据涉疫程度分批上传个人信息：其一是依托现有济南、广州等地的联盟链防疫系统优先上传济南、广州等联盟链防疫实践地区的疫苗接种者、确诊、疑似、无症状患者及密切接触者的个人信息；其二是上传当前及近期中、高风险地区的疫苗接种者、确诊、疑似、无症状患者及密切接触者的个人信息；其三是上传当前及近期中、高风险地区其他人员、境外入境人员、高危感染人员的个人信息；其四是进行疫苗接种者、曾经确诊、疑似及无症状感染者的个人信息上传；其五是进行全国范围内的普遍上传。

其次，应当建立信息利用的技术处理规则，按照分层分级储存、根据权限下载的原则利用个

〔44〕 参见黄茂汉：《基于区块链技术的疫情防控情报系统模型研究》，载《情报科学》2021 年第 8 期。

〔45〕 杨杨、杜剑等：《区块链技术对税收征纳双方的影响探析》，载《税务研究》2019 年第 2 期，第 116 页。

人信息。数字防疫中涉及的信息处理主体众多，个人信息的利用程序需要得到规范。因此，应当建立信息利用的技术处理规则，将节点搜集到的个人信息根据不同属性和来源利用非对称加密技术分级、分层储存，并依照防疫部门的权限确定其访问和使用的边界。个人信息在节点去标识化上链储存后，分为不同保密级别的信息。保密级别较低的信息主要包括去标识化的身份信息、活动轨迹等基础信息，对防疫主体的访问权限限制较低。保密级别较高的信息主要包括实名身份信息、接触史等个人涉疫信息，只允许具有较高权限的防疫主体访问。应当通过联盟链的共识机制和非对称加密机制设立差异化的信息访问权限，以此保证个人信息安全。

（二）构建与联盟链相适应的法律治理机制

法律是数字防疫中个人信息治理的前提和基础。在“链”“法”协同治理机制中，需要构建与联盟链相适应的数字防疫个人信息法律治理机制。法律应当改变传统的治理模式，适应联盟链环境并与之共同构建全方位的协同治理机制。具体可以从以下三个方面展开：

1. 明确联盟链的法律地位和效力

推动联盟链在数字防疫中个人信息治理方面的应用，应当考虑相关技术应用的法律基础，明确联盟链的法律地位和法律效力是“链”“法”协同作用的前提。首先，应当明确联盟链的法律地位。目前，我国个人信息治理的法律规则规定于由《民法典》和《个人信息保护法》组成的个人信息保护制度体系中，但其未对重大突发公共卫生事件背景下个人信息的治理和智能技术的应用给予明确规定，而仅为一些纲领性的总括，导致这一特殊背景下智能技术在个人信息应用方面的相关法律规范仍分散于诸多法律文本中。而联盟链对个人信息治理具有重大促进作用，将从技术手段破解原有信息治理难题。对此，应当肯定联盟链作为治理手段和治理工具的法律地位，并制定相关激励条款，肯定并鼓励联盟链在个人信息治理方面的应用，促进联盟链乃至智能技术在个人信息治理方面相关产业的发展。其次，应当明确联盟链的法律效力。目前，联盟链已经在司法层面初步得到肯定。最高人民法院在《关于互联网法院审理案件若干问题的规定》中对于利用哈希值校验、区块链技术搜集的证据予以认可，部分司法裁判中也已肯定利用区块链技术存证的法律效力。〔46〕但如果想让联盟链在数字防疫和个人信息治理中更好地发挥作用，需要给予更高层面的确认。联盟链可以成为法律的补充，和法律协同化解数字防疫给个人信息治理带来的风险。因此，应当出台相关法规或调整相应规范，对联盟链的分布式记账本的信息记录、智能合约等有效性进行确认，肯定联盟链在个人信息治理方面的法律效力。

2. 构建适合联盟链的节点责任制度

构建基于联盟链的节点责任制度是法律适应联盟链分布式分类账环境的重要转变。联盟链的分布式记账使得系统内并不存在传统平台上的唯一中心化管理主体，原中心化职能被分散给相关多个中心节点。故在“链”“法”协同机制中，为适应联盟链这一特征，可以立足于系统节点，建立适应联盟链的节点责任制度。

首先，应当通过法律明确节点为责任主体。节点对于分布式记账本具有重要意义，是整个联盟链系统的参与主体，系统通过节点之间的相互验证、记录得以运转。联盟链的节点身份固定且

〔46〕 参见吴京辉、胡兰：《区块链技术助推中小企业票据融资的法律完善》，载《江西社会科学》2019 年第 12 期。

透明，由防疫部门、监管部门组成，可以准确定位节点对应的防控主体，并不存在其他区块链系统因节点匿名而无法追责的问题。根据本次防控实践，个人信息可能部分泄漏于防疫机关。因此，应当明确联盟链系统节点的责任主体资格，即节点应当作为承担责任的主体。其次，应当明确系统节点的责任内容。我国对区块链系统节点的义务与责任已有初步规定。国家网信办《区块链信息服务管理规定》规定了提供区块链信息服务的主体或节点的管理、配合监管等义务及相关的责任，但该文本中的规定较为粗糙，更多的是一些纲领性的宣誓条款，其中一些概念的具体含义并不明确。〔47〕因此，应当对该部门规章进行修改，或就该文本展开进一步的解释与探讨。在数字防疫中，应当明确防疫主体在原信息处理相关义务外，作为联盟链系统节点而具有的权利、义务和责任，并明确其责任形式及追责程序。通过追责弥补联盟链“技治”无法涵盖的部分漏洞和不足，如联盟链可以通过激励机制保证链上信息的真实性，但对于上传前信息的真实性无法保证，对此可以发挥法律的约束功能，明确上传虚假信息的责任和相关过错或知情方的责任以弥补联盟链的不足，实现联盟链的技术激励与法律的制度约束的协同。同时，对于节点责任的形式应当注重民事、刑事和行政责任的并用，在对违反义务的行为加大行政处罚力度的同时辅以民事赔偿责任。此外，还要明确节点代表主体责任人的责任并落实到人，对于达到刑事责任标准的行为加以刑法的规制以发挥刑法的震慑作用。

3. 建立适应联盟链的动态监管制度

建立基于联盟链系统的动态监管制度可以助推法律由事前准入、事后监督的传统监管模式转向全程动态监管模式以适应联盟链系统。联盟链的加密机制、链式结构等将联盟链系统分隔为链上链下两个世界，链上的空间运行状态公开透明，每个节点都在参与系统的运行，而基于联盟链的多中心化特征也适合嵌入若干监管节点。故在“链”“法”协同机制中，可以构建基于联盟链系统的全程动态监管模式，将部分中心节点设为监管节点并使监管部门加入其中。如此不仅能够借助联盟链实现实时监管，还可以监测并预防联盟链应用可能带来的未知风险。首先，应当成立超级监管节点。在系统中将部分中心节点改造为监管节点，监听链上广播、储存信息，更新全网总账，掌握系统动态。一方面，监管部门通过监管节点实时获取系统内的共享信息，掌握链上活动，可以及时发现违法违规现象，提高监管效率。另一方面，监管部门通过监管节点实现一定程度上的自动执行和实时决策，可以及时根据系统运行情况变动系统规则进而有效预防可能发生的风险。其次，应当成立公权力监管部门，并通过法规或部门规章赋予其超级监管节点资格。即明确将数字防疫中个人信息治理监管权交由国家统一调度，由国务院主导，工信部会同网信办负责，协调多方职能部门，设立中央和地方层面的数字防疫中个人信息治理联盟链系统监督管理委员会。该委员会统筹领导联盟链系统的推进及监管工作，并作为超级节点被加入系统中，对系统进行实时监测。〔48〕同时明确该监管部门在事前审查、事中管理以及事后追责等阶段使用的程序和对应职责。还要赋予该监管部门独立的执法权和管理权，避免部门之间互相推诿等情况，促进数字防疫中个人信息治理联盟链系统监管规范化。最后，应当设立社会层面的行业协会。有必要

〔47〕 参见贾翱：《区块链信息服务监管对象研究——以〈区块链信息服务管理规定〉第二条为中心》，载《大连理工大学学报（社会科学版）》2020 年第 2 期。

〔48〕 参见时明生：《区块链技术在征信业的应用探析》，载《征信》2018 年第 1 期。

在监管部门之外设立独立的行业协会，并给予其一定自主权限。该协会可以针对联盟链系统发展的形势制定行业自律标准和实施细则，对系统进行定期风险评估与调查监测，同时促进信息持续上链和系统平稳运营以减轻公权力机关负担。

六、结　语

联盟链对于化解数字防疫的个人信息治理风险具有天然优势，可望缓解数字防疫与个人信息传统法律治理之间的冲突龃龉问题，进而破解个人信息治理之“危”，利用数字进行防疫之“机”。但基于联盟链的“技治”并不能完全取代基于法律的“制治”，以代码替代法律的设想也不可行。应当发挥联盟链的长处，结合法律治理的优势来构建数字防疫中个人信息“链”“法”协同治理机制。在大数据、人工智能等技术基础上继续应用联盟链是一项系统工程，应当在不断实践的基础上充分把握联盟链、法律各自的优势，以及数字防疫和个人信息治理的发展趋势，缓解联盟链与法律、数字防疫与个人信息治理之间的双重张力。同时需要指出：以联盟链为代表的区块链技术毕竟属于新兴技术，在应用方面仍处于探索阶段。联盟链应用可能带来的风险和挑战还需要进一步的探讨。

Abstract：In this epidemic prevention and control，digital technologies such as artificial intelligence and big data not only reduce the risk of epidemic spread，but also make personal information management face new risks. Alliance chain has been widely used in many fields in recent years，and has become a feasible tool to resolve the risk of personal information governance in digital epidemic prevention. However，while applying alliance chain governance risk，it is also necessary to optimize the corresponding system，so as to realize the “joint governance” of alliance chain and law under the action of technical iteration and system optimization. Therefore，we should eliminate the tension between alliance chain and law，and then build a “chain” and “law” coordination mechanism based on legal governance and supplemented by alliance chain governance. Specifically，by building an alliance chain governance mechanism matching the law and a legal governance mechanism matching the alliance chain，and integrating the respective advantages of blockchain technology and law，the “chain” and “law” coordination mechanism can improve its ability in personal information governance in digital epidemic prevention，thus improve the level of modernization of national governance.

Key Words：digital epidemic prevention，personal information governance，risk government，alliance blockchain，synergy between “blockchain” and “law”

（责任编辑：殷秋实　赵建蕊）

财经法学 No. 2，2023
pp. 51 - 67

数字政府建设中个人信息保护的风险规制路径

刘绍宇*

内容提要：公共部门个人信息保护制度的完善是建构数字法治政府的必由之路。我国《个人信息保护法》采取了公私部门一体调整的宣示性立法模式，目前既无法为公共部门个人信息保护提供足够的规则指引，也未充分满足数字政府建设的需要。数字政府个人信息保护规则的建构，不仅需要考虑公共部门相对私人部门在个人信息处理活动中的特殊性，还要兼顾数字政府在技术和治理这两个层面的革新，进而制定专门规则。风险规制模式不仅是世界范围内个人信息保护制度的发展趋势，而且能够为一体调整模式提供理论基础。通过风险预防原则的适当运用，对个人信息权利的风险化解释与调适，风险管理、风险交流和风险评价等风险规制机制的灵活运用，以及合作治理、独立规制机构、技术治理、回应治理、试验规制和软法之治等风险规制策略的共同配合，建构以风险规制为导向的数字政府个人信息保护机制是我国未来的最优选择。

关键词：数字政府　个人信息保护　风险规制

一、问题的提出

近年来，我国一直致力于推动数字政府建设，并取得了令人瞩目的成绩。在数字政府建设中，政府汇集了整个社会的数据资源，并利用其实现大数据治理，这在提升行政服务水平、促进数字经济发展和推动国家治理现代化的同时，也带来了极大的数据安全和个人信息风险。数据安全和个人信息保护是数字政府建设中不可忽视的议题，一直受到我国政府的高度重视。中国共产党第十九届四中全会作出的《中共中央关于坚持和完善中国特色社会主义制度 推进国家治理体

* 刘绍宇，中国社会科学院法学研究所助理研究员。

本文为国家社会科学基金重大项目“行政诉讼类型制度的构建研究”（19ZDA163）、中国博士后科学基金第 14 批特别资助“论私法主体的公法管控：以网络平台为考察对象”（2021T140727）阶段性研究成果。

系和治理能力现代化若干重大问题的决定》明确提出“推进数字政府建设，加强数据有序共享，依法保护个人信息”。而在 2022 年 6 月 23 日发布的《国务院关于加强数字政府建设的指导意见》中，国务院更是以专章规定“构建数字政府全方位安全保障体系”，其中包括“加大对涉及国家秘密、工作秘密、商业秘密、个人隐私和个人信息等数据的保护力度”。

与此同时，我国个人信息保护法律体系建设也正稳步推进。尤其是 2021 年《中华人民共和国数据安全法》（以下简称《数据安全法》）和《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）这两部法律的颁行，标志着我国个人信息保护法律制度基本成型。然而，尽管个人信息保护对数字政府建设来说至关重要，但个人信息保护制度的建构似乎与数字政府建设平行进行，并未为后者提供足够的制度供给。《个人信息保护法》采取公共部门与私人部门一体调整模式，被认为是一种“象征性立法”〔1〕，远远无法满足数字法治政府建设的制度需求，“数字政府建设过程中的个人信息保护尚未得到应有的重视”〔2〕。一体调整模式既无法为公共部门个人信息保护提供足够明晰的规则指引，也未回应数字政府建设的需要，“个人数据权利保护的制度供给不足是当前掣肘数字政府变革的重要因素之一”〔3〕。

如何规范公共部门个人信息处理活动，尤其是如何建构与数字政府兼容的个人信息保护制度，是建设数字政府和完善个人信息保护制度的重大议题之一。尽管目前学界已对政府处理个人信息活动的规范展开了深入研究，〔4〕但绝大多数研究并未充分考虑政府数字化转型的时代背景，而仍是在传统政府视角下的探讨。事实上，学界普遍认为数字政府给个人信息保护制度带来了极大的挑战，有学者直接指出数字政府与个人信息保护之间存在难以弥合的矛盾，〔5〕还有学者考察了开放政府、数据治理、平台政府与个人信息保护之间的冲突，〔6〕以及知情同意原则、目的限制原则与数字政府之间的张力〔7〕。

对于如何建构数字政府个人信息保护制度这一问题，学界存在权利保护路径和风险管理路径之间的争议。权利保护路径侧重于探讨个人信息保护原则以及个人信息权利如何在数字政府中实现，风险管理路径则认为应通过政府内部风险管理实现个人信息保护。本文认为应整合上述两种

〔1〕 王锡锌：《行政机关处理个人信息活动的合法性分析框架》，载《比较法研究》2022 年第 3 期，第 94 页。

〔2〕 马颜昕等：《数字政府：变革与法治》，中国人民大学出版社 2021 年版，第 370 页。

〔3〕 董筱文、胡雯：《以法治化赋能数字政府建设》，载《中国社会科学报》2022 年 8 月 10 日，第 8 版。

〔4〕 参见赵宏：《告知同意在政府履职行为中的适用与限制》，载《环球法律评论》2022 年第 2 期；喻文光、郑子璇：《数字时代政府机关处理个人信息告知义务制度的公法建构》，载《人权》2022 年第 3 期；彭錞：《论国家机关处理个人信息的合法性基础》，载《比较法研究》2022 年第 1 期；孙清白：《国家机关处理个人信息的特殊风险及其法律规制》，载《安徽大学学报（哲学社会科学版）》2022 第 3 期；程子栋、王鹏彪、罗海宁：《对数字政府安全技术合规分析的建议》，载《中国信息安全》2022 年第 8 期。

〔5〕 Vgl. Roßnagel/Laue, Zweckbindung im Elektronik Government, DÖV12 (2007), 543, 544; Hansen, Die ambivalente Beziehung zwischen eGovernment und Datenschutz, DuD 10 (2021), 664, 664; Stutz, Verantwortlichkeit und Datenchutz im E-government, in: Wind/Kröger (Hrsg.), Handbuch IT in der Verwaltung, 2006, S. 347.

〔6〕 参见宋烁：《论政府数据开放中个人信息保护的制度构建》，载《行政法学研究》2021 年第 6 期；宋华琳、郑琛：《论政府数据开放中的数据安全保护制度》，载《中国司法》2022 第 3 期；彭箫剑：《平台型政府及行政法律关系初论》，载《兰州学刊》2020 年第 7 期。

〔7〕 参见马颜昕、吴敏慧：《数字政府建设中〈个人信息保护法〉适用的挑战与展望》，载《网络信息法学研究》第 11 期，中国社会科学出版社 2022 年版，第 122 页。

路径的优劣，提出一种风险规制路径，为建构数字政府中的个人信息保护提供理论基础和制度指引。本文第一部分从权力、技术和组织这三个层面系统讨论数字政府建设如何对个人信息保护制度构成挑战，在此基础之上，第二部分提出个人信息保护的风险规制路径，并对其在数字政府中的运用予以证成，最后探讨如何在风险规制路径下完善数字政府个人信息保护制度。

二、数字政府建设对个人信息保护制度带来的挑战

学界普遍认为我国个人信息保护制度与数字政府建设之间存在难以弥合的矛盾，数字政府建设给个人信息保护制度带来严峻挑战。这主要是因为，在目前的一体调整模式下，我国以私人部门为范式建构的个人信息保护规则并未考虑到公共部门的独特之处和数字政府的最新发展。本文结合数字政府的主要特征，从公共属性、技术进步和治理革新这三个层面分析数字政府建设何以为个人信息保护制度带来挑战。

（一）公共属性给个人信息保护制度带来的挑战

我国《个人信息保护法》确立的一体调整模式，本质上是将以私人部门为范式建构的个人信息保护规则适用于公共部门，并未顾及数字政府的公共属性。公共属性是政府的固有属性，意味着政府主要是为了完成取向于公共福祉和公共利益的公共任务，进而被法律赋予职权。政府的公共属性并不因为其数字化转型而丧失，而应予以特别保护。公共部门之所以要有专门的个人信息保护规则，主要是基于其公共属性，这也是一体调整模式制度供给不足的首要原因。正基于此，在个人信息保护立法较为悠久的德国，公共部门个人信息保护立法一直独立于私人部门存在。

公共部门之所以给以私人部门为范式建构的个人信息保护制度带来挑战，主要是基于两个方面的原因。一方面，政府完成公共任务主要是为了维护公共利益，而个人信息保护制度主要是一种维护个人权益的机制。政府在履行公共职责时，个人信息保护原则和个人信息权利均会因为公共利益的优位性而受到限制。欧盟《保护警察和刑事司法当局使用的个人数据指令》（以下简称LED）和德国各州公共机构数据保护立法之中均对知情同意原则、目的限制原则和透明原则有不同程度的放宽，对个人信息权利也有一定限制。〔8〕甚至有学者认为目的限制原则被完全突破，因为与欧盟《通用数据保护条例》（GDPR）不同的是，只要符合合法性和必要性原则的要求，个人信息被再次处理的目的并不需要与初始目的兼容。〔9〕另一方面，政府无论是从事秩序行政还是服务行政，个人信息主体均处于一种非对等关系的弱势地位，诸如“同意”这样的个人信息保护机制基本失灵。有德国学者以疫情防控软件为例，指出该情境下政府搜集个人信息获取的同意根本无法实现有效的权利保护。〔10〕

〔8〕 See Mark Leiser & Bart Custers, The Law Enforcement Directive: Conceptual Challenges of EU Directive 2016/680, 5 (5) *European Data Protection Law Review* 367, 373 (2019).

〔9〕 See Catherine Jasserand, Law Enforcement Access to Personal Data Originally Collected by Private Parties: Missing Data Subjects' Safeguards in Directive 2016/680?, 34 (1) *Computer Law & Security Review* 154, 163 (2018).

〔10〕 Vgl. Samardzic/Becker, Die Grenzen des Datenschutzes: Der beschrankte Schutz durch Freiwilligkeit und Einwilligung bei Corona-Apps, EuZW 31 (2020), 646, 646.

根据政府活动公共属性的高权程度不同，个人信息保护规则也应有所不同，而我国目前的一体调整模式并未作出这种区分。以欧盟为例，政府警察、刑事司法活动和一般行政活动的个人信息保护规则并不相同。一般来说，政府活动高权程度越高，相应的公共属性越强，对公民基本权利的影响越大，对以私人部门为范式建构的个人信息保护制度形成的挑战越大，特别规则的建立也越有必要。根据高权程度的不同，政府活动可以区分为警察和刑事司法活动、秩序行政、服务行政和私行政。结合前述原理，私行政活动可参照《个人信息保护法》其他部分的规定，因此“同意”在政府处理个人信息中也有适用空间。〔11〕警察和刑事司法活动高权属性最强，绝大多数国家建立了专门的个人信息保护规则。我国刑事诉讼法学界也对此展开了专门的深入研究，普遍认为应进行刑事诉讼个人信息保护专门立法。〔12〕一般秩序行政和服务行政则基本可以参照私部门个人信息保护规则，适用一体调整模式。不过，由于各个国家对警察、犯罪和刑事司法等概念的理解存在差异，警察、刑事司法活动和秩序行政实际上存在一定区分难度，在欧盟实践中已经造成困扰。〔13〕

（二）技术手段给个人信息保护制度带来的挑战

数字政府给个人信息保护制度带来挑战的另一关键原因在于，数字政府广泛运用了大数据、人工智能、区块链、云计算、物联网乃至虚拟现实和深度合成等新型数字技术。个人信息保护制度的本质是技术监管工具，〔14〕从监管理论上来说，其应随着技术进步而更新，否则会造成规制滞后。我国目前的个人信息保护制度整体上根植于 20 世纪 80 年代的公平信息实践，上述每一项技术革新均给其带来冲击，对此法律与技术界已展开了深入的探讨。〔15〕而数字政府是上述技术的综合运用，〔16〕更给个人信息保护带来系统性风险和根本性挑战。具体来说，数字技术的发展在以下几个方面给个人信息保护制度带来挑战，这些挑战目前已在数字政府建设中凸显。

1. 个人信息与非个人信息的区分

传统个人信息保护制度是建立在个人信息与非个人信息二分基础之上，个人信息被认为是个人信息保护立法的核心与前提。而在数字政府建设的大背景下，为了充分发挥大数据技术的治理潜力，数据融合越来越频繁，个人信息与非个人信息的区分开始模糊，非个人信息被重新识别的难度越来越低。早在《个人信息保护法》出台之前，关于个人信息的界定处于众说纷纭的状态，司法实践中也是莫衷一是。《个人信息保护法》出台后，尽管其对个人信息作出了较为明确的定义，但上述分歧并未完全消失。至今，个人信息的界定，仍然困扰着理论与实务界。在大数据时代，这一问题在未来根本无法得到解决，本质上是因为大数据技术使得重新识别越来

〔11〕 参见前引〔4〕，彭錞文。

〔12〕 参见裴炜、张桂贤：《论刑事诉讼中个人信息保护的知情规则》，载《成都理工大学学报（社会科学版）》2022 年第 4 期；郭烁、杨默涵：《受限、契合与独立：论刑事诉讼数据处理原则》，载《北京航空航天大学学报（社会科学版）》2022 年第 4 期；郑曦：《刑事诉讼个人信息保护论纲》，载《当代法学》2021 年第 2 期。

〔13〕 Vgl. Kugelmann, Anwendungsbereich und Spielraume der Landesdatenschutzgesetze, in: Seckelmann (Hrsg.), Digitalisierte Verwaltung Vernetztes E-government, 2. Aufl., 2019, S. 432.

〔14〕 Vgl. Vogel, Das Datenschutzrecht als Instrument der Technikregulierung, in: Susanne/Carsten/Brian (Hrsg.), Digitalisierung, Automatisierung, KI und Recht. Festgabe zum 10-jährigen Bestehen der Forschungsstelle RobotRecht, 2020, S. 645.

〔15〕 See Tal Zarsky, Incompatible: The GDPR in the Age of Big Data, 47 (4) *The Seton Hall Law Review* 995 (2016).

〔16〕 国务院发布的《全国一体化政务大数据体系建设指南》中指出，积极运用云计算、区块链、人工智能等技术提升数据治理和服务能力。

越容易。

2. 目的限制原则

目的限制原则是我国个人信息保护制度的基础原则，规定在《个人信息保护法》第6条第1款中。所谓目的限制原则，是指个人信息的收集和利用均限于最初确立的目的，与该目的保持一致。从一定程度上说，目的限制原则和大数据技术的运作模式存在根本冲突。在数字政府的大背景下，大数据技术的要义便在于不断去发掘数据的价值，使数据发挥在搜集时难以预料到的作用。而目的限制原则要求个人信息的利用限于搜集时的目的，阻碍了新功能和新服务的研发，不利于数据利用价值的发挥。因此，在数字经济建设的大背景下，目的限制原则受到越来越多的批判，不少国家也通过引入兼容性使用标准、无法预料标准和尊重场景原则等来缓和目的限制原则的严格要求。〔17〕而我国则仍坚持了严格的目的限制原则，因而加剧了个人信息保护制度与数字政府建设，尤其是大数据治理之间的冲突。〔18〕

3. 知情同意原则

知情同意原则是世界范围内个人信息保护法的核心机制，在我国个人信息保护制度中也发挥关键作用。《网络安全法》一度将同意作为个人信息处理唯一的合法性基础，《个人信息保护法》尽管规定了更加多元化的合法性基础，但知情同意原则仍具有基础地位。然而，知情同意原则作为落实个人信息自决的机制，其前提在于个人信息主体具有独立自主决定的能力，对此《个人信息保护法》也专门规定，要求知情同意必须“由个人在充分知情的前提下自愿、明确作出”。而在数字政府背景下，数字技术的应用使得个人信息主体根本不可能满足这一前提条件，用户对其个人信息的控制是虚幻的。〔19〕由于个人根本无法理解隐私协议，也无法理解数字政府建设中的数字技术，以及其对个人信息所带来的风险，这种同意并不是建立在充分知情基础之上。

4. 个人信息权利

个人信息权利在不少数字技术中也难以实现，具有代表性的例子是人工智能、区块链和云计算技术。就人工智能来说，在机器学习中如何确保删除权和被遗忘权在国内外数据合规实践中已经成为一个难题，“数据删除的要求实际上已经游离在一种不可能的边缘”〔20〕，“完全删除数据是一项计算密集工作，既不经济实用也不环保”〔21〕。就区块链技术来说，删除权和被遗忘权〔22〕等个人信息权利的行使与区块链记录的完整性、防篡改性、可追溯性等原生特性存在悖论，在技术

〔17〕 参见朱荣荣：《个人信息保护“目的限制原则”的反思与重构——以〈个人信息保护法〉第6条为中心》，载《财经法学》2022年第1期。

〔18〕 参见刘权：《论个人信息处理的合法、正当、必要原则》，载《法学家》2021年第5期。

〔19〕 See Neil Richards & Woodrow Hartzog, The Pathologies of Digital Consent, 96 (6) *Washington University Law Review* 1461, 1473 (2018).

〔20〕 翟凯：《论人工智能领域被遗忘权的保护：困局与破壁》，载《法学论坛》2021年第5期，第142页。

〔21〕 Michèle Finck, The Limits of the GDPR in the Personalisation Context, in U. Kohl & J. Eisler eds., *Data-Driven Personalisation in Markets, Politics and Law*, Cambridge University Press, 2021, p. 100.

〔22〕 Vgl. Martini/Weinzierl, Die Blockchain-Technologie und das Recht auf Vergessenwerden, NVwZ 17 (2017), 1251, 1251.

上难以实现。〔23〕就云计算技术来说，删除权和可携带权等个人信息权利在云计算架构中难以实现。〔24〕

5. 个人信息保护责任

数字技术的发展不仅给个人信息权利带来挑战，而且给个人信息保护责任分配也造成威胁，这在区块链和云计算技术中尤为明显。个人信息风险管理以确定个人信息处理者为前提，进而课以个人信息处理者一系列义务责任。在区块链技术中，由于其去中心化的架构特征，中心化的个人信息处理者并不存在，如何认定个人信息处理者，至今仍是困扰理论界和实务界的难题，导致个人信息保护责任难以明确。〔25〕在云计算技术中，由于涉及各方均难以决定个人信息处理目的，个人信息处理者与个人信息受托人，以及欧盟法上的数据控制者与数据处理者之间的区分很难明晰，〔26〕进而影响了个人信息保护责任的分配。

（三）治理理念给个人信息保护制度带来的挑战

除了技术手段之外，数字政府所蕴含的治理理念也给传统个人信息保护制度带来极大的挑战。从传统政府到数字政府，本质上是为了“建设人民满意的服务型政府”，在治理理念上发生了整体政府、合作政府和平台政府的转变，传统个人信息保护制度无法满足变革所带来的制度需求。尽管数字技术在建构数字政府进程中发挥着举足轻重的作用，但治理理念的变革更为重要。理念是目的，技术只是工具，否则数字政府只会沦为一种形象工程。

首先，从政府内部关系来说，数字政府正在向整体政府转型。整体政府理念最早源自西方，核心在于整体性协作，其内容十分广泛，既包含不同层级政府之间的上下协作，也包含同一层级不同政府之间以及同一政府不同部门之间的左右协同，还包括政府与企业和非营利组织之间的内外合作。近年来，我国行政管理改革和法治政府建设也被认为发生了向整体政府的转变，〔27〕尤其是数字政府建设更是贯穿了整体政府的理念。在数字时代，数字技术的兴起和运用使得整体政府的理念更容易得到贯彻，整体政府进而也成为数字政府的重要特征。尤其是政府组织内部的数据共享打破了以往各个机构之间的信息孤岛，在线协作、跨部门协同和线上线下的交互融合协同，实现了整体性协同运行的路径建设。

其次，从政府企业关系来说，数字政府正在向合作政府转型。数字政府建设需要大量的技术支撑和资源投入，政府根本没有足够的能力单独完成，此时只能引入民间资本和企业力量才能满足技术、资金、人力等方面的需求。因此，公私合作成为我国乃至全球数字政府建设的普遍模式，对私人企业的依赖是以往任何公私合作形式所无法比拟的，数字政府也基本成了一种合作政府。无论是数据治理、数据共享还是数据开放，公私合作均发挥着重要作用。以数据治理为例，

〔23〕 参见陈爱飞：《解释论视域下的区块链个人信息删除权》，载《南京社会科学》2022 年第 6 期。

〔24〕 See Marina Škrinjar Vidović, EU Data Protection Reform: Challenges for Cloud Computing, 12 (1) *Croatian Yearbook of European Law & Policy* 171, 183 (2016).

〔25〕 参见前引〔22〕，Martini、Weinzierl 文，第 1257 页。

〔26〕 参见前引〔24〕，Marina Škrinjar Vidović文，第 176 页。

〔27〕 参见王太高：《我国整体政府思想的形成及其展开——以〈法治政府建设实施纲要（2021—2025 年）〉切入》，载《探索与争鸣》2022 年第 1 期。

不少政府的大数据决策监测技术系统均是由私人企业提供；以数据共享为例，目前全国范围内各地政府均采取了公共数据授权运营的模式，将公共数据授权给企业运营。

最后，从政府公民关系来说，数字政府正在向平台政府转型。平台政府的理念与实践发源于英国，近年来受到我国学界的高度关注。平台政府是我国数字政府建构的重要面向，搭建政务服务平台是近年来的主要工作。尽管国内外理论与实务界对平台政府的界定尚未达成共识，但整体上来说其具有如下两个方面的特征：组织技术上借鉴平台企业运用了双边平台治理技术和组织架构；治理理念上突出社会开放性、权力多中心、双向互动和公众参与。从外部关系来说，平台政府体现了开放、参与、便民和透明的价值导向；从内部关系来说，平台政府体现了协作、整体、效能和集成的管理理念。

数字政府具有显著的整体性、系统性、开放性和协同性特征，不仅将公共部门各个实体有机融合，而且将公共部门和私人部门高度整合。正基于此，越来越多的学者提出数字生态理论，认为数字政府、数字社会和数字公民构成了一个生态系统，充分体现了数字政府的治理转型。〔28〕随着数字经济的发展和数字政府建设的推进，这种特性会越来越强。而传统个人信息保护制度是建立在公私部门相互隔离和数据处理者分散独立的基础之上的以数据处理者为中心的调控模式，难以满足数字治理生态系统下的个人信息保护需求。基于此种范式，公共部门与私人部门之间的数据传输并未受到足够的规范，这在欧盟数据保护法中已经有所体现，〔29〕数据使用中的公私合作被认为处于法律真空状态，〔30〕在我国则更为明显；政府机构之间，政府机构与私人企业之间以及私人企业之间任何跨实体的数据流动被严格规范，个人信息一旦在不同的实体之间流动，便受到法律的管控；个人信息保护主要依赖于政府的行政监管和数据处理者自身的内部控制，个人信息主体参与性较低。

随着数字政府的不断发展，数字政府与传统政府在治理理念上的不同，已经演化为原则冲突甚至规则冲突。政府数字化转型所带来的治理理念变革被形塑为数字政府原则，甚至被进一步具体化为规则，例如，政府数据共享中的“以共享为原则、不共享为例外”正是整体政府的体现，一次搜集原则则同时体现了整体政府和平台政府的理念。但目前个人信息保护制度仍是基于传统政府而建构，严格的目的限制原则即是集中体现，即一旦个人信息被用于搜集时所确立目的之外的目的，均要得到授权。因此，有人提出一次搜集原则和目的限制原则存在冲突，〔31〕目的限制原则与整体政府之间存在冲突〔32〕。

〔28〕 参见孟天广：《数字治理生态：数字政府的理论迭代与模型演化》，载《政治学研究》2022 年第 5 期；丁晓东：《从公开到服务：政府数据开放的法理反思与制度完善》，载《法商研究》2022 年第 2 期；Groß/Krellmann，Das Okosystem der Digitalisierung，in：Stember/Eixelsberger/Spichiger/Neuroni/Habbel/・(Hrsg.)，Handbuch E-Government：Technikinduzierte Verwaltungsentwicklung，2019，S. 7.

〔29〕 参见前引〔9〕，Catherine Jasserand 文，第 155 页。

〔30〕 See Thilo Gottschalk，The Data-Laundromat? Public-Private-Partnerships and Publicly Available Data in the Area of Law Enforcement，6 (1) *European Data Protection Law Review* 21，21 (2020).

〔31〕 Vgl. Martini/Wenzel，„Once only“ versus „only once“：Das Prinzip einmaligerErfassung zwischen Zweckbindungsgrundsatz und Bürgerfreundlichkeit，DVBL 132 (2017)，749，749.

〔32〕 参见前引〔7〕，马颜昕、吴敏慧文，第 122 页。

三、风险规制路径下的个人信息保护及其在数字政府中的应用

基于上述分析可发现，数字政府建设与传统个人信息保护制度之间存在内在矛盾，数字政府个人信息保护制度须进行体系性重构。本文提出一种风险规制路径来回应数字政府给个人信息保护制度带来的挑战，认为应以风险控制为导向，坚持适度预防原则，完善风险管理机制，并以风险规制理念重构传统个人信息保护规则。

（一）个人信息保护风险规制模式的提出及其与数字政府的契合

从全球范围来看，个人信息保护可以区分为“权利保护”和“风险管理”这两种模式，各国个人信息保护法均由这两种模式共同构成。权利保护模式起源于“公平信息实践”，随着个人信息保护在宪法层面的不断强化而被日益肯认，尤其是德国法上的信息自决理念和欧盟法上作为基本权利的个人信息保护观念的确立极大巩固了该模式。然而，该模式在如今互联网大数据时代受到越来越多的批判，其制度渊源（公平信息实践）和理论基础（信息自决）均受到各界的集体反思，不仅被认为无法满足时代发展的需求，〔33〕甚至还被批判有损于个人信息保护〔34〕。具体来说，一方面该模式依赖于个人信息主体对数据的控制，而这在互联网大数据时代由于数字技术的飞速发展、数据流动的日益频繁和平台权力的优势地位等因素根本无法真正实现；另一方面该模式使得人们陷入虚幻的安全，误以为对个人信息能够绝对控制，而忽视真正的风险。

在这一大背景下，各国数据保护法又开始了一场个人信息保护的风险革命，〔35〕风险管理的因素被越来越多地融入个人信息保护制度之中，进而形成了个人信息的风险管理模式。GDPR 正是这一观念转变的产物，其中大量规定了风险管理的内容，包括第 24 条规定的数据控制者基于风险的责任、第 25 条规定的通过设计的数据保护和默认的数据保护、第 35 条规定的数据保护影响评估。以上三种机制环环相扣、相互协调，构成了所谓的“风险三角”。〔36〕因此，GDPR 被认为发生了从权利保护法到市场监管法的转型。〔37〕

我国个人信息保护制度的建构过程尽管时间较短，但同样伴随着上述两种模式之间的争论。2016 年出台的《网络安全法》首次以法律形式系统规定个人信息保护制度时，便将知情同意原则作为唯一的个人信息处理合法性基础，充分体现了权利保护模式的理念。而在《中华人民共和国民法典》（以下简称《民法典》）编纂过程之中，在民法学界的大力推动下，个人信息更是被写入《民法典》人格权编，个人信息权有成为一项独立的人格权的趋势，权利保护模式得到进一

〔33〕 See Margot E. Kaminski, The Case for Data Privacy Rights (or, Please, a Little Optimism), 97 (5) *Notre Dame Law Review Reflection* 385 (2022).

〔34〕 See Ari Ezra Waldman, Privacy's Rights Trap, 117 *Northwestern University Law Review Online* 88 (2022).

〔35〕 See Claudia Quelle, The 'Risk Revolution' in EU Data Protection Law: We Can'T Have Our Cake and Eat It, Too, in R Leenes et al. eds., *Data Protection and Privacy: The Age of intelligent Machines*, Hart Publishing, 2017, p. 33.

〔36〕 See Claudia Quelle, Enhancing Compliance under the General Data Protection Regulation: the Risky Upshot of the Accountability-and Risk-based Approach, 9 (3) *European Journal of Risk Regulation* 502, 505 (2018).

〔37〕 Vgl. Schröder,„ Paradim Shift “ im Datenschutzrecht? -Wirtschaftsverwaltungsrechtliche Instrumente in der Datenschutz-Grundverordnung, in: Kronke (Hrsg.), Regulierung in Zeiten der Digitalwirtschaft: Ausgewahlte Fragen des Offentlichen Wirtschafts-, Informations-und Medienrechts, 2019, S. 13f.

步强化。而在《个人信息保护法》立法过程中，《民法典》所秉持的权利保护模式开始受到质疑，越来越多的学者提出风险控制的理念，〔38〕风险管理模式开始形成。至今，尽管《个人信息保护法》已经颁行，但这场争论尚未结束。〔39〕而从《个人信息保护法》的文本来看，立法者采取了折中路线，同时保留了这两种模式。

事实上，无论是权利保护模式还是风险管理模式，均存在利弊之处。尽管与权利保护模式相比，风险管理模式被认为是互联网大数据时代的更优选择，但其仍存在难以克服的不足。风险管理模式依托于元规制的规制理念，主要依赖于企业自身的内部控制，而由于风险概念的不确定性，很可能会导致个人信息保护的不均衡。由于企业占据主导地位，其在自身利益驱动下一旦缺乏刚性监管机制便很容易走向形式主义。对此，不少学者表达了深深的担忧，认为依靠企业自我规制的个人信息保护可能只是“口头上说说而已”，〔40〕甚至沦为一个走过场的纸质清单〔41〕。实践也证明了这种担忧，美国是风险管理模式的代表，尽管各互联网巨头均建立了表面看起来十分完善的风险管理体系，但是个人信息风险事件仍层出不穷。

有鉴于此，近年来越来越多的学者提出个人信息保护的风险规制模式。〔42〕该模式将权利保护和风险管理两种模式有机融合，将个人信息保护视为对数字技术的风险规制，认为个人信息保护制度的根本目的在于规制个人信息处理活动给公民权利、社会利益和国家安全等法益带来的风险。在风险规制模式中，个人信息权利并不被完全放弃，只不过不再被视为一种绝对权利，而是在风险理念下予以重构，被视为风险预防原则的体现和风险规制的工具。〔43〕国内外实务界在落实个人信息原则和保障个人信息权利时同样运用了基于风险的方法，间接证明了这点。不仅如此，通过设计和默认的数据保护，个人信息原则和权利被整合到企业内部风险管理之中，成为数据处理的一部分。在风险规制模式下，无论是权利保护还是风险管理，均服务于个人信息风险的预防，只不过侧重点有所不同：前者是以一种定型化的刚性方式，为个人信息保护划定最低限度的标准，后者则是以量体裁衣的灵活模式，由个人信息处理者根据具体情境自行把控，两者形成了一种相互配合刚柔并济的协作关系。〔44〕不仅如此，风险规制中的公共治理特征，与近年来个人信息保护理论中强调人与人之间关系的集体利益面向呼应。

〔38〕 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；吴伟光：《大数据技术下个人数据信息私权保护论批判》，载《政治与法律》2016 年第 7 期；周汉华：《个人信息保护的法律定位》，载《法商研究》2020 年第 3 期。

〔39〕 参见刘权：《个人信息保护的权利化分歧及其化解》，载《中国法律评论》2022 年第 6 期。

〔40〕 参见前引〔36〕，Claudia Quelle 文，第 524 页。

〔41〕 See Bert-Jaap Koops, The Trouble with European Data Protection Law, 4 (4) *International Data Privacy Law* 250, 255 (2014).

〔42〕 See Alessandro Spina, A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics, 8 (1) *European Journal of Risk Regulation* 88 (2017); Maximilian von Grafenstein, Refining the Concept of the Right to Data Protection in Article 8 ECFR-Part II: Controlling Risk through (Not to) Article 8 ECFR against Other Fundamental Rights, 7 (2) *European Data Protection Law Review* 190 (2021).

〔43〕 参见王锡锌：《重思个人信息权利束的保障机制：行政监管还是民事诉讼》，载《法学研究》2022 年第 5 期。

〔44〕 See Raphaël Gellert, We Have always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-based and the Risk-based Approaches to Data Protection, 2 (4) *European Data Protection Law Review* 481, 481 (2016).

本文认为，为了解决上文所述数字政府给个人信息保护带来的挑战，应以风险规制模式指导数字政府个人信息保护制度的建构。风险规制模式不仅是目前世界范围内个人信息保护的最优路径，而且能够为一体调整模式提供法理基础。近年来，世界范围内一体调整模式正在成为主流。在德国，尽管存在专门的公共部门数据保护规则，但是其和私人部门保护规则存在同构性。而在日本，分别立法模式也被转化为一体调整模式。这在风险规制模式下很容易理解，因为无论是私人部门还是公共部门的个人信息保护制度，其功能均在于规制数字技术带来的风险。风险规制模式不过分强调公共部门与私人部门之间的差异，而是侧重于在数字生态系统下数字风险本身的防范。正如德国联邦内政部在其发布的《数据保护法的现代化》报告中指出的那样，“一般数据保护原则同样适用于公共部门和非公共部门”，因为“在这两个领域必须保证同等的数据保护水平，这取决于风险而非领域”〔45〕。

（二）数字政府个人信息保护风险规制模式的建构

根据风险规制的理论与实践，风险规制是一种面向不确定性的规制，预防原则是其核心原则，风险管理、风险评价和风险交流是其主要内容，去中心化规制、试验规制、回应规制、技术规制、情境规制和独立规制机构是其规制特征，法律的不完整性与诸如标准等软法的突出地位是其表现形式。事实上，越来越多的研究和实践表明，目前个人信息保护法已经高度体现出了上述特征。考虑到数字政府本身的特点，本文就如何建构数字政府个人信息保护风险规制模式提出如下建议：

1. 数字政府个人信息保护风险预防原则的妥当运用

风险预防原则是要求决策者对不确定性引发的问题保持特殊注意的一项原则，〔46〕是风险规制的基本原则。近年来，越来越多的学者主张将风险预防原则引入个人信息保护制度之中。〔47〕其核心要义是于风险不确定之时即采取预防措施，这实际上早已在各国数据保护法之中充分体现。无论是传统个人信息保护原则，包括知情同意原则、目的限制原则、最小必要原则，还是新兴个人信息风险管理机制，例如个人信息保护影响评估，以及通过设计的个人信息保护，均是在风险尚未确定时即对数据处理活动进行限制，具有风险预防的功能。风险预防原则同样具有阻碍创新和限制产业的风险，因而也受到各界的诸多批评。在数字经济语境下，过于严苛的风险预防原则会阻碍数字技术的进步和数字经济的发展，如何平衡安全和创新之间的关系成为妥当运用风险预防原则的关键。德国学者将基于风险的路径与风险预防原则比较，在承认两者具有高度相似性的同时，指出前者由于风险评估等机制比后者更加精确。〔48〕风险预防原则被学界指责过于粗糙，因而也正在朝精细化的方向发展，例如苏宇提出在风险预防原则之中引入等级化或概率化的

〔45〕 Vgl. Roßnagel/Pfitzmann/Garstka, Modernisierung des Datenschutzrechtes-Gutachten im Auftrag des Bundesministeriums des Innern, 2001, Bundesministerium des Innern, S. 14.

〔46〕 参见赵鹏：《风险、不确定性与风险预防原则——一个行政法视角的考察》，载《行政法论丛》第 12 卷，法律出版社 2009 年版，第 105 页。

〔47〕 See Raphaël Gellert, Data Protection: a Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative, 5 (1) *International Data Privacy Law* 3 (2015); Joanna Mazur, Automated Decision-making and the Precautionary Principle in EU Law, 9 (4) *TalTech Journal of European Studies* 3 (2019).

〔48〕 Vgl. Appel/Mielke, Strategien Der Risikoregulierung: Bedeutung und Funktion eines Risk-Based Approach bei der Regulierung im Umweltrecht, 2014, S. 17 - 32.

合比例性要求，普遍建立反向证明机制及风险预防措施动态调整机制。如此精细化的风险预防原则和基于风险的路径殊途同归。〔49〕

具体来说，政府引入数字技术时应进行充分的风险评价和分析，在证明确实存在高度不确定风险时应适用严格的风险预防原则。近年来，人脸识别技术在国内外私人部门和公共部门都得到日益广泛的应用。作为一项新技术，人脸识别的风险具有高度的不确定性，其造成的损害一旦发生很可能难以挽回。对于这种存在巨大不确定性风险的新技术，政府有义务基于风险预防原则限制其使用。除此之外，对于大规模政务数据共享平台的建立，也应严格进行风险评价和分析，如果没有切实可行的数据安全与个人信息保护保障机制，集中化数据库会带来大量数据泄露风险，此时应考虑适用风险预防原则。〔50〕

2. 数字政府个人信息主体权利的风险化解释与调适

权利保护路径不应被完全放弃，其在目前仍具有不可替代的功能，但在大数据互联网经济的时代背景下应发生风险化转型，即以风险管理的理念对其予以解释和调适。这一做法不仅在理论上被不少学者所主张，在实践中也已经广泛运用。具体来说，在落实个人信息保护原则和保障个人信息权利时，应将它们视为风险规制的工具进而采取基于风险的方法，结合具体场景进行风险与收益的权衡，并通过法律、管理和技术的手段将其融入个人信息处理者风险管理之中。

对于数字政府语境下个人信息的判定，也应结合场景根据风险管理的方法展开。将匿名化的信息视为非个人信息是全球数据保护的通行做法，匿名化成为区分个人信息与非个人信息的关键。而如何认定匿名化在实践中遭遇了难题，这是因为其是一个具有较大弹性的相对概念，最终的判断只能是一项风险收益的权衡。〔51〕 尽管匿名化措施能够在一定程度上降低个人信息风险，但绝对的匿名化在技术上不可能实现，且会损耗数据的使用价值，带来不菲的技术成本。如果数据进入公共领域，即便经过匿名化处理，其所面临的风险也更高。因此，在数字政府语境下，公共数据开放中的匿名化要求应比行政机关数据共享中更为严格。

就知情同意原则来说，同意机制在私人部门语境下尽管遭遇困境，但通过风险化转型仍能发挥重要作用。但是在数字政府语境下，其不仅面临互联网大数据时代的技术挑战，还受到公权力强制性和非对等性的侵蚀，进而基本丧失功能，甚至可能成为滥用数据权力的工具。不过本文认为，即便在数字政府语境下，同意机制也不应完全放弃，在服务行政领域仍有适用余地。此时同意机制构成了风险规制中的公众参与机制，即让公民自行决定是否承担个人信息风险。〔52〕 知情权则仍发挥着风险交流作用，我国《个人信息保护法》也采取了保留知情权废除同意机制的做法。在数字政府语境下，知情权保障尤为重要，只有为了保障重要的法益才能被限制，且应符合法律保留和比例原则等法律原则的要求。

就目的限制原则来说，其尽管同样在互联网大数据时代由于阻碍数据治理和数字技术革新受

〔49〕 参见苏宇：《风险预防原则的结构化阐释》，载《法学研究》2021 年第 1 期。

〔50〕 参见邢会强：《政务数据共享与个人信息保护》，载《行政法学研究》2023 年第 2 期。

〔51〕 See Michèle Finck & Frank Pallas, They Who Must Not be Identified-distinguishing Personal from Non-personal Data under the GDPR, 10 (1) *International Data Privacy Law* 11, 11 (2020).

〔52〕 参见前引〔47〕，Raphaël Gellert 文，第 10 页。

到越来越多的批判，但是对于对抗数据权力、降低个人信息风险和保障公民基本权利来说发挥着关键作用，〔53〕尤其在数字政府中没有同意机制的情况下其重要性更加凸显。不过，为了避免目的限制原则过于僵化，应对其予以风险化转型，即放弃传统权利保护理念下的严格立场，而转向风险管理路径下的场景分析。此时目的限制原则构成了一种风险预防机制，即在风险尚未成为现实危害之前提前采取预防措施。在数字政府语境下，目的限制原则的适用同样应结合具体场景展开风险收益权衡。例如在反恐等涉及大量公民生命权等重要法益的情况下，可以考虑适当突破目的限制原则的要求，但仍应严格遵循比例原则和法律保留原则的要求，并采取法律、管理和技术等方面措施尽可能将风险降低。除此之外，目的限制原则应融入政府个人信息合规管理流程之中，成为内部风险管理机制的组成部分。罗斯纳格尔（Roßnagel）教授专门指出，目的限制原则与数字政府之间的矛盾可以通过诸如内部权限管理这样的适法技术架构来克服。〔54〕

把目光投向个人信息权利，也可以得出类似的结论。个人信息权利并非实现个人对其数据控制的工具，而是风险规制手段。与知情同意一样，查阅复制权、删除权和解释说明权仍是实现风险交流和公众参与的方式，而更正补充权则是为了避免数据错误所带来的风险。在这种风险规制路径下，个人信息权利只能在风险规制之中发挥次要作用。为了真正规制风险，政府应起到首要作用，主动承担风险交流责任，推动公众参与，而不是被动地等待公民主张自身权利。实践表明，个人信息权利在公共部门所发挥的作用有限，公民向政府主张个人信息权利的积极性不高。在欧盟，有学者指出，为了实现更好的个人信息保护，较少关注个人信息主体的权利似乎有违直觉，但是从实际角度来看可能更为现实。〔55〕以解释权为例，政府应主动履行风险交流义务，向社会公众解释数据治理中算法的风险，解释权所能发挥的作用十分有限，〔56〕这种义务应成为政府个人信息合规管理的组成部分。

3. 数字政府个人信息保护风险管理制度的稳步建构

《个人信息保护法》出台后，我国企业纷纷开始建立个人信息保护合规管理体系。尤其是对于大型个人信息处理者来说，建立个人信息保护合规管理体系是实现数据合规的必备之举。因此，《个人信息保护法》在第 58 条第 1 项对超大互联网平台课以“建立健全个人信息保护合规制度体系”的义务。正如前文所指出的那样，数字政府具有整体性和协同性特征，属于大型个人信息处理者，参考《个人信息保护法》第 58 条的规定同样具有建立个人信息保护合规管理体系的义务。然而从目前来看，我国尚没有政府尝试建立个人信息保护合规管理体系，更多的是建立政务数据安全治理体系。尽管这两者之间存在共同之处，例如均属于风险管理活动，但是仍存在不少差异，前者主要围绕权利展开具有法律面向，而后者则围绕安全展开以技术面向为主。今后应努力在政务数据安全治理体系之中融入个人信息保护合规内容，着重从如下几点入手：

---

〔53〕 See Isabel Hahn, Purpose Limitation in the Time of Data Power: Is There a Way Forward?, 7 (1) *European Data Protection Law Review* 31, 31 (2021).

〔54〕 参见前引〔5〕，Roßnagel、Laue 文，第 549 页。

〔55〕 参见前引〔8〕，Mark Leiser、Bart Custers 文，第 378 页。

〔56〕 See Lilian Edwards & Michael Veale, Slave to the Algorithm? Why a ‘Right to an Explanation’ Is Probably Not the Remedy You Are Looking for, 16 (1) *Duke Law & Technology Review* 18, 18 (2017).

（1）完善数字政府个人信息保护合规管理。其一，设置专门个人信息保护负责人。《个人信息保护法》第52条规定，处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人。如果严格根据一体调整原则，绝大多数政府处理个人信息均能达到国家网信部门规定数量，应指定个人信息保护负责人。从目前我国各地数字政府情况来看，不少地方开始探索设置政府首席数据官，而其主要职能在于数据治理，并不具有个人信息保护职责。在欧盟法中，GDPR也要求公共部门设立数据保护官。2022年5月31日，法国国家信息保护委员会（CNIL）向法国22个城市发出通知，要求22个城市的地方政府必须在4个月内任命一名数据保护官（DPO），以符合GDPR的规定。在德国，设置数据保护官对于公共部门来说是一项强制性义务，而对于私人部门仅是一项自愿性义务。公共部门机构普遍设立了数据保护官，各州数据保护法均对数据保护官的任命、权限和职责问题进行了详细规定。这一模式未来也值得我国借鉴，未来可以考虑由政府首席数据官进一步承担个人信息保护职责，不过最优路径仍是设置专门的政府个人信息保护负责人。

其二，加强数字政府个人信息合规管理体系建设。私人部门丰富的个人信息合规管理实践经验为公共部门提供了参考，我国政务数据安全治理体系也基本包括了数据分级分类制度、内部管理制度和操作规范、安全技术使用规范、数据安全培训制度、安全审查和审计制度、第三方管理制度和突发事件应急管理制度。上述制度可以适用于个人信息保护，但并未充分考虑个人信息保护的特殊性。就目前来说，一方面应在政务数据安全治理体系之中融入个人信息合规管理，例如将个人信息纳入数据分级分类制度，在数据安全审计中纳入个人信息保护指标等；另一方面，还应结合个人信息保护特殊性建立一些专门的个人信息保护合规管理机制，例如个人信息保护投诉举报机制、个人信息权利响应机制、个人信息风险交流机制和个人信息跨境管理机制等。

其三，加强政府工作人员个人信息保护培训工作，建设公共部门个人信息保护合规文化，尤其应强化领导干部个人信息保护意识。个人信息保护工作高度依赖于人的观念、意识和知识，因此各国均高度重视个人信息保护培训工作和合规文化建设。就目前来说，我国针对政府首席数据官的培训工作在个别地方已经展开，但是个人信息保护并未成为重点授课内容。通过个人信息保护培训，能够强化政府工作人员的个人信息保护知识和技能，提升个人信息保护意识，进而在整个系统形成隐私和个人信息保护的文化。

（2）应建立政府个人信息风险评估机制。《个人信息保护法》第55条和第56条确立了个人信息保护影响评估制度，尽管该条文似乎是针对私人部门设计，但无论从法理还是域外实践来看，其应同样适用于公共部门。〔57〕随着数字政府建设的推进，大数据技术应用越来越广泛，政府个人信息处理活动的风险也与日俱增，不少风险存在不确定性，有必要予以评估。尽管我国政务数据安全治理体系之中已经包括数据安全风险评估，不少地方公共数据管理办法也规定了公共数据安全风险评估，但这并不意味着没有必要建立个人信息风险评估机制。前者仅能从技术角度对安全风险予以测评，而后者则是直接全面深入地对个人处理活动对公民权利、社会利益和国家

〔57〕 参见刘权：《论个人信息保护影响评估——以〈个人信息保护法〉第55、56条为中心》，载《上海交通大学学报（哲学社会科学版）》2022年第5期。

安全可能带来的风险进行分析。

（3）建立政府个人信息保护风险交流机制。风险交流是指风险信息的沟通，在风险规制中具有不可或缺的作用。[58] 具体来说，是由政府机构主导，在专家和公众之间建立一定的交流平台，如互联网、媒体等，使专家和公众可以相互交换风险信息和观点，在帮助公众克服风险信息认知中的障碍和偏见的同时，也使公众对风险认知的一些价值判断成为风险规制机构作出风险决策的考量因素，从而弥补专家知识与公众认知之间的信息不对称。作为一种风险规制机制，个人信息保护也有必要引入风险交流机制。个人信息风险交流的不顺畅，也可能像环境领域那样引发激烈的、具有潜在破坏性的社会抗争活动。近年来，美国多个地区先后发生了大规模的反对人脸识别的游行示威，这是各地出台立法禁止人脸识别技术应用的重要原因之一，亚马逊、IBM、微软等公司都宣布终止了人脸识别产品的销售。

我国应从如下方面建构数字政府个人信息保护风险交流机制：首先，建立个人信息保护风险交流的责任机制。须明确的是，对于数字政府个人信息保护风险交流，政府应承担主体责任。而在政府内部，个人信息保护监管部门应成为风险交流的组织者，明确各方责任，为利益相关者的风险交流搭建平台。各地方政府和政府部门应由个人信息保护负责人作为风险交流执行者，向社会公众传递和提示个人信息保护风险，并向个人信息保护监管部门传递个人信息保护风险信息。其次，探索个人信息风险交流工具。要建立个人信息保护风险交流机制，还应努力探索合适的风险交流工具。从域外经验来看，风险信息交流主要是通过软法实现。在数字政府个人信息保护之中，也应充分发挥软法作用实现风险信息交流，例如制定《政府个人信息风险交流指南》。对于大规模搜集个人信息的公共服务应用，应向社会发布个人信息保护风险情况。最后，发挥专家在风险交流中的作用。作为“诚实的代理人”，专家既可为规制者服务，也可为被规制企业、利害关系方或一般公众服务。[59]

（4）加强个人信息保护风险规制中的公众参与。公众参与也是风险规制活动中的必备要素，其与风险交流存在密切关联，但也存在区别，两者容易混淆。风险交流侧重对风险信息的沟通，包括社会公众对风险信息的了解，而公众参与则在风险交流基础之上更进一步，强调社会公众参与风险规制决策。在数字政府建构中，有学者提出在政府中心主义路径之外借助数字技术的力量采取市民授权机制，[60] 通过个人信息的公共信托和数据合作社等形式使利益相关者参与到数据治理体系之中，[61] 这本质上是一种电子化的公众参与形式，在今后数字政府建设中可以探索采用。

4. 数字政府个人信息保护风险规制策略的灵活使用

从规制策略上来说，风险规制具有合作规制、独立规制机构、技术治理、回应治理、试验规制、软法之治和情境规制等诸多特征，这些规制策略对于数字政府个人信息保护建构来说也颇有

〔58〕 参见沈岿：《风险交流的软法构建》，载《清华法学》2015 年第 6 期。

〔59〕 参见金自宁：《风险规制中的信息沟通及其制度建构》，载《北京行政学院学报》2012 年第 5 期。

〔60〕 参见高翔：《超越政府中心主义：公共数据治理中的市民授权机制》，载《治理研究》2022 年第 2 期。

〔61〕 参见王锡锌：《数治与法治：数字行政的法治约束》，载《中国人民大学学报》2022 年第 6 期。

借鉴意义。

就合作规制来说，上述风险交流和公众参与，以及政务个人信息保护的政企合作均是合作规制的重要面向，即政府、企业和公民共同参与到政府个人信息保护的风险规制之中。除此之外，作为合作规制表现形式的公共部门的私人规制，〔62〕即通过私人规制公共部门的活动，在数字政府个人信息保护之中也应有所体现。例如可以鼓励多方主体参与推动数字政府个人信息保护国家标准、地方标准和团体标准等标准制定工作，考虑在法治政府评估指标体系中引入个人信息保护合规指标。

因为风险规制往往针对科技创新而开展，而科技一直处于高速发展之中，加上风险具有高度不确定性，所以回应规制和试验规制也构成了风险规制的惯常规制策略。〔63〕在数字政府建构中，诸多数字技术不断引入并更新迭代，这是个人信息风险的主要来源。为了应对数字技术所带来的不确定性风险，回应规制和试验规制的规制策略不可或缺。具体来说，应针对不断更新的数字技术及时通过试点和监管沙盒等形式探索与之匹配的规制机制。例如，近年来区块链和云计算技术在数字政府中的引入给个人信息保护带来挑战，应及时采取法律和技术的应对措施进行回应。欧盟在2022年计划系统解决公共部门云服务数据合规问题，尤其是云服务中的控制者和处理者关系与数据国际传输问题。

就软法之治来说，一直以来诸如标准这样的软法在风险规制领域扮演着尤为重要的角色。这在个人信息保护领域同样如此，有学者指出数据保护立法的非完全性，而这种非完全性在很多情况下正是通过标准的形式来补充。以我国《个人信息保护法》的实施为例，标准在个人信息保护合规实践中发挥着不亚于《个人信息保护法》本身的作用。目前，数字政府数据安全与个人信息保护的标准起草工作正在进行之中，尚没有专门政务领域的个人信息保护标准，现有标准中关于个人信息保护的内容也较少。从风险规制原理来说，个人信息保护法律制度供给的不足是一种合理状态，因为这更多需要软法来补足。公共部门个人信息保护制度的建构同样如此，未来应加强数字政府个人信息保护标准建设。不过值得注意的是，对于警察与刑事司法这样高权性较强的领域，应遵循严格的法律保留原则，禁止通过标准的形式规定个人信息保护规则。〔64〕

就技术治理来说，技术治理是风险规制的重要特征，通过设计的保护（Protection by Design）的理念最早兴起于化学监管和药品监管等风险规制领域。〔65〕在私人部门，通过设计的个人信息保护已经成为国内外数据保护的普遍实践，在实现数据合规中发挥着重要作用。对于公共部门个人信息保护来说，该理念也有重要的价值。除此之外，隐私计算通过数据的可用不可见对于目前公共部门和私人部门日益融合的数据治理生态具有巨大的潜力，〔66〕已经在私人部门和

〔62〕 参见〔英〕科林·斯科特：《规制、治理与法律：前沿问题研究》，安永康译，清华大学出版社2018年版，第91页。

〔63〕 参见董正爱、王璐璐：《迈向回应型环境风险法律规制的变革路径——环境治理多元规范体系的法治重构》，载《社会科学研究》2015年第4期。

〔64〕 Vgl. Marsch /Rademacher, Generalklauseln im Datenschutzrecht: Zur Rehabilitierung eines zentralen Bausteins des allgemeinen Informationsverwaltungsrechts, VERW 54 (2021), 1, 35.

〔65〕 See Mirella Miettinen, "By Design" and Risk Regulation: Insights from Nanotechnologies, 12 (4) *European Journal of Risk Regulation* 775, 775 (2021).

〔66〕 参见郑谐维：《隐私计算在政务数据共享中的应用》，载《上海信息化》2022年第4期。

公共部门得到了一定的应用，国务院办公厅印发的《全国一体化政务大数据体系建设指南》多次提及隐私计算技术。技术治理还能够通过技术方案实现更加有效的个人信息保护、风险交流和公众参与。例如私人部门的个人信息管理系统和同意管理工具均可运用于公共部门，公民可在其系统之中管理授权、查看个人信息访问情况和及时更正个人信息，进而能够更好地实现其个人信息权利和获知个人信息风险。

就独立规制机构来说，史蒂芬·布雷耶在论述风险规制体系时，首先提出的建议是建立独立规制机构。〔67〕建立独立规制机构可以说是风险规制的共同特征。作为一种风险规制活动，个人信息保护也有必要建立独立规制机构，这也是全球数据保护监管的一个趋势。〔68〕在域外实践中，数据保护监管机构不仅要负责监督私人企业，而且还要监督公共部门，进而形成政府内规制。〔69〕在欧盟，数据保护监管机构一直以来同样负责监督公共部门的个人信息保护，并在 LED 指令的意见中建议各个成员国成立专门数据保护监管机构，同时负责公共部门和私人部门的个人信息保护监督。欧盟数据保护机构（EDPS）在 2022 年初要求欧洲刑警组织删除与犯罪活动无关联的所有个人信息。日本 2021 年《个人信息保护法》修改过程中，赋予个人信息保护委员会（PPC）监督公共机构的权限。在我国，由于不存在个人信息保护独立监管机构，可以由《个人信息保护法》规定的履行个人信息保护职责的部门对各级政府个人信息保护合规状况进行监督。

四、结　论

对于数字政府个人信息保护制度的建构，学界存在权利保护模式和风险管理模式之间的分歧。本文认为上述两种模式各有利弊，无论何种模式均无法单独担负起个人信息保护的任务，因此提出风险规制模式作为数字政府个人信息保护的理论基础与实践指引。该模式有机整合了权利保护模式和风险管理模式，是个人信息保护制度的最优选择。更为重要的是，风险规制模式着眼于数字政府、数字社会和数字公民构成的数字生态中数字风险的一体化防范，同样适用于数字政府，进而构成了公共部门与私人部门一体调整模式的法理基础。正基于此，私人部门在数字化转型中积累的丰富风险规制经验可以运用到公共部门。

数字政府个人信息保护的风险规制模式，在行政法上还具有更加深远的启发意义。一直以来，传统行政法主要关注外部法律关系，即便是近年来行政法中兴起的规制理论也主要侧重于政府对市场主体的监管。这是因为，在物理世界中，私人部门是主要的风险来源。公共部门对公民的威胁主要来自其高权性，控制权力和保护权利构成传统行政法的核心任务。而随着数字时代的到来，数字技术所带来的风险不仅来自私人部门，而且同样会由公共部门产生。面对公共部门中的数字技术风险，传统行政法中的权力控制和权利保护机制不足以应对，私人部门中的风险规制

〔67〕 参见〔美〕史蒂芬·布雷耶：《打破恶性循环——政府如何有效规制风险》，宋华琳译，法律出版社 2009 年版，第 1 页。
〔68〕 参见高秦伟：《论个人信息保护的专责机关》，载《法学评论》2021 年第 6 期。
〔69〕 参见前引〔62〕，科林·斯科特书，第 9 页。

经验可以发挥重要作用。〔70〕这在不少国家行政管理实践中已经得到印证，公共部门开展风险管理、内部控制和合规管理的现象越来越多，〔71〕在个人信息保护领域尤为明显，这为内部行政法的进一步发展提供了新的素材。

Abstract：The improvement of the personal information protection system in the public sector is the only way to build a digital government ruled by law. China's personal information protection law adopts a declarative legislative model of integrated adjustment of the public and private sectors. At present, it can neither provide sufficient rules and guidance for the protection of personal information in the public sector, nor meet the needs of digital government construction. The construction of personal information protection rules of digital government should not only consider the particularity of the public sector compared with the private sector in personal information processing activities, but also take the innovation of digital government in terms of technology and governance into account, and then formulate special rules. The risk regulation model is not only the trend of personal information protection system worldwide, but also provides a theoretical basis for the integrated adjustment model. Through the proper application of the risk precautionary principle, the risk interpretation and adjustment of personal information rights, the flexible use of risk regulation mechanisms such as risk management, risk communication and risk evaluation, and the joint use of risk regulation strategies such as cooperative governance, independent regulatory institutions, technical governance, responsive governance, experimental regulation and soft law governance, it is the best choice for our country to construct a risk regulation-oriented digital government personal information protection mechanism.

Key Words：digital government, personal information protection, risk regulation

（责任编辑：刘　权　赵建蕊）

〔70〕 Vgl. Englisch/Schuh, Algorithmengestützte Verwaltungsverfahren-Einsatzfelder, Risiken und Notwendigkeit ergänzender Kontrollen, VERW 55 (2022), 155, 189.

〔71〕 Vgl. Stober/Ohrtmann, Compliance: Handbuch für die öffentliche Verwaltung, 2015.

财经法学 No. 5，2022
pp. 81 - 94

论超大型平台独立机构的功能构造
——以《个人信息保护法》第58条为中心

韩　阳*

内容提要：《个人信息保护法》第58条第1项规定超大型平台企业应成立主要由外部成员组成的独立机构对个人信息保护情况进行监督，目前存在三种制度设计方案。第三方独立机构方案比较优势不明显，不符合风险预防理念，难以承载监督功能期待，因此应当被舍弃。管理监督型独立机构方案属于日常性合规管理模式，是董事会对经理层的管理监督，独立机构在董事会领导下开展活动，无法解决合规动力问题，难以厘清董事会与执法机构之间的紧张关系。决策监督型独立机构方案属于危机性合规整改模式，是执法机构对董事会的整改督导，组建董事会专门委员会，依托独立董事进行内部控制，但独立董事法律责任模糊，容易造成董事会负担过重。两种方案各有优劣侧重，应当区分问题场景分别应用，实现对公民个人信息的系统性和持续性保护。

关键词：超大型平台　独立机构　管理监督　决策监督

一、问题的提出

为加强超大型平台监管，我国《个人信息保护法》新增了独立机构这一制度要求。《个人信息保护法》第58条第1项规定，提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督。问题随之而来：独立机构的功能定位、人员构成、权利义务和法律责任应如何设计？怎样保持该机构的独立性？如何实现有效监督？本文尝试对此进行探索。

为什么要求超大型平台成立独立的监督机构？与个人信息保护负责人是什么关系？缘何独立

* 韩阳，北京大学法学院博士研究生。

机构主要由外部成员组成呢？对于这些问题，立法资料显示“有的部门、专家建议，强化超大型互联网平台的个人信息保护义务，并加强监督”，全国人大宪法和法律委员会经研究建议增加这一款。〔1〕2021 年 8 月 20 日，经过三次审议，十三届全国人大常委会第三十次会议表决通过了《个人信息保护法》，全国人大常委会法工委经济法室副主任杨合庆对《个人信息保护法》进行了解读。他表示：“为了提高大型互联网平台经营业务的透明度，完善平台治理，强化外部监督，形成全社会共同参与的个人信息保护机制……个人信息保护法对这些大型互联网平台设定了特别的个人信息保护义务。”〔2〕由此可见，我国立法机关将独立机构的功能定位为外部监督，通过多元主体参与构建平台治理的开放式关系结构。

从法律条文看，独立和监督是该机构的两个显著特征，外部是对组成人员的要求。监督是该机构的功能定性，是设计这一机构的出发点和落脚点。独立性包含组织独立、职权独立和人员独立三个方面。只有在监督者和监督对象都明确的前提下，是否独立才能够最终研判。如何实现独立监督呢？学界和实践中存在三种方案，分别是第三方独立机构方案、管理监督型独立机构方案和决策监督型独立机构方案，以下分别进行讨论。部分方案内容较少，本文尝试进行拓展并做利弊分析。

二、第三方独立机构方案

在《个人信息保护法》生效前，部分超大型平台企业已经进行了初步尝试。腾讯在 2021 年 10 月 15 日公开招募外部成员，组建个人信息保护外部监督委员会，文字表述为“第三方独立监督机构”，职责包括独立评议腾讯公司及各产品隐私保护相关工作、提出指导和修改建议等。“委员会首批成员为 15 个人左右，计划包括法学专家、技术专家与行业协会等个人信息保护领域的专业人士，也将涵盖律师、媒体等其他公众。首批成员将通过公开招募和定向邀请等方式产生。”〔3〕携程在 2021 年 10 月 25 日发布公告，决定近期成立“个人信息保护外部监督专家团”，同样表述为“第三方独立机构”。〔4〕在外部监督的功能定位下，超大型平台希望通过第三方独立机构的形式实现外部监督效果，将独立性理解为“外部独立”，监督机构独立于本平台企业。但这种做法比较优势并不明显，不符合风险预防的治理理念。

第一，《个人信息保护法》第六章专门规定了履行个人信息保护职责的部门，这些职能部门完全独立于企业，属于纯粹外部监督的国家机构。无论立法目的追求的是“独立性”或是“监督性”，负有监管职责的国家机关都是最佳主体，而不是所谓的第三方独立机构。近年来行政执法强调柔性执法和治理导向，存在许多企业发声和公众参与的合法渠道。反观这些所谓的独立机

〔1〕 参见《全国人民代表大会宪法和法律委员会关于〈中华人民共和国个人信息保护法（草案）〉修改情况的汇报》。

〔2〕 朱宁宁：《8 章 74 条，个人信息保护法来了！权威解读十大亮点》，载 https://mp.weixin.qq.com/s/Y-031EBzOsbbN2JAEcOGBQ，最后访问时间：2022 年 7 月 23 日。

〔3〕《这是一封来自鹅厂隐私官的邀请函，请查收！》，载 https://mp.weixin.qq.com/s/2ZvcExeY_l-J3dfw02zTFg，最后访问时间：2022 年 7 月 23 日。

〔4〕 参见《携程“个人信息保护外部监督专家团”招募公告》，载 https://view.inews.qq.com/a/20211025A093AW00，最后访问时间：2022 年 7 月 23 日。

构，实际上难以摆脱超大型平台的干扰，平台企业主导之下的民主参与和监督强度都存在问题。用户代表或公众代表的产生，专家学者的挑选，都有可能被超大型平台把持，使所谓的独立监督机构沦为平台权力的装饰。

第二，即便追求平台治理的多元参与，实际上也并无必要。现实中已经广泛存在着第三方独立机构，各类行业协会、学会智库和科研高校等等，如在 APP 专项整治活动中发挥作用的中国网络空间安全协会，每年发布个人信息保护测评报告的北京大学互联网法律中心。这些机构或独立存在，或由政产学研媒一同发起成立，各大头部平台企业也参与其中。它们定期发布研究报告，组织企业调研、立法研讨和独立监督，实际上已经发挥了社会监督的客观作用。这些社会组织通过内部章程对成员形成约束力，通过法律程序获得登记备案，不需要专门立法予以合法性确认。这些社会组织的经费人员更具有独立性，它们通过声誉机制和竞争机制进行自我监督，相较企业自设机构具有一定的制度优势。

第三，外部监督无法实现事前事中监管，难以有效影响超大型平台企业决策。如果按照两家企业的制度设想展开，独立机构对超大型平台进行形式监督，仅仅作出指导、提出建议和咨询培训，那么独立机构极容易沦为装饰企业形象的花瓶，监督功能将被完全掏空。独立机构无法深入平台企业内部决策，否则就将与外部监督的职能定位相冲突。超大型平台企业的各种业务和不同流程都与个人信息有关，个人信息被滥用有时候只是一个最终结果，更多问题可能出在事前决策和事中执行。尤其是很多敏感个人信息，如生物识别信息，一旦被泄露滥用将会给自然人带来不确定风险。有学者提出：“区别于传统的‘危险’，个人生物识别信息应用风险具有不确定性与复杂性，因果关系具有模糊性与非线性，损害具有严重性与不可逆性，因此政府监管理念应当从消极的‘危险消除’向积极的‘风险预防’转变。”〔5〕

三、管理监督型独立机构方案

该方案由张新宝教授提出，主张“作为企业内部的‘独立监督机构’，主要是指独立于企业的日常经营管理机构（如总经理）、产品或者服务研发推广机构等业务部门，因为这些机构和部门往往会以利润导向进行管理和经营而忽视个人信息保护”〔6〕。该方案下独立机构包含两项具体职责：其一，监督大型互联网平台企业自身的个人信息保护合规情况；其二，监督大型互联网企业对商业用户的个人信息处理活动予以规范的合规情况。〔7〕除此之外，独立机构在董事会的领导下，还有提出建议和合规指导的功能。超大型平台的业务部门是该方案的预设监督对象，本质是董事会对经理层的管理监督。数据合规在我国仍处于发展初期，该方案有助于专家参与企业合规制度建立，同时制度上防范经理层和业务部门的数据滥用行为，方案内容丰富具有很强的操作性和执行性。在讨论独立机构与国家个人信息保护部门的关系时，张新宝教授主张：“独立监督机构对企业个人信息保护事项作出的决定或者提出的鉴定意见，原则上将得到国家个人信息保护

〔5〕 于洋：《论个人生物识别信息应用风险的监管构造》，载《行政法学研究》2021 年第 6 期，第 111 页。
〔6〕 张新宝：《大型互联网平台企业个人信息保护独立监督机构研究》，载《东方法学》2022 年第 4 期，第 44 页。
〔7〕 参见前引〔6〕，张新宝文。

部门的认可。在发现企业在个人信息保护方面存在重大隐患或者严重违法情形时，独立监督机构应当及时向企业的权力机构提出意见和建议。企业权力机构拒绝接受的，经独立监督机构多数成员表决同意，应将相关情况报告国家个人信息保护部门。”〔8〕这一制度设计极大增强了独立机构的实际权力，仿佛达摩克利斯之剑一样悬在超大型平台企业头顶。但是产生两个问题需要解释：第一，如果独立机构受董事会领导，为什么决定和鉴定意见要征得监管部门认可，为什么可以越过董事会，直接向监管部门报告；第二，如果独立机构照此运行，会不会干扰企业的自主经营活动。

在规制理论中，该方案属于内部管理型规制理论（management-based regulation）〔9〕的实际运用，“实际上是行政权对企业内部治理的介入，在实质上构成对企业经营自主权的限制”〔10〕。对于内部管理型规制，国外学者将生产流程划分为规划、执行和产出三个部分，在不同阶段采取的规制策略，被称作内部管理型规制、技术标准规制（technology-based regulation）和绩效标准规制（outcome-based regulation）。根据内部管理型规制，公司应制定符合一般标准的计划，以促进有针对性的社会目标。监管标准规定了每个计划应该具备的要素，如危险识别、风险防范措施、监测纠正程序、员工培训政策，以及其他社会目标评估和完善公司管理的具体措施。〔11〕“内部管理型规制不规定特定的技术要求或绩效结果，而是要求企业针对行政目标，制定适合自身的内部经营计划、管理流程及决策规则，从而将社会价值内部化。”〔12〕这一规制类型属于元规制（meta regulation）的典型类型，与自我规制具有高度关联性。“元规制是指外部规制者有意促使规制对象本身针对公共问题，作出内部式的、自我规制性质的回应，来要求或塑造规制对象的自我规制。”〔13〕

结合内部规制理论，该方案具有三点积极意义：第一，针对个人信息风险，应该采用风险预防的规制策略。“互联网的复杂结构以及大数据处理过程随机性、相对性和模糊性特征，表明数据主体基于个人信息与数据控制者建立的信息关系影响因素存在高度的不确定性。传统规制模式以规则为规制工具，通过行为和结果的确定性联系进行危险排除，并不符合数字时代信息分享的风险特征。”〔14〕第二，当风险不明、标准不清时，实际上难以判断个人信息是否被滥用泄露，事后监督难以挽回实际损失。需要深入平台企业内部，对个人信息管理体系进行优化改造，政府规制视角应该由外入内。第三，个人信息保护问题异质性强，平台、部门和流程之间都不一样，需要编制细密的行动规范。但是，个人信息保护法律制度建立初期，诸多制度细节、技术标准和行

〔8〕 前引〔6〕，张新宝文，第 48 页。

〔9〕 也有学者将其翻译为“以管理为基础的规制”或“基于管理的规制”。参见洪延青：《“以管理为基础的规制”——对网络运营者安全保护义务的重构》，载《环球法律评论》2016 年第 4 期；高秦伟：《社会自我规制与行政法的任务》，载《中国法学》2015 年第 5 期。

〔10〕 孔祥稳：《论个人信息保护的行政规制路径》，载《行政法学研究》2022 年第 1 期，第 144 页。

〔11〕 See Cary Coglianese & David Lazer, Management-Based Regulation: Prescribing Private Management to Achieve Public Goals, 37 *Law & Society Review* 694 (2003).

〔12〕 谭冰霖：《论政府对企业的内部管理型规制》，载《法学家》2019 年第 6 期，第 75 页。

〔13〕〔英〕罗伯特·鲍德温、马丁·凯夫、马丁·洛奇：《牛津规制手册》，宋华琳等译，上海三联书店 2017 年版，第 167 页。

〔14〕 谢尧雯：《基于数字信任维系的个人信息保护路径》，载《浙江学刊》2021 年第 4 期，第 82 页。

业要求都需要进一步明确。因此，应将规则自由裁量权下放给企业，监管机构不宜采取硬标准强要求。

但是，运用内部规制理论分析建构超大型平台独立机构，存在固有缺陷难以克服。内部管理型规制本质上仍是一种外部监督，无法解决合规动机问题。经过与监管机构的沟通确认，企业制定实施了各类内部管理制度，既有可能出于提升公司绩效考虑，也可能是为了应付检查粉饰门面。企业并非自发遵守合规计划，而是考虑制度成本、外界压力和管理层意见。制度运行成本较低，契合企业盈利模式，得到管理层的支持，内部管理制度可以有效运行；但如果遇到任何一个障碍，内部管理制度运行就可能是“部分的、象征性和半心半意（half-heated）”。〔15〕监管者真正应该关心的是企业管理的实际行动，而不是浮于表面的规章制度，“管理远比管理体系重要”〔16〕。对企业行为的规制，仅仅停留在管理制度上是不够的，需要干预企业管理层或控股股东的合规动机。在这个层面上独立机构的监督职能或许更有意义。

2019 年 7 月美国联邦贸易委员会（FTC）对脸书（Facebook）达成新的和解令，以惩罚脸书违反 2012 年和解令中“禁止虚假陈述”的要求。除了开具 50 亿美元的天价罚单，2019 年和解令还要求脸书改变其董事会构成，设立专门独立隐私委员会。它的所有成员都必须是独立董事，由独立提名委员会产生，每年至少召开 4 次会议。有权任命或免职隐私合规官，每 12 个月审核隐私合规官提交的隐私计划执行情况书面说明。有权任命或免职第三方隐私评估机构，每季度应在没有管理层出席的情况下与其举行会议。每季度审核管理层提交的简报，内容涵盖隐私计划状态、和解令执行情况和存在重大风险情况等等。〔17〕美国联邦贸易委员会的执法意图十分明确，约束限制管理层尤其是控股股东扎克伯格在隐私方面的权力。委员会委员罗希特·乔普拉（Rohit Chopra）发表声明称，脸书通过对外销售用户的行为数据换取广告收入，有强烈的动机获取越来越多的用户数据。只要广告商愿意为用户消费特定内容付费，像脸书这样的公司就有动机以影响用户的心理状态和实时偏好的方式来管理内容。作为一家上市公司，脸书需要与利润丰厚的第三方开发者保持合作，实现公司利益的最大化。〔18〕委员会主席乔·西蒙斯（Joe Simons）和委员诺亚·约书亚·菲利普斯（Noah Joshua Phillips）、克里斯汀·S·威尔逊（Christine S. Wilson）发布声明称，该命令消除了扎克伯格单方面做出隐私决策的能力，赋予业务部门、首席隐私官和隐私委员会相关责任。尽管没有移除扎克伯格对董事会的全部控制权力，但明显地削弱了他的权力，这是迄今为止世界上没有哪个监管机构能做到的。〔19〕

〔15〕 See Christine Parker & Vibeke Lehmann Neelsen, Do Businesses Take Compliance Systems Seriously? An Empirical Study of Implementation of Trade Practices Compliance Systems in Australia, 30 *Melbourne University Law Review* 441 (2006).

〔16〕 前引〔13〕，罗伯特·鲍德温、马丁·凯夫、马丁·洛奇书，第 154 页。

〔17〕 See United States of America v. Facebook Inc, Case No. 19-cv-2184 (United States District Court for the District of Columbia. 2019).

〔18〕 See Rohit Chopra, Dissenting Statement of Commissioner Rohit Chopra, In re Facebook, Inc. Commission File No. 1823109 (July 24, 2019), available at https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf, last visited on Mar. 3, 2022.

〔19〕 See Joe Simons, Noah Joshua Phillips & Christine S. Wilson, Statement of Chairman Joe Simons and Com-missioners Noah Joshua Phillips and Christine S. Wilson In re Facebook, Inc. (July 24, 2019), available at https://www.ftc.gov/system/files/documents/public_statements/1536946/092_3184_facebook_majority_statement_7-24-19.pdf, last visited on Mar. 3, 2022.

通过分析脸书 2012 年和 2019 年两宗案件可知，如果没有触及超大型平台的盈利模式，以及管理层或控股股东对个人信息利用的绝对控制，单纯对超大型平台进行事后监管和流程改造，无法对平台企业的合规动机进行根本影响。因此，需要监督的对象实际是超大型平台的管理层或控股股东。事实上，2012 年和解令最终确定的 4 个月后，脸书就允许第三方开发人员违规使用用户个人信息。〔20〕

由此可见，超大型平台独立机构的制度建构，不仅需要引入政府规制理论，而且应该引入公司治理视角。超大型平台企业的迅速崛起只是近二十年的事情，不少创始人仍然牢牢掌控已经上市的平台企业，并未实现所有权与经营权的分离。脸书的公司结构为 B 级股股东提供了“超级投票权”，扎克伯格的投票决定了董事选举和其他需要股东投票的事项。〔21〕“脸书股东厌倦了扎克伯格，但对他们无能为力。”〔22〕我国存在类似的情况，“作为企业家的发起人或创始股东珍视控制权以实现自己的愿景和抱负，这种对控制权的珍视体现为对发起人或创始股东权利的特殊安排”，如 B 站的双层股权结构、京东的投票委托权和阿里巴巴的合伙人制度等等。〔23〕相较于美国，中国互联网企业模式创新有余而技术创新不足，更加依赖个人信息和人力资源投入。具有类似的公司结构，承担着巨大的利润压力，依靠大量采集个人信息以维持商业运转，我国超级平台管理层或控股股东的合规动力更加匮乏。

四、决策监督型独立机构方案

为加强对管理层或控股股东的控制，不少国家规定董事会负责内控机制建设，赋予董事一定的法律义务。如日本《公司法》规定了董事构建内控机制的任务，《公司法实施规则》规定了构建内控机制的具体内容。〔24〕我国也有学者建议：“想让外部的监督发挥实效，就必须通过内部的决策机构。而内部决策机构最好的做法就是仿效独立董事的相关制度——在董事会下面设立一个主要由独立董事承担监督作用的个人信息保护专门委员会。”〔25〕如果公司董事会全部由管理层组成，那么董事会的存在就没有实际意义，董事会就变成了一个拥有高级头衔的管理委员会了。决策监督型独立机构方案下，我国不少学者建议将外部监督成员理解为公司的独立董事，独立董事组成独立机构负责对企业的个人信息保护作出判断和监督。〔26〕该方案如何展开，具有哪些优势

〔20〕 See FTC Imposes $ 5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook, Federal Trade Commission (July. 24, 2019), available at https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions, last visited on Mar. 3, 2022.

〔21〕 参见前引〔18〕，Rohit Chopra 文。

〔22〕 Michael Hiltzik, Facebook Shareholders are Getting Fed Up with Zuckerberg but Can't Do Anything about Him, Los Angeles Times: Business (Apr. 16, 2019), available at https://www.latimes.com/business/hiltzik/la-fi-hiltzik-mark-zuckerberg-facebook-20190416-story.html, last visited on Mar. 13, 2022.

〔23〕 参见汪青松、宋朗：《合规义务进入董事义务体系的公司法路径》，载《北方法学》2021 年第 4 期。

〔24〕 参见梁爽：《内部控制机制的法律化路径——以日本法上董事内部控制义务为视角》，载《金融法苑》2015 年第1 期。

〔25〕 隐私护卫队：《外部机构如何监督企业个人信息保护？许可：不能存在经济依附》，载 https://www.sohu.com/a/509672335_121258695，最后访问时间：2022 年 7 月 23 日。

〔26〕 参见张平主编：《中华人民共和国个人信息保护法理解适用与案例解读》，中国法制出版社 2021 年版，第 225 页；龙卫球主编：《中华人民共和国个人信息保护法释义》，中国法制出版社 2021 年版，第 260 页。

与弊端？现有文献没有对此进行讨论，本文尝试进行探索展开。

（一）方案的理论渊源

该方案与公司治理中的内部控制理论有关。内部控制在会计学和审计学中较为常见，近年来随着法学界对企业合规的关注，逐渐进入法学视野。“内部控制起源于企业财务舞弊、财务失败事件的不断发生，内部控制的发展与美国公司会计造假、破产倒闭事件周期性的发生有着密不可分的关系，每一轮的公司财务舞弊、破产倒闭事件都促进了内部控制理论的发展。”〔27〕例如美国《反海外贿赂法》（FCPA）要求证券发行者必须设计和维持有效的内部会计控制系统。〔28〕我国法律对内部控制理论也有类似应用，例如2021年6月中国人民银行发布的《中华人民共和国反洗钱法（修订草案公开征求意见稿）》第3章“反洗钱义务”第27条第3款规定：“金融机构应当通过内部审计或者独立审计等方式，监督检查反洗钱内部控制制度的有效实施，金融机构的负责人对反洗钱内部控制制度的有效实施负责。”

个人信息保护与企业财务管理存在较大相似性，都涉及企业的不同环节和各个流程，与企业经营模式和利润收支息息相关，关乎企业的生死存亡。尤其在消费者信息隐私意识觉醒的今天，对于超大型平台企业而言，个人信息保护不仅应是其努力控制的成本线，而且应该是严格遵守的生命线。因此，类比财务风险管理，个人信息风险控制完全可以应用内部控制理论。正如学者所说：“内部控制发展到今天，已经演变成一种过程，内化于企业的各个流程、各个环节，和企业的各类人员相联系，但从内部控制的对象和目标来看，其本质并没有发生变化，依然是一种风险控制活动。”〔29〕内部控制与风险管理属于一体两面，本质上都是对风险的有意控制。“内部控制就是控制风险，控制风险就是风险管理。”“内部控制主要是从风险控制的方式和手段说明风险控制的，风险管理就是从风险控制的目的来说明风险控制的。”〔30〕为强调对管理层和控股股东的力量制衡，避免风险管理和企业管理概念混淆，本文采用内部控制的概念。

对于内部控制的定义，美国国家金融欺诈信息委员会（Treadway委员会）下属的“发起组织委员会”（COSO）〔31〕发布的《COSO内部控制—综合框架（2013）》指出，内部控制是一个由实体董事会、管理层和其他人员实施的过程，旨在为实现运营、报告和合规相关目标提供合理保证。合规目标与遵守实体法律法规有关。这一框架包含控制环境、风险评估、控制活动、信息交流和监控活动五个组成部分。〔32〕我国财政部、证监会、银监会等五部委于2008年5月发布的《企业内部控制基本规范》第3条规定：“本规范所称内部控制，是由企业董事会、监事会、经理

〔27〕 李维安、戴文涛：《公司治理、内部控制、风险管理的关系框架——基于战略管理视角》，载《审计与经济研究》2013年第4期，第5页。

〔28〕 See The Foreign Corrupt Practices Act of 1977 § 15 U. S. C. § 78dd-1, et seq.

〔29〕 前引〔27〕，李维安、戴文涛文，第6页。

〔30〕 谢志华：《内部控制、公司治理、风险管理：关系与整合》，载《会计研究》2007年第10期，第41页。

〔31〕 COSO英文全称为Committee of Sponsoring Organizations of the Treadway Commission。COSO在美国成立于1985年，旨在赞助国家金融欺诈信息委员会（Treadway委员会）。Treadway委员会最初由位于美国的以下五家主要专业会计协会和机构发起和共同资助：美国注册会计师协会（AICPA）、美国会计协会（AAA）、国际财务执行官（FEI）、内部协会审计师（IIA）和管理会计师协会（IMA）。

〔32〕 See The Committee of Sponsoring Organizations of the Treadway Commission (COSO), COSO Internal Control-Integrated Framework (2013) (May 14, 2013), available at https://assets.kpmg/content/dam/kpmg/pdf/2016/05/2750-New-COSO-2013-Framework-WHITEPAPER-V4.pdf, last visited on Feb. 13, 2022.

层和全体员工实施的、旨在实现控制目标的过程。内部控制的目标是合理保证企业经营管理合法合规、资产安全、财务报告及相关信息真实完整，提高经营效率和效果，促进企业实现发展战略。”企业控制目标的实现需要由股东会、董事会、监事会和管理层等各个组织机构共同完成。构建合规制度体系是内部控制目标，无论由董事会或监事会设置独立机构，它们开展的内部监督活动都属于风险控制的内部过程。

该理论强调应发挥董事会内部控制的主导作用，例如《上海证券交易所上市公司内部控制指引》第 4 条规定：“公司董事会对公司内控制度的建立健全、有效实施及其检查监督负责，董事会及其全体成员应保证内部控制相关信息披露内容的真实、准确、完整。”比较法上，韩国存在类似的“合规监查人”制度。“合规监查人通常从公司内部的董事或业务执行负责人中选任，其虽由董事会任命，但却独立履行职务，其业务活动不受董事会或代表董事的干预。为了保障其独立性地位，韩国《金融公司治理结构法》第 30 条要求金融公司应当通过章程保障合规监查人独立履行职务，并为其履行职务提供必要的资料和信息；对合规监视人的任免虽由公司自主决定，但须在作出决定之日起 7 天内向金融委员会报告。公司未按规定设置合规监视人或未按照合规要求进行报批和运营的，根据该法第 43 条第 16—22 款的规定，可对其处以罚款。”〔33〕

美国学者提出了应由董事会承担内部控制最终责任的两点理由：第一，企业高管有可能扭曲信息流动。解决信息不对称问题，创造竞争性的信息来源。第二，存在管理机会主义问题。管理层面临业绩压力，任期薪酬与企业盈利高度相关。在一笔违反公司政策或法律规则的交易中，预期的利润通常是巨大、现实和生动的。相比之下，从经理的角度来看，违反公司政策或法律规则可能造成的损失往往微不足道、苍白、非常遥远，尤其是考虑到发现的可能性极低时，情况更是如此。董事们不寻求晋升，通常不负责短期利润决策判断，因而对于公司整体和长远利益更加看重。〔34〕脸书案件体现了该学者的公司治理思路，2019 年和解令创造了加强脸书隐私监管的四个信息流，建构了一种重叠的合规监督渠道（overlapping channels of compliance），以提高风险防控效率。〔35〕为加强对某一重要事项的整体管理，董事会设置专门委员会的做法在实践中已经很常见。如很多上市公司在董事会设立社会责任专门委员会和环境保护专门委员会。〔36〕

（二）设在董事会下而不是监事会下

内部控制职责的权能配置，实际上与不同国家公司法规定的组织结构有关。“英美法国家实行的主要是以外部董事为核心的监督制度，它与我国的独立董事制度相似。在以德国为代表的大陆法国家，实行的主要是以监事会为核心的监督制度。”〔37〕我国《公司法》规定董事会和监事会两个组织机构负责内部监督职能。有的学者认为转换到中国背景下监事同样负有内部控制义务。〔38〕我国《公司法》虽然没有明确规定外部监事制度，但是部分企业早已开始探索实施，如

〔33〕 赵万一：《合规制度的公司法设计及其实现路径》，载《中国法学》2020 年第 2 期，第 76 页。

〔34〕 See Melvin A. Eisenberg, The Board of Directors and Internal Control, 19 *Cardozo Law Review* 237, 250 (1997).

〔35〕 参见前引〔19〕，Joe Simons、Noah Joshua Phillips、Christine S. Wilson 文。

〔36〕 参见蒋大兴：《公司社会责任如何成为“有牙的老虎”——董事会社会责任委员会之设计》，载《清华法学》2009 年第 4 期。

〔37〕 高旭军：《对我国上市公司“双核心监督机制”的反思》，载《东方法学》2016 年第 2 期，第 58 页。

〔38〕 参见邢会强：《上市公司虚假陈述行政处罚内部责任人认定逻辑之改进》，载《中国法学》2022 年第 1 期。

中国人民银行2002年就曾发布《股份制商业银行独立董事和外部监事制度指引》。有学者提出独立董事的监督是决策中的监督，监事会的监督体现为事后监督。〔39〕以上观点和实践都具有借鉴意义，存在两个内部监督机关的情况下，董事会和监事会都可以承担个人信息保护的内部控制职责。需要进一步思考的是，为落地实施《个人信息保护法》，是否需要《公司法》相应修改，董事会和监事会哪一个组织更具有设置独立机构的制度潜力。

本文认为在坚持现有公司法框架下，独立机构更适合设置在董事会中，主要成员由独立董事担任。为了解决监事会存在的问题，我国引入了独立董事制度。公司监事会作为专门监督机构，普遍存在“监事会地位低下、资源匮乏，职工监事制度徒具其形，监事缺乏适当的考核和激励机制，与独立董事关系不清、叠床架屋，受制于高管控股股东”等问题。〔40〕不同学者总结的原因或有出入，但是监事会孱弱无力确是现实，无力对抗控股股东实施有效监督。我国《公司法》规定监事会由股东代表和职工代表组成，职工代表的比例不得低于三分之一，意图加强股东和雇员对公司的自我监督。但股东代表产生受制于控股股东，职工代表履职遭雇佣关系掣肘。即便允许外部监事加入，也难以改变监事会的固有缺陷。独立机构要求主要由外部成员组成，这与监事会的人员比例要求也存在出入。董事会拥有解聘或聘任管理层和制定规章制度等事项的决定权，可以有效建构个人信息保护内控合规体系。但是监事会仅具有建议、质询和调查等权利，只能列席董事会会议，没有投票表决权和否决权。我国超大型平台企业多赴美股和港股上市，就个人信息保护问题对董事会进行改造，与英美公司法传统不存在较大差异，更有利于企业降低合规成本。

（三）独立董事需要平衡股东利益与公共利益

独立机构由独立董事构成，独立董事实际开展监督活动，但是独立董事应该对谁负责，却鲜有学者深入研究。有专家观察到存在利益冲突的可能，有针对性地提出“如果认为独立监督机构对社会公众负责，公司的发展利益或将不作为独立监督机构考虑的范畴，有可能导致公司发展利益受损”〔41〕。这些观察实际上点出了问题的实质，独立董事应该对公共利益负责，还是对企业利益和股东利益负责？《上市公司独立董事规则》第5条规定独立董事应该维护公司整体利益，尤其要关注中小股东的合法权益不受损害。但是超大型平台收集了大量的公民个人信息，即便个人信息处理者投入了汗水劳动，个人信息蕴含的人格利益仍然属于公民或用户个人。空泛地说，公司利益、股东利益与社会公共利益当然是一致的，企业违反法律规定侵犯公共利益受到法律制裁，也会损害企业利益和股东利益。“但这个观点其实只是体现了一种‘大家好才是真的好’的良善价值导向，在逻辑上就如同个体利益和群体利益可以两全的论断一样脆弱，如果真的可以两全就不会有损公肥私和牺牲小我完成大我的问题。”〔42〕事实上滥用公民个人信息的现象已经如此普遍，大量的违法行为并没有被发现惩处，有些人甚至怀疑是否还有继续保护的必要。因此，实践中公司利益、股东利益与公共利益广泛存在着利益冲突。努力追求私人利益，既有可能成为创

〔39〕 参见施天涛：《让监事会的腰杆硬起来——关于强化我国监事会制度功能的随想》，载《中国法律评论》2020年第3期。

〔40〕 参见郭雳：《中国式监事会：安于何处，去向何方？》，载《比较法研究》2016年第2期。

〔41〕 虞伟：《个保法要求建外部独立监督机构，互联网平台为何按兵不动》，载https://xw.qq.com/cmsid/20211111A009I900，最后访问时间：2022年7月23日。

〔42〕 前引〔23〕，汪青松、宋朗文，第81页。

新创业的动力源泉，也有可能是公地悲剧的罪魁祸首。盲目乐观与有意回避都不可取，在流通利用中个人信息才能发挥实际价值。真正值得思考的是，如何通过法律规则调整实现不同利益平衡。

传统公司法理论认为董事仅对股东利益负责，追求股东利益最大化。基于公司所有权与经营权分离的现实情况，股东选举产生董事负责实际经营，股东与董事之间属于委托代理关系，董事对股东负有信义义务，通说认为至少包含忠实义务和勤勉义务。尽管从 19 世纪 30 年代开始，美国学界开启的企业社会责任讨论一直延续至今，但是这一框架仍是公司法的基本理论模型。正如前美国特拉华州最高法院首席大法官小利奥·E·斯特林（Leo E. Strine，Jr.）所说，“这些公司的董事会认为，他们所管理的共和国应该对唯一公民忠诚，而这些公民被称为股东。这些公司的董事会并不认为自己对其他选区有任何国家的忠诚度，他们认为自己是股权资本共和国的民选官员。”〔43〕但是董事追求股东利益并非没有限度，必须遵守法律的各项要求，意味着对于法律强制性规定事项，董事不能进行成本收益比较，这实际上在法律框架内限制了股东利益。伴随着美国公司所有权与经营权的分离，众多学者提出应该考虑企业的社会责任，公司董事会不仅要对股东利益负责，而且要考虑消费者、社区、雇员、客户和环境保护等非股东利益，由此产生了诸如利益相关者理论、公司公民理论、公司善治运动等理论思潮。〔44〕公司生产经营会产生各种社会成本，污染环境、劳工、金融风险等问题都需要公司经营者认真考虑。立法者希望通过成文立法解决这些问题，规定企业相应的法律义务，我国《个人信息保护法》也是如此。企业毕竟不是政府，企业存在的根本目的仍是追逐利润。曾经有人建议在公司董事会设立代表不同群体利益的公益董事，有学者评论说，即便全部董事追求公司利益最大化，都不一定可以实现意见统一。如果董事会充斥着目标不同相互竞争的支持者，那将是大多数管理者的噩梦。〔45〕如果赋予企业过多的公共责任，可能会将企业经营变成政治活动，董事之间的实质性利益冲突会导致公司无法经营。由此可知，如同公司一样，董事会既不可能彻底坚持“股东至上”，也无法完全替代政府追求公共利益，坚持维护股东利益兼带平衡公共利益才是现实选择。在个人信息保护问题上同样如此，个人信息只有在聚合、加工和利用之后才能发挥最大价值，平台企业的产品创新和商业开发在其中发挥了不可替代的作用，规范利用是最终目的，违规惩戒只是手段。因此，独立机构作为董事会的下设机构，需要平衡股东利益和公共利益。部分学者认为它不对个人信息处理者负责、单纯维护公共利益、应该保持中立性的观点是错误的。

独立董事作为独立机构的成员，应追求实现企业利益，我国《公司法》第 147 条和《上市公司独立董事规则》第 5 条均有直接规定。与《公司法》立法目的不同，《个人信息保护法》不要求独立董事关注中小股东的合法权益，而是强调他们对个人信息保护情况进行有效监督，主要关注广大力量分散的公民个人信息权益，本质上属于一种利益相关者权益。这部分利益与中小股东利益风险偏好存在明显不同，但是它们都依附在公司整体利益之上。无论是维护中小股东利益，

〔43〕 Leo E. Strine Jr.，Corporate Power is Corporate Purpose II：An Encouragement for Future Consideration from Professors Johnson and Millon，74 *Washington and Lee Law Review* 1，13（2017）.

〔44〕 参见施天涛：《〈公司法〉第 5 条的理想与现实：公司社会责任何以实施?》，载《清华法学》2019 年第 5 期。

〔45〕 See Alfred F. Conard，Reflections on Public Interest Directors，75 *Michigan Law Review* 941，950（1977）.

还是为了公民个人信息权益，法律为分散的利益群体选派代表，都试图打破控股股东的非对称权利结构，努力干预影响公司决策。二者在规制思路上是相似的，这是嫁接独立机构职能与独立董事职责的基础。股东利益、公司利益和公共利益，三者在合规层面是一致的。法律底线不容利益权衡，遵纪守法保障企业长远。这解释了为什么设置独立机构是构建合规体系的一部分，为什么独立机构与合规体系共同组成《个人信息保护法》第58条第1项。

（四）独立董事承担的法律义务之性质

结合我国《公司法》，独立董事的这种内部控制行为属于什么法律义务？我国《公司法》第147条规定董事对公司负有忠实和勤勉义务，《上市公司独立董事规则》第5条规定独立董事对上市公司及全体股东负有诚信与勤勉义务。这里出现了三种义务类型：忠实义务、诚信义务和勤勉义务，内部控制与三者是什么关系？法律义务这一概念本质要求主体行为符合法律规定，文字意义上所有部门法规定的各项法律义务都属于“合规义务”，但是某一种“合规行为”能否成为独立具体的法律义务就值得讨论了。这些新增的合规义务是否属于信义义务？或者它们可以成为一种新的“合规义务”？存在独立的内部控制义务吗？目前主要存在三种观点：第一，内部控制行为属于忠实义务或诚信义务的一种。诚信义务是否属于一种单独的信义义务类型，在美国公司法上存在着“三分法”和“二分法”的争议。本文无意对此进行明确区分，故将忠实义务与诚信义务进行并列。有学者提出，美国法上在董事违反内部控制机制建构义务的案例中，如Caremark案以及Stone案，法院一般认为董事故意忽视自身职责，往往会判定董事违反忠实义务。〔46〕第二，内部控制行为属于勤勉义务或注意义务的一种。有学者提出：“就履行个人信息保护法定义务而言，在学理上属于公司董事、高管应当履行的勤勉义务，即公司管理者应当保障公司能够切实履行法律规定的保护个人信息的义务，从而维护公司的利益，避免公司因义务不履行而遭受不利的法律后果，诸如，损害赔偿、行政处罚，甚至刑事处罚。”〔47〕有学者认为内部控制义务是董事勤勉义务的具体化和内在化，认为“对企业发生的重大事件或事故，即使是无需董事亲自决策和具体实施的小事直接引起的，如果该重大事件或事故与内部控制的不健全有关联，是和未能建立健全能尽早发现纠正违法违规事件的源头原因，防止事件发生的公司内部控制有关联，在一定条件下，也应认定董事违反了内部控制义务，董事应对公司承担相应的损害赔偿责任”〔48〕。还有学者分析德国公司法，论证从业务执行机构的谨慎义务中引申出来的合法性管控义务可以成为合规组织义务的法律基础。〔49〕第三，内部控制属于一种特殊的合规义务，与董事信义义务并列。有学者认为“董事信义义务的产生原因系董事与公司及股东间的委托代理关系和利益冲突，旨在减少公司治理中的代理成本。而董事的合规义务源于公司行为的合法性要求从组织层面向个体层面的下沉，旨在减少公司经营中的社会成本”，两种法律义务的产生原因存在根本不同，因此势

〔46〕 参见梁爽：《董事信义义务结构重组及对中国模式的反思——以美、日商业判断规则的运用为借鉴》，载《中外法学》2016年第1期。

〔47〕 张怀岭：《公司治理视域下个人信息保护的实现路径——以〈公司法〉第147条的具体化为中心》，载《财经法学》2018年第5期，第28页。

〔48〕 刘惠明、祁靖：《内部控制义务——董事勤勉义务的具体化与内在化》，载《东南大学学报（哲学社会科学版）》2012年第5期，第76页。

〔49〕 参见王东光：《组织法视角下的公司合规：理论基础与制度阐释》，载《法治研究》2021年第6期。

必产生张力与冲突。〔50〕

客观分析上述观点学说都有其合理之处，内部控制并非一个法学概念，包括公司治理、风险管理和企业合规的各个流程，这决定了其行为本身可能属于广义信义义务其中的一种类型，需要将《个人信息保护法》第 58 条和信义义务的子义务做综合理解，利用忠实义务、诚信义务和勤勉义务拓展个人信息保护义务的实质内容。应该避免法律义务的“大词化”倾向，尽量提供一些充满血肉的制度安排。《公司法》修订过程中，部分学者建议将合规义务确立为公司和相关成员的基本义务，借此建构整个合规理论体系。〔51〕但是加入合规义务可能导致本就抽象的信义义务更加混乱，增加无谓的概念重叠与指向冲突。因此，本文不建议将内部控制行为作为一种新型合规义务，借由合规义务与信义义务并列的方式在《公司法》上确立下来。正如学者所说：“一个连注意义务都没有能力去具体界定的法律制度，如何去设定在此基础上更复杂的合规？”〔52〕

（五）职能设计和人员构成

在职能设计上，独立机构的监督职能体现为两方面：第一，监督职能本质上是督导并举而非狭义监督，应该扩充独立机构的实际职能。不同于外部监督事后纠错，独立机构的监督活动是对个人信息风险的内部控制活动，不仅局限于监控活动，而且包括控制环境、风险评估、控制活动、信息交流四个环节。第二，监督职能属于系统监督而非具体监督，应该减轻独立机构的职责负担。超大型平台企业规模巨大，包含各种业务类型，难以指望任职董事进行具体监督。“董事负有对公司作为一个运行良好的系统的‘设计者’和‘维护者’的职责，负有督导（monitor）的义务。”〔53〕系统监督与具体监督的不同，是划分独立机构与个人信息保护负责人工作职责的重要标准。

在人员构成上，专门委员会人员数量应保持单数，由三名或三名以上成员组成。可根据实际情况，由董事会提名委员会动态调整。独立董事应至少占全部人员三分之二及以上。其余三分之一，控股股东和负责个人信息保护的高级管理人员不得担任。为不干扰企业正常经营，在日常性管理中独立董事由超大型平台企业自行选任，平台企业应及时向主管部门备案公示。在合规整改时，为保证整改措施及时到位，可由主管部门指定独立董事人选。独立董事的任职条件，除了符合《上市公司独立董事规则》的各项要求外，还应该强调专业性与多样性。鼓励企业聘请具有一定个人信息保护专业知识的法律、计算机、企业管理等领域专家进入专门委员会。考虑到承担系统监督的工作职责，专门委员会成员理应从平台企业领取适当报酬。

（六）方案存在的弊端

决策监督型独立机构方案将独立机构设置在董事会内部，由独立董事具体履行监督职责，独立于董事经理等高级管理人员，具有一定的合理之处。同时也存在诸多弊端：第一，各种独立董事组成的专业委员会过多，容易造成董事会负担过重。机构人员臃肿效率低下。环境保护委员会、合规委员会、劳工权益委员会、可持续发展委员会、社会责任专门委员会等各种委员会都多

〔50〕 参见前引〔23〕，汪青松、宋朗文。

〔51〕 参见前引〔33〕，赵万一文。

〔52〕 邓峰：《公司合规的源流及中国的制度局限》，载《比较法研究》2020 年第 1 期，第 44 页。

〔53〕 邓峰：《领导责任的法律分析——基于董事注意义务的视角》，载《中国社会科学》2006 年第 3 期，第 143－144 页。

少已经存在，有些是法律强制规定的，有些是企业根据自身情况设立的，不同委员会之间存在职能重叠，很容易造成独立董事身兼多职负担过重。第二，独立董事平衡股东利益、利益相关者利益和公共利益，虽然理论上可以抽象证成，但实际操作存在困难。加之独立董事职能责任众多，很难周全各种利益诉求。第三，独立董事法律责任不明，容易挫伤独立董事的积极性。2021 年 11 月 12 日广州市中级人民法院判决康美药业五名独立董事因违反勤勉义务承担连带责任，合计赔偿金额最高约 3.69 亿元。此案引发了有关独立董事法律责任的争论。我国独立董事多为兼职担任，无论是信息来源、时间精力，还是对企业业务的了解程度，实际上都无法与公司董监高相比，在客观条件受限的情况下倡导提高独立董事法律责任存在一定问题。我国《公司法》欠缺对勤勉或注意义务的制度化建构，二者本身是一个不确定法律概念，内涵外延都有待明确。《个人信息保护法》虽然已颁布实施，但是为时尚短仍需实践，不少具体规则也仍在探索之中，极有可能造成权责畸轻畸重。

五、结语：合规监督的模式选择

根据上文分析可知，第三方独立机构方案欠缺独立性，不具有比较优势，无法承载《个人信息保护法》第 58 条第 1 项的功能期待，因此该方案应该被否定舍弃。管理监督型独立机构方案可以实现对经理层和业务部门的日常监督，但无法解决独立机构对谁负责的问题，由于难以介入董事会决策，始终面临企业合规动力不足的问题。决策监督型独立机构方案，虽然实现了对企业管理层的全面监督，但是容易发生利益冲突，日常情况下难以区分不同利益诉求，受制于法律义务规定模糊，容易承担过重的法律责任。由此可见，无论是管理监督型独立机构方案，还是决策监督型独立机构方案，都存在合理之处与固有弊端。能否通过制度安排扬长避短呢？超大型平台侵犯个人信息具有隐蔽性，宏观决策、中观执行和微观操作都需要进行有效合规和必要监督。两种监督方案都属于合规监督的具体类型，只能在各自的制度场景下合理运行，无法通过一种模式解决所有问题，需要明确两种方案所属的合规监督模式。

根据已有文献研究，管理监督型独立机构方案应属于“日常性合规管理模式”的具体展开，该模式是指“企业在没有违法、违规或者犯罪的情况下，根据常态化的合规风险评估结果，为防范企业潜在的合规风险，开展合规管理体系建设”〔54〕。这种合规监督模式关注日常管理和风险预防，独立机构主要监督业务部门实际运作和搭建完整合规体系，在企业没有出现重大安全风险和受到法律制裁时，只需对董事会负责即可，显然无需任何决定和认定都向主管部门报告。决策监督型独立机构方案应属于“危机性合规整改模式”，该模式是指“企业在面临行政执法调查、刑事追诉或者国际组织制裁的情况下，针对自身在经营模式、管理方式、决策机制等方面存在的漏洞和隐患，进行有针对性的制度修复和错误纠正”〔55〕。在此种模式下，该方案的问题可迎刃而解。为指导涉事企业有针对性进行合规整改，执法机构可选派政府工作人员或法律专家担任企业

〔54〕 陈瑞华：《有效合规管理的两种模式》，载《法制与社会发展》2022 年第 2 期，第 6 页。

〔55〕 前引〔54〕，陈瑞华文，第 6 页。

独立董事，此时仍处于危机应对阶段，因此各方利益诉求相对清晰，实现企业合规和恢复正常经营是多方主体的最大利益公约数。根据执法机构出具的合规整改意见，独立董事的监督义务明确，由此承担不合比例法律责任的情形很难出现。同时，独立机构的监督对象是整个企业管理层，外部监督直接介入企业运行，此时独立董事向主管部门汇报整改情况，在法律上也并不存在解释障碍。综上所述，管理监督型独立机构方案适用于日常性合规管理模式，决策监督型独立机构方案适用于危机性合规整改模式。在区分日常管理和危机应对两种合规监督场景下，两种方案的制度优势可以最大程度发挥，而制度劣势可以相对减弱。

Abstract: Paragraph 1 of Article 58 of the Personal Information Protection Law stipulates that super large platform enterprises should establish independent institutions mainly composed of external members to supervise the protection of personal information. At present, there are three system design schemes. The third-party independent institution scheme has no obvious comparative advantages, does not conform to the concept of risk prevention, and is difficult to carry the expectation of supervision function, so it should be abandoned. The plan of management and supervision independent institution belongs to the daily compliance management mode, which is the management supervision of the board of directors to the managers. The activities of independent institutions under the leadership of the board of directors can not solve the problem of compliance motivation, and it is difficult to clarify the tension between the board of directors and law enforcement agencies. The decision-making supervision type independent institution scheme belongs to the crisis compliance rectification mode, which is the rectification supervision of the law enforcement agency to the board of directors. A special committee of the board of directors is established to rely on independent directors for internal control. However, the legal responsibilities of independent directors are vague, which is easy to cause overburden on the board of directors. The two schemes have their own advantages and disadvantages, and should be applied separately according to the problem scenarios to realize the systematic and continuous protection of citizens' personal information.

Key Words: super large platform, independent institution, management supervision, decision supervision

(责任编辑：周　游　赵建蕊)

财经法学 No. 1，2022
pp. 18 - 31

个人信息保护“目的限制原则”的反思与重构
——以《个人信息保护法》第 6 条为中心

朱荣荣*

内容提要：目的限制原则作为个人信息处理的基本原则，要求信息处理活动不得溢出信息收集时的初始目的，以保障信息主体对个人信息的自主控制与支配。然而，大数据时代个人信息的多维度利用日趋常态化与复杂化，导致信息处理目的难以在信息收集阶段完全确定下来，严格的目的限制原则忽视了个人信息的利用价值。信息保护与信息利用均为法律追求的价值目标，不能顾此失彼，因此，有必要在个人信息类型化视角下重塑目的限制原则的规范内涵。申言之，处理个人敏感信息必须恪守目的限制原则，禁止超越初始目的范围处理之；处理个人一般信息原则上亦须遵从目的限制原则，但特殊情形下允许超越初始目的而处理信息，前提是不得引发高于信息主体所预期的风险。

关键词：目的限制原则　信息保护　信息利用　个人敏感信息　风险限定

大数据时代，对于个人信息的获取与利用愈益普遍，信息处理者在挖掘、分析个人信息时可能在一定程度上侵害信息主体的合法权益。为规制不当的信息处理行为，《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）第 6 条确立了目的限制原则，该条规定“处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息”。目的限制原则作为个人信息保护制度的基石，[1] 能够有效避免滥用个人信息现象的发生。

随着大数据分析技术的不断发展，社会对于个人信息的利用需求达到了前所未有的高度，目的限制原则要求处理个人信息应当具有明确、合理的目的，且后续的信息处理应当与初始目

* 朱荣荣，南京大学法学院博士研究生。

〔1〕 Vgl. Peter Schantz, DS-GVO Art. 5 Grundsätze für Die Verarbeitung Personenbezogener Daten, in Heinrich Amadeus Wolff, Stefan Brink (eds), BeckOK Datenschutzrecht (33rd edn, 2020), Rn. 12.

的直接相关，极大地压缩了信息利用的空间，不符合信息保护与信息利用动态平衡之立法理念。有鉴于此，有必要对目的限制原则进行深度考察，寻求其在新时代背景下合理的因应之道。

一、目的限制原则的内涵阐释与法理基础

（一）目的限制原则的基本内涵

根据《个人信息保护法》第6条可知目的限制原则包含两个方面，即目的明确与使用限制。前者指收集个人信息应当具有明确、合理的目的，不得过度收集个人信息；后者指个人信息的处理应当与初始目的直接相关，如果信息处理行为超出了初始目的则为法律所不许。可见，目的明确与使用限制是不可分割的有机整体，两者相辅相成、相互制约，目的明确原则是信息处理行为的逻辑起点，只有在收集阶段明确告知信息处理的具体目的并获取信息主体的有效同意方可处理他人信息。同时，为确保信息处理目的的效力性，后续的信息处理行为应当与处理目的直接相关，不得超越初始目的可能的范围恣意处理个人信息，否则目的明确原则将形同具文。

目的明确原则是维护个人基本尊严的重要工具，在收集和利用个人信息时，忽视或淡化“目的”意味着人格尊严将受到严重的侵蚀。〔2〕信息主体与信息处理者之间信息不对称的客观事实要求信息处理者在收集信息之时应当善尽说明义务，避免信息主体因信息的不充分而做出错误的决策。目前，我国《民法典》第1035条、《网络安全法》第41条、《消费者权益保护法》第29条等诸多规范都要求信息处理者明示信息处理的目的，但对于“目的”的具体要求则未言明。《个人信息保护法》第6条规定，目的明确原则应当满足两个要件，即目的明确与目的合理。目的明确性要求收集个人信息应当具有明确的、特定的目的，过于宽泛与模糊的目的可能被认为是不合法的，目的明确性迫使信息处理者在收集信息之前审慎思考信息处理的目的，可以在一定程度上制约信息处理者恣意处理信息。信息处理者在形成明确的信息处理目的之后，还须将此目的以一种可被理解的方式清楚地表达出来，确保相关主体对信息处理目的的认知不存在歧义。关于目的明确性的形式要求，立法没有明文规定，从规范目的来看，目的明确性旨在保障信息主体充分知悉信息处理的目的，因此，信息处理者借助于何种形式表明其目的在所不问。目的合理性要求信息处理目的必须符合社会一般人的事理认知，不得违反基本的伦理道德与公序良俗。目的合理性包含两个要素，即制度层面的目的合法与价值层面的目的正当。目的合法是信息处理的最低要求，信息处理者处理他人个人信息应当具备合法性事由，包括约定事由与法定事由，约定事由指双方当事人可以自行约定信息处理的具体事项，法律不得无故加以干涉。法定事由则指法律所规定的无需获取信息主体同意即可处理信息的事由，包括订立或履行合同所必需、履行法定职责

〔2〕 See Joseph A. Cannataci, Jeanne Pia Mifsud Bonnici, The End of the Purpose-Specification Principle in Data Protection, 24 *International Review of Law, Computers & Technology*, 102 (2010).

或法定义务等。目的正当性指收集个人信息必须具有充足的价值基础，合理兼顾信息主体与信息处理者的利益，目的正当性的判定依附于个案具体情境，随着社会的发展以及立法理念的变迁而动态调整。

目前，我国对于使用限制的判定标准采取的是“关联性”，要求信息处理行为不得与初始目的不具有关联性。然而，立法对于“关联性”的具体内涵没有予以明确，《个人信息保护法》认为信息处理行为应当与信息收集时的初始目的具有“直接关联性”，张新宝教授起草的《个人信息保护法（专家建议稿）》主张信息处理行为应当与初始目的具有“合理关联性”。《信息安全技术 个人信息安全规范》（2020 年）则认为，“关联性”包括“直接关联性”与“合理关联性”，其规定“使用个人信息时，不应超出与收集个人信息时所声称的目的具有直接或合理关联的范围”。对于何谓“合理关联”，《信息安全技术 个人信息安全规范》（2020）并没有给出明确的答案，而是具体描述了属于“合理关联”的信息利用情形，其认为“将所收集的个人信息用于学术研究或得出对自然、科学、社会、经济等现象总体状态的描述，属于与收集目的具有合理关联的范围之内”。不同于我国，域外立法采取的是“兼容性”标准，第 29 条数据保护工作组指出，不同于初始目的的进一步处理并不意味着与初始目的自动地不兼容，某些情况下，信息处理虽然与初始目的不同，但二者可能是相符的。〔3〕关于“关联性”与“兼容性”的关系，有学者认为，在大数据产业下，数据机构对数据的二次利用往往跟初始目的没有关联性，但这并不意味着一定不相兼容。〔4〕换句话说，较之“关联性”，“兼容性”的涵摄范围更广，“关联性”要求后续的信息处理对于初始目的的严格遵循，可能在一定程度上阻碍大数据产业的发展以及创新型社会的构建。

（二）目的限制原则的法理基础

第二次世界大战结束后，国际社会开始深刻反思战争期间各种非人道的行为，普遍呼吁建立尊重基本人权的法律制度。黑格尔认为，人格的要义在于，我作为这个人，在内部任性、冲动和情欲以及在直接外部的定在等一切方面都完全是被规定了的和有限的，并在有限性中知道自己是某种无限的、普遍的、自由的东西。〔5〕当前，不论英美法系抑或大陆法系，相关制度安排均强调对于个人信息的利用不得以牺牲人格尊严为代价。受社会和他人尊重是人的一种基本需要，是人作为法律关系主体所享有的最基本的人格价值，自然人维护个人信息的准确性、控制个人信息的利用范围是保证个人尊严得到社会认可的体现。〔6〕在“小数据时代”，由于信息收集技术与收集能力普遍处于不发达状态，信息主体尚能有效控制信息是否被处理以及处理的方式，然而，随着大数据技术的突飞猛进，通过个人信息介入个人生活的广度和深度实现了从量变到质变，当个人成为纯粹的“个人信息客体”，被随意监控、分析和操纵，个人的内在决策和外在形象都被控

〔3〕 See Article 29 Data Protection Working Party, Opinion 03 /2013 on purpose limitation 15 (Article 29 Data Protection Working Party 00569/13/EN 2013), p. 21.

〔4〕 参见谢琳：《大数据时代个人信息使用的合法利益豁免》，载《政法论坛》2019 年第 1 期。

〔5〕 参见〔德〕黑格尔：《法哲学原理》，范扬、张企泰译，商务印书馆 2017 年版，第 51 页。

〔6〕 参见张涛：《个人信息的法学证成：两种价值维度的统一》，载《求索》2011 年第 12 期。

制时，个人作为人的完整性和主体地位便已分崩离析，个人的独立和尊严将直接受到挑战。〔7〕为稳固个人的主体性地位，《个人信息保护法》构造了以“人”为中心的制度体系，确保个人对信息的自主性与控制性，目的限制原则即是个人控制体系中重要的组成部分。

目的限制原则要求信息处理者在收集信息时明确告知信息主体信息处理的具体目的，并严格限定后续信息处理的方式，同时给予信息主体同意或反对的权利，能够在一定程度上保障信息主体自主控制信息被以何种方式处理，防止信息处理者以信息主体未能预见到的方式处理信息。自主决定与自愿承担风险是私人自治的重要体现，尊重个人自主决定是否接受信息处理可能造成的风险形塑了个人自治空间，法律对于信息主体真实的意思表示应予尊重，不得任意干涉。作为个人信息的原始所有者，信息主体对于个人信息的收集与利用享有绝对的支配力与控制力，除法律明确规定信息处理的合法性基础外，信息处理者只有在获得信息主体的同意或授权时才能收集或利用信息。目的限制原则要求信息处理者在收集信息阶段应向信息主体详细披露信息处理的方式、可能产生的风险等事项，并承诺在约定的目的范围内处理信息。一般而言，借由信息处理者收集信息时的说明义务，信息主体能够预判让渡信息可能需要承受的风险，并在此基础上作出是否许可他人使用其信息的意思表示。信息主体对于自我信息的控制力与支配力是目的限制原则的理论基础，亦是制约信息处理者尊重目的限制原则的动力来源，只有承认信息主体有权自主决定信息被如何收集与利用，才能促使信息处理者主动寻求信息主体的授权许可。为了获得信息主体的有效同意，信息处理者须将信息处理的目的向信息主体明示，并承诺在约定的目的范围内处理信息，信息处理者超过约定的目的范畴处理信息可能承担违约或侵权责任。

二、大数据时代目的限制原则的现实困境

目的限制原则的效力范围从信息收集开始，及于整个信息处理过程，在包括个人信息的存储、变更、传递与使用等的各个阶段，始终可以发挥其作用。〔8〕目的限制原则这种充足的法律效力力求全面保障信息主体的合法权益，然而在具体实践中，目的限制原则面临以下诸多龃龉。

（一）信息处理目的难以在收集阶段完全确定

目的限制原则要求信息处理的目的应在不迟于信息收集之时予以确定，且目的必须是明确的、合理的。目的限制原则可以有效保证信息主体事先知道信息利用的目的和范围，并能够控制信息收集在事先约定的范围内进行。〔9〕然而，在信息的流转、共享等信息的二次利用成为信息产业普遍遵循的商业运作模式的背景下，传统的目的限制原则受到挑战。目的限制原则依赖于一个前提条件，即信息处理目的在收集信息之时予以确定是可能的，然而大数据分析技术的价值恰恰在于提取隐藏的信息或对信息进行变革性利用，这使得信息处理者无法在信息收集阶段详细阐

〔7〕 参见郭瑜：《个人数据保护法研究》，北京大学出版社 2012 年版，第 84 页。

〔8〕 参见谢永志：《个人数据保护法立法研究》，人民法院出版社 2013 年版，第 57 页。

〔9〕 参见王秀哲：《大数据时代个人信息法律保护制度之重构》，载《法学论坛》2018 年第 6 期。

明信息的所有可能用途。〔10〕于此情形，信息处理者为保障信息处理活动的顺畅进行，倾向于将信息处理目的以一种模糊或宽泛的方式表达出来，导致信息主体无法预期后续的信息处理行为，这种信息的不对称可能引发社会歧视、差别性对待等不公平现象。

目的限制原则要求对于信息的处理必须与信息收集时的初始目的具有直接相关性，反向推之，当信息处理目的与初始目的不一致时，信息处理者应当及时告知信息主体变更目的的缘由并再次征得信息主体的同意。大数据技术的运用使得在信息收集、利用、存储等任何阶段都可能发生信息主体同意信息收集时所未预期的信息处理方式，过于频繁地向信息主体告知变更事项不仅增加了信息处理者的工作负担，也在一定程度上干扰了信息主体的正常生活。此外，目的限制原则植根于私人自治理论，该理论预设信息主体只有充分了解信息处理目的才能决定是否将信息移交给信息处理者。然而，大数据环境中信息处理的复杂性，尤其是自动化决策技术的运用，增加了信息主体理解与选择的难度。实践中，信息主体很少仔细阅读冗长而繁杂的隐私协议，或者囿于自身有限的理性及相关知识的匮乏难以理解具体条款的含义，减损了信息主体同意的有效性。更为重要者，由于信息主体与信息处理者在市场地位、议价能力等方面具有实质不对等性，信息主体即使认识到隐私协议的不合理性也无法要求信息处理者对相关事项予以更正。

（二）忽视了个人信息的利用价值

个人信息所承载的利益形态具有多元性与复杂性，随着大数据处理技术逐渐渗入社会生活各个方面，在日常的人际交往与社会生活中，个人需要不断地与他人交换信息，公务机关与非公务机关亦频繁收集大量信息以改善行政管理或提供更好的服务，社会对于个人信息的客观需求愈益增多。实际上，个人信息不仅与人格尊严及人格自由密切相关，更是相关产业存在和发展的基石，因此不能只关注信息保护，而应将信息保护与信息利用放在同一维度。〔11〕值得肯定的是，立法不再单方面强调信息主体利益的保护，欧盟《一般数据保护条例》（General Data Protection Regulation，GDPR）及我国《个人信息保护法》都开宗明义地指出，应注重信息保护与信息利用之间的平衡。近年来，我国信息产业发展迅速，对个人信息利用的需求也越来越大，大数据分析技术通过结合不同来源的数据可能发现新的趋势、模式和关系，目的限制原则制约了大数据的规模和使用，可能造成经济和社会效益的重大损失。〔12〕根据目的限制原则的逻辑进路，当信息处理目的实现时信息处理者必须尽快删除个人信息，不得留存个人信息，更不得将信息用于其他目的，这严重降低了信息的利用效率，阻碍了信息价值的开发与再利用。从实际层面考量，多数情况下大数据分析所涉及的方法和使用模式是信息处理者以及信息主体在收集信息时没有预料到的，为了遵守目的限制原则，信息处理者必须密切监视处理过程以确保信息处理没有超出约定的范围，然而采取这些措施可能是代价高昂的、困难的甚至是不可能的。〔13〕

〔10〕 See Alessandro Mantelero，The Future of Consumer Data Protection in the E. U. Rethinking the "notice and Consent" Paradigm in the New Era of Predictive Analytics，30 *Computer Law & Security Review*，643－660（2014）.

〔11〕 参见谢远扬：《〈民法典人格权编（草案）〉中"个人信息自决"的规范建构及其反思》，载《现代法学》2019 年第6 期。

〔12〕 See Bart Custers，Helena Ursic，Big Data and Data Reuse：A Taxonomy of Data Reuse for Balancing Big Data Benefits and Personal Data Protection，6 *International Data Privacy Law*，5（2016）.

〔13〕 See Tal Z. Zarsky，Incompatible：The GDPR in the Age of Big Data，47 *Seton Hall Law Review*，1006（2017）.

大数据时代的一个显著特征是，个人信息的价值不再单纯地来自其基本用途而更多源于信息的二次利用，很多信息在收集之时并无意用作其他用途，最终却产生了很多创新性的用途。〔14〕目的限制原则要求信息处理的方式应严格限定于初始目的范围内，不利于新产品、新服务的研发。此外，目的限制原则过于强调信息主体利益的保护，忽视了目的范围之外的信息利用可能造福于社会。2008 年，Google 公司利用用户的搜索关键词成功预测流感爆发趋势即为很好的例证，Google 公司最初收集用户搜索关键词的目的在于改善搜索引擎功能，对于流感趋势的预测显然逾越了 Google 公司收集信息时的初始目的，但毋庸置疑的是，流感趋势预测对于公共卫生部门及时采取防治措施提供了较大帮助。可见，严格的目的限制原则不符合大数据背景下信息多样性利用的现实需求，阻碍了信息经济与信息产业的进一步发展。

三、目的限制原则的改革方案及评价

（一）域外立法变革路径——以欧美为考察对象

目的限制原则最早由美国学者艾伦·威斯汀（Alan Westin）提出，威斯汀主张政府所收集的个人信息只能用于特定目的，不得用于其他目的或者进一步流转，除非提供信息的个人或群体的身份特征已经完全从该信息中移除，或者他们自由地对进一步流转表示同意。〔15〕立法上，目的限制原则可以追溯至 1980 年的《关于隐私保护与个人数据跨境流动的指南》，可以说，欧美国家对于目的限制原则关注的时间较早，积累了丰富的经验，通过考察欧美法的相关规定，可以为我国目的限制原则的优化调整寻求经验借鉴。

为缓和严格的目的限制原则适用上的僵硬性，95 指令规定了“兼容性使用”（compatible use），但并未正面规定“兼容性使用”的具体内涵以及判断标准，以致欧盟国家在评估兼容性时采取了不同的判定标准。具体来说，比利时主要根据信息主体的“合理期待”来判断兼容性，英国和希腊则通过“公平性”（fairness）与“合法性”（lawfulness）衡量兼容性，德国和荷兰则借助于“平衡测试”（balance tests）加以判定。〔16〕2013 年，第 29 条数据保护工作组发布了有关目的限制原则的意见书，明确指出“不同于初始目的的进一步处理并不意味着与初始目的自动地不兼容，在某些情况下，虽然信息的处理与初始目的不同，但二者可能是相符的”〔17〕。关于如何判定“兼容性”，第 29 条数据保护工作组认为应当考虑信息收集目的与信息处理目的之间的关系、信息收集的具体情境与信息主体的合理预期、信息的性质与信息处理对信息主体的影响以及

〔14〕 参见〔英〕维克托·迈尔－舍恩伯格、肯尼斯·库克耶：《大数据时代：生活、工作与思维的大变革》，盛杨燕、周涛译，浙江人民出版社 2013 年版，第 197 页。

〔15〕 参见梁泽宇：《个人信息保护中目的限制原则的解释与适用》，载《比较法研究》2018 年第 5 期。

〔16〕 See Judith Rauhofer, Look to Yourselves, That We Lose Not Those Things Which We Have Wrought: What Do Proposed Changes to the Purpose Limitation Principle Mean for Public Bodies' Rights to Access Third-Party Data, 28 *International Review of Law, Computers & Technology*, 146－147 (2014).

〔17〕 前引〔3〕，第 21 页。

信息处理者采取的保障措施等。〔18〕《一般数据保护条例》承继了第 29 条数据保护工作组关于兼容性使用的判定方式，成为指导欧盟域内判断信息处理是否合乎初始目的的重要依据。有学者认为，虽然相关立法列举了“兼容性”的考量因素，但实践中判定信息处理是否与初始目的相兼容，仍需根据个案具体情境加以判断。〔19〕有学者更是直言，“兼容性评估”在大数据背景下有些抽象和困难，兼容性评估要求考虑信息收集时的具体情境、信息的性质等各种因素，而大数据的运行需要分析不同环境中的数据，使得静态的要素评价几无可能。〔20〕“兼容性使用”作为一个转接通道，为超越初始目的之外的信息利用提供了理论基础，缓和了信息保护与信息利用之间的紧张关系，拓展了信息利用的空间，具有一定的积极意义。然而，“兼容性使用”在判断后续的信息处理是否具有正当性时仍以信息收集时的初始目的为基点，忽视了时间、环境等外在因素的变迁可能导致信息处理目的的更迭。2017 年，第 108 号公约协商委员会主张，不应以信息主体可能认为无法预料的、不适当的或令人反感的方式处理信息，将信息主体暴露于不同的风险或比初始目的所预设的更大的风险，可以视为以无法预料的方式处理信息。〔21〕指南改变了欧盟一直以来所遵循的目的限制原则的调整思路，为目的限制原则在新时代背景下的灵活运用开辟了新的方向，遗憾的是，指南仅具有参考性意义，不具有强制的法律效力。

不同于欧盟立法，美国主要通过场景规则的构建来改革目的限制原则所面临的困境，场景规则的提出与美国隐私概念的不确定性有关，自 1890 年沃伦（Samuel D. Warren）与布兰迪斯（Louis D. Brandeis）提出隐私这一概念以来，理论界关于隐私的具体内涵一直存在争议。在此背景下，美国学者海伦·尼森鲍姆（Helen Nissenbaum）提出了场景完整性理论（contextual integrity theory），主张隐私的保护应与特定情境联系起来，信息的收集和传播应当符合具体情境并遵守特定情境下的相应规则，隐私是否受到侵害需要综合考量具体场景下的多种因素。〔22〕场景完整性理论由于其强大的包容性与灵活性得到立法者的青睐，2012 年，白宫在一份文件中明确提出“尊重场景原则”（respect for context principle），消费者有权期待企业收集、使用以及披露个人数据的方式与其提供数据时的场景相一致。〔23〕与此同时，联邦贸易委员会强调在符合一定场景下企业可以直接收集或使用消费者信息而无需征得消费者的同意，除非企业以信息收集时所声称的实质性不同的方式使用信息或出于某些目的而收集敏感信息。〔24〕2018

〔18〕 参见前引〔3〕，第 23－26 页。

〔19〕 See Bert-Jaap Koops, The (In) Flexibility of Techno-Regulation and the Case of Purpose-Binding, 5 *Legisprudence*, 179 (2011).

〔20〕 See Tal Z. Zarsky, Incompatible: The GDPR in the Age of Big Data, 47 *Seton Hall Law Review*, 1008 (2017).

〔21〕 See Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data, available at https://rm.coe.int/16806ebe7a, last visited on May 27, 2021.

〔22〕 See Helen Nissenbaum, Privacy as Contextual Integrity, 79 *Washington Law Review*, 136－157 (2004).

〔23〕 See See White House, Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, available at https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf, last visited on Aug. 20, 2021.

〔24〕 See Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid change, March. 2012, available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, last visited on Jul. 19, 2021.

年，《加州消费者隐私法案》（California Consumer Privacy Act，CCPA）吸收了“尊重场景规则”，法案明确“若个人信息的处理符合信息收集时的具体情境，则认为信息处理行为是合理的、适当的”〔25〕。“尊重场景规则”主张不应严格固守信息收集时的初始目的，若后续的信息处理符合信息收集时的具体场景则判定信息处理行为是合法的，但“场景”具有流动性与易变性，不利于当事人合理预期的形成。有鉴于此，2020 年的《加州隐私权法案》（The California Privacy Rights Act，CPRA）对目的限制原则进行了调整，采取“初始目的”与“场景路径”双重认定模式，其规定“企业收集、使用、存储、共享消费者个人信息应当是合理的、必要的，并且与信息收集时的初始目的相符，或具有与信息收集时的情境相适应的其他披露目的”。易言之，若个人信息的后续处理与初始目的或信息收集时的场景相符，就应当认定为正当的信息处理行为。

（二）理论界的改革方案

大数据环境下，目的限制原则暴露出来的弊端愈来愈多，学界对此进行了反思并提出不同的改革方案。“合法利益测试说”认为“目的限制原则”已经无法适应社会发展的需要，应当评估为实现某项合法利益可以在何种程度上正当化信息处理行为，以此决定信息处理行为是否妥当。〔26〕“扩张解释目的说”主张综合考量信息收集时的情形、信息的性质以及信息处理对信息可能造成的后果等因素，来扩张解释信息收集时初始目的，禁止任何逾越初始目的的信息利用行为。〔27〕“风险限定说”建议融入场景与风险的理念，以“风险限定”替代“目的限定”，亦即处理个人信息不能引发高于原有程度的、用户无法预期的风险。〔28〕风险限定论认为，判定信息的利用是否具有正当性关键在于信息处理是否引发了不合理的风险，这种不合理的风险包括精神压力、差别待遇、人身财产损害的可能性以及是否符合信息主体的预期与信息披露时的情境。〔29〕

关于前述改革方案，“合法利益测试说”的观点较为激进，其认为应当彻底放弃“目的限制原则”的基础性地位，主张以“合法利益”作为信息处理是否具有正当性的唯一判断标准，如果信息处理是为实现某项合法利益所必需，则该信息处理具有妥适性，反之则否。“合法利益测试说”在一定程度上缓和了后续信息处理受限于初始目的的局限性，能够为实践中信息处理的适时变动提供理论依据。然而，“合法利益”是模糊且抽象的法律概念，其具体内涵及外延有待于个案情境中予以判定，由此可能导致不同主体对于“合法利益”存在不同的解释，无法为司法实践提供明确的指导。从实际层面考量，信息主体由于信息不对称、专业能力的匮乏等现实因素很难举证证明信息处理者所声称的“合法利益”是否合理，可能致使“合法利益测试”异化为强势地

〔25〕 The California Consumer Privacy Act of 2018（CCPA），available at https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121，last visited on Jul. 11，2021.

〔26〕 See Lokke Moerel，Corien Prins，Privacy for the Homo Digitalis：Proposal for a New Regulatory Framework for Data Protection in the Light of Big Data and the Internet of Things，available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2784123，last visited on Apr. 23，2021.

〔27〕 参见前引〔15〕，梁泽宇文。

〔28〕 参见范为：《大数据时代个人信息保护的路径重构》，载《环球法律评论》2016 年第 5 期。

〔29〕 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 2019 年版，第 200 页。

位的信息处理者肆意处理他人信息的辩护工具。“扩张解释目的说”避免了后续信息处理溢出初始目的范围可能面临的“目的落空”之诘问，保障了“初始目的”存在的价值，但其通过采取综合考量模式来扩张解释信息处理的初始目的不仅不合理地改变了原本意义上的“目的”，还在一定程度上淡化了目的明确性，导致当事人无法产生合理的预期。需明确的是，个人信息保护并非旨在保护信息本身不被收集、利用，而是保护信息主体免受信息处理可能造成的伤害，严格限制信息的收集而放松信息的利用不符合时代发展趋势。“风险限定说”不要求信息处理者对于初始目的的严格遵循，只要信息处理者将信息处理可能引发的“风险”控制在合理范围之内就可以自由处理信息，符合实践中多元化的信息利用需求。然而，罔顾信息收集时的初始目的，不利于信息主体合理预期的形成以及社会的有序发展。

四、个人信息的类型化分析

（一）个人信息类型化的必要性

1. 个人信息固有的差异性

个人信息范围广泛、种类繁杂，不同的个人信息与自然人的关联性是不同的，面对丰富庞杂的个人信息集群，统一个人信息的保护模式忽视了个人信息的差异性及其对个人的影响程度，因此，区分规制个人信息从而提供更为细致的保护实乃现实必需。

司法实践中，法院首先认为信息的内容决定信息处理风险的高低，如果所涉信息的内容是普通个人信息，则诉请通常不会得到法院的支持，但如果相关的个人信息涉及当事人的隐私，或者个人信息属于敏感事项，那么相关的诉请就有很大的可能获得法院的支持，因此，只有对受保护的个人信息进行类型化处理，才能“避免个人信息概念的模糊性缺陷，防止规范适用的空洞化”〔30〕。个人信息固有的差异性要求我们对不同个人信息给予不同程度的保护，这是平等原则的内在要求，平等并非意味着忽视个人信息的差异性刻意追求均等化保护。平等原则包括两重含义：平等的必须平等对待，不平等的必须不平等对待。这意味着平等原则不仅仅允许差别的存在，而且允许差别对待。〔31〕个人信息之间天然地存在差异，不加区分地对所有个人信息实行同等保护，违背了平等原则的实质内涵。

2. 促进信息市场有序发展

历史上，无数次思想启蒙与思想解放运动的经验告诫我们，人类从愚昧无知走向文明发展的关键就在于信息的获取与利用。目前，信息的共享与流通已成必然趋势，信息壁垒逐渐被打破，任何阻碍或隔绝信息流通的行为都是违背社会实际发展现状的。信息时代对于个人信息利用的内在需求要求我们必须摒弃传统的只关注于信息主体利益的滞后观念，适度地释放信息的经济价值才能有利于社会的有序发展。在信息处理过程中，信息主体的利益与信息处理者的利益处于持续

〔30〕 前引〔11〕，谢远扬文，第 146 页。

〔31〕 参见〔德〕伯恩·魏德士：《法理学》，丁小春、吴越译，法律出版社 2003 年版，第 165 页。

的博弈之中，过于强化信息主体利益的保护，必将侵蚀信息的合理利用空间；反之，偏重信息处理者的利益，则势必影响信息主体的利益。

大数据时代，信息经济已成为我国市场经济发展的重要组成部分，个人信息一体化的保护模式增加了信息处理者处理信息的顾虑，信息处理者可能因惧怕动辄承担法律责任而放弃信息产品的研发与升级，这对于我国信息产业的长足发展是不利的。从成本收益的角度分析，统一保护模式虽然使公民信息得到了绝对的保护，但国家为此投入了大量成本，包括司法成本、社会成本等，总体上无益于社会效益的增加，因而并非是最优的资源配置方式。〔32〕

（二）个人信息类型化的路径选择

1. 个人信息类型化的理论尝试与规范应对

关于个人信息的类型化区分，我国理论层面与规范层面存在不同的观点，就理论层面来说，可谓众说纷纭，以下简要概述。有学者依据个人信息与人格关系的紧密程度将个人信息区分为人格紧密型个人信息和人格疏远型个人信息，凡符合直接识别性、敏感性、个体性强三个特征之一的个人信息即为人格紧密型个人信息，反之则为人格疏远型个人信息。〔33〕还有学者立足于个人信息生命周期及其在不同周期阶段呈现的利益形态，将个人信息划分为个人私密信息、个人事实信息以及个人预测信息。〔34〕还有学者将个人信息划分为自然性个人信息与社会性个人信息，自然性个人信息是信息主体与生俱来且无法轻易改变的信息，社会性个人信息是信息主体为了社会生活所必须而由个人主动或被动地获取的相应符号或信息。〔35〕由上述不完全列举可知，我国学者在个人信息类型化问题上各执己见，但其区别规制个人信息的意旨均在细化个人信息的保护方式，并在此基础上平衡信息主体与信息处理者的利益。

就规范层面来说，截至目前，我国诸多规范均对个人信息的类型化予以了明确规定。2012年发布的《信息安全技术 公共及商用服务信息系统个人信息保护指南》第3.2条明确表示“个人信息可以分为个人敏感信息和个人一般信息”。《民法典》第1034条第3款依据信息的私密性将个人信息区分为私密信息与非私密信息，第1036条则根据公开与否将个人信息区分为已经合法公开的个人信息与未公开的个人信息。新近颁布的《个人信息保护法》延续了区别规制个人信息的立法理念，将个人信息区分为个人一般信息与个人敏感信息以及已公开的个人信息与未公开的个人信息。可见，我国立法对于个人信息的类型化存在不同的规定，由此引发的问题是，不同类型化的个人信息之间可能存在交叉重叠之处，例如，性取向可能同时属于个人敏感信息、私密信息以及非公开个人信息，此时应当选取何种保护路径不仅关系当事人合法权益的保护，还关系法律体系的内在协调。

---

〔32〕 参见董悦：《公民个人信息分类保护的刑法模式构建》，载《大连理工大学学报（社会科学版）》2020年第2期。

〔33〕 参见项定宜、申建平：《个人信息商业利用同意要件研究——以个人信息类型化为视角》，载《北方法学》2017年第5期。

〔34〕 参见袁泉、王思庆：《个人信息分类保护制度及其体系研究》，载《江西社会科学》2020年第7期。

〔35〕 参见刘迎霜：《大数据时代个人信息保护再思考——以大数据产业发展之公共福利为视角》，载《社会科学》2019年第3期。

2. 个人信息类型化的理想选择

上述个人信息类型化的学说有一定的说服力，但都不足以成为重构目的限制原则的根本性的类型划分。笔者认为，以信息的敏感度将个人信息区别为个人一般信息与个人敏感信息进而对目的限制原则采取不同的解释路径，能统筹兼顾信息主体利益与信息处理者利益，实现信息保护与信息利用之间的动态平衡。根据《个人信息保护法》第 28 条之规定，“敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息”。可见，个人敏感信息与个人一般信息的区分触及了个人信息保护实质意义上的差异性，较之于个人一般信息，侵害个人敏感信息对信息主体造成的损害更为严重，因而需要对其予以更严格的保护。

此外，以个人敏感信息与个人一般信息的区分来构建个人信息保护规范体系符合国际立法趋势，也契合了我国的立法规范。目前，比较法上大多国家和地区采取区别规制个人敏感信息与个人一般信息的立法体例。例如，1981 年欧洲理事会颁布的《关于个人数据自动化处理的个人保护公约》、2018 年生效的《欧盟一般数据保护条例》、2018 年日本修正的《个人信息保护法》等。我国规范层面，《民法典》《个人信息保护法》《征信业管理条例》以及《信息安全技术 公共及商用服务信息系统个人信息保护指南》《信息安全技术 个人信息安全规范》等诸多规范性文件或直接或间接规定了敏感信息。司法实践中，法院亦认为应当对于敏感信息予以特殊对待。在“罗某与巢某土地登记纠纷”一案中，法院认为，合法权利人对于房屋相关权属信息为个人敏感信息，在非法定情形下，未经权利人同意不应公开。〔36〕在“朱烨与百度网讯科技公司隐私权纠纷”一案中，法院认为，将个人信息区分为个人敏感信息和非个人敏感信息的一般个人信息而允许采用不同的知情同意模式，能够在保护个人人格尊严与促进技术创新之间寻求最大公约数。〔37〕可以说，个人敏感信息与个人一般信息的区别规制能够成为我国个人信息分类保护的基础性框架，是适合于我国个人信息类型化保护的理想的路径选择。

五、类型化视角下目的限制原则的重构

（一）个人敏感信息：禁止目的外利用

个人敏感信息与信息主体的人格尊严以及人格自由密切相关，非法收集或不当利用敏感信息可能对信息主体的人身权益造成严重损害，这种损害不局限于隐私侵害，而是包括财产损失、歧视性待遇、精神伤害等在内的各种形式的物质性以及非物质性损害。处理敏感信息具有高度的危险性，因而在处理敏感信息时应当恪守目的限制原则，禁止超越初始目的范围处理敏感信息。

〔36〕 参见江苏省南京市中级人民法院（2020）苏 01 行终 480 号行政判决书。

〔37〕 参见江苏省南京市中级人民法院（2014）宁民终字第 5028 号民事判决书。

如前所述，收集个人敏感信息必须具有明确、合理的目的，其中“合理性”的判定涉及价值层面冲突关系的利益衡量，可以借助于公法上的比例原则进行判定。比例原则缘起于德国警察法，后发展为公法领域的“帝王条款”，比例原则内含三个子原则，即适当性原则（Geeignetheit）、必要性原则（Erforderlichkeit）及狭义比例原则（Verhltnismigkeit im engeren Sinne）。〔38〕近年来，比例原则在我国呈现出不断扩张的趋势，不仅行政法、刑法等公法领域强调比例原则的指导价值，私法领域也逐渐认可比例原则的作用空间，更有学者主张比例原则应当作为民法的一项基本原则，强调比例原则在私法领域的普适性。〔39〕比例原则作为方法论意义上的工具性原则，〔40〕考察的是目的与手段之间是否均衡，处理敏感信息是否具有“合理性”亦在评价信息处理者的处理行为与其所意愿达成的目的之间是否合理，与比例原则内蕴的价值取向具有一致性。此外，比例原则内含的三个子原则呈现阶层式的构造，在具体适用上具有严格的顺序限制。比例原则的阶层式构造以及顺序判断模式提供了精致的分析工具，使得“合理性”的判定既不过于空洞也有章可循。具体来说，适当性原则要求信息处理者的行为应当有助于合法利益的实现，此处的“合法利益”应作广义的解释，不仅包括法律明确规定的正当性利益，还包括法律虽然没有明确规定但从规范目的可推导出的合法性利益。需注意的是，适当性原则要求信息处理者的行为具有实现合法权益之可能性即可，并不要求该合法利益必须真切地实现，由于事物的普遍联系性，客观上有利于实现合法利益的信息处理行为可能无限绵延，行为的作用力大小亦不相同，但不得将过于遥远的作用力纳入合理性范畴，否则可能堵塞信息主体获取救济的途径。必要性原则要求信息处理者在处理敏感信息时必须选择对信息主体侵害最小的处理措施，且所采取的措施必须具有经济性与便利性，若实现该信息处理目的成本过高，应否定信息处理行为的合理性。均衡性原则要求处理敏感信息可能对信息主体利益造成的损害应当与所要实现的目的具有相称性，不能显著失衡，相称性内蕴多元的价值评价，需要在具体个案中综合考量。

（二）个人一般信息：适度允许目的外利用

大数据时代，个人的生活交往以及社会的存续发展离不开个人信息的收集与利用，对于与信息主体联系不甚紧密的个人一般信息，应更多关注于其在社会生活中的流转与利用，原则上来说，信息处理者必须谨遵目的限制原则，但为满足社会对于信息利用的需求，应当允许信息处理者在一定条件下超越初始目的范围利用信息，前提是不得给信息主体造成不合理的风险。

现代社会是风险社会，各种各样的风险无处不在。贝克认为，风险的概念直接与反思性现代

〔38〕 Vgl. Landessozialgericht Hamburg. Begrenzung der Erlschenswirkung bei Nichtanzeige einer Beschftigung，2006 Heft 1，S. 18.

〔39〕 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；纪海龙：《比例原则在私法中的普适性及其例证》，载《政法论坛》2016 年第 3 期。

〔40〕 See Aharon Barak，Proportionality，Constitutional Rights and Their Limitations，Cambridge University Press，2012，p. 131.

化的概念相关，风险可以被界定为系统地处理现代化自身引致的危险和不安全感的方式。〔41〕还有学者认为，风险是某种不可预见情形出现的可能性，其可能是自然事件或人类活动的结果，也可能是两者共同作用的结果。〔42〕可见，“风险”一词具有多重面向，其在不同语境中具有不同的含义。个人一般信息更多体现为信息利用价值，因此不宜片面强调信息处理对于初始目的的严格遵循，而应要求信息处理者将信息处理可能引发的风险控制在合理范围之内，以符合大数据时代信息多元利用的趋势。一般来说，影响信息处理风险程度的因素主要有以下几项：第一，信息的敏感性程度。个人信息的核心特征在于识别性，识别包括直接识别与间接识别，直接识别指通过该信息可以直接确认某一自然人的身份，间接识别指通过该信息虽然不能直接确认某人的身份，但可以结合其他信息加以确定。〔43〕个人信息的此种特性决定了个人信息的范围具有广泛性与动态性，具体个案中，如果信息的敏感度越高，则信息处理行为受到的限制越多。第二，信息处理者的风险控制能力。特定的行为或活动与特定的风险相联系，当行为人以其行为开启一定的风险或者维持一定的风险状态时，该风险实现时则行为人难辞其咎。〔44〕通常来说，信息处理活动产生的风险是由信息处理者制造的，信息处理者在享受信息处理带来利益的同时亦负有合理控制风险的义务。风险实现的可能性以及风险的严重性与信息处理者控制风险的能力密切相关，信息处理者控制风险的能力越强，则风险发生的可能性越低、风险的严重性亦越低。第三，信息主体的预见能力。合理的信赖受法律保护，信息处理者不得以信息主体基于信息收集时的初始目的所无法预期的方式处理信息。〔45〕信息处理者对于信息主体信赖其以约定方式利用信息的合理预期负有保护义务，不得无故使信息主体的合理预期落空，否则有碍于构建良性的信息处理环境，若信息处理产生的风险高于信息主体的合理预期则为法律所不允许，信息处理者需将相关风险告知信息主体并重新获得信息主体的授权同意。须注意的是，即使信息处理产生的风险在合理范围之内，但信息主体明确表示拒绝接受信息处理的，信息处理者亦不得继续处理信息，除非信息处理者有证据证明信息处理的利益大于信息主体的利益。

六、结　语

法律需要稳定，但不能一成不变，所有关于法律的思考都是在努力调和稳定与变化这两种相互冲突的需求。〔46〕目前，大数据技术渗透到社会生活的各个方面，信息科技的快速变革要求个人信息保护理念应从严格限制信息收集转向平衡兼顾信息保护与信息利用，传统的目的限制原则

〔41〕 参见〔德〕乌尔里希·贝克：《风险社会》，何博闻译，译林出版社 2004 年版，第 19 页。

〔42〕 参见〔英〕罗伯特·鲍德温、马丁·凯夫、马丁·洛奇编：《牛津规制手册》，宋华琳等译，上海三联书店出版社 2017 年版，第 348 页。

〔43〕 参见黄薇主编：《中华人民共和国民法典人格权编解读》，中国法制出版社 2020 年版，第 209 页。

〔44〕 参见叶金强：《风险领域理论与侵权法二元归责体系》，载《法学研究》2009 年第 2 期。

〔45〕 See Dag Elgesem, The Structure of Rights in Directive 95/46/EC on the Protection of Individuals with regard to the Processing of Personal Data and the Free Movement of Such Data, 1 *Ethics & Information Technology*, 283 - 287 (1999).

〔46〕 See Roscoe Pound, Interpretations of Legal History, Cambridge University Press, 1967, p. 1.

无法有效应对社会的发展变化，有必要对其加以修正。

个人信息种类繁杂，不同个人信息与信息主体的紧密程度差异甚大，统一的个人信息保护模式无法合理兼顾信息保护与信息利用之双重价值目标，类型化构建个人信息保护制度实有必要。具体而言，由于个人敏感信息关系信息主体基本的人格尊严，在处理敏感信息时必须恪守目的限制原则，禁止恣意扩大初始目的应有的范围，而对于个人一般信息，可以适度允许超越初始目的范围的信息利用行为，但不得超过信息收集时信息主体能够合理预期的风险。我国《个人信息保护法》虽然规定了目的限制原则，但基本沿用传统的保护路径，存在不足之处，应适度调整目的限制原则的内涵以期助力我国信息产业与信息社会的有序发展。

Abstract：As the basic principle of personal information processing，the purpose limitation principle requires that information processing activities shall not overflow the scope of the original purpose at the time of information collection，which guarantees the subject of the information independent control and dominate over personal information. However，in the era of big data，the diverse use of information is becoming more and more normal，and the purpose of information processing is difficult to be fully determined at the information collection stage. Besides，the strict purpose limitation principle ignores the use value of personal information. Information protection and information utilization are both value goals pursued by the law，and we can't ignore one and lose the other. Therefore，it is necessary to reshape the connotation of the purpose limitation principle from the perspective of personal information typology. In other words，when dealing with personal sensitive information，we must strictly abide by the purpose limitation principle，and processing beyond the scope of the original purpose is prohibited. In principle，the processing of personal general information must also comply with the purpose limitation principle，but under special circumstances，it is allowed to process information beyond the initial purpose，provided that it shall not cause risks higher than expected by the subject of personal information.

Key Words：the purpose limitation principle，information protection，information utilization，personal sensitive information，the risk limitation

（责任编辑：王叶刚　赵建蕊）

财经法学 No. 5，2022
pp. 95 - 106

个人信息私法救济中的“损害赔偿”困境与应对路径

赵贝贝 *

内容提要：作为救济个人信息权益损害的民事责任之一，损害赔偿责任在侵权责任承担方式体系中具有核心地位。然而，实证数据和案例分析表明，司法实践对侵害个人信息损害赔偿责任的适用多持严苛态度，其中损害的认定已成为其中的首要障碍。从风险规制理论的视角来看，将信息风险性损害纳入法律上的损害范畴是一种高效的风险分配路径，更是化解私法保护困境的有效出路。此外，为确保信息侵权损害赔偿责任的落实，应凭借“差额说”将信息风险性损害具体化为附带财产损失和焦虑引起的精神损害等样态；适当缓和精神损害的严重程度要求；明确财产损失、精神损害、惩罚性赔偿的赔偿数额之计算规则，以更好地发挥损害赔偿填补损失的功能。

关键词：个人信息权益　风险性损害　损害赔偿规则　惩罚性赔偿

一、问题的提出

我国公法对个人信息权益保护的立法回应虽早于私法，但因刑事责任或行政责任的着眼点在于向国家承担责任，对私权利的救济仍需仰赖具有财产性质的民事责任。正因如此，《个人信息保护法》第 69 条第 1 款规定：“处理个人信息侵害个人信息权益造成损害，个人信息处理者不能证明自己没有过错的，应当承担损害赔偿等侵权责任。”这使得损害赔偿成为信息侵权民事责任的“代名词”。但在个人信息侵权领域，单纯侵害个人信息极少伴随着信息主体财产、身体实际

* 赵贝贝，武汉大学法学院博士研究生。

本文为教育部人文社会科学研究规划基金项目“民法典制定背景下程序法与实体法融合机制研究”（17YJA820017）的阶段性成果。

受损等直接物质性损害，通常带来的是风险或焦虑不安等非物质性损害。对此，信息主体主张的损害类型较为多元：一是实际发生了诈骗等侵权行为并造成现实经济或精神损害；二是个人信息的孤立经济价值减损；三是个人信息泄露带来的未来损害风险及内心焦虑不安；四是因信息侵权行为而增加的预防风险费、诉讼费、交通费等附带财产支出。然而，由于外部风险或内心焦虑等损害难以被传统侵权法损害概念所接纳，法院常以信息主体无法证明其已遭受实质性损害或无法律依据为由否定第三、四种情形下的损害。在个人信息被过度收集、滥用等侵权行为不断见诸报端、而人的行为风险又无法根除的现代社会，为使处于风险中心的信息主体获得司法的有效救济，我们必须反思：信息主体可主张的损害是否应当包括外部风险或内心焦虑；若包括，需满足的条件要求是什么以及如何凭借“差额说”将风险性损害予以具体化；在信息损害确定后，又如何使事实上的损害真正转变为可获合理赔偿数额的法律上的损害。上述问题正是社会生活高度信息化带来的挑战，而及时应对这些挑战对积累裁判经验和消除实务分歧不无益处。

二、实务视角下的个人信息损害赔偿责任

损害赔偿是侵权法的核心功能，《民法典》侵权责任编将原《侵权责任法》第二章“责任构成和责任方式”修改为“损害赔偿”，进一步明确了以损害赔偿为中心的侵权责任承担方式体系。〔1〕为系统展现个人信息保护的损害赔偿责任现状，本部分以《民法典》施行后的个人信息保护纠纷案件作为分析样本，又虑及规范层面隐私权与个人信息权益在适用规则与案由上存在交叉之现实，笔者分别以“个人信息保护纠纷”“隐私权、个人信息保护纠纷”为案由在“聚法案例网”中做民事案件的检索，共获得裁判文书 359 份（截至 2022 年 2 月 8 日）。在排除撤诉、重复等无效样本的基础上，可将有效个人信息保护纠纷裁判文书进一步限缩为 176 份，围绕主要民事责任方式及审理程序而展开的实证统计结果如表 1、表 2：

表 1　　主要民事责任方式

	停止侵害	赔礼道歉	财产损失赔偿	精神损害赔偿
诉讼请求（份）	103	115	86	106
裁判支持率	82.52%（85/103）	75.65%（87/115）	40.69%（35/86）	26.41%（28/106）

如表 1 所示，信息主体寻求法律救济时，其所主张的停止侵害、赔礼道歉等非赔偿性民事责任诉求一般可通过诉讼程序实现，但对于财产损失赔偿和精神损害赔偿而言，司法实践多持严苛态度。其中法院对精神损害赔偿的裁判支持率仅为 26.41%，呈现出信息主体对损害赔偿的急需与人民法院的微量供给之间的紧张关系。如表 2 所示，损害赔偿责任不仅成为一审和二审争论的问题，连再审率都达到了 4.79%。这在一定程度上说明实务对个人信息损害赔偿责任的认定争议较大，进一步说明以个案为切入点立体剖析赔偿性民事责任之价值。

〔1〕 参见王利明：《我国〈民法典〉侵权责任编损害赔偿制度的亮点——以损害赔偿为中心的侵权责任形式》，载《政法论丛》2021 年第 5 期。

表 2　　审理程序

	一审	二审	再审
损害赔偿诉求（份）	102	37	7
占比	69.80%	25.41%	4.79%

微观视之，司法实务中的个人信息损害赔偿责任主要有以下几方面的问题需要解决：

（一）信息泄露等侵权行为本身是否造成财产损失认定不一

个人信息受侵害时可能会导致或促成下游侵害的发生，并产生相应的财产损失，如不法分子利用被泄露的个人信息实施金融诈骗、伪造证件等行为，〔2〕当引发明显财产性损失时，信息主体主张财产损失赔偿自不待言。问题在于，若下游侵害未现实发生，信息泄露或滥用等侵权行为本身是否造成财产损失呢？侵权法以填补损害为主要目的，若无损害则无填补之必要，〔3〕个人信息权益侵权领域也莫能外。实务中，针对信息被侵害而未造成现实的人身或财产损失时，信息主体主张的财产损失类型通常有两类，即个人信息自身经济价值减损和财产权益未来被侵害的风险。

就个人信息自身的经济价值而言，其以企业数据为表征后无疑蕴含经济利益，部分法院也对此予以了认可。〔4〕但孤立个人数据的经济价值并不高，据相关计算，单个普通人贡献的数据价值为 0.007 美元，而经常出差的富人价值为 1.78 美元。〔5〕在“俞某诉北京乐某达康科技有限公司等网络侵权责任纠纷案”〔6〕中，当事人也仅是根据个人信息的经济价值象征意义的主张 1 元或 2 元赔偿。因个人信息侵权呈现出损害轻微的特点，实务中也并无多少人花费一审、二审甚至再审的高额诉讼成本去追求几元赔偿，法院也常忽视个人信息本身的经济价值。事实上，个人信息的非法交易有着庞大的买家需求，信息泄露的源头行为容易成为其他网络犯罪的“抓手”，因此，人们对于信息泄露等侵权行为的恐惧不在于个人信息自身的价值，而是担忧下游侵害发生的可能性，亦即侵害风险增加或某种机会丧失等。诚然，相对于财产损失或人身伤害易于评估、量化而言，风险多少显得不那么真实。也正是风险与损害确定性标准之间的鸿沟，使得风险能否被损害概念所容并具有赔偿性面临着实践中的挑战。在“孙国燕与被告移动滨州分公司、山东移动公司隐私权、个人信息保护纠纷案”〔7〕中，法院认为被告的电话推销行为直接侵犯了信息主体的知情权与拒绝处理权等信息权利，但对信息主体以未来损害风险为由所主张的财产损失赔偿请求未予支持。而在“孙某某诉沈阳某某家居有限公司隐私权纠纷案”〔8〕中，法院虽然认为被告将个人信息发送到微信群中的侵权行为未造成现实财产损失，但仍认可了信息泄露行为本身造成了财产损失而酌定赔偿 800 元。在个人信息侵权领域，不乏因信息受到侵害而积极维权的当事人，而司法实践对未来风险是否属于侵权损害问题并未形成统一的认识，这无疑将对个人信息的

〔2〕 参见商希雪：《侵害公民个人信息民事归责路径的类型化分析——以信息安全与信息权利的“二分法”规范体系为视角》，载《法学论坛》2021 年第 4 期。

〔3〕 参见王泽鉴：《侵权行为》，北京大学出版社 2009 年版，第 175－176 页。

〔4〕 参见广东省深圳市中级人民法院（2019）粤 03 民终字第 20512 号民事判决书。

〔5〕 参见申卫星：《论数据用益权》，载《中国社会科学》2020 年第 11 期。

〔6〕 参见北京市海淀区人民法院（2018）京 0108 民初字第 13661 号民事判决书。

〔7〕 参见山东省滨州市滨城区人民法院（2021）鲁 1602 民初字第 83 号民事判决书。

〔8〕 参见沈阳市大东区人民法院（2020）辽 0104 民初字第 6814 号民事判决书。

私法保护实践产生消极影响。

（二）附带财产损失是否属于“合理费用”存在理解分歧

发生个人信息侵权行为后，信息主体在个人信息本身损害之外，还存在因利用国家审判制度以实现救济而产生的一些无法避免的律师费、打印费、误工费、交通费等维权成本，以及为避免身份盗用或欺诈风险升高而采取的预防风险支出，上述费用可被统称为附带财产损失，那么信息主体能够以此费用支出诉请赔偿吗？针对侵权损害赔偿范围的划定，我国《民法典》采纳了合理性标准，〔9〕在第 1179 条和第 1181 条第 2 款列举了交通费、误工费等法定赔偿项目，并以“合理费用”作为判断其他损害项目是否属于“等”范围之内的标准。《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》（以下简称《网络侵权司法解释》）第 12 条第 1 款也明确将被侵权人为制止侵权行为所支付的调查费用以及律师费用视为合理费用。由此可见，预防风险支出、部分维权成本等附带财产损失并不属于现行规范明确列举的法定赔偿项目，那么，是否可以归入具有经济赔偿性的“合理费用”范围呢？对此，司法实践中也存在不同的认识。在“戴森、李玉梅与敖馨月隐私权纠纷案”〔10〕中法院认为，原告为维护合法权益委托其丈夫出庭参加诉讼，必然会产生误工损失，因此对其主张的误工费（法定赔偿项目）予以支持。而在“黄茂安与中国移动宜黄县分公司、中国移动抚州分公司等个人信息保护纠纷案”〔11〕中，对原告主张的打印费、交通费、咨询律师费，法院均以没有法律依据为由不予支持。就该案而言，法官在未对交通费、律师费等法定明确赔偿项目予以支持的情况下，反而对并非法定明确赔偿项目的鉴定费予以支持，令人费解。在司法实践中，诸如此类的问题并不在少数，且因为孤立个人信息本身的经济价值微小，受害人主张财产损失赔偿的主要依据又通常是附带财产损失，所以，明确附带财产损失的性质以遏制脱离合理性的裁判分歧现象，是个人信息侵权裁判中无法绕开的话题。

（三）精神损害赔偿认定艰难

个人信息损害通常具有无形性，法院常以信息主体无法证明其已遭受实质损害为由，不支持其财产损失赔偿主张，这几乎挫败了所有基于未来侵害风险提出的财产损失赔偿请求，信息主体对信息侵权损害的救济也转而寄希望于被纳入精神损害赔偿。从个人信息的类型视之，私密信息具有隐私权与个人信息的双重特点。当个人私密信息因被泄露而直接或间接导致明显侵犯隐私权的侵害时，信息主体常通过隐私权保护逻辑主张精神损害赔偿。但在个人信息侵权案件中，精神损害赔偿的支持率仅为 26.41%，而焦虑不安难以被认定为精神损害的子类型，是个人信息精神损害赔偿认定艰难的原因之一。由于个人信息具有数据属性，在个人信息被恶意电子化存储后，不法分子可能会永久获得个人信息数据，受害者因担忧未来被侵害也可能一直处于焦虑不安的精神状态中，〔12〕此种焦虑不安能否被解释为精神损害的子类型呢？与众多裁判文书否定未来风险

〔9〕 参见王磊：《侵权损害赔偿范围的确定机制》，载《法学》2021 年第 4 期。

〔10〕 参见四川省攀枝花市仁和区人民法院（2021）川 0411 民初字第 717 号民事判决书。

〔11〕 参见江西省宜黄县人民法院（2021）赣 1026 民初字第 422 号民事判决书。

〔12〕 See Justin Dion & Nicholas M. Smith, Consumer Protection—Exploring Private Causes of Action for Victims of Data Breaches, 41 *Western New England Law Review* 253, 260 (2019).

性焦虑具有损害赔偿性相反，在“刘云超与被告北京顺丰速运有限公司，第三人严颜个人信息保护纠纷案”〔13〕中，法院不仅支持了原告的赔礼道歉请求，还将原告因个人信息失控产生的可能被用于违法事宜的焦虑不安情绪认定为损害，并部分支持了其主张的精神损害抚慰金。尽管在该案中法院认可了内心焦虑成立损害，但总体而言，法院在审判实践中对内心焦虑的认定持谨慎态度。

此外，即使此类内心焦虑能纳入精神损害的范畴，其也受《民法典》第1183条第1款规定的“严重”要件限制。实践中，法院在大量案件中以损害未达到严重程度为由，拒绝支持信息主体主张的精神损害诉求。例如，在“蔡小燕与赵延安隐私权、个人信息保护纠纷案”〔14〕中，被告未经原告同意将原告及其两子的户籍信息张贴在公开场合，法院支持了原告公开赔礼道歉的请求，但以精神损害未构成严重为由驳回了原告主张仅1元的精神损害赔偿请求。甚至在部分信息主体因个人信息泄露而导致被原公司解雇或遭遇诈骗等行为时，法院仍然认为其精神痛苦不够严重。〔15〕由此可见，法院在审判实践中是普遍默认赔礼道歉责任轻于精神损害赔偿的，即使该精神损害赔偿额为1元也倾向于作出赔礼道歉等非赔偿性民事责任，信息主体若想获得精神损害赔偿绝非易事。

三、对“损害”的界定应与风险规制理论相契合

从以上个人信息侵权案例反映的情况来看，审判实务中的问题主要围绕损害类型展开。按照损害赔偿的基本原理，受害人主张损害赔偿责任时需要证明自身遭受了法律上可补救的损害，〔16〕而信息风险性损害能否被纳入法律上的损害范畴，已成为信息主体寻求私法救济的阻碍。《民法典》第1165条第1款作为侵权责任的一般条款，仅提及“损害”一词而未否定风险成立损害的可能性，因此，本部分将从风险规制视角出发，探讨信息风险构成损害的正当性。

（一）风险规制路径：风险控制和风险分配

自20世纪伊始，伴随科技的多次革命性飞跃，愈益频繁爆发的风险致害造成的大规模损害引发人们对工业社会法律思维模式的批判，在此背景下，德国思想家乌尔里希·贝克首倡“风险社会”理论。风险社会中的“风险”是与自然风险（如各种自然灾害）相对应的风险，其内在于科学技术，“可被定义为以系统的方式应对由现代化自身引发的危险和不安”〔17〕。随着科学技术的广泛应用，人类面对和遭受的风险数量和级别大大提高。就风险分布而言，尽管有权势和财富的社会阶级也不能逃脱风险的危害，但若不通过法律、政策对风险进行控制或分配，那么将形成风险与财富呈反比分配的不公状态。〔18〕基于此，国家的任务转向“以未来为目标的对科技发展

〔13〕 参见北京市顺义区人民法院（2020）京0113民初字第16062号民事判决书。

〔14〕 参见湖南省益阳市赫山区人民法院（2021）湘0903民初字第1506号民事判决书。

〔15〕 参见北京市第三中级人民法院（2020）京03民终字第2049号民事判决书；北京互联网法院（2018）京0491民初字第1905号民事判决书。

〔16〕 参见王叶刚：《论侵害人格权益财产损失赔偿中的法院酌定》，载《法学家》2021年第3期。

〔17〕〔德〕乌尔里希·贝克：《风险社会：新的现代化之路》，张文杰、何博闻译，译林出版社2018年版，第7页。

〔18〕 参见何国强：《风险社会、风险分配与侵权责任法的变革》，载《广东社会科学》2018年第3期。

可能给社会造成的危险进行预防”〔19〕，即如何规制风险成为现代国家的一项重要任务。根据公共性程度可将风险分为公共风险和个体风险两类，〔20〕两类风险的特点决定了规制方式的差异。个体风险是指“那些分散制造的，地方化的，可受个人控制或者是来自本体的风险”〔21〕，由于该风险的主体关系单一且损失相对固定，法律能够做到通过个案判断对个体风险进行分配与化解。因此，规制个体风险的路径是风险分配，重心在于对被害人的风险损害予以赔偿。而公共风险其实是个体风险扩散的结果，具有广泛的扩散性、蔓延性，显然难以简单依靠传统的私人自治或市场机制来防控。相较于个体风险而言，在公共风险的规制上，应注重从整体上控制风险的蔓延和扩张，即通常采取以追求秩序为价值取向的风险控制路径。风险控制路径和风险分配路径之间存在互补性的特点，前者是一种事前的规制思维，后者是一种事后的规制思维。鉴于此，在将风险作为规制目标时，常规的风险规制做法是并行适用上述两种路径，进而发挥出两种路径融合规制风险的优势。

（二）引入风险分配路径的方式：认可信息风险性损害

在大数据背景下，人们对数据、信息的依赖导致风险不可避免地裹挟而至，信息流转共享本身即是一种典型的社会风险活动，这可从《个人信息保护法》多次使用“风险”概念中得到证实。因此，法律对个人信息的规范面临着如何有效平衡信息安全保障与信息流转共享之间的关系，即在最大程度地满足信息处理者对信息需求的情况下，通过设置合理的风险控制或者风险分配路径，避免信息主体在信息处理活动中承受不合理的风险。

个人信息具有典型的复合法益性质，信息之上不仅汇集了各方主体不同类型和性质的利益诉求，各类风险也相应伴生于各方主体的活动之中。就公共风险而言，我国现行规范规定的风险控制路径较为多元，不仅通过《刑法》《治安管理处罚法》等公法来达到风险控制的效果，更是在《个人信息保护法》中明确规定了国家网信部门承担的监督管理义务，个人信息处理者承担的风险评估、告知同意等义务，来应对个人信息领域的公共风险。但受社会认知的限制，在采取风险控制措施的情况下仍存在剩余风险的可能，这就涉及风险分配的问题。

鉴于“从危险中获取经济利益者也经常被视为具有制止危险义务的人”〔22〕，剩余风险理应由作为信息风险之源与主要获益者的信息处理者承担。按照法经济学理论，“纯粹的风险分配与损害分配是重合的”〔23〕，亦即在剩余风险转化为现实的诈骗、身份窃取等损害之前，信息处理者所承担的风险在资本逻辑中可通过赔偿的方式进行转移。然而，信息风险性损害与传统侵权损害概念的抵牾阻断了风险性损害的转移，这使得信息主体以私法手段特别是侵权责任手段寻求损害赔偿的整体效果不尽人意。归结而言，信息风险分配路径的缺位导致司法实务中频现信息损害认定难的问题，因此，在风险控制的基础上引入风险分配路径成为必要，而将满足特定条件的信息风

〔19〕〔德〕乌尔里希·巴斯特：《德国行政法读本》，于安等译，高等教育出版社 2006 年版，第 53 页。

〔20〕参见侯东德、周莉欣：《风险理论视角下智能投顾投资者的保护路径》，载《华东政法大学学报》2021 年第 4 期。

〔21〕Peter Huber, Safety and The Second Best: The Hazards of Risk Management in the Courts, 85 *Columbia Law Review* 277, 278 (1985).

〔22〕〔德〕克雷斯蒂安·冯·巴尔：《欧洲比较侵权行为法》（下册），张新宝译，法律出版社 2001 年版，第 271 页。

〔23〕前引〔18〕，何国强文，第 233 页。

险性损害视为法律上承认的损害，无疑是一种高效的风险分配路径。

（三）认可信息风险性损害的正当性：符合风险分配正义

风险分配实质上是“风险成本、风险责任、风险损失在主体间的承担”〔24〕，由于风险具有不利益，为确保数字经济的健康发展，风险分配必须把实现正义作为最重要的目标追求。在个人信息保护的问题上，认可信息风险性损害不仅阻断了不公平分配风险现象的扩展，又能包容性地促进新兴信息产业的发展。具体而言：其一，认可信息风险性损害意味着让真正制造风险且获取收益的主体承担风险。个人信息侵权损害极少伴随着信息主体财产、人身受损等直接物质性损害，通常带来的是外部风险或焦虑不安等非物质性损害，该类损害具有不确定性、无限性和难以计量等特点。由于风险性损害与侵权法框架下的多数损害特征以及人们对损害的一般认识存在差异，法院常以损害不存在为由驳回受害人的损害赔偿请求，这等于纵容了信息处理者肆无忌惮地使用信息，并将风险转嫁给无辜且缺乏预防能力的信息主体。认可信息风险成立损害，并将损害分配给风险预防能力较高的信息处理者，客观上遏制了风险分配的不公现象，有助于保障处于弱势地位的信息主体的权益。其二，认可信息风险性损害具有预防风险的功能，有利于保障社会整体利益。风险分配正义以实现多数人的合法利益为目的，即通过合理的制度安排使风险对公众的总体损害降至最低。〔25〕相较于个人信息主体，信息处理者掌握更多资源和技术，在风险预防方面处于能力更强的位置，可以通过采取提高产品质量或采购风险防控设备等方式分散风险。而认可信息风险性损害相当于一种事后的惩戒机制，能够倒逼个人信息处理者积极采取上述措施，从而达到预防信息风险的目的。

事实上，司法实践中，风险性损害在环境污染、医疗损害赔偿、毒物侵害等领域已经得到认可与适用。在比较法上，欧盟立法也采用了抽象的损害概念，信息主体因数据泄露而导致身份盗窃或欺诈、声誉受损等非物质性损害，都有权要求信息处理者承担损害赔偿责任，〔26〕《德国联邦数据保护法》第 83 条第 2 款与《印度个人数据保护法案》第 3 条第 20 项同样也认可了个人信息风险性损害。

四、以信息损害为中心续造损害赔偿规则

损害与赔偿如影随形，是开启损害赔偿的“钥匙”。鉴于个人信息风险性损害的特点及既有损害赔偿规范的不足，为使事实上的信息损害真正转变为可获合理赔偿的法律上的损害，仍需回应信息风险性损害的具体样态、精神损害赔偿的条件以及损害赔偿数额的计算规则等问题。

（一）明确信息风险性损害的样态和识别因素

1. 风险性损害的具体样态

损害是权利或利益被侵害的后果，我国现有法律规范并未就损害这一概念进行正面界定。在

〔24〕 徐钝：《社会风险分配失衡的社会资本矫正——以法理型社会资本培育为中心》，载《学术论坛》2013 年第 7 期，第 70 页。

〔25〕 参见张晒：《风险分配何以公正？——基于新冠肺炎疫情的哲学审思》，载《北京理工大学学报（社会科学版）》2020 年第 3 期。

〔26〕 参见解正山：《数据泄露损害问题研究》，载《清华法学》2020 年第 4 期。

损害赔偿法的历史上，“差额说”一直占据着重要地位，〔27〕认为对损害的界定起决定性作用的并非具体法益遭受的侵害，而是受害人在侵权行为发生后实际享有的利益状态（减数）与若侵权行为未发生时的假设利益状态（被减数）之差额。因此，在判断信息风险性损害的样态时，可凭借“差额说”将信息风险性损害具体化为信息主体遭受的各种损害。

（1）外部风险性损害：附带财产损失

个人信息具有“可识别性”，且基因信息、生物识别信息等敏感信息又是不可更改和删除的，一旦暴露，将给信息主体带来身份被窃取或欺诈的风险。而个人信息在网络空间中又具有传播的即时性和复刻的便利性等特征，这使得信息主体面临未来遭受损害的风险升高。为避免未来损害的发生，信息主体通常会采取预防措施来应对风险，如购买风险监控服务、更换手机号等，以及因个人信息侵权行为而增加诉讼费、误工费等合理诉讼支出，这些实质上可被视为信息风险性损害。预防费用、诉讼成本支出等附带财产损失在性质上虽为“自愿的支出”，但这些费用在个人信息被侵权之前是无需支出的，在侵权行为发生之后则成为必要，且其中有些诉讼成本支出具有风险预防性质，实质上可被扩大解释为《网络侵权司法解释》第 12 条第 1 款规定中所称的“被侵权人为制止侵权行为所支付的合理开支”。〔28〕事实上，依《民法典》第 995 条规定的消除危险等人格权请求权，信息主体本就可向信息处理者主张消除危险等责任，若受害人已经采取相应措施，支出的合理预防费用和具有风险预防性质的诉讼成本支出当然构成事实上的损害。外部风险性损害直观传达的是一种面向未来的可能性，而将上述附带财产损失视为外部风险性损害，除了能够按照合理财产损失的标准对外部风险进行量化外，亦能增强信息主体界定信息损害赔偿范围的可预期性，从而调动个人采取预防措施的积极性，有助于避免更大损害的发生。

（2）风险引发的内心焦虑：精神损害

“精神损害是指受害人在人格权或其他权利受到侵害后，而遭受的生理痛苦、精神痛苦以及其他不良情绪。”〔29〕循此定义及《民法典》第 1183 条的规定可知，精神损害赔偿救济的对象是人格权、身份权和人格利益、身份利益等人身权，基本形态包括身体疼痛和精神痛苦。尽管《民法典》《个人信息保护法》等规范将个人信息的保护层级界定为法益而非权利，但因个人信息权益属于人格利益而可通过精神损害赔偿获得救济，且其损害形态往往归于精神痛苦。实务中，通过隐私权保护逻辑获得精神损害赔偿自无争议，法律适用的最大瓶颈在于焦虑不安等精神状态能否构成精神损害。信息主体因信息泄露而使身份或财产处于风险之中的常态反应，通常是无法言明的担忧或焦虑等消极精神状态，与确定的身体疼痛和因侵犯隐私权或名誉权引起的精神痛苦相比，并不那么直观而不易被认可。其实，在个人信息特别是生物识别信息、行踪信息等敏感信息因泄露而发生现实损害之前实为一颗“不定时炸弹”，涉及此类信息的侵权行为无疑破坏了个人

〔27〕 参见徐建刚：《〈民法典〉背景下损害概念渊流论》，载《财经法学》2021 年第 2 期。

〔28〕 参见杨立新：《侵害个人信息权益损害赔偿的规则与适用——〈个人信息保护法〉第 69 条的关键词释评》，载《上海政法学院学报》2022 年第 1 期；田野：《风险作为损害：大数据时代侵权“损害”概念的革新》，载《政治与法律》2021 年第 10 期。

〔29〕 张新宝：《精神损害赔偿制度研究》，法律出版社 2012 年版，第 17 页。

生活安宁和安全稳定预期。由此产生的焦虑随着时间的流逝，足以造成精神损害。〔30〕此外，在信息侵权领域，因大规模数据泄露而频繁发生的受害者遭受财物或其他严重财产损失的事件表明，〔31〕还未遭受现实损害的信息主体对风险的担忧并非凭空产生的心理压力，损害后果不言而喻，因此，认可内心焦虑属于精神损害并具有可赔偿性无疑是大数据时代的大势所趋。

2. 确定风险性损害的参考因素

承认信息风险性损害具有正当性，但风险性损害是否确定发生应建立在合理可靠的未来风险预测基础之上。法官对个案中风险性损害的预判取决于未来的信息流通过程，应由法官参考相关因素裁量确定。具体而言，对风险性损害的认定有影响的因素主要包括如下几项：（1）个人信息的种类。个人信息被侵害后成立风险损害的可能性与信息的性质相关，一般而言，私密或敏感信息相较于一般信息更具重要性，故其被侵权后造成的风险更容易成立损害。因此，在我国信息风险性损害的认定普遍艰难的现状下，基于现行立法在私密或敏感信息的处理上以禁止为原则，以有条件允许为例外的立场之考量，〔32〕对个人信息保护采取分而治之的策略极有必要，即私密或敏感信息的暴露本身即视为“现实损害”，对一般个人信息风险需满足特定条件才予以认可成立损害。（2）信息处理者的主观目的。在无形的网络空间中，信息处理者实施侵害行为时的主观状态对损害的判断至关重要，该主观状态一般可通过间接的方式推知。例如，在黑客攻击导致的数据泄露事件以及因平台收集数据产生的消费操控或歧视等侵权案件中，侵权人恶意获取或违法使用个人数据的主观故意是非常明显的，即使未立即利用获取的信息开展欺诈或歧视等下游侵权行为，违法使用信息是迟早的事，认可该种情形下的风险成立损害具有合理性。（3）信息侵权损害的迹象。风险性损害具有伴随时间的推移逐渐显现的特点，若在同一信息泄露活动中已有部分信息主体遭受身份窃取或欺诈，这表明尚未遭受现实侵害的信息主体在未来也有受到类似损害的风险，这可成为法官裁量的重要参考因素。当然，现实中个人信息风险的情形千差万别，法院裁定参考因素的类型无法一一列举，司法实践中还需由法官根据个案的具体场景综合判断。

（二）适当缓和可获赔偿的精神损害程度要求

精神损害赔偿意味着受害人能够通过金钱来缓解精神痛苦，更为关键的是实现了身体与灵魂在法律上的平等对待。〔33〕认可信息风险引发的内心焦虑成立精神损害，意味着信息主体可通过内心焦虑损害及隐私权损害两种途径主张精神损害赔偿，而以“严重”作为获取精神损害赔偿的条件，无疑将造成损害赔偿与精神损害之间的逻辑断裂。从理论视角观之，“严重”要件的基础主要是侵权法上的“忽略轻微损害”规则和现代侵权法中的“水闸理论”，两者都以协调权利保护与行动自由为目的。〔34〕然而，随着人们对人格尊严的逐渐重视，该限制条件的正当性正在受到挑战。其一，有违精神性人格权高于财产权利的民事权益位阶理论。精神层面的权益保护映射

〔30〕 See DJ. Solove，DK Citron，Risk and Anxiety：A Theory of Data Breach Harms，96 *Texas Law Review* 737，765 (2018).

〔31〕 参见湖南省张家界市中级人民法院（2021）湘08刑终字第112号刑事裁定书；云南省楚雄彝族自治州中级人民法院（2021）云23刑终字第229号刑事裁定书。

〔32〕 参见《民法典》第1033条，《个人信息保护法》第28条。

〔33〕 参见谢鸿飞：《精神损害赔偿的三个关键词》，载《法商研究》2010年第6期。

〔34〕 参见李昊：《纯经济上损失赔偿制度研究》，北京大学出版社2004年版，第53页。

出人类文明的发展程度，从《民法典》人格权编的规定可推知，“与其他法益，尤其是物质性的利益相比，人的生命和人格尊严处于更高的位阶”〔35〕，亦即精神性人格权因属高于财产权利的民事权益理应获得优先保护。〔36〕但现实是被侵权人主张财产损失赔偿并不以“严重”为限制条件，而是奉行全部赔偿原则（包括轻微损害），且在人身伤害案件中的精神损害赔偿请求通常都会被支持。与之相反，尽管当事人所受的精神痛苦在非物质性人身权益的损害中有可能处于唯一地位，立法仍以“严重”这一高门槛作为获得精神损害赔偿的前提条件，这不仅使得介于微小与严重之间的精神损害无法获得赔偿，更会变相助长侵权人侵权的动力。其二，非以“严重”作为限制条件并不会引发大量精神损害赔偿请求如洪水般涌向法院。从实证层面考察，对于真正受到精神痛苦的受害人而言，其坚持诉讼并不以赔偿金的数额为主要目的，而是“有”或者“没有”获得赔偿金。恶意诉讼主体虽以追求高额损害赔偿为目的，但赔偿金数额普遍并不高的现实会使其丧失诉讼的动力，所以无需过度担忧诉权被滥用。

此外，从比较法视角观之，《德国民法典》第 253 条未将“严重”作为适用精神损害赔偿的法定条件，欧盟《一般数据保护条例》第 82 条第 1 款与德国《联邦数据保护法》第 83 条第 2 款，也体现了取消精神损害严重性要求、降低精神损害赔偿门槛的趋势。〔37〕就我国而言，可获赔偿的精神损害的适用范围呈逐步扩大的趋势，如《民法典》肯定了违约精神损害赔偿、侵害“具有人身意义的特定物”的精神损害赔偿等，凸显了立法对人格尊严的重视。因此，为确保个人信息处理不逾越人格尊严底线，降低精神损害赔偿的条件实属必要。当然，适当降低精神损害严重性的条件并不意味着对精神损害的一概承认，而使信息处理者动辄因显著轻微的权益损害行为对信息主体赔偿精神损害，被侵权人因个人信息侵权而主张精神损害赔偿请求时，仍应向法院提供其遭受精神压力或痛苦的初步证据。

（三）厘清信息损害赔偿数额的计算规则

1. 损害赔偿数额的计算依据

损害赔偿责任的落实依赖于损害赔偿数额的计算依据。《个人信息保护法》第 69 条第 2 款借鉴了《民法典》第 1182 条规定的计算方法，将信息主体“受到的损失”和信息处理者“获得的利益”在适用顺位上合并为同一层次，赋予受害人在损害赔偿与返还获利之间进行选择的权利以实现保护的最大化，当根据以上两种计算方法难以确定赔偿数额时，则由法院“根据实际情况确定”。当个人信息因权益被侵害而遭受财产损失时，依据该计算规则主张损害赔偿数额自不待言，问题在于，《民法典》第 1182 条规定的损害赔偿性质是侵害他人人身权益造成的财产损失而非精神损害，那么，《个人信息保护法》第 69 条规定的损害赔偿性质如何呢？这涉及精神损害赔偿数额的计算依据。

上已述及，在个人信息侵权领域，风险引发的内心焦虑能够成立精神损害，这表明《个人信息保护法》第 69 条第 1 款中的“损害赔偿”应当包括精神损害，而第 2 款规定的计算方法又是针对第 1 款中的损害赔偿责任设计的，因此，无论是财产损失还是精神损害，都可以按照第 2 款的规定确定赔偿数额。但由于“受到的损失”和“获得的利益”这两种计算方法的侧重点不同，

〔35〕〔德〕卡尔·拉伦茨：《法学方法论》（第六版），黄家镇译，商务印书馆 2020 年版，第 421 页。

〔36〕参见王利明：《论民事权益位阶：以〈民法典〉为中心》，载《中国法学》2022 年第 1 期。

〔37〕参见张建文、时诚：《个人信息的新型侵权形态及其救济》，载《法学杂志》2021 年第 4 期。

财产损失和精神损害在具体计算规则的适用上存在差异。通说认为，“受到的损失”应被解释为财产损失，不宜扩张至精神损害，〔38〕这意味着“受到的损失”这一计算方法侧重救济的是个人信息权益人受到的财产损失，排除了精神损害赔偿责任通过该计算方法得以落实的可能。就“获得的利益”而言，利益是指个人信息处理者侵害个人信息权益获得的财产利益，而精神损害赔偿责任的最终体现方式是支付精神损害抚慰金，因此，将“获得的利益”作为落实精神损害赔偿责任的计算方法更为妥当，有助于解决精神损害难以量化之难题。所谓“根据实际情况确定赔偿数额”，其实是指由法院依职权酌定赔偿数额，财产损失和精神损害均是法官酌定的对象。需要注意的是，法官在酌定时的考量基础除了信息主体“受到的损失”和信息处理者“获得的利益”外，还需要“根据侵权人的过错程度、具体侵权行为和方式、造成的后果和影响等确定”〔39〕。

2. 惩罚性赔偿数额的确定

就个人信息侵权损害赔偿责任而言，除部分案件中存在能够按照合理财产损失的标准进行量化的预防风险支出和维权成本等实际损害外，多数案件中的信息损害具有个体损失数额较小的特点。在个人信息侵权行为发生后，若仅以单个个人信息的实际价值来计算赔偿数额，每笔赔偿 1 元或 2 元，这样的结果不仅不能惩治信息处理者利用个人信息非法获利的行为，也难以调动权利人维权的积极性，因此，有必要在个人信息侵权损害赔偿责任中规定惩罚性赔偿责任。“惩罚性赔偿又称报复性赔偿，是指由法院判决作出的赔偿数额超出实际损害数额，对侵权人具有惩罚功能的损害赔偿责任。”〔40〕相较于《侵权责任法》，《民法典》将惩罚性赔偿的适用范围扩展至知识产权和破坏生态领域，表明《民法典》注重对恶意侵权行为进行惩罚的态度。事实上，欧盟《一般数据保护条例》第 83 条已就高额罚款作出了规定，在英国的司法实践中，也存在因航空公司泄露乘客信息而被开出 1.839 亿英镑罚款的案例。〔41〕一旦明确应当在个人信息侵权领域设置惩罚性赔偿责任，就涉及惩罚性赔偿数额的确定问题。对此，应当从计算基数和倍数两方面着手。计算基数的一般规则应当是依照侵权行为造成的实际损失计算，〔42〕根据《个人信息保护法》第 69 条第 2 款的规定，在个人信息侵权领域，惩罚性赔偿的计算基数应当是信息主体“受到的损失”和信息处理者“获得的利益”。关于计算倍数，在已成熟适用惩罚性赔偿的知识产权、消费者权益保护等领域，并未形成统一的标准，但基本处于 1～5 倍之间，因此，信息侵权惩罚性赔偿中的计算倍数可由法官在 1～5 倍的范围内自由裁量。

综上可知，在个人信息侵权行为发生后，个人信息处理者需要对财产损失、精神损害、惩罚性赔偿承担责任。但由于多数信息侵权案件中被侵权人受到的损失较微小，按照计算依据得出的上述三种赔偿数额的总和通常也不能达到惩罚恶意侵权人的目的，因此，实行损害赔偿最低赔偿标准就十分必要。我国台湾地区“个人资料保护法”规定，每人每事件新台币 500 元以上 2 万元以下计算，美国《加州消费者隐私法案》所认定的赔偿范围是 100 美元至 750 美元之间。〔43〕其实，我国《消

〔38〕 参见王利明：《民法》（下册），中国人民大学出版社 2020 年版，第 532 页。

〔39〕 黄薇：《中华人民共和国民法典侵权责任编释义》，法律出版社 2020 年版，第 57 页。

〔40〕 杨立新：《〈民法典〉惩罚性赔偿规则的具体适用》，载《荆楚法学》2022 年第 1 期，第 65 页。

〔41〕 参见孙莹：《大规模侵害个人信息高额罚款研究》，载《中国法学》2020 年第 5 期。

〔42〕 参见前引〔40〕，杨立新文。

〔43〕 参见刘云：《论个人信息非物质性损害的认定规则》，载《经贸法律评论》2021 年第 1 期。

费者权益保护法》《食品安全法》也早已规定了损害最低赔偿标准，分别是 500 元和 1000 元。就侵害个人信息的微额损害而言，因个人信息可被进一步分为普通和敏感两类，结合现行法在产品、食品领域的微额损害赔偿标准的规定，侵害普通信息时可以按照每人每事件 500 元，侵害敏感信息时可以按照每人每事件 1000 元，如此方能确保被侵权人的维权成本和胜诉利益之间的平衡。

五、结　语

在大数据时代，被转化为数据的海量个人信息是云计算、区块链等尖端科技的“燃料”，如何实现个人对自身信息的“脱控”而不“失控”，所受损害得到充分救济是法律适用最为关注之点。对此，《个人信息保护法》在以往信息保护规范的基础上全面规定了个人信息保护规则，但因个人信息侵权损害与传统侵权法上的损害认定标准间的不匹配性，通过私法保护个人信息的司法实践力有不逮。在风险社会背景下，立法者不应仅将着眼点置于非赔偿性民事责任，还应当在潜在损害风险转化为诈骗等现实损害之前对风险进行分配，即通过损害赔偿责任对信息主体承担的风险损害进行补偿。诚然，对风险性损害的认可无疑将对法律适用的稳定性造成一定程度的冲击，因此，笔者又从信息风险性损害的具体样态、精神损害赔偿的条件以及损害赔偿数额的计算依据等方面进一步完善了信息损害赔偿规则，以期能够破解个人信息权益保护之司法难题。

Abstract: As one of the civil liabilities for the relief of personal information rights and interests damage, the liability for damages has a core position in the system of tort liability. However, empirical data and case analysis show that the judicial practice of information protection takes a strict attitude towards the application of liability for damages, and the differences and difficulties in the identification of damages have become the primary obstacles for information subjects to seek relief of private law. From the perspective of risk regulation theory, it is an efficient way of risk distribution to bring information risk damage into the category of legal damage, and it is also an effective way to solve the dilemma of private law protection. In addition, in order to ensure the implementation of the liability of information tort damages, we should rely on the “difference theory” to concretize the information risk damage into collateral property loss and mental damage caused by anxiety. We need to take appropriate mitigation of the severity of mental injury requirements, and clarify the calculation rules of the amount of compensation for property loss, spiritual damage and punitive damages, so as to make compensation for damages play a better function of filling the loss.

Key Words: personal information rights, risk damage, rules for damages, punitive damages

（责任编辑：徐建刚　赵建蕊）

财经法学 No. 3，2023
pp. 110 - 125

安全作为个人信息保护的法益

贺　彤*

内容提要：法律创设的查阅、更正、删除等权利不是个人信息保护的目的。人格、财产权利损害非由违法处理个人信息直接、定然造成，而应归咎于后续独立的实害行为，故人格、财产权利非违法处理的侵害对象，亦非个人信息保护的直接目的。违法处理的直接后果是使权利被侵害的风险升高，其侵犯的利益是安全。安全减损引起注意义务的增加和法律资源的消耗等利益变动，但由于此等利益差额无法举证和计算，亦未产生可预见的危险，故无法适用侵权救济。与侵权保护相区别，《个人信息保护法》设置了处理规则、权利义务、职权和责任等规范，其目的并非弥补损失，而是保护和恢复安全法益。个人信息保护与侵权保护相对独立，《个人信息保护法》第69条是两种保护规范的衔接规定。

关键词：违法处理个人信息　实害行为　识别性　侵权保护　安全法益

一、问题的提出：个人信息保护到底保护什么？

自20世纪70年代始，国外便已探索个人信息保护模式，防范泄露、篡改或过度利用个人信息对个人利益的损害。2018年欧盟出台了严格保护个人信息的《通用数据保护条例》（以下简称GDPR），赋予信息主体知情、更正、数据移转和清除等8种权利，〔1〕使信息主体在一定情形和条件下对个人信息处理全过程进行控制或干预。〔2〕《中华人民共和国个人信息保护法》（以下简称《个保法》）也规定了查阅、复制、更正、删除等权利（束），信息主体得以请求的方式向信息处

*　贺彤，东南大学法学院博士研究生、东南大学人权研究基地研究人员。

本文为江苏高校项目“人格权重大疑难问题研究”（2020SJZDA091）、江苏省研究生科研创新计划项目“个人信息公法保护机制研究”（KYCX21_0072）的阶段性成果。

〔1〕 参见《通用数据保护条例》，载 https://gdpr.eu/tag/gdpr/，最后访问时间：2021年12月26日。

〔2〕 参见高富平：《论个人信息处理中的个人权益保护——“个保法”立法定位》，载《学术月刊》2021年第2期。

理者行使之。但个人信息保护所保护的是这些请求权利吗？显然，它们本身没有分离或单独转让的价值，〔3〕非人身、财产等实体权利，而只是制定法所创设的、用以制衡信息处理者的工具。〔4〕假设这些请求权利未被设立，个人信息保护的利益依然存在。况且，个人信息保护更多依靠公权力来规制处理活动，无论是欧盟的GDPR、美国的信息隐私保护执法实践，还是我国个人信息保护制度，行政监管占据了主导地位。〔5〕可见，《个保法》中的请求权利，不是法律所保护的利益目的，而只是保护利益的一种工具。

根据《个保法》第1条“为了保护个人信息权益……制定本法”可知，保护个人信息的目的是保护“个人信息权益”。但这一答案仍不清晰。目前，我国学者对个人信息权益的属性和内涵已作了大量讨论，主要思路是将之定性为财产、人格等权利：或认为个人信息是有价值的商品，需给予财产权（主要是知识产权）保护；〔6〕或认为个人信息是人格尊严的体现，主张权利人对个人信息享有支配与自主决定的权利，依人格权获得救济；〔7〕或持人格权兼财产权的观点，认为个人信息兼具人格要素和财产要素。〔8〕

与其陷入理论争执，不如观察生活实践。法律所保护的“利益本身并不是立法者创造的，立法者只是在法律中确认和保护某种利益”〔9〕。《个保法》的制定是为了规制个人信息被不当处理而引发利益侵害的失序状态，故违法处理侵害的对象就等于《个保法》所保护的利益。因此，可以通过考察实践中违法处理“侵害了什么”，来解答“个人信息权益是什么”。如果个人信息权益是人格、财产权利，那么违法处理个人信息将会造成信息主体权利受损的结果；而若违法处理不会造成信息主体上述权利受损，那么个人信息权益的财产权说、人格权说则值得怀疑。在著名的“人脸识别第一案”中，原告在事实理由中表达了对被告强制收集和利用个人信息所产生的安全隐患的担忧，法院在判决中未判定被告存在欺诈等权利侵害行为。因此，有关个人信息权益是权利的学说尚且存疑，个人信息权益是什么的问题，有待进一步发现。

二、违法处理未必损害权利但直接减损安全

违法处理个人信息一般包括对个人信息的非法收集、利用、买卖与泄露、篡改、丢失等。实

〔3〕 参见叶名怡：《论个人信息权的基本范畴》，载《清华法学》2018年第5期。

〔4〕 参见王锡锌：《国家保护视野中的个人信息权利束》，载《中国社会科学》2021年第11期。

〔5〕 参见王锡锌：《重思个人信息权利束的保障机制：行政监管还是民事诉讼》，载《法学研究》2022年第5期。

〔6〕 参见谢立斌、李艺：《个人信息的宪法财产权保护》，载《江西财经大学学报》2021年第5期；任丹丽：《民法典框架下个人数据财产法益的体系构建》，载《法学论坛》2021年第2期。

〔7〕 参见程啸：《论个人信息权益》，载《华东政法大学学报》2023年第1期；张新宝：《论个人信息权益的构造》，载《中外法学》2021年第5期；程啸：《论我国民法典中个人信息权益的性质》，载《政治与法律》2020年第8期；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；杨立新：《个人信息：法益抑或民事权利——对〈民法总则〉第111条规定的“个人信息”之解读》，载《法学论坛》2018年第1期；王利明：《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》，载《现代法学》2013年第4期。

〔8〕 参见彭诚信：《论个人信息的双重法律属性》，载《清华法学》2021年第6期；前引〔3〕，叶名怡文；任龙龙：《个人信息民法保护的理论基础》，载《河北法学》2017年第4期；刘德良：《个人信息的财产权保护》，载《法学研究》2007年第3期。

〔9〕 张明楷：《法益初论》（上），商务印书馆2021年版，第180页。

践中，违法处理并不直接、定然造成权利损害，二者之间隔着“风险的发生”这一条件。权利损害实际由违法处理之后的实害行为所致，而实害行为并不定然发生，违法处理只是为其提供了条件和可能性。故违法处理的直接后果是增加权利受损风险，易言之，减损安全。

（一）违法处理未必直接、定然造成权利损害

考察案例中“行为—损害”的因果关系可知，违法处理与权利损害之间并无直接因果关系。首先考察违法处理个人信息引发财产权利受损的情况，以“周裕婵诉广东快客电子商务有限公司、东莞市易得网络科技有限公司网络侵权责任纠纷案”为例。〔10〕该案中，法院在认定第三人诈骗的基础上，以侵权规则来解决该民事纠纷，认为个人信息处理者违反了《中华人民共和国网络安全法》第 40 条的“用户信息严格保密”义务，使第三人利用获得的个人信息实施诈骗，遂应承担侵权赔偿责任。这一判决看似是将周某被诈骗的财产损失结果直接归因于个人信息的泄露，实则非也。根据法院的事实认定和判决结果可知，法院认为泄露信息与财产损失之间具有“间接”的因果关系：（1）法院将泄露用户信息的举证责任倒置于快客公司，而快客公司因无法排除自己的责任而被推定存在泄露用户信息的事实；（2）网名为“售后楚楚”者利用从快客公司获取的用户信息，以快客公司“售后”的名义欺诈周某，这种表见的代理行为使周某有理由产生合理信赖并向其转账，故造成周某财产损害的直接原因是“售后楚楚”的诈骗行为，这是独立于泄露行为的、另一主体实施的实害行为；（3）法院在判决书中认定，“快客公司作为网络运营者未能履行保护用户信息的义务，对于因此给周裕婵造成的损失负有一定的过错”，可见，法院并未将周某财产损害的结果直接、完全归因于个人信息泄露，而是认为泄露行为与财产损失之间具有间接、“一定”的因果关系。由此可见，利用个人信息实施诈骗，使被害人遭受财产损失，这一结果的直接原因是诈骗行为而非泄露行为。将诈骗行为造成的财产损害完全归责于泄露个人信息的行为，有悖法院判决的本意。

其次考察违法处理个人信息引发人格权利受损的情况，以“蔡小燕与赵延安个人信息保护纠纷案”为例。〔11〕该案中，法院认为，被告未经原告同意将原告及其两子的户籍与二孩出生证明泄露，侵害了原告及其两子的隐私权。显然，法院在明确被告泄露原告个人信息的事实后，却以隐私规则裁判案件，其间的因果关系需补充说明。本案中，被告除了泄露原告及其子女的个人信息外，还张贴了“寻找原告之子蔡子明生父”的寻人启事，据此宣扬蔡某二孩非婚内所生，有损原告及二孩的名誉，也构成对原告隐私的泄露、刺探。可见，户籍登记与出生证明中的信息都是能够为人共享的个人信息，而真正带给原告精神痛苦的则是“寻人启事”的发布，人们据此对蔡某的私生活品头论足或猜测打听，造成对蔡某名誉和隐私权的侵害。因此，人格权受损与违法处理是间接而非直接的因果关系，两者之间还存在独立实施的人格侵权行为。

通过分析上述案例可知，在违法处理个人信息引发的财产、人格侵权案件中，还存在独立的实害行为。违法处理行为只是为后续实害行为提供条件，本身并非造成权利损害的直接原因，故不能将权利损害直接归咎于违法处理。

〔10〕 参见广东省深圳市中级人民法院（2019）粤 03 民终 3954 号民事判决书。

〔11〕 参见湖南省益阳市中级人民法院（2021）湘 09 民终 1585 号民事判决书。

此外，在现实生活中，大多数违法处理个人信息行为并未引发财产、人格权利致损的结果，这充分证明违法处理与权利损害之间不是直接、定然的因果关系。如在“陈瑜婷与上海瑞慈瑞兆门诊部有限公司隐私权纠纷案”〔12〕中，原告虽认为被告对其个人信息的泄露造成其在“信息安全及居住安全”方面的较大精神及心理压力，但没有表示有关隐私、名誉以及财产等权利受到损害。法院审理后认为，本案因所涉个人信息“难以归入隐私权的私密信息范畴”，故不构成隐私侵权；尽管“被告在处理原告个人信息的过程中确实存在不妥之处”，但并未造成权利损害结果，遂驳回其精神损害赔偿的诉讼请求；判决被告赔礼道歉，并非有充分事实、法律依据，只是因为“被告愿意”且“于法不悖”。可见，违法处理有时并不会造成人格、财产权利的损害，既然如此，个人信息权益并不等同于人格或财产权利。

有学者已注意到违法处理个人信息行为并不直接、定然造成权利损害，但仍将权利损害视为违法处理的危害后果，称作“下游损害”。〔13〕谢鸿飞教授表示：“当下游损害发生时，信息泄露本身造成的权益损害往往被司法实践忽视，它往往被下游损害所吸收。”〔14〕这一观点已认识到违法处理带来的权益侵害与权利损害有所区别，但仍将二者合一，将权利损害直接归责于违法处理行为。对违法处理侵害权益的忽视，导致个人信息保护与侵权保护难以界分。显然，这种认识不符合“行为—结果”一一对应的逻辑关系，也有悖于法治的基本精神，容易带来“连坐”之后果，即虽未实施欺诈等后续行为，却因具有一定关系而要连带承担欺诈等行为所对应的责任。

总之，在违法处理与权利损害之间，还有实害行为的介入，故须严格区分违法处理行为与后续实害行为。违法处理行为具有独立的侵害后果，不应将之与权利损害结果混为一谈，否则无法辨别个人信息上真正被侵害（或受保护）的对象。

（二）违法处理的直接后果是减损安全

既然违法处理个人信息实施了独立的侵害，那其直接后果是什么？违法处理在客观上为后续可能的实害行为提供了有利条件，使权利更容易、更可能受到损害，即“风险升高”。有学者认为，个人信息的暴露本身即为损害，无须再寻找其他的损害，〔15〕这种观点较为极端。个人信息暴露必然会带来风险，但人们早已习惯或需要被陌生人了解，若将个人信息的暴露当作损害而排除个人信息上的任何风险，那么人类交往将局限在熟人社会而无法进入开放市场，故不能直接将之当作损害。此外，更多学者认为应当对个人信息的无形损害实行损害的推定，〔16〕或将风险升高视为损害，〔17〕由此适用侵权救济。尽管这些观点有待推敲，但违法处理所致风险升高的不利益性，显然已被较多人接受。风险升高只是描述了不利益状态，与之相对应的利益应当是

〔12〕 参见上海市普陀区人民法院（2020）沪0107民初5934号民事判决书。

〔13〕 参见商希雪：《侵害公民个人信息民事归责路径的类型化分析——以信息安全与信息权利的“二分法”规范体系为视角》，载《法学论坛》2021年第4期。

〔14〕 谢鸿飞：《个人信息泄露侵权责任构成中的“损害”——兼论风险社会中损害的观念化》，载《国家检察官学院学报》2021年第5期，第29页。

〔15〕 See Maxwell E. Loos, *Exposure as Distortion: Deciphering “Substantial Injury” for FTC Data Security Actions*, 87 George Washington Law Review Arguendo 42 (2019).

〔16〕 参见徐明：《大数据时代的隐私危机及其侵权法应对》，载《中国法学》2017年第1期。

〔17〕 See Jennifer Wilt, *Cancelled Credit Cards: Substantial Risk of Future Injury as a Basis for Standing in Data Breach Cases*, 71 Southern Methodist University Law Review 615 (2018).

安全。

在 2021 年 4 月由最高人民检察院发布的个人信息相关公益诉讼典型案例〔18〕中，行为人违法收集、使用、出售或泄露个人信息，因牵涉的人数和个人信息数量较大，涉及公共利益，故引发检察机关提起公益诉讼。在数起典型案例中公民权利未遭受损害，但违法处理行为仍应受法律规制，这是因为该行为减损了公民所信赖的安全。典型案例中检察机关对侵害后果和履职活动的表述，可以验证这一观点。一方面，公民“合法权益”和社会“公共利益”是检察机关频繁用来描述侵害对象的用语，但也未能清晰展现被侵害对象的具体内涵。根据检察机关表述的“易引发犯罪”“威胁财产乃至生命安全”“具有危害财产安全的可能性”等用语可知，个人信息被违法处理后，诈骗等尚未发生，但这为侵权行为提供了有利条件，使不法者更易“趁虚而入”，增加了损害发生的可能性。因此，违法处理对公民合法权益和社会公共利益的侵害，实际上是对个人或群众人身、财产的安全造成减损。另一方面，“个人信息安全”是检察机关频繁用来描述保护目的的用语，其实质就是人身、财产权利的安全。安全是人所享有的利益或状态，作为工具和抓手的个人信息本身并不存在安全问题。〔19〕只有与信息主体利益相关时，信息安全才有保护的价值。检察机关打击个人信息违法犯罪的目的，是要消除违法处理给信息主体人身、财产权利带来的风险因素，使之恢复到合法安全状态。因此，“个人信息安全”就是信息主体的人身、财产安全。

综上，违法处理与公民人身、财产权利损害呈间接的因果关系，其间存在两个行为、两个结果、三层关系。如图 1 所示：违法处理直接造成安全减损结果；安全减损可能（而非定然）引发实害行为；违法处理后的实害行为是直接造成权利损失结果的原因。由于处理者造成了权利的高风险后果，且应当预见后续可能会发生权利侵害，故有义务采取妥当措施使信息主体脱离高风险状态，使之不会遭受后续实害行为的损害；若其放任风险发生，则应当对侵害结果承担一定的责任。〔20〕

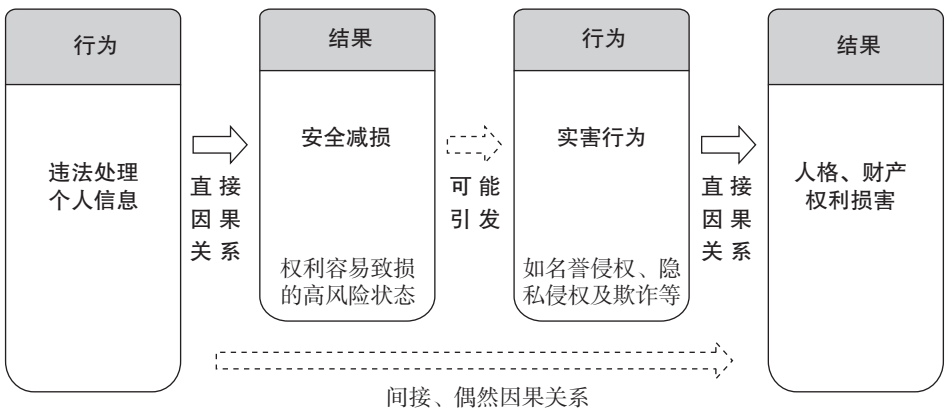

图 1　违法处理个人信息行为与权利损害结果关系示意图

〔18〕 参见《最高检发布检察机关个人信息保护公益诉讼典型案例——斩断个人信息侵权与电信网络诈骗之间的利益链条》，载 https://www.spp.gov.cn/spp/xwfbh/wsfbt/202104/t20210422_516357.shtml#1，最后访问时间：2021 年 11 月 26 日。

〔19〕 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；丁晓东：《个人信息的双重属性与行为主义规制》，载《法学家》2020 年第 1 期。

〔20〕 参见杨会：《浅论间接结合行为的界定》，载《法治研究》2013 年第 5 期。

三、安全减损源于个人信息识别特性

如前文所述，违法处理个人信息的直接后果是安全减损，而造成此种后果的根源就在于个人信息的“识别性”。他人识别个人信息的用途具有不确定性，故信息主体会因个人信息的不当处理而面临权利受损风险。如果无法识别个人，处理行为将不会引发针对个人的权利侵害。可见，不当处理个人信息减损安全的根源在于个人信息的识别本质，故个人信息识别性决定了个人信息保护的目的是安全。

（一）个人信息用于限缩范围以识别个人

国际标准化组织（ISO）将信息定义为“关于在特定语境下具有特定含义之客体——例如事实、事件、东西、过程或思想包括理念——的知识”〔21〕，这一定义凸显了信息对客体的“关联性”。作为信息的子项，“个人信息”增加了“个人”这一定语，故个人信息是与个人关联的信息。个人信息与个人的关联是“相关”还是“专属”，决定了个人信息的特性。

首先，个人信息不是专属于个人的信息，它向来为人们所共享。理由如下：其一，个人信息不是由个人生产出来的。记录个人信息的媒介往往由数据处理者提供，若没有记录媒介，个人信息难以存在，故个人和处理者均对个人信息的产生作出贡献，〔22〕个人信息不能单独为个人所有。其二，个人信息无法被自主控制，其价值在于交流。从古至今，无论是国家赋税还是社会活动，都需要每位成员提供个人信息以便管理，不提供个人信息的人通常是社会不安定因素。不同于有形、有限的物质，个人信息一旦为他人所知，便“一传十十传百”，不再受个人控制；个人信息可以被获得者同等、充分利用，再利用也不会使之贬值。故无论出于公共管理的目的还是社会生活的需要，信息主体必然会与他人分享个人信息而不将之独占。其三，个人信息由人共享。比如，每个人与亲朋共享自己的姓名以便相互称呼；熟人之间共享住址、联络方式等信息。显然，个人信息不专属于个人，且无论从伦理还是技术方面，我们都无法从与他人共享的信息中摘取专属个人的信息片段。而那些只有自己知道并不愿为他人所知的信息，是自己的隐私、秘密，而非用于交流的个人信息。

其次，个人信息不是泛指所有与个人有关的信息，而是在具体场景下对识别个人起到实质作用的信息。根据事物普遍联系的特性，一切信息都与个人具有千丝万缕的关联，若如此，个人信息将漫无边际。既然个人信息凸显的是与特定主体的关联性，故应当将其限定在有助于识别个人的信息范围内。一方面，个人信息是能够实质限缩识别范围的信息。前文案例中，行为人不当处理姓名、住址、电话号码、指纹和人脸信息等个人信息，减损信息主体的安全，这是因为以上个人信息能够反映个人特征、锁定个人并与之取得联系。其中，有的信息能够单独锁定个人，如指纹、虹膜和人脸信息（但需要相关技术支持）；而有的需结合其他信息，如姓名、住址、电话号

〔21〕 该定义原文为“Information：knowledge concerning objects，such as facts，events，things，processes，or ideas，including concepts，that within a certain context has a particular meaning”，载 https://www.iso.org/obp/ui/#iso：std：iso-iec：2382：ed-1：v1：en. 最后访问时间：2021 年 12 月 13 日。

〔22〕 参见前引〔8〕，彭诚信文。

码等需结合识别，从重名者或同一地区的人中锁定个人。尽管存在识别效率高低之分，但毋庸置疑，个人信息能够实际限缩识别范围。另一方面，个人信息是场景主义下的动态概念。识别是“根据特点辨别，做出判断，以便找出或认定某一对象”〔23〕的活动，是从不特定多数中辨认特定个体的过程，故那些不能反映个人特征、无法与他人区别的关联信息不属于个人信息。与集体成员共同的身份信息，相对于其他集体而言，能够反映一定的个人特征，属于个人信息；但在集体内部，则不具有缩小识别范围的作用，不属于个人信息。由此观之，个人信息的特性在于识别。

最后，个人信息处理活动正是利用了个人信息识别特性。在数字社会（尤其是数字经济）中，个人信息因作为商业分析的重要资源而具有商业价值，商家可运用个人信息形成的数据产品获得巨大商业利润。〔24〕而个人信息之所以能被分析和运用，正是因为它与个人稳定联系，据此得以把从真实的人身上得来的信息预测结果，再运用回真实的人身上，比如个性化推送抑或诈骗电话。如果个人信息处理针对的是抽象的或匿名的人，那么这种信息分析结果的利用将不具有针对性，只能依照所揭示的一般大众需要来开展商业活动，无法发挥个人信息的真正价值，如个性化推送和服务。因此，处理个人信息活动本质上是利用个人信息的识别特性开展后续的利益撷取。

有学者否定个人信息的识别本质，认为“随着大数据分析技术深度嵌入社会生活以及信息共享技术的广泛运用，大量不具有可识别性的信息能够按照特定的算法被关联、融合，进而能够将相关信息与特定的个人相联系”〔25〕。这种观点令人困惑，若不识别个人，将如何对抽象的分析结果进行具体运用呢？那些通过多重数据融合与交叉验证来确定信息主体的信息，〔26〕看似去除了个性化特征，但既然能够通过算法联系到个人，则说明这种“数据＋算法”具有限缩识别范围、辨别个人特征的作用。实际上，只要是从不特定多数中指向特定个人，则必然需要某些具备个性化因素的条件。

个人信息的识别本质，还可以由与其功能相反的“匿名”信息得出。根据《个保法》第 73 条可知，匿名的功能在于消除个性，使信息在客观上无法用于识别、锁定个人，并且，由于该信息不具有能够辨认个性化的内容，信息主体不会认为该信息与自己相关，即便发生违法处理也不会产生权利可能受到侵害的不安心理。因此，个人信息和匿名信息的根本区别就在于可识别性。《个保法》第 4 条第 1 款规定“个人信息……不包括匿名化处理后的信息”，将匿名化的信息排除在个人信息之外，这也意味着匿名信息不具有个人信息保护的利益。毋庸置疑，“识别”是个人信息的本质特征。

（二）可识别性决定个人信息保护的目的是安全

在利用个人信息识别特定主体的活动中，被识别者是具体、确定的，但识别者是谁、是否可被信任，以及识别后是否行为、行为对被识别者是否有害，这些问题在通信高度便利、违法成本极低的陌生人社会充满了不确定性。故识别活动本身具有风险，这决定了个人信息保护的目的是

〔23〕 中国社会科学院语言研究所词典编辑室编：《现代汉语词典》（第 7 版），商务印书馆 2016 年版，第 83、1185 页。

〔24〕 参见前引〔8〕，彭诚信文。

〔25〕 郑晓剑：《个人信息的民法定位及保护模式》，载《法学》2021 年第 3 期，第 120 页。

〔26〕 参见刘迎霜：《大数据时代个人信息保护再思考——以大数据产业发展之公共福利为视角》，载《社会科学》2019 年第 3 期。

风险控制，即保障安全。

首先，非自主选择的识别者的可信任程度较低。在所有识别活动中，最明确且最值得信任的识别者就是自己，而社会交往的需要使得个人信息不为个人所私有，〔27〕必须被他人识别。在多数情况下，人们分享个人信息并被他人识别，不能完全依据自己意愿作出决定。出于顺利开展社会交往的需要，人们不得不与软件平台、服务机构、所在单位、政府部门等分享能够识别自己的信息。由于这些组织中的识别者难以确定且不为人知，而被识别者通常缺乏技术且精力不足，因而无法对其充分监督，故这些识别者的可信任程度较低，无法保证其在获取个人信息后不对被识别者实施侵害。实践中，违法处理个人信息的往往是那些有信息处理能力又隐藏在幕后的识别者。

其次，他人在识别后实施违法行为的成本较低。在信息时代，个人信息被电子或者其他方式记录，并通常被上传至网络空间。具备一定信息处理能力的识别者，能够通过搜索、购买等方式获取那些被电子化记录的个人信息。识别者掌握的信息技术越发达，则越隐蔽，其被发现、追究的可能性越低，故实施后续违法犯罪行为的成本也就越低。可见，识别者通过处理个人信息而具有实施后续实害行为的可能，并因行踪、身份隐蔽而具备实施侵害的有利条件。故被识别者在他人识别其个人信息后，便处于被动的不安全状态。

最后，他人在识别后可能造成不确定的损害。被识别者是确定的，识别者可以利用个人信息将之准确锁定，但识别者是不确定的，其在识别之后将在何时、何地以及如何行为，这对被识别者而言充满了不确定性，因此，他人尤其是缺乏信赖关系的人识别个人信息，就像是一颗“不定时炸弹”，给个人权利带来诸多不确定因素。有学者将风险进行量化，试图将风险解释为损害而囊括到侵权法体系之中。〔28〕风险若可被量化、确定，则可以准确预防利益侵害，也可以适用侵权救济。但风险的可怕之处正在于无法估计和预测，其辐射范围亦不可确定。正因如此，才需要强调国家履行保护义务，防范违法处理带来不可挽回的后果。

综上可知，处理者能够利用个人信息创造效益，并在不当处理后造成个人安全的减损，根源在于个人信息具有“识别”特性。正因如此，规制个人信息的违法处理，防范处理者对主体的任意识别，就是为了保障主体的安全。

四、安全利益区别于侵权法益

在法经济学的视角下，各种权利义务充当法律行为的成本因素和收益因素，〔29〕而减损他人安全在客观上将增设防范风险的个人注意义务，并消耗国家预防违法犯罪的法律资源，这些在安全减损前后出现的利益变动表明，安全是一种包含人格、财产与公共利益的复合型利益。在违法处理个人信息引发权利损害的“事后环节”，权利损害能够“激活相关民事实体权益的救济机制”〔30〕，适用侵权法救济；但违法处理直接造成的安全减损，是一种理念上的抽象不利益，

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

〔28〕 参见田野：《风险作为损害：大数据时代侵权“损害”概念的革新》，载《政治与法律》2021 年第 10 期。

〔29〕 参见冯玉军：《法经济学范式》，清华大学出版社 2009 年版，第 231 页。

〔30〕 王锡锌：《个人信息权益的三层构造及保护机制》，载《现代法学》2021 年第 5 期，第 115 页。

不具有“已发生或迫近”与“具体”等侵权特点，且实践中风险防范支出要么不存在，要么因具有假设性或推测性而难以证明，〔31〕故亦不具有需要“填补”的利益损害。〔32〕因此，安全减损无法被视作侵权损害，安全利益区别于侵权责任保护的利益。

（一）安全是抽象的复合型利益

在现代化进程中，生产力的指数式增长，使风险和潜在自我威胁的释放达到了前所未有的程度，现代风险以系统的方式引发普遍甚至全球性的危险和不安。〔33〕贝克在提出风险社会的时候，人类还没有进入数字时代。时至今日，信息技术的威胁迫近。不当处理个人信息可能引发的权利损害，或许是大范围的甚至跨国性的。面对此等风险，国家积极采取保护措施，通过建构和运行一套关于个人信息处理的法律制度来履行保护义务，帮助个人对抗大规模、持续化信息处理中权利减损的风险，〔34〕“使风险处于社会观念可容忍的水准之下”〔35〕。是以在国家保护之下，违法处理个人信息将有损可信赖的安全秩序，引起个人和国家利益的变动。

一方面，违法处理个人信息为信息主体增设注意义务。数字背景下，个人信息与储蓄、不动产等私有财产以及人们重视的名誉、肖像等人格要素有着高度关联，而违法处理将突破国家对公民权利的基本安全保护，破坏被识别者对自身权利的安全预期，从而增加被识别者对自身权利的注意义务，即处理者将社会交往中应尽的控制或降低风险的危害防免义务转移给了被识别者。〔36〕注意义务的增设，迫使被识别者要么选择积极防御，以恢复至（令其感觉）安全的状态，由此承担实际支出和机会成本，即信息主体将有限资源用于防范风险而丧失其他用途的可能收益；〔37〕要么选择节省支出而忍受风险，由此承受可能出现的损害。可见，个人利益在违法处理前后产生变动，故安全是关乎信息主体权利的一项利益。

另一方面，违法处理个人信息将消耗国家机关的法律资源。由于违法处理个人信息为利用个人信息违法犯罪带来可能，而事后追究法律责任往往难以挽回受损利益，且难度大、耗时长，故国家机关出于正义和效率价值之考虑而倾向于采取事前预防，即通过规制违法处理个人信息活动，打击侵犯个人信息犯罪，以防范利用个人信息所实施的其他违法犯罪。正如检察机关所言：“打击利用互联网出售、提供、非法获取公民个人信息等侵犯公民个人信息犯罪，切断其与电信网络诈骗等犯罪的犯罪链条，从源头上预防和减少犯罪发生。”〔38〕显然，对违法处理行为的治理会增加国家机关的法律负担，消耗国家有限的司法资源，故检察机关常用“公共利益”来概括违法处理行为所侵害的对象。因此，保持权利处于安全状态，能节省国家机关在预防违法犯罪、维

〔31〕 See Emily Schmidt, *Article III Standing in Data-Breach Litigation: Does a Heightened Risk of Identity Theft Constitute an Injury-in-Fact?*, 49 Cumberland Law Review 389 (2019).

〔32〕 参见王泽鉴：《侵权行为》，北京大学出版社 2009 年版，第 175－176 页；王利明：《侵权责任法研究》（上卷），中国人民大学出版社 2010 年版，第 302 页。

〔33〕 参见〔德〕乌尔里希·贝克：《风险社会：新的现代化之路》，张文杰、何博闻译，译林出版社 2018 年版，第 3－7 页。

〔34〕 参见王锡锌：《个人信息保护的国家义务及展开》，载《中国法学》2021 年第 1 期。

〔35〕 王贵松：《论法治国家的安全观》，载《清华法学》2021 年第 2 期，第 24 页。

〔36〕 参见张新宝、唐青林：《经营者对服务场所的安全保障义务》，载《法学研究》2003 年第 3 期。

〔37〕 机会成本是指把一定的资源在用于某种用途时放弃其他用途所丧失的潜在利益。参见汪金锋、祁雄编：《西方经济学（微观部分）》，北京理工大学出版社 2018 年版，第 69 页。

〔38〕 2017 年 5 月 16 日《最高检发布六起侵犯公民个人信息犯罪典型案例》典型案例 3：“章某某等诈骗、侵犯公民个人信息案”，载 https://www.spp.gov.cn/xwfbh/wsfbt/201705/t20170516_190645.shtml#2. 最后访问时间：2021 年 12 月 13 日。

护法律秩序上的治理成本，故安全也包含公共利益。

综上可知，安全不仅是个人信息所蕴含的一种价值理念，〔39〕还是一种能够保障人们合理预期且客观存在的“人的生活利益”（menschliche Lebensinteressen）或“生活条件”（Lebensbedingung），〔40〕是一项包含人格、财产与公共利益的复合型利益。安全作为利益的成本收益分析，如图 2 所示。

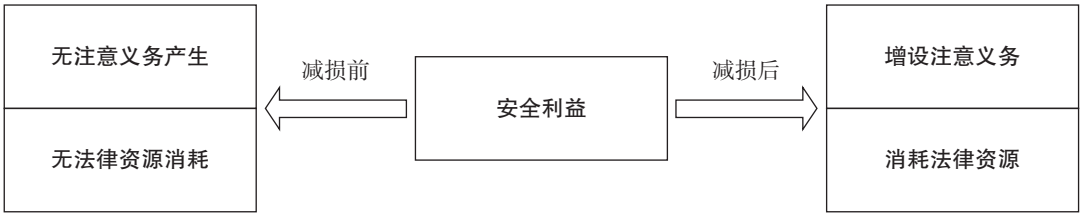

图 2　“安全”的利益分析

（二）风险不属于侵权损害

为化解个人信息保护中信息处理者责任无从追究的困境，有学者尝试把违法处理个人信息造成的“风险”解释为具有确定性的“损害”，由此将个人信息权益纳入侵权保护的范围，对处理者追究侵权责任。为满足成立侵权责任之要求，田野教授依靠证明风险的“高发性”和“利益差额”的可计算性，来解决风险作为“损害”的认定问题。〔41〕尽管违法处理所造成的权利风险升高客观存在，但由于风险发生的几率极低，且无法对风险升高前后的利益进行客观比较以确定损害，故风险升高作为“损害”的观点难以成立。此外，违法处理个人信息造成的风险，与侵权责任法中防御性请求权所对抗的危险有显著区别。后者是已着手的侵权行为所带来的紧迫且可被证明的妨害，前者是指发生侵权行为可能性的提升，二者所保护的利益并不相同。因此，安全利益区别于侵权法益。

1. 对风险“高发”的质疑

风险不具有高度盖然性和损害紧迫性。正如前文所述，违法处理个人信息并不定然带来人身、财产权利致损之结果，风险的发生属于偶然事件。在生活中，泄露或不当处理个人信息的行为大量存在，很多人身上都发生过接到推销房产、培训、保险等的本地、外地甚至境外陌生电话的情况，不少推销者清楚地知道接听者的姓名等个人信息，但实际上，由此发生电信诈骗、隐私刺探、恐吓骚扰、冒名顶替等情况的概率极小。“腾讯守护者计划”发布的《2017 年第四季度反电信网络诈骗大数据报告》显示，全国“第四季度诈骗电话拨打 1.6 亿次，收到诈骗短信人数为 467 万……诈骗案件共 23.9 万件”，即月均泄露和违法利用个人信息 0.55 亿条以上，而每月发生诈骗案件为 8 万件，故违法处理个人信息后诈骗风险的发生几率为≤0.15%。〔42〕综合这些数据

〔39〕 参见凌霞：《安全价值优先：大数据时代个人信息保护的法律路径》，载《湖南社会科学》2021 年第 6 期。

〔40〕 参见前引〔9〕，张明楷书，第 42 页。

〔41〕 参见前引〔28〕，田野文。

〔42〕 月均泄露和违法利用个人信息数量：(1.6+0.0467)亿条/3 月≈0.55 亿条/月；违法处理个人信息后诈骗风险的发生几率：8 万件/0.55 亿条=0.15%。参见《反电信网络诈骗大数据报告》，载 https://tg110.qq.com/newspage/report_center_20180208page1.html，最后访问时间：2021 年 11 月 17 日。

来看，在通信高度发达的数字时代，泄露、非法利用个人信息的行为在广泛、频繁地发生着，但是，利用个人信息实施诈骗等违法犯罪并造成实际损害的情况，相较于信息泄露等不当处理而言，少得多。因此，违法处理个人信息的风险“高发”实际指的是发生数量较多，而非发生几率较高。可见，个人信息处理致损的风险不具有高度盖然性。正因风险大概率不会暴发，且无法被预见何时何地暴发，故亦不具有紧迫性。

2. 对风险“损害”可计算的质疑

除不具有高发性外，风险还不具有确定性。田野教授尝试用三种“利益差额”来甄别、计算风险的“损害”，包括“个人信息暴露导致的风险升高”“预防风险的支出”“风险引发的焦虑”，但因缺乏可操作性与客观标准而无法用作“损害”的确定方法。

首先，“个人信息暴露导致风险升高”的利益差额无法证明。田野教授认为，风险在成为现实损害之前看起来风平浪静，实则暗流涌动，一旦暴发，想要补救为时已晚，因此，有必要在悲剧发生之前认可风险本身即是一种可获赔偿的损害。〔43〕但是，风险施加有害作用是“多么飘忽不定和不可捉摸”〔44〕。一方面，由于尚未出现实害行为，人身、财产权利在个人信息暴露前后不具明显差异，信息主体虽表示担忧，却仍能够正常行使权利。另一方面，风险升高是抽象的侵害，因不具有客观表现形态而不可预见，无从估算，无法举证，通常由主观感觉来认知，猜测权利在个人信息暴露后更易发生危害，而猜测性不符合侵权损害的确定性特征，故无法采取侵权救济。〔45〕

其次，预防风险的支出无法客观确定。基于理性经济人的理论假设，〔46〕面对权利风险，人们通常会在防御的支出与可能的损害之间进行利益对比，由此在忍受和防范之间进行选择。由于风险是否发生、何时何地发生以及发生的范围、程度等均无法预测，无法对风险升高前后的利益差额进行估计，遂无法作出理性选择。故在生活中，尽管违法处理个人信息案件频发，但多数人因无从对比而忍受权利风险，只有在侵害发生、权利受损后才选择维权，此时法院支持的诉讼请求是赔偿权利损害而非预防成本。田野教授以“沈晴与上海容蓁汽车用品有限公司姓名权纠纷案”为例，认为法院判令被告赔偿原告的 2500 元中，有部分属于预防风险的成本。但据判决书所述，“原告沈晴作为具有会计从业资格的财务工作人员，在正常的执业中受到了影响，产生了一定的财产损失”〔47〕，法院综合被告所得收益（即“减少必要用工成本”）和原告必要维权成本等因素，确定赔偿金额。可见，法院计算得出的赔偿金额是用于恢复原告财产损失的，而预防风险的支出在其中并未体现。在美国司法判决中，法院同样以无法确定损害（lack of a cognizable harm）为由，驳回信息主体的侵权赔偿请求。〔48〕因此，在违法处理个人信息致损的案件中，适用侵权救济的是权利损害，而非安全减损。

〔43〕 参见前引〔28〕，田野文。

〔44〕 前引〔33〕，乌尔里希·贝克书，第 15－16 页。

〔45〕 See Filippo Lancieri, *Narrowing Data Protection's Enforcement Gap*, 74 Maine Law Review 15 (2022); Steven Shavell, *Liability for Harm versus Regulation of Safety*, 13 Journal of Legal Studies 357, 357－363 (1984).

〔46〕 参见周林彬、董淳锷：《法律经济学》，湖南人民出版社 2008 年版，第 86 页。

〔47〕 上海市闵行区人民法院（2019）沪 0112 民初 26438 号民事判决书。

〔48〕 See Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 Texas Law Reriew 737, 737－739 (2018).

少数人具有较强的风险防范意识，在权利损害发生前积极防范风险，但无法通过侵权救济途径填补有关防范风险的支出。在“人脸识别第一案”中，原告为了防范权利风险而向法院提起诉讼，最终得到“合同利益损失及部分交通费”的赔偿与部分诉讼费的承担。其中，交通费的赔偿是基于违约责任而非侵权责任，诉讼费的支出亦未弥补。同样地，在“陈瑜婷与上海瑞慈瑞兆门诊部有限公司隐私权纠纷案”中，作为胜诉方的原告不仅没有获得维权支出的赔偿，还要承担主要的诉讼费用。可见，信息主体试图以侵权救济来恢复安全，但实际上并未由此填补防范风险的诉讼支出。此外，为防范风险而购买的风险监控和管理等商业服务（如保险、信用状况监督），其实际支出和机会成本具有较强的主观性。这是因为，风险无法被准确预见，信息主体遂无法采取针对性的防范措施，故其为恢复安全所做的实际支出均为猜测而非必需；此外，机会成本是一种假计成本，没有实际支出且不可计量。〔49〕因此，把猜测的预防支出和抽象的机会成本归责于违法处理行为，这将突破“过错责任”“过错与责任相适应”等侵权法原则。由此观之，采用“预防风险的支出”来确定风险造成的“利益差额”不具有可行性。

最后，风险引发的焦虑不应属于侵权法中的精神损害。一方面，依据《中华人民共和国民法典》（以下简称《民法典》）第1183条，侵权法的精神损害赔偿须以侵害“人身权益”或“具有人身意义的特定物”为基础，“只能对人格权受到侵害导致的精神痛苦、生理疼痛以及其他不良情绪提供补偿”〔50〕，故安全减损因缺乏人格权利损害而不能主张精神损害赔偿。另一方面，将焦虑这一主观感觉认定为精神损害，将造成法律秩序的混乱。如在陈瑜婷案中，信息主体虽表达了对安全的焦虑和担忧，但只停留在模糊的感觉上，对后续实害是否发生、何时何地发生、多大范围内发生以及造成何种程度的损失均不清楚。与这种焦虑相比，生活中因恋爱、婚姻、工作、学业等产生的诸般焦虑可能严重百倍，如果承认风险引发的焦虑为精神损害，那么将有无数伴侣、家人、单位、学校会出现在精神损害赔偿案件的被告席，造成滥诉。因此，将“风险引发的焦虑”解释为“利益差额”不具有可行性且将有害于法律秩序。

3. 与“危及人身、财产安全”之区别

《民法典》第1167条规定：“侵权行为危及他人人身、财产安全的，被侵权人有权请求侵权人承担停止侵害、排除妨碍、消除危险等侵权责任。”显然，该条作为防御型侵权责任的一般规定，也提到了“安全”。但是，这里的“安全”对应的是侵权行为带来的现实妨害和可预期危险，与个人信息保护的安全利益有显著不同。

根据民法学界通说，停止侵害、排除妨碍、消除危险可归结为妨害排除和妨害防止两个方面。〔51〕妨害排除适用于侵害行为已经发生或正在进行的情况，即以“因现存的妨害源而产生的妨害在持续”为要件。〔52〕在该情况下，人身、财产权利已实际受到妨害，亟需去除妨害权利行

〔49〕 参见李欣隆：《机会成本与道德的关系探微》，载《道德与文明》2018年第1期；毛洪涛：《西方经济学成本基本范畴研究》，载《会计研究》2000年第10期。

〔50〕 许中缘、崔雪炜：《论合同中的人格利益损害赔偿》，载《法律科学（西北政法大学学报）》2018年第3期，第129页；张新宝主编：《精神损害赔偿制度研究》，法律出版社2012年版，第57页。

〔51〕 参见杨彪：《非损害赔偿侵权责任方式的法理与实践》，载《法制与社会发展》2011年第3期；茅少伟：《防御性请求权相关语词使用辨析》，载《法学》2016年第4期。

〔52〕 参见前引〔51〕，茅少伟文。

使的“瑕疵”以恢复至完满状态。故妨害排除请求权所保障的，实为人身、财产权利本身。

妨害防止请求权以存在重复发生之危险为要件，行使于侵权行为发生之前，目的是使行为人不再从事威胁他人的特定行为。〔53〕其中，“危险”的概念决定了防御性请求权的边界。根据人格权法和物权法，防御性请求权所针对的危险应当是现实且可被证明的。《民法典》第 997 条的人格权禁令制度，是为更好实现《民法典》第 1167 条中有关人身利益安全的程序保障。〔54〕该条规定了权利人主张人格禁令的基本条件：行为人应当即将或正在实施侵害人格权的违法行为；且民事主体应就侵害行为以及可能造成的损害后果提交必要的证据等。〔55〕简言之，行使人格权妨害防止请求权，须能够证明存在紧迫或至少是可预见的现实威胁，而不能基于无法确定的、推测性的风险。〔56〕同样地，物权的妨害防止请求权并非请求权人主观上一感受到危险即可行使，〔57〕亦须满足对物的支配存在明确威胁之条件，即“根据一般的基准（标准）或情形，妨害（侵害）发生的危险性或可能性系明确、清楚”〔58〕。因此，妨害防止请求权所防范的是可预见、明确的现实威胁，且能够证明其权益受到的妨害存在着为社会所认可的确实可能性，而不能是无法预见、无法证明的风险。

总之，《民法典》第 1167 条规定的防御性请求权虽然涉及“安全”，但这与个人信息保护的安全并不相同。前者对应的是正在发生的妨害或可预见的现实危险，而后者对应的是无法预见和证明的风险，即相较于无违法处理时发生侵害行为的更大可能性。故个人信息保护的安全利益不是《民法典》第 1167 条中的“安全”，与侵权法益相互独立。

综上，个人信息保护的安全利益包含了人身、财产利益与公共利益，区别于侵权保护的法益。个人信息保护的安全利益是违法处理行为发生前，信息主体人身、财产保持原有低风险状态，以及公共法律资源未被增加使用的复合型利益。而侵权保护则主要是在侵权行为发生后对损害的填补，以及对正在发生的妨害和可预见的现实威胁的制止。有学者认为：“将个人信息权益理解为权益集合的观点会对整个侵权法的归责体系造成毁灭性破坏。”〔59〕但实际上，个人信息保护的利益目的和适用领域与侵权保护有着显著区别，前者并不会对后者取而代之。

五、《个保法》中安全法益的规范证成

违法处理造成的安全减损，因无法计算并证明损害结果而无法适用侵权法救济。但这并不意味着法律对该不利益状态的放任。通过规范分析可知，《个保法》正是用于防范和化解这种不利益，保护和恢复安全。

（一）《个保法》对违法处理的防范是为了保护安全法益

《个保法》规定了个人信息处理规则、处理者义务以及对处理活动的监督机制等，用来预防

〔53〕 参见曹险峰：《防御性请求权论纲》，载《四川大学学报（哲学社会科学版）》2018 年第 5 期。
〔54〕 参见程啸：《论我国民法典中的人格权禁令制度》，载《比较法研究》2021 年第 3 期。
〔55〕 参见张红：《论〈民法典〉之人格权请求权体系》，载《广东社会科学》2021 年第 3 期。
〔56〕 参见毕潇潇、房绍坤：《美国法上临时禁令的适用及借鉴》，载《苏州大学学报（哲学社会科学版）》2017 年第2 期。
〔57〕 参见范雪飞：《请求权的一种新的类型化方法：攻击性请求权与防御性请求权》，载《学海》2020 年第 1 期。
〔58〕 陈华彬：《论所有权人的物上请求权》，载《比较法研究》2020 年第 1 期，第 88 页。
〔59〕 前引〔7〕，程啸文，第 9 页。

违法处理行为的发生，规避信息主体的权利风险，保障信息主体的权利处于安全状态，即保护安全利益。

首先，《个保法》设置了规范个人信息处理的规则，约束处理活动以保护安全法益。一方面，“知情同意”是个人信息处理的合法基础与核心规则，〔60〕据此，信息主体依靠自身意愿与风险评估，来理性地选择是否进入信息处理活动之中。〔61〕另一方面，《个保法》要求处理活动符合必要（最小）原则，在有助于目的实现的必要范围内运用对个人权益影响最小的手段，包括收集最少够用的个人信息、个人信息不得用于其他目的、在授权目的与合理期限内合理使用或存储个人信息。可见，知情同意与必要原则的设置用于规制个人信息处理活动，使处理活动被限制在可容忍、可控的限度内，从而尽可能降低不当处理个人信息所引发的权利侵害可能，故其保障的是安全法益。

其次，《个保法》规定了处理者的义务，以保护安全法益。处理者采取必要措施最大程度保障个人信息安全，是个人信息处理必要原则的重要内涵。〔62〕为防止对个人信息进行未经授权的访问或违法处理，法律规定个人信息处理者应当依据“可能存在的安全风险”采取系列措施，包括：制定内部管理制度和操作规程，对个人信息实行分级分类管理，采取相应的加密、去标识化等安全技术措施，合理确定个人信息处理的操作权限，并定期对从业人员进行安全教育和培训，制定并组织实施个人信息安全事件应急预案（《个保法》第 51 条）。《个保法》为处理者设置的管理和组织等义务，防范的是“可能存在的安全风险”而非权利危险或损害，即保障信息主体的安全法益。

最后，《个保法》对个人信息处理活动设立了监督机制以保护安全法益，包括自我监督、国家监督和公民监督。在自我监督方面，法律要求“处理个人信息达到国家网信部门规定数量”的个人信息处理者，安排专人或设立专门机构，负责个人信息保护事务，并公布责任人姓名和联系方式，还要求个人信息处理者对其开展的处理活动与保护措施进行定期的合法、合规审计，对信息处理活动产生的风险进行动态监督、风险评估、报告发布等（《个保法》第 52—56、58 条）。在国家监督方面，法律规定了国家网信部门及有关部门对处理活动的监管职责，包括询问、查阅、复制、检查和调查等（《个保法》第 60—63 条）。在公民监督方面，法律赋予信息主体查询、复制等监督权利，赋予组织、个人投诉、举报的权利（《个保法》第 45、65 条）。这些机制的设置均用于对个人信息处理活动的常态化监督，对可能的侵权风险进行监控，以避免违法处理个人信息的发生，对安全法益予以保护。

由此可见，《个保法》通过设置处理规则、处理者义务以及监督机制，防范违法处理的发生，规避权利受损风险，使处理活动按照法定轨道开展，使潜藏于其中的权利风险保持在人们普遍接受和可控的限度内，使权利处于可信赖的安全状态，〔63〕即保护安全法益。

---

〔60〕 参见《关于〈中华人民共和国个人信息保护法（草案）〉的说明——2020 年 10 月 13 日在第十三届全国人民代表大会常务委员会第二十二次会议上》，载 http://www.npc.gov.cn/npc/c30834/202108/fbc9ba044c2449c9bc6b6317b94694be.shtml，最后访问时间：2021 年 12 月 26 日；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 年第 6 期；万方：《隐私政策中的告知同意原则及其异化》，载《法律科学（西北政法大学学报）》2019 年第 2 期。

〔61〕 参见前引〔19〕，梅夏英文；丁晓东：《个人信息保护：原理与实践》，法律出版社 2021 年版，第 67 页。

〔62〕 参见刘权：《论个人信息处理的合法、正当、必要原则》，载《法学家》2021 年第 5 期。

〔63〕 参见周学峰：《个人信息保护立法中的基础问题探讨》，载《北京航空航天大学学报（社会科学版）》2020 年第3 期。

（二）《个保法》对违法处理的规制是为了恢复安全法益

《个保法》规定了违法处理发生之后的规制，主要从处理者的义务履行、网信等部门的职责履行和信息主体的权利行使三个维度展开。分析可知，这些规制措施用于化解违法处理所升高的风险，对安全法益予以恢复。

首先，《个保法》要求处理者在违法处理后及时履行补救和通知义务，以降低风险，并使信息主体自主评估和控制风险。根据《个保法》第 57 条第 1 款，个人信息处理者采取补救措施的条件是“发生或可能发生个人信息泄露、篡改、丢失”，这表明此时尚未出现对信息主体权利的损害或威胁，故补救义务的内容是个人信息的不当处理状态而非权利损失。结合《个保法》第 57 条第 2 款可知，通知义务履行的条件是“履行个人信息保护职责的部门认为可能造成危害的”，其目的是使个人在知晓风险的基础上做好风险应对。若风险不可避免，及时告知个人泄露、篡改、丢失的信息种类、原因和可能造成的危害，已采取的补救措施和个人可以采取的减轻危害的措施，以及处理者的联系方式，亦是规避风险的必要之举。故《个保法》设置处理者在违法处理后的补救和通知义务，是出于恢复安全法益之目的。

其次，《个保法》设置了网信等部门对违法处理行为的惩治规则，为安全法益的恢复提供强制力保障。依据《个保法》第 64 条之规定，在监督过程中发现个人信息处理活动存在较大风险或者发生个人信息安全事件后，有关部门通过履行约谈、合规审计等职权，要求处理者“采取措施，进行整改，消除隐患”。从中可知，消除隐患是采取措施和进行整改的目的。“隐患”意指潜藏的祸患，即产生危害的可能，故对违法处理者的约谈、合规审计等是为了消除违法处理所带来的危害可能，即恢复安全。若处理者拒不改正，则依据《个保法》第 66—67 条之规定，有关部门有权对其处以罚款、没收违法所得等行政处罚。这正是《个保法》为安全法益的恢复所提供的强制力保障。

最后，《个保法》赋予公民“个人信息权利束”，目的是能够更高效地规制个人信息处理活动，〔64〕及时恢复安全法益。依据《个保法》第 46—50 条，信息主体通过行使更正、补充权利，使个人信息完整、正确；通过行使删除权利，使个人信息被最小化利用；在处理者拒绝个人行使权利请求之后，个人有权向法院提起诉讼。而保证个人信息的完整、正确和最小化利用，目的并非救济财产、人格损害，而是及时发现和纠正个人信息的违法处理行为，避免发生个人信息被违法利用并致其权利受损的情况。并且，这些“个人信息权利束”是在国家规制框架中对个人进行的赋权，是国家为保障安全法益而设置的监管机制的组成部分。〔65〕故《个保法》赋予工具性权利，亦是为了恢复安全法益。

综上，“个人信息权益”就是安全法益。《个保法》着重对违法处理行为本身进行规制，设置多种机制来保护和恢复安全。“安全”在我国《宪法》中以概括性的形式出现。《个保法》中的“根据宪法”条款表明，国家在个人信息保护制度中为个人安全提供保障，〔66〕故个人信息保护的

〔64〕 参见前引〔5〕，王锡锌文。

〔65〕 参见梅夏英：《社会风险控制抑或个人权益保护——理解个人信息保护法的两个维度》，载《环球法律评论》2022 年第 1 期。

〔66〕 参见前引〔35〕，王贵松文。

安全法益具有宪法基础。

六、结　语

个人信息权益不是财产、人格权利，而是安全法益，故个人信息保护与侵权保护是相互独立的两种制度。《个保法》第69条涉及违法处理个人信息致损的侵权责任，容易发生个人信息保护与侵权保护的混淆，需要予以说明。如前所述，“处理个人信息侵害个人信息权益造成损害”存在两个行为，即违法处理和实际侵害。违法处理不直接造成损害，故在损害发生前适用个人信息保护规则。在损害发生后的侵权救济中，由于处理者具有保障信息安全的严格的注意义务，并掌握证据资料和调查取证的技术优势，〔67〕更具有实施侵害的便利条件，故《个保法》第69条的侵权规则要求其承担过错推定责任。易言之，处理者若不能证明自己没有过错，则应当推定其对实害行为发挥积极作用，应承担损害赔偿等侵权责任。可见，《个保法》第69条不是个人信息保护与侵权保护的混淆，而是权利损害发生后两种保护规则的衔接。

Abstract: The rights of access, correction and deletion created by law are not the purpose of personal information protection. The damage to personality and property rights is not directly and inevitably caused by the illegal handling of personal information, but should be attributed to the subsequent independent infringement. Therefore, personality and property rights are not the object of illegal handling, nor the direct purpose of personal information protection. The direct consequence of illegal handling is to increase the risk of infringement to rights. Thus the interest of the nuisance is security. Security derogation causes the increase of duty of care and the consumption of legal resources. However, since the difference of interests cannot be proved and calculated, nor did foreseeable danger occur, tort remedy cannot be applied. Different from tort protection, the Personal Information Protection Act sets up norms of handling rules, rights and obligations, powers and responsibilities, and the purpose of which is not to compensate for damage, but to protect and restore safety. Personal information protection and infringement protection are relatively independent. Article 69 of the Personal Information Protection Act is a convergence of the two protections.

Key Words: illegally handling personal information, harmfully infringing, identifiability, tort protection, security legal interest

（责任编辑：殷秋实　赵建蕊）

〔67〕 参见孔祥稳：《论个人信息保护的行政规制路径》，载《行政法学研究》2022年第1期。

财经法学 No. 2，2023
pp. 21 - 35

敏感个人信息的界定及其完善

莫　琳*

内容提要：敏感个人信息的界定是我国《个人信息保护法》的重要内容。因为比非敏感个人信息更能反映和影响个人信息主体的重大利益，《个人信息保护法》对敏感个人信息采用更为严格的保护制度。《个人信息保护法》第 28 条第 1 款对敏感个人信息的界定采取客观风险标准。在法学视角下，“敏感”与“高度损害风险”相关联，敏感个人信息处理的损害风险程度较高。损害风险可以单独或同时来源于个人信息内容的固有性、个人信息被非法使用时的工具性以及非敏感个人信息与敏感个人信息的关联性。《个人信息保护法》对敏感个人信息的界定尚不能涵盖所有损害风险来源，应在第 28 条第 1 款的基础上辅以场景化路径界定敏感个人信息，具体以个人信息是否揭示或关联敏感内容、受损害主体是否包括其他关联利益人为客观考虑因素。

关键词：个人信息保护法　敏感个人信息　损害风险　场景一致性理论

一、引　言

2021 年 8 月 20 日，我国在个人信息保护领域的专门立法《个人信息保护法》出台，明确将个人信息分为敏感个人信息和非敏感个人信息。由于敏感个人信息比非敏感个人信息更能反映和影响个人信息主体的重大利益，且与个人人身、财产权利的联系更为密切，敏感个人信息在一般个人信息处理规则的基础上，适用更为严格的保护制度。《个人信息保护法》在第二章中设专节规定敏感个人信息的处理规则，主要包括：个人信息处理者处理敏感个人信息的前提条件为“具有特定目的＋充分必要性＋采取严格保护措施”（第 28 条第 2 款）；应当取得个人的单独同意或是书面同意（第 29 条）；处理不满 14 周岁未成年人个人信息应当取得其父母或者监护人的同意，

* 莫琳，暨南大学法学院博士研究生。
本文为国家社会科学基金重大项目“国际法与国内法视野下的跨境电子商务建设研究”（17ZDA141）的阶段性成果。

并为此制定专门规则（第 31 条）；应当遵守法律、行政法规规定的其他限制条件（第 32 条）。个人信息处理者处理敏感个人信息的义务还包括必须进行事前影响评估（第 55 条）。纵观不同法域的理论基础、立法情况以及行业规范，敏感个人信息保护规则存在的意义在于，防范其处理过程中极易产生的高度损害风险。敏感个人信息处理规则是我国《个人信息保护法》的重要内容之一，给予敏感个人信息特殊保护的做法与世界主流个人信息保护立法规则保持一致，标志着我国从制度上保证了个人信息保护体系的完善，为信息化社会中新型经济的有序发展提供了坚强有力的保障。

敏感个人信息特殊保护的首要问题应聚焦于如何界定敏感个人信息。《个人信息保护法》对此采取了“抽象概括＋非穷尽式列举”的界定方式。“概括”涉及法律如何给出概念（即下定义），“列举”涉及行为如何罗列。〔1〕其第 28 条第 1 款规定，敏感个人信息是指“一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息”。此为在法律规范中抽象界定敏感个人信息的内涵和外延，给予综合性定义，并明确列举敏感个人信息的非穷尽性示例。列举类型既依据信息内容，又以年龄为划分界限。该款规定凸显了我国当下急需保护的敏感个人信息类型，具备实践上的指引性，该表述也为未来技术与商业模式变化所可能出现的新型敏感个人信息预留了一定空间。

我国《个人信息保护法》中的“敏感”一词已完成由日常语境向法律语境的含义转化，但敏感个人信息的界定依然存在边界模糊的争议，尚不能涵盖所有损害风险来源。虽体现了敏感个人信息损害风险来源中的个人信息内容的固有性和个人信息被非法使用时的工具性，但却忽略了非敏感个人信息与敏感个人信息的关联性，难以及时跟上未来个人信息保护进程。因此，有必要进一步完善敏感个人信息的界定，以场景化路径丰富敏感个人信息的界定视角。本文首先深度剖析敏感个人信息的内涵，解释“敏感”一词在法律语境中的含义转化，对敏感个人信息的高度损害风险进行类型化分析。其次，基于损害风险来源检视我国《个人信息保护法》第 28 条第 1 款，进而结合场景一致性理论框架论述其在敏感个人信息方面的应用考量。最后，为推动我国构建多层次敏感个人信息保护体系而提出彰显时代性的敏感个人信息界定的完善建议。

二、敏感个人信息的内涵界定

（一）“敏感”一词在法律语境中的含义转化

如何理解法律语境中的“敏感”一词，是明确界定敏感个人信息内涵的首要前提。“敏感”在日常语境下具有较强主观性，通常用来表示个人的强烈感官输入。在心理学领域，敏感通常与焦虑等情绪相生相伴。“焦虑敏感性”是指应激事件使个体产生的担心、恐惧等情绪，是个体身上的一种稳定人格特质。〔2〕“感觉加工敏感程度”（sensory processing sensitivity，简称 SPS）

〔1〕 参见谢晓尧：《法律文本组织技术的方法危机——反思“互联网专条”》，载《交大法学》2021 年第 3 期。

〔2〕 参见杜艳玲、郎红娟、高丽、贺世喆、曹宝花：《军人焦虑敏感与心理应激关系及心理弹性中介作用的研究》，载《华南国防医学杂志》2021 年第 2 期。

被描述为一种由遗传决定的气质或人格特征，能够反映个体中枢神经系统敏感程度的增加以及个体对身体、社会和情绪刺激的深层次认知加工。〔3〕敏感情绪是一种“感官防御”（sensory defensiveness），与自身的经历、经验和行为有密切关系。〔4〕由于心理学上的个体敏感程度高低极具差异，“敏感”一词在法律语境中的含义需进行转化理解，不能直接以日常语义理解敏感个人信息。显然，敏感个人信息并非单纯指代“令个人产生敏感情绪的个人信息”。否则，无异于将界定敏感个人信息的决定权完全交由个人信息主体，缺乏明确标准。因此，在法学视角下，“敏感”与“高度损害风险”相关联，意味着处理敏感个人信息而产生的损害风险程度较高。通过剖析我国《个人信息保护法》第28条第1款的内在逻辑可知，界定敏感个人信息采取客观风险标准。正是由于敏感个人信息处理往往伴随着高度损害风险，才值得法律对其严格保护。

世界主流国家的敏感个人信息保护理论和实践，都基本完成了对“敏感”一词在法律语境中的含义转化。美欧信息隐私法认为敏感个人信息往往与更大的风险相关联，因此，对敏感个人信息处理进行风险评估是必不可少的步骤。〔5〕在个人信息保护中，风险评估具有重要意义。〔6〕根据美国法律，处理敏感个人信息被认为是高风险行为。21世纪初，美国《关于执行电子政府法案的指南》（Guidance on Implementing the E-Government Act）就已指出，考虑到个人健康和财务信息的隐私风险增强，要求监管机构在处理个人健康和财务信息前对其进行隐私风险影响评估。欧盟《一般数据保护条例》（General Data Protection Regulation，简称GDPR）以个人信息的性质为基石，在其鉴于条款中指出，敏感个人信息值得法律特别保护的基本理由在于，敏感个人信息在具体处理场景下可能会对个人基本权利和自由造成重大风险。〔7〕即敏感个人信息是其处理可能给基础权利和自由带来高度损害风险的一类个人信息。

“敏感”一词的法律化过程虽弱化了其主观性，但并非完全摒弃个人信息主体的内在感受。界定敏感个人信息离不开社会公众基于一般经验和生活常识的整体性价值认可。〔8〕法律依然需要考虑社会公众在具体场景下对个人信息敏感与否的认可程度，而非指个案中单一个人信息主体的纯粹心理情绪。保罗·欧姆（Paul Ohm）评估某一个人信息是否敏感时指出，需要考虑处理该个人信息的风险是否反映了多数主体的利益。〔9〕有学者对比多个国家和地区的隐私保护法律后发现，法律规范已列举的敏感个人信息类型获得社会公众的较高认可。〔10〕受区域历史文化、道德观念等多方面因素的影响，大多数国家和地区都认可医疗健康信息是敏感个人信息。其来源

〔3〕 See E. N. Aron, A. Aron & J. Jagiellowicz, Sensory Processing Sensitivity: A Review in The Light of The Evolution of Biological Responsivity, 16 (3) *Personality and Social Psychology Review* 262 (2012).

〔4〕 See Sofie Boterberg & Petra Warreyn, Making Sense of it All: The Impact of Sensory Processing Sensitivity on Daily Functioning of Children, 92 *Personality and Individual Differences* 80, 81 (2016).

〔5〕 See Muge Fazlioglu, Beyond the “Nature” of Data: Obstacles to Protecting Sensitive Information in the European Union and the United States, 46 (2) *Fordham Urban Law Journal* 271, 306 (2019).

〔6〕 参见刘颖：《我国〈个人信息保护法〉中的“守门人”条款》，载《北方法学》2021年第6期。

〔7〕 See General Data Protection Regulation, Recital 51.

〔8〕 See Karen McCullagh, Data Sensitivity: Proposals for Resolving the Conundrum, 2 (4) *Journal of International Commercial Law and Technology* 190 (2007).

〔9〕 See Paul Ohm, Sensitive Information, 88 (5) *Southern California Law Review* 1125, 1155 (2015).

〔10〕 参见王敏：《敏感数据的定义模型与现实悖论：基于92个国家隐私相关法规以及200个数据泄露案例的分析》，载《新闻界》2017年第6期。

于个人信息主体在医疗、健康、卫生领域的社会活动，不仅是反映个人人格权益的信息载体，还是具有公共属性的社会工具。〔11〕这反映了社会公众对某类个人信息是否敏感存在着合理期待，具有不希望其被泄露和非法使用的诉求。〔12〕因此，在具体场景中判断敏感个人信息是否符合社会公众的合理期待，应是法律所允许的合理考虑。

（二）敏感个人信息的高度损害风险

1. 损害的类型

敏感个人信息的高度损害风险不只是带来主观上的人格损害，即个人信息一旦被泄露或者被非法使用给个人信息主体造成的消极感受，还包括在客观上造成的人身损害和财产损害。第一，人格损害关乎个人基本权利与自由，如侮辱、羞耻以及遭受歧视性待遇等强烈主观性不适带来的精神损害。敏感个人信息的损害风险类型已从传统的识别型向歧视型、控制型扩散。〔13〕与非敏感个人信息相比，敏感个人信息更容易导致人格损害已在国际立法层面形成共识。1981 年，欧洲理事会公布的《关于个人数据自动化处理的个人保护公约》（Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data，简称 108 公约）特别指出，数据处理应采取保障措施防止敏感个人信息对个人信息主体的利益、权利和基本自由可能造成的风险，特别是造成歧视的风险。同时，反对任何形式的歧视行为也是联合国人权保护的重要内容。比如，未经本人同意透露一个人的遗传信息可能会使其在就业、保险、教育和社会生活的其他领域受到歧视。〔14〕“保障人权”和“守护人类尊严”等全球性伦理准则共同为保护敏感个人信息以防范人格损害提供了理论支撑。因此，宗教信仰、医疗健康以及特定身份等敏感个人信息被多数国家的个人信息保护立法所认可，并为不同国家的社会公众所普遍珍视。

第二，人身损害是指敏感个人信息的不当处理可能危及个人人身安全。涉及保障人身安全目的的敏感个人信息包括身份证件号码、电话号码、电子邮件地址、家庭和工作地址以及实时位置等信息。这些敏感个人信息的损害风险来源于，其能够高度识别个人身份并与个人人身安全相关联。一旦泄露极易被不法使用，容易导致个人信息主体遭受人身损害。

第三，财产损害指的是经济价值损失，包括财产实际损失和期待利益损失。例如，作为敏感个人信息的金融财务信息往往容易导致可以衡量的经济损害。支付宝平台中的花呗、芝麻信用等信贷产品改变了许多人的消费习惯。我国法院在案件处理过程中意识到，金融服务行业涉及诸多敏感个人信息类型，与公民的资金安全直接相关，若处理不当可能引发金融风险。〔15〕我国司法实践中已有不少案例表明，处理贷款情况、征信报告、银行流水账单等个人信息具有高度损害风

〔11〕 参见莫琳：《公共卫生安全视角下医疗健康个人信息的保护与限制》，载《电子知识产权》2022 年第 5 期。

〔12〕 参见吴标兵、许和隆：《个人信息的边界、敏感度与中心度研究——基于专家和公众认知的数据分析》，载《南京邮电大学学报（社会科学版）》2018 年第 5 期。

〔13〕 参见宁园：《敏感个人信息的法律基准与范畴界定——以〈个人信息保护法〉第 28 条第 1 款为中心》，载《比较法研究》2021 年第 5 期。

〔14〕 参见联合国经济及社会理事会决议《基因隐私权与不歧视（E/2004/L. 13/Rev. 1）》（2004/9 ）。

〔15〕 参见“蚂蚁科技集团股份有限公司与海南庆德大信息科技有限公司侵害商标权纠纷案”，杭州铁路运输法院（2020）浙 8601 民初 489 号民事判决书；“芝麻信用管理有限公司、蚂蚁科技集团股份有限公司等与山西有码科技有限公司侵害商标权纠纷案”，浙江省杭州市西湖区人民法院（2020）浙 0106 民初 4288 号民事判决书；“蚂蚁科技集团股份有限公司与杭州融动科技有限公司侵害商标权纠纷案”，浙江省杭州市西湖区人民法院（2020）浙 0106 民初 4289 号民事判决书。

险，符合社会公众对此类信息的认知程度和整体性期待。此外，处理敏感个人信息还容易造成期待利益损失。在相关案例中，个人信息处理者不当处理医疗健康个人信息，容易造成个人信息主体的期待利益损失。例如，药店留存的个人用药记录存在错误录入的情况，将导致消费者无法购买商业保险保障自身权益，之后就医使用医保卡也难以得到相关保障，〔16〕这对医疗健康个人信息的应用活动造成了财产损害。

2. 损害发生的可能性

损害发生的可能性是界定敏感个人信息时必须考虑的因素，这是敏感个人信息与非敏感个人信息的关键区别。我国《个人信息保护法》第 28 条第 1 款使用“容易导致”这一表述，实际上指向的是一种相对的概率，即损害发生的可能性。对于一般自然人而言，敏感个人信息本身并不必然具有明确的实质性价值，而是更多地体现为一种价值载体。个人信息处理者处理敏感个人信息过程中更容易侵害人格权利和人身、财产安全等实质性价值目标。由于敏感个人信息处理行为并非必然使个人遭受明确的、固定的损害，对敏感个人信息严格保护的目的不在于要求损害后果的实际发生，而是要求存在造成个人信息主体的不特定法益被侵害的可能性。

受个人信息处理者掌握的信息识别技术的应用能力、个人信息主体与个人信息处理者的特殊关系等因素影响，不同场景中损害发生的可能性存在差异。例如，随着现代电子信息技术的逐渐成熟，电子交易类型的个人信息更容易被个人信息处理者非法使用。再如，在医疗、法律等专业服务场景中，个人信息主体和个人信息处理者存在较强的信赖关系，个人信息处理者作为特殊信赖主体对个人信息主体负有保密义务。此时，一旦个人信息处理者超出原始目的不当处理敏感个人信息，损害发生的可能性便迅速增高。在我国《个人信息保护法》的立法过程中，敏感个人信息损害发生的可能性要求发生了变化。《个人信息保护法（草案）》和《个人信息保护法（草案二次审议稿）》采取相对宽泛的标准，无论何种类型的损害，其发生存在可能性即可，仅仅要求“可能”导致个人受到歧视或者人身、财产安全受到严重危害。而最终出台的《个人信息保护法》则反映了立法者的严谨考量，规定敏感个人信息是“容易”导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，明确了敏感个人信息损害发生的可能性较高。从“可能导致”到“容易导致”的表述，《个人信息保护法》对敏感个人信息处理行为提出了更高的合规要求，清晰指出处理敏感个人信息比非敏感个人信息更容易导致损害的发生，进一步明确我国个人信息保护体系，有益于全面提升个人信息保护水平。

三、基于损害风险来源检视我国敏感个人信息的界定

（一）敏感个人信息的损害风险来源

进一步而言，敏感个人信息的损害风险究竟来源于何处，是个人信息保护规范必须清晰认识到的另一重要问题。唯有如此，方能使敏感个人信息的界定趋于完善。保罗·欧姆认为隐私损害

〔16〕 参见“程某等与开州区亿鑫药品超市侵权责任纠纷案”，重庆市开州区人民法院（2020）渝 0154 民初 5576 号民事判决书；“程某等与开县长沙镇桔香村卫生室侵权责任纠纷案”，重庆市开州区人民法院（2020）渝 0154 民初 5749 号民事判决书。

(privacy harm) 揭示了敏感个人信息的多样性形式，主要涵盖固有敏感个人信息 (inherently sensitive information)、工具敏感个人信息 (instrumentally sensitive information) 和推断敏感个人信息 (inferentially sensitive information)。〔17〕本文借鉴此种分类方法，认为敏感个人信息的损害风险来源可以分为以下三种类型：个人信息内容的固有性、个人信息被非法使用时的工具性以及非敏感个人信息与敏感个人信息的关联性。敏感个人信息的损害风险可以单独或同时来源于以上三种不同类型。换句话说，只要个人信息满足三种来源中的一种，即应界定为敏感个人信息。

1. 个人信息内容的固有性

个人信息内容的固有性是指，信息内容所传达的实质含义是个人信息敏感与否的内在决定因素，同时也影响了潜在处理风险的高低。在处理个人信息过程中，信息内容本身一经泄露便容易导致个人信息主体遭受损害，使其具备敏感性。如医疗健康信息，其信息内容本身的泄露即可侵害人格尊严。欧盟立法机构始终坚持以保障人格权利为出发点进行个人信息保护，他们意识到个人信息内容的固有性便足以引起个人权益侵害风险，触发敏感个人信息的特殊保护机制。欧盟第 29 条数据保护工作组 (Article 29 Data Protection Working Party，简称第 29 条工作组) 强调，基于风险方法 (risk-based approaches) 评估个人数据处理风险时必须考虑个人数据的内容和性质。〔18〕由于历史背景和文化传统不同，损害风险来源于个人信息内容固有性的个人信息具体类别，最终因各法域的公众整体性期待和社会包容度不同而存在差异。例如，美国和欧盟法律均将政治观点明确列举为敏感个人信息，但对于财务信息是否作为敏感个人信息保护则有不同的选择。〔19〕而我国《个人信息保护法》列举的敏感个人信息中并未包括政治观点，仅在标准和指南等规范性文件中提及政治观点具有一定程度的敏感性。〔20〕

2. 个人信息被非法使用时的工具性

个人信息被非法使用时的工具性是指个人信息作为工具被非法使用时的损害风险。个人信息的工具性决定其具有社会性与公共性，体现在能够使得个人在社会中标识自己并与社会建立更为广泛的联系。〔21〕个人信息不仅是反映个人权益的信息载体，还是人类发挥主观能动性改造世界的重要决策依据，承载着在公共领域中发挥信息交换功能以促进社会进步的使命。在信息化时代，个人信息的财产属性日益凸显，作为社会交往工具的个人信息被非法利用的可能性陡然剧增。美国经济学家霍肯在 20 世纪曾断言，信息商品市场将取代传统的物质商品市场从而占据经济主导地位。在信息技术尚不发达的年代，个人信息通常被记录于纸质载体，不具备强烈的财产属性。但在信息化社会中，海量增长的信息数据被用于投入生产物品与劳务，成为实体经济产业

〔17〕 参见前引〔9〕，Paul Ohm 文，第 1170 页。

〔18〕 See Artical 29 Data Protection Working Party, Statement on the Role of a Risk-Based Approach in Data Protection Legal Frameworks, 2014, p. 4.

〔19〕 See Amitai Etzioni, A Cyber Age Privacy Doctrine: More Coherent, Less Subjective, and Operational, 80 (4) *Brooklyn Law Review* 1263, 1278 (2015).

〔20〕 参见《信息安全技术 个人信息安全规范》(GB/T 35273—2020) 第 9.4 条；《信息安全技术 公共及商用服务信息系统个人信息保护指南》(GB/Z 28828—2012) 第 3.7 条。

〔21〕 参见高富平：《个人信息保护：从个人控制到社会控制》，载《法学研究》2018 年第 3 期。

数字化发展的基础性战略资源。为了生活便利或获取经济利益，个人信息主体逐渐接受对敏感个人信息进行商业化利用的行为。随着技术允许虹膜、指纹、人脸等生物识别信息作为密码完成身份认证程序，生物识别信息的应用场景在不断拓展，指纹解锁、刷脸支付设备得到广泛应用。例如，被称为我国“人脸识别第一案”中的原告为了获取微信支付年卡费的便捷和经济利益，对身份证号、银行卡号等敏感个人信息采取了积极主动的商品化利用。〔22〕然而，在巨大的经济利益诱惑下，成熟的信息技术应用使得敏感个人信息容易被非法使用，从而导致高度损害风险。如今，个人信息处理者利用公民身份号码、电话号码、家庭地址等信息进行诈骗、跟踪等非法活动已经成为网络犯罪惩治的重中之重。

3. 非敏感个人信息与敏感个人信息的关联性

敏感个人信息的损害风险还可以来源于非敏感个人信息与敏感个人信息之间的关联性。信息分析技术日新月异，个人信息范围快速扩张。个人信息大量聚合处理极易模糊非敏感个人信息和敏感个人信息之间的边界，使得原本不敏感的个人信息通过结合其他个人信息亦能够揭示或关联敏感内容，这些推断结果容易产生侵犯个人信息权益的高度损害风险。消费记录并非法律明文列举的敏感个人信息类型，但在具体处理场景中，消费记录可以推断得出敏感个人信息或与敏感个人信息相关联的其他信息。比如，保险公司根据饮食消费记录推断得出个人健康信息，并据此针对消费者调整健康保险费用，很可能导致投保成本增加，使个人遭受经济价值损失。再如，肤色、身高等信息可以揭示健康或种族信息等敏感内容。

进一步而言，非敏感个人信息和敏感个人信息并非泾渭分明，它们之间可以相互转换。2021年，荷兰数据保护局（DPA）对于其国内一政治党派泄露了支持者电子邮箱的行为进行处罚。〔23〕在这一场景中，电子邮箱信息的性质发生了变化。电子邮箱由原本的一般个人信息可以转化成揭示政治观点的敏感个人信息。该党派支持者的电子邮箱信息被泄露，意味着电子邮箱持有者的个人政治观点信息同时被披露。因此，应当合理地认为，个人信息是否敏感还应在不同的场景中加以具体判断。在“庞理鹏与趣拿公司等隐私权纠纷案”中，我国法院即是运用了场景化认定方法对个人信息敏感与否进行具体分析。法官充分考虑了本案中预订机票的特殊场景，结合当事人行程安排信息推断原本属于一般个人信息的姓名、电话号码具有整体上的敏感属性。〔24〕“黄某与腾讯公司隐私权、个人信息权益网络侵权责任纠纷案”的法官也认为，判断个人信息内容的性质时，有必要深入实际处理场景，以“场景化模式”探讨该场景中是否存在侵害隐私的行为。〔25〕

（二）对我国《个人信息保护法》第28条第1款的检视

《个人信息保护法》第28条第1款以“抽象概括＋非穷尽式列举”界定敏感个人信息具有可

〔22〕 参见“郭兵诉杭州市野生动物园服务合同纠纷案”，浙江省杭州市富阳区人民法院（2019）浙0111民初6971号民事判决书。

〔23〕 See European Data Protection Board News, Dutch DPA: PVV Overijssel fined for failing to report data breach, available at https://edpb.europa.eu/news/national-news/2021/dutch-dpa-pvv-overijssel-fined-failing-report-data-breach_en, last visited on Jan. 23, 2022.

〔24〕 参见北京市第一中级人民法院（2017）京01民终509号民事判决书。

〔25〕 参见北京互联网法院（2019）京0491民初16142号民事判决书。

操作性，抽象概括为在法律实践中判断个人信息是否敏感提供了指引，非穷尽式列举又为新类型敏感个人信息的鉴别预留了一定空间。然而，明确列举的敏感个人信息类型具有强涵摄性，立法者的有限理性无法完全准确预测个人信息敏感程度之变化，现有的列举主义必将很快显得捉襟见肘，对判定普罗透斯之面似的敏感个人信息应接不暇。各列举项包含诸多具体的个人信息类型，应视作对敏感个人信息常见类别的提示。〔26〕若将列举信息类型一概认定为敏感个人信息，既可能保护过度又可能保护不足。因此，敏感个人信息的界定仍需置于处理场景中作具体判断。

对敏感个人信息的部分列举，似乎表明敏感可以被客观地归因于特定的个人信息类型。这种理解并不全面，实际上掩盖了敏感与相关场景因素之间的相互依存关系。我国《个人信息保护法》第 28 条第 1 款明确敏感个人信息容易导致个人人格尊严和人身、财产安全受到损害，体现了损害风险来源中个人信息内容的固有性和个人信息被非法使用的工具性，但却忽略了非敏感个人信息与敏感个人信息之间的关联性。敏感个人信息的表现形式日益丰富，忽视非敏感个人信息与敏感个人信息之间的关联性容易导致该条款的实际适用障碍，无益于敏感个人信息主体的个人权益保护和信息化技术的更新迭代。

场景化界定路径是司法实践中具体判断敏感个人信息范畴的可行路径。敏感个人信息范畴之所以难以准确界定，与敏感个人信息保护和其他权利的冲突，以及实践中判断敏感与否高度依赖具体处理场景有关。个人信息保护立法需要特别关注非敏感个人信息和敏感个人信息之间的关联性和可转化性。在高度损害风险标准之下，敏感个人信息的界定须结合场景因素，融入场景化界定路径。如从血液中提取的蛋白酶信息和 DNA 信息是否敏感，需结合个人信息处理者应用能力、识别能力和识别目的等具体场景因素进行综合判断。为了避免敏感个人信息的界定无法回应科技进步带来的新问题、无法解决司法实践中出现的新情况，应在现有“抽象概括＋非穷尽式列举”界定方式的基础上，辅以场景化界定路径构建多层次敏感个人信息保护体系，方能使我国《个人信息保护法》在基本理念上顺应历史发展规律，为敏感个人信息保护和信息化经济建设的长足发展预留充分的空间。

四、敏感个人信息场景化界定路径的理论框架及应用考量

（一）场景一致性理论框架

大数据处理场景的广泛性已然宣告场景化时代的到来，站在科技的风口上，便真如斯考伯和伊斯雷尔所预测的那样，占据场景便能赢得未来。〔27〕在复杂的网络传播环境下，能否掌握个人信息处理场景已经成为信息产业角力的重要考量。在信息传播场景化导向的背景下，个人信息处理场景日趋多元，个人信息保护立法及后续配套政策和标准文件必须尽快形成对策，以应对个人信息处理场景的复杂性。因此，个人信息场景化保护愈发受到学界的广泛关注。

〔26〕 参见前引〔13〕，宁园文。

〔27〕 参见〔美〕罗伯特·斯考伯、谢尔·伊斯雷尔：《即将到来的场景时代》，赵乾坤、周宝曜译，北京联合出版公司 2014 年版，第 1 页。

由于个人信息商品化活动持续活跃，〔28〕美国学者较早重视个人信息保护，认为个人信息是一种新类别的“黄金”，大力倡导对个人信息的场景化保护。〔29〕近年来，我国学者曾尝试论证场景化保护应用于我国个人信息保护领域的合理性，大多受到美国学者海伦·尼森鲍姆（Helen Nissenbaum）的场景一致性（contextual integrity）理论的启发。场景抽象地泛指日常生活中经历着的各种独立性社会空间，主要包括技术场景、商业场景、行业场景和社会场景四类理解，海伦·尼森鲍姆倾向于将场景理解为社会领域（social domain）。〔30〕场景由决定和支配着行为者、行为和限制等关键方面的规范构成，来源包括历史、文化、法律、惯例等。〔31〕场景既包括空间和环境，也包括具体行动的实时状态，其作为社会交往的基础条件和核心构成显示出强烈的流动性。〔32〕尊重场景即是遵守各领域的内生规范。

在美国隐私政策碎片化的背景下，场景一致性理论深受迈克尔·沃尔泽（Michael Walzer）的多元正义理论（pluralist theory of justice）影响，倡导尊重隐私保护的场景以挑战传统隐私保护理论。场景一致性理论被称为“隐私的替代基准”，以“适当性规范（appropriateness）—流动性规范（distribution）”为保护框架探析公民对公共监控（public surveillance）的不安根源，以应对信息技术带来的隐私挑战。场景一致性理论立足于预期的个人信息流（personal information flow），依据不同场景中的具体因素来保护信息隐私，强调个人信息的衍生利用行为不得与初始场景相悖，以确保个人信息流通适当。以场景中的规范来评估个人信息处理行为是否侵犯隐私取决于三个关键变量，包括行为主体（actors）、信息类型（information types）和传输原则（transmission principles）。〔33〕若有任何一个变量存在问题，就会出现“表面上的违反”（prima facie violation）。因此，个人信息的收集和传播必须在具体场景中是适当的，并遵守该场景的内部流通规范。

适当性规范是个人信息场景化保护的基础，要求在特定场景中，某一类信息的处理符合常理且具有必要性。如在医疗环境中，患者向就诊医生提供个人健康状况信息是恰当的，反之则为不恰当。流动性规范强调衍生数据的合理使用，要求个人信息从发送方向接收方或其他第三方的转移尊重个人信息流的场景规范。这与多元正义理论强调每个领域都有属于本领域的独特正义规范保持一致。“个人信息的使用和流通是否遵守信息流的场景规范”与“个人信息在某个特定场景中的使用具有适当性”同等重要，共同构建了有序利用个人信息的场景化监督体系。〔34〕场景一致性理论揭示了社会领域对适当性个人信息流的高度依赖，强调信息隐私逐渐涵括个人信息被恰当流通的权利。在现代生活中，信息隐私极具相对独立的社会空间性，倘若脱离了场景而孤立地审视个人信息，便无法准确判断该个人信息处理行为是否侵犯个人隐私。因此，尊重场景，便是

〔28〕 See Paul M. Schwartz, Property, Privacy, and Personal Data, 117 (7) *Harvard Law Review* 2056, 2069 (2004).

〔29〕 See Helen Nissenbaum, Privacy as Contextual Integrity, 79 (1) *Washington Law Review* 119, 121 (2004).

〔30〕 See Helen Nissenbaum, Respecting Context to Protect Privacy: Why Meaning Matters, 24 *Science and Engineering Ethics* 831 (2018).

〔31〕 参见前引〔29〕，Helen Nissenbaum 文，第 138 页。

〔32〕 参见王敏芝：《媒介化时代“云交往”的场景重构与伦理新困》，载《暨南学报（哲学社会科学版）》2021 年第9 期。

〔33〕 参见前引〔30〕，Helen Nissenbaum 文。具体而言，信息类型与信息性质相关；行为者系场景中涉及的角色，包括主体、发送方和接收方的参与人；传输原则包括个人信息共享和进一步传播的条件以及在场景中因素变化的潜在影响阈值等。

〔34〕 参见林凌、程思凡：《个人信息场景化传播困境及保护研究》，载《当代传播》2021 年第 5 期。

尊重权利人在不同社会空间中的隐私诉求。

（二）场景一致性理论应用于敏感个人信息界定的考量

场景一致性理论认为，个人信息的敏感程度是决定隐私侵权发生与否的关键因素。该理论解决隐私侵权问题的思路在于，摒弃传统上的敏感与非敏感个人信息的固定二分法，充分考虑信息处理场景判断个人信息敏感与否，并运用场景规范使个人信息处理活动符合“适当性规范—流动性规范”保护框架。〔35〕由于个人信息的敏感程度极不稳定，容易在不同的个人信息处理场景下发生变化，〔36〕需要对个人信息进行差别化场景保护。场景一致性理论中的“敏感”概念极具隐私意义，在很大程度上保留了心理学上的主观色彩。其认为界定敏感个人信息除了符合社会公众心理预期的客观标准之外，还应该在具体场景中考虑个人信息主体的主观感受，以此评估个人信息处理是否可能给个人信息主体带来损害风险。个人信息敏感与否取决于个人信息主体对信息处理场景的预测与假设，如果个人信息的处理活动违反了个人信息主体的合理期待，便会产生自身利益受到侵害的主观感受。〔37〕但即使是同一种类型的个人信息，个人信息主体在具体场景中依然会产生不同的主观感受，代表着不同的合理期待。〔38〕例如，个人政见信息在政治会议场景中处理是合适的，但不适合被应用于零售、医疗等场景。因此，当个人信息主体认为某一类型信息为敏感个人信息时，便同时确定了其对该类型个人信息在特定处理场景中的合理期待。《金融服务现代化法案》（Gramm-Leach-Bliley Act，简称 GLBA）中对敏感个人信息的保护便体现了极强的主观考量，从遵循个人信息主体的意愿角度区分敏感个人信息，一旦个人信息主体认为某一个人信息具有敏感程度，即可拒绝金融机构对该个人信息进行处理。〔39〕

场景一致性理论以多元正义理论为基石，力图避免某一场景内侵犯隐私的“暴政”，有助于应对信息科技时代下的公共监视问题，从而具有很强的政治哲学意义。在识别一种新的信息应用实践如何影响隐私权利方面，该理论是非常有效的。〔40〕然而，场景一致性理论有其自身的局限性，从而决定其无法具有独立的规范效力。场景是保护隐私的重要因素，但它不应该取代包括敏感个人信息保护规则在内的启发式规则。〔41〕许多学者试图进一步发展场景一致性理论思想并将其应用于实践，但均发现这一概念并不容易融入正式法律。〔42〕

---

〔35〕 参见前引〔29〕，Helen Nissenbaum 文，第 136 页。

〔36〕 See Kirsten Martin & Helen Nissenbaum, Measuring Privacy: An Empirical Test Using Context to Expose Confounding Variables, 18 (1) *Columbia Science and Technology Law Review* 176, 215 (2016).

〔37〕 See Helen Nissenbaum, A Contextual Approach to Privacy Online, 104 *the Journal of the American Academy of Arts & Sciences* 32, 38 (2011).

〔38〕 See Paula Kift & Helen Nissenbaum, Metadata in Context: An Ontological and Normative Analysis of the NSA's Bulk Telephony Metadata Collection Program, 13 (2) *A Journal of Law and Policy for the Information Society* 333 (2017).

〔39〕 See Federal Trade Commission, How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act, available at https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm, last visited on Jan. 4, 2023.

〔40〕 See Gabe Maldoff & Omer Tene, Putting Data Benefits in Context: A Response to Kift and Nissenbaum, 13 (2) *A Journal of Law and Policy for the Information Society* 383 (2017).

〔41〕 参见前引〔9〕，Paul Ohm 文，第 1146 页。

〔42〕 See Bernd Justin Jütte & Annelies Vandendriessche, Responsible Information Sharing: Converging Boundaries between Private and Public in Privacy and Copyright Law, 10 *Journal of Intellectual Property, Information Technology and Electronic Commerce Law* 310 (2019).

其一，场景一致性理论中的场景因素复杂繁多，若独立运用其界定敏感个人信息缺乏可供实践的明确标准。场景是一个模棱两可的术语，它有可能使任一个人信息在某一场景下成为敏感个人信息。〔43〕并且，场景是影响个人信息处理风险的外因。〔44〕倘若判断个人信息敏感与否仅仅依据场景，则使敏感个人信息保护制度陷入被动，法律规则的预防功能将无法实现，进一步加深司法实践中认定敏感个人信息的标准鸿沟，为个案判断带来不堪重负的压力。其二，场景一致性理论下，从隐私权利中衍生的“敏感”概念过于宽泛，强调个人信息主体对敏感个人信息处理场景的个体性期待，以超强的主观感受界定敏感个人信息，并以此评估个人信息处理风险，难以达成充分发挥敏感个人信息保护兼具个人属性和社会属性的平衡效果。司法实践中，法院判断微信好友列表和读书信息的性质时，认识到敏感个人信息保护和隐私保护均体现了自然人的人格尊严和人格自由价值，但个人信息权益同时涉及信息利用和流通价值。〔45〕因此，敏感个人信息保护与隐私保护的不同之处在于，后者保护个人不愿为他人知晓的信息私密性，强调个人主观意愿，前者更强调个人信息不当利用导致信息主体遭受的客观风险。进一步而言，即使在相对一致的场景下，由于互联网产品和相应用户的广泛性和差异性，不同个人信息主体对同一信息具有不同程度的敏感期待。如在电子商务平台购物时，有的用户对针对性的广告推送十分反感，而有的用户则乐意接受该定向广告推送带来的便利。显而易见，若敏感个人信息是指信息被披露便使个人信息主体容易感到尴尬或不安的信息，那么在此定义下，所有的个人信息都有可能因其披露条件的变化而变得敏感。这会引起敏感个人信息过强保护的失控局面，“同案不同判”的司法诉累情况将不可避免。

鉴于场景一致性理论中个人信息“敏感”概念的自身局限性，场景化保护不能独立作为界定敏感个人信息的路径。因此，场景一致性理论可为我国《个人信息保护法》第 28 条第 1 款提供一种理论上的启发和制度上的有益补充，但实践难题的具体适用方案仍需进行适当调整。

五、我国敏感个人信息界定的完善

梅因深刻地指出，社会需求和社会主张总是或多或少地领先于法律，我们可能会无限地接近弥合它们之间的鸿沟，但永久的趋势是他们会重新拉开差距；因为法律是稳定的，社会是进步的，一个民族的幸福程度取决于鸿沟缩小的速度。〔46〕个人信息保护作为信息化社会经济生活迅猛发展的制度保障，必须紧密结合特定时期的社会需求和社会主张，不断适应社会生活变化，及时回应和解决个人信息保护面对的现实问题。目前，实践中我国《个人信息保护法》在界定敏感个人信息的具体类型方面存在较大解释空间。在科技爆炸时代，法律规范界定敏感个人信息应与时俱进，才能有针对性地回应由科技进步带来的种种新问题，并充分满足信息化社会中敏感个人信息保护的需要。我国尚未形成完善的敏感个人信息保护体系，此时寻求敏感个人信息界定的更

〔43〕 参见前引〔30〕，Helen Nissenbaum 文。

〔44〕 参见前引〔13〕，宁园文。

〔45〕 参见北京互联网法院（2019）京 0491 民初 16142 号民事判决书。

〔46〕 See Henry Sumner Maine, *Ancient Law*, Cosimo Classics, 2005, p. 15.

优解，以有效发挥我国个人信息保护立法的后发优势可谓正当其时。本文建议在《个人信息保护法》第 28 条第 1 款的基础上，辅以场景化路径以完善敏感个人信息的界定，具体考虑个人信息是否可以揭示或关联敏感内容、受损害主体是否包括其他关联利益人，最终构建多层次敏感个人信息保护体系。

（一）辅以场景化界定路径构建多层次敏感个人信息保护体系

我国个人信息保护理论和法律实践中应具备不采取一刀切的方式来理解和保护敏感个人信息的智识。将敏感个人信息概括划入相对固定的概念中，并不是有效保护敏感个人信息的唯一选择。实证研究已经表明，个人信息敏感与否离不开信息处理场景的考量。〔47〕性别、出生日期、籍贯等人口统计学信息通常被认为不敏感。但在求职场景中，人口统计学信息与身份号码、照片、健康状况等个人信息相结合，其敏感程度陡然增高，应被认为属于敏感个人信息。此前，我国的行业标准指南在界定敏感个人信息时，已经体现场景化界定的思路。各行业敏感个人信息的具体内容根据接受服务的个人信息主体意愿和各自业务特点确定，〔48〕为敏感个人信息的场景化界定留下解释空间。在我国司法实践中，场景化界定也已欣然可见，司法机关立足于具体场景衡量个人信息敏感程度。在一般生活场景中，特别是熟人群体中，真实姓名并不敏感，但在电子商务交易中真实姓名则被认为属于敏感个人信息。在“安娜与淘宝公司网络服务合同纠纷案”中，法院认为电子商务平台的自然人商家在开设淘宝店铺时留存的真实姓名、手机号码等个人信息具有敏感性，不宜全部对外公示。〔49〕淘宝公司作为平台经营者，对自然人商家在开设店铺时留存的敏感个人信息有保障责任。

未来，针对不同的信息处理场景，单一的敏感程度衡量标准应当发展成一个差异化、动态调整的标准体系。我国《个人信息保护法》应在积极利用概括列举式界定保持敏感个人信息保护体系可操作性的同时，以场景化界定路径作为补充和辅助手段。一是规定其他规范性文件可以参考各行业特点，定期适当调整敏感个人信息范围；二是在具体个案中，由司法机关依据信息处理的特殊情况，判断法律规范明文列举范围之外的个人信息是否属于敏感个人信息；三是通过执法和司法实践的不断归纳总结，结合技术专家组的意见，形成更具场景操作性的敏感程度界定标准。把定期调整、更新敏感个人信息清单的权利适当下放给各行业领域，可以全面保障敏感个人信息保护的有效性。允许各行业领域进行场景化界定可使敏感个人信息保护更契合行业特征，有利于对法律规范并未明文列举的敏感个人信息作出差异化安排，加快构建多层次敏感个人信息保护体系。

（二）敏感个人信息场景化界定路径的客观考虑因素

1. 个人信息是否揭示或关联敏感内容

敏感个人信息的损害风险不仅来源于个人信息内容本身和被非法使用时的工具性，还来源于

〔47〕 See David L. Mothersbaugh et al., Disclosure Antecedents in an Online Service Context: The Role of Sensitivity of Information, 15 (1) *Journal of Service Research* 76 (2012).

〔48〕 参见《信息安全技术 公共及商用服务信息系统个人信息保护指南》(GB/Z 28828—2012) 第 3.7 条。

〔49〕 参见杭州互联网法院 (2019) 浙 0192 民初 5468 号民事判决书。

非敏感个人信息与敏感个人信息的关联性，后者往往容易被法律所忽视。在大数据和人工智能时代，我国《个人信息保护法》需要特别关注敏感个人信息和非敏感个人信息之间的转化可能。美欧个人信息保护法律中的敏感个人信息范围，包括能够揭示或关联所列信息种类的个人信息。欧盟1995年的《数据保护指令》（Data Protection Directive，简称DPD）和GDPR规定特殊类别的个人信息时，同时使用了“揭示”（revealing）和“关联”（concerning）的表述。根据GDPR第9条第1款规定，敏感个人信息包括可能揭示种族或民族起源、政治观点、宗教或哲学信仰、工会成员资格的个人数据，以及有关健康、自然人的性生活或性取向的数据。对此，应理解为敏感个人信息不仅涵盖了在信息性质上具有敏感程度的信息，还包括可以揭示和关联敏感内容的个人信息。〔50〕欧洲数据保护委员会（European Data Protection Board，简称EDPB）指出敏感个人信息除了明确列举的种类，还包括其他被认为敏感的个人信息。〔51〕举例而言，照片并非GDPR所列举的敏感个人信息种类，但GDPR仍然承认在具体场景中认定照片的敏感程度。如果处理照片时使用了能够识别自然人的特殊技术手段，照片可被敏感个人信息中的生物识别信息的定义所涵盖。第29条工作组也认为，如个人照片和图像可以显示种族或健康信息，可被视为敏感个人信息。〔52〕美国《弗吉尼亚州消费者数据保护法》（The Virginia Consumer Data Protection Act）、《加州隐私权利法案》（The California Privacy Rights Act）、《华盛顿州隐私法案》（The Washington Privacy Act）等法律界定敏感个人信息范围也使用了关键词“揭示”。美国的立法草案中，敏感个人信息范围囊括了处理或传输是为了识别敏感个人信息的其他任何类型的信息，以及与敏感个人信息定义中各信息种类相关的个人信息，〔53〕进一步强化了避免因为信息类型之间的相互转化而逃脱监管的情形。

敏感个人信息范围不局限于法律规范所列举的信息类型，非敏感个人信息结合其他额外信息可能与敏感个人信息相关联，或者可以揭示敏感内容。如电子商务平台收集的手机号码、收货地址等个人信息与购物列表、搜索记录等辅助个人信息结合起来，可以揭示或关联个人信息主体的宗教信仰等敏感内容。在此场景下，手机号码、收货地址、购物列表和搜索记录可一并属于敏感个人信息。假设个人信息处理者已知一个清真寺的地理位置，同时获取了个人信息主体前往该地理位置的频率信息，则个人宗教信仰信息已然被揭示。因此，此场景中的地理位置信息应当被认定为敏感个人信息进行特殊保护。此外，揭示犯罪历史和人物社会危险性的犯罪记录、能够从中推断学生品行的教育记录等个人信息，因与敏感内容密切关联也应属于敏感个人信息。然而，我国《个人信息保护法》并未强调能够揭示或关联敏感内容的个人信息为敏感个人信息。因此，《个人信息保护法》中敏感个人信息界定的完善思路应该着眼于能够覆盖损害风险来源的因素。揭示或关联敏感内容的个人信息也应列入敏感个人信息范围，此为场景化界定

〔50〕 See Artical 29 Data Protection Working Party, Advice paper on special categories of data (sensitive data), 2011, p. 5.

〔51〕 See European Data Protection Board, Recommendation 01/2019 on the draft list of the European Data Protection Supervisor regarding the processing operations subject to the requirement of a data protection impact assessment [Article 39. 4 of Regulation (EU) 2018/1725], 2019, p. 5.

〔52〕 参见前引〔50〕，第29条工作组文件，第8页。

〔53〕 See United States Consumer Data Privacy Act of 2019; Consumer Online Privacy Rights Act.

路径的重要内容。

2. 受损害主体是否包括其他关联利益人

一般而言，非敏感个人信息仅仅影响个人信息主体。而敏感个人信息因具有高度损害风险，更容易导致个人信息主体本身以外的其他受到实质性影响的关联利益人同时遭受损害。因此，受损害主体包括其他关联利益人的个人信息也应被认为是敏感个人信息。敏感个人信息保护规则应同时保障个人信息主体以及其他受到实质性影响的关联利益人。唯有如此，才能真正保障敏感个人信息主体的切身利益免受损害。对于受损害主体问题，GDPR 第 82 条规定“任何遭受物质或非物质损害的人”都有权获得控制者或处理者的赔偿。普遍的限制性解释是，GDPR 最终旨在保护数据主体的权利，只有数据主体才能援引第 82 条获得民事救济。但有学者不同意这种限制性解释，认为有权获得损害救济的主体应扩大解释为任何可能遭受损害的人。〔54〕这符合 GDPR 的宗旨，即毫无例外地保护自然人的所有基本权利和自由。诸如，遗传基因信息的不当使用所造成的损害深远、长久而不可逆，且受损害主体难以预计。联合国经济及社会理事会决议《基因隐私权与不歧视》也承认，与一个可识别的人相关的遗传信息有时可能与该人家庭成员或其他人有关，因此在处理这类个人信息时也应考虑到关联利益人的权益。我国《个人信息保护法》要求网信部门统筹协调、推进敏感个人信息保护具体规则的制定工作，构建完善的敏感个人信息保护体系的重要性不言而喻。敏感个人信息的界定是较为复杂的系统工程，我国需充分考虑敏感个人信息场景化界定的客观因素，确保敏感个人信息保护的多维视角。

六、结　语

信息技术对人类社会影响的深度和广度都是空前的，个人信息保护和利用的角力在敏感个人信息方面表现得更为焦灼。敏感个人信息保护的目标应是在充分保护个人信息主体重大利益的同时，尽可能地释放敏感个人信息的社会价值。如今，部分敏感个人信息已存在合法进入数据市场的现实需求。如医疗健康个人信息不仅关乎个人权益，还在很多场景中蕴含极大的公共利用价值。《福州市健康医疗大数据开放开发实施细则》中就有关于根据不同的处理场景对敏感个人信息进行脱敏脱密处理后开放的规定。

法律无法脱离社会经验而存在。敏感个人信息保护体系不应也无法抛弃个人信息主体集合下的实质性利益，对敏感个人信息的界定正需要基于生活经验尽可能地反映社会公众对于“敏感”的整体认可度。即使我们无法全面预估科技发展的最终走向，但我们至少可以看到，敏感个人信息的损害风险来源、敏感个人信息处理导致的损害类型以及损害发生的可能性都是有增无减。我国《个人信息保护法》未来应在制度安排上作出有力回应，在现有“抽象概括＋非穷尽式列举”界定方式的基础上，辅以场景化界定路径回应信息社会的风险需要。具体而言，需以个人信息是否揭示或关联敏感内容、受损害主体是否包括其他关联利益人为场景化界定路径的客观考虑因

〔54〕 See A. B. Menezes Cordeiro, Civil Liability for Processing of Personal Data in the GDPR, 5 (4) *European Data Protection Law Review* 492, 495 (2019).

素，有效控制敏感个人信息处理过程中的损害风险。如此，方能为科技发展带来的敏感个人信息界定变化预留足够的空间，也才能更好实现敏感个人信息保护与利用的平衡。

Abstract：The definition of sensitive personal information is an important content of the Personal Information Protection Law. Because it can reflect and affect the major interests of the subject of personal information more than non-sensitive personal information, the Personal Information Protection Law adopts a more strict protection system for sensitive personal information. Article 28 (1) of the Personal Information Protection Law defines the objective risk standard for sensitive personal information. From the perspective of law, "sensitive" is associated with "high risk of damage", and sensitive personal information processing has a higher degree of risk of damage. The risk of damage can be derived independently or simultaneously from the inherence of personal information content, the instrumentality of illegal use of personal information, and the relevance of non-sensitive personal information and sensitive personal information. The definition of the sensitive personal information in the Personal Information Protection Law is still can not cover all damage risk sources, and should define sensitive personal information with contextualized aspects path on the basis of Article 28 (1). In particular, objective factors are considered based on whether the personal information reveals or concern sensitive content and whether the damaged subject includes other related interests.

Key Words：personal information protection law, sensitive personal information, risk of damage, contextual integrity

（责任编辑：武　腾　赵建蕊）

财经法学 No. 2，2023
pp. 36 - 50

论私密个人信息的合理使用困境与出路

刘　磊*

内容提要：《民法典》第1034条第3款确立的私密信息隐私权保护优先规则导致私密信息应有的合理使用空间被不当限缩，有必要引入《个人信息保护法》中的个人信息合理使用规则。在将私密信息划分为非敏感私密信息和敏感私密信息的基础上，前者可通过《民法典》第1034条第3款后半句“没有规定的，适用有关个人信息保护的规定”直接适用《个人信息保护法》第13条第1款第2项至第7项中的个人信息合理使用情形，后者则可基于敏感个人信息保护规则应优先于隐私权保护规则适用的解释思路，在符合《个人信息保护法》第28条第2款“敏感个人信息处理规则”的前提下，再适用《个人信息保护法》第13条第1款第2项至第7项中的个人信息合理使用情形。

关键词：隐私权　个人信息　私密信息　敏感信息　合理使用

一、引言

在著作权法中，合理使用是社会对他人著作财产权的一种限制，表现为在著作权人的专有领域内，法律通过直接规定在使用条件或方式上划分一定的“合理”范围，从而排除对该行为的侵权认定。〔1〕我国民法学者多认为，人格权或个人信息权益的合理使用制度是从著作权法中借鉴而来。〔2〕基于此，《中华人民共和国民法典》（以下简称《民法典》）人格权编第一章“一般规定”部分第999条新增有关人格权合理使用制度的规定，即“为公共利益实施新闻报道、舆论监督等

* 刘磊，中国政法大学比较法学研究院博士研究生。

〔1〕 参见吴汉东：《论合理使用》，载《法学研究》1995年第4期。

〔2〕 参见陈甦、谢鸿飞主编：《民法典评注·人格权编》，中国法制出版社2020年版，第68页；江波、张亚男：《大数据语境下的个人信息合理使用原则》，载《交大法学》2018年第3期；卢震豪：《我国〈民法典〉个人信息合理使用的情形清单与评估清单——以“抖音案”为例》，载《政治与法律》2020年第11期；张建文、刘啸天：《保护和利用之间：个人信息合理使用的判断标准》，载《北京邮电大学学报（社会科学版）》2021年第6期。

行为的，可以合理使用民事主体的姓名、名称、肖像、个人信息等”。不过，由于该条文并没有明确“合理使用”的定义，民法学者们多是围绕某项具体人格权益的合理使用进行学理上的概念界定。例如，有学者认为，肖像权的合理使用是指在法律规定的条件下，既不必征得肖像权人的同意，又不必向其支付报酬，基于正当目的而使用他人肖像的合法行为。〔3〕还有学者认为，个人信息的合理使用是指处理者可以不取得自然人或者其监护人的同意就对个人信息进行包括收集、存储、使用、加工、传输、提供、公开等在内的处理行为。〔4〕虽然上述定义的语言表述不同，但其本质上都是在表明，法律虽然尊重和保护民事主体的人格权益，但该保护力度并不是无限大的，仍需要为公共利益等正当目的的合理使用留出必要的空间。

就私密信息而言，其既属于隐私，也属于个人信息，这便会不可避免地导致隐私权保护规则和个人信息保护规则在保护上出现交叉。《民法典》第1034条第3款出于隐私权受保护程度更高的考虑而采取了隐私权保护规则优先的立场，〔5〕但这也同时导致私密信息的合理使用空间被不当限缩。例如：在新型冠状病毒感染疫情期间，政府部门为应对这种突发的公共卫生事件而收集自然人的私密信息，即使并未经自然人的知情同意，也不能说这是违法的个人信息处理行为；公安机关为侦破案件而收集犯罪嫌疑人的私密信息，也无需征得自然人的知情同意，这是履行法定职责所必须；用人单位基于规范用工管理的需要而处理劳动者必要的私密信息，也不能认为这种处理行为侵犯劳动者隐私，因为这应属于合理使用的范畴。〔6〕但在隐私权保护规则下，我们却很难找到直接的法律依据主张合理使用抗辩。即使存在个人信息保护规则中的合理使用抗辩事由，但由于隐私权保护优先规则的确立，这些抗辩事由无法适用于隐私权保护规则。

因此，我们有必要反思目前的隐私权保护规则优先的立场是否导致私密信息当有的合理使用空间被不当限缩；如果是的话，我们需要研究应当采取何种解释论的方案进行解决。本文将围绕这些问题展开讨论，并尝试提出可能的解决方案。

二、隐私权保护优先规则下私密信息的合理使用困境

在信息社会，要维护自然人的私生活安宁和私生活秘密不受侵害，就必须保护自然人的私密信息不被随意收集、公开或者滥用。〔7〕但是，由于私密信息在数字时代也具有重要的经济和社会价值，〔8〕法律在注重个人对其个人信息的保护诉求的同时，也应关注到信息业者及政府对个

〔3〕 参见张红：《肖像权保护中的利益平衡》，载《中国法学》2014年第1期。

〔4〕 参见程啸：《论我国民法典中的个人信息合理使用制度》，载《中外法学》2020年第4期。

〔5〕 尽管无论从《民法典》第1034条第3款的规定，还是从其释义书来看，都确立了私密信息隐私权保护优先的规则，但是，从学界的讨论情况来看，学者们已经逐渐认识到该条款引发的弊端，并对该规则持否定态度。参见李昊：《个人信息侵权责任的规范构造》，载《广东社会科学》2022年第1期；刘承韪、刘磊：《论私密信息隐私权保护优先规则的困局与破解——以〈民法典〉第1034条第3款为中心》，载《广东社会科学》2022年第3期；程啸：《论个人信息权益与隐私权的关系》，载《当代法学》2022年第4期；王道发：《个人信息处理者过错推定责任研究》，载《中国法学》2022年第5期。

〔6〕 参见上海市第一中级人民法院（2020）沪01民终10935号民事判决书。

〔7〕 参见程啸：《人格权研究》，中国人民大学出版社2022年版，第431页。

〔8〕 参见冉克平：《论〈民法典〉视野下个人隐私信息的保护与利用》，载《社会科学辑刊》2021年第5期。

人信息的利用需求，〔9〕这就需要妥当维系保护与利用之间的平衡关系。即使是在隐私权保护规则下，也应在信息利用和隐私权保护之间寻求动态平衡，〔10〕但通过比较隐私权保护规则与个人信息保护规则下的合理使用抗辩事由可以发现，隐私权保护规则下基本不存在可直接援引的合理使用抗辩事由，而隐私权保护优先规则的确立又排斥个人信息保护规则下合理使用抗辩事由的援引，从而导致私密信息的合理使用空间被过度限制。

（一）隐私权保护规则与个人信息保护规则下合理使用抗辩的差异

在《民法典》人格权编第六章“隐私权和个人信息保护”中并没有关于隐私权合理使用的规定，而仅在第一章“一般规定”第 999 条规定“为公共利益实施新闻报道、舆论监督等行为的，可以合理使用民事主体的姓名、名称、肖像、个人信息等”。那么该条中的“等”字，能否将隐私包含在内？从该条的立法沿革来看，立法者对隐私的合理使用持否定态度。全国人大常委会于 2018 年 9 月发布的《民法典各分编（草案）》第 779 条第 2 款曾规定：“行为人为维护公序良俗实施新闻报道、舆论监督等行为的，可以在必要范围内合理使用民事主体的姓名、名称、肖像、隐私、个人信息等。”但全国人大常委会于 2019 年 4 月发布的《民法典人格权编（草案二次审议稿）》第 781 条之一却将上述规定修改为“实施新闻报道、舆论监督等行为的，可以合理使用民事主体的姓名、名称、肖像、个人信息等”。很显然，在草案二次审议稿中，针对隐私的合理使用规则未予保留，此后的历次审议稿及最后正式通过的《民法典》均保持同样的立法态度。

有学者认为，《民法典》总则编中的平等原则、自愿原则、公平原则、诚实信用原则、公序良俗原则等民法的基本原则，以及紧急避险、正当防卫、自助行为等制度，属于人格权合理使用的抽象性规范，均可以对人格权的行使进行适当限制。〔11〕的确，上述基本原则或制度位于总则部分，对民法领域内的民事法律关系都能起到调整作用。不过，民法的基本原则只是民事法律法规的基本解释依据，仅在现行法上没有直接裁判依据而出现法律漏洞时，才可直接适用其裁判案件。〔12〕而紧急避险、正当防卫、自助行为等制度，尽管可以作为人格权合理使用的依据，但实践中能以此作为依据的情况实在太少，而且这几种制度所规制的人格权合理使用情形也极其有限。就此而言，隐私权保护规则下私密信息的合理使用抗辩基本上是不存在的。

与隐私权保护规则下的合理使用抗辩事由相比，个人信息保护规则下的合理使用抗辩不仅可援引《民法典》总则编中的抽象性规范，还可以援引《民法典》人格权编第一章“一般规定”中关于人格权合理使用的共通性规范，以及《民法典》人格权编第六章“隐私权和个人信息保护”和《个人信息保护法》中关于个人信息合理使用的专门性规范。人格权合理使用的共通性规范主

〔9〕 参见张新宝：《从隐私到个人信息：利益再衡量的理论与制度安排》，载《中国法学》2015 年第 3 期。

〔10〕 参见郭秉贵：《大数据时代信息自由利用与隐私权保护的困境与出路——以“中国 Cookie 隐私第一案”为分析对象》，载《深圳社会科学》2021 年第 4 期。

〔11〕 参见冷传莉、曾清河：《人格权合理使用制度的立法检视与司法展开》，载《福建师范大学学报（哲学社会科学版）》2021 年第 6 期；前引〔4〕，程啸文。

〔12〕 参见梁慧星：《民法总论》（第 5 版），法律出版社 2017 年版，第 46 页；王轶：《论民法诸项基本原则及其关系》，载《杭州师范大学学报（社会科学版）》2013 年第 3 期。

要体现为《民法典》人格权编第999条关于人格权合理使用的规定。从该条“为公共利益实施新闻报道、舆论监督等行为的，可以合理使用民事主体的姓名、名称、肖像、个人信息等”的表述来看，由于私密信息也属于个人信息，当然也可以被合理使用。而个人信息合理使用的专门性规范主要是指《民法典》人格权编第1036条第2项“合理处理该自然人自行公开的或者其他已经合法公开的信息”、第3项“为维护公共利益或者该自然人合法权益”而合理使用的情形，以及《个人信息保护法》第13条第1款第2项至第7项中的“为订立、履行个人作为一方当事人的合同所必需”“按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需”“为履行法定职责或者法定义务所必需”“为应对突发公共卫生事件，或者紧急情况下为保护自然人的生命健康和财产安全所必需”“为公共利益实施新闻报道、舆论监督等行为”“对个人自行公开或者其他已经合法公开的个人信息”而进行的合理使用情形。此外，《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）第26条规定的“为维护公共安全所必需而在公共场所安装图像采集、个人身份识别设备”的合理使用情形，以及第34条、第35条、第37条规定的国家机关或法律、法规授权的具有管理公共事务职能的组织“为履行法定职责处理个人信息”的合理使用情形，都属于上述专门性规范的进一步细化规定。

（二）隐私权保护优先规则下私密信息合理使用的过度限制

《民法典》第1034条第3款规定：“个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。”这显然是采取了隐私权保护规则优先的立场。之所以如此规定，立法机关释义书给出的理由是，隐私权对私密信息的保护程度更高。〔13〕有观点对此持肯定态度，并进一步认为，个人信息可能承载公共利益，法律对个人信息权益的保护需要在利益平衡中进行，始终协调保护和利用的关系，不能像隐私权那样受到绝对保护而不允许对隐私进行所谓的合理使用。〔14〕

问题在于，隐私权保护优先规则下的私密信息保护是否真的就不存在利益平衡或合理使用。至少从《民法典》第998条的规定来看，并非如此。《民法典》第998条引入动态系统论的观点，根据该条规定，除生命权、身体权和健康权这三种物质性人格权外，在判断其他非物质性人格权益是否遭受侵害时，应综合考虑行为人和受害人的职业、影响范围、过错程度，以及行为的目的、方式、后果等因素。〔15〕无论是隐私权，还是个人信息权益，显然都应属于非物质性人格权益。两者在具体案件中是否应受到保护，都要根据第998条的规定结合具体案件情况进行动态的利益衡量。因此，无论信息主体是以隐私权还是以个人信息权益主张对私密信息的保护，法院都要结合案件中的具体因素进行衡量，但这与隐私权保护规则或个人信息保护规则本身并没有太多关系，两者对私密信息的保护程度应是相同的。或许有观点会质疑称，即使隐私权保护规则下的私密信息保护应结合第998条的规定进行动态的利益衡量，但隐私权作为民事权利

〔13〕 参见黄薇主编：《中华人民共和国民法典人格权编解读》，中国法制出版社2020年版，第212页。

〔14〕 参见王利明：《和而不同：隐私权与个人信息的规则界分和适用》，载《法学评论》2021年第2期；程啸：《个人信息保护法理解与适用》，中国法制出版社2021年版，第525页。

〔15〕 参见王利明：《民法典人格权编中动态系统论的采纳与运用》，载《法学家》2020年第4期。

所具有的应比民事利益受保护程度更高的法律性质，也决定了隐私权保护规则在动态的利益衡量下可以受到更高程度的保护。但实际上，私密信息本身的特性才是决定其应受何种程度保护的根本因素，如果针对私密信息的处理涉及隐私权或个人信息权益与合理使用之间的利益权衡，也不应因以隐私权主张保护还是以个人信息权益主张保护而得出不同的结论，下文将会对此作进一步分析。

此外，还有观点受人格权商品化理论的影响，认为隐私权作为消极性人格权，仅具有防御功能而对其权利客体并不享有支配利用的积极权能，故隐私不能作为合理使用的权利对象。〔16〕该观点有待商榷。首先，人格权商品化更确切地说其实是指人格权主体对其人格要素享有的经济利益，〔17〕即人格权主体通过对其人格特征的商业化利用从而获得一定的经济利益。〔18〕尽管《民法典》第 993 条规定“民事主体可以将自己的姓名、名称、肖像等许可他人使用”，而未对“隐私”进行明确列举，但从实践中的典型情形来看，存在将“隐私”列入上述法条中“等”字的解释空间。例如，网络主播对其个人生活起居、工作等具体情况进行直播的，实际上便属于人格权主体对其隐私的商业化利用。〔19〕再例如，人们公开发表含有自己隐私的日记、利用自己的身体作为绘画或拍摄电影作品的素材，也都属于人格权主体对其个人隐私的积极利用。〔20〕其次，与人格权商品化强调人格权主体对其人格要素的商业化利用不同的是，合理使用是对人格权主体所享有的人格权利的限制，是人格权向国家利益、公共利益等更为优越的利益所做的必要让步。从侵权责任的构成上讲，合理使用是行为人可以主张的违法阻却事由，可免于侵权责任的承担。

总之，在目前的隐私权保护优先规则下，过于强调隐私权的保护强度，而忽略了私密信息应当具有的合理使用空间，导致个人信息保护规则中有关个人信息的合理使用规则无法适用于私密信息，从而形成了隐私权保护优先规则下合理使用抗辩被过度限制的局面。

三、隐私权保护优先规则下合理使用困境的反思

《民法典》第 1034 条第 3 款确立隐私权保护优先规则的出发点在于，隐私权作为民事权利的受保护力度更强。这便意味着在适用隐私权保护规则时，不能适用个人信息保护规则中的合理使用抗辩事由，否则便不能体现出这种保护强度的优越性。但问题在于，这种立场的坚持是否具有足够的正当性，对此有必要进行理论上的探讨。

（一）隐私权的位阶并非绝对高于个人信息权益

有观点认为，现行立法分别对侵害隐私权和个人信息权益的行为进行了列举，但针对前者的列举属于权利化模式下的典型列举，在列举情形之外仍具有开放性，而针对后者的列举则属于行

〔16〕 参见前引〔11〕，冷传莉、曾清河文。

〔17〕 参见前引〔7〕，程啸书，第 117 页；前引〔2〕，陈甦、谢鸿飞主编书，第 32－33 页。

〔18〕 参见王泽鉴：《人格权法：法释义学、比较法、案例研究》，北京大学出版社 2013 年版，第 281 页。

〔19〕 参见王利明：《人格权法》（第 3 版），中国人民大学出版社 2021 年版，第 92 页。

〔20〕 参见张红：《人格权各论》，高等教育出版社 2015 年版，第 524 页。

为规制模式下的封闭式完全列举，故权利化模式为行为人留下的自由空间比行为规制模式更狭小，保护力度当然也就相对更强一些。〔21〕还有观点认为，隐私权系民事权利，而个人信息仅为民事权益，法律对前者的保护力度显然高于后者，德国法中的权利和利益区分保护模式即对此提供了有力例证。〔22〕虽然上述观点的表达形式有所不同，但实际上却存在共同的论证基点，即民事权利在价值位阶上优于民事利益，那么隐私权作为民事权利的受保护程度便应高于作为民事利益的个人信息权益。具体而言，隐私权作为民事权利，性质上属于绝对权，法律对其保护的绝对性程度较高，可以最大限度地排斥合理使用、公共利益的干扰。而个人信息权益作为民事利益，立法仅在划定的封闭性行为样态范畴内对其进行保护，留给了行为人更为广阔的自由空间，而个人信息权益的保护空间当然也就更容易受到合理使用、公共利益的挤压。

但问题在于，民事权利的受保护程度是否一定比民事利益更高。学界一直以来都对此存在较大争议，尤其以《中华人民共和国侵权责任法》（以下简称《侵权责任法》）第 6 条第 1 款引发的民事权利与民事利益是否应当区别保护的争论最为激烈。《民法典》第 1165 条第 1 款是由《侵权责任法》第 6 条第 1 款演变而来，学界因《侵权责任法》第 6 条第 1 款引发的民事权利与民事利益是否应当区分保护的争议，在《民法典》第 1165 条第 1 款下同样适用。有学者认为，该条的文义解释含义是民事权利和民事利益能够获得同等程度保护，为避免产生理论上的灾难，应参照德国法上的权利和利益区分保护模式对该条文进行目的性限缩。〔23〕还有学者也基本持同样观点，即民事权利和民事利益的受保护程度不同，应对前者设置较低的保护门槛，而对于后者的保护应进行严格限制，通常只有在行为人具有主观恶意等情况下，才能对民事主体遭受的利益侵害进行侵权法上的救济。〔24〕更有学者进一步研究了德国民法中侵权法上的“归属效能”“排除效能”和“社会典型公开性”这三个权益区分标准，以此界定民事权利与利益的保护区分。〔25〕上述观点受《德国民法典》中“三个小一般条款”的规定影响颇深，即第 823 条第 1 款对权利进行过错责任下的全面保护，而对利益，仅在违反第 823 条第 2 款的保护性法规以及第 826 条有关恶意违背善良风俗的规定时才提供保护。

值得注意的是，民法学界已开始对上述观点进行反思，民事权利的价值位阶并非绝对高于民事利益。首先，德国法的“三个小一般条款”本身存在着保护范围过于狭小的缺陷，为了弥补其不足，德国法因此发展出交往安全义务、营业权、一般人格权条款。〔26〕其次，即使权利与利益应受不同程度的保护，也应是基于二者的不同特性，并且应将因特性不同而导致的受保护程度不同具体落实在侵权责任既有责任成立要件上，而非使权利或利益的侵害适用不同的归责原理。〔27〕

〔21〕 参见前引〔8〕，冉克平文；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。

〔22〕 参见前引〔14〕，王利明文。

〔23〕 参见葛云松：《〈侵权责任法〉保护的民事权益》，载《中国法学》2010 年第 3 期。

〔24〕 参见王利明：《侵权法一般条款的保护范围》，载《法学家》2009 年第 3 期；王成：《侵权之“权”的认定与民事主体利益的规范途径——兼论〈侵权责任法〉的一般条款》，载《清华法学》2011 年第 2 期。

〔25〕 参见于飞：《侵权法中权利与利益的区分方法》，载《法学研究》2011 年第 4 期。

〔26〕 参见叶金强：《〈民法典〉第 1165 条第 1 款的展开路径》，载《法学》2020 年第 9 期。

〔27〕 参见陈忠五：《论契约责任与侵权责任的保护客体：“权利”与“利益”区别正当性的再反思》，载《台大法学论丛》第 36 卷第 3 期。

最后，即使是仍赞同权益区分保护模式的学者，也开始认为这只是针对两者的保护在方法论上的区分，即侵害权利的违法性直接被认定，但侵害利益的违法性则需要民事主体的证明，故侵权责任法对两者的保护应有所区分。不过，这并不意味着民事权利在价值位阶上优于民事利益，因为如果法律明确规定了某种利益应受到保护，其与权利的保护在本质上并不存在差别，甚至还会出现遭受权利侵害的民事主体因无法证明其他构成要件导致侵权责任法对其保护程度还不如利益的情形。〔28〕

（二）隐私权保护规则下合理使用被过度限制的不合理性

也许有观点会质疑称，如果在同一个案件中私密信息遭受信息处理行为的侵害，即便需要按照《民法典》第 998 条的规定进行动态衡量，隐私权的绝对权性质决定了其在衡量过程中也会受到比个人信息权益更高程度的保护。这种质疑观点看似有力，实则经不起推敲。私密信息作为隐私内容之一，当然可以受到隐私权的保护，但这种保护并非没有限度，同样应为来自公共利益、社会正常交往、交易关系及人力资源管理等方面的合理使用留出足够的空间。

第一，根据我国《宪法》第 51 条规定，个人的自由和权利应在合理范围内向公共利益作出必要的让步。如果认为《民法典》第 1036 条第 3 项以及《个人信息保护法》第 13 条第 1 款第 3 项、第 4 项、第 5 项有关合理使用的规定仅适用于个人信息权益，便意味着针对私密信息最多可能适用《民法典》人格权编第 999 条规定的为公共利益实施新闻报道、舆论监督的合理使用。更有甚者，如果认为第 999 条的“个人信息”不包括私密信息，而该条又没有明确体现“隐私权”，那么针对私密信息的合理使用连第 999 条也不能适用。按照这种推论，针对私密信息的合理使用空间非常狭小，甚至可以说基本不存在。但问题在于，《民法典》第 1036 条第 3 项以及《个人信息保护法》第 13 条第 1 款第 3 项、第 4 项、第 5 项中有关为履行法定职责或者法定义务、为应对突发公共卫生事件等情形下的合理使用显然具备足够的正当性，也符合《宪法》第 51 条的规定。

第二，国务院的有关行政法规也认为，即使是自然人的个人隐私，在必要的情况下也应让位于公共利益。例如，根据国务院《政府信息公开条例》第 15 条的规定，涉及个人隐私的政府信息，考虑到一旦公开会对第三方合法权益造成损害，原则上行政机关不得公开，但如果不公开又会对公共利益造成重大影响的，予以公开。尽管有行政法学者认为，该条中的“个人隐私”存在不易识别、授权过于宽泛等方面的问题，但同时也认为应将“个人隐私”聚焦于“私密信息”以构建和完善私密信息的公开豁免制度。〔29〕

第三，私密信息也并非绝对的封闭，而多数是在不同场景中特定多数主体之间分享，只要该信息仍是在该特定群体间传播，并符合该信息主体的预期，这种合理使用就应当被允许。〔30〕就此而言，《民法典》第 1036 条第 2 项及《个人信息保护法》第 13 条第 1 款第 6 项中有关合理使用个人自行公开或法定公开的个人信息的规定可适用于私密信息，当然在合理使用的认定上，应

〔28〕 参见方新军：《侵权责任利益保护的解释论》，法律出版社 2021 年版，第 354 页。

〔29〕 参见李卫华：《民法典时代个人隐私信息公开豁免条款的困境及完善》，载《行政法学研究》2021 年第 6 期。

〔30〕 参见胡凌：《个人私密信息如何转化为公共信息》，载《探索与争鸣》2020 年第 11 期。

当尤其严格。

第四，基于交易关系对私密信息的处理一般表现为两种形式：一是私密信息本身的传输即涉及交易行为；二是其他交易行为的完成需要私密信息的提供。〔31〕前一种形式应以信息主体的知情同意为前提，并无合理使用的空间。后一种形式则属于《个人信息保护法》第13条第1款第2项规定的为订立、履行个人作为一方当事人的合同所必需而合理使用个人信息的情形。例如，在“庞某某诉东航公司、趣拿公司隐私权纠纷案”中，〔32〕庞某某通过趣拿公司下辖的网络平台购买机票，该网络平台只有在收集庞某某的姓名、身份号码、联系方式等私密信息后才可以提供购票服务，这便是为双方之间服务合同的履行而必须处理一方个人私密信息的情形。再例如，通过12306手机APP向中国国家铁路集团有限公司订购火车票时，在合同订立阶段就需要把姓名、身份号码、联系方式等私密信息输入，才能够进一步选定具体的座位，这也属于合理使用的情形。此外，《个人信息保护法》第13条第1款第2项规定的为实施人力资源管理所必须而合理使用也基本如此，招聘、社保办理、工资发放、绩效考核、业务培训等各个环节都涉及个人信息的处理，〔33〕为使企业的人力资源管理工作得以正常进行，应当允许这种对个人信息的合理使用。

第五，欧盟《一般数据保护条例》（General Data Protection Regulation，简称GDPR）在第6条已经规定个人数据处理合法性的情况下，考虑到特殊种类的个人数据与自然人的基本权利和自由紧密相关，对该种类数据进行处理将对自然人的基本权利和自由产生重大影响，〔34〕第9条又特别规定了特殊种类的个人数据处理。该条第1款规定原则上应禁止对特殊种类的个人数据进行处理，但第2款除（a）项关于应取得数据主体的明示同意才能处理其个人数据的规定外，其余（b）～（j）共9项可以进行处理的事由其实都属于未经同意可以合理使用的范畴。GDPR第9条所称特殊种类的个人数据其实就是指敏感数据。〔35〕尽管敏感信息（数据）与私密信息不能等同，但不可否认的是二者之间至少存在一定交叉，在GDPR中至少可以解释出对敏感私密信息合理使用的空间。

四、隐私权保护优先规则下私密信息合理使用的解释路径

通过上述分析可以发现，即使是私密信息也应当有足够的合理使用空间，当然在适用条件上应当严格把握。需要特别说明的是，这种从严把握是基于私密信息本身的特性，与采隐私权保护规则还是采个人信息保护规则并无关系。换言之，对私密信息进行保护无论是适用隐私权保护规则还是个人信息保护规则，针对私密信息的合理使用空间都应该是无差别的。因此，有必要对目

〔31〕 参见前引〔8〕，冉克平文。

〔32〕 参见北京市第一中级人民法院（2017）京01民终509号民事判决书。

〔33〕 参见前引〔14〕，程啸书，第129页。

〔34〕 See Christopher Kuner, *The EU General Data Protection Regulation (GDPR): A Commentary*, Oxford University Press, 2020, p. 366.

〔35〕 参见前引〔34〕，Christopher Kuner书，第373页。

前的隐私权保护优先规则采取缓和化的解释路径。

（一）私密信息合理使用规则的理论划分

有观点认为，为保持私密信息保护与利用之间的平衡，不妨将私密信息划分为敏感私密信息和非敏感私密信息，从而适用不同的合理使用标准。〔36〕法律应为敏感私密信息提供强化保护，虽然该保护仍包含保护和利用两个维度，但对其利用的标准和要求应更高。〔37〕该观点值得肯定，以敏感性程度对私密信息进行划分具有合理性。

首先，个人信息的敏感程度与人格尊严和自由呈现正相关的紧密关联，故敏感程度更高的个人信息应受到更高程度的保护，这种更高程度的保护便集中体现为法律对个人信息处理者的处理行为提出的更高要求。从另一个角度看，既然敏感程度更高的个人信息应受到更高程度的保护，便意味着个人信息处理者针对敏感程度更高的个人信息进行处理时可援引的合理使用抗辩空间相对较小。其次，在个人信息的类型划分方面，《民法典》与《个人信息保护法》具有不同的规范目的。前者将个人信息划分为私密信息与非私密信息，其规范目的在于协调个人信息权益与隐私权的关系，〔38〕即个人信息原则上并不适用隐私权保护规则而应适用个人信息保护规则，只有个人信息中的私密信息应优先适用隐私权保护规则；后者将个人信息划分为敏感信息与非敏感信息则是出于规范不同的个人信息处理行为、协调个人信息的保护与利用的考量，〔39〕对于敏感信息的保护程度更高，合理使用的标准也相对更为严格。由此来看，《民法典》划分私密信息与非私密信息的规范目的实则在于区分隐私权保护规则和个人信息保护规则，〔40〕以扭转适用隐私权保护规则保护个人信息的传统做法。〔41〕而由于私密信息既属于隐私，又属于个人信息，注定了对于私密信息的保护不仅无法从隐私权保护规则中剥离，还会不可避免地造成隐私权保护规则与个人信息保护规则的交叉。为解决由此产生的法律适用问题，《民法典》第 1034 条第 3 款确立了私密信息隐私权保护规则优先的立场，但却导致了私密信息的合理使用空间被不当限缩的局面。《民法典》所作的私密信息与非私密信息的类型划分，其直接的出发点本身并不涉及个人信息的保护与利用问题。而从《个人信息保护法》划分敏感信息和非敏感信息的规范目的来看，其直接的出发点原本就是为了平衡个人信息的保护与利用问题。就此而言，即使是个人信息范畴内的私密信息与非私密信息，在衡量其存在多大的合理使用空间方面，仍应以敏感程度作为划分标准。此外，更有观点对《民法典》划分私密信息与非私密信息的做法提出了质疑。因为根据《民法典》第 1032 条第 2 款的规定，所有未公开的个人信息都可纳入私密信息的范畴，但未公开信息的范围实在过于宽泛，相比之下，敏感信息在客体范围上更具确定性，应以“敏感信息”取代

〔36〕 参见前引〔8〕，冉克平文。

〔37〕 参见前引〔9〕，张新宝文。

〔38〕 参见郑晓剑：《论〈个人信息保护法〉与〈民法典〉之关系定位及规范协调》，载《苏州大学学报（法学版）》2021 年第 4 期。

〔39〕 参见程啸：《论我国个人信息保护法中的个人信息处理规则》，载《清华法学》2021 年第 3 期。

〔40〕 参见程啸：《个人信息保护中的敏感信息与私密信息》，载《人民法院报》2020 年 11 月 19 日，第 5 版；江必新、李占国主编：《中华人民共和国个人信息保护法条文解读与法律适用》，中国法制出版社 2021 年版，第 102 页。

〔41〕 参见前引〔38〕，郑晓剑文。

“私密信息”。〔42〕但无论如何，《民法典》既已施行，为了缓解《民法典》第1034条第3款确立的私密信息隐私权保护优先规则导致的私密信息合理使用空间被不当限缩，只能在目前的立法框架下寻求可能的缓和化解释方案。

不过，在将私密信息划分为非敏感私密信息和敏感私密信息的基础上，对于二者的合理使用，当存在不同的解释路径。原因在于，非敏感私密信息的考量因素仅为“私密”，而敏感私密信息的考虑要素为“敏感”和“私密”，前者仍需在隐私权保护优先规则内寻求解释方案，而后者则存在由于具有“敏感”因素而绕过隐私权保护优先规则的可能，从而在敏感个人信息的保护规则内寻求解释方案。对此，有学者提出了非常有意义的问题，那便是当敏感私密信息遭受侵害时，应优先适用隐私权保护规则，还是应优先适用个人信息保护规则。〔43〕具体而言，《民法典》第1034条第3款只是确立了私密信息的隐私权保护优先规则，即当私密信息遭受侵害时，应优先适用隐私权保护规则，而个人信息保护规则仅在隐私权保护规则没有规定时才可以适用。但当敏感私密信息遭受侵害时，是否仍应优先适用隐私权保护规则呢？

实际上，对于敏感私密信息应如何保护的重要考量因素已不再是“私密”，而是“敏感”，敏感私密信息本身已经是私密信息范围内的进一步划分。因此，对于敏感私密信息的保护，个人信息保护规则中有关敏感个人信息的相关规定应作为特别规则而优先适用。此外，从私密信息的侵权责任构成上看，适用隐私权保护优先规则确实也没有任何优势，甚至可以说存在一定的弊端。首先，隐私权保护规则适用的是过错责任，而个人信息保护规则适用的却是过错推定责任，这意味着适用个人信息保护规则实际上更有利于对信息主体的保护，〔44〕因为信息主体无需再就过错要件进行举证证明，而是由法律直接推定个人信息处理者存在过错。其次，虽然法律应强调对敏感私密信息的高强度保护，但这种保护仍然应为合理使用留出足够的空间。但正如上文所述，在隐私权保护规则下，私密信息的合理使用抗辩都基本不存在，遑论敏感私密信息的合理使用抗辩。

此外，《个人信息保护法》第28条第1款规定敏感个人信息是“一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息”，并将生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息及不满十四周岁未成年人的个人信息作为典型进行列举。但有观点认为，该条款只是确立了敏感个人信息的权益侵害风险基准和风险内容、风险程度及风险发生方式三个方面的具体风险维度，但对于如何判定个人信息处理者的处理行为是否达到了这种敏感的风险维度则没有明确。〔45〕还有观点认为，上述法条中列举的7种类型的个人信息显然并不足以覆盖全部的敏感个人信息，对于未予以列举的敏感个人信息则需

〔42〕 参见石佳友：《隐私权与个人信息关系的再思考》，载《上海政法学院学报（法治论丛）》2021年第5期。

〔43〕 参见王利明：《敏感个人信息保护的基本问题——以〈民法典〉和〈个人信息保护法〉的解释为背景》，载《当代法学》2022年第1期。

〔44〕 参见前引〔5〕，李昊文；前引〔5〕，刘承韪、刘磊文。

〔45〕 参见宁园：《敏感个人信息的法律基准与范畴界定——以〈个人信息保护法〉第28条第1款为中心》，载《比较法研究》2021年第5期。

要结合理论标准予以明确。〔46〕实际上，上述问题本质上都是“敏感性”的确定问题。美国的尼森鲍姆（Nissenbaum）教授提出的场景理论，主张对于隐私是否应受到保护应结合所处的具体场景进行考量，〔47〕并将信息发送者、信息接收者、信息主体、信息类型及传输原则等作为具体的考量因素。〔48〕我国学者受此启发，多主张在敏感个人信息的“敏感性”判断上也应引入场景理论，〔49〕但对于“敏感性”判断的具体考量要素却并未达成一致。可以说，尼森鲍姆教授所提出的场景理论只是为“敏感性”的判断提供了一种思路，而具体的考量因素却因各国具体情况不同而有所不同，这有待于学者们的进一步努力。

有观点认为，场景理论中应考量的场景要素不仅可以作为判断“敏感性”的归入标准，还可以作为择出标准，即符合社会场景目的的个人信息处理行为，已经平衡了个人价值与公共价值及社会价值，原本的敏感个人信息在此情况下可被视为一般个人信息处理。〔50〕该观点有待商榷。按照该观点，有关敏感个人信息的保护与利用都将集中在“敏感性”的判断上，但该观点却忽视了合理使用本身作为判断标准的功能，而且也与我国民法理论中的侵权责任构成不相符。具体而言，在敏感个人信息的侵权责任构成中，合理使用是作为违法阻却事由予以考虑，有着自身独立的存在价值。而运用场景理论对“敏感性”的判断，其作用仅限于在具体的场景中判断某项个人信息是否为敏感信息，至于个人信息处理行为是否涉及社会利益和公共利益，则应由合理使用这一抗辩事由予以判断。

（二）非敏感私密信息的合理使用规则

如上所述，由于非敏感私密信息的重要考量因素仅为“私密”，故对于非敏感私密信息的合理使用，仍应以《民法典》第 1034 条第 3 款确定的隐私权保护优先规则为中心寻求可能的解释方案。《民法典》第 1034 条第 3 款前半句规定“个人信息中的私密信息，适用有关隐私权的规定”，确立了隐私权保护规则的优先性地位。《民法典》1034 条第 3 款后半句则规定“没有规定的，适用有关个人信息保护的规定”，其立法目的在于明确个人信息保护规则是隐私权保护规则对私密信息在保护方式上的补充。〔51〕为避免目前的隐私权保护优先规则对非敏感私密信息保护过度而忽略了非敏感私密信息应有的合理使用空间，应对作为补充保护方式的个人信息保护规则的适用做广义上的理解。具体而言，《民法典》第 1034 条第 3 款后半句“没有规定的，适用有关个人信息保护的规定”应理解为不仅可以适用个人信息保护规则中的保护性规定，还可以适用个人信息保护规则中的合理使用抗辩事由。

〔46〕 参见前引〔43〕，王利明文；王苑：《敏感个人信息的概念界定与要素判断——以〈个人信息保护法〉第 28 条为中心》，载《环球法律评论》2022 年第 2 期。

〔47〕 See Helen Nissenbaum, Privacy as Contextual Integrity, 79 *Washington Law Review* 119 (2004).

〔48〕 See Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Standford University Press, 2010, pp. 141 - 145.

〔49〕 参见前引〔43〕，王利明文；前引〔46〕，王苑文；前引〔45〕，宁园文；汤敏：《个人敏感信息保护的欧美经验及其启示》，载《图书馆建设》2018 年第 2 期；陈红旭：《敏感个人数据的特殊保护》，载《重庆理工大学学报（自然科学版）》2019 年第 4 期；张勇：《敏感个人信息的公私法一体化保护》，载《东方法学》2022 年第 1 期；孙清白：《敏感个人信息保护的特殊制度逻辑及其规制策略》，载《行政法学研究》2022 年第 1 期。

〔50〕 参见前引〔46〕，王苑文。

〔51〕 参见前引〔13〕，黄薇主编书，第 212 页。

在隐私权保护优先规则下，可适用的个人信息保护规则中的合理使用抗辩事由分为两部分：第一部分是指《民法典》中有关个人信息保护规则的合理使用抗辩事由，《民法典》第999条和第1036条第2项、第3项都属于这部分；第二部分则是指《个人信息保护法》中有关个人信息保护规则的合理使用抗辩事由，主要是指《个人信息保护法》第13条第1款第2项至第7项无需取得个人同意也可处理其个人信息的情形。

值得注意的是，《民法典》第999条和第1036条第2项、第3项中的合理使用抗辩事由都可以在《个人信息保护法》第13条第1款第2项至第7项中找到对应条款。实际上，《民法典》与《个人信息保护法》中的私法规则部分本就是一般法与特别法的关系，前者确定的个人信息权益的性质及其在民事权利体系中的位置，是后者具体适用的基础和依据，〔52〕而后者则是前者在个人信息保护领域的具体的专门性规定。因此，《个人信息保护法》第13条第1款第2项至第7项可以说是《民法典》第999条和第1036条第2项、第3项的具体化规定。《个人信息保护法》第13条第1款第5项基本对应《民法典》第999条中“为公共利益实施新闻报道、舆论监督等行为的，可以合理使用民事主体的个人信息”的规定；《个人信息保护法》第13条第1款第6项及第27条基本可对应《民法典》第1036条第2项“合理处理该自然人自行公开的或者其他已经合法公开的信息，但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外”的规定；《个人信息保护法》第13条第1款第3项至第4项基本可对应《民法典》第1036条第3项“为维护公共利益或者该自然人合法权益，合理实施的其他行为”的规定，并将“公共利益”的情形细化为“履行法定职责”“履行法定义务”“应对突发公共卫生事件”这几种具体情形，将“该自然人合法权益”细化为“自然人的生命健康和财产安全”。此外，《个人信息保护法》第13条第1款第2项还新增了“为订立、履行个人作为一方当事人的合同所必需，或者按照依法制定的劳动规章制度和依法签订的集体合同实施人力资源管理所必需”的情形作为合理使用事由，第7项新增了“法律、行政法规规定的其他情形”的兜底性规定。

因此，对于非敏感私密信息的合理使用，个人信息处理者原则上可直接援引《个人信息保护法》第13条第1款第2项至第7项中的合理使用抗辩事由。另外，考虑到《个人信息保护法》第72条第1款“自然人因个人或者家庭事务处理个人信息的，不适用本法”的规定，个人信息处理者在无法援引《个人信息保护法》第13条第1款第2项至第7项中的合理使用抗辩事由的情况下，可援引《民法典》第999条和第1036条第2项、第3项中的合理使用抗辩事由。

（三）敏感私密信息的合理使用规则

虽然针对敏感私密信息的处理，应优先适用个人信息保护规则中有关敏感个人信息保护的规定，但对于我国《个人信息保护法》中有关敏感个人信息的合理使用规则应当如何具体适用，也是个值得讨论的问题。《个人信息保护法》第二章“个人信息处理规则”第一节“一般规定”的第13条第1款规定了7项个人信息处理者可合法处理个人信息的事由，除第1项应“取得个人

〔52〕 参见王利明：《论〈个人信息保护法〉与〈民法典〉的适用关系》，载《湖湘法学评论》2021年第1期。

的同意”的事由外，第 2 项至第 7 项均为无需取得信息主体个人同意的合理使用事由。而第二章“个人信息处理规则”第二节“敏感个人信息的处理规则”中共有第 28 条至第 32 条这 5 个条文，但却没有单独规定敏感个人信息合理使用的抗辩事由。从体系解释来看，似乎可以认为在同一章“一般规定”中第 13 条的合理使用抗辩事由可以直接适用于敏感个人信息的合理使用抗辩。但问题在于，如果是直接适用，又如何能体现出对敏感个人信息的特别保护呢？

以 GDPR 为例，第 9 条（特殊类别的个人数据处理）第 2 款规定了（b）～（j）9 项合理使用事由，尽管这 9 项中的某些事由与第 6 条（处理的合法性）第 2 款的（b）～（f）中的某些事由相类似，但第 9 条第 2 款在具体要求上明显更为严格。例如，第 6 条的（d）项规定数据处理是为了保护数据主体或另一自然人的重大利益所必需时，可构成合理使用而无需数据主体同意。虽然第 9 条也作了类似的规定，但在前提条件的设置上，除满足第 6 条（d）项中的要求外，还需满足“数据主体物理上或法律上无法给予相关同意”的要件。再例如，第 6 条的（e）项规定数据处理是为执行公共利益领域的任务所必须时，可以构成合理使用而无需数据主体的同意。尽管第 9 条也作了类似的规定，但却分别在（g）项、（i）项及（j）项将公共利益限定于“为实现重大公共利益所必需”“为实现在公共健康领域的公共利益所必需”及“为公共利益进行档案管理”等具体情形，同时在各项规定中附加了依据的法律与实现的目的成比例、为数据主体的根本权益提供相应保障措施等条件。此外，GDPR“序言”第（53）部分还提及，对于敏感个人数据的处理，除了适用该等处理的特殊要求外，有关合法处理的条件方面的规则也应同时适用。这意味着，针对个人数据的处理，如果连第 6 条的合法处理条件都无法满足，就更不能满足第 9 条中的条件要求，前者是后者合法性处理的底限性要求。

在立法思路上，我国《个人信息保护法》第 13 条基本对应 GDPR 第 6 条，而《个人信息保护法》第 28 条至第 32 条关于“敏感个人信息的处理规则”的规定则基本对应 GDPR 第 9 条。但通过比较可以发现，《个人信息保护法》第 28 条至第 32 条并未如 GDPR 第 9 条那样单独规定敏感个人信息的合理使用规则。对此，有学者认为，对于敏感个人信息的处理，GDPR 采取的是“原则禁止＋例外允许处理”的禁令模式，而我国《个人信息保护法》采取的则是对处理条件进行严格限制基础上的一般允许处理模式。〔53〕 的确，虽然我国《个人信息保护法》对于敏感个人信息的处理也采取了一般允许处理的立法模式，但并不意味着敏感个人信息的处理条件与一般个人信息相同。《个人信息保护法》第 28 条第 2 款规定的“敏感个人信息的处理要件”便起到了对敏感个人信息的处理进行严格限制的功能：（1）《个人信息保护法》第 6 条第 1 款规定“处理个人信息应当具有明确、合理的目的”，《个人信息保护法》第 28 条第 2 款在此基础上，又进一步要求针对敏感个人信息的处理还应具有“特定的目的”。例如，《汽车数据安全管理若干规定（试行）》规定收集指纹、声纹、人脸、心律等生物识别特征信息，应出于增强行车安全的目的，而不能是出于智能驾驶、导航等其他目的。再例如，立法机关仅授权科研机构收集患者的敏感私密信息用于研发新冠疫苗，那么该科研机构便不得将收集的敏感私密信息用于研发其他用途的疫苗

〔53〕 参见前引〔46〕，王苑文。

或其他超出授权范围的用途。此外，对于“特定目的”的认定，还应结合个人信息处理者的身份以及其所提供的商品或服务、履行的法定职责或法定义务的性质等综合认定。例如，只有诊疗、体检、保险机构为特定目的才可以处理个人的医疗健康信息。〔54〕（2）《个人信息保护法》第28条第2款要求针对敏感个人信息的处理应具有“充分的必要性”，如果对于处理敏感个人信息的特定目的实现没有充分的必要性，仍不应处理自然人的敏感个人信息。例如，《汽车数据安全管理若干规定（试行）》规定收集指纹、声纹、人脸、心律等生物识别特征信息，应对于增强行车安全的目的有充分的必要性，如果对于增强汽车安全的目的实现是可有可无的，便不得收集上述敏感个人信息。（3）《个人信息保护法》第28条第2款要求针对敏感个人信息的处理应采取“严格保护措施”。例如，《个人信息保护法》第55条规定个人信息处理者处理敏感个人信息，应当事前进行个人信息保护影响评估，并对处理情况进行记录。再例如，针对个人生物识别信息的传输和储存，需要采取加密等安全措施，并将个人生物识别信息与个人身份信息分开储存，原则上不储存原始样本。〔55〕

因此，对于敏感个人信息的合理使用，应首先符合《个人信息保护法》第28条第2款的规定，才可以进一步适用《个人信息保护法》第13条第1款第2项至第7项中的合理使用情形。不过，有观点认为，《个人信息保护法》第28条第2款的规定过于抽象，存在任意解释的可能，可仿照GDPR的规定对敏感个人信息处理的法定事由进行列举，并以“公共利益”作为兜底性规定。〔56〕但实际上，《个人信息保护法》第28条第2款并非独自发挥功能，其实际上是对《个人信息保护法》第13条规定的个人信息处理者可处理个人信息的合法事由在敏感个人信息处理方面提供的强化保护标准，该强化标准当然也适用于敏感个人信息的合理使用。换言之，如果个人信息处理者主张其处理行为符合《个人信息保护法》第13条第1款第2项至第7项中的合理使用情形，但若不符合《个人信息保护法》第28条第2款规定，便不能构成对敏感个人信息的合理使用。这也是《个人信息保护法》与GDPR对于敏感个人信息处理的规定有所不同的地方。

五、结　语

在私密信息隐私权保护优先规则之下，出现了隐私权保护规则与个人信息保护规则在合理使用抗辩方面相冲突的局面。具体而言，隐私权保护规则下可直接援引的合理使用抗辩事由基本不存在，而《民法典》第1034条第3款确立的隐私权保护优先规则基于隐私权作为民事权利受保护程度更高的立场又排斥个人信息保护规则中合理使用抗辩事由的援引。尽管隐私权的位阶并非绝对高于个人信息权益，但《民法典》已然确立了私密信息隐私权保护模式优先的规则，也只能在解释论上为隐私权保护优先规则下私密信息合理使用被过度限制的困境寻求出路。基于此，本

〔54〕 参见杨合庆主编：《中华人民共和国个人信息保护法释义》，法律出版社2022年版，第86页。

〔55〕 参见前引〔54〕，江必新、李占国主编书，第103页。

〔56〕 参见孙清白：《敏感个人信息保护的特殊制度逻辑及其规制策略》，载《行政法学研究》2022年第1期。

文在将私密信息划分为非敏感私密信息和敏感私密信息的基础上，分别适用不同的具体解释路径，从而在私密信息隐私权保护优先规则下引入个人信息保护规则中的合理使用情形，以解决私密信息的合理使用空间被不当限制的问题。

Abstract: The rule of priority protection of the right to privacy of private information established in paragraph 3 of Article 1034 of the Civil Code leads to the improper restriction of the fair use space of private information. It is necessary to introduce the rule of fair use of personal information in the Personal Information Protection Law. On the basis of dividing private information into non sensitive private information and sensitive private information, the former can directly apply the fair use of personal information in items 2 to 7 of paragraph 1 of Article 13 of the Personal Information Protection Law through the second half sentence of paragraph 3 of Article 1034 of the Civil Code. The latter can be based on the interpretation that the rules for the protection of sensitive personal information should take precedence over the rules for the protection of privacy. On the premise of complying with the "rules for the processing of sensitive personal information" in paragraph 2 of Article 28 of the Personal Information Protection Law, the fair use of personal information in items 2 to 7 of paragraph 1 of Article 13 of the Personal Information Protection Law can be applied.

Key Words: rights of privacy, personal information, private information, sensitive information, fair use

(责任编辑：殷秋实　赵建蕊)

财经法学 No. 3，2022
pp. 65 - 79

“国家在场”视角下个人信息保护的实践检视与路径探索

王　娅*

内容提要：个人信息的保护与利用牵涉个人、企业和政府之间的利益与权力关系。国家需要作为独立的行为主体，调和参与者之间的冲突，整合个人信息保护实践。维护个人的知情同意规则、约束企业的隐私政策以及要求政府的行政规制这三种实践表明：在个人信息保护领域，国家在场是一个既成事实。然而，国家在场的实践存在两方面问题：一是内容上全面兼顾了个人权利、企业责任与政府义务，但各主体的履行实效欠佳，难以切实维护个人的合法权益；二是形式上以规范信息处理者的活动为主，但规制策略的取向不明，难以恰当界定企业自我规制与政府规制之间的关系。因此，信息时代国家的有效在场，需要重申人性尊严的基本理念，以维护个人的主体地位，也需要重述规制策略的主要共识，确立回应型规制，以妥善对待企业与政府之间的互动。

关键词：国家在场　个人信息保护　知情同意　企业自我规制　政府规制

一、问题的提出

全球个人信息保护立法的实践，如欧盟《通用数据保护条例》、美国《隐私权法》以及我国《个人信息保护法》，呈现出很强的国家引领和布局的色彩。个人信息保护立法的本质是国家对个人信息处理行使规制权。〔1〕个人信息保护是国家事务的组成部分，也是国家治理的重要场域，深受国家影响与支配。国家自始至终伴随着个人信息的书写、解释和演进，与个人信息保护紧密相

* 王娅，吉林大学法学院博士研究生。

本文为国家社科基金重大专项项目“核心价值观融入法治建设研究：以公正司法为核心的考察”（17VHJ007）、教育部人文社会科学研究专项项目“新时代中国特色社会主义法治思想研究”（18JF210）的阶段性成果。

〔1〕 See Colin Bennett, Charles Rabb, *The Governance of Privacy: Policy Instruments in Global Perspective*, Ashgate, 2003, p. 95.

连并持续互动，国家的显现也是个人信息能被持续保护的重要动因。因此，在个人信息保护领域，国家以何种方式在场，产生了什么影响以及未来努力的方向何在，是必须予以清晰回答的重要问题。对这些问题的有效回答，一方面有助于提高国内整体的个人信息保护水平，另一方面也有助于增进国际社会对中国个人信息保护制度的认可，为后续推进跨境数据流通机制创造积极条件。

既有的学术探讨主要围绕个人信息保护的权益基础、〔2〕归属的法益领域、〔3〕实践中的价值取向、〔4〕理论导向，〔5〕以及未来的路径选择〔6〕等方面展开。这些研究虽贡献了诸多智识，但大都以个人信息为关注点，过滤了对个人信息保护进行宏观全面认识的可能。进而言之，既有研究多从“如何保护”这一内部路径探寻着手，忽略了“国家如何主导参与者的互动实践”这一外部视角的观察与省思，这导致既难以对参与者之间的互动与博弈进行细致观察，又难以精准把握未来个人信息保护的方向与行动。因此，有必要爬梳国家在个人信息保护中的表现形式及其影响，并探索如何更好地将《个人信息保护法》中的国家意志具体化，以实现宏观议题的微观切换。

本文拟采用“国家在场”视角审视个人、企业与政府〔7〕之间的具体互动与典型实践，阐明国家对个人信息保护实践的影响，并在此基础上探讨个人信息保护的未来方向与行动要旨。

二、个人信息保护领域“国家在场”视角的引入

“国家在场”视角被广泛用于解释我国的经济、社会、法律与文化等领域的诸多现象和问题，取得了丰硕成果。然而，学者们对此概念的内涵尚未形成完整明确的界定。因此，在考察“国家

〔2〕 例如，欧盟有人格权保护模式，美国有隐私权保护模式。也有人称之为“数据保护法模式”和“消费者保护模式”。两者之间的主要区别在于默认规则，前者仅在法定理由之下才允许收集和处理数据；后者则相反，一般允许收集和处理个人信息，除非特别禁止。See William McGeveran，Friending the Privacy Regulators，58 *Arizona Law Review*，966（2016）.

〔3〕 主要有公法保护模式、私法保护模式和综合保护模式之争。参见赵宏：《〈民法典〉时代个人信息权的国家保护义务》，载《经贸法律评论》2021 年第 1 期；宋亚辉：《个人信息的私法保护模式研究——〈民法总则〉第 111 条的解释论》，载《比较法研究》2019 年第 2 期；程关松：《个人信息保护的中国权利话语》，载《法学家》2019 年第 5 期。

〔4〕 有过程保护与结果保护的分野，也有分享优先与控制优先的选择。参见蔡培如：《个人信息保护原理之辨：过程保护和结果保护》，载《行政法学研究》2021 年第 5 期；陆青：《数字时代的身份构建及其法律保障：以个人信息保护为中心的思考》，载《法学研究》2021 年第 5 期；杨贝：《个人信息保护进路的伦理审视》，载《法商研究》2021 年第 6 期。

〔5〕 主要有个人信息自决论、社会控制论和国家保护义务论的理念反思。参见高富平：《个人信息保护：从个人控制到社会控制》，载《法学研究》2018 年第 3 期；王锡锌：《个人信息国家保护义务及展开》，载《中国法学》2021 年第 1 期。

〔6〕 主要有法律保护、技术设计与伦理审视等多种进路。参见郑志峰：《通过设计的个人信息保护》，载《华东政法大学学报》2018 年第 6 期；肖成俊、许玉镇：《大数据时代个人信息泄露及其多中心治理》，载《内蒙古社会科学（汉文版）》2017 年第 2 期；前引〔4〕，杨贝文。

〔7〕 政府是国家意志的合法代理者，“国家”与“政府”往往相互替用。但本文将国家定位为超然的、中立的角色，用以居中调和个人、企业和政府之间的权益冲突。一方面是因为国家本身可以如西达·斯考切波（Theda Skocpol）所期望的那样，作为独立的“行为体”参与并追求某些社会目标；另一方面，政府兼具利用者与监管者的双重身份，始终难以对这两类身份保持反思性隔离，甚至在实践中很可能不经意地以双重身份相互解释或者错位使用。因此，把政府置于国家视角之下去思考，某种程度上避免了这种尴尬境地。再者，《个人信息保护法》中也将“国家”“处理个人信息的国家机关”“履行个人信息保护职责的部门”三者之间进行了称谓和职能上的区分，比如“国家”出现了 2 次，用以表明国家在个人信息保护方面的态度和行为，即建立健全个人信息保护制度以及积极参与个人信息保护国际规则的制定。See Peter B. Evans，Dietrich Rueschemeyer，Theda Skocpol，*Bringing the State Back in*，Cambridge University Press，1985，p. 9.

在场”视角下个人信息保护实践之前，有必要对“国家在场”的学术意涵做进一步限定。从结构上考察，“国家在场”具备实体论与方法论两个维度。就实体内容而言，“国家在场”是重要的理论模式，表达的是国家及其公权力对传统公共领域乃至私权领域的渗透。〔8〕作为一种重要的方法论，“国家在场”有助于对复杂的社会关系网络和多样的社会生产结构做出二元化透视，便于揭示隐匿于人类生活中的社会规律。〔9〕学者们使用“国家在场”，多是基于方法论层面，将其作为一种分析框架实现对社会现象的合理认知。

（一）“国家在场”的学术意涵与理论脉络

“国家在场”最早出自美国学者乔尔·米格代尔（Joel S. Migdal），意指一种“国家在社会中”的研究视角（a state in society perspective），〔10〕被用来检视国家和社会之间分组整合及其合纵连横的互动过程。20世纪90年代初，我国学者高丙中较早使用这一方法并引起广泛关注。他把米格代尔的“国家在社会中”直译为“国家在场”，即“以国家的视角来研究社会问题，进而对既往社会研究中所普遍存在着的内生主义倾向进行纠偏”〔11〕。此后，这一分析框架不断扩充，先后渗透到民族学、政治学、社会学等相关领域，为重新认识国家与社会的关系提供了一种新的解释模式。〔12〕但是，已有的研究并没有明确界定这一概念，只是用来描述国家对社会的影响以及社会对国家的回应之现象。

除了上述整体性理解之外，“国家在场”的概念还存在“国家＋在场”的组合式理解。作为概念组合的“国家在场”，其重点在于对“场（域）”的理解。“场域”概念的使用源于布尔迪厄（Pierre Bourdieu）。受黑格尔影响，他在“场域”的思考中加入“现实的关系”之因素。其后，他受马克思启发，给“场域”的思考注入“客观存在”的因素。因此，在布尔迪厄看来，场域是“在各种位置之间存在的客观关系的一个网络或一个构型（configuration）”〔13〕。他认为，当场与权力结合起来时，国家就是一个不可规避的权力结构，且与其他社会力量相结合，表现为一种多维度、多向度的运行。〔14〕因此，“国家在场”即是以国家的力量影响、作用或控制各种社会关系。

〔8〕参见王建生：《西方国家与社会关系理论流变》，载《河南大学学报（社会科学版）》2010年第6期；邓正来：《国家与社会：中国市民社会研究》，中国法制出版社2018年版，第16－18页。

〔9〕参见廉睿、高鹏怀：《“国家在场”与族群法治知识功能再造——基于西北T自治县生态保护的田野调查》，载《广西民族研究》2018年第4期。

〔10〕20世纪80年代，以彼得·埃文斯（Peter Evans）为代表的学者仅关注国家自主权和国家能力等方面的研究，这被称为国家中心主义。但国家中心主义很快受到挑战，以米格代尔为代表的学者坚持社会中心主义的立场，以回应国家中心主义的研究。参见〔美〕乔尔·米格代尔等编：《国家权力与社会势力：第三世界的统治与变革》，郭为桂等译，江苏人民出版社2017年版，第1页。

〔11〕高丙中：《民间的仪式与国家的在场》，载《北京大学学报（哲学社会科学版）》2001年第1期。不过，仍有一些研究国家与社会关系的学者依然使用“国家处在社会中”或“社会中的国家”这样的表达。参见肖瑛：《从“国家与社会”到“制度与生活”：中国社会变迁研究的视角转换》，载《中国社会科学》2014年第9期；侯利文：《国家与社会：缘起、纷争与整合——兼论肖瑛〈从“国家与社会”到“制度与生活”〉》，载《社会学评论》2018年第2期。

〔12〕其他研究参见何平：《“国家在场”下的妇女地位提升——以建国初期的妇女解放为例》，载《中共宁波市委党校学报》2008年第2期；秦永章：《藏传佛教活佛转世与“国家在场”》，载《西藏研究》2020年第5期；张锦鹏、刘丽凤：《国家在场：从清代滇南盐官营看国家边疆治理》，载《云南社会科学》2021年第4期。

〔13〕〔法〕皮埃尔·布尔迪厄、〔美〕华康德：《实践与反思——反思社会学导引》，李猛、李康译，中央编译出版社1998年版，第133－134页。

〔14〕参见前引〔13〕，皮埃尔·布尔迪厄、华康德书，第156页。

米格代尔的“国家”观念借用并改编了布尔迪厄关于“场域”的界定，〔15〕而且，米氏认为：“国家不是固定不变的实体，社会也不是。他们共同在相互作用的过程中改变各自的结构、目标、规则以及社会控制。它们是持续相互影响的。”〔16〕因此，无论是组合概念还是整体概念，“国家在场”就是被建构起来的一个研究方法，用来探讨国家权力在社会领域中的存在与体现，即国家通过政策、法律、行动、仪式等方式对社会产生影响，社会采取一定的方式和策略对国家进行回应。

（二）“国家在场”引入个人信息保护的可行性与必要性

作为舶来品，“国家在场”在具体运用方面需要进行理论探讨与实践检验。〔17〕除了在民族学与社会学等领域的运用，一些学者对“国家在场”做了进一步的延伸理解与扩展运用。比如，卫跃宁用它来表达法益变迁时所坚持的一种国家本位主义，突出国家主导的优势及作用；〔18〕陈洪等学者用它来描述国家以某种形态，通过干预、分化、渗透、整合及引领等各种方式和途径参与经济和社会事务的运作；〔19〕廉睿和高鹏怀用它来透视族群法治知识以获得对民族法治现象的合理解读；〔20〕任文启用它来检讨涉罪未成年人服务个案的实践；〔21〕许超等学者用它来思考全球治理中国家的地位与作用〔22〕等。因此，对“国家在场”这一分析框架的价值挖掘，已成为学者们不谋而合的共识。

本文亦借鉴这一研究范式，试图通过研究视角上的革新，分析并反思国家如何干预、渗透、整合及引领个人信息保护实践，并寻求理念与制度上的突破。从表征上看，这是一种视角革新，在强调学科交融与知识共享的语境中，具备形式层面的可接受性。从实质上看，由于国家作用于个人信息保护领域是一个既成事实，这一分析框架可用来透视国家参与个人信息保护的实践、影响及其不足。个人信息保护作为重要的社会问题，不仅是个人、企业与政府表达利益需求的场域，而且是国家表达权威的舞台。因此，“国家在场”视角的引入，就是立足外部观察的视角，检视国家如何渗透并规范个人信息处理活动，从而实现个人信息保护与利用的平衡。换言之，本文的目的在于审视国家在个人信息保护方面的微观运作、实践影响以及后续的调整方向。

〔15〕 米格代尔放弃了韦伯关于理想型国家的界定，反而在借鉴布尔迪厄“场域”概念的基础上，认为国家是一个权力场，集观念和实践于一体。在观念上，国家是一个被公众承认的整体性组织概念，但在实践中，国家与社会之间的互动呈现出四类结果类型：一是国家渗透致使社会力量消亡或顺从的完全转型；二是国家吸纳社会力量建立统治模式，社会也影响了国家；三是社会力量吸纳国家，虽然统治模式没有变化，但国家各组成部分的面貌发生变化；四是国家在努力渗透（社会）时完全失败。参见〔美〕乔尔·米格代尔：《社会中的国家：国家与社会如何相互改变与相互构成》，李杨、郭一聪译，张长东校，江苏人民出版社 2013 年版，第 22 页。

〔16〕 前引〔15〕，乔尔·米格代尔书，第 58 页。

〔17〕 参见崔榕：《“国家在场”理论在中国的运用及发展》，载《理论月刊》2010 年第 9 期。

〔18〕 参见卫跃宁：《由“国家在场”到“社会在场”：合规不起诉实践中的法益结构研究》，载《法学杂志》2021 年第 1 期。

〔19〕 参见陈洪等：《“国家在场”视角下英国竞技体育治理实践研究》，载《体育科学》2019 年第 6 期。

〔20〕 参见前引〔9〕，廉睿、高鹏怀文；廉睿、高鹏怀、卫跃宁：《由“乡土中国”到“国家在场”——族群法治知识在民族地区社会治理中的运行机制研究》，载《社会科学战线》2017 年第 10 期。

〔21〕 参见任文启：《国家如何在场？——国家亲权视野下涉罪未成年人服务个案的实践与反思》，载《青少年犯罪问题》2020 年第 5 期。

〔22〕 参见许超：《全球治理中国家如何在场——兼与刘建军教授商榷》，载《探索与争鸣》2021 年第 8 期；任剑涛：《找回国家：全球治理中的国家凯旋》，载《探索与争鸣》2020 年第 3 期；刘建军、莫丰玮：《国家从未离场，何须找回——兼与任剑涛教授商榷》，载《探索与争鸣》2021 年第 1 期。

正是基于上述考虑，“国家在场”这一分析框架被引入个人信息保护领域，使得阐述并揭示国家与个人信息保护制度的互动成为可能。“国家在场”视角的引入主要有以下三点理由：（1）现有的个人信息保护以个人为中心来对抗企业与政府，但个人受限于认知能力和经济能力，难以应对动态化、复杂化和风险不确定的个人信息处理过程，也无法回应数据权力蕴含的技术性和资本性的基本特性。而且，个人信息保护的有效性有赖于国家规制，实践中处于维权第一线的往往是监管机构而非个人本身。〔23〕（2）国家保护个人信息具有规范基础。虽然我国《宪法》并未对个人信息保护做出明确规定，但《宪法》第33条第3款对人权保障的规定以及第38条关于公民人格尊严的强调，无不切实地指引并评价国家权力的行使。〔24〕《个人信息保护法》亦从国家层面建立个人信息保护制度，推动在政府、企业、相关社会组织和公众之间形成共同参与个人信息保护的良好环境。（3）国家介入具有强烈的现实需要。数字经济的蓬勃发展使得个人信息成为生产生活的关键环节和核心内容。各主体一方面共享某些价值追求和利益结构，另一方面却因立场、利益取向和社会角色不同而产生冲突。〔25〕但基于个人信息生成的数据权力，却被企业和政府垄断，〔26〕使得个人正处于并将长时间处于被观察、被记录与被操纵的境地。因此，需要国家以中立的姿态介入，运用多种方式或不同工具，去调整个人、企业与政府之间的互动。

三、“国家在场”视角下个人信息保护的实践与功能

个人信息保护是国家的权力实践，但国家意志的嵌入较为隐蔽，需要逐步解析国家的实践与功能，以便真切凸显“国家”的存在，进而促进对国家权威的认同。国家作为形塑力量在场，其姿态是主导者和施惠者，而政府、企业和个人则是参与者和受惠者。本部分就分别从“个人—企业—政府”的主体维度去观察并分析国家在个人信息保护实践中的在场。

（一）维护个人利益的知情同意规则

原则、规则或标准等具有表达特定思想情感、传递主流价值取向、引导规范主体行为的作用。因此，个人信息保护才会成为日常生活的公共谈资，知情同意规则才会作为信息处理最重要的合法性基础。〔27〕国家嵌入的一条路径就是通过“知情同意”规则进行多渠道、多形式的输出，使公众不自觉地成为这一规则的“传导者”和“发酵者”，完成规则主导权的“潜在让渡”和规则精神的内在化。具体而言，公众在以实用和自利为导向的生活逻辑支配下，通过直接援引部分与日常生活相近的法律文本，如《民法典》《个人信息保护法》，将“知情同意”规则结合日常经验进行再理解或转换成“近经验”，从而实现这一规则的具体化。此外，知情同意规则的力量还在于塑造主体和客体的思想和行为，即通过宣传、鼓动、强制、引导与塑造等方面的功能，帮助个人建构、维持或瓦解社会权力关系。一方面，知情同意规则有助于维护和发展个人信息自决的

〔23〕 参见张新宝：《我国个人信息保护法立法主要矛盾研讨》，载《吉林大学社会科学学报》2018年第5期。
〔24〕 参见前引〔5〕，王锡锌文。
〔25〕 参见程啸：《论我国个人信息保护法中的个人信息处理规则》，载《清华法学》2021年第3期。
〔26〕 参见前引〔5〕，王锡锌文。
〔27〕 参见王成：《个人信息民法保护的模式选择》，载《中国社会科学》2019年第6期。

理念；另一方面，知情同意规则的形成及散播方式又深刻地影响各种社会力量及其相互关系。经由知情同意规则的确立与引导，国家意志就在个人信息保护中得以彰显，扎根于“民众的集体无意识之中”〔28〕。

因为信息主体与信息处理者之间存在着信息不对称和谈判力量不均衡的情况，所以在具体规则的设计上需要对个人进行倾斜保护，以平衡信息市场中出现的非对称权力结构。知情同意规则在发展过程中，通常与国家权力相伴相生、互为增益，呈现出一种“隐秘性共谋关系”。例如在“黄某诉微信读书案”中，原告指出，微信读书没有征得原告的有效同意，而随意迁移微信好友关系，默认向未关注的微信好友公开读书信息。在“凌某某诉抖音案”中，原告预先清空了手机通讯录并拒绝软件读取，但在“可能认识的人”一栏中，抖音依然向他推荐多年未联系的同学、朋友等。在两案中，北京互联网法院均支持了原告的诉讼请求。〔29〕这就说明，当知情同意规则深入人心，会激励用户积极维权，司法体系也会及时回应。知情同意规则的承认意味着，虽然个人信息具有很强的社会性和公共性，〔30〕但个人信息自决依然是应坚持的基本理念。换言之，个人信息的处理活动需要个人参与，个人信息不能不受限制地被轻易交换和出售。

（二）约束企业行为的隐私政策

在知情同意规则指引之下，企业需要制定隐私政策以供用户选择产品和服务时参考，这是国家对企业所能提出的要求之一，也是世界多个国家和地区的通行做法。“仪式及其包含的符号是至关重要的，因为个人成为个人，社会成其为社会，国家成其为国家并不是自然天成的，而是通过文化、心理的认同而构成的，而这种认同又是通过符号和仪式的运作所造就的。”〔31〕隐私政策就是国家在保护个人信息时面向企业要求的文本实践。所谓隐私政策，是一种关于信息将如何被使用的通知形式，以及一种限制信息未来使用的默认合同承诺。〔32〕不过，它绝非透明的中性要素，而是表征了一种权力意志，即国家对于企业开展个人信息保护所持有的价值判断。因此，隐私政策被视为一种企业自我规制的工具。〔33〕当企业将个人信息保护实践公之于众时，也为行政机关提供了规制其行为的依据。〔34〕

隐私政策在个人信息保护领域中的绑定，不仅为保护个人信息注入“合法性”或部分“合法化”的国家力量，而且在借用国家力量的同时获得对企业行为的引导与塑造。比如美国联邦贸易委员会鼓励企业自我规制，自我规制在欧盟实践中也是不可或缺的组成部分。隐私政策是国家在场的文本具象，它负载着许多保护个人信息的说明与解释，而且文本的符号体系使这些描述呈现

〔28〕 申恒胜：《乡村社会中的“国家在场”》，载《理论与改革》，2007 年第 2 期，第 14 页。

〔29〕 参见《微信读书被判侵犯用户隐私“流量变现”的边界在哪里》，载 https://finance.eastmoney.com/a/202008031578777585.html，最后访问时间：2021 年 11 月 9 日。

〔30〕 参见前引〔5〕，高富平文。

〔31〕 前引〔11〕，高丙中文。

〔32〕 See Daniel J. Solove, Privacy and Power: Computer Databases and Metaphors for Information Privacy, 53 *Stanford Law Review*, 1448 (2001). 其后，丹尼尔·索洛夫（Daniel J. Solove）和伍德罗·哈佐格（Woodrow Hartzog）在 2014 年发表的一篇文章中这样定义隐私政策，它是指互联网企业以在线文件的方式自愿披露其对用户个人信息保护的原则和措施。See Daniel J. Solove, Woodrow Hartzog, The FTC and the New Common Law of Privacy, 114 *Columbia Law Review*, 594 (2014).

〔33〕 See Joel R. Reidenberg et al., Privacy Harms and the Effectiveness of the Notice and Choice Framework, 11 *I/S: A Journal of Law and Policy*, 490 (2015).

〔34〕 参见高秦伟：《个人信息保护中的企业隐私政策及政府规制》，载《法商研究》2019 年第 2 期。

出某种规则和运行方向，比如企业如何收集、使用、存储和分享个人信息，如何保证信息安全，用户享有哪些权利，设置了哪些隐私功能等等。隐私政策虽然是被规定的，其功用也相对稳定，但这一切并非是固定不变的。在某些情况下，隐私政策也是变量。比如当企业变更或修订他们的隐私政策时，就应该在登录及版本更新时以推送通知、弹窗或其他符合法律要求的适当形式向个人展示变更后的指引。

（三）要求政府作为的行政规制

隐私政策合规的过程中可能出现各种各样的困境，如企业违反承诺或自身能力不足等。因此，政府作为国家意志的直接代理人有必要加以干预，通过相应的积极作为，以回应个人对个人信息保护的高度关切。这是国家对于政府所能提出的要求之一，也与域外经验相一致。比如美国联邦贸易委员会会审查相关的信息或直接联系企业，如果必要，还会向企业发出正式函件，要求提供文件和信息，进行约谈或要求作证，并可能访谈第三方。欧盟各成员国政府会审查各行业的行为规范，在确保规范内容与法律一致的情况下，还会征求信息主体和其他利害关系人的意见。〔35〕政府规制强调的是外部监督和处罚，旨在使隐私政策真正产生拘束效果。同时，由于个人信息侵权案件举证困难，政府介入可以弥补个体举证能力的不足。政府规制表征的是一种权力意志的自上而下的传达，即国家对于政府履行个人信息保护职责的行为要求和立场预设。一方面，个人信息保护充分运用了政府资源，使自身价值得到政府的正式承认和维护；另一方面，政府也从个人信息保护中收获了“政治意义和经济价值”，并最终转化为政府规制的动力。

政府规制的提倡是因为国家充分意识到在个人信息保护中，仅靠知情同意规则和企业自我规制具有难以避免的消极作用。因此，国家充分运用积极的“功能替代”策略以实现相应的保护目标。从这个意义上来说，政府规制就是个人信息保护实践的强力后盾。不过，为了确保企业创新与经济发展，政府仅在个人和企业的行为难以维护个人利益时实施其规制。政府也可以主动组织开展个人信息保护的宣传教育，对应用程序的隐私保护情况进行测评，制定个人信息保护细则与标准等。政府运用科层治理的运作逻辑，自上而下地实现对个人信息保护的控制。一方面，由国家网信部门统筹协调个人信息保护工作和相关监督管理链条，让监管责任得以层层传达与落实。另一方面，在个人信息有序保护中，个人的信息保护需求与企业的信息利用需求也得到极大满足。政府通过治理链条的逐级向下延伸，也将企业与个人隐秘地吸纳到国家权力运作的规范框架内。

四、个人信息保护领域“国家在场”的影响与局限

“国家在场”的既成事实并不意味着国家恰当有效地在场。国家可能在某一方面过度在场，而在另一方面又在场不足，从而引发个人信息保护目的与效果之间的错位。〔36〕“国家在场”的实践评价不以程度来划分，而以效果为基准，即实现对个人信息保护的“负责任关怀”（respon-

〔35〕 参见前引〔34〕，高秦伟文。

〔36〕 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。

sible care)。〔37〕正如诺思所言："国家的存在是经济增长的关键，然而国家又是人为经济衰退的根源。"〔38〕这在个人信息保护中也得到了印证。国家一方面推动个人信息保护在意义和内容方面的转型升级，另一方面，国家的介入也打破了个人信息利用的原有格局，产生了预期内或预期外的新问题。

（一）内容上全面兼顾但实效欠佳

虽然我们仅用了知情同意规则、企业自我规制和政府规制这三种情形表征国家在场，但这并不意味着国家仅在这些方面实现了在场。围绕个人、企业和政府这三个主体的维度，国家分别找到了具体在场的意义和价值。个人信息保护关涉的参与者主要分为个人、企业和政府这三类，〔39〕因此，国家在场是全面的，且对每一主体都有相应的要求，只不过要求的兑现可能因应各种情形而呈现差异。那么各个主体兑现承诺的实际情形是怎样的呢？

其一，关于知情同意规则的实践情形。知情同意规则是个人信息处理中应该坚持的基本前提，但实质上却处于履行弱化或无能的境地。〔40〕已有社会学研究证明，如果给予个人足够的信息控制能力与条件，反而增加他们披露敏感信息的意愿。也就是说，如果他们泄密的意愿增加得足够多，这种控制的增加反而会使他们更加脆弱。〔41〕因此，不假思索地点击同意按钮是当下普通人的常态操作，知情同意规则只是信息处理者娴熟使用的一块遮羞布而已。

其二，关于企业隐私政策合规的实践情形。隐私政策是对法律规定的具体内化，但往往也是相对简短的承诺，是一种语法上而不是实质性的公共关系；往往是为外部消费设计的，而不是为了影响企业的内部功能。〔42〕隐私政策的实践本身也存在流于形式、〔43〕搭便车、规避责任以及受控于其他机会主义行为诱惑等情形。〔44〕特别是，个人信息更多集中于少部分互联网企业手中，难以保证它们在信息市场上不会滥用支配地位，在非价格竞争要素的个人信息保护方面不会不当地削减服务水平。〔45〕因此，隐私政策更多是企业因应法律规定和现实情势而做出的面子工程，

〔37〕"负责任关怀"是一种很高的标准，是我们对个人信息保护实践中国家有效作用的最高期待。"负责任关怀"始于 20 世纪 80 年代中期的加拿大化学品生产商协会，用以应对像博帕尔毒气泄露事件这样的严重化学品事故。负责任的关怀包括一系列自愿的行为守则，这些守则使参与的公司能够达到对环境负责任的管理的高标准。

〔38〕〔美〕道格拉斯·C·诺思：《经济史上的结构和变革》，厉以宁译，商务印书馆 2011 年版，第 25 页。

〔39〕本文为写作需要只列出了个人、企业与政府这三类主要的参与者，但个人信息保护实践中还存在一些其他的、独立的利益相关者，比如研究机构、记者和国际组织等等。有学者甚至认为数据应该被公认为"全球公域"（global commons），并被提供给所有可能的参与者加以利用以发挥数据的巨大社会价值。See Jennifer Shkabatur, The Global Commons of Data, 22 *Stanford Technology Law Review*, 354 (2019).

〔40〕比如隐私条款冗长且隐秘，专业且晦涩，个人没有时间、没有能力去阅读并理解；隐私条款简而无用，多而无功，但个人为了使用产品和服务默认同意；企业利用的内容与个人同意的内容不一致，或者超出个人同意的范围；个人信息处理的即时性特征也使得同意难以实际展开；现实中也确实存在着无须用户同意即可收集的情形等等。

〔41〕See Laura Brandimarte et al., Misplaced Confidences Privacy and the Control Paradox, 4 *Social Psychological and Personality Science*, 340 (2013).

〔42〕参见前引〔1〕，Colin Bennett、Charles Rabb 书，第 121－138 页。

〔43〕有学者分析了美国 1999 年至 2005 年间 50 家金融公司在《格雷姆—里奇—比利法》生效以来的情况，发现金融隐私通知更加完整和合规，但它们仍然能够收集大量关于客户的信息，并与关联公司广泛共享这些信息，但提供给消费者的选择并没有重大变化。See Xinguang Sheng, Lorrie Faith Cranor, An Evaluation of the Effect of US Financial Privacy Legislation Through the Analysis of Privacy Policies, 2 *I/S: A Journal of Law and Policy*, 943 (2006).

〔44〕See Dennis Hirsch, The Law and Policy of Online Privacy: Regulation, Self-Regulation, or Co-Regulation? 34 *Seattle University Law Review*, 468 (2011).

〔45〕参见韩伟、李正：《反垄断法框架下的数据隐私保护》，载《中国物价》2017 年第 7 期。

纸面上的承诺与现实中的行动存在脱节。

其三，关于政府规制的实践情形。政府规制是对个人信息被侵犯的情形以及公众对隐私安全高度关切的回应。现代规制理论主张，在充分发挥市场机制和企业自我规制作用的前提下，政府规制也不能缺位。〔46〕但传统政府规制多以命令和控制为主，实施过于严格、僵化，存在阻碍创新与竞争的可能；〔47〕信息时代的政府规制又面临着平台权力、信息过载以及系统性威胁等方面的问题〔48〕。换言之，由于数据资源和处理能力的差异，政府呈现出无力通过传统治理机制作用于科技企业的算法型运作过程，由此产生治理失灵或监管真空的情况。〔49〕因此，政府规制的目标设置以及方向调整还需要进一步的细化和一致，否则就会导致行政成本上升、行动效益大打折扣，进而影响个人信息保护的治理效果。

（二）形式上规制为主但取向不明

规范个人信息处理活动是国家的核心关注。赋权与规制是个人信息保护的常用手段。不过，赋权本身受制于个人的有限性与复杂的社会现实，难以有效实现，规制反而是可欲且可及的选择。〔50〕虽然知情同意规则、企业自我规制以及政府规制都存在或多或少的问题，但国家在场的核心关切依然落脚在企业自我规制与政府规制的博弈上。个人信息保护并非保护个人对其个人信息的控制性权益，而是为了规制个人信息处理风险，防范与救济个人数据处理与利用活动可能产生的侵害后果。〔51〕

综观各国规制实践，虽然美国一再强调以自我规制为主要形态，但其政府规制也发挥了巨大作用。同样地，企业自我规制与政府规制的结合，正成为欧盟及其成员国的主要做法。〔52〕因此，企业自我规制与政府规制并非互相排斥的关系。换言之，个人信息保护实践需要企业自我规制和政府规制的合力。这两种规制之间应该是什么关系，国外学者对此莫衷一是。〔53〕有学者认为自我规制是政府规制的同义词，可根据具体情况作为政府规制的有效补充。〔54〕有学者则认为自我

〔46〕 参见前引〔34〕，高秦伟文。

〔47〕 See Jerry Louis Mashaw, David Harfst, From Command and Control to Collaboration and Deference: The Transformation of Auto Safety Regulation, 34 *Yale Journal on Regulation*, 277 (2017).

〔48〕 See Julie Cohen, The Regulatory State in the Information Age, 17 *Theoretical Inquiries in Law*, 369 (2016).

〔49〕 参见张兆曙、段君：《网络平台的治理困境与数据使用权创新：走向基于网络公民权的数据权益共享机制》，载《浙江学刊》2020年第6期。

〔50〕 当然，规制本身也不是有效保护个人信息的灵丹妙药。相反，规制通常需要在不同情况下结合不同的策略。而所有的执行都是不完美的，规则总是会被一些人违反。

〔51〕 参见王锡锌：《个人信息权益的三层构造及保护机制》，载《现代法学》2021年第5期。

〔52〕 参见前引〔34〕，高秦伟文。不过之前的研究认为，自我规制与政府规制是根本不同的实体，这意味着它们不能很好地融合。See Darren Sinclair, Self-Regulation Versus Command and Control? Beyond False Dichotomies, 19 *Law and Policy*, 530 (1997).

〔53〕 有学者根据政府干预程度的不同，将自我规制分为纯粹的自我规制、替代的自我规制和条件的自我规制；有学者则根据规制力度的渐变确立了自我规制、强制性的自我规制、自由裁量惩罚的命令规制、无自由裁量惩罚的命令规制这一规制的金字塔结构；还有的学者将自我规制分为强制的、促进的和默认支持三种类型。See Philip Eijlander, Possibilities and Constraints in the Use of Self-Regulation and Co-Regulation in Legislative Policy: Experiences in the Netherlands-Lessons to Be Learned for the EU? 9 *European Journal of Comparative Law*, 4 (2005); Ian Bartle, Peter Vass, Self-regulation within the Regulatory State: Towards a New Regulatory Paradigm? 85 *Public Administration*, 901 (2007); Ian Ayres, John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate*, Oxford University Press, 1992, p. 39.

〔54〕 See Anil K. Gupta, J. Lad Lawrence, Industry Self-Regulation: An Economic, Organizational, and Political Analysis, 8 *The Academy of Management Review*, 416 (1983).

规制是政府规制进程的一部分，必要时候还可能加强政府规制。〔55〕

根据上述讨论，自我规制与政府规制处于理论坐标的两极，中间是连续的光谱，通过调整各自的占比，以形成适应一定国情、阶段和需要的规制进路。〔56〕实证调研指出：在规制更加模糊的国家，如德国、美国，尽管文化和法律环境非常不同，但都具有最强大的企业隐私管理实践；而更受规则约束的国家，如法国和西班牙，倾向于遵从程序，而不是嵌入隐私。〔57〕那么，在我国，企业自我规制与政府规制之间应该采取何种策略呢？

目前，我国《个人信息保护法》只是将企业自我规制与政府规制的内容分别纳入“个人信息处理者的义务”和“履行个人信息保护职责的部门”的法律条文之下，未曾就两者之间如何自处与互动做更进一步的规定，也未就现阶段采取什么样的规制策略给予明确的指引，政府在个人信息领域的规制边界也难以划定。〔58〕因此，基于上述域外经验的启发与反思，在个人信息保护领域，关于我国规制策略的取向依然是一个开放的、可以继续讨论并完善的课题。

五、“国家在场”视角下个人信息保护的再造与表达

我们在前文既描述了国家的具体实践，也评价了国家实践的主要影响，并指出：国家虽然对各方主体有针对性的要求，但也未能有效地保护个人利益，维护个体尊严；虽然手段上以规制为主但也未能恰当地规范个人信息处理活动，安置好企业与政府之间的关系。因此，国家权力的参与有服务于个体权益与公共福祉的一面，但也难以避免国家在具体的制度设计或策略选择方面的缺憾。不过，所谓的不足或缺失，亦是进一步夯实国家实践的基石。

（一）理念重申：内化人性尊严

虽然法律制度和文化背景存在差异，但各国个人信息保护的立法与执法实践都证明了尊重个体是不变的坚守。换言之，人性尊严作为宪法的基本原则能够从不同的制度和文化土壤中找到依据，虽然在具体内容上各有侧重，但都是国家意志的核心表征。〔59〕因此，提倡个人信息保护，其目的在于保护个人的合法权益，使其人性尊严免于减损或矮化。重申人性尊严是对康德“任何时候以人作为目的，而不是仅仅当做手段”〔60〕观念的具体确认，也是个人信息保护实践的保护依据与行动理由，用以调整、指引或辩护人们的行动选择。“只有本人能够控制自己的个人信息，才可能自由发展个人人格。如果个人无法知晓自己的个人信息在何种程度上、被何人获得并加以

〔55〕 参见前引〔53〕，Ian Bartle、Peter Vass 文，第 890 页。

〔56〕 比格纳米（Francesca Bignami）认为，美国以透明的行政诉讼、惩罚性行政执行以及普遍的规制诉讼为主，而欧盟则以威慑导向的规制执行和企业自我规制为主。See Francesca Bignami, Cooperative Legalism and the Non-Americanization of European Regulatory Styles: The Case of Data Privacy, 59 *American Journal of Comparative Law*, 412 (2011).

〔57〕 See Kenneth A. Bamberger, Deirdre K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*, The MIT Press, 2015, pp. 12 - 14.

〔58〕 不过，在政府规制内部则体现出多主体监管的架构：一方面，国家网信部门对个人信息保护有统筹协调和监督管理的职能；另一方面，国务院有关部门、县级以上地方人民政府有关部门，在相应的职责范围内也负有监管职能。

〔59〕 参见〔德〕瓦尔特·施瓦德勒：《论人的尊严：人格的本源与生命的文化》，贺念译，人民出版社 2017 年版，第 148 - 150 页。

〔60〕〔德〕康德：《道德形而上学的奠基》（注释本），李秋零译注，中国人民大学出版社 2013 年版，第 55 页。

利用，则个人将失去作为主体参与的可能性，而沦为他人刻意操纵的信息客体，被沦为客体正是人性尊严被侵害的同义语。"〔61〕因此，个人信息保护最终针对的不是个人信息本身，也不是要限制个人信息处理，而是保护个人信息之上的自然人的人性尊严。〔62〕当个人信息之于人的人格尊严、人格自由发展价值被渐次肯定时，法律规则从充分尊重市场交易自由逐渐向维护信息主体人性尊严倾斜。〔63〕

但是，现实场景中个人的主体性地位面临的挑战日渐增加，以致人性尊严的理念指引愈发无力并衰颓。个人基本上难以从信息网络，尤其是电子化场景中抽身退出，公民习惯于命令—服从模式，因此，通过个人信息的收集和处理，个人就不再是独立的个体，而是一个个以名字、符号和标识为载体的档案，〔64〕公民生活也越来越成为可见的、可计算的、可预期的资源库〔65〕。而企业与政府不仅无法切实地践行彼此的承诺与职责，而且在某种程度上实现了共谋，共同控制个人生活以谋取私利。当个人信息遭受侵权时，由于信息处理者的技术和资本优势，私人维权面临取证难、成本高和赔偿低的困境。因此，当个人在面对强大的组织和信息处理者，在面临动态化、复杂化和不确定的过程时，更需要强化人性尊严以维护自身的独立与自主性，更需要公私机构对个人利益保持尊重和克制。正如《迈向新的数字伦理：数据、尊严和技术》报告中所指出的那样，个人信息保护相关于个人的个性发展，只有更好地尊重和保障人的尊严，才可以制衡个人面临的无所不在的监视和权力不对称。〔66〕因此，我们需要在个人与企业、个人与政府的互动中，重申人性尊严的基本理念以规范具体的信息处理行为。

重申人性尊严的价值理念，其意义表现在两个方面：首先，人性尊严理念要求公私机构的行为必须受到限制，即企业与政府应依据法定权利和法定程序收集、处理、公开与共享个人信息，否则，公民就有沦为客体的风险，难以实现信息主体的自决与自主。在信息社会，每个公民客观上已成为数据权力项下的一个"信息符号"，并被视为可以被计算、预测和控制的客体来对待。〔67〕因此，当外部侵害的风险加剧时，为防范公民成为"被处理的客体"，必须树立人性尊严理念。其次，人性尊严具体指向个人自治以及随之得到保障的不歧视（平等）、身份识别（信息的正确与完整性）、信息安全与财产利益以及社会信任等附加的实体价值与其他基本权利。〔68〕因此，个人信息保护的标准应以人为尺度，体现人的目的性，并融入人类文化之中。比如企业可以听取用户的使用建议，不直接使用"不同意即退出"的模式，而是将网络产品与服务的功能区分

〔61〕 杨芳：《个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体》，载《比较法研究》2015 年第 6 期，第 25－26 页。

〔62〕 参见前引〔51〕，王锡锌文。

〔63〕 参见郑维炜：《个人信息权的权利属性、法理基础与保护路径》，载《法制与社会发展》2020 年第 6 期。

〔64〕 See Ruth N. Cohen, *Whose File is it Anyway*, *National Center for Civil Liberties*, Civil Libertise Trust, 1982, p. 10.

〔65〕 参见胡水君：《全球化背景下的国家与公民》，载《法学研究》2003 年第 3 期。

〔66〕 See European Data Protection Supervisor, Towards a New Digital Ethics: Data, Dignity and Technology, available at https://edps.europa.eu/sites/default/files/publication/15－09－11_data_ethics_en.pdf, Last visited on May 25, 2021.

〔67〕 See John Cheney-Lippold, *We Are Data: Algorithms and the Making of Our Digital Selves*, New York University Press, 2017, p. 141.

〔68〕 参见前引〔5〕，王锡锌文。

为核心业务功能和附加业务功能。〔69〕这一方面有助于吸纳新用户扩展注册信息的来源与数量，另一方面有助于老用户固着、细化关键信息的利用与共享。

正是通过这两方面的意义阐释，个人才能够真正参与到个人信息保护实践中，并从个人信息的利用中受益。因此，人性尊严的内化之于个人的重要性就在于，使个人得以找回被消解的主体性，重获参与群体生活与复杂理性活动的能力与品质。

（二）基本共识：重述规制理念

规范个人信息处理活动的首要难题并不是如何明确企业与政府之间的规制边界或设计某种规制方案，而是梳理规制背后应该坚持的主要共识，否则规制本身就是任意的或不切实际的，不仅治标不治本，而且遏制了数字红利和企业创新。那么，信息时代的规制策略应该坚守哪些共识呢？

其一，应该要求合作而不是对抗，〔70〕即以建立有序共赢的公私伙伴关系为目的。长期以来，我国的立法和实践普遍将政府规制、企业自我规制截然分开，要么放任企业恣意活动，要么由政府直接干预，突出两者的对抗而忽略合作的内涵，强调规制结果而忽略了规制的过程，导致规制效果不尽人意。〔71〕再者，企业自我规制与政府规制之间各有优劣，两者结合可能发挥更好的作用。比如巴特尔（Ian Bartle）和瓦斯（Peter Vass）根据英国近些年来的自律政策和实践指出，自我规制具有可实现的公共利益目标，虽然可能带来某些严重的系统性威胁，但可借助问责与透明的议程来实现政府规制对其的监督，以更好地实现个人数据的利用与管理。〔72〕

其二，正视市场自由化的反应，承认规制过程中的压力。在相互依存以及权力和知识分散的现代性条件下，规制不是单向的，即从公共到私人，而是私人行动者可以充当政府的监管者。〔73〕出于市场竞争或制度供给不完备的压力，因其规制者与规制对象的一体性，自我规制掌握了更多的知识与信息，从而可以找到最符合成本有效性要求的解决方案。因此，自我规制作为有效且高效的社会控制手段的正当性不能被低估。〔74〕而且，政府规制应保持自我克制的品性。一方面是因为政府规制往往具有极强的管制色彩，有可能阻碍个人信息的有效利用和增值提升。另一方面是因为政府权力运作本身受制于人力、金钱和时间等客观因素，不能想当然地“拍脑袋”决定，而是需要细致的成本收益分析。比如有学者就指出，政府规制的出场受制于无序成本与权力成本的比较。〔75〕

其三，规制应该是阶段性、动态的。“我们踩在一块完全陌生的薄冰上，很少有人了解约束

〔69〕 核心功能旨在满足用户注册产品或服务后的基本要求，附加功能则是为提升用户体验而设计。

〔70〕 参见前引〔47〕，Jerry Louis Mashaw、David Harfst 文，第 167 页。

〔71〕 参见前引〔34〕，高秦伟文。

〔72〕 参见前引〔53〕，Ian Bartle、Peter Vass 文，第 885 页。

〔73〕 See Colin Scott，Private Regulation of the Public Sector：A Neglected Facet of Contemporary Governance，29 *Journal of Law and Society*，56 (2002).

〔74〕 See Neil Gunningham，Joseph Rees，Industry Self-regulation：an Institutional Perspective，19 *Law and Policy*，363 (1997).

〔75〕 政府规制介入与否，依赖于对无序成本（disorder cost）与权力成本（dictatorship cost）的衡量。无序成本是指私人（此处指企业）损害其他人利益的能力，权力成本则是指政府或政府官员损害他人利益的能力。只有当自我规制已经无法控制无序成本时，才需要政府规制的介入。See Andrei Shleifer，Understanding Regulation，11 *European Financial Management*，443 (2005).

企业信息流动所产生的商业道德、法律问题和政治问题。"〔76〕而且，"无论是关乎私人信息保护，抑或是关乎国家安全，私人服务、公共服务和规制利益之间的界限本质上是模糊的"〔77〕。因此，我们不能僵硬地坚持某一种或混合的规制策略，而是要因应社会现实的变化增减不同规制手段的分量。传统观点认为，欧盟的规制要求过于严格，而美国的规制则较为松懈。但比格纳米的研究却发现，美国的规制较为严格精确，而欧盟的规制则趋于宽松。〔78〕因此，一国规制风格的选择并不是固定不变的，而是因时而异的。

（三）具体路径：确立回应型规制

目前，国外规制实践的共识是企业自我规制与政府规制的结合，但具体如何安排却有不同的操作。有学者基于美国和爱尔兰对 Facebook 规制措施的调查与研究，提出了回应型规制（responsive regulation）的策略，即减少对抗，拒斥传统惩罚，政府规制更多的是最后的手段。〔79〕也有学者提出企业和政府之间进行合作规制（co-regulation）的混合模式，认为这是一种可执行的、严格的方法，既能保护个人隐私，又能跟上并满足日益增长的互联网经济的需求。〔80〕无论是回应型规制还是合作规制，都不是新的现象，也面临着不少质疑。比如合作规制被认为缺乏透明和问责，以致有做空社会公共利益，并致使企业俘获政府的可能；〔81〕回应型规制也被认为增加了政府被俘获的可能性，高估了企业的理性和道德行为，削弱了人们对执法严肃性的信心〔82〕等等。

每一种规制策略都包含风险。现阶段我们需要试验并评估哪种方式是适合我国的切实有效的策略。在充满变化和不确定性的技术革新时代，我国可以确立回应型规制的阶段性选择，这既能够较好地处理信息技术发展与个人信息保护的关系，又能够有效地促进企业自我规制机制的形成与发展。与任何良好的友谊一样，回应型规制对企业和政府都有利。之所以未选择合作规制，是因为合作规制之于具体实践更多的是一个想法，而不是现实。〔83〕而回应型规制在很大程度上本身就指向企业的善意与合作，强调较少的对抗技术以调动企业积极合规的能动性来实现。〔84〕回

〔76〕〔美〕阿尔文·托夫勒：《权力的转移》，黄锦桂译，中信出版社 2018 年版，第 170 页。

〔77〕 Martin Lodge，Andrea Mennicken，Reflecting on Public Service Regulation by Algorithm，in Algorithmic Regulation，in Karen Yeung，Martin Lodge ed.，*Algorithmic Regulation*，Oxford University Press，2019，p. 195.

〔78〕 See Francesca Bignami，Cooperative Legalism and the Non-Americanization of European Regulatory Styles：The Case of Data Privacy，59 *American Journal of Comparative Law*，416（2011）.

〔79〕 参见前引〔2〕，William McGeveran 文，第 959 页。

〔80〕 合作规制又称协同规制，是指机构与行业团体或其他第三方合作，制定详细的实质性规则。这些规则随后可能成为可执行的法律，经常（虽然不总是）受到政府监管机构的批准或许可。See Dennis Hirsch，The Law and Policy of Online Privacy：Regulation，Self-Regulation，or Co-Regulation? 34 *Seattle University Law Review*，441（2011）. 艾拉·鲁宾斯坦（Ira S. Rubinstein）也主张，合作规制应该成为经济社会问题的重要思路和措施，他甚至提出了合作规制取得成功必备的五个标准：开放和透明、完整性、解决搭便车问题的策略、监督和执行，以及使用第二代设计特征。See Ira Rubinstein，Privacy and Regulatory Innovation：Moving Beyond Voluntary Codes，6 *I/S*，*A Journal of Law and Policy for the Information Society*，380（2011）.

〔81〕 参见前引〔44〕，Dennis Hirsch 文，第 442 页。

〔82〕 See Steve Tombs，Understanding Regulation? 11 *Social and Legal Studies*，126（2002）.

〔83〕 合作规制是一个很有前途的机制，但存在重大局限性，比如受制于特定的历史文化影响，难以切实有效地达成共识。合作规制与回应型规制之间的区别主要有：（1）前者主要关注规则的内容，后者主要关注执行规则的方法，而不是规则的实质；（2）前者实践的前提是许多利益相关方达成广泛共识，后者只是影响监管机构对所有被监管实体的行为；（3）后者应用时也可着眼于合作；（4）后者切实地存在并运用着。参见前引〔2〕，William McGeveran 文，第 981 页。

〔84〕 参见前引〔52〕，Darren Sinclair 文，第 534 页。

应型规制本身也可以模糊不同地区间本应明显的区别，便于有效、灵活和合作地改进现实世界的数据保护实践。〔85〕

我国的立法实践虽然没有明确我国的规制策略，但也可以从一些具体规定解读出“先自我规制后政府规制”的意味。第一，《个人信息保护法》第 58 条规定，提供重要互联网平台服务、用户数量巨大、业务类型复杂的个人信息处理者，应当履行“按照国家规定建立健全个人信息保护合规制度体系，成立主要由外部成员组成的独立机构对个人信息保护情况进行监督”的义务。这预示着，关于企业信息处理行为，优先适用内部合规并外部监督的行为规范策略，政府规制只在有必要的时候出场。第二，《个人信息保护法》第 61 条关于个人信息保护主管部门的职责范围，主要提及宣传教育、接受投诉与举报、组织测评并公布结果以及调查与处理违法个人信息处理活动等，这些内容不同于常规的惩罚措施，而是一种内含企业自身改进的主动引导与被动回应的治理要求。第三，《个人信息保护法》第 62 条确立了国家网信部门承担统筹协调职责。这是一种辅助性（subsidiarity）的规制形式要求，意味着政府可以不直接或间接地积极参与，但政府对大多数规制计划必须保证有某种形式的参与。即自我规制构成对政府规制的一种回应，如果企业不采取任何行动，政府就会采取行动。〔86〕第四，《个人信息保护法》第 63 条与第 64 条是关于具体监管措施的规定，从询问、调查到约谈、审计，再到移送公安机关依法处理等，从中可以看出政府的力量根据情境的轻重缓急而相应地从“督促改进到直接惩罚”发生变化。这说明，“监管机构一开始假设美德（他们应该以合作作为回应），但当他们的期望落空时，他们会以逐步惩罚和以威慑为导向的策略做出回应，直到被监管机构顺从”〔87〕。

因此，回应型规制虽然不是国家应对新现实的唯一方式，却是现阶段的一种可为的经济性选择。〔88〕一方面，回应型规制体现了规制的灵活性、包容性和敏感性，实现了多主体参与动态性规制，大大降低政府规制的成本以及避免规制失灵的问题。〔89〕比如政府主动改变直接提供保障的全能角色，转变为向企业购买服务，并鼓励和支持企业开展个人信息保护的研究、推广、宣传、培训和咨询等服务。另一方面，回应型规制实现了从外在强制到内在激励的转化。换言之，回应型规制的采用可以使政府规制的外在要求同企业保护个人信息的内在激励相容，促使企业认真对待个人信息保护实践，将个人信息保护的期望实质性地整合进工作流程中，而不是单纯停留于“如果你同意，请点击”的形式保证或避免制裁的消极应对上。

六、结　语

个人信息保护表面上围绕着个人、企业与政府之间的权利义务责任关系而展开，但其运作的背后离不开国家这一行为主体的渗透、干预、整合与引领。国家形塑个人信息保护实践主要是通

〔85〕 参见前引〔2〕，William McGeveran 文，第 959 页。

〔86〕 See Robert Baldwin, Martin Cave, Martin Lodge, *Understanding Regulation: Theory, Strategy, and Practice*, Oxford University Press, 2012, p. 138.

〔87〕 Neil Gunningham, Darren Sinclair, Integrative Regulation: A Principle-Based Approached to Environmental Policy, 24 *Law and Society Inquiry*, 864 (1999).

〔88〕 参见前引〔53〕，Ian Bartle、Peter Vass 文，第 885 页。

〔89〕 参见前引〔86〕，Robert Baldwin、Martin Cave、Martin Lodge 书，第 136－140 页。

过其对个人、企业与政府这三类主体的要求与互动而展开。知情同意规则、企业隐私政策以及政府规制这三类实践某种程度上实现了国家对个人的赋权和对企业与政府的规制。不可否认的是，这些实践仍然存在着这样或那样的现实窘境与不利因素，以至于不仅个人利益的维护大打折扣，而且企业自我规制与政府规制之间的关系取向未定。因此，需要以国家之名，重申人性尊严的理念，避免个人被视为客体；重述规制策略的共识，酝酿信息时代规制国家的行动准则；确立回应型规制，指引个人信息保护的未来议程。

Abstract：The protection and utilization of personal information involves the interests and power relations among individual，enterprise and government. State need to act as independent actor to mediate conflicts among participants and integrate personal information protection practices. The three practices of maintaining informed consent rules of individual，restricting privacy policies of enterprise and requiring administrative regulation of the government show that state presence is a fait accompli in the field of personal information protection. However，there are two problems in the practice of state presence. One is that the content gives full consideration to individual rights，enterprise responsibilities and government obligations，but the performance of each subject is not effective enough to effectively protect the legitimate interests of individual. The other is that the form is mainly to regulate the activities of information processors，but the orientation of regulation strategies is unclear，and it is difficult to properly define the relationship between enterprise self-regulation and government regulation. Therefore，the effective presence of the state in the information age needs to reaffirm the basic idea of human dignity to maintain the subject status of the individual. At the same time，the main consensus of regulation strategy is restated and responsive regulation is established to properly treat the interaction between enterprise and government.

Key Words：a state in society，personal information protection，informed consent，enterprise self-regulation，government regulation

（责任编辑：赵　真　赵建蕊）

财经法学 No. 4，2023
pp. 118 - 133

网络空间中信息安全守门人的刑法义务

喻浩东*

内容提要：拒不履行信息网络安全管理义务罪的增设为网络空间中信息安全守门人的刑法义务提供了实定法根据。鉴于司法实务所遭遇的困境，有必要对信息安全义务的目的、性质和范围展开教义学上的体系化解读。在目的构建上，无论用户信息专有权说还是信息网络安全管理秩序维护说都存在难以克服的缺陷。应当提倡一种系统耦合的法益观，将该义务的目的界定为保障信息共享的互惠性风险分配机制，以实现法律系统与数字经济系统间的有效沟通。在性质界定上，义务犯论错误地理解了积极义务的产生根据，将支配犯与作为犯、义务犯与不作为犯不当混同。信息安全义务的本质是对网络服务提供者数字生产权力的纠偏，因而应当归属为基于组织管辖产生的消极义务而非基于制度管辖产生的积极义务。在明确保护目的和义务性质的基础上，对该义务保护范围的确定，既要实现保障信息共享的互惠性风险分配机制的规范目的，也应对其中内含的危险给予正当性控制。

关键词：网络服务提供者　信息安全守门人　系统耦合的法益观　拒不履行信息网络安全管理义务罪

一、问题的提出

在信息网络世界中，数据的收集、处理、利用等环节均控制在占据技术主导优势的各类网络服务提供者之手，因此在风险管辖方面，网络服务提供者实际扮演着“守门人”的关键角色。基于此，国际社会普遍要求作为数据控制者或处理者的网络服务提供者承担数据保护的法律义务。我国亦不例外，十余年来经由《中华人民共和国网络安全法》（以下简称《网络安全法》）、《工业和信息化领域数据安全管理办法（试行）》、《中华人民共和国数据安全法》等多部法律法规的颁行逐步构建起一套有关平台数据安全保护义务的制度体系。

为了稳定规范化预期、发挥积极一般预防的刑法功效，我国立法机关在《中华人民共和国刑

* 喻浩东，复旦大学法学院讲师。

法修正案（九）》中增设了286条之一，规定网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，致使用户信息泄露，造成严重后果的，应当追究刑事责任。不过，该条自颁行以来几乎未曾得到实际适用。〔1〕个中原因除了行政前置性程序的设置导致很多案件未进入刑事程序之外，主要还在于信息网络安全管理义务究竟为何模糊不清。〔2〕

在首起电信运营商因拒不履行这一信息安全义务被判处刑罚的案件中，法院认定被告人李小全负有查验、评估、审核行业卡使用情况的职责，明知远特公司曾三次违反实名制的管理规定，仍将大量带有个人信息的回收卡交给亚飞达公司，违反用户实名制进行挑卡，造成严重后果，且在两年内经监管部门多次责令改正而拒不改正，构成拒不履行信息网络安全管理义务罪。〔3〕可是，法院并未明确被告人的上述行为到底违背了哪部法律、行政法规中的哪一义务。本案中远特公司曾被三次责令改正的法律根据是《电话用户真实身份信息登记规定》，但该规定并未达到法律或行政法规的层级，而且，法院并未论证用户信息泄露造成的严重后果能够归责于被告人违反法律、行政法规义务的行为。

由此看来，解读网络服务提供者的信息安全义务理应构成信息刑法的重要议题。本文将试图在追求数据安全保护与数据有序流动相对平衡的价值理念下，从以下三个方面展开体系性论述：首先需要明确这一安全义务的目的何在。目的是全部法律的创造者，〔4〕科处义务必须回答“这样做意在保护什么”的问题。其次需要界定立法者为实现这一目的采用了何种规制方式，也即安全义务的性质。这种义务究竟归属义务犯的积极义务还是支配犯的消极义务，对于归责原理的适用而言具有显著影响。最后在明确该义务的目的和性质的基础上，体系化地构建其实体内容并划定其合理边界。

二、信息安全义务的目的重构

既有学说对保护目的的界定无论在方向还是结论上都存在难以克服的缺陷，其共同症结在于，未能意识到并发挥法益作为法律系统与其他社会子系统间媒介的作用。

（一）既有学说的缺陷所在

1. 对“用户信息专有权说”的批评

有论者认为，信息法益就是信息主体所享有的信息权利。信息专有权的核心是基于法规范明确授权的对数据处理的“允许”。同时，又因为立法者将该罪设置在《中华人民共和国刑法》（以下简称《刑法》）第六章第一节“扰乱公共秩序罪”中，所以要将法益进一步限缩为具备公共利益属性的信息专有权。〔5〕

但无论在事实还是规范层面，都谈不上用户的信息专有权。在事实层面上，用户信息是用户

〔1〕 相关实证研究报告，参见杨新绿：《拒不履行信息网络安全管理义务罪司法适用问题及化解》，载《湖北警官学院学报》2020年第5期。

〔2〕 参见李世阳：《拒不履行网络安全管理义务罪的适用困境与解释出路》，载《当代法学》2018年第5期。

〔3〕 参见云南省昆明市盘龙区人民法院（2020）云0103刑初1206号刑事判决书。

〔4〕 Vgl. Rüthers/Fischer/Birk, Rechtstheorie mit Juristischen Methodenlehre, 10. Aufl., 2018, § 15 Rdn. 520.

〔5〕 参见敬力嘉：《论拒不履行信息网络安全管理义务罪——以网络中介服务者的刑事责任为中心展开》，载《政治与法律》2017年第1期。

在社会交往中产生的，是用户与各类智能设备互动的产物，本身就具有公共属性，严格来说只能是“与用户有关的信息”。海量的用户信息被控制在各类网络平台的手中，而用户个体根本无法像控制财产那样控制这些信息。〔6〕从规范层面来说，强调用户对信息的专有，人为地在法律上制造资源的稀缺，无异于禁锢思想、阻吓交流，本质上是不受限制地限制他人的自由。〔7〕且单就其中个人信息的保护而言，不同领域中的个人信息应当受到保护的程度也不相同，要根据信息的利用可能性、信息利用的目的以及经由信息科技所开启的处理可能性等因素来区分不同的保护层级。〔8〕

另外，该论者将“信息网络安全管理”不当限缩到网络信息传播治理的范畴，但不论是就用户信息的保护，还是就刑事证据的保存而言，其都难以归入该范畴之中。我国有学者曾对网络信息传播犯罪的类型进行了概括：类型一是该信息传播行为本身就是《刑法》所禁止的构成要件或构成要件行为的一部分；类型二是发布或传播不法信息本身并非构成要件的实行行为，只有当该类信息的发布或传播与行为人自己或他人在现实世界的行为结合才会造成法益侵害。〔9〕显然，网络服务提供者不履行对用户信息或刑事证据的保护或保存义务造成法益侵害的，并不属于上述两类传播犯罪中的任何一类。

2. 对“信息网络安全管理秩序说”的质疑

更多论者基于体系解释的原理，将法益界定为信息网络安全的管理秩序。〔10〕对此本文也难以认同，提出如下质疑理由：

其一，特定领域的管理秩序是否为适格的集体法益，并非不言自明。对此，德国学者格雷科给出了三个消极性标准：（1）循环性测试，即如果不假定某种集体法益存在，就无法将特定的刑罚法规正当化，这一事实并不是认定这种集体法益确实存在的理由；（2）分配性测试，即很多个体都有意愿分享某种利益，这一事实并不是认定一个集体法益存在的理由；（3）非特定性测试，即如果侵害某一所谓的集体法益总是同时以侵害个人法益为前提，那么就不允许将这种集体法益认定为特定刑罚法规的保护利益。〔11〕信息网络安全管理秩序无法通过这三个标准的检验：首先，并不是非要假定该秩序利益的存在，才可以对信息安全义务予以正当化。秩序利益的形成反倒以保障个人权益为前提。其次，尽管社会成员都对信息网络安全秩序享有利益，但这并不是将该秩序本身作为法益保护的理由。再次，由于拒不履行信息安全义务总是以侵犯用户的人身和财产权益为前提，因此无法将更为抽象的管理秩序作为该义务的保护法益。

其二，将特定领域的管理秩序界定为法益，是对规范与法益的混淆，会致使单纯的行政不服从被认定为犯罪。社会秩序，意指社会进程中存在某种程度的一致性、连续性和确定性。人们在生活安排方面对连续性的诉求与他们要求在相互关系中遵守规则的倾向之间是存在联系的。只要人的行为受到法律规范的控制，重复规则性这一要素就会被引入社会关系之中。遵循规则化的行

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

〔7〕 参见杨芳：《个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体》，载《比较法研究》2015 年第6 期。

〔8〕 Vgl. Thilo Weichert, Datenschutzstrafrecht-ein zahnloser Tiger? NStZ 1999, 490.

〔9〕 参见王莹：《网络信息犯罪归责模式研究》，载《中外法学》2018 年第 5 期。

〔10〕 参见谢望原：《论拒不履行信息网络安全管理义务罪》，载《中国法学》2017 年第 2 期；前引〔2〕，李世阳文；杨新绿：《论拒不履行信息网络安全管理义务罪的法益》，载《北方法学》2019 年第 6 期。

〔11〕 Vgl. Luís Greco, Gibt es Kriterien zur Postulierung eines kollektiven Rechtsguts? FS-Roxin, 2011, S. 208.

为方式，为社会生活提供了很高程度的有序性和稳定性。〔12〕所以，这里的秩序体现了规范运作的实际状态，但法益则是行为规范所保护的客体，是秩序所要保护的价值，这说明秩序与法益不能混同。〔13〕强调某一特定社会秩序需要加以维护，仅仅是表达了国家想要运用公权力对该领域进行行政管理的意愿之事实，并没有交代管理的目的何在。将特定领域的社会管理秩序界定为法益，无疑是站在政府的一端，其追求的管理秩序无非就是该领域参与者服从行政管理的有序状态。〔14〕这样的法益观容易导致将管理法规等同于管理秩序的套套逻辑，而且将单纯违反行政法规的行为认定为犯罪，也不符合变动社会中法益理论的应然走向。杨仁寿在《法学方法论》中指出，倘若社会急剧变迁，法律目的与社会目的不同，就应当以社会目的来解释法律。〔15〕信息网络领域由一元化的国家管制逐渐迈向多元主体共治的局面，也正要求法律与时俱进，改变其“压制的性格”，转而成为社会各个子系统自我运作与自我治理的协调机制。

（二）保护目的的重新界定

1. 系统耦合的法益观之提倡

既有学说共通的弊病在于，无论是从《刑法》条文规定的行为对象来确定法益，还是从具体犯罪所属的类罪来确定法益，〔16〕均只是在刑法体系内部对《刑法》条文保护目的的逻辑推导。这样做的消极后果有二：其一，以预设目的为导向的解释，无非是朝着解释者想要达致之结论的循环论证。〔17〕其二，完全侧重于方法论意义的法益理论，致使法益概念逐渐丧失了批判立法的机能，因为除非相应的道德观念土崩瓦解，否则刑法保护就很容易获得正当性。〔18〕由刑法体系内部确定的法益不仅在价值取向上可能与他系统中应当保护的利益南辕北辙，且据此所进行的构成要件解释很可能导致将他系统中原本应予鼓励的行为不当认定为犯罪，实质上是法律系统粗暴干预他系统自主运作的表现。

想要走出当前法益理论深陷的泥潭，就不得不将现代社会建立在二阶观察基础上的社会沟通模式纳入法益的构建当中。现代社会分化为若干自创生的子系统，这些子系统均是封闭运行的实体，它们借助其要素的递归式生产自我创生和自我维持。〔19〕尽管如此，封闭运作的系统又具有开放的面向，系统对其环境保持着认知上的开放性和敏感度。在环境为系统自创生的延续制造问题时，系统就会以自己固有的方式产生激扰。〔20〕虽然系统与其环境之间没有直接的接触，但却通过其自身运作对环境形成观察。这种观察是系统内部的活动，它以区分系统和环境为前提，同时具有自我指涉和外部指涉的面向，通过与外部环境的沟通实现认知上的开放。〔21〕其中，法律

〔12〕 参见〔美〕E·博登海默：《法理学：法律哲学与法律方法》，邓正来译，中国政法大学出版社 2010 年版，第 228、239 页。

〔13〕 参见马春晓：《经济刑法的法益研究》，中国社会科学出版社 2020 年版，第 127 页。

〔14〕 参见蓝学友：《互联网环境中金融犯罪的秩序法益：从主体性法益观到主体间性法益观》，载《中国法律评论》2020 年第 2 期。

〔15〕 参见杨仁寿：《法学方法论》（第 2 版），中国政法大学出版社 2013 年版，第 72 页。

〔16〕 参见张明楷：《刑法分则的解释原理》（第 2 版）（上），中国人民大学出版社 2011 年版，第 350－352 页。

〔17〕 参见〔德〕英格博格·普珀：《法学思维小学堂》，蔡圣伟译，元照出版公司 2010 年版，第 96 页。

〔18〕 参见〔德〕伊沃·阿佩尔：《通过刑法进行法益保护？——以宪法为视角的评注》，马寅翔译，载赵秉志、宋英辉主编：《当代德国刑事法研究》（第 1 卷），法律出版社 2017 年版，第 57 页。

〔19〕 Vgl. Georg Kneer, Armin Nassehi, Niklas Luhmanns Theorie sozialer Systeme: eine Einführung, 2000, S. 65.

〔20〕 参见前引〔19〕，Georg Kneer 书，第 61 页。

〔21〕 参见前引〔19〕，Georg Kneer 书，第 98 页。

系统依照“合法/非法”的符码形成封闭的自我运作，以区隔于以“支付/不支付”为符码的经济系统和以“有权/无权”为符码的政治系统。

法律系统的唯一功能在于稳定规范性预期，违法事实的发生并不会导致法律无效，因为法律系统会反事实地坚持预期，拒绝做出相应调整。正是由于该系统的沟通排斥“合法/非法”以外的所有第三种价值，脱离外部的社会脉络而维持反事实的“规范性”，其他社会子系统才得以自主运行。在此意义上，法律具有保障经济发展、政治稳定、科学繁荣、宗教自由等多种成效。〔22〕但符码本身并不具有单纯凭借自身而生存的能力，唯有在法律系统的纲要层次上展开悖论，它们才能以自我再制的方式具有生产性。这里的纲要补充符码的语意和使用符码的条件，分派“合法/非法”价值的判断标准。在这一层次上，法律系统认知环境，汲取非法律价值，从而保障自身的学习能力，使之不至于在获得“自主性”的同时丧失对环境的适应性和敏感度。〔23〕经由纲要的运作，环境的变动被建构为“法律事件”，对法律系统内部的既有状态形成激扰，迫使该系统自身做出相应的调整。〔24〕由此，法律系统与经济、政治系统间形成“结构耦合”的关联模式。在这一过程中，法益充当了系统间沟通的媒介，它将刑法体系外部的信息也即各种价值判断、政策因素和利益衡量纳入系统自我指涉的介质。基于此，无论认定哪种犯罪，都需要对行为特定领域的运作逻辑和沟通模式进行考察，在此基础上进行刑法构成要件的判断。〔25〕

2. 目的重构：信息共享的互惠性风险分配机制

根据系统耦合的法益观，确定具体罪刑规范的保护目的，需要首先关注该规范外部指涉的他系统中的利益诉求，然后思考将这种利益诉求在刑法系统内部转化为何种法益。

古典社会的经济理论假设个人对私利的追求是驱动经济增长的唯一有效方式。个人追求私利的根本原因在于对稀缺资源的竞争压力及对是否能够获得合理的稀缺资源的不确定性。彼时隐私权保护意识的兴起，就来源于对社会成员之间不当竞争的必要限制。私权利制度赋予了社会成员足够的理性，使其可以根据自身意愿来自我决定并为相应后果负责。然而，有机社会的成员针对稀缺资源将会是合作分享取代竞争占有，“共同创造—共享—按需分配”取代了“分工—私权—交易”模式。〔26〕在大数据时代，个人数据信息具有充裕性，对数据的挖掘、开放和处理产生出众多衍生信息或结果，很多都是一开始无法预测的。因此，早在 1996 年，互联网先驱佩里·巴洛就在《网络空间宣言》中倡导信息的自由分享。美国维基百科计划的实施、我国网络上的字幕组、戏仿和知识共享等在线社群努力创造的开放式环境，反映了信息分享和协作的模式受到关注。而后，从 Web 2.0 时代去中心化的信息交互到 Web 3.0 时代的网际和数据互通，技术的升级和应用创新都在不断促进信息分享和盈余扩大。〔27〕核心交互既是网络平台出现的根本原因，也是其所追求的基本目标。平台想要促进有价值的核心交互，就必须将生产者和消费者吸引过来，为之提供方便且易于联系和交换的工具与规则，同时还要利用相互之间的信息有效匹配生产

〔22〕 参见高鸿钧、赵晓力主编：《新编西方法律思想史（现代、当代部分）》，清华大学出版社 2015 年版，第 328 页。

〔23〕 参见前引〔22〕，高鸿钧、赵晓力主编书，第 329－330 页。

〔24〕 参见前引〔22〕，高鸿钧、赵晓力主编书，第 341 页。

〔25〕 参见刘涛：《系统理论下刑法与社会关系研究》，中国法制出版社 2023 年版，第 326－329 页。

〔26〕 参见吴伟光：《大数据技术下个人数据信息私权保护论批判》，载《政治与法律》2016 年第 7 期。

〔27〕 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。

者和消费者，使其互惠互利。〔28〕

对于信息共享这一他系统中的利益诉求，必须经由刑法纲要转化为法律系统内部的具体法益。实际上，民法和刑法上有关信息保护的规范，其最终目的都指向了信息共享，但各自的侧重面向并不相同：民法上对个体的赋权和对信息处理者的赋责，更多地为了提升信息利用的效率和平衡相关主体间的利益。例如有论者指出，倘若以财产权方式来保护个人信息并规范其使用，因为受制于信息主体的意志，往往会使主体陷入要么全部同意要么全部拒绝的两难境地，不利于提升信息使用的质量和效率。〔29〕与此不同，刑法对信息权益的保护，则更侧重于防范信息共享中的负外部性效应，其关注的是风险如何公平分配、谁应当对风险的实现负责的问题。经济学中的外部性，是指有人承担了他人行为引起的成本或获得别人行为创造的收益。如果社会成本大于个人成本，这时有人承担了行为人带来的伤害，我们就称其为负外部性。〔30〕而在信息时代的法律规制中，刑法主要侧重防范由网络服务提供者等信息控制者和处理者的行为导致的隐私侵害等负外部性效应。〔31〕对于刑法系统的运作而言，必须确立并保障一套指向信息共享的风险分配机制，以形成“合法/非法”的判断符码，通过制裁破坏该风险分配机制的行为来确证规范的效力。

公平的风险分配机制的核心在于互惠原则。该原则要求个人的利他必须带来足够合作的盈余，而且群体成员在他人没有给予互惠行为的回报时，可以在未来不再做出利他行为。在有限的群体和空间中，对于这一原则可以通过查明和惩罚非互惠者并将其踢出群体的方式来加以维护。〔32〕而在超越时空的网络空间中，社群规范的互惠约束机制或许不再能够适用，通过法律对违反互惠分享规范的行为进行规制就必不可少。信息的互惠分享也是数据生产论的题中之义：如果把数据比作小麦，网络平台就是小麦被收集、研磨、精炼为面粉的加工厂。对于用户来说，数据只是他们浏览互联网的副产品，但对于平台来说，这些就是重要的生产资料。只有平台才能够将个人信息与行为数据加工提取为生产要素。〔33〕然而，如果任由他人侵犯用户的信息权益，最终致使用户对于平台的整体信任崩塌，不再放心将自己的信息提供给网络服务提供者，就会像釜底抽薪一样剥夺作为生产者的平台最为基本的生产原料。〔34〕所以，对于违背互惠原则、强制用户承担其不应承担的信息风险的行为，刑法就应当予以制裁，以保障公平的风险分配机制的效力。当然，互惠的风险分配也要求刑法将保护目的最终指向信息的共享，也即，对信息处理者的风险分配也应当有利于促进信息共享目的的实现。倘若将数据收集、利用与流转的决定权完全置于用户之手，不仅事实上不可能，而且也不利于生产者充分挖掘数据潜藏的巨大价值。如此也就不难理解，为什么个人数据的私权保护理论遭遇了猛烈抨击。〔35〕

〔28〕 参见〔美〕杰奥夫雷·G. 帕克等：《平台革命》，志鹏译，机械工业出版社 2017 年版，第 39－47 页。

〔29〕 参见郑维炜：《个人信息权的权利属性、法理基础与保护路径》，载《法制与社会发展》2020 年第 6 期。

〔30〕 参见张维迎：《理解公司：产权、激励与治理》，上海人民出版社 2014 年版，第 65－67 页。

〔31〕 参见〔德〕克劳斯·施瓦布、〔澳〕尼古拉斯·戴维斯：《第四次工业革命——行动路线图：打造创新型社会》，中信出版集团 2018 年版，第 11 页。

〔32〕 参见前引〔27〕，梅夏英文。

〔33〕 参见张凌寒：《数据生产论下的平台数据安全保障义务》，载《法学论坛》2021 年第 2 期。

〔34〕 世界经济论坛的一篇报告指出，个人和数据控制机构间存在的严重信息不对称，造成了严重的信任危机，影响数据的真实产生和自由流动，阻碍创新和大数据潜力的发挥。参见个人信息保护课题组：《个人信息保护国际比较研究》，中国金融出版社 2017 年版，第 44 页。

〔35〕 参见高富平：《个人信息保护：从个人控制到社会控制》，载《法学研究》2018 年第 3 期；前引〔6〕，欧阳本祺文。

因此，不但刑事立法者不应当忽视数字经济发展中的利益诉求，网络运营者实施的有利于促进数据共享的行为不应当纳入刑事处罚的范围，而且刑事司法也应参照同样的思路来区分“合法/非法”，如后文所述，应通过目的性对“用户信息”“泄露”等构成要件要素予以解释，合理地确定网络服务提供者的信息安全义务之边界。

三、信息安全义务的性质界定

《刑法》第 286 条之一实际规定了三种类型的信息网络安全管理义务，而其中针对用户信息的安全管理义务，应当从数字生产权力纠偏的维度对其性质予以界定。

（一）义务类型：消极义务和积极义务

有论者援引了罗克辛关于义务犯成立的根据——对行为人所承担的社会角色和规范义务的违反——认为拒不履行信息安全管理义务罪属于典型的义务犯。该论者据此指出，作为犯以积极制造法益风险的方式支配犯罪进程和法益侵害结果，而不作为犯主要体现为违背义务导致原本可以不发生的结果发生，两者分属存在论和规范论的范畴。〔36〕

但这种观点恐怕将支配犯和作为犯、义务犯和不作为犯不当混同。作为与不作为的区分显然是存在论意义上对行为人之行为形态的客观描述，与之相反，支配犯和义务犯的区分则是规范论意义上关于哪一行为人构成正犯的规范性评价。在存在论层面上，人们观察某行为是否体现为一种积极的能量投入，而在规范论视域中，基于“从实然中不能推导出应然”的方法二元论，某一存在结构（作为或不作为）并不能决定规范评价（犯罪支配或义务违反）的结论。在规范论的意义上，有论者甚至宣称，所有犯罪的成立都必须满足义务违反的前提要件。〔37〕 至少对于过失作为犯来说，注意义务的违反是法定的构成要件要素，而过失结果的归责还必须满足注意义务违反与结果之间的规范关联。对于故意作为犯来说，如果认为其和过失作为犯仅是位阶关系，那么也可以说前者是具备更高不法程度和责任程度的后者。〔38〕

值得注意的是，我国学者曾提出的支配维度和义务维度的结果归责的二分模式，与这里所说的支配犯与义务犯的二元划分并不能同日而语。支配维度的结果归责，基本上对应于行为人对导向结果的因果流程拥有事实性操控的作为的情形，而义务维度的结果归责，则主要用来解决行为人对结果并未施加现实作用力的场合如何归责的问题。〔39〕 但对结果是否施加了现实作用力，并不是义务犯成立与否的判准。只有当行为人所负担的义务是具有人身专属性的特别义务时，才有讨论义务犯的余地。

实际上，只有将犯罪划分为基于组织管辖和基于制度管辖的二元类型，才能真正为判断信息安全义务是否属于义务犯的特别义务提供实质判准。雅各布斯提出以“管辖”来统摄全部犯罪行

〔36〕 参见周光权：《拒不履行信息网络安全管理义务罪的司法适用》，载《人民检察》2018 年第 9 期。

〔37〕 Vgl. Otto, Grundkurs Strafrecht-Allgemeine Strafrechtslehre, 7. Aufl., 2004, § 5 Rdn. 10 ff.

〔38〕 Vgl. Puppe, Strafrecht Allgemeiner Teil: im Spiegel der Rechtsprechung, 4. Aufl., 2019, § 7 Rdn. 1 ff.

〔39〕 具体的论述，参见劳东燕：《事实因果与刑法中的结果归责》，载《中国法学》2015 年第 2 期。

为的归责判断，〔40〕至于行为人根据什么对某一事件负有管辖义务，既可能基于自由行动所带来的组织圈的扩张，也可能基于社会制度所附加的团结义务。对管辖义务做这样区分的理由在于，人们可以组织世界，当然也一直生活在一个被组织了的世界（带有制度的世界）中，因此对于社会交往得以可能必不可少的是稳定人们的规范性期待，这种期待关联到两种不同的对象领域：其一，应当可以期待，所有人都会组织好自己的交往圈，从而不会导致他人遭到来自外部的伤害。这种期待仅仅具有消极性的内容。其二，同样可以期待，原初的社会制度可以正常运转。这种期待具有积极性的内容。〔41〕为了稳定这两种规范性期待，人们必须分别履行消极义务和积极义务。

消极义务要求人们不要无视他人的组织圈而安排自身的活动。17 世纪的德国学者普芬道夫就曾说道，在所有的绝对义务中，首先是不侵犯他人的义务。这是最基本的义务，没有它就根本不会有人类的社会生活。〔42〕不过，不去侵犯他人的义务并不等同于不能做什么的禁止规范，因为当行为人负有义务去阻止一个侵害他人法益的因果流程时，他显然是要积极地做点什么（作为义务）。不作为犯中对危险源的管理（基于先行行为、交往安全义务等）义务就要求行为人为防止危险源的扩散而采取积极举动。这种作为义务的产生根本上还是基于行为人自由组织自身的活动，而不需要特殊的制度理由。

积极义务不仅要求人们避免自己的组织行为侵犯他人，还要求人们为保障某种状态的完好或促进他人的组织行为，即共同建设一个美好世界而做点什么。〔43〕对此，普芬道夫也曾指出，为了共同的社会性而承担的第三个普遍义务是，每个人都应尽其所能有益于他人。仅仅不伤害他人、不轻视他人是不够的。我们还必须给予（至少是分享）他人能增进相互间善意的东西。〔44〕人们之所以能够感受到法律赋予他们的自由，前提是为法律所承认的社会关系暨制度的长久存在。父母与子女的关系，婚姻关系，国家的统治关系，对安全和秩序的维护以及立法和行政等等，均属此类。只有在法律上被纳入该制度的人，才负有积极义务。〔45〕

（二）数字生产的权力纠偏与原初义务

那么，信息安全义务究竟属于消极义务还是积极义务？本文认为，基于网络服务提供者在知识和技术上的绝对优势，信息安全义务的科处是对其从事数字生产活动的权力纠偏，因而是一种原初义务，并不需要制度提供特殊的理由。

随着经营体量和经济实力的迅速扩大，网络平台的身份特征和法律形象也在转变，早已不是仅具中立性质的网络接入、存储或宿主服务的技术提供者。与这种去中立化、复杂化相伴而来的是网络平台控制力的明显增强。〔46〕如果将网络空间比喻成生态系统，谁掌控了平台，谁就是开

〔40〕 Vgl. Jakobs, Die Strafrechtliche Zurechnung von Tun und Unterlassen, 1996, S. 32 ff. 转引自何庆仁：《义务犯研究》，中国人民大学出版社 2010 年版，第 142 页。

〔41〕 Vgl. Jakobs, Strafrecht Allgemeiner Teil, 2. Aufl., 1991, § 5 Rdn. 7.

〔42〕 参见〔德〕塞缪尔·普芬道夫：《人和公民的自然法义务》，鞠成伟译，商务印书馆 2009 年版，第 79 页。

〔43〕 Vgl. Jakobs, System der strafrechtlichen Zurechnung, 2012, S. 83.

〔44〕 参见前引〔42〕，塞缪尔·普芬道夫书，第 86 页。

〔45〕 Vgl. Kindhäuser/Hilgendorf, Lehr-und Praxis Kommentar, StGB, 8. Aufl., 2020, § 13 Rdn. 38.

〔46〕 参见王华伟：《德国网络平台责任的嬗变与启示》，载《北大法律评论》第 19 卷第 1 辑，北京大学出版社 2019 年版，第 134 页。

放、共享幕后的生态系统的支配者。即便是同样作为私主体参与到网络空间的活动中，网络平台与其他私主体间也分属“枢纽节点”和“普通节点”，由此颠覆了网络空间乌托邦的幻梦。〔47〕这种不平等关系意味着支配和权力。这种权力体现在其他私主体的身上，则是面临“要么接受，要么离开”的格式选项。

在网络平台收集、处理用户的个人信息时，用户除了能在形式上对最初的环节表达同意之外，根本无权在充分知情的情况下参与数据处理的过程，而网络平台不仅免费获取了法律上的特权，且声称自己就是数字生产要素的创造者。在平台服务提供者看来，正是基于其所拥有的庞大的计算能力和尖端算法，孤立的个人信息和行为数据才被组合起来，并被充分挖掘其中潜在的巨大价值。用户个体则不可避免地沦为数字生产的资源，丧失了自我控制和主体性。〔48〕对此，各国大多以立法形式明确了知情同意制度，企图解除平台对个体权利的威胁。然而，数据处理的极度专业性与处理过程的非透明性，往往致使用户根本无法事实上做出“同意”：相比于一般产品而言，用户在收集、理解与运用隐私政策中披露的相关信息时，不仅面临时间、精力、专业、能力方面的难题，也面临系统性风险与不确定性的难题。〔49〕如果说用户对于自身信息被处理的过程中可能遭受何种风险都无法预测，那也就谈不上做出了真正的同意。同时，网络平台所拥有的这种权力也使得拥有公权力的政府难以对其进行有效约束。政府不仅无能力介入数据加工、流转等流程，亦无能力检测平台的数据安全质量，这导致网络平台对于数字公共安全也形成了威胁。〔50〕

要求网络服务提供者承担信息安全的刑法义务，正是力图对其基于技术优势所形成的权力进行纠偏。毫无疑问，这种基于“行动自由—后果责任”而生成的义务是一种基于组织管辖的原初义务。这是一种最低限度的安全保障义务，其具有以下两个特点：其一，这项义务不同于网络服务提供者对国家或个体负有的如一般经营主体的其他义务，不以任何具体主体作为履行义务的对象。其二，该义务内生于网络服务提供者成立之时，贯穿于其为网络用户提供网络服务的全过程，即便是在其退出该领域之时，也需为该义务的履行进行最为妥当的安排。〔51〕基于这种界定，私法保护路径中所提倡的信息信托理论在此就无法适用，该理论主张，网络服务提供者与用户之间应被类比于律师之于用户、医生之于病人、雇主之于雇员的关系，前者相较后者占据专业知识优势且相互间具有委托与信赖关系。网络服务提供者作为受托人必须为了委托方的利益尽到谨慎义务与忠诚义务，但同时受托人也有权利和义务进行自由裁量。〔52〕可是一方面，这种谨慎义务与忠诚义务一般仅在特定主体之间存在，因此与信息安全义务的普遍性不相符合；另一方面，在刑法中，诸如背信犯罪人就是违背基于信赖关系产生的谨慎义务与忠诚义务，但往往被界定为典

〔47〕 参见〔美〕巴拉巴西：《链接：商业、科学与生活的新思维》，沈华伟译，浙江人民出版社 2013 年版，第 85 页。

〔48〕 参见前引〔33〕，张凌寒文。

〔49〕 参见丁晓东：《个人信息保护：原理与实践》，法律出版社 2021 年版，第 98 页。

〔50〕 参见前引〔33〕，张凌寒文。

〔51〕 参见梅夏英、杨晓娜：《网络服务提供者信息安全保障义务的公共性基础》，载《烟台大学学报（社会科学版）》2014 年第 6 期。

〔52〕 参见前引〔49〕，丁晓东书，第 98－99 页；Jack M. Balkin，*Information Fiduciaries and the First Amendment*，49 University of California Davis Law Review 1183（2016）.

型的义务犯，〔53〕理由在于，这种义务并非原生于义务主体，而是基于制度的要求。

相反，对于拒不履行信息网络安全管理义务罪中的另外两项义务，即违法信息的管控义务和刑事证据的保存义务，则应当界定为基于制度管辖所负担的积极义务。尽管立法者将这三项义务全部规定在了同一个法条中，但正如有学者反思的那样，多罪一名是我国刑法罪名体系的显著特征。也即，在我国《刑法》条文当中常有一个罪名实际包含多个犯罪构成的现象。但是其指出，讨论刑法问题的基本平台只能是犯罪构成而不是罪名。〔54〕的确，上述三项义务的对象不同，保护目的指向不同，违反义务所造成的后果也不同，事实上分别对应三种不同的犯罪构成。这个结论也可以在比较法上获得论据。

以德国立法为例，基于“核心刑法—附属刑法”二元分立的立法体例，网络服务提供者的法律责任被规定在1997年的《电信服务法》中，其中第5条就已经明确采取了限缩责任的立场。受到欧盟颁布的《电子商务指令》的影响，德国联邦议会先后多次修订该法并最终于2007年通过新的《电信媒体法》，其中第7条规定了网络服务提供者责任的一般原则，即网络服务提供者对于所传输和存储之信息原则上不负有监督义务。而在第8—10条中，立法者又具体地给三种不同类型的服务提供者规定了免责条件。〔55〕这实际就是避风港原则在德国立法中被采纳的体现。与之相反，有关数据保护的法律条文则规定在《联邦数据保护法》中：该法第42条为刑事罚则，分别针对故意将个人数据向不特定多数人公布的行为、未经许可加以处理或者通过错误信息骗取的行为设置了相应的刑罚后果；第64—66条则分别规定了数据处理中的安全义务、个人数据遭损害时向联邦官员报告的义务和向受害者报告的义务。〔56〕与此类似，我国也早在2006年颁布的《信息网络传播权保护条例》中就引入了避风港原则，即力图限缩网络服务提供者对于违法信息内容的监管义务。但对于数据保护则在《网络安全法》等法律法规中详细明确了数据控制者、处理者的信息安全保障义务。

综上所述，可以认为，我国《刑法》第286条之一所规定的信息安全义务是一种消极义务，适用支配犯的归责原理。

四、信息安全义务的范围划定

在明确信息安全义务之目的与性质的前提下，对该义务保护范围的确定，一方面是厘定保护对象的范围，另一方面则是合理地划定保护边界。

（一）保护对象的厘定

在确定何种用户信息处于该保护义务的范围之内时，应当以信息共享的互惠性风险分配为这一保护目的作为构成要件解释的基点。

〔53〕背信犯罪在我国《刑法》中体现为第161条违规披露、不披露重要信息罪，以及第169条之一背信损害上市公司利益罪。参见前引〔40〕，何庆仁书，第124页。

〔54〕参见丁胜明：《以罪名为讨论平台的反思与纠正》，载《法学研究》2020年第3期。

〔55〕参见王华伟：《避风港原则的刑法教义学理论建构》，载《中外法学》2019年第6期；Hilgendorf/Valerius，Computer-und Internetstrafrecht：Ein Grundriss，2. Aufl.，2012，Rdn. 193.

〔56〕Vgl. Schlösser-Rost/Koch，in：Wolff/ Brink，BeckOnline Kommentar，Datenschutzrecht，36. Aufl.，2021，§ 42，§ 64－66.

1. 用户信息与非用户信息

在《刑法》第 286 条之一中，立法者将保护对象限定在用户信息上，在本文看来可以作以下两方面的合理解释：

第一，只有当信息的收集、处理、利用是发生在网络服务提供者和享受服务的用户之间时，两者才处于一个利益与共的共同体关系中。如前所述，数据经济潜力的发挥，必须依靠数据的自由流动、融合以及进一步的创新。因此从数字生产论的角度，社会公众失去对数据保护体系的信任，是一个非常危险的信号。〔57〕但是，只有利益与共的网络服务提供者与用户之间才谈得上相互的信任和依赖，并基于此来巩固互惠分享的关系。

第二，从支配的角度来看，网络服务提供者对于用户信息基于其组织管辖的行为而形成了保护性的支配关系，而支配的另一面则是答责（verantworten）。因此，对于那些非用户的信息，既然网络服务提供者并没有实施收集、处理、利用和流转的组织行为，也就并不负有基于保护性支配而产生的原初义务。除非，对于第三人侵犯该非用户的信息权益或滥用其信息实施违法犯罪的行为，网络服务提供者基于外部制度的要求而履行积极的管辖义务。

以意大利的“谷歌案”加以说明。2006 年 9 月 8 日，谷歌网站上的一段视频展示了一个残疾的大学生被三名同学虐待的过程（其中一个同学正在用他的手机录音，而另外十几个同学则眼睁睁地看着这一幕而无动于衷）。这个残疾学生遭受着自闭症的折磨，其听力和视力也遭到损害，完全成为心理和身体暴力的客体。这个持续 3 分钟的视频被超过 5000 人次大批量地观看。在某一特定时间点上，这个视频甚至位列最受欢迎的娱乐视频。谷歌的用户对该视频评论颇多，其中有一些认为该视频的内容不合适，甚至发邮件给谷歌要求删除该视频。从该视频被放到网上开始，它可供观看的时间已经超过了 2 个月。〔58〕根据《意大利数据保护法》的规定，四名谷歌领导层成员涉嫌非法处理敏感信息却未经过被害人的同意，而且没有得到数据保护机构的授权。法官认定谷歌领导层成员有罪的理由在于，谷歌在处理这些视频的时候，并没有采取足够谨慎的措施去避免对他人隐私的侵犯，尤其是并没有提醒视频上传者要履行消极义务（也就是不要上传这样的视频的义务）。有论者对此批评道，这样的提醒义务与告知数据主体有关数据处理范围和目的的义务并不相同，后者才是可能引发刑事制裁的义务。网络服务提供者的确应当避免侵害第三方的隐私权利，但是其承担赔偿责任的理由在于侵权法上的严格责任原则。因此，该案的审查重心应当转向：上传包含第三方健康信息的视频是否属于违法内容的传播，而谷歌作为网络服务提供者是否有义务来阻止这样的传播过程。〔59〕

2. 用户信息与个人信息

对于“致使用户信息泄露，造成严重后果”的解释，2019 年最高人民法院、最高人民检察院关于《办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》第 4 条全面沿用了 2017 年“两高”《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解

〔57〕 参见前引〔34〕，个人信息保护课题组书，第 44 页。

〔58〕 See Giovanni Sartor & Mario Viola de Azevedo Cunha, *The Italian Google-case: Privacy, Freedom of Speech and Responsibility of Providers for User-Generated Contents*, 18 International Journal of Law and Information Technology 356, 357 (2010).

〔59〕 参见前引〔58〕，Giovanni Sartor、Mario Viola de Azevedo Cunha 文，第 368 页。

释》第5条的规定，特别注意与后者保持衔接和协调，将用户信息区分为高度敏感、敏感和一般信息，数量标准则按照侵犯公民个人信息罪入罪标准的十倍来掌握。〔60〕对此，最高人民法院喻海松法官提醒道，用户信息与公民个人信息存在交叉竞合，但不能等同，除了公民个人信息之外，还应包括账号、密码、数字证书等用于确认操作权限的身份认证信息，上网轨迹、交易记录、浏览记录等网络行为信息，通信信息等，而且基于全面保护的原则，用户信息不限于不能被公开获取的信息。〔61〕但对此还需要进一步予以限定。《刑法》第286条之一不可能旨在保护所有的用户信息，其保护范围要受保护目的的制约。

首先，用户信息肯定包含了公民个人信息，但在保护范围上有必要与侵犯公民个人信息罪有所区分，因为后者主要着眼于个人信息在公法上的受保护权，而前者则更加强调促进数据的互惠分享。对于高度敏感信息和敏感信息而言，对公民个人信息的保护与对数据互惠分享的保护具有一致性，因为这两类信息毫无疑问对于公民个人具有重大利益上的关联性，一旦遭到泄露、滥用而造成严重的人身或财产损害，自然人用户整体上将会丧失对网络服务提供者的信任，必定阻碍数据的提供和共享。但对于其他个人信息或与个人有关的信息是否要纳入用户信息义务的保护范围，则需要考虑该信息之于用户个人重大利益的相关性以及该信息是否主要具有公共属性和流通属性：（1）对于没有公开且对个人的人身、财产安全至关重要的一般信息，例如网银账号和密码等，应当纳入保护范围。（2）对于没有公开但对个人的人身、财产安全并无直接影响的一般信息，例如上网轨迹、交易记录等，考虑到这些信息之于数字经济的潜在价值，不应当纳入保护范围。（3）对于已经公开的个人信息，应当按照情境原理考察其后续利用是否会显著违背信息主体的合理期待。不过原则上来说，由于第三方是否会滥用已公开的个人信息从事侵害权利人等违法犯罪活动，已经脱离了网络服务提供者的支配范围，不应当强制其履行保护义务，但是，一旦网络服务提供者已经明显认识到个人信息会被用于违背信息主体合理期待的目的，就不能被免除阻止该信息滥用过程的义务。（4）单纯的数据财产权交易，尽管并未征得用户同意，但由于交易双方对该用户数据的使用场景相同、目的也一致，不会带来额外的隐私风险，也不会打破用户的合理预期，〔62〕所以也不应当被纳入到信息安全义务的范围之中。

其次，用户信息还应当包括企业信息。在文义上，相较于个人信息而言，将用户信息解释为包括企业信息实际面临更少的障碍。〔63〕在合目的性上，对企业信息权益的保护也有助于促进数据的互惠分享：对于企业拥有的半公开或者未公开数据，如果法律提供了足够保护，避免数据的公开与获取对企业形成竞争劣势，那么企业就会选择更多地公开此类数据或信息。相反，如果法律没有对企业的商业秘密或者涉及竞争利益的数据提供足够保护，那么就会促使企业采取更为严格的保密措施或设置反爬虫等技术壁垒，〔64〕这显然不利于数据的互惠分享。当然，相较于个人信息而言，

〔60〕 参见缑杰、吴峤滨：《〈关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释〉重点难点问题解读》，载《检察日报》2019年10月27日，第3版。

〔61〕 参见喻海松：《网络犯罪二十讲》，法律出版社2018年版，第88页。

〔62〕 参见张忆然：《大数据时代“个人信息”的权利变迁与刑法保护的教义学限缩——以“数据财产权”与“信息自决权”的二分为视角》，载《政治与法律》2020年第6期。

〔63〕 参见王肃之：《论法人信息的刑法保护》，载《中国刑事法杂志》2020年第3期。

〔64〕 参见丁晓东：《论企业数据权益的法律保护——基于数据法律性质的分析》，载《法律科学（西北政法大学学报）》2020年第2期。

企业信息具有更多的公开性和公共性，因此需保护性应有所降低。对于第三方抓取开放数据的网络爬虫等行为，既然其本身不构成侵权和犯罪，那么网络服务提供者自然没有义务予以阻止；相反，对于未经授权抓取限制访问、获取数据的行为，网络服务提供者原则上负有阻止义务。〔65〕

（二）保护边界的划定

保护义务边界的确定应兼顾目的性和正当性的考量：一方面，履行保护用户信息的义务能够保障信息共享的互惠性风险分配机制；另一方面，也要防止该义务的过度科处给义务主体的基本权利带来不当侵蚀，因此，义务的科处必须具有事实上的可能性和规范上的可期待性。

1. 保护边界的目的性划定

如前所述，刑法通过保护用户信息权益来实现信息互惠共享的终极目的。问题在于，网络服务提供者拒不履行保护义务导致用户信息出现何种程度的损害后果时，才会被认为破坏了信息共享的互惠性风险分配机制呢。这里涉及两项构成要件要素的解释：一是用户信息泄露，二是造成严重后果。

用户信息泄露，一般是指信息被未经授权地访问、窃取或公开，涉及对信息的机密性和完整性的破坏。〔66〕但是，保障信息互惠共享的规范目的会将破坏信息可用性的行为同样视为破坏互惠性风险分配机制，从而应当将其纳入“泄露”的定义中来。例如个人、企业的信用记录被第三方出于报复目的而更改或者删除，导致个人、企业遭到歧视或遭受名誉和经济上的损失，其危害性绝不亚于狭义上的数据遭泄露或者丢失的后果。因此，《欧盟数据保护条例》第 4 条定义的第 12 项就明确写道，“个人数据泄露”是指个人数据在传输、存储或进行其他处理时的安全问题引发的个人数据被意外或非法破坏、丢失、更改、未经授权披露或访问。〔67〕

对于严重后果的解释，2019 年“两高”颁布的《关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》第 4 条划分了以下几类情形：一是用户信息的大量泄露，二是用户信息泄露导致人身伤害，三是用户信息泄露导致重大经济损失，四是用户信息泄露导致社会秩序的严重混乱。这反映了信息泄露后果兼具实体性和非实体性的类型：实体性后果诸如人身伤害或者经济损失容易被识别和量化，而非实体性后果包括信息泄露导致未来实体性侵害的风险显著增加、个体因此焦虑不已、社会因信息大量泄露而动荡不安。〔68〕基于信息泄露的损害特点，对于义务违反与损害结果间因果关系的要求可以做出适当缓和，从而更加周延地保护法益：其一，对于因信息泄露导致的自伤、自杀等原本应当由被害人自我答责的后果，应当纳入严重后果当中；〔69〕其二，网络服务提供者的义务违反并不一定单独导致了损害后果，对此可以采纳累积犯的法理，让网络服务提供者为自身义务违反所导致的信息泄露负责。例如在人肉搜索案件中，某个体的多类敏感信息被从不同的网站上非法获取，最终形成损害该个体名誉并造成其自杀后果的用户画像的，〔70〕网络服

〔65〕 参见杨志琼：《数据时代网络爬虫的刑法规制》，载《比较法研究》2020 年第 4 期。

〔66〕 See Clara Kim, *Granting Standing in Data Breach Cases: The Seventh Circuit Paves the Way towards a Solution to the Increasingly Pervasive Data Breach Problem*, 2 Columbia Business Law Review 544, 548 (2016).

〔67〕 参见中国信息通信研究院互联网法律研究中心、京东法律研究院编：《欧盟数据保护法规汇编》，中国法制出版社 2019 年版，第 56 页。

〔68〕 参见解正山：《数据泄露损害问题研究》，载《清华法学》2020 年第 4 期。

〔69〕 有关“缓和的结果归属”的学理论述，参见张明楷：《论缓和的结果归属》，载《中国法学》2019 年第 3 期。

〔70〕 Vgl. Kubiciel/Großmann, Doxing als Testfall für das Datenschutzstrafrecht, NJW 2019, 1050 ff.

务提供者应当为自己违反规范的累积危险行为个别性地承担刑事责任。〔71〕

为防止以上损害后果的发生，理应在法律和行政法规的框架之内，从技术性措施和管理性措施两个面向全面构建网络服务提供者的信息安全义务。根据《网络安全法》第42条、《中华人民共和国民法典》第1038条以及《中华人民共和国个人信息保护法》第51条的规定，信息处理者应当对个人信息进行分类管理并采取加密、去识别化等技术措施，防止未经授权的访问、泄露、篡改、丢失。在实际的信息安全等级保护制度中，不同分级配套的管理规范和技术标准构成了安全保护义务的主要内容，而保护等级则由两个定级要素决定：保护对象受到破坏时侵害的客体和对客体造成侵害的程度。只要根据保护等级要求落实了所有项的要求，就被认为履行了安全保护义务。但是，仅仅以侵害后果为着眼点采取保护措施，忽略了动态变化的侵害频率，而且，静态式的合规措施并未考量网络安全攻防技术的进步，仅仅达到安全底线也并不意味着保护了用户安全的实质需求。〔72〕对此，应当更加重视以管理为基础的规制以避免刻舟求剑式的技术措施导致的漏洞，具体来说：（1）在事前的风险预防阶段，网络服务提供者应当以风险评估机制的建立为中心，制定对用户信息的保护策略，按照最先进的保护标准定期对风险变化进行评估并适时调整保护策略。在此过程中，尤其要考虑到与第三方主体的交往过程中是否履行了必要的谨慎义务，以避免黑客等侵入者借助第三方通道来达到非法获取用户信息的目的。（2）在事后的实害阻止阶段，网络服务提供者应当及时采取补救措施防止损害的发生或扩大，同时应当履行法定的对监管部门和权利主体的通知义务，以便后者及时采取补救或自救措施。除非其所采取的措施能够确保用户信息即便泄露也不会导致损害后果。（3）在全过程的风险防控中，互联网公司领导层需要制定组织计划，将数字生产所应承担的危险识别、观察及消除的义务分配给数据合规官以及公司执行层成员。〔73〕较为清晰地划分各成员间的负责范围，有助于反制现实中责任意识稀薄化的现象。领导层成员还负有义务对组织计划的可靠性进行持续监管，因此其应当谨慎选任有资质的监管人员，持续向成员充分讲解与其履职相关的法律法规，并为担负相应职责的成员提供足够的配备。〔74〕

2. 保护边界的正当性基础

按照支配犯的法理，只有创设风险的行为人才负有义务消除风险。同时，为了控制义务的目的性追求所内含的危险，有必要从事实和规范两个层面对其加以限定：一方面，义务的履行必须在事实上具有可能性，也就是说采取保护措施能够有效避免损害后果的发生；另一方面，义务的履行在规范上应当具有可期待性，行为规范的设立应使得相关主体间的利益取得相对平衡。

首先，只有当信息泄露风险是由网络服务提供者共同创设时，其才有义务消除风险。如果该风险是由侵害方和用户通过互动过程共同创设的，那么只要网络服务提供者在技术和管理措施上没有失职行为，就不应当为损害后果的发生承担责任。例如，在著名的“机票款项诈骗案”中，

〔71〕 参见张志钢：《论累积犯的法理——以污染环境罪为中心》，载《环球法律评论》2017年第2期。

〔72〕 参见洪延青：《“以管理为基础的规制”——对网络运营者安全保护义务的重构》，载《环球法律评论》2016年第4期。

〔73〕 Vgl. Dannecker/Dannecker, Fahrlässigkeit in formalen Organisationen, in: Knut Amelung (Hrsg.), Individuelle Verantwortung und Beteiligungsverhältnisse bei Straftaten in bürokratischen Organisationen des Staates, der Wirtschaft und der Gesellschaft, 2000, S. 217.

〔74〕 Vgl. Eidam, Unternehmen und Strafe, 5. Aufl., 2018, § 7 Rdn. 107 ff.

被害人通过某订票网提供的电话预订机票，被客服人员要求用网银汇款。被害人汇款后虽查询扣款成功，但对方称钱未到账，还需要通过 ATM 联网操作使付款生效。被害人按照其引导在 ATM 上输入所谓 18356 的激活码（实际输入到转账数额一栏），之后相应数额随即被转入诈骗人的账户。〔75〕 在本案中，信息泄露或数据丢失的风险是由诈骗行为人而不是网络服务提供者创设的，因为没有证据表明后者在系统安全上存在漏洞。而且，银行系统本就是为了帮助用户实现自主利益而设立，既然用户基于“自愿”主动向对方提供自己银行账户的信息，那么银行系统的运营者就不可能反过来审查该交易的真实性和合法性。

其次，只有当网络服务提供者有能力履行义务以避免结果的发生时，才应当为损害结果的发生负责。遵守规范的前提是拥有遵守规范的能力，不能超越规范接收者的实际能力对其设定义务。因为作为义务的规范只是告诉行为人应当采取何种方式避免结果的发生，但它没有表明行为人在何种程度上受到义务的约束，也就是说，在何种程度上，行为人必须为了实施合义务的行为而将他的能力维持在必要的水平之上。对于这一问题的回答属于刑法中制裁规范的任务，也即，在何种条件下，要将刑罚施加于一个违反规范的行为。〔76〕 某一行为是否合乎规范，是一个应从事后予以回答的逻辑的推演问题。但只有当行为人本可以实施与当为命令相符且能够阻止结果发生的合法替代行为时，他所实施的违反规范的行为才能被作为义务违反归责于他。因此，只有在具备足够的行为能力的范围内，一个规范接收者才受到规范的约束。〔77〕 所以，必须在具体情境下检验作为义务的履行是否能够有效避免损害结果的发生。事前风险预防义务的履行，如果能够在很大程度上避免损害后果的发生，就应当认为义务具备履行可能性。事后实害阻止义务尤其是通知义务的履行，由于涉及通知对象之自由决定的介入，在判断合义务的替代行为能否避免结果发生时，应当采取规范论的思维，假设监管人员等负有处置义务的主体会按照义务的要求履行监管职责，〔78〕 在此基础上来判断通知义务对于阻止结果发生的实效。此外，只有当义务的设置充分考虑了义务主体的社会角色及其相应的利益需求，使得义务主体为履行该义务不必过度牺牲行动自由时，该义务的履行才具有规范上的可期待性。对于网络服务提供者而言，保护义务的承担应当以合乎比例的经济利益的损失为前提，〔79〕 只能要求其将信息安全风险降低到一个相对可接受的范围之内，而不是绝对地消除风险。当其保护措施足以实现这一目的时，不应当要求其承担更高的注意义务。

五、结　论

网络信息犯罪的治理绝不只是在封闭的法律体系内部进行，而必须是在法律系统与其他社会

〔75〕 参见秦新承：《认定诈骗罪无需“处分意识”——以利用新型支付方式实施的诈骗案为例》，载《法学》2012 年第 3 期。

〔76〕 Vgl. Kindhäuser, Erlaubtes Risiko und Sorgfaltswidrigkeit, GA 1994, S. 200.

〔77〕 Vgl. Kindhäuser, Gefährdung als Straftat: rechtstheoretische Untersuchungen zur Dogmatik der abstrakten und konkreten Gefährdungsdelikte, 1989, S. 50.

〔78〕 Vgl. Puppe, Brauchen wir eine Risikoerhöhungstheorie? FS-Roxin, 2001, S. 287；徐凌波：《义务违反的竞合与结果可避免性》，载《南京大学学报（哲学·人文科学·社会科学）》2018 年第 2 期；喻浩东：《不作为因果关系判断中的自由意志与规范假设》，载《政治与法律》2022 年第 4 期。

〔79〕 Vgl. Georg Freund, Strafrecht Allgemeiner Teil, 2. Aufl., 2009, § 1 Rdn. 20.

子系统的有效沟通中进行。信息安全守门人刑法义务的构建，首先应当关注数字经济系统的保护需求，在此基础上确定刑法规范的保护目的与规制需要，进而确定该义务的具体内容。通过以上体系化的论述，本文得出以下结论：

其一，信息安全义务的目的既不是保障用户信息专有权，也不是维护信息网络安全管理秩序，而是保障信息共享的互惠性风险分配机制。

其二，信息安全义务的性质是支配犯的消极义务，而不是义务犯的积极义务。该义务的科处是对网络服务提供者的数字生产权力的纠偏。

其三，信息安全义务的范围基于该义务的保护目的和义务性质得以实质地厘定。对该义务的保护对象和保护范围的确定，既应当促成规范目的的实现，也应当为其提供正当性的基础，从而对目的追求所内含的危险进行必要控制。

Abstract: The addition of the crime of refusing to fulfill the obligations of information network security management provides a basis for the criminal law obligations of information security gatekeepers in cyberspace. In view of the dilemma encountered in judicial practice, it is necessary to carry out a systematic interpretation of the purpose, nature and scope of information security obligations in doctrine. In terms of purpose construction, both the exclusive right to user information and the maintenance of information network security management order have insurmountable defects. A systematic coupling view of legal interests should be advocated, defining the purpose of the obligation as a reciprocal risk allocation mechanism to guarantee information sharing, in order to achieve effective communication between the legal system and the digital economy system. In terms of nature definition, the obligatory offense theory misunderstands the basis for the creation of positive obligations, and improperly confuses dominant offenses with acting offenses, and obligatory offenses with inaction offenses. The essence of information security obligation is the correction of the digital production power of network service providers, so it should be classified as a negative obligation based on organizational jurisdiction rather than a positive obligation based on institutional jurisdiction. Based on the clarification of the purpose of protection and the nature of the obligation, the scope of protection of the obligation should be determined in order to achieve the normative purpose of guaranteeing the reciprocal risk allocation mechanism of information sharing, and also to justify the control of the dangers inherent in it.

Key Words: internet service provider, information security gatekeeper, systematic coupling view of legal interests, crime of refusing to fulfill the information security management obligations

（责任编辑：简　爱　赵建蕊）

财经法学 No. 1，2022
pp. 45 - 61

论侵犯公民个人信息罪的司法适用误区及其匡正

郑朝旭*

内容提要：在目前的司法实践中，对公民个人信息的认定同时存在着内涵不清与外延不当扩张的缺陷，其根源在于未能充分认识到识别性标准与个人信息权对于判断公民个人信息所具有的重要作用。理论研究一方面对识别性的识别限度未予以足够的重视，另一方面则缺失对个人信息权之权利属性与构造的深入挖掘，以致无法为实务提供理想的操作方案与背书理由。应当在限定识别深度与明确个人信息权之权利内涵的基础上，采取由识别性至个人信息权的双重检视路径，将侵犯公民个人信息罪的适用范围限制在因非法出售、提供、获取具备识别性的信息而侵害公民个人信息权的场合。

关键词：公民个人信息　识别性　个人信息权　双重检视

一、侵犯公民个人信息罪的适用误区：识别限度与法益的缺位

因个人信息被不当获取、滥用、泄露所引发的侵害公民人身、财产安全的案件，已成为困扰我国社会稳定、公民安全的严峻问题，且呈现愈演愈烈的态势。〔1〕《中华人民共和国个人信息保护法》（以下简称《个人信息保护法》）的颁行，使得我国在个人信息保护的制度构建上开始告别分散立法模式，〔2〕保护个人信息的规范性文件之间各行其是甚至相互矛盾的态势在一定程度上得到了扭转。但《个人信息保护法》所界定的“个人信息”和规定的信息主体权利，与《中华人

* 郑朝旭，中国人民大学刑事法律科学研究中心博士研究生。

〔1〕 本文以“刑事案由”为方向、以“侵犯公民个人信息罪”为案由，在中国裁判文书网共搜得 9438 份判决书。其中，2015 年计 24 份判决书，2016 年计 398 份判决书，2017 年计 1376 份判决书，2018 年计 2350 份判决书，2019 年计 2748 份判决书，2020 年计 2373 份判决书，而 2021 年，截止到 3 月 18 日，已公布了 169 份判决书。参见 https://wenshu.court.gov.cn/website/wenshu/181217BMTKHNT2W0/index.html?pageId = e372b9fd7664d99785f7484ced8ec8e8&s8 = 02，最后访问时间：2021 年 3 月 18 日。

〔2〕 参见齐爱民：《拯救信息社会中的人格：个人信息保护法总论》，北京大学出版社 2009 年版，第 177 - 184 页。

民共和国刑法》（以下简称《刑法》）第 253 条之一侵犯公民个人信息罪中的“公民个人信息”及该罪法益内涵，存在着语境和规范目的上的差异，若奉行“拿来主义”对于改善当前的司法现状可能并无裨益。在当前的司法实践中，从认定公民个人信息出发，论证涉案行为构成侵犯公民个人信息罪，依然存在着方法论与基本立场上的缺陷。

案例一：马某、刘某（均另案处理）雇佣被告人胡某、王某通过驾驶汽车与网络实时定位等方式对某机关领导所配专用公车进行跟踪，胡、王二人将目标车辆行驶的路线、停车地点进行记录，并将相关信息交给马某、刘某。法院经审理认为，胡某、王某构成侵犯公民个人信息罪。〔3〕

案例二：被告人张某等为实施网络诈骗活动，通过在网上获取的企业信息及法定代表人通讯录，假冒公司负责人要求财务人员将钱款汇入到其指定的银行账户。对检方所控告之侵犯公民个人信息罪，辩护人辩称，该案中的公司信息属于公开信息，不应被认定为公民个人信息。但法院以涉案信息可以被用来识别特定自然人的身份，足以威胁他人人身、财产安全为由，认定张某等构成本罪。〔4〕

从上述代表性案例的具体论证过程、判决理由来看，当前的判决存在着以下不足之处：其一，虽然“识别性”已成为判断公民个人信息的标准，但受制于对“识别性”概念及识别深度缺乏具体的阐释，法院在判决书中并未就涉案信息是否具备识别性或其识别深度进行论证。例如，案例一的核心争议即在于是否可依据行踪轨迹识别出被害人，但法院并未从正面给出行踪轨迹属于公民个人信息的理由，而是以行踪轨迹具有个人专属性、能够反映公民的某些个人特征、关乎公民生活安宁等非法收集信息所可能导致的危害后果这一角度来反证行踪轨迹属于公民个人信息。〔5〕其二，公开信息处于任何人皆可获取的状态，并不具有隐私性，收集、编辑公开信息的行为并不违法，〔6〕但对于后续的利用行为是否成立侵犯公民个人信息罪，以案例二为代表的判决既没有从构成要件的角度论证这些利用行为符合该罪的实行行为之特征，也没有说明这样的行为侵犯了本罪的什么法益，而是以该行为对他人的人身、财产安全具有危害性为由，进而认定为本罪。如此模糊处理争议点、回避问题的操作使得判决结论在教义学上遭遇巨大的质疑。其三，上述判决均存在的问题是，没有将公民个人信息的识别性特征与本罪的法益结合起来，进而导致在判决中要么以相关信息具备识别性从而顺理成章地侵犯了本罪的法益为由，认定构成犯罪，要么以被告人利用信息的行为已危害到被害人的人身、财产安全、必定侵害了本罪的法益为由，证明涉案信息具备识别性。但是，识别性本身只是对公民个人信息的判断，并不能理所当然地代替对本罪法益的判断；同样，本罪法益可以涵盖对犯罪对象、行为方式的解释，是否侵犯本罪法益，需要在明确法益内涵的基础上，检验涉案信息是否属于公民个人信息。一言以蔽之，识别性

〔3〕 参见最高人民法院刑事审判第一、二、三、四、五庭主办：《刑事审判参考》2014 年第 4 集（总第 99 集），法律出版社 2015 年版，第 53－56 页。

〔4〕 参见广西壮族自治区宾阳县人民法院（2018）桂 0126 刑初 486 号刑事判决书。

〔5〕 参见前引〔3〕，最高人民法院刑事审判第一、二、三、四、五庭主办书，第 55－56 页。

〔6〕 根据《个人信息保护法》第 13 条第 2 款的规定，原则上，处理个人信息需要取得信息主体的同意；但有第 13 条第 1 款第 2 项至第 7 项所列之情形（基本属于为履行法定职责、承担法定义务、维护公共利益以及个人自我决定）的，不需要取得信息主体的同意。其中，只是收集或者编辑已合法公开的个人信息属于第 13 条第 1 款第 6 项所列之情形。另外，根据该法第 27 条，单纯的收集、编辑行为也不构成对信息主体的权益有重大影响的行为，不需要取得信息主体的同意。即便在该法颁行之前，单纯收集、编辑自行公开的个人信息或者依法公开的个人信息的行为，既没有违背信息拥有主体的意愿，也没有利用这样的信息实施其他违法行为的，不构成对他人信息权利的侵犯。

与本罪法益之间存在着双向的互动关系。这是目前司法实践在论证中最为薄弱的环节，也是理论研究亟待深化的方向。

二、公民个人信息的法益：个人信息权的确证

（一）法益之争与评析

总体来说，关于该罪法益的讨论可区分为非人格权论的立场与人格权论的立场，前者以公民个人信息所蕴含的经济价值或社会秩序为基础，主张从财产利益、公共安全的视角解读本罪的法益，后者则以公民个人信息是公民人格权的延伸、侵犯公民个人信息的行为是对人格利益的妨害为总论点。不过，基于非人格权论立场所展开的财产权说、〔7〕公共信息安全说、〔8〕新型民事权利说〔9〕等，由于存在着与保护个人信息安全、刑法平等保护的价值理念背道而驰、〔10〕贬损公民个体的信息安全价值、以经验事实代替规范判断、〔11〕与侵犯公民个人信息罪的体系位置相冲突等缺陷，已渐渐退出了该罪法益之争的视野。因此，立足人格权论的立场形成了隐私权说、信息权说的论争。

1. 隐私权说容易导致本罪适用混乱

该说的特色在于，对公民个人信息的保护最终指向或涵盖对隐私权的保护。不过，在是否完全以隐私权建构本罪法益这一问题上，有的观点认为，本罪法益是公民的隐私权，只有体现个人隐私权的那一部分个人信息才属于刑法保护的对象，〔12〕且将本罪视为保护隐私权的条款也有助于填补《刑法》缺失公民个人隐私保护条款的漏洞〔13〕。另有观点则在承认本罪的法益是公民的信息权益的同时，又认为隐私权属于与信息权相并列的权益，进而二者共同构成本罪的法益，其代表性的见解认为，本罪的法益除了公民个人的信息权外，还包括个人隐私不受侵犯的权利。〔14〕

〔7〕 参见刘德良：《论个人信息的财产权保护》，载《法学研究》2007 年第 3 期；汤擎：《试论个人数据与相关的法律关系》，载《华东政法学院学报》2005 年第 5 期。

〔8〕 参见王肃之：《被害人教义学核心原则的发展——基于侵犯公民个人信息罪的反思》，载《政治与法律》2017 年第 10 期；张勇：《APP 个人信息的刑法保护：以知情同意为视角》，载《法学》2020 年第 8 期。

〔9〕 参见刘艳红：《民法编纂背景下侵犯公民个人信息罪的保护法益：信息自决权——以刑民一体化及〈民法总则〉第 111 条为视角》，载《浙江工商大学学报》2019 年第 6 期。

〔10〕 参见王利明：《论个人信息权在人格权法中的地位》，载《苏州大学学报（哲学社会科学版）》2012 年第 6 期。

〔11〕 虽然《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（以下简称《解释》）第 5 条第 1 款对本罪的成立提出了信息数量的要求，但这是司法定量的惯性使然，且按照司法解释的规定，侵犯一位公民的信息安全达到入罪数量时，依然构成犯罪，这也是公共信息安全说难以解释的。

〔12〕 参见蔡军：《侵犯个人信息犯罪立法的理性分析——兼论对该罪立法的反思与展望》，载《现代法学》2010 年第 4 期。

〔13〕 参见王昭武、肖凯：《侵犯公民个人信息犯罪认定中的若干问题》，载《法学》2009 年第 12 期。

〔14〕 参见周光权：《刑法各论》，中国人民大学出版社 2016 年版，第 71 页（需要说明的是，周光权教授原先认为，侵犯公民个人信息罪在保护公民个人信息权之外，还保护个人隐私。但其在 2021 年版的《刑法各论》中，一方面将本罪的法益总括为“公民的个人信息自由决定权”，其中既保护公民对个人信息享有自由使用的权利，也保护个人隐私，这基本沿袭了其之前的立场；但另一方面，其还认为，本罪法益具有多重性，除了公民个人的信息自决权外，与个人信息相关联的（狭义的）社会管理秩序也是本罪的保护法益。这使得本罪的法益兼具非人格权论与人格权论的色彩，虽然有积极性、全面性地预防与惩治因个人信息侵权问题所引发的各类犯罪的现实背景与需求，但就观点本身而言，似乎使得本罪法益出现了超出其保护公民人格权利之内容的些许瑕疵，导致本罪法益“不堪重负”。参见周光权：《刑法各论》，中国人民大学出版社 2021 年版，第 78 页）；黎宏：《刑法学各论》，法律出版社 2016 年版，第 269 页；张明楷：《刑法学》（下），法律出版社 2016 年版，第 921 页。

首先，所谓个人信息，是指可以识别公民身份的信息，而非泛指一切与个人有关的信息，如此一来，所有可以识别个人身份的隐私当被涵盖在个人信息范围之内，将不具有识别性的隐私也纳入本罪的规制范围，将使得本罪的适用范围无限扩张。其次，即便认为《个人信息保护法》第 4 条第 1 款规定的是与公民个人“有关”的信息，且《个人信息保护法》第 28 条将宗教信仰、行踪轨迹等更应被纳入个人隐私的信息作为个人信息甚至是敏感个人信息而予以特别保护，也难以认为本罪的法益就是隐私权。这是因为，对于涉及侵犯个人隐私的行为，完全可以通过保护个人隐私的民事法律来规制，而且对于宗教信仰、行踪轨迹这类不以身份信息为背书的信息，通常都是在已知晓特定个人的情况下才能获取的信息，这就脱离了识别这一方法的范畴，将其纳入敏感个人信息之中，只不过是出于这类信息被非法获取或利用后可能产生严重后果的考虑而非其具有识别性。这样的外延扩张纵使在《个人信息保护法》中有其最大化保护公民个人信息的必要性，但在以刑罚为惩治手段的《刑法》中，若也通过严重后果来反向扩张个人信息的外延，有类推之嫌。况且根据《个人信息保护法》第 73 条第 4 项的规定，匿名化后的信息是无法识别个人身份且不能复原的信息，那么具备识别性的信息才可被匿名化，而对于一些原本就不具有识别性的信息，将其纳入个人信息之中，稍显矛盾。再次，信息主体积极参与各种活动所导致的信息社会化也使得该说无法涵盖侵害此类信息的行为，即便是不属于隐私的信息，若没有经过信息主体的同意，而非法获取、泄露、使用该信息，则依然成立本罪。最后，个人信息与个人隐私是两个不同的法律概念，前者关注的是对信息的利用，后者关注的是与人格尊严密切相关的私生活秘密是否遭到泄露，由此导致对二者的保护、利用、责任承担均会存在显著的差别，〔15〕故不宜将二者混同。

2. 信息权益说存在方法论与前提证立不足的缺陷

该说认为，随着公民个人信息概念的急剧扩张，其不仅具有人格权的性质，还兼具财产权、其他信息相关权利等内容，因此，若将公民个人信息的权利属性局限于纯粹的人格权、财产权或隐私权等权利内，既不利于充分保护公民个人信息之安全，也不符合法律、司法解释对公民个人信息范围的界定。此外，就回应公民个人信息的保护需求与实践而言，将公民个人信息提升至权利保护的高度，也有其必要性。〔16〕

该说的缺陷是：其一，在信息权益的证成方面存在方法论上的不足，刑法作为保障法，其本身并不能也不应创设某种权利与利益，即不能用法益本身来论证法益，否则即是循环论证；其二，虽然在侵犯公民个人信息安全的场合可能伴随着对公民人身安全、财产的侵害，但这是犯罪客观现象，现有的理论与法条都足以对其做到充分评价，且《刑法》将侵犯公民个人信息罪置于侵犯公民人身权利、民主权利罪之中，着眼于对公民人格权利的保护，但该说所确立的信息权益不同于纯粹的人格权与财产权，而是介于二者之间，以至要对侵犯公民个人信息罪进行重新定位，将部分行为解读为“预备行为实行化”，〔17〕这既与《刑法》存在抵牾，也存在权利属性暧昧

〔15〕 参见韩旭至：《个人信息与个人隐私的区分》，载《网络法律评论》2016 年第 2 期。
〔16〕 参见刘艳红：《侵犯公民个人信息罪法益：个人法益及新型权利之确证》，载《中国刑事法杂志》2019 年第 5 期。
〔17〕 参见于志刚：《“公民个人信息”的权利属性与刑法保护思路》，载《浙江社会科学》2017 年第 10 期

不清的嫌疑；其三，公民对个人信息享有的究竟是民事权利抑或仅仅是受保护的民事利益，这取决于对《中华人民共和国民法典》（以下简称《民法典》）第111条〔18〕的解释，民法学界也因此存在权利说〔19〕与利益说〔20〕之争，在缺乏对观点之争予以充分讨论的前提下径直得出信息权益的结论，缺失了论证的过程与充分的理由；其四，虽然《民法典》将公民个人信息置于第五章“民事权利”中，但并未将其明确规定为权利，且《民法典》是在具体人格权的规定（第110条〔21〕）之后，身份权、财产权（第112条至第132条）之前，对公民个人信息作出规定。因此，从体系解释的角度而言，也有学者认为立法者更倾向于将其作为一项需要保护的人格利益，这也可以从《民法典》第111条的后半句得到印证，因为其是从其他民事主体对自然人的个人信息负有保护义务的角度所作出的规定。〔22〕

综上所述，以人格权为核心主张本罪法益系隐私权或信息权益的各种学说的症结在于，要么因未厘清个人信息与个人隐私之间的关系，从而陷入看似全面保护个人信息、个人隐私，却实际上混淆了保护对象与法益之区分的局面，要么没能在区分一般人格权与具体人格权的基础上论证信息权益为何是一项新型的具体人格权，以致在说理上有所欠缺。

（二）本文观点：具体人格权视角下的个人信息权

1. 具体人格权视角的优势

首先，公民的个人信息不仅是受保护的民事利益，还具备民事权利的内涵，有着显著的民事权利属性。这具体体现在，第一，姓名、性别、年龄、民族、婚姻、住址、个人信用等个人信息都以自然人的真实存在为前提，且大多通过自然人的社会活动产生，每个自然人都是自身信息的主体，可禁止、排除他人对这些个人信息的非法收集、利用、泄露等行为，归结起来便是处于对自身信息的绝对控制地位，“对这些个人信息的控制，本身体现的就是一种私益，这是个人信息能够成为民事权益的根本原因”〔23〕。第二，个人信息不只有受到侵害后需要保护的一面，还存在着通过积极利用个人信息创造经济价值的一面，因而在利用的过程中，权利人当然可以就利用的限度、方式、价值分配、损害赔偿等提出自己的要求，这也是为何理论上将其纳入财产权保护的原因所在。事实上，在当前社会中对个人信息的利用已经是无可避免且必不可少的，正因如此，才更应在权利观念的基础上，追求对其的合理使用，如匿名化处理、中性使用公开信息、基于公

〔18〕《民法典》第111条规定：“自然人的个人信息受法律保护。任何组织或者个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。”

〔19〕参见杨立新：《个人信息：法益抑或民事权利——对〈民法总则〉第111条规定的“个人信息”之解读》，载《法学论坛》2018年第1期；王成：《个人信息民法保护的模式选择》，载《中国社会科学》2019年第6期。

〔20〕参见王利明主编：《中华人民共和国民法总则详解》（上），中国法制出版社2017年版，第465页；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。不过，也有观点认为，无论是权利说还是利益说，都是试图以传统的民事权利话语体系来界定个人信息的保护，难以避免地导致了各种矛盾，而将个人信息控制权认定为一项新型的公法权利或许更加合理。参见周汉华：《个人信息保护的法律定位》，载《法商研究》2020年第3期。

〔21〕《民法典》第110条规定：“自然人享有生命权、身体权、健康权、姓名权、肖像权、名誉权、荣誉权、隐私权、婚姻自主权等权利。法人、非法人组织享有名称权、名誉权和荣誉权。”

〔22〕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；程啸：《论我国民法典中个人信息权益的性质》，载《政治与法律》2020年第8期。

〔23〕前引〔10〕，王利明文，第69页。

共利益的有限使用等。〔24〕此外，相比于民事利益的设定，作为民事权利的个人信息权还存在着抗衡公权力不当利用、给受害人提供充分保护、为其他法律保护奠定基础、与其他保护机制相衔接和补充等优势。〔25〕

其次，将公民个人信息的法益定位于民事权利，存在着一般人格权与具体人格权两条路径。虽然站在一般人格权的层面建构个人信息权有高屋建瓴之效，但其本身内容的模糊性并不利于对本罪构成要件的解释。一般人格权是相对于具体人格权而言的，具体而言，一般人格权以人格尊严、人格平等、人格自由为内容，是具有高度概括性和权利集合性特点的权利。〔26〕具体人格权则以特定的人格利益为内容，具有明确的构成要件与救济手段。相较而言，一般人格权虽然以保护人的自由发展为核心价值理念，将人格尊严、人格平等、人格自由作为框架，能结合案件的实际情况，通过解释予以适用，但由于欠缺明确的构成要件，与其认为它是一项权利，不如说它提供了对具体人格权之创造、解释的价值指引功能。如果将公民个人信息视为一项一般人格权，极易导致在个案裁判中过于依赖裁判者个人的价值取舍与利益衡量，再考虑到在收集、利用公民个人信息的场合常存在着诸如集体法益与个人法益、人格自由与社会防卫等冲突，因此必然使得这样的价值判断与利益衡量不具有客观性与合理性。〔27〕

最后，以一般人格权作为公民个人信息的权利本质，即便肯定其对于保护人格尊严、人格平等、人格自由方面具有相比于具体人格权更为宽广的适用范围，但这正是该种观点最为致命之处。具体而言，第一，只有在具体人格权缺位或无法涵盖相应客体的场合，才考虑以一般人格权的价值理念来弥补具体人格权的有限性。然而，个人信息权以识别性信息为内容，由公民自身控制，禁止任何对其的非法收集、利用、泄露，否则需承担相应的法律责任，就此而言，个人信息权具备明确的构成要件与救济手段，不存在适用一般人格权填补漏洞的空间。第二，且不论前述的财产权、隐私权、信息权益等观点周延与否，就保护的路径而言，论者们均是在财产权、人格权的角度展开己见，这也从侧面说明，现有的民事权利类型已足以涵盖对公民个人信息的保护，只不过存在着因公民个人信息内容繁杂、价值多样而导致的保护取向偏差。第三，公民个人信息这一概念的最大问题在于，缺失对“识别性”的限定导致其外延不断扩张，若以同样抽象的一般人格权作为权利本质诠释个人信息权，其结果便是公民个人信息变得更加抽象与不确定，对公民个人信息的认定会陷入“公说公有理，婆说婆有理”的困境。

2. 个人信息权的法益构造：信息控制权与信息利用权

作为一项具体人格权，根据《个人信息保护法》第 44 条的规定，个人信息权由知情权与控制权构成，第 45 条至第 50 条对控制权的具体权能予以了展开，例如查阅、复制、更正、补充、删除等。就《刑法》第 253 条之一而言，其规制的是非法出售、提供及获取公民个人信息的行

〔24〕 参见刘艳红：《公共空间运用大规模监控的法理逻辑及限度——基于个人信息有序共享之视角》，载《法学论坛》2020 年第 2 期。

〔25〕 参见前引〔10〕，王利明文。

〔26〕 参见王利明：《人格权法研究》，中国人民大学出版社 2012 年版，第 147 页。

〔27〕 参见杨惟钦：《个人信息权之私权属性与内涵思辨——以实现个人信息权益的合理保护为视角》，载《晋阳学刊》2019 年第 2 期。

为，因此，本文认为，应当结合该罪的实行行为来理解个人信息权的法益构造。具体而言，包括以下两个方面：

其一，信息控制权，即权利主体对自我信息的控制与排除他人非法获取的权利。虽然公民个人信息不是以有体物的形式存在，无法对其进行物理上的占有与支配，但这并不意味着信息主体无法对其进行控制，相反，信息主体的地位使其实现了对公民个人信息的法律控制。这种控制意味着，除了《个人信息保护法》第13条第1款所规定的例外情形，信息主体的同意或授权是其他组织或个人收集与利用个人信息的必要前提。况且，依据公共利益所收集的个人信息也仅限于在特定的方面或特定的目的下使用，而不得随意向任何人透露甚至公开。当然，针对信息主体的同意究竟在多大程度能发挥其作为合法化事由的效力及是否有必要维持此种知情同意的架构，存在着不少质疑。例如，有观点认为，以同意作为个人信息的保护架构已过时且无益，理由在于许多人并不会认真阅读关于个人信息的隐私声明，或为使用产品、服务而被迫同意，抑或对个人信息被收集的事实并不知情，难以及时行使权利进行救济；〔28〕还有观点认为，同意原则作为犯罪阻却事由存在着难以求知真实意愿及不确定等缺陷，进而主张在涉及公共利益时以比例原则作为收集、利用公民个人信息的正当性基础〔29〕。本文认为，公民个人信息可被视为公民人格尊严的表征之一，以同意原则作为收集、利用个人信息的合法化事由是对公民人格尊严、自由的尊重和保障。尽管在实践中出现基于防控疫情或社会安定的需要，而未能充分征得公民同意即收集其个人信息的情况，但这不是同意原则本身所引发的缺陷，而是法律体系完善与执法文明的问题。换言之，“法律不能以个人信息用户行使权利困难为由，虚置或抛弃个人信息知情同意的基本原则”〔30〕。因此，解决问题的理想方案并不是否定或者弱化同意作为个人信息保护的合法性与正当性基础，而是应当通过构建更为精细、清晰的同意规则来协调个人信息保护与利用上的冲突，例如从同意的形式到实质加强对同意的审查。〔31〕而且在《个人信息保护法》中，信息主体的同意得到了进一步的强调，例如该法第15条、第16条即明确了信息主体可拒绝或撤回其所作出的同意，第17条也要求信息处理者必须以显著方式、清晰易懂的语言真实、准确、完整地向信息主体告知信息处理事项，且针对当前许多并不需要以个人信息作为使用该产品或服务的条件的应用程序，其中的“不同意隐私条款即不可使用本产品或服务”条款违反了该法第16条的规定。至于以比例原则作为收集、使用公民个人信息的正当化根据，这在《个人信息保护法》中也得到了确证，但其本身是利益衡量的产物，且也仅适用于维护公共利益的场合，并不是降低同意作为处理个人信息的终极原则之地位的理由。

其二，信息利用权，即信息主体决定是否使用个人信息及如何使用的权利。应当说，从《个人信息保护法》的控制权角度而言，其包含了如何利用个人信息的内涵，只不过出于具体化法益

〔28〕 参见范为：《大数据时代个人信息保护的路径重构》，载《环球法律评论》2016年第5期。

〔29〕 参见江海洋：《论疫情背景下个人信息保护——以比例原则为视角》，载《中国政法大学学报》2020年第4期。

〔30〕 叶名怡：《论个人信息权的基本范畴》，载《清华法学》2018年第5期，第154页。

〔31〕 参见陆青：《个人信息保护中“同意”规则的规范构造》，载《武汉大学学报（哲学社会科学版）》2019年第5期。

的考虑，本文将其中的利用权能予以单独、特别地解释。随着信息时代的发展，公民个人信息已经成为一项具有丰富价值的社会资源，由此催生出基于各种目的的利用方式。根据《个人信息保护法》第 1 条的规定，制定该法的目的之一即在于“促进个人信息合理利用”，同时该法第 10 条禁止的是非法处理个人信息的行为，而依法利用个人信息的行为受法律保护。既然信息利用权是公民个人所享有的人格权，那么对公民个人信息的利用必须由信息主体决定，这是民事权利的应有之义。公民个人无疑可以在遵守法律的前提下，对本人信息予以利用，包括公开信息、编辑个人信息等；信息主体也可以授权或同意他人基于合法目的将其个人信息运用于商业、公益等活动，例如，实践中常见的通信运营商根据用户协议收集用户个人信息，并将之用于改善用户体验等情形。因此，由公民的信息利用权所引申出来的当然结论是，即便公民自行决定公开个人信息，或同意、授权其他组织、个人获取其个人信息，甚至政府基于公共利益公开公民个人信息，虽然取得公民个人信息的行为并不违法，但若未就利用公民个人信息取得相关权利主体的同意，依然属于侵权（犯罪）行为。例如，《个人信息保护法》第 24 条禁止利用个人信息在交易中实施差别化待遇，第 26 条也规定出于维护公共安全所收集的个人信息仅限用于维护公共安全的目的，第 27 条虽然支持合法处理公开信息的情形，但是如果这些处理行为对个人权益有重大影响，也应当另行取得信息主体的同意，而且在该法第 29 条进一步重申或加强了对信息利用的事先同意。因此，就侵犯公民个人信息罪而言，将收集或编辑后的公开信息予以非法出售、提供的，才属于本罪之中的非法利用情形。

三、识别性：模式选择、必要性与限制

《刑法》本身并没有对“公民个人信息”这一构成要件作出明确的规定，这导致对“公民个人信息”的认定需要结合相应的前置法来判断。虽然许多规范性文件已将“识别性”作为认定公民个人信息的核心标准，但其内涵与限度并不明确，以致在司法实践中对“公民个人信息”的认定相当恣意。此外，还存在着放弃“识别性”标准的见解与规定，对这些见解与规定又该如何看待？是否还有必要维持其核心标准的地位？对其限度又该如何限制？

（一）识别模式的选择

大体上，我国的规范性文件对公民个人信息的定义模式经历了由混合模式到识别模式的转变。

1. 混合模式。起先，《全国人民代表大会常务委员会关于加强网络信息保护的决定》（以下简称《决定》）第 1 条〔32〕提出认定公民个人信息的两个要点，即识别性与隐私性。换言之，能够识别公民个人身份和暴露公民个人隐私的信息才能被纳入公民个人信息的范围（混合模式）。随后，紧接着《决定》出台的《关于依法惩处侵害公民个人信息犯罪活动的通知》（以下简称

〔32〕《决定》第 1 条规定：“国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息。任何组织和个人不得窃取或者以其他非法方式获取公民个人电子信息，不得出售或者非法向他人提供公民个人电子信息。”

《通知》）第2条〔33〕基本沿袭了《决定》判断公民个人信息的两项标准，并没有就“识别性”的概念与范围作出明确定义，而且《通知》突破了《决定》针对公民个人信息进行保护的立场，将“数据资料”也纳入公民个人信息的范畴。应当说，单个的、零星的个人数据并不成为信息，只有经过数据处理后，其所蕴含的信息价值才会有所增长，进而可能形成个人信息，由此才能提供可识别性的内容。换言之，个人数据“可以”但不“必然”是个人信息的形式，个人信息也“可以”但不“必然”是个人数据所反映的内容。〔34〕因此，区分信息内容与信息载体的意义，更多在于对犯罪对象的法律识别，对二者的区分需要根据较为客观的技术标准来判断，而不必考虑信息载体与信息主体之间的联系。〔35〕

2. 识别模式。与《决定》《通知》所采取的混合模式不同，《中华人民共和国网络安全法》（以下简称《网络安全法》）第76条第5项、〔36〕《民法典》第1034条第2款〔37〕与《解释》第1条〔38〕未将公民个人信息与个人隐私相并列规定，而是直接对公民个人信息作了定义，采用“概括＋列举”的方式初步明确了公民个人信息的内涵与外延，并将识别性标准细化为单独识别与结合识别两种方式。

3. 第三条路径：识别性舍弃论。就《个人信息保护法》第4条第1款相比于前述的规范性文件针对个人信息的定义而言，存在着极为扩张个人信息外延的一面。虽然《决定》《通知》也将个人隐私纳入个人信息的范围，但却是通过“识别性”与“隐私性”相并列的方式展现的，最少在表面上保持了二者的区别，但《个人信息保护法》在判断某项信息是否属于个人信息时，只要是“与自然人有关”的各种信息都属于个人信息，即该信息与自然人“有关”即可，如此一来，即便该条款中存在着“识别”二字，也可以说是放弃了“识别性”的要求。这样的条文设计虽然在侵权案件中可以大大降低甄别个人信息的难度，为被侵权者提供较为充分的保护，在我国信息侵权形势较为严峻的当下有着巨大的法律价值和实践意义，但如果对侵犯公民个人信息罪中的“公民个人信息”也作此安排或理解，则无疑使得本罪的适用范围被无限扩张。例如，按照这样的理解，偷拍裙底这样的行为属于获取“与已识别的自然人有关的信息”，从而构成本罪。因此，将识别公民身份的信息置换为与自然人相关的个人信息，这导致该概念的适用空间极为巨大，以致刑事法网过于扩张。而且匿名的状态是相对的，在大数据技术下完全存在着被

〔33〕《通知》第2条规定：“……公民个人信息包括公民的姓名、年龄、有效证件号码、婚姻状况、工作单位、学历、履历、家庭住址、电话号码等能够识别公民个人身份或者涉及公民隐私的信息、数据资料。……”

〔34〕参见周斯佳：《个人数据权与个人信息权关系的厘清》，载《华东政法大学学报》2020年第2期；王成：《个人信息民法保护的模式选择》，载《中国社会科学》2019年第6期。

〔35〕参见岳林：《超越身份识别标准——从侵犯公民个人信息罪出发》，载《法律适用》2018年第7期。

〔36〕《网络安全法》第76条第5项规定：“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自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。”

〔37〕《民法典》第1034条第2款规定：“个人信息是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。”

〔38〕《解释》第1条规定：“……（公民个人信息）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身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。”

破解的风险，即匿名化处理后的个人信息依然存在着被再识别的风险，将其排除在个人信息的范围外，不具有合理性。有鉴于此，本文认为，必须在与识别模式保持一致的前提下，对《个人信息保护法》所规定的“个人信息”在《刑法》第 253 条之一的适用中进行目的性限缩，只将其中具备识别性的信息纳入规制范围。这既避免了规范上的条文冲突，也给刑事制裁、行政处罚、民事侵权诉讼各自留下了必要的适用空间。所以，第三条路径在刑事层面上是不应当得到承认的。

我国关于公民个人信息的定义模式经历了混合模式到识别模式的转变。但是，这一定义模式只不过解决了认定公民个人信息判断方向上的问题，就识别的程度或范围而言，任何规范性文件都未就“识别性”作进一步解释或规范，由此导致司法者在判断某些信息是否属于公民个人信息时，需首先定义“识别性”。但就公布的判决书来看，几乎都未涉及对“识别性”的解释，仅简单地以“涉案信息可反映公民的某些特征”等为由径直得出犯罪成立的结论，故稍显语焉不详、论证粗糙。〔39〕由此，需要进一步回答的问题是，虽然判决回避了对识别性的考察，但从全面保护个人信息的立场出发，是否需要在公民个人信息中保持“识别性”及如何限定识别深度。

（二）保持“识别性”标准的必要性

识别性是否属于公民个人信息的题中应有之义？换言之，识别性是判断公民个人信息的附加性要求，还是其本身即为公民个人信息的本质特征。若持前者的观点，则可能基于扩大公民个人信息认定范围的立场，否认识别性存在的必要性，也即前文所称的“识别性舍弃论”。除了《个人信息保护法》第 4 条第 1 款所提供的法条根据外，理论上也存在着这样的见解。例如，有观点认为，由于《刑法》并未针对个人隐私设置保护规范，出于弥补处罚漏洞的需要，应当放弃对公民个人信息附加识别性的要求，还其本来面目，即侵犯公民个人信息罪的法益是个人信息权，此处的个人信息既包括身份信息又包括隐私信息，识别性只是身份信息的必备特征，在隐私信息中则无其存在的余地，如此一来，非法出售、提供、收集隐私信息的行为亦应以侵犯公民个人信息罪论处。〔40〕

本文认为，识别性舍弃论的观点存在着可商榷的余地。其一，公民个人信息不同于与公民个人有关的信息，〔41〕前者仅指可以识别公民个人身份的信息，后者则是指一切与公民相关的、反映公民之存在的信息，其范围极为广泛，无论是否具备隐私性、是否可以识别个人身份，都可被纳入其中，可见将不具备识别性的个人隐私解释为公民个人信息，并不符合公民个人信息的本意，且有为了论证自身预设的观点而牵强地解释法条用语的嫌疑。其二，既认为本罪的法益是公民个人对信息的自我决定权，又进一步舍弃了识别性的标准，则侵犯任何与公民个人相关的信息

〔39〕 本文以“刑事案由”为方向、以“侵犯公民个人信息罪”为案由，在中国裁判文书网共搜得 9438 份判决书，再以“识别”为关键词对这些判决书进行筛选，共得 934 份判决书，即大约仅有 9.90％的判决书涉及对身份识别的说理。但深究发现，其中要么是对立法规定、司法解释关于公民个人信息之定义的表述，如江西省兴国县人民法院（2019）赣 0732 刑初 202 号刑事判决书，要么只是在阐述某项信息属于公民个人信息时作为结论性表述使用，如江苏省苏州市中级人民法院（2019）苏 05 刑终 488 号刑事判决书。

〔40〕 参见晋涛：《刑法中个人信息“识别性”的取舍》，载《中国刑事法杂志》2019 年第 5 期。

〔41〕 参见周光权：《侵犯公民个人信息罪的行为对象》，载《清华法学》2021 年第 3 期。

都属于侵犯了本罪法益。虽然在扩张本罪处罚范围的立场上可谓一以贯之，但将诸如不具备识别性的个人隐私等与公民个人相关的信息都纳入公民个人信息的范围，必定导致本罪适用范围的极度膨胀，从而使得本罪成为一切与个人信息相关之犯罪的兜底条款。其三，个人隐私常常与公民的个人关键信息密切相关，且大多包含着有关公民的人身安全、财产安全的信息，明显应当给予更为严格的保护，将其排除在公民个人信息的范围外，似有立法缺陷之嫌。但是，既然认为个人隐私与个人信息密切相关，那么将可以识别个人身份的个人隐私纳入个人信息的范围内，自然不存在解释上的障碍，且这样的解释并非扩大解释，而是个人信息的应有之义。即便认为个人隐私与个人信息有别，那么基于识别性判断标准，对于无法识别个人身份，亦无法威胁到人身安全、财产安全的个人隐私而言，其自始至终便不在本罪的保护范围之内，也就谈不上立法缺陷。况且就保护公民个人信息的旨趣与保护公民隐私的旨趣而言，二者亦有所区别：在当前的数字经济时代，公民个人信息具有巨大的经济价值，因此法律注重的是规范公民个人信息的收集、利用等行为；而对于隐私而言，法律则关注的是保护此类信息不被非法披露或公开。因此，对公民个人信息的保护不能也不宜采取与传统隐私权相同的方式，那么对个人信息的界定则应与个人隐私有所区别。〔42〕其四，以刑事政策上的处罚必要性来论证对个人隐私的全面保护，也会遭到刑法谦抑性的质疑，即在尚未穷尽行政规制措施与民事救济手段的情况下，径直对收集、出售或提供不具备识别性的个人隐私的行为予以刑事处罚，未免操之过急。因此，识别性作为公民个人信息的本质特征，仍有其理论意义与实践价值。

（三）对识别深度的限制

侵犯公民个人信息罪的重点是判断某项信息是否具备识别性，而就判断的方法或路径而言，可从以下两个方面展开：一是识别，即基于信息来识别特定个人身份；二是关联，即在已知特定个人的情况下判断某项信息是否有助于识别出该人。上述两种路径之间并不是互相独立或毫无关系的，事实上，在一些情形中，通常都需要将两种路径结合起来判断某项信息是否属于公民个人信息。〔43〕但是，特别需要强调的是，在利用关联方法的场合，不能因为已知特定个人，进而先入为主地将涉案信息认定为公民个人信息，必须站在事前的立场，基于当时的技术条件、行为人的认识能力来判断这些信息是否有助于识别特定个人身份。

识别性信息包含直接识别（单独识别）与间接识别（结合识别）两大类信息。顾名思义，前者是指某项信息单独即可识别出公民个人身份，如身份证号；后者是指某项信息必须与其他信息结合在一起后方能识别出公民个人身份，如重名是司空见惯的现象，依据姓名尚不能识别公民个人身份，但若将其与出生年月日、家庭住址、工作单位、职务等信息结合在一起后便能实现对公民身份的识别。在大数据时代，能直接（单独）识别出特定个人的信息自不待言，即便是一些非常边缘的信息，一旦被结合起来依然可以识别出特定个人，由此导致几乎所有与个人相关的信息

〔42〕 参见田宏杰：《窃取 APP 里个人信息的性质认定——兼及个人信息与个人隐私之界分》，载《人民检察》2018 年第 7 期。

〔43〕 例如，有观点认为，关联是识别的前提阶段，关联是可识别的决定因素，即先判断涉及个人信息的要素是否与信息主体存在关联，而后再根据具体场景判断是否达到了“可识别”的程度。参见商希雪：《个人信息隐私利益与自决利益的权利实现路径》，载《法律科学（西北政法大学学报）》2020 年第 3 期。

都可以借助“识别性”被纳入公民个人信息的范围，但如此扩张的信息范围自然面临着刑事法网过分严密的诘难。例如，有观点指出，间接识别这一方法看似最大限度地保护公民个人信息，但实际上是将公民个人信息置于动态化和场景化的危险之中，且适用间接识别时还将遭遇以何种知识水平的人为认定标准，以及是否对能用来判断公民个人信息的资料予以限制的问题。〔44〕破解这一困境的最有效路径便是对“识别性”的深度进行限定。对此，理论上存在以下观点。一种观点认为，判断相关信息是否属于公民个人信息时，可以从信息的重要程度、需要结合其他信息的程度、行为人主观目的三个方面考察。〔45〕另一种观点认为，即便间接（结合）识别类信息可以被用来识别特定个人，但如果其与国家认证身份之间的关联异常遥远，则没有必要将其纳入公民个人信息的范围。〔46〕

总体而言，上述观点都存在值得商榷的余地。第一种观点的问题在于，各个要素之间并不存在先后位次或内在逻辑，以致考虑的要素越多，越会造成要素之间取舍的困难。例如，行为人的主观目的并非指向识别特定个人，但该信息又很重要，此时，是否应将该信息纳入“公民个人信息”的范畴呢？该观点的初衷是通过考察信息的客观价值、主观用途来限定“识别性”的识别深度，但这样主客观混杂的方案在现代大数据技术的冲击下，可能无法达到论者所预期的效果。第二种观点将公民个人信息同国家认证身份结合起来的思路具有启发性，但其问题在于如何判断一项信息与国家认证身份之间的关联异常遥远。

本文认为，对识别深度应做以下几点限制。其一，公民个人身份信息并不限于国家认证身份，对于一些虽不是由国家赋予但在特定领域内具备识别特定个人身份效果的信息，依然具有保护的必要性。例如，学号是每个学校为在该校就读的学生所编制的号码，其本身不一定属于国家认证的身份，也无法单独识别特定个人，但若将其与学校结合起来，即可确定到特定个人。其二，概念本身的模糊性虽然确实导致公民个人信息的范围不断扩张，但必须承认的是，大数据技术的进步、信息社会的发展同样是造成这一局面的原因。因此，在判断某项信息是否属于公民个人信息时，应当考虑行为时的方法、技术是否可以通过该信息识别出特定个人。换言之，识别具有相对性，应当结合行为人的识别能力、技术方法等进行综合判断。其三，某项信息与公民身份之间的关联是否遥远，取决于该信息是否包含涉及公民身份的因素。详言之，对于行为人来说，其最终需要的是可以识别特定个人身份的信息，其他一些信息即便对此有所助益，但若本身无法指向特定个人，则不能被纳入公民个人信息的范围。同样的，对于司法人员来说，其也需要对涉案的信息进行甄别，从中区分出哪些属于公民个人信息、哪些不属于公民个人信息。例如，病床号、用药情况虽然可以通过结合姓名、身份证号等精确定位公民个人，但其自身并不包含任何涉及公民身份的因素，至多只是一项辅助判断的信息。〔47〕因此，最为重要的问题是，如何将这种辅助信息与公民个人信息区分开来。本文认为，直接（单独）识别类信息由于具有较强的识别

〔44〕 参见齐爱民、张哲：《识别与再识别：个人信息的概念界定与立法选择》，载《重庆大学学报（社会科学版）》2018 年第 2 期。

〔45〕 参见喻海松：《侵犯公民个人信息罪司法适用探微》，载《中国应用法学》2017 年第 4 期。

〔46〕 参见岳林：《超越身份识别标准——从侵犯公民个人信息罪出发》，载《法律适用》2018 年第 7 期。

〔47〕 参见喻海松：《侵犯公民个人信息罪的司法适用态势与争议焦点探析》，载《法律适用》2018 年第 7 期。

性，故一般较为稳定，能够清晰地与间接识别类信息、辅助信息区分开来；但是，间接识别类信息是通过各项信息之间的相互印证来识别出特定个人身份，其与辅助信息之间的界限较为模糊，所以辅助信息与识别类信息的区分才是重点。辅助信息与间接识别类信息之间最为关键的区别在于是否具有身份指向性。所谓身份指向性，是指某项信息需要以公民的个人信息为背书或需要公民的个人信息为条件产生某项信息，如此一来，辅助信息所包含的信息只不过反映了自然人的活动轨迹或存在，如通话记录、行动轨迹等。相反，间接识别类信息则可以基于与其他信息（不论是辅助信息还是其余的间接识别类信息）的结合来识别出特定个人的身份，如在现今实名制要求下的微博账号等。

四、识别性与个人信息权的双重检视

就目前的司法实践而言，对识别性的适用缺乏深刻的认识导致常常出现以行为妨害了公民个人隐私、生活安宁、公共安全等利益来反证涉案信息属于公民个人信息的论证路径，或者在确认相关信息属于公民个人信息的情况下，径直地得出行为人构成侵犯公民个人信息罪的结论，而并未考虑是否存在法益受到侵害的事实。此外，学界也对识别性与个人信息权在实际案件的适用中的关系没有给予足够的关注，难以为司法实务提供成熟、充分的理论指导。本文认为，识别性与个人信息权对判断相关行为是否构成侵犯公民个人信息罪发挥着不可替代、相辅相成的作用。就具体的适用而言，需要考虑以下两个方面：一方面，虽然个人信息权作为本罪的法益，对构成要件的解释具有方向性的指引作用，但也需要警惕以法益侵害反证客观行为之危害的倾向，故对侵犯公民个人信息罪的认定而言，不能因为确认相关行为侵犯了本罪法益，便径直地将所有的涉案信息认定为公民个人信息；另一方面，以识别性为标准确定了涉案信息属于公民个人信息之后，尚需进一步检验相关行为是否侵害了个人信息权，换言之，识别性的价值仅在于判断某项信息是否属于公民个人信息，而是否成立侵犯公民个人信息罪尚需在此基础上进一步结合本罪的其他主客观要件予以考量。

（一）坚持对“识别性”的优先判断

如前所述，目前实务对将识别性与个人信息权结合起来运用在侵犯公民个人信息罪之证立上的重视不足，且呈现出立场不一、论证粗糙、逻辑混乱的倾向。例如，在案例一中，法院的审判逻辑是，跟踪车辆、利用工具对手机进行实时定位等行为所获取的行动轨迹具有个人专属性，且侵犯了公民的隐私与生活安宁，所以被害人的行动轨迹便属于公民个人信息。〔48〕不难看出，法院在审理该案时并没有从正面定义何为公民个人信息，然后据此论证行动轨迹是否属于公民个人信息，而是以行动轨迹反映公民个人的社会活动及一旦暴露会危及公民的生活安宁等危害后果来反证其属于公民个人信息。且不说是否要以识别性为标准将不具有识别性的个人信息排除在外，这种以“危害结果补充行为不法”的司法操作必然导致任何信息都可以借助危害后果被纳入公民

〔48〕 参见前引〔3〕，最高人民法院刑事审判第一、二、三、四、五庭主办书，第55－56页。

个人信息的范围，由此使得本罪的公民个人信息丧失单独判断的意义。此外，虽然存在着像陈明侵犯公民个人信息罪案〔49〕那样尝试从正面认定涉案信息的判例，但遗憾的是，法院并未坚定地贯彻识别性标准，舍弃了对邮箱的账号和密码具备可识别性的论证，而是以邮件内容可以反映用户的活动情况来反推邮箱的账号和密码属于公民个人信息，由此导致判决立场模棱两可、论证思路自相矛盾。既然能够通过邮箱的账号和密码识别出公民个人身份，则完全满足了识别性的要求，可以确认邮箱的账号和密码属于公民个人信息，且判断的对象是邮箱的账号和密码本身，应围绕账号和密码是否具备识别性展开，而不能以邮件来证成账号和密码具有识别性，否则便偏离了判断的基准。

另一种情况是，在依据部分涉案信息即可认定犯罪成立的前提下，将全部涉案信息认定为公民个人信息。换言之，以个人信息权遭受侵害为前提代替或舍弃了对全部涉案信息的再次判断，如通话记录、行踪轨迹等信息，其本身难言包含着识别性信息，以犯罪成立为前提将其理所当然地纳入犯罪对象的范围，明显不当，赵某某侵犯公民个人信息罪案〔50〕即是适例。该案涉及的公民个人信息种类较多，其中如车辆信息、征信、住宿等信息由于记载有公民的身份信息，故将其纳入公民个人信息的范围并无问题，但对于行踪轨迹、通话记录等信息为何具备识别性进而可被纳入公民个人信息的范围，法院在判决中并未言及。由此可见，实践所暴露出的问题并非可以仅通过强调贯彻或细化操作标准、补充论证解决的，而是需要审视识别性与个人信息权之间的适用逻辑、互动关系，以二者的双重验证解决涉案信息判断和罪名成立上的反证操作、逻辑矛盾等问题。

只有具备识别性的个人信息才会侵害公民的个人信息权，因此，对任何一起侵犯公民个人信息的案件来说，首先需要判断的是，涉案信息是否具备识别性。如果从一开始即以行为人主观上具有侵犯他人个人信息权的故意，且客观行为对他人的生活、安全产生不良影响等为由，认定行为人所获取的信息属于公民个人信息，则几乎可以在任何案件里得出行为人构成犯罪的结论。认定犯罪成立的合理路径当是，优先判断客观上是否存在侵害或危及法益的实行行为，这既有利于规制故意的认识对象、明确过失的认识能力标准，也有助于避免主客观混合判断所导致的主观归罪倾向。就侵犯公民个人信息罪的客观行为判断而言，主要包括是否存在非法出售、提供、获取等行为及该行为是否指向公民个人信息两个方面。

如前所述，对识别性的适用围绕身份指向性展开，不具备身份指向性的信息充其量只是辅助信息，而仅有辅助信息根本不足以侵害公民的个人信息权，也就应以不存在非法出售、提供、获取公民个人信息的行为排除犯罪的成立。案例一中行踪轨迹本身只不过反映了自然人的移动范围，并不需要以自然人的身份信息作为产生条件，法院之所以将其视为公民个人信息，是因为认

〔49〕 本案案情为：被告人陈明通过黑客网站下载获取他人的邮箱账号和密码，后通过 QQ 等渠道多次提供给赵某等人。一审法院判决陈明构成侵犯公民个人信息罪，但陈明以仅凭邮箱账号和密码无法识别出特定自然人的身份为由提出上诉。二审法院经审理，认为可以根据邮箱的注册信息对应使用人的身份情况，甚至可以通过查看邮件知晓使用人的活动情况，故认定邮箱账号与密码属于公民个人信息。参见江苏省苏州市中级人民法院（2019）苏 05 刑终 488 号刑事判决书。

〔50〕 本案案情为：被告人赵某某以非法牟利为目的，通过购买等方式非法获取行踪轨迹、车辆信息、征信、通话记录、住宿信息等各类公民个人信息后，将上述信息出售、提供给他人。参见江苏省无锡市中级人民法院（2018）苏 02 刑终 418 号刑事判决书。

为收集行踪轨迹的人员在事先便已知晓被害人的身份，那么所获取的行踪轨迹当然可以对应到该被害人，但这不过是循环论证。事实上，若是以被害人从工作单位地址到家庭住址的行踪来证明行动轨迹属于公民个人信息，则恰恰说明行踪轨迹本身就不是公民个人信息。理由在于，具备识别性的是被害人的工作单位、家庭住址等信息，若是将这些信息指代成行踪轨迹，那么行踪轨迹的内涵就并非如法院所认为的那般系指自然人的移动范围。不过，实践中也存在着从正面肯定身份指向性进而以识别性认定涉案信息属于公民个人信息的判例。在杨木侵犯公民个人信息罪案〔51〕中，被告人一方最为重要的上诉理由是，涉案手机号码及其套餐情况并不以身份信息为产生条件，也就无法识别公民个人身份。二审法院并未以被害人获利数额巨大、利用职务便利实施犯罪、出售号码的行为影响机主的生活安宁等避实就虚的理由回避对涉案手机号码是否可以识别公民身份的认定，而是首先从正面肯定识别性系判断公民个人信息的标准，然后通过抽样鉴定的方法确认该案中的绝大多数号码都属于实名制信息，也即具备身份指向性，进而认定涉案手机号码属于公民个人信息。像这样以识别性为出发点判断涉案信息的属性，而后再据此论证其他犯罪成立要件的司法逻辑应当得到足够的重视与严格的贯彻，使涉案信息接受识别性的全面验证，充分发挥识别性作为侵犯公民个人信息罪第一道关卡的作用。

（二）犯罪成立的二次检验：个人信息权

涉案信息经过识别性的检视而被确认为公民个人信息后，排除犯罪成立的另一道关卡是行为是否侵犯了公民的个人信息权。然而，实践中频繁采取的操作却是在得出涉案信息属于公民个人信息的结论后，直接绕过或放弃第二道关卡的检验，未能进一步考虑是否存在非法出售、提供、获取等侵犯公民个人信息权的实行行为，从而也就难以确保判决结论合理。例如，在案例二与连福顺侵犯公民个人信息罪案〔52〕中，且不说公司名称、注册资本等法人信息难以被视为公民个人信息，即便认为涉案的姓名、电话号码等信息属于公民个人信息，也需要考虑涉案信息作为工商登记信息或公开信息，企业本身有向社会公开的义务或信息主体已自我决定向公众公开，根据《个人信息保护法》第27条的规定，这样的行为不构成对信息主体权利的侵犯，况且其他公民也可通过相关主管部门的信息公开制度或其他合法渠道获取。以“天眼查”为代表的企业信息查询软件，其数据的主要来源渠道是政府、法院等官方网站，〔53〕任何人都可以在这些网站上获取企业的登记信息，只不过“天眼查”基于其所开发与应用的数据技术，将企业或某个股东、企业高

〔51〕 本案案情为：被告人杨木系中国移动通信集团四川有限公司成都分公司员工。某公司负责人李某因公司开展业务需要，遂与杨木商议以每条0.1元的价格购买移动公司的客户消费信息（含电话号码和资费情况）。其后，杨木分多次向李某出售移动客户信息数百万条。一审法院判决杨木犯侵犯公民个人信息罪，但宣判后，杨木及其辩护人以涉案数据为电话号码及相应套餐情况，并不能据此识别特定自然人身份及反映自然人活动信息，认为本案不应被定性为侵犯公民个人信息罪等为由，提出上诉。二审法院经审理认为，涉案信息包含用户电话号码及相应资费信息，且根据公安机关筛选了96000条数据并经核实后，仅有2084条系非实名制的情况，可以认定本案所涉绝大多数信息属于实名制信息，故维持了一审判决对本案系属侵犯公民个人信息罪之定性。参见四川省成都市中级人民法院（2019）川01刑终211号刑事判决书。

〔52〕 本案案情为：被告人连福顺为实施诈骗，购买了一个名为“天眼查”软件的会员，从该软件上收集姓名及电话号码等公民个人信息，并将事先编写好的诈骗短信发送给机主。案发后，公安机关从其电脑内提取到公民个人信息共计11578条。参见广西壮族自治区田林县人民法院（2019）桂1029刑初43号刑事判决书。

〔53〕 参见“天眼查”官网免责声明条款，载https://www.tianyancha.com/property/5，最后访问时间：2021年3月18日。

层的所有企业相关信息整合在一起，以便查询人省时省力地直观了解其所要查询的企业或公民个人的企业信息。由此，通过这些渠道获取公民个人信息并不违法，所支付的会员费等不过是购买大数据集合技术服务的使用费。但这两起案件的审理法院却没有考虑到这一情况，而是以这些信息属于公民个人信息且被用于实施诈骗犯罪为由认定行为人构成侵犯公民个人信息罪，不得不说在论证上稍显草率。如果考虑到个人信息权的法益构造，这样的问题就能得到妥善的解决。

详言之，本罪规制的是非法获取与非法利用公民个人信息的行为，其中，非法利用具体表现为非法提供和非法出售两种形式。在案例二中，在确认行为人获取公民个人信息的行为并不违法后，只需要考虑其后利用公民个人信息实施诈骗的行为是否属于非法提供或非法出售公民个人信息这两种实行行为。案例二的行为人从一开始就形成了诈骗罪的共犯，在共同获取涉案信息后便将之用于骗取财物，并未向其他人提供或出售涉案信息，也就不存在非法提供或非法出售公民个人信息等侵犯信息利用权的行为，对行为人等只能论以诈骗罪。因此，基于识别性的标准确认涉案信息属于公民个人信息之后，个人信息权作为第二道关卡的价值在于判断获取、利用公民个人信息的行为是否违背了权利主体的意思自治，从而检视是否存在非法获取、非法利用公民个人信息的行为。以前述赵某某侵犯公民个人信息罪案为代表的判例虽然在论证涉案信息属于公民个人信息上存在些许瑕疵，但该判决既评价了行为人非法获取公民个人信息的事实，又论证了行为人此后的非法出售等行为，可谓充分考虑了个人信息权的法益构造，依然有值得肯定之处。

任何以识别性、个人信息权相互代替来判断彼此是否成立，从而论证侵犯公民个人信息罪是否成立的理论方案或实务操作必然遭遇逻辑混乱、立场颠倒的诘问。将识别性与个人信息权作为两道关卡检视侵犯公民个人信息案件的实务操作，并非出于学术上的自我满足，而是以正确适用罪名、严格贯彻逻辑推演、规范评价为价值取向，呼吁在实践之中形成从以识别性认定公民个人信息到通过个人信息权验证客观危害行为的司法适用逻辑。应当说，如此从客观行为入手、判断犯罪是否成立的方案相较于目前的司法实务现状，有其优势。

五、结　论

综上所述，可以得出以下几点结论：

第一，以识别性为标准判断公民个人信息具有妥当性，仍有必要保留，因此不宜直接采纳《个人信息保护法》对个人信息的定义。不过，必须对识别性的识别深度予以限定，既要把握只有以公民的身份信息为背书，才可能被认定为公民个人信息的方向，也要结合现存的技术手段、行为人的认识能力等来具体判断涉案信息是否可以被用来识别特定个人的身份。

第二，相较于一般人格权视角下的个人信息权，以具体人格权为基础建构的个人信息权无论是在解释的明确性上，还是在实务判决的说理上，都存在着明显的优势。就侵犯公民个人信息罪的具体适用而言，应当重点考察是否存在对信息控制权与信息利用权的侵害。

第三，在涉嫌侵犯公民个人信息的场合，首先必须以识别性为标准判断涉案信息是否属于

公民个人信息，只有在得出肯定结论的前提下，方可进入下一层面的判断，即是否存在非法出售、提供、获得公民个人信息的行为，以及这样的行为是否侵害了公民的个人信息权。因此，将识别性与个人信息权作为检视侵犯公民个人信息罪实务操作的两道关卡，并以此二者作为论证判决的逻辑进路，更有利于合理划定本罪的适用范围，在刑法的积极适用与必要谦抑间保持平衡。

Abstract: In the current judicial practice, there are some defects in the identification of citizens' personal information, such as unclear connotation and improper extension. The root of the defects lies in the failure to fully realize the important role of identification standard and personal information right in judging citizens' personal information. On the one hand, the theoretical research does not pay enough attention to the identification limit of identifiability; on the other hand, it lacks the in-depth exploration of the right attribute and structure of personal information right, which makes it impossible to provide ideal operation scheme and endorsement reason for practice. On the basis of defining the depth of identification and clarifying the connotation of the right of personal information, we should take the dual inspection path from identification to the right of personal information, and limit the scope of application of the crime of infringing citizens' personal information to the occasions where citizens' personal information right is infringed by illegally selling, providing and obtaining the identifiable information.

Key Words: personal information of citizens, identifiability, personal information right, dual inspection

(责任编辑：简　爱　赵建蕊)

财经法学 No. 2，2023
pp. 3 - 20

人工智能司法的可解释性困境及其纾解

周　媛　张晓君*

内容提要：加强对人工智能司法发展及风险的研究是时代课题，其中人工智能司法的可解释性困境尤为关键。人工智能司法可解释性指的是司法决策或行为的可理解与透明性，涉及基础数据、目标任务、算法模型以及人的认知这四类关键要素。不可解释困境主要是由数据失效、算法黑箱、智能技术局限、决策程序和价值缺失等因素所致。但是，人工智能司法的不可解释困境其实是一个伪命题，可解释性具备认知层面和制度层面两方面基础。纾解困境的具体策略包括：构建司法信息公开共享制度，提高有用数据的甄别与利用效率；从软硬法结合视角建构司法系统的运行标准与制度规则；从全过程视角强化主体之间的协同治理；通过指导性案例和司法解释赋权法官的司法解释空间，提高法律解释技术；强化交叉学科人才建设，提高对人工智能司法决策模型的引领；发挥法官的自律与能动性，实现司法智能决策的人机协同。未来，不仅需要把握司法价值与技术理性的平衡，还需考虑人工智能对司法的差异化介入，推动人工智能司法战略目标实现。

关键词：人工智能　司法　算法　可解释性　协同治理

一、问题的提出

党的二十大报告明确提出："构建新一代信息技术、人工智能、生物技术、新能源、新材料、高端装备、绿色环保等一批新的增长引擎。"自 2015 年起，人工智能与司法工作深度融合发展战略上升为国家战略，各地纷纷开启智慧法院建设步伐。〔1〕从智慧司法 1.0 到 4.0，人工智能司法已成为一种现实，深刻地改变着传统法院的组织能力与管理结构，冲击着诉讼架构和程

* 周媛，上海交通大学凯原法学院博士研究生；张晓君，西南政法大学国际法学院教授。

本文为国家社会科学基金项目"城市更新中促进绿色建筑发展法律机制研究"（21BFX136）的阶段性成果。

〔1〕 如上海刑事案件智能审判系统、北京"睿法官"审判辅助系统、河北"智审"审判系统和浙江"金融智慧庭审平台"等。参见聂友伦：《人工智能司法的三重矛盾》，载《浙江工商大学学报》2022 年第 2 期。

序机制，重塑法律人的理念、情感、行为乃至结果模式，甚至影响整个司法权力在国家权力架构中的定位。〔2〕但对于智慧法院建设，学界呈现两种分歧立场：一种观点认为，从司法本质看人工智能司法具有主体正当性，从司法裁判的手段看智能裁判具有逻辑正当性，从司法过程看人工智能司法具有程序正当性，从司法结果看智能司法具有结果正当性，因此，人工智能司法的整体正当性充足。〔3〕另一种观点认为，人工智能司法的运用程度有限，只能作为一种实现司法正义的辅助手段，不能排斥法官的心证和裁量，这是其运用所应遵守的基本原则。〔4〕然而，法律是一种风险控制机制，习近平总书记在中国共产党第十九届中央政治局第九次集体学习时强调："要加强人工智能发展的潜在风险研判和防范，维护人民利益和国家安全，确保人工智能安全、可靠、可控。要整合多学科力量，加强人工智能相关法律、伦理、社会问题研究，建立健全保障人工智能健康发展的法律法规、制度体系、伦理道德。"〔5〕法律是风险识别和控制的主要手段。法律是一种社会建构。因此，对法律的合适态度，应该是审慎而非颂扬（celebration）。〔6〕法律的保守主义立场使得我们更需要保持一种批判主义研究进路。

目前学界对人工智能司法的批判性研究成果大致可归为以下几个方面：一是人工智能司法产品运用过程中外部技术环境的限制，最为典型的是作为智能司法决策基础的司法数据样本存在"伪充分性"，〔7〕还包括法律语言与计算机语言的隔阂等；二是人工智能内在的技术困境，典型的是算法歧视、算法黑洞与算法霸权；三是人工智能的伦理与价值困境，体现在人工智能无法对司法正义作出实质性权衡，也无法复制法律人的"情怀"和"匠心"；〔8〕四是人工智能受到司法环境的制约，如国家的政策性、政治性因素，地域因素，习惯规则以及法律体系的差异等。作为一项智能推理与决策技术，无论是人工智能司法数据的"伪充分性"、算法黑洞困境，还是人工智能的伦理与价值困境，都指向人类如何正确使用人工智能，而至于人工智能又如何满足人类对司法正义与价值目标的追求，透明性、可解释性及由此产生的可信赖性成了解决问题的关键。2019 年 4 月，欧盟委员会发布的《人工智能道德准则》提出了值得信赖的透明性规则；2021 年 1 月，欧洲议会和理事会发布的《关于人工智能的统一规则（人工智能法）并修正某些联合立法行为》同样对人工智能的透明性和可理解性进行了着重强调。〔9〕2021 年 9 月，我国国家新一代人工智能治理专业委员会发布了《新一代人工智能伦理规范》，明确提出人工智能发展需遵守"确保可控可信、强化责任担当"等六项基本伦理要求，基于可解释性才能实现验证、审核、预测与信赖。事实上，我国以人民为中心的司法审判工作本质是一种"回应型司法"或"纠纷解决型司法"，〔10〕回应型的内

〔2〕 参见徐骏：《智慧法院的法理审思》，载《法学》2017 年第 3 期。

〔3〕 参见彭中礼：《司法裁判人工智能化的正当性》，载《政法论丛》2021 年第 5 期。

〔4〕 参见季卫东：《人工智能时代的司法权之变》，载《东方法学》2018 年第 1 期。

〔5〕 习近平：《加强领导做好规划明确任务夯实基础 推动我国新一代人工智能健康发展》，载《人民日报》2018 年 11 月 1 日，第 01 版。

〔6〕 参见〔英〕哈特：《法律的概念》（第 3 版），许家馨、李冠宜译，法律出版社 2018 年版，第 1 页。

〔7〕 参见前引〔1〕，聂友伦文。

〔8〕 参见马长山：《司法人工智能的重塑效应及其限度》，载《法学研究》2020 年第 4 期。

〔9〕 参见刘艳红：《人工智能的可解释性与 AI 的法律责任问题研究》，载《法制与社会发展》2022 年第 1 期。

〔10〕 参见〔美〕米尔伊安·R. 达玛什卡：《司法和国家权力的多种面孔——比较视野中的法律程序》（修订版），郑戈译，中国政法大学出版社 2015 年版，第 14－15 页。

在向度正是追求司法活动的透明性和可解释性。例如，行政诉讼领域的“行政争议的实质性解决”，法理逻辑即是通过充足的沟通与恰当的交流平台，让诉讼活动评价回归当事人的“体验感”，提高当事人的司法获得感，从而增强司法判决的可接受性。行政裁判的可解释性正是实质性解决行政争议的前提条件。

虽然近年来对于人工智能的可解释性的研究逐渐升温，但事实上人们对人工智能“黑洞”的内在原因及破解路径仍然疑问重重，就像 2017 年 AlphaGo 如何战胜了两位世界围棋冠军，赛后柯洁坦言其策略是那么让人惊诧。国内法学界聚焦人工智能司法的可解释性这类子领域的有力研究成果并不多见。〔11〕因此，下文从人工智能司法可解释性困境的具体表现入手，阐释人工智能可解释性的具体内涵，探寻可解释性困境的具体方面及其形成的机理，进而对可解释性的主客观基础作出研判，得出纾解人工智能司法可解释性困境的有效之道。

二、可解释性界定与人工智能司法可解释性困境

概念是逻辑研究的起点。对解释性的界定成为本文研究的起点。由于理解活动“具有双重的主观性：理解对象的主观性和自身活动的主观性”〔12〕，在对研究概念和对象进行界定和选取时要尽可能做到多维度、多视角。

（一）解释与可解释性：多学科融合视角

“解释”在汉语中包含两层词义：分析阐明和说明含义、原因、理由等。但在科学哲学领域，“解释”一词的词义往往从本体含义转移至语境功能层面，关联到解释主体和对象之间的逻辑关系。例如，亚里士多德就曾通过物理学的观察提炼出“四因说”，得出解释其实就是对事物（解释项）与事物（被解释项）之间“为什么”产生、发展、变化、消亡等一系列动因的说明。学者亨普尔（Carl G. Hempel）和奥本海姆（Poul Oppenheim）在《解释的逻辑研究》一书中进一步明确解释的“阐释”作用，即解释是对解释项与被解释项之间关系与逻辑的重构，或达到论证某种关联的目的。〔13〕由此，这种解释功能也被定义为对解释项与被解释项因果关系的挖掘，如美国哲学家刘易斯（Clarence Irving Lewis）直接将解释等同于因果关系的说明，“解释一个事件就是提供一些关于其因果历史的信息。在解释的行为中，一个拥有一些关于某个事件的因果历史的信息（我称之为解释性信息）的人试图把它传达给其他人”〔14〕。但是，因果关系并非事物关联性的全部，并非所有的因果关系都存在唯一的解释形式，由此，解释的路径和方法具有多元性，特别是科学哲学领域不同的逻辑将引导出不同的可解释性方法。例如，在知识图谱的推理方法中，至少存在“符号主义”“行为主义”“连接主义”“新型混合”四种可解释知识推理类型，不同的

〔11〕 相关文献参见前引〔9〕，刘艳红文；姚叶：《人工智能算法的不可解释性：风险、原因、纾解——兼论我国“举报人免责制度”的具体建构（英文）》，载《科技与法律（中英文）》2022 年第 3 期；苏宇：《优化算法可解释性及透明度义务之诠释与展开》，载《法律科学（西北政法大学学报）》2022 年第 1 期等。

〔12〕〔德〕马克斯·韦伯：《社会科学方法论》，韩水法、莫茜译，商务印书馆 2020 年版，序言第 17 页。

〔13〕 See Carl G. Hempel & Paul Oppenheim, Studies in the Logic of Explanation, 15 *Philosophy of Science* 135 (1948).

〔14〕 转引自闫坤如：《可解释人工智能：本源、进路与实践》，载《探索与争鸣》2022 年第 8 期，第 107 页。

推理类型又对应着不同的推理方法。〔15〕这就需要以一种多学科融合的角度来理解人工智能领域的解释。

回到人工智能领域，人工智能领域的解释本质是指人工智能的可理解性或透明性，亦即人工智能的“演绎法则”能够被人所认识、领悟。从亚里士多德的“四因说”出发，人工智能的可解释性作为语境词汇，至少会涉及基础数据、目标任务、算法模型以及人的认知这四类关键要素。其一，数据是人工智能得以存在的前提，人工智能本质即是借用计算机对大数据强大的搜索统计、计量分析、深度学习等功能，而形成的一种计算认知，足够多、足够好与足够真实的大数据是人工智能的必要条件。但采集哪些数据不采集哪些数据，对于人工智能而言似乎并不是一个不言自明的清晰逻辑，它有待于目标任务的明确设定。其二，目标任务在逻辑上是为达到某种效果或完成某种行为，但如何将这种效果或行为设定转换为计算机语言以完成人类语言向数智语言的转变，需要抓住的关键是两类“语言”之间的联结点在哪里。一般而言，事物的规律性是两者之间的联结点，因此可以通过足够优质的大数据进行因果逻辑抑或形式逻辑的推理，建立两者之间的确定性或概率性的关联，形成一种以事物的规律性和逻辑自洽为中心的算法模式。其三，算法模型是数据充足、目标明确的基础上所刻画的一种客观逻辑结果，它也是人工智能可解释性的关键所在，按照可解释性的程度大致可划分出三类算法模型：〔16〕（1）参数模糊型，主要是指由于任务的复杂性与数据的繁杂性，算法模型并非设定一个单一的清晰的范围值或确定的任务目标，只是在一个可能的概率值范围内搜索更多的可能有用的数据，从而完成相对模糊的逻辑关联运算，如深度学习模型；（2）参数明确型，主要是指任务较为明确、逻辑较为清晰的目标运算，这类运算通常在给定的范围值内，搜集较大关联性的数据，从而得出较为公认或公式化的算法模型，如统计学习模式；（3）参数外显型，相比于明确型，这类算法本身具有透明性，也可称为“白盒模型”，需要提取哪些数据以及目标设定都十分明确，得出的结果也自然较为单一，通常遵循条件式因果推理规律，如专家知识模型。其四，人的认知是这四类关键要素的决定因素，相对于算法模型而言，人的认知与意志更具主观性，主观性会加剧对人工智能决策过程的理解差异，不同群体由于知识范围的差异对算法决策的理解能力自当不同，如何弥合主观与客观之间的鸿沟成为打开算法“黑盒”的金钥匙。

人工智能融入司法，相应的可解释性问题自然而然转移到对司法基础数据、司法目标任务、司法决策算法模型以及法官的认知这四类关键要素的理解上。首先，司法数据从内容和对象来看，是人民法院“在司法工作中形成的审判流程、执行信息、法律文书、庭审活动信息、司法政务、司法人事、外部协查等数据的总和及其关联关系”〔17〕；但从结果来看，它主要指向司法裁判文书以及相应的裁判技术。司法数据的存在是人工智能介入的基础，司法数据“质量”决定人工智能司法决策的真实性、可靠性，若是司法数据偏差自然会引发可理解性困境。其次，司法目标

〔15〕 参见夏毅、兰明敬、陈晓慧、罗军勇、周刚、何鹏：《可解释的知识图谱推理方法综述》，载《网络与信息安全学报》2022 年第 5 期。

〔16〕 参见刘桐、顾小清：《走向可解释性：打开教育中人工智能的“黑盒”》，载《中国电化教育》2022 年第 5 期。

〔17〕 孙晓勇：《司法大数据在中国法院的应用与前景展望》，载《中国法学》2021 年第 4 期，第 124 页。

任务是司法裁判要达成的政治效果和社会效果，我国司法的目标是以人民为中心，惩戒犯罪、化解社会矛盾，实现公平公正高效的司法服务。然而这一目标决定人工智能司法的行为逻辑或演绎规则必须纳入利益平衡与价值考量，而这正是计算机语言难以充分解释的又一困境之所在。再次，司法裁判的过程是对案件事实与证据、法律规则要素以及法官裁量标准的综合性判断，随着事实与证据的量化、法律规则以及法官裁量的标准化，司法裁判逐渐走向自动化，司法决策算法模型是自动化的一种表现，但事实与证据的模糊性、法律规则的滞后性以及法官裁量的主观性都可能导致算法决策模型难以形式化。事实上，目前的人工智能司法模型多体现为较为简单的统计学习型，如何进行智能司法深度学习是一大理论难题。最后，法官对法律的理解以及价值观的培育是司法目标能够达成的关键，统一法官的思维模式可保证司法目标的一致性，但在具体的案件类型、地区差异以及场景化司法运行过程中，法官基于实质平等的法律解释与续造所发挥的主观能动性恰是实现司法公平、公正的重要前提，而这增加了人工智能司法技术标准的设计难度，自然增加了不可解释性空间。司法这四个基础要素导入人工智能领域在实践中衍生出以下可解释性困境具体形态。

（二）人工智能司法可解释性困境的具体形态

第一，司法数据“低劣”引发人工智能决策失真。马云曾说，在21世纪数据好比支撑社会经济发展的“石油”。“司法大数据与人工智能技术的实质是建立了一种基于海量数据挖掘的认知范式，数据具有绝对的前置性。”〔18〕以数据为中心的司法智能是从相关的类案情节中提取判决规律的一种非理论预设的认知技术。足够多、足够优质的类案数据既是司法公正决策的前提，更是获得人们理解的基础。仅凭单个或特殊案例所总结的判决结论往往不具有较强的说服力，“坏的”“低劣”的数据也会导致人们对司法决策理解的偏差。从司法样本数据来看，“不充分”和“低劣”数据主要表现在：一是司法数据本身存在主观性，哪些数据可以公开、哪些不能公开，已经受到人为因素的左右，基于主观筛选和缺失样本所进行的司法决策很可能会背离实践真实样态，导致人们对司法决策能力和效果的误解。例如，在行政协议纠纷中涉及政府利益和商业秘密的案件一般不被公开，这些案件往往最能体现行政的本质；在刑事案件中，一般轻微伤或自诉案件可能按撤诉或协商处理，一旦撤诉或协商处理，相关定罪样本或要素就无法有效得以统计，计算机自然不能进行深度学习。二是司法数据分类或标记的科学性存疑。计算机是靠代码进行识别的，存在相应的代码才能进行统计或归纳，但对司法案件的代码分类或标记因素会因法官或研究人员的理解差异而参差不齐。例如，刑事判决书中，被告人的犯罪动机、犯罪环境等因素往往很难得到类型化标记；在刑事被告人赔偿案件中，赔偿数额及相关酌定情节也通常属于不被标记的范畴。因此，“这些未被标记的因素便会游离于所得数据之外，继而造成数据充分性问题，导致预测模型失准”〔19〕。三是司法数据的变换性使得精确性不足。在主观性之外，数据所依赖的环境同样重要。换言之，数据样本的真实性与数据所产生的特定环境密切相关，“人们在特定环境中分

〔18〕 王禄生：《司法大数据与人工智能技术应用的风险及伦理规制》，载《法商研究》2019年第2期，第102页。

〔19〕 前引〔1〕，聂友伦文，第68页。

析数据并将意义赋予了数据”〔20〕才能消除样本的分歧增进标注代码的可理解性。然而，也会存在司法异地差异、人为差异等因素导致的数据非真实性或系统性错误，这就会引发“错误的前提导致错误的结论”〔21〕(garbage in，garbage out)，加深人们对人工智能司法决策的误解。

第二，人工智能算法黑箱冲击司法透明，导致司法不公。算法是第二类关键性要素，但算法黑箱问题一直是困扰理论与实务界的头号难题。算法的不透明性大致存在三种情形：一是因国家秘密、商业秘密等保密之需要而形成的不透明，二是因技术的不成熟而引发的不透明，三是人工智能算法内部的复杂性而产生的不透明。〔22〕不论何种情况，由于价值平衡、技术有限以及民众知识差异等因素的制约，算法公开的程度都十分有限。这种限度不仅体现在由计算机技术人员和法律专业人员组成的审查机构审查的广度和深度有限，还体现在审查结果要尽量避免损害私人权利以及抑制新技术创新的负面效应。实践中，这三类不透明性往往交错在一起，加剧算法的不透明性。例如，目前概率建模下司法要素被压缩为几个方面，而采取启发式算法系统可模拟法官的思维，但这种思维决策过程是如何运作的往往无法被“追溯与验证”。〔23〕腾讯研究院也明确表示：“在 AI 深度学习模型的输入数据和输出结果之间，存在着人们无法洞悉的‘隐层’，深埋于这些结构底下的零碎数据和模型参数，蕴含着大量对人类而言都难以理解的代码和数值，这使得 AI 的工作原理难以解释”。〔24〕人工智能算法黑箱易引发的可解释性问题主要是，司法数据的关联性错误、法律适用的歧视性加深、司法决策的结果难以预测以及危及司法的公信力等。在司法关联性数据领域，由于缺乏足够的因果逻辑可能使得看似存在正负增长关联的事件之间，其实是一种虚假关联关系，从而可能错误地揭示司法规律。而由于无法看清司法决策规则，也不能参与其中，只能被动接受决策结果，往往可能导致算法偏见无法纠正而形成“滚雪球”效应，如美国黑人的犯罪率更高。同时，在无法理解算法模型的基础上，也可能导致结果的不可控性，特别是针对实质性的同类案件，某些外在参数不同竟然导致预测结果大相径庭。这种难以接受的算法偏见与歧视，自然也会影响司法的公信力。

第三，技术理性对司法理性的侵蚀导致内在隔阂。相对于算法黑箱而言，技术的有限性侧重于阐释目前人工智能应用于司法领域的技术瓶颈和固有缺陷。在类型层面，人工智能存在“弱”“强”“超”之级别区分，毫无疑问，目前人工智能司法只停留在“弱”人工智能阶段，其司法智能化程度并不高。由于人工智能是一种技术理性，司法决策是一种司法理性，司法理性“更多乃是依靠司法工作人员的认知、心性、德行并结合案件发生的客观现实环境”〔25〕，技术理性偏重于标准化与程式化的规则，因而，技术理性与司法理性之间存在一种天然的隔阂。加之法律语言与计算机语言的差异，法律与技术之间的融合存在较大的跨界障碍。从世界各国司法实践情况来

〔20〕〔德〕罗纳德·巴赫曼、吉多·肯珀、托马斯·格尔策：《大数据时代下半场：数据治理、驱动与变现》，刘志则、刘源译，北京联合出版公司 2017 年版，第 205 页。

〔21〕〔英〕维克托·迈尔、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 211 页。

〔22〕See Jenna Burrell，How the Machine “Thinks”：Understanding Opacity in Machine Learning Algorithms，3 *Social Science Electronic Publishing* 1 (2015).

〔23〕参见马靖云：《智慧司法的难题及其破解》，载《华东政法大学学报》2019 年第 4 期。

〔24〕腾讯研究院等：《可解释 AI 发展报告 2022：打开算法黑箱的理念与实践》，腾讯研究院 2022 年发展研究报告，第 2 页。

〔25〕陈灵峰：《司法人工智能的技术效应与应用边界》，载《求索》2021 年第 6 期，第 186 页。

看，人工智能系统主要运用于数据管理平台建设、类案检索和推送、证据审查和抽检等审判辅助层面，如美国联邦法院的“案件管理和电子案件档案系统”（CM/ECF）、欧洲的 ERP 系统及职位分配管理系统软件（OUT ILGREF）、新加坡的社区司法和裁判系统（CJTS）、韩国的电子案件归档系统（ECFS）等。〔26〕以辅助审判为主的“弱”人工智能司法意味着其决策本身的准确性与应用深度有限，“从某种意义上分析，这种应用程度及准确性缺陷导致的技术保守态度与解释困境是其内部机理不可解释性的重要原因”〔27〕。换言之，越是成熟的越具有实践经历的算法模型，随着时间的推移相应的黑箱问题越能迎刃而解。事实上，在人工智能算法模型建设初期，因计算机技术人员的水平有限、精力以及项目投入不足，经常导致算法模型的粗糙和固有缺陷，而引发不可解释性困境。

第四，逻辑运算对司法正当程序的冲击降低主体认同。法律程序很大程度上是一种交流和沟通装置，同时也是进行个人权益分配、提高商谈效能、保障人们尊严和维护自由主义传统的适当机制。〔28〕在司法领域，正当程序被视为“看得见的正义”的代名词，其首要贡献在于强调司法主体之间的“交往”，即“旨在通过使用符号（包括前符号、符号和元符号），来协调大家的行为和举止，以求得沟通和共识”〔29〕。人工智能司法决策程序的不透明直接导致这种“交往”受阻。在司法自动化模式下，由原告、被告、当事人、法院等多方主体参与的交互式辩论法庭模式，变成输入关键词得出结果的单一形式逻辑运算过程，后疫情时代催生的线上庭审模式一定程度上加剧了司法决策程序的形式化与非透明化。“这样的司法操作模式不仅会严重解构法官的主体性价值，削弱司法进行动态社会整合的内在张力，更会导致法律系统像停止生长的珊瑚礁那样，变成一堆毫无生机的死化石。”〔30〕更重要的是，缺失交往性的人工智能司法决策无法达致哲学层面“他者”向“自我”的身份更新与主体认同，因而就无法得到人们发自内心的司法信仰和精神服从。

第五，人工智能无法答责，引发司法归责模糊。“法律责任的本质是答责，不具有可解释性的人工智能不能自我答责，因此，其无法承担法律责任。”〔31〕责任承担问题又与人工智能的主体地位直接挂钩。意志自由是自我应责的前提，只有明晰责任后果、具有答责能力的人才是自由的主体。而在责任的功能层面上，责任往往与伦理道德一起共同发挥惩罚、修复或预防作用。在 H. D. 刘易斯看来，“责任……仅仅意味着做一个有道德的人，这意味着做一个有能力正确或错误地行为的人，在这个意义上，行为的道德上即相应是好的或坏的”〔32〕。人工智能无论在意志自由抑或道德判断上都无能为力。实践中，人工智能产品的责任承担者往往是在使用者、制造者与监督者之间平衡，但具体如何平衡尚未得出较为权威的规则。人工智能司法

〔26〕 参见郑曦：《人工智能技术在司法裁判中的运用及规制》，载《中外法学》2020 年第 3 期。

〔27〕 翁晓斌、饶淑慧：《人工智能司法决策的可解释性及其路径研究》，载《学习论坛》2022 年第 5 期，第 132 页。

〔28〕 参见〔美〕瑞·L. 马肖：《行政国的正当程序》，沈岿译，高等教育出版社 2005 年版，序言，第 2－10 页。

〔29〕 曹卫东：《交往理性与权力批判》，上海人民出版社 2016 年版，第 126 页。

〔30〕 陈洪杰：《从技术智慧到交往理性：“智慧法院”的主体哲学反思》，载《上海师范大学学报（哲学社会科学版）》2020 年第 6 期，第 90 页。

〔31〕 前引〔9〕，刘艳红文，第 85 页。

〔32〕〔澳〕皮特·凯恩：《法律与道德中的责任》，罗李华译，商务印书馆 2008 年版，第 88 页。

决策责任的模糊问题存在以下两个层面：一是人工智能司法决策错误产生的原因存在多种可能，可能是人工智能代码的错误，也可能是法官操作的失误，还有可能是人工智能技术固有的缺陷；二是人工智能司法决策责任承担的模糊性，由于错误产生背后的原因各异，责任的归属也并非清晰，如人工智能代码的错误或法官操作的失误，这类责任者相对较为明确，但因人工智能技术固有的缺陷所引发的责任，其责任承担者就并非清晰，它有可能是研发者，也有可能是法官，还有可能是国家等。责任者的模糊可能导致司法决策本身的随意与偏见，加大司法者与当事人之间的法律鸿沟，缺乏公平责任的司法体制设计也会使得新技术的应用陷入可解释性“整体危机”。

第六，人工智能无法进行价值衡量，削弱司法正义的基础。人工智能在司法正义判断上的困境也使得算法的可理解性和可接受性大为降低。一者，在法律的适用过程中其无法真正实现“同案同判”，同案本身就是基于两种案件结果价值相似性的判断，而人工智能恰恰无法基于司法正义价值对案情进行整体判断和关照。例如，“于欢案”中涉及对正当防卫制度的重新理解，仅仅将此案编入故意杀人罪一类案件将发生严重的司法不公。换言之，人工智能“无法避免建立‘错误的相关性’，即两个案件尽管具有事实特征上的相似性，但这种相似性却不具有法律意义或不应与法律后果发生关联，而机器学习算法却将其当作了‘链接’法律后果的前提”〔33〕。二者，某些法律价值不存在位阶排序无法进行计算与权衡，这导致算法无能为力。例如，经典的“电车难题”实际拷问的即是生命价值的无可计量性。事实上，在诸多法治之善之间都需要法官依照现实世界的逻辑观和心中世界的正义观作出权益平衡与实质判断，基于相关性的概率计算无法理解大脑神经元“黑箱”，也导致其无法被人脑理解。三者，人工智能有限的数据库和无限的司法要素事物发展之间形成张力。人工智能司法决策是基于已被标记和筛选的过往数据，作旧的数据使得人工智能对新事物的感知能力和关联能力不足，无法应对层出不穷的司法新事物和新形势。例如，部分金融刑事案件的入罪标准需要综合东中西部经济发展状况作出动态平衡，而非采取“一刀切”的算法标准。

三、人工智能司法可解释性的正当逻辑

“我们不可能从对那个时代的详细研究的结果中获知世界大事的意义，即使是这个结果极其完善；相反，我们必须能够创造出意义本身。”〔34〕逻辑分析是客观认识事物意义的前提。人工智能司法可解释性困境的存在说明构建人工智能的可解释性规则存在现实必要性。但这并不等于说构建人工智能司法可解释性规则具有可行性。这首先需要揭示学界关于人工智能司法不可解释性立场的伪科学性，进而构建人工智能司法可解释性规则的逻辑基础。

（一）对人工智能司法不可解释性立场的批判

人工智能实际是计算机科学下模拟“类人智能”所形成的一套计算规则，它的核心技术无疑

〔33〕 雷磊：《司法人工智能能否实现司法公正？》，载《政法论丛》2022 年第 4 期，第 77 页。

〔34〕 前引〔12〕，马克斯·韦伯书，第 9 页。

是算法，算法被定义为“解决某一特定问题而采取一种有限、确定、有效并适合用计算机程序来实现的解决问题的方法，是计算机科学的基础”〔35〕。学界普遍有一种惯常思维，认为可解释性的最大障碍是算法的“黑箱”存在，其导致人工智能司法决策本身具有“黑洞”空间而无法让人理解。但事实真的如此吗？从逻辑上分析可知，这种立场具有伪科学性。

首先，区分事实和价值、实现客观与主观的有限分离是近现代哲学科学的逻辑起点。在法律适用过程中所形成的算法，虽然经过了人的目的性加工，但本质还是一种运算规则或代码符号，是一种客观产物。就此而言，算法并非像人的主观意志一样，是一种不可重复、复制与展示的“黑箱”，而是一种可探知、重复的客观物质。物质主要有四类特征，即遵守能量守恒定律、具有可探测性、时空有限、遵循因果规律，正是由于人工智能不具有意识这类非物质特征才使得其不能成为人性主体。〔36〕作为一项可重复的运算规则，算法具有高度的形式化特征。算法通常只有三种运算规则，即“是”“非”“或”，其根据相应的技术代码植入，作出相应的精确性指令。就此而言，打破算法“黑箱”或还原算法的自主运算过程在逻辑上是可能的，只不过是技术或成本问题。例如，在司法决策过程中，虽然根据正当防卫这一指令，相应的算法会进行海量数据筛选与深度学习辨识，但得出的结果与基础要素之间总是存在一些线索或访问痕迹，如一些关键性的基础数据要素，包括“侵害”“反击”“急迫”“平衡”等，明确两者之间的关联性需要相当高的支撑技术，但不代表不可能。而这即是物质客观性与实在性的体现，也是可解释性的客观性基础。

其次，按照前述常规思维路径，算法存在“黑箱”等因素，导致或加剧算法的歧视，因此，这种算法歧视是人工智能固有的缺陷，致使人工智能决策的可理解性和可接受性锐减。但实际上，算法决策的“歧视”或“不公”归根结底还是现实社会中制度、规则不公的真实映射。一个很典型的案例即是，如果司法层面习惯报道黑人犯罪事件或选择性公开黑人犯罪数据，那么经过大数据的推演所得出的结论自然是，黑人是犯罪的高概率群体，黑人无疑被贴上犯罪标签。显然这种歧视并非算法“黑箱”所导致的结果，而是社会歧视本身的映射。与此同时，另一种情况是，算法本身是一种中立的统计或分配规则，但人们的固有情愫往往认为一种算法规则比另一种更公平。例如，在美国教育平权案中曾存在两种招生录取算法，个体主义的直接加分规则和特定群体的倾斜加分政策。初看之，对特定群体的倾斜加分政策会比个体主义的直接加分规则更易引发“反向歧视”，但事实不然，从算法结果角度而言，无论是个体主义进路（加分政策），还是群体主义进路（配额政策），都旨在提高某些族裔（特别是黑人）的录取率，都不过是一种“纠偏行动”（affirmative action）。〔37〕就此而言，算法本身并非价值中立或非中立，真正的问题在于如何选取适当的“基于社会效果的法律解释模式与方法”。

最后，退一步而言，即使存在算法“黑箱”，也是因人的社会活动及相应规则所致，而非物

〔35〕〔美〕塞奇威克、韦恩：《算法》（第4版），谢路云译，人民邮电出版社2012年版，第1页。

〔36〕参见程承坪：《人工智能：工具或主体？——兼论人工智能奇点》，载《上海师范大学学报（哲学社会科学版）》2021年第6期。

〔37〕参见丁晓东：《算法与歧视——从美国教育平权案看算法伦理与法律解释》，载《中外法学》2017年第6期。

质（算法）的不可知性。例如，在客体层面，基于司法领域的国家秘密、商业秘密、个人隐私以及知识产权的保护之需要，需要对算法决策系统的数据及规则进行保密，防止黑客攻击、商业剽窃以及隐私泄露的风险，这就导致数据的秘密性；在主体层面，人工智能司法运算场域内的主体知识结构多元，虽然计算机专家熟知算法代码，但法官及诉讼当事人未必理解晦涩难懂的计算机语言，司法算法模型中的许多代码与标量并非像“年龄”和“性别”一样清晰，它往往具有更为抽象的行为序列或模拟符号特征，某些代码与标量也难以用人类语言或可视化图表予以标记。〔38〕在此情况下，一定程度的算法“黑箱”是因这个时代发展过程中主观或客观性制度而延伸的一种“遗产”。真正需要解决的问题是，提高人工智能司法的问责程度和及时提供救济的能力，从而保障当事人的诉讼权利，实现司法公平。利用法律解释和裁判说理等程序方式提高人工智能司法决策的透明性与可理解性，只是直接目的而已。

（二）对人工智能司法可解释性逻辑基础的挖掘

1. 人工智能司法可解释性的认知基础

人工智能司法可解释性的认知基础是指法律文本可通过相应的符号转化成为计算机语言，并促成法律解释到法律解析的飞跃。法律语言转化为计算机语言的核心问题是，法律概念的形式化。而恰巧法律概念具备形式化的条件，这是可解释性的认知基础。

一方面，法律概念形式化的基础在于法律的形式理性，这使得法律规则和算法规则逻辑趋同。在基本结构上，算法主要是一种数字逻辑规则，0 或 1 是其运算的基本参数。而法律为实现规则的精确性与稳定性往往借用数学、经济学、逻辑学等运算规则或符号予以推理论证与表达，如司法机关法律文书效力的公法经济分析，必然涉及数学函数的表达。因此在某种意义上，两种规则实际是置于相同逻辑范式下应用于不同领域的语言体系而已。在运行模式上，算法的认知逻辑无非是基于数据的偏好、节点的分析与预测；在类型上，符号主义认识模式侧重符号逻辑的推理，联结主义认知模式侧重数据单位之间的节点关联性，行为主义认知模式则更加强调强化学习的重要性。与之相比，法律规则在运行模式上也是对主体行为进行提前预设与编入，法律适用的过程大多是一个三段式的自动化应用过程，符合算法符号主义认知模式的基本逻辑。因此，基于本体推理方法的自动化适用是两者共同的运行逻辑。在结果面向上，人工智能在司法裁判领域的运用具有正当性，能够从海量的司法裁判文书中提炼出案件事实、类型、引用的法律法规及判决结论等关键信息，而大部分裁判要素信息都具有类同性与可重复性，通过算法决策自动化能够提高裁判的效率和准确性。就此而言，法学和计算机学都在致力于解决秩序的稳定性问题，计算机法学应运而生。

另一方面，法律概念形式化的表现在于本体要素的提出，这可以实现法律概念知识和计算机算法符号之间的互通。本体要素是指在给定领域内概念的要素化与具象化，以及各个要素对象之间形式化的、明确化的一般性规范结构。通过抽取法律现实生活中概念的本体要素，并以计算机代码标记之，就能对相应的法律规则进行“运算”，得出法律适用的结论。在此，本体要素提供

〔38〕 See Lilian Edwards，Michael & Veale，Slave to the Algorithm? Why a “Right to an Explanation” is Probably Not the Remedy You are Looking for，16 *Duke Law and Technology Review* 18 (2017).

的正是计算机算法运行的“知识概念词汇表”〔39〕。按照本土要素的一种常规提炼方法，首先，需要对一个法律规则进行文本范围分类，确定为哪种法律领域或部门法系统下的法律规范信息；其次，需要对法律规则的规范类型进行认定，如是授权性规范、义务性规范抑或禁止性规范等；再次，需要对法律规范的逻辑结构进行提炼，通常一个完整的法律规则包括假定条件、行为模式和法律后果，有些会省略法律后果或假定条件，但行为模式必不可少；最后，需要对法律规范中存在的一些附加信息进行归类提炼。例如，非结构化信息管理架构类型系统“卢依马系统”，将司法判决按照在法律论证中的功能差异进行层级类型化，一共列出了 9 个层级，分别是对法律规则的“引用”、锁定“法律规则”、寻找“法律裁定或法律裁判”、挖掘“基于证据的事实发现”与“基于证据的中间推理”、提炼“证据”、明晰“法律政策”、形成“基于政策的推理”、得出“特定案例的过程或程序事实”。〔40〕这些法律句子的层级类型化对法律论证检索非常有用，能够对给定的案例文本进行三段论的注解，即案例适用的法律规则是什么、提炼哪些可以支撑法律规则适用的证据以及这些法律规则的渊源来自哪里，由此能快速实现法律论证的自动化搜索。这也说明，司法裁判领域的人机协作具有较大的潜力。

2. 人工智能司法可解释性的制度基础

从现有的法律规范体系来看，可解释性存在较多的制度与规范基础。首先，以知情权、参与权为核心内容的行政参与及信息公开制度是促进可解释性的公法基础。行政参与制度主要体现在行政正当程序的告知制度、阅览制度、听取意见以及异议制度，它是对抗算法权力“黑箱”及异化的主要手段之一。在司法领域，裁判说理制度可以通过对裁判依据、事实、理由及结论的阐释、说明与公示实现裁判过程的公开，裁判文书上网增强了司法裁判的透明性；同时在司法决策过程中存在的最后陈述、当庭宣判、上诉告知等程序机制有利于保障诉讼当事人的参与和知情权。其次，以信息披露、风险预警及责任分担为核心内容的市场合规与监管机制是促进可解释性的私法基础。市场交易强调意思自治与公平竞争，通过告知、披露、风险提示及事后责任等法定义务的设置实现交易双方信息的对称性。例如，在《民法典》《消费者权益保护法》以及金融、证券、医疗、科技等特殊行业的法律法规，都规定了在涉及个人权益、公共利益及市场秩序保护的领域，相应的技术人员、工作人员承担告知、风险警示、信息披露等法定义务。人工智能司法决策系统作为一项市场交易产品也必须遵守市场交易规则，以保护消费者（诉讼当事人）的健康权、知情权及相关权利。最后，以数据权和算法解释权为核心内容的权利保障制度是促进可解释性的混合基础。一方面，数据权是促进可解释性的间接基础。数据权是一项混合型权利，权利的核心在于如何保护数据中包裹着的个人利益信息并协调数据利益冲突形态，“在数据企业对数据要素化利用的普遍期待之外，用户和数据企业同业竞争者对于数据的利益期待之有无，取决于商业模式中所利用的数据是否承载个人信息以及是否处于公开状态”〔41〕，基于“知情同意规则”的

〔39〕〔美〕凯文 D. 阿什利：《人工智能与法律解析——数字时代法律实践的新工具》，邱昭继译，商务印书馆 2020 年版，第 211－212 页。

〔40〕 参见邱昭继：《人工智能、法律解析与未来法律实践》，载《政法论丛》2022 年第 4 期。

〔41〕 沈健州：《数据财产的权利架构与规则展开》，载《中国法学》2022 年第 4 期，第 100 页。

数据利用已成为商业数据产品开发的首要原则，用户对数据的异议权、更正权及删除权可大幅度促进算法的可解释性与透明性。另一方面，算法解释权是促进可解释性的直接基础。一般认为，直接创设算法解释权的法律依据是 2018 年欧盟实施的《通用数据保护条例》（GDPR）第 7 部分“数据主体的权利”下面的“自动化个人决策相关权利”一节第 4 条，其明确指出：“对该条款所涉及的任何处理，都应当采取适当的保障措施，包括向数据主体提供具体信息以及要求人为干预、表达其观点、要求对此类评估后作出的决策进行解释以及质疑此类决策的权利。”国内学者基于此提出了构建本土算法解释权的基本思路及构想，〔42〕通过证成算法的权利属性，增强国家机关、市场责任主体等的信息公开及阐释义务，打开算法“黑箱”歧视的救济通道，从而提高人工智能的透明性。

四、人工智能司法可解释性困境的纾解之道

传统观点认为：“司法的本质是理性，法律推理是一种理性过程，裁决者不能有利益、感情牵涉，中立是最基本的要求。”〔43〕显然，这样的一种观点有夸大司法客观性之嫌疑。正如任何一种法治都有其政治基础一样，任何一套司法体系都是当代社会制度综合的结果。司法作为一种法律运用，既是一种实践理性（practical reason），同样也是人类精神的高级“创造状态”，“是一种不可模式化的实践巧智慧”〔44〕。在理性主义和非理性主义立场之间保持张力平衡正是司法的艺术。人工智能司法在某种意义上有利于保持司法价值判断之客观化，但这又与法秩序规则之主观化存在一定的抵牾。因而，人工智能司法既有必要、也应始终处于客观性与主观性的平衡和交融之中，客观性主要是从制度与机制着手，主观性主要是从人的认识层面着手。解决人工智能司法的可解释性悖论也需要从客观性与主观性平衡和交融的角度来思考。具体包括以下对策：

（一）构建司法信息公开共享制度，提高有用数据的甄别与利用效率

信息公开是人工智能司法可解释性的制度基础。传统的信息公开，一是主要停留在政府管理层面，二是主要强调“知情权”而未突出信息的共享与使用。公共数据共享是一种以数据利用和公平赋权为核心价值目标的公共服务，它突破了政府信息公开在主体、范围和结果上的限制，将其提升至为社会公众创造共同财富的高度。它是一种以“权力—权利”作对位的双向互动法律结构，使国家拥有一定的数据配置权并承担合理利用义务，使公民拥有获取公共数据资源的权利并承担不予滥用的义务。“在这种结构中，国家不是简单地对数据资源进行控制、支配和管理，也不是放任私人自由攫取和使用数据资源，而是建构并维护一种公平合理的数据利用秩序，促进公

〔42〕 参见张恩典：《大数据时代的算法解释权：背景、逻辑与构造》，载《法学论坛》2019 年第 4 期；姜野、李拥军：《破解算法黑箱：算法解释权的功能证成与适用路径——以社会信用体系建设为场景》，载《福建师范大学学报（哲学社会科学版）》2019 年第 4 期；解正山：《算法决策规制——以算法“解释权”为中心》，载《现代法学》2020 年第 1 期；张欣：《算法解释权与算法治理路径研究》，载《中外法学》2019 年第 6 期等。

〔43〕 陈端洪：《司法与民主：中国司法民主化及其批判》，载《中外法学》1998 年第 4 期，第 39 页。

〔44〕 雷磊：《类比法律论证——以德国学说为出发点》，中国政法大学出版社 2011 年版，第 3－4 页。

共数据利用的开放性、公平性、效益性。”〔45〕司法数据共享可转变单向度的司法数据公开现状，将司法数据作为一种有效益的权利资源，促使司法参与者以更加积极的权利主体身份参与司法运行的全过程。同时，权力享有者也应努力提高自己维护公平合理的司法数据共享的意识，仅仅停留在裁判说理制度、裁判文书公开制度等是不够的。一方面应为人工智能司法决策提供更为真实、全面的基础样本，另一方面应为诉讼当事人及民众提供更为准确的司法判决指引。事实上，在既往的刑事案件领域，涉黑、贪污等部分案件与国家层面的刑事政策密切相关，由于存在信息的不对称，部分案件的司法决策过程存在较大的不透明性，这也影响了人工智能在此领域的运用和发展。在新媒体赋权下，部分案件虽通过司法场域的外部系统予以披露，但也会形成基于个别律师单方面发表过激言论的负面情形。倘若司法等职能部门能够采取“充分和具有选择性的开放式许可”〔46〕模式，将传统的司法信息公开转化为公平的数据利用，可以更好地预见人工智能在此领域应用的潜在风险，提高司法决策的效率与可接受性。在具体实施层面，司法信息公开共享制度是前提，制度的最终意义在于实现对有用性数据的甄别、筛选及应用，使之应用于人工智能司法。目前，最高人民法院法院网、中国司法裁判文书网、北大法宝网以及地方法院裁判网提供了不少裁判文书信息，但有效数据仍存在不足。需要联合司法部门、行政部门建立合作机制，推动相应的有用数据的甄别与利用，为人工智能司法提档升级铺路。

（二）从软硬法结合视角建构司法系统的运行标准与制度规则

引发人工智能司法决策不可解释性与多重困境的一个重要原因是，人工智能重塑和颠覆了传统的法律关系结构，引发法律变革，但相应的制度规则及运行标准并未完全建立，如人工智能司法决策模型黑洞问题、人工智能司法决策程序漏洞问题、人工智能司法决策责任模糊问题等，即是由人工智能司法系统的决策标准、程序标准及责任标准与规则未能完全明确而导致。然而，从一个体系层面而言，完善人工智能司法系统的运行标准与制度规则并非仅仅依靠单一的“国家法”手段，还应将“社会法”“行业法”等软法统筹进来，实现硬法和软法的融合、公法和私法的合力。硬法层面主要是设定禁止性规范和义务性规范，这是对算法决策危险的及时禁止和基本权利的救济，主要活跃在公法领域。例如，欧盟《通用数据保护条例》（GDPR）第 22 条第 1 款就对完全自动化决策进行了“一般性禁止”，即“个人有权不受完全依据自动化处理作出的且对其产生法律或类似重大影响的决策的约束”，这也被称为一般性“反对权”，其主要目的是实现“算法控制者不得通过编造的人为干预而规避对自动化决策的一般性禁止，任何名义上或象征性的人工干预均不对自动化决策构成实质性影响”〔47〕。与之相比，美国并未进行统一的立法禁止性规制，而是突出行业规则和依靠法院的算法解释规则。例如，在美国量刑领域的人工智能算法的主要问题是算法解释请求权的法律基础，从现有的依据来看，宪法领域的正当程序权利可作为宽

〔45〕 王锡锌、黄智杰：《公平利用权：公共数据开放制度建构的权利基础》，载《华东政法大学学报》2022 年第 2 期，第 63 页。

〔46〕〔美〕瑞恩·卡洛、迈克尔·弗鲁姆金、〔加〕伊恩·克尔编：《人工智能与法律的对话》，陈吉栋、董惠敏、杭颖颖译，上海人民出版社 2018 年版，第 171 页。

〔47〕 A29WP，A29 WP，Guidelines on Automated Individual Decision—making and Profiling for the Purposes of Regulation，2016/679，17/EN. WP 251rev. 01（Feb. 6，2018），转引自前引〔42〕，解正山文，第 183 页。

泛的权利基础，不仅包括传统的知情权，还包括正当性的解释权，后者是一种真正的“解释权”，即被告可以毫无限制地获取源代码以及算法结果所依赖的逻辑的权利。〔48〕通过已有的法律法规体系及权利请求规制与救济通道，实现权利对权力的规制。软法方面主要是设定行业安全标准和构筑自我规制体系，这是对算法决策风险的及时预防和侵权的救济，主要活跃在私法领域。从人工智能司法解释义务的场景化标准类型来看，它属于公共事业领域的一种衡量标准，相比于一般商业领域而言，在合理性和透明性方面具有更高的要求，在系统上线投入市场使用前，需要经过较为严格的安全性测试，包括安全性、准确性、稳定性、可靠性、保密性等基本要求，同时还必须形成体系化的设计标准、性能标准、运行标准、监管标准、救济标准等。除了行业的自律标准外，算法侵权救济必不可少，即人工智能司法本身出现歧视等大规模侵权事件时，可考虑借鉴欧盟《通用数据保护条例》（GDPR）的代表机构追偿模式，实现群体司法案件的同类化、集约化处理。

（三）从全过程视角强化主体之间的协同治理

人工智能司法决策的治理是涉及多元主体、多个领域的复杂互动与联合规制的议题。因此，不仅需要形成明确的人工智能司法系统的运行标准与制度规则，还需要考虑在司法内部和外部复杂的互动过程中调试出覆盖全过程、全流域的协同治理机制。在聚焦制造主体首要义务、解释模型推进，利用主体审慎义务、解释权的保证，监管主体规制义务、责任公平分担，对象主体反馈义务、合理公平救济的同时，还需要结合内部和外部视角、技术和法律标准、道德和伦理要求、社会和国家互动关系构建一种超越单一权利或权力标准的协同治理机制。其一，从制造主体的角度看，需要强化培育者的信息控制能力与善良动机，从自我规制的角度实现信息与技术的风险控制。问责机制是算法实施透明的重要保障机制，但问责通常具有事后性，通过正面激励和反向问责的双重机制实现培育者的风险自控。其中包括对人员的规制、对算法决策风险管理的目标设定以及完善算法决策风险影响评估制度。例如，欧盟的“AP29 指南”对算法培育主体的治理提出了这样的要求：“企业应当构建有效的内部监督机制，对个人将产生重大影响的算法应当向内部独立的数据保护官提供影响评估的相关信息。同时，企业内部技术团队应当配备专业权威人员对系统的准确性负责，确保其信息可被公众获得，并为救济制度随时启动奠定基础。”〔49〕其二，从利用主体角度看，司法机关需要坚持“技术制衡技术”〔50〕的理念，即提高自身对技术的把握程度，善于将司法规则和理念“代码化”或者“技术化”，将抽象的规制原则或理念转换为实际场景运用规则，防止出现被机器人操控的未知或盲目自信的利用过失。例如，司法机关对人工智能模型的可解释性需要进行审查与评估，可建立由法学专家牵头，吸纳计算机、人工智能、哲学、心理学等多学科交叉领域的专家组成的统一委员会，事前对可解释性的内在透明性进行审查与评估，事后对可解释性的结果保真性与一致性进行认定与审查。其三，从监管主体角度看，主要利用的是一种回应型规制，即将“威慑式规制策略”和“遵从式规制策略”结合起来的混合型规制模式，〔51〕

〔48〕 参见前引〔42〕，解正山文。

〔49〕 张欣：《算法解释权与算法治理路径研究》，载《中外法学》2019 年第 6 期，第 1443 页。

〔50〕 张涛：《探寻个人信息保护的风险控制路径之维》，载《法学》2022 年第 6 期，第 68 页。

〔51〕 参见〔英〕罗伯特·鲍德温、马丁·凯夫、马丁·洛奇主编：《牛津规制手册》，宋华琳、李鸽、安永康、卢超译，上海三联书店 2017 年版，第 134－135 页。

既设置严格禁止、处罚等规则，又强调合作、教育、说服、指导等柔性治理手段，以实现人工智能司法行为的事前、事中与事后规制的全覆盖。其四，从对象主体角度看，要提升自己对人工智能风险的识别，加强沟通，及时作出反馈和救济请求。对象主体主要是指诉讼当事人，也包括律师和其他诉讼参加人，事实上，在线上立案、庭审、结案、电子化文书送达等智慧法院模式建设以来，部分诉讼当事人未能完全适应与转化过来，导致其在智慧法院模式中的被动，甚至不知所云，这自然也会加深对人工智能司法的误解及风险的不可控，因而建立常态化的沟通和反馈机制必不可少。

（四）通过指导性案例和司法解释赋权法官司法解释空间，提高法律解释技术

法律结构的不明确是导致人工智能司法技术难以有效运用的认知障碍之一。虽然在理性实践主义的引领下，法律结构一直被形式化与教义化，但作为法理学上“恼人不休”的话题之一，法律语言的“空缺”和法律结构的开放性，导致司法判例总是存在不确定性。如哈特所言：“英国的判决先例‘理论’对于使用判例实务的理论描述，在某些点上仍旧具有高度的争议：的确，即使在理论当中，‘判决理由’（ratio decidendi）、‘案件事实’（material facts）、‘（法律）解释’这些关键词，也含有不确定的阴影地带。”〔52〕由于不确定性概念和开放性结构的存在，按照对立法冲击程度的排序，法官对法律的适用存在法律解释、法律续造和填补立法几种可能的情形，越是靠后要求法官的能动性越大，因其对现有的法秩序冲击也愈大，受到法体系的限制也越高。我国不是判例法国家，原则上法官适用法律的模式被限定为法律解释和狭义的法律续造，即不可突破法律体系内的限制，主要是对模糊法律语言的一种具体化与情景化解释，以能够让一般民众所理解。实现人工智能司法的可理解性，并非消除法律语言的模糊性和法律结构的不确定性，而是要找到计算机语言和法律语言的衔接点。事实上在形式理性的形塑下，法律规则和算法规则逻辑具有较强的契合性。但这又引发了另一问题，法律不确定性概念和开放性结构如何合理、有效地形式化。法典化是一体解决法律不确定性和开放性的一种手段，但企图一劳永逸的立法又将陷入脱离社会基础的风险。面对这种双向悖论，解决方法一方面是努力增强法律结构的明确性，保持法律规则和算法规则有较高的契合度；另一方面是承认两者之间的裂缝，通过激发法官的创造力、提高法律解释技术，积累更多真实、合理、有效的判决文书，为人工智能学习系统提供实践的“智慧数据”，最大程度弥合裂缝。实践中，通过指导性案例肯定正面的法律解释、赋权法官的司法解释空间，是激发法官的创造力、提高法律解释技术的一种有效途径；在一定的司法解释领域和范围成熟后，还可出台专门的司法解释指导意见，进一步促成法律解释的明确性与透明性。

（五）强化交叉学科人才建设，提高对人工智能司法决策模型的引领

司法算法决策模型设计的合理性、正当性是人工智能司法决策透明性和可理解性的关键要素之一，决定算法决策模式可解释性的核心指标又在于参数的明确程度，参数的明确程度分为模糊型、明显型和外显型三种。例如，在美国的刑事司法实践中 COMPAS 智能量刑模型，不仅采用

〔52〕 前引〔6〕，哈特书，第 199 页。

了标准回归算法，还结合了以实践司法数据筛选为基础的智能学习与分析模型。〔53〕虽然能够打破传统的机械量刑弊端，但对智能算法深度学习的过程和结果可理解性提出了更高的要求。在提高透明性的菜单中有一种溯源机制，即借助区块链技术，将算法过程用分布式账本的形式进行记录，形成过程的不可更改性和结果的可溯源性，解决了运算过程的步骤难以理解的难题。〔54〕目前，我国司法人工智能领域的实践状况是：在参数层面未能充分保障数据的真实有效性，同时缺乏有深度的智能学习与分析司法模型；在解释技术层面也缺少相应的成熟的支撑基础和机制。对于参数基础而言，有学者进行过调研，发现“当下不少所谓的法律科技公司或研究团队严重依赖自己事先假定的知识图谱来提取、印证规范化的裁判模式，其打造的裁判模式可能严重脱离实践模式……稍微复杂的文书识别往往极其困难，因为机器识别在抽取多样、微妙的语言时经常出错，从而影响到大样本材料提取的准确性，最终给出误差很大甚至错误的解读”〔55〕。对于深度学习技术而言，传统法学界习惯于法教义学的推理论证，倾向于定性分析而薄弱于定量分析，学科之间的交融深度有限，很大程度上限制了“面向实践的、统计式的、机器学习介入的研究范式、裁判模型机制”〔56〕的打造。因此，我们加强对人工智能司法决策模型的引领，还需要在参数和深度学习技术层面进行努力，不仅需要更为可靠有效的参数，更需要科学合理的学科交融研究范式、计算机解释及运用技术。在实践层面，一个有效的途径是强化交叉学科人才培养。在目前的学科评估体系中，国内高校，特别是双一流或重点高校可充分利用学位自主审核权以及学科自主评估的机遇，强化交叉学科建设，实现人工智能、法学以及相关学科领域的大融合，为人工智能司法决策模型引领提供人才保障。

（六）发挥法官的自律与能动性，实现司法智能决策的人机协同

在真正的奇点到来之前，人工智能都只是人类意志的一种“延伸”。而真正具有自主意识的人工智能出现时也意味着人类命运将被改写。因此，只有在人类中心主义下人工智能司法才有讨论价值。但是，这也让人工智能司法决策嵌入了司法正义判断困境这一基础性缺陷。由于这一缺陷的根本性，它事实上是难以根除的。司法正义的实现是一个法官运用经验、利益衡量、价值判断、法律解释、制度实施的“司法—社会”互动的过程，“法官在‘司法—社会’的互动中，主要以语言为载体，处理复杂社会关系中的纠纷，司法裁判的形成与其说是是非曲直的判断结果，毋宁说是一场规范与实践之间互动商谈的对话结果，并以此为人们确立了未来的行动标准和行为方向”〔57〕。人工智能的技术即是对人脑海量信息运算不足的弥补，但人工智能必须接受人类规则的规制。在此，经常提及的是人工智能的伦理规制，例如，2017 年“阿西洛马会议”提出的 23

〔53〕 See Megan T. Stevenson & Jennifer L. Doleac, Algorithmic Risk Assessment in the Hands of Humans, available at http://humcap.uchicago.edu/RePEc/hka/wpaper/Stevenson_Doleac_algorithmic-risk-assessment-humans.pdf, last visited on Nov. 25, 2022.

〔54〕 See Ilaria Tiddi, Freddy Lecue, Pascal Hitzler et al., *Knowledge Graphs for Explainable AI—Foundations, Applications and Challenges. Studies on the Semantic Web*, IOS Press, 2020, pp. 243 - 261.

〔55〕 左卫民：《AI 法官的时代会到来吗——基于中外司法人工智能的对比与展望》，载《政法论坛》2021 年第 5 期，第 11 页。

〔56〕 前引〔55〕，左卫民文，第 12 页。

〔57〕 胡铭、宋灵珊：《“人工＋智能”：司法智能化改革的基本逻辑》，载《浙江学刊》2021 年第 2 期，第 22 页。

条人工智能原则。事实上，法律的实施也需要伦理规制，两者都需要人性之善的引领，“有理智的欲望又需要善的价值引导，能够给人们带来好处或益处，而什么是好处或益处则需要有所共识”〔58〕。未来人工智能在人工智能司法决策中完全有可能承担主要作用或主要任务，但司法智能决策的人机协同不在于工作承担量之大小，而在于价值的引领和方向的引导，即遵循国际、国内同行的法律行业标准，坚守司法正义，回应人民诉求。实践中重在对法官进行相应的培训与指导，解决的办法是，对法官进行培训与规训，使其在自律的基础上对人工智能的价值目标不断进行矫正与引领。

五、结语与展望

大数据时代，“人工智能＋”的模式已然成为推动生产力发展的重要手段，人们的生活、工作、环境场域乃至思维方式都在发生大革命。人工智能司法有利于推动法律适用走向一个新的发展阶段、获得新的认知价值。但作为一项计算机认知技术和推理规则，它在面对法律的模糊性、开放性和价值性时不免遇到形式化规则和实质化正义之间的张力。人工智能司法可解释性悖论是这种张力外化的一种表现，消解人工智能司法的可解释性悖论也成为时代发展不可回避的课题之一。人工智能司法可解释性问题主要涉及基础数据、目标任务、算法模型以及人的认知这四类关键要素。但从理论层面而言，人工智能司法可解释性悖论是一个伪命题，这种悖论可以从认知基础和制度基础两个方面进行消解。基于认知基础和制度基础的可解释性基础，也衍生出客观主义和主观主义两种消解悖论的路径，具体包括：构建司法信息公开共享制度，提高有用数据的甄别与利用效率；从软硬法结合视角建构司法系统的运行标准与制度规则；从全过程视角强化主体之间的协同治理；通过指导性案例和司法解释赋权法官的司法解释空间，提高法律解释技术；强化交叉学科人才建设，提高对人工智能司法决策模型的引领；发挥法官的自律与能动性，实现司法智能决策的人机协同。

当然，人工智能司法在运用的过程中要考虑全国各地的实际情况。我国是一个幅员辽阔、区域差异化较大的社会主义大国。大国治理既要注重法治统一，又要注重地区差异。人工智能司法技术在各地区运行过程中，必然会存在技术差异、场景差异以及案件类型的差异。例如，在技术层面，东部地区更为先进与普及，而西部地区相对落后和短缺；在场景层面，在司法数据收集、司法辅助审判和司法决策中算法的精确性存在差异；在类型层面，刑事案件、行政案件以及民事案件对证据的关联程度以及因果链条的要求逐渐降低，人工智能决策可解释性与透明性的要求也有所差异，同时各地方在应用人工智能司法的重心存在差异，如云南地区比内部省份对毒品犯罪的司法智能审判更高。基于这些差异，人工智能应当根据具体技术水平、场景要求、案件类型等因素对司法进行差异化介入，而非打造普适性人工智能司法决策系统，在全国范围内无差别性地推广。

〔58〕〔美〕阿拉斯代尔·麦金泰尔：《现代性冲突中的伦理学：论欲望、实践推理和叙事》，李茂森译，中国人民大学出版社 2021 年版，第 11 页。

人工智能司法治理是一项长期工程，需要以回应时代需求的态度加强人工智能司法决策解释机制、运行程序、问责制度、影响性评估、监管组织架构等核心议题的研究，同时深化司法改革步伐，注重法律价值和技术理性的平衡，以实现占领未来人工智能司法高地的战略目标。

Abstract: Strengthening the research on the development and risk of artificial intelligence justice is a topic of the times, in which the interpretability dilemma of artificial intelligence justice is particularly critical. AI judicial interpretability refers to the comprehensibility and transparency of judicial decisions or behaviors, involving four key elements: basic data, target tasks, algorithm models and human cognition. Unexplainable dilemma is mainly caused by factors such as data failure, algorithm black box, limitations of intelligent technology, decision-making procedures and lack of value. However, the unexplained paradox of AI justice is actually a false proposition, which has two aspects of cognitive and institutional basis. The specific strategies to relieve the dilemma include building a judicial information public sharing system and improving the screening and utilization efficiency of useful data, constructing the operation standards and system rules of the judicial systems from the perspective of the combination of soft and hard laws, strengthening the collaborative governance between the subjects from the perspective of the whole process, empowering judges with judicial interpretation space and improving legal interpretation technology by guiding cases and judicial interpretation, strengthening the construction of interdisciplinary talents and improving the guidance of AI judicial decision-making model, giving judges scope for their self-discipline and initiative, and realizing the human-computer coordination of judicial intelligent decision-making. In the future, it is not only necessary to grasp the balance between judicial value and technical rationality, but also need to consider the differential intervention of AI in justice, so as to promote the realization of AI judicial strategic objectives.

Key Words: artificial intelligence, justice, algorithm, explainability, collaborative governance

（责任编辑：赵　真　赵建蕊）

财经法学 No. 3，2022
pp. 16 - 28

公共决策算法的程序规范
——以立法性算法为例

刘佳明*

内容提要：立法性算法是有权机关依照一定程序使用的、能够对公民权利义务产生实质性影响的公共决策算法。与传统立法一样，立法性算法会改变社会资源的分配格局以及人们行为的活动空间，甚至能对公民的权利和义务产生实质性影响。但是，立法性算法所固有的技术性特征，规避了公众对立法性算法程序设计的参与和监督。一方面，构成立法性算法的人工语言与普通公众熟知的自然语言之间存在巨大鸿沟，普通公众因不具备人工语言相关基础知识，难以在算法程序设计中与之进行平等对话和有效沟通，从而使得作为民主性补充渠道的公众参与难以有效进行，进而可能引发监督失效、权责失衡的问题。另一方面，立法性算法会不自觉地嵌入设计者的个人偏好和价值判断，它并不能完全展现“技术中立”理想下的客观和真实，甚至还会出现偏差，从而可能引发算法寻租和算法滥用的问题。要克服立法性算法的缺陷，就要求算法程序的设计必须以透明度和问责制为主要原则，确保公众对立法性算法的充分参与和必要的权利救济途径。

关键词：立法　算法　立法程序　立法性算法　公共决策算法

在法学领域，有关算法的研究主要聚焦于讨论算法与法律之间的内在关系。或是将算法视为法律，认为人类正逐渐成为算法统治的客体；〔1〕或是将法律视为算法，认为法律职业者面临即将被算法所取代的危机；〔2〕或是认为算法和法律二者是协同共生的关系，寻求用算法推动法律、用法律规训算法的双向规范策略〔3〕。也许“算法即法律”在当前还言过其实，〔4〕但是，不可否认，

* 刘佳明，南京大学法学院博士研究生。

〔1〕 又称“算法法律化”，即人类正逐渐进入算法统治的时代。参见郑戈：《算法的法律与法律的算法》，载《中国法律评论》2018 年第 2 期。

〔2〕 也称“法律算法化”，即法律职业者的推理和判断在多大程度上能够被算法所取代，或者说，法律在多大程度上能够被算法所取代。参见胡凌：《人工智能的法律想象》，载《文化纵横》2017 年第 2 期。

〔3〕 算法和法律二者是协同、共生的关系，即算法和法律相互影响。参见马长山：《智慧社会的治理难题及其消解》，载《求是学刊》2019 年第 5 期。

〔4〕 参见陈景辉：《人工智能的法律挑战：应该从哪里开始?》，载《比较法研究》2018 年第 5 期。

无论在私人领域还是公共领域，人类越来越依赖于算法来进行相关决策。通过将大数据分析和预测技术相结合，算法主体透过算法技术有能力增强其对公民的影响力甚至控制力，从而能够在事实上扩张自身的权力，并实质性影响到公民的权利义务关系，因而必须通过法律对此进行有效规制。〔5〕但是，当前对公共决策领域中算法的规制未能深入系统内部的运行逻辑，导致权力主体对通过程序执行法律的背后行动理由未能提供合理论据和说明，因而也就难以有效应对可能出现的算法寻租和算法滥用问题。对此，应当将公共决策领域中的一部分算法视为立法性算法，从而将立法的民主化和科学化价值导向渗透到算法程序的设计之中，并通过信息公开、公众参与和专家辅助等制度，以民主机制和正当程序保护对算法程序设计的共同体进行持续有效的监控、质询和改造，从而促进立法性算法“黑箱”的程序性净化。

一、何为立法性算法

（一）何为算法

目前学界关于何为“算法”尚未达成共识，有关算法的概念在计算机科学、数学和人文社科等领域不尽相同，试图为算法寻找一个能够涵盖所有领域的概念十分困难。在计算机科学领域，算法被看作是用某种方法解决问题的策略机制，它被具体化为一组准确且完整的描述或一系列清晰的指令。在数学领域，算法则通常被用来描述解决某一问题的操作步骤，它们可以通过数字符号、算盘、图表和计算工具等来执行。〔6〕人文社科中所讨论的算法主要是决策算法，“即在特定情况下所采取的最佳行动，对数据进行最佳解释的算法，这些算法能否增强或取代人类的分析和决策，通常取决于数据和规则的范围或规模”〔7〕。一般而言，针对任何可用于计算的程序操作或决策过程，都可以归入算法的认识范畴，但是，这并不意味着所有与算法有关的问题都可以被纳入公众的讨论范围。事实上，人们对那些公共利益遭受损害，并有可能引发权利义务冲突的算法决策更为关心。在法学领域，人们的关注点聚焦于算法决策的不确定性和不透明性，前者是指基于算法所作出的决策难为他人预测，后者则是指通过算法形成决策所依赖的实质理由和价值取舍难为他人所知。这种算法决策被形象地称为算法“黑箱”。这意味着那些受自动化算法影响的人无法确定决策是如何产生的，也无法对决策背后的因果关系进行逻辑和推理解释，公众因而也就丧失了对其问责的可能。

从实践来看，算法作为一种特殊的决策机制，同时也被视为一种用于建构社会秩序理想模型的方式。在公共政策与公共治理中，权力主体能够借助算法实现政策制定与治理过程的动态化、精细化，从而影响社会主体之间的利益分配关系。〔8〕一方面，以大数据分析和预测技术为基础

〔5〕 参见周辉：《算法权力及其规制》，载《法制与社会发展》2019年第6期。

〔6〕 参见〔美〕瑟格·阿比特博、吉尔·多维克：《算法小时代：从数学到生活的历变》，任轶译，人民邮电出版社2017年版，第6页。

〔7〕 孙保学：《人工智能算法伦理及其风险》，载《哲学动态》2019年第10期，第94页。

〔8〕 参见前引〔5〕，周辉文。

的自动化算法被广泛用于社会治理领域，从而产生大量为受监管实体量身定制的决策或指令，这些决策或指令影响和塑造着不同的社会主体。另一方面，在算法治理之下，这些决策和指令能够参与选择、决定与我们生活相关的各类信息，并最终发展成为管理、判断、调节，甚至能够限制或约束人们行动和生活的强大实体，在客观上也就具有权力属性。〔9〕因此，就公共领域中的某些决策算法而言，其与传统立法在调整社会关系与分配社会利益上具有同质性，即二者都向社会主体提供行为规范，都能改变社会主体之间既有的利益分配格局和行为活动空间，甚至还能对其权利义务产生实质性影响。〔10〕例如，在公共政策制定与社会治理领域，包括经济政策的精准预测和分析，民生管理的精准调度和服务以及公共场所日益增长的自动化监控，这些算法的使用都会涉及立法的内容。

（二）立法性算法的基本内涵

算法与立法既存在共性，也存在一定的差异性。根据算法主体的不同，可以将其划分为公权力算法和私权力算法。前者是指公权力机关所运用的算法，后者一般是指平台企业、数据服务公司等私人主体所运用的算法。而“公权力算法”根据程序性标准又可以划分为“立法性算法”和“非立法性算法”。立法性算法是指有权机关依照一定程序运用的，能够对公民的权利义务产生实质性影响的公共决策算法。例如在疫情防控期间，各地使用的健康码，其背后使用的算法就是严格依照国务院有关部门制定的《个人健康信息码》系列国家标准所形成，这些算法能够根据获取的数据信息自动作出决策对公民行为进行规范和调整，甚至还能对公民的权利义务关系产生实质性影响，如影响公民的消费、出行、工作、生活等。而非立法性算法则是指非经特定程序运用的，但同样能够对公民的权利义务产生实质性影响的公共决策算法。例如“文明码”作为健康码功能的延伸已经从防疫扩展至医疗、养老等其他民生领域，它采用积分模式来对公民的权利义务产生实质性影响，但是，该算法缺乏明确的法律授权，或没有依照特定的立法程序产生，因此，该算法属于非立法性算法。此外，包括公共领域中广泛运用的人脸识别监控算法、社会信用评分算法、智能辅助公共决策算法等，这些算法的使用范围都有可能涉及公民的实质性权利义务，但由于其产生过程未严格依照立法程序进行，因而属于非立法性的算法。因为立法性算法和非立法性算法以其产生过程是否受到立法程序的约束为标准而进行划分，〔11〕所以对立法性算法的产生过程进行程序性规范也就显得尤为重要。事实上，公共决策领域中广泛存在的算法是立法性算法，但算法固有的技术特征规避了立法程序对算法设计的监督和约束作用，从而导致大量立法性算法以非立法性形式在社会治理领域呈现。但是，立法是一种带有价值判断和利益取向的行为秩序安排活动，要使法更好地符合社会需求，就必须通过立法程

〔9〕 关于“算法作为一种权力”的观点最早是由大卫·比尔（David Beer）提出，他认为算法能对每个人施加控制力和影响力，在客观上也是作为一种权力形态而存在。See David Beer, Power through the Algorithm? Participatory Web Cultures and the Technological Unconscious, 11 *New Media & Society*, 985 (2009).

〔10〕 参见蒋舸：《作为算法的法律》，载《清华法学》2019 年第 1 期。

〔11〕 本文将立法视为是一种对不同群体之间利益矛盾和权利冲突进行化解和协调的行为秩序安排。如果用以表示此行为秩序安排的形式是规则化的法律语言，那么此立法就是成文法。如果是裁判，则是判例法。而如果它的表达形式是算法，那么就是立法性算法。

序将不同利益主体的认识纳入评判立法质量的标准体系之中。〔12〕

人们之所以需要法律，是因为人类社会归根结底是一个由各种利益关系交织在一起的复杂体，法律对社会关系的调整实质上也是对社会利益的调整，而权利义务或权力责任等法律概念只是社会主体利益需求在法律上的具体表现形式。“利益作为客观范畴，对法律起着决定性的作用。”〔13〕而人们之所以需要以立法的形式来制定法律，是因为立法作为一种创制权，它以对权力和权利为代表的利益进行分配为目标，立法能够以其公开和透明的程序让普通民众参与其中，并通过合理的整合机制使不同利益群体得以和谐相处。〔14〕因此，立法过程也就是不同社会主体利益需求的表达和博弈过程。〔15〕以司法部 2020 年 2 月 27 日发布的《外国人永久居留管理条例（征求意见稿）》为例，该条例自公布以来就引发了社会各界的高度关注，它的本意是通过赋予外国人永久居留资格来吸引国外人才参与本国建设，从而促进国内经济社会发展。但是，该条例所规定之内容存在诸多不足，导致其自公布以来就受到社会舆论的关注。所幸《中华人民共和国立法法》（以下简称《立法法》）第 67 条专门规定行政法规的起草过程应当向社会公布，并广泛听取公众意见。因为将立法公之于众，无疑会对立法者的选择和决断产生一种无形的压力，从而促使立法活动能够更充分地吸纳并听取公众意见。如果不对立法性算法的产生进行类似规范，这些问题将会同样出现。

而公权力机关之所以需要借助算法的形式实施社会管理，也主要是因为算法对优化治理流程、改善治理精准度以及提升治理效能具有明显的帮助作用。〔16〕然而，在算法治理过程中，看似理性的算法却会引发一系列的算法危机，“算法歧视”“算法合谋”“算法黑箱”等问题层出不穷。〔17〕因为随着社会数字化程度的提高，每个人的生活细节将变得越来越数据化，政府收集和处理数据的算法系统会对公民权利义务产生实质性影响。数据作为算法的根基，决定着算法的目标和实现路径。与此同时，算法也可以被简化为以数据和假设为基础的归纳过程。然而，数据的缺失和预设条件的不合理将直接影响算法的输出结果。当不同决策参数的权重不是由公众参与选择，而是基于特定主体的个人判断之时，算法总是会存在某种程度的不可预测性。即使公众能够直接亲历算法程序设计的全过程，由于对每一个算法程序设计参数缺乏必要的理解，普通民众也将很难做出有效的选择。事实上，在智慧城市建设中，“以支持政府决策和治理为名的大数据中心建设虽然如火如荼，但以算法形式改善决策和治理的成功案例却十分稀少”〔18〕。因为算法程序的设计过程是封闭的，普通公众难以参与到立法性算法程序的设计当中，而在这种公众参与缺失和监督失效的情形下，更容易诱发算

〔12〕 参见张恭善：《立法学原理》，上海社会科学院出版社 1991 年版，第 62 页。

〔13〕 张文显：《法理学》，法律出版社 2009 年版，第 143 页。

〔14〕 参见黄信瑜、石东坡：《立法博弈的规制及其程序表现》，载《法学杂志》2017 年第 2 期。

〔15〕 参见杨炼：《论现代立法中的利益结构》，载《理论月刊》2011 年第 11 期。

〔16〕 参见陈鹏：《智能治理时代的政府：风险防范和能力提升》，载《宁夏社会科学》2019 年第 1 期。

〔17〕 参见张欣：《连接与失控：面对算法社会的来临，如何构建算法信任?》，载《法治周末》2019 年 5 月 30 日，第 12 版。

〔18〕 胡小明：《政府大数据应用效益反省》，载 https://www.chinathinktanks.org.cn/content/detail?id=hapu4w96，最后访问时间：2021 年 9 月 20 日。

法寻租和算法滥用问题。

二、立法性算法对立法程序的规避

（一）立法程序之于立法性算法的重要性

作为一种社会规范形式，法律的本质是对各种利益进行调节和分配，其终极目标是保障全民利益的相对均衡，而立法则是为实现利益均衡进行的制度设计和选择，立法过程也就被视为一个多重相互冲突的利益之间进行博弈和选择的过程。〔19〕在这个过程中，面对不同群体的利益诉求和相互冲突，立法部门不仅要对利益做出合理选择和价值取舍，还需要通过完善的制度安排使不同利益群体得以和谐相处。但是，现代社会是一个利益格局多元化的社会，由立法者代表立法已经越来越难以充分反映和实现不同民众之间的利益需求。一方面，由于立法是一项专门性活动，立法权只掌握在少部分人手中，但是，权力始终会存在被滥用的可能，而现代法治的基本要求是对各种权力，尤其是作为公共权力的立法权予以合法性和正当性的制约，从而防止权力不当使用。因此，寻求对立法权进行有效控制是现代法治要求的应有之义。另一方面，代议制民主不仅仅意味着“大多数人的统治”和“少数服从多数”，它还必须实现对弱势群体的保护以及对少数人的尊重。这就需要在一定程度上实现立法权的回归，以公众参与弥补立法代表在反映民意方面之不足。〔20〕对权力机关而言，保证公众亲历立法过程，可以在更加全面、客观和公正的把握民意的基础之上，最大限度地减少立法失误，实现立法的科学性和民主性要求。对民众而言，通过直接亲历立法过程，能够更加直观地表达自己的利益诉求，从而保障自己的监督权，这些在我国《立法法》的相关规定中都有充分的证明。

根据我国《立法法》第 4、5 条之规定，立法应当依照法定程序，体现人民意志，坚持立法公开以及保障人民通过多种途径参与立法。此项规定不仅具有传达并听取公众意见的形式意义，更重要的是它对保障公众参与和监督立法过程所切实发挥的作用具有实质性的意义。在美国，公众参与立法不仅比较普遍，而且所涉及范围也较广，基本包括宪法修改、国家基本法律的制定，甚至地方政策的出台都有公民参与其中。美国公众参与立法的合法性权利最早来源于《联邦宪法第一修正案》的相关规定，〔21〕此外，美国联邦程序法、〔22〕信息自由法以及联邦咨询委员会立法等法律规范文件也都对公民参与立法的合法性权利作出了明确而又细致的规定，并逐渐形成了集立法听证制度、公众评议反馈制度和立法信息公开制度“三位一体”的法律程序保护模式。尽

〔19〕 参见前引〔14〕，黄信瑜、石东坡文。

〔20〕 参见易有禄：《立法程序的功能分析》，载《江西社会科学》2010 年第 5 期。

〔21〕《美国联邦宪法第一修正案》规定：“国会不应当就设立宗教及其事务制定法律，也不应当通过制定法律限制公民的言论自由、新闻自由、和平集会的权利，以及向政府申请获得救济的权利。”它可以解释为赋予国会一项积极的责任，即为公民提供一种充分的机会，能够就公共事务进行有意义的讨论和辩论。而任何对公民为维护公共利益而实施的各种合法行为进行的限制或阻止均不受宪法保护，并且公民可以就此申请救济。

〔22〕《美国联邦程序法》第 552 条规定公众参与机制的规则制定情形，而第 553 条列举了不适用公众参与机制的规则制定情形。

管美国的现实国情和立法模式与我国有很大的不同，但法律的制定、修改以及实施等过程所追求的目标具有重叠性，即通过公众参与来保障立法过程的公开和透明。要言之，民主进程的推进需公众的普遍参与，他们须相互接触和了解，并通过公开讨论来参与公共生活，从而确定相互之间的共同利益并达成共识。〔23〕与此同时，公众的有效参与和监督还能以规范化的内部操作节省法律的外部执行成本，从而避免立法实践中的种种弊端。对阿伦特而言，公共政治生活需要人与人之间的相互辩论和理解，他们通过讨论和辩论确定共同的利益和价值目标，并努力实现这些目标，这种公开讨论能够使人们搁置争议、凝聚共识。〔24〕因此，强调公众对立法性算法程序的有效参与和监督具有实践必要性。

（二）立法性算法规避立法程序的危害性

算法通常被描述为通过“黑箱”将输入转换为输出，一般公众无法通过“黑箱”去理解这种转变如何发生，也不能用传统统计的直观和因果语言来描述这种关系。如果算法在公共决策领域的使用遭遇广泛质疑，也主要是因为算法与传统人类决策存有本质不同。首先，算法决策不能用人类所能理解的术语来进行解释，它不可避免地会不透明。其次，这些决策是基于大量数据识别的相关关系，而不是经证实的因果关系，在某种意义上还带有明显的随机性，因而不可避免地会出现错误。最后，算法决策不可避免地会反映特定群体的价值判断和选择，因而会带有较强的主观性。〔25〕这些特点以看不见的方式成为威胁现代民主法治框架的关键性要素。进一步而言，算法技术的专业特性还会对公众有效参与立法性算法程序设计造成阻碍。因为算法决策的形成通常包含对历史数据的收集与分析、为实现某个目标而构建模型和编码、为算法提供输入以及对输入数据的应用规定进行算法操作等流程。〔26〕这意味着那些无法产生数字数据的人可能会因此丧失参与公共事务讨论的重要机会。即使有，公众参与决策的过程也具有被动性或间接性，他们无法充分表达自己的利益需求和价值偏好，也缺乏必要的途径将其转化为立法选择。即使公众与立法机关之间存在直接沟通的数字交流平台，但“算法是一个随机的过程，不同变量之间往往会存在复杂的、不可预测的交互作用效应”〔27〕。换言之，算法“黑箱”的性质会对结果差异造成影响，这种可能性已被大多数学者和政策制定者所认识。更为重要的是，算法决策结果不能直观地被解释，也不能支持传统上立法机关对立法行为的背后因果关系进行辩护和说明。〔28〕这些都构成立法程序无法限制和约束立法性算法的重要理由。

然而，在算法治理过程中，“当国家获得数据产权和算法制定主导权，垄断了作为未来主要

〔23〕 See Czapanskiy K. Syma，Manjoo R，The Right of Public Participation in the Law-making Process and the Role of Legislature in the Promotion of This Right，19 *Duke Journal of Comparative & International Law*，1，15 (2008).

〔24〕 See Saliternik Michal，Big Data and the Right to Political Participation，21 *University of Pennsylvania Journal of Constitutional Law*，713，727 (2019).

〔25〕 See Berman Emily，A Government of Laws and Not of Machines，98 *Boston University Law Review*，1277，1283 (2018).

〔26〕 See Brauneis Robert，Ellen P. Goodman，Algorithmic Transparency for the Smart City，20 *Yale Journal of Law and Technology*，103，113－114 (2018).

〔27〕 Coglianese Cary，Lehr David，Regulating by Robot：Administrative Decision Making in the Machine Learning Era，105 *Georgetown Law Journal*，1147，1172，1199 (2017).

〔28〕 参见前引〔27〕，Coglianese Cary、Lehr David 文，第 1167 页。

公共产品的人工智能技术，并通过这种技术无限地干预社会，国家与社会的关系很大程度上将依赖于政府在推广和应用该项技术时是否遵循民主原则，并与社会进行广泛深入的协商”〔29〕。由于立法性算法并非立法者根据法定程序与公众平等对话沟通缔造之物，而是一种复杂的算法程序，并且立法文本也不是传统意义上的自然语言文本，而是非专业人士难以理解的人工语言文本，立法性算法程序的设计可能会面临公众参与的缺失和监督的失效，而在这种公众可参与性和可监督性降低的情况下，其不利影响可能更为明显。美国学者科恩曾将民主比喻为一种社会管理体制，在该体制中，社会成员大体上能直接或间接地参与公共决策。〔30〕就立法程序而言，公众参与是以公开的立法活动来保障那些可能受立法结果影响的普通民众，能够拥有平等的机会来参与立法的全过程，并对立法结果产生实质性的影响。这不仅关乎权力之间的分工和配合，也是公民权利对立法权力制约和限制的体现。

三、立法性算法何以规避立法程序

程序对法律制度的挑战由来已久，心理学家一直致力于运用程序正义原则来研究法律制度的公平感。顾名思义，程序正义只关注纠纷解决的程序性事项，而不涉及实质性结果，因而它与“实质”的公平无关，而与人们对公平的认识有关，是对人们所认为的公平程序的研究。程序正义的社会心理学研究揭示，“当法律权威无法让人们得到一个他们所期望的结果时，通过一个公平的程序来做出决定，更有可能获得人们的认可和接受”〔31〕。程序公开一直以来被视为是实现程序正义的基本标准和内在要求。就立法程序而言，程序公开要求立法过程和结果都要向社会公开，使公众能够亲历立法全过程，并为监督立法提供一种可能。作为程序民主的重要运行机制，公众参与的核心正是以一种较为完善的程序正义来确保实质正义，用公平正当的立法程序来保障立法结果的实质公正。程序正义在算法决策领域的研究发现，决定一个人是否相信某一特定算法程序的公平性有以下四个重要因素：（1）决策者是否以平等的态度对待他人与自己的互动；（2）决策者是否被认为是中立的；（3）决策者是否被认为是可信的；以及（4）个人是否有平等的机会参与决策过程。〔32〕如果运用这些因素来评估立法性算法，在算法未向公众充分披露、公众难以有效参与立法性算法程序设计过程之时，公众的程序正义感要大大降低。

（一）算法语言具有复杂性

算法是为实现特定行为而设计，必须按照给定的流程和轨道运行，其中包括构成算法的技术、

〔29〕 张春满、王震宇：《未来已来？人工智能的兴起与我国国家治理现代化》，载《社会主义研究》2019 年第 4 期，第 99 页。

〔30〕 参见〔美〕科恩：《论民主》，聂崇信等译，商务印书馆 1988 年版，第 10 页。

〔31〕 李昌盛、王彪：《“程序公正感受”研究及其启示》，载《河北法学》2012 年第 3 期，第 63 页。

〔32〕 See Ric Simmons, Big Data and Procedural Justice: Legitimizing Algorithms in the Criminal Justice System, 15 *Ohio State Journal of Criminal Law*, 573, 575 - 576 (2018).

工具和方法，它们有自己特殊的词汇、语法，以及编译单词、句子和文本的规则。〔33〕而语言正是由复杂的语义和句法结构的网、链和矩阵构成，它由基本符号、语形规则、语义规则三个部分组成。语言根据形成方式的不同可以分为自然语言和人工语言，前者可称之为日常语言，是人们在日常生活中在特定的语言范围内所反复使用的某种民族语。后者则是人类根据特殊需求而创造的符号或符号体系，其根本属性是人造语言。〔34〕算法正是借助于一套人工语言符号系统运用演绎体系以使其严格化的一套程序或方法，因此，算法语言属于人工语言的一种。但是，算法语言又与人工语言有很大不同，因为算法语言不是机器的符号表征系统，而是人类语言的符号表征系统。〔35〕在其符号表征系统的最基本层次上，计算机只能有两种状态，即存在或不存在某种电磁现象。它可以处理任何信息，无论是文字、图形或声音，这些都可以用二进制数字符号在计算机程序中得以表示。〔36〕数字是计算机领域运用的一种基本语言，它们与技术有着千丝万缕的联系。布尔逻辑与二元数字的融合形成了计算机设计的基本结构，它蕴含了三个基本运算 and、or 和 not，主要处理两种实体，比如 true 或 false，yes 或 no，open 或 closed，on 或 off，0 或 1。当程序按照布尔原理予以排列时，其能创建一种既可以执行数学运算又可以执行逻辑运算的电路。算法主体能够通过借助计算机程序来完成复杂的社会治理目标，这些目标由机器翻译成一个庞大的目录，其中包含所有可能场景的简单命令。在算法世界里，这些指令被认为是算法主体依据治理目标以及个体行为来进行校准的。〔37〕例如算法主体可能越来越依赖由大数据支持的方法来定制微观指令，或通过数据化分析对社会主体进行自动化监管，而不是依据法律或一般规则。

语言是一种信息交换的符号系统。哈贝马斯将交往活动视为以符号为媒介的相互作用和理解，而“相互作用是按照必须遵守的规范进行，它规定着相互行为的期待，并且必须得到至少两个行动主体（人）的理解和承认”〔38〕。虽然“语言是人们按照一定的规则表达和交流自己思想意志的工具，而立法语言作为表达法律规范内容的唯一工具，只能以特定的语言形式而存在”〔39〕。但构成立法性算法的人工语言对普通公众而言难以理解。因为信息在人和机器之间至少需通过三个层次的传递，每个层次都有其独特的语言，第一层次是机器可读的二进制语言，第三个层次是只有人类才能理解的自然语言，连接这两个层次的是一组人和机器都能理解的编程语言。〔40〕而公众参与立法中的“公众”应该是一个能够自主表达和接受意见，并能够自觉、自主地参与讨论

〔33〕 See Alexey V. Lisachenko, Law as a Programming Language, 37 *Review of Central and East European Law*, 115, 118 (2012).

〔34〕 参见胡泽洪：《现代逻辑视野中的语言与思维》，载《哲学研究》1997 年第 6 期。

〔35〕 关于符号表征系统，皮亚杰认为符号表征是认知发展的核心，是指个体用来代表其他事物的东西，符号表征能力是人类所独有的一种能力。

〔36〕 See J C. Smith, Machine Intelligence and Legal Reasoning, 73 *Chicago-Kent Law Review*, 277, 279 - 280 (1998).

〔37〕 See Casey A. Niblett A, The Death of Rules and Standards, 92 *Indiana Law Journal*, 1401, 1405, 1418 (2017).

〔38〕〔德〕尤尔根·哈贝马斯：《作为“意识形态”的技术与科学》，李黎等译，学林出版社 1999 年版，第 49 页。

〔39〕 前引〔12〕，张恭善书，第 254 页。

〔40〕 See Anne von der lieth Gardner, An Artifificial Intelligence Approach to Legal Reasoning, MIT Press Cambridge, 1987, pp. 24 - 26.

并影响立法决定的普通群体。〔41〕这就需要以同等的语言作为沟通媒介。法律虽是以特定话语进行程式化的表达，构成立法性算法程序的人工语言和自然语言之间存在的差别，在某种意义上可以视为专家话语和公众话语在立法互动过程中的差别。然而，作为一种利益协调和分配机制，法律还必须与社会其他制度相互联结。特别是，在自然语言交流中它还必须寻求与任何可能存在的人际交往建立确定的联系。〔42〕就立法性算法而言，如果过度关注人工语言的一般性，而忽视自然语言的内在特性，以及它在促进人际交往和实现制度安排方面的价值和意义，往往容易导致公众在算法程序设计过程中的缺失。而一旦大数据与人工智能成为立法权力机关的主要信息来源，作为民主性补充渠道的公民立法参与机制将较难发挥作用，这是因为公民由于不具备与此相关的专业知识，而无法表达其利益或反驳相应的科学依据，即使表达出与之相反的意见也可能被斥以误解科学技术的立法依据〔43〕。因此，在算法治理之下，协商式民主的真正难题可能并非在于保证不同利益群体达成共识，而在于如何跨越自然语言和人工语言之间的鸿沟，为公众参与立法提供一个能够平等对话和沟通的桥梁。

（二）算法决策具有非中立性

在算法决策中，表面上中立的算法可能会产生社会实质性的偏见结果。因为，“技术本身是一种带有明显偏向性的思维和结构（structure），它影响和塑造了形形色色的‘行动者’（agent），而技术的后果往往也会超出人们的原初设定”〔44〕。尽管算法决策的产生可能遵循相同的程序规则，但它仍会强化系统中业已存在的偏见和误差。在特殊情况下，算法对输入数据做出的假设并不总是正确，也并非总是按照设计者的预期进行运作。无论这些因素是故意还是偶然所致，算法总会或多或少地受到个人或集体偏见的影响。例如，在算法程序的价值渗入上主要存在两种路径，“一是程序开发人员在设计算法时，参数设定会受到主观价值偏好的影响；二是用户在使用智能设备之时，可以根据自己的需要设置相应的算法应用参数”〔45〕。而在一个复杂算法程序中，算法的实际偏差很可能是由不同程序员指定的规则组合而成的，单个程序员的偏见通过汇集可能会产生更大的累积效应，由此作出的决策虽然能够有效代替传统人脑的决策形式，但也可能会使其遭受质疑。此外，数据挖掘对算法偏差也特别敏感，为确保数据挖掘揭示的模式比分析中的特定样本更适用，样本必须按比例代表整个人群。〔46〕一旦某个样本中包含特定类别不成比例的代表，那么该样本的分析结果可能偏向于支持或反对代表过多或不足的类别。因此，将算法视为客观中立的想法实质上会掩盖算法内部运行的复杂情况，会忽视算法内部逻辑的系统性和结构性不公平因素，同时也会对算法的非中立性技术

〔41〕 参见王怡：《认真对待公众舆论——从公众参与走向立法商谈》，载《政法论坛》2019 年第 6 期。

〔42〕 See Waldron Jeremy，Law and Disagreement，Oxford University Press，1999，p. 105.

〔43〕 参见钱大军：《立法权回收中人工智能的应用及其悖反》，载《上海师范大学学报（哲学社会科学版）》2019 年第 6 期。

〔44〕 袁光锋：《政治算法、“幻影公众”与大数据的政治逻辑》，载《学海》2015 年第 4 期，第 51 页。

〔45〕〔美〕温德尔·瓦拉赫、科林·艾伦：《道德机器：如何让机器人明辨是非》，王小红等译，北京大学出版社 2017 年版，第 1 页。

〔46〕 See Solon Barocas，Andrew D. Selbst，Big Data's Disparate Impact，104 *California Law Review*，671，686（2016）.

特性缺乏清醒的认识。

事实上，立法性算法同样并非具有中立性，一旦算法程序只是由特定主体控制产生，那么据此作出的决策，其公平性和合法性就将大大降低。因为公共决策的产生不能仅仅代表某一群体价值偏好或利益取向的简单集合，它须是受影响者之间真正协商的结果，其中包括交流合理的观点和建议以及共同寻求解决问题的办法，这种协商模式能够强化参与者的能动性和自我实现，同时也能保证决策的科学性和民主性。在桑斯坦看来，协商可以聚合信息和观念，使群体作为一个整体比其最好的成员知晓更多，做得更好，而协商的一个关键目标就是确保能够获得广泛分散的信息，并将其纳入公共决策系统之中。〔47〕虽然算法技术的诞生是为了将无限包围在有限之中，但算法“黑箱”的出现却加深了人类对算法运行过程中数据输入或输出的认知盲点，从而打开了通向无限的大门。〔48〕在立法领域，传统立法权能够受到宪法、法律或社会公众等诸多力量的有效监督和制约，而立法性算法的生成过程则对这些限制性力量构成了突破，并有可能规避来自后者的制约和限制，这是人类可能面临的新难题。

四、立法性算法的程序再规范

在当下，有权机关利用算法可以较为快速、准确地掌握社会公众关注的焦点问题，并能真正了解社会公众的真实需求，从而提高社会治理效率并推动国家治理绩效的改进，以及改变部分领域的治理格局。〔49〕但是，数据输入和输出、程序的设计也有可能会受到特定主体的影响和控制，使得受算法影响的主体被排除在参与和监督的程序之外。为避免由此可能产生的不利后果，立法性算法的产生必须在遵循法定的程序要求下进行。与传统立法中的立法公开、公众参与、社会听证等制度所能带来的效果类似，公开透明及其问责两个维度的算法治理目标同样可以在保障公众参与和监督算法程序设计上发挥重要作用。

（一）通过算法公开保障公众对立法性算法的参与

立法程序对立法性算法的再规范应当要求算法公开透明，这成为立法性算法规制领域的一个原则性建议。算法治理目标的实现最终能否获得理想效果，取决于公众是否能够准确、及时地获取有效的算法设计信息，并能对其决策内容展开自由和公开的辩论。因此，权力机关在使用算法之前，应当严格遵照《立法法》第5条关于立法公开、公众参与相关规定之要求。一方面，根据立法公开的基本原则，算法程序需要披露相关算法规则，其中包括正在优化的目标函数、用于优化的方法以及算法的输入变量和源代码，如此方能保证公众对算法程序设计的知情权，从而有利于社会公众（尤其是专业人士）针对立法性算法实施监督，以及对算法决策提出公平性和合理性质疑。另一方面，算法程序的设计既要注重公众的形式参与，同时也要注重公众的实质参与，公众意见在立法性算法程序中得以反映则是公众参与的实质性表现。国外学者

〔47〕 参见〔美〕桑斯坦：《信息乌托邦》，毕竞悦译，法律出版社2008年版，第52－56页。

〔48〕 See Erika Giorgini, Algorithms and Law, 5 *Italian Law Journal*, 131, 148, 149 (2019).

〔49〕 参见陈鹏：《算法时代的国家治理：在算法与法律之间》，载《法治社会》2019年第6期。

认为通过引入“法律设计”〔50〕思维的概念，将用户的意见集中于嵌入算法系统之中，以确保技术解决方案从一开始就设计为满足法律技术终端用户的需求，〔51〕以此提升公众对算法程序设计的参与感。作为一种评估和创建法律服务系统的新模式，它主要通过对算法的过程、思维方式和机制的控制来帮助人类构建和测试更好的法律行为模式，从而使非技术专业群体都能参与其中并获得授权。〔52〕

另外，随着公众需求的多样化、利益主体的多元化以及立法技术的复杂化，有效的公众参与既要重视个体化的单方参与，同时也要重视组织化的社会参与。前者能为个人发表意见提供平等对话沟通之平台，而后者能够弥补个体因知识欠缺、能力不足导致立法参与缺失之不足。一方面，鉴于算法决策有可能加剧新的社会分层和拉大不同社会群体的差距，其程序的设计至少必须为那些生活在数据流之外的边缘群体提供保障，保证那些数据足迹较小的群体在分配公共产品或服务之时有足够的发言权，以致不会受到算法的不平等对待。〔53〕与此同时，还应当保证算法决策须是根据同一套特定程序产生，并在每种情况下都平等一致地适用于任何人。因为对特定程序的遵守能够代替那些对公民权利义务产生实质性影响的算法决策产生的严格证明，并确保算法决策的产生是依赖于同样的一套技术标准。须注意的是，算法程序设计的公开虽然能够为公众参与大开方便之门，但并不意味着所有人都能够平等参与其中，即使可以，也会因流于形式而违背立法公开制度设计的初衷，而公众参与算法程序设计的实际效果也会大大降低。由于算法所包含的知识内容通常比较晦涩难懂，鉴于算法技术的专业性和算法语言的特殊性，在很多情况下，缺乏必要专业知识基础的普通公众很难参与到立法性算法程序设计当中。对此，可通过引入“交流型专家”〔54〕来协助技术内核部分，“在专家和公众之间实现知识传递和共识达成，并在决策过程中细化和具化公众参与的能力，从而保障公众的实质参与”〔55〕。作为连接公众和权力机关的中间桥梁，“交流型专家”的作用在于将一些难以理解的算法人工语言向普通公众进行传递，并对算法程序的设计提出专业性的意见和建议。〔56〕

在科学技术与民主关系的认知、判断与冲突之中，公众对立法性算法程序设计的有效参与，还须保证其拥有掌握或了解算法技术的基础知识与判断能力，从而为立法性算法的民主化和科学化发展提供必要的条件，这既是在人工智能时代保持公众独立思考和批判能力的基本要求，也是应对社会治理领域算法化方向转变的重要举措。因此，注重立法方法和

〔50〕 斯坦福大学法律设计实验室的玛格丽特·哈根是最早提出“法律设计”一词的人之一。哈根将其定义为一种以用户为中心的意识形态，被视为实现以人为中心的设计的过程、思维方式和机制集。

〔51〕 See Toohey Lisa、Moore Monique，Dart Katelane，Toohey Dan，Meeting the Access to Civil Justice Challenge：DigitalmInclusion，Algorithmic Justice，and Human-Centred Design，19 *Macquarie Law*，133，153（2019）.

〔52〕 参见前引〔51〕，Toohey Lisa、Moore Monique、Dart Katelane、Toohey Dan 文，第 153－154 页。

〔53〕 See Lerman Jonas，Big Data and Its Exclusions，66 *Stanford Law Review Online*，55，61（2013－2014）.

〔54〕 谭笑：《技术问题决策中的专家话语和公众话语——柯林斯（重思专能）的方案》，载《开放时代》2014 年第 6 期，第 220 页。

〔55〕 前引〔54〕谭笑文，第 220 页。

〔56〕 See Danielle K. Citron，Technological Due Process，85 *Washington University Law Review*，1249，1312（2007－2008）.

观念的时代转变，培育公众对立法性算法程序设计的参与技能，增强公众的民主参与意识也显得尤为重要。

（二）通过算法解释保障公众对立法性算法的监督

事实上，对于涉及一些随机因素的决策过程，即使是系统源代码、输入、操作环境和结果的完全透明，也不能排除结果可能以不可检测的方式被错误地固定的可能性。〔57〕算法的语言和操作系统对于普通民众来说非常难以理解，即使专家也常常难以理解算法程序的全部运行过程。因此，算法公开对于保障公众有效的参与和监督而言，其作用范围十分有限。在此基础之上，学界普遍认为通过设计算法责任机制来促使利益相关者实现问责的目标，同样能达到监督和约束效果。算法问责体现为算法解释，它能让算法决策相对人有机会在充分知情的情形下主张自己的权利，并要求算法控制者以自然语言或可视化技术对算法逻辑尤其是输入数据与输出结果之间的相关性进行解释。〔58〕就立法性算法的解释而言，则表现为算法主体对算法决策产生逻辑的解释要清晰、合理和言之有据，不能违背宪法、法律相关规定的基本要求，并在算法解释程序上能够妥善处理公众可能提出的质疑。

传统上，立法解释的目的主要服务于法律实施，立法解释工作是通过阐明法律概念、填补法律漏洞以及探究立法原义等方式，来促使存在争议的法律规则能够得以有效实施。而对立法性算法进行解释的原理同样在于，通过赋予公众获得关于立法性算法解释的权利，以明确权力机关的解释义务和技术责任，提高算法的透明度和公众参与度，实现权力主体的可归责性和公众权利的可救济性，从而推动立法程序和立法性算法的深度融合，最终能够形成利益均衡、公平一致的算法决策。作为一种对算法决策产生过程公开原则之不足的补救办法，对立法性算法的解释既直观地表现为一种打开“黑箱”的手段，通过公众对算法程序的参与和监督允许公众对算法决策提出质疑和纠正，同时也为公众权利救济提供一种必要的途径。然而，作为一种事后的规制手段，对算法进行解释必须受到立法程序的严格限制。因为根据权力的性质和层级不同，其解释的主体和程序以及解释的效力也有所不同。因此，立法性算法解释的相关程序设置理应在立法解释的框架范围内进行。

五、结　语

在现代民主社会里，社会正义和制度正义的实现要求保障和促进不同利益群体以合法的形式进行立法需求的表达和主张。而立法程序的意义就在于限制和消除立法活动中的恣意因素，广泛听取和接纳不同群体的主张，以协调不同群体之间的利益冲突，进而制定出体现实质正义的法律。尽管当下人们还无法对算法程序的设计和应用进行有意义的控制，但立法性算法与一般算法不同，它的产生必须严格依照立法程序的相关规定进行，保证公众对立法性算法程序设计全过程

〔57〕 See Joshua A. Kroll, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson, Harlan Yu, Accountable Algorithms, 165 *University of Pennsylvania Law Review*, 633, 650 (2017).

〔58〕 参见解正山：《算法决策规制——以算法“解释权”为中心》，载《现代法学》2020年第1期。

的知情、参与和监督。这既是保障公民权利的重要体现，也是实现算法决策民主化和科学化的关键环节。因此，要实现立法程序对立法性算法的再规范，就要求算法程序的设计必须以公开透明和问责制为主要原则，以确保公众对立法性算法的充分参与和必要的权利救济。

Abstract: Legislative algorithm means public decision algorithm formulated by authorities in accordance with certain procedures, which even have a substantial impact on citizens' rights and obligations. Just like traditional legislation, legislative algorithm will change the distribution patten of social resources and people's space, also, legislative algorithm have a substantial impact on the citizens' rights and obligations. However, legislative algorithm may base on the inherent technical characteristics to avoid the public participation and supervision of legislative algorithm programming. On the one hand, there is a big difference between the artificial language that constitutes legislative algorithm with the natural language, which familiar to the general. Because the general public doesn't have the knowledge of artificial language, it's difficult for them to get an equal dialogue and effective communication in the algorithmic programming, which may cause the problem of power-responsibility imbalance and supervision failure. On the other hand, the legislative algorithm embed the designer's preferences and value judgments unconsciously, and it can't fully demonstrate the objectivity and truth under the ideal of "technology neutrality", and even may produce deviations, which may lead to the problem of algorithm abusing and algorithmic bias. In order to overcome these shortcomings, it's required that the design of algorithm programs must take transparency and accountability as the main principles to ensure the full participation of the public in legislative algorithm and provide necessary rights remedy.

Key Words: legislation, algorithm, legislative procedure, legislative algorithm, public decision algorithm

（责任编辑：于文豪　赵建蕊）

财经法学 No. 1，2023
pp. 61 - 75

自动化行政中算法的法律控制

王　宾*

内容提要：自动化行政中的算法可分为转译型算法和自我学习型算法。算法的运用面临合法性危机：处于私主体地位的算法设计师将法律语言转译成机器语言时会嵌入自身的判断，带来改写法律的风险；算法决策有时在事实上超出法律授权范围，且缺乏畅通的救济机制。算法的合法性控制方式应与算法类型适配。针对转译型算法，需结合算法的性质以及技术特点，从转译主体、所译法律的明确性、转译过程的透明度等方面施以控制。针对自我学习型算法，首先应当确立“民主—科学”的合法性框架，其次应当从建立算法信任的角度，围绕保障公众主体地位和算法科学性对算法进行控制。

关键词：自动化行政　形式合法性　行政民主　行政科学　算法信任

一、引　言

随着人工智能技术的迅猛发展，数字技术越来越多地被嵌入公共行政领域，数字法治政府建设已上升为一项国家战略。中共中央、国务院印发的《法治政府建设实施纲要（2021—2025年）》提出健全法治政府建设科技保障，全面建设数字法治政府，坚持运用互联网、大数据、人工智能等技术手段促进依法行政，着力实现政府治理信息化与法治化深度融合，优化革新政府治理流程和方式，大力提升法治政府建设数字化水平。《国务院关于加强数字政府建设的指导意见》提出“将数字技术广泛应用于政府管理服务，推进政府治理流程优化、模式创新和履职能力提升，构建数字化、智能化的政府运行新形态”。数字法治政府建设的潮流不可逆转，其中需要关注的重点问题之一是如何保证“数字”与“法治”共生。由于技术水平的迭代发展，政府开展行政活动所借助的数字技术已经超出了亚里士多德所想象的“按照人的意志或命令自动工作的无生

* 王宾，北京大学法学院博士研究生。

命工具”〔1〕的范畴。机器学习通过算法，让机器可以从外界输入的大量数据中学习到规律，从而进行识别判断。〔2〕机器学习算法都有一定程度的自主性，它们通常无法为证明行政决策合理性的这类因果陈述提供任何依据（例如“因为 X 导致 Y，所以 X 是正当的”）。〔3〕当行政机关使用机器学习系统作出行政决策时，很难保证该决策体现的是特定人的意志。

有观点认为，行政国家的自动化程度越高，就越有可能减损行政国家存在的正当性，理由有二：一方面，自动化系统的复杂性使得利用其执行任务的行政机关工作人员并不了解系统的运行原理，更无法在法庭上给出任何解释说明；另一方面，行政规则以机器语言的形式被嵌入自动化系统之后，行政机关再也无法像过去一样通过行使裁量权来回应变动不居的实际情况。〔4〕在高度自动化行政的背景下，行政机关同时放弃了专业知识和裁量权。行政机关对专业知识和裁量权的放弃，意味着其将行政权力让渡给了自动化系统。而自动化决策的正当性、合理性、合法性是数字法治政府建设中应当认真对待的重要基础和法治前提。〔5〕有学者对无人工介入的自动化行政提出合法性疑问：由第三方主体设计的机器和程序过程取代行政机关一方的意思表示是否具有权力主体上的合法性，用以作出行政决定的算法是否如实复刻了实体法中的内容。〔6〕对此，有观点认为，在自动化行政中，算法设计师在转译法律语言时，可能会扭曲法律法规的内容，导致法律规则的异化执行或适用，不符合形式合法性的要求，而且，由于自动化行政中存在技术壁垒，公众的知情权、异议权和建议权难以实现，行政过程缺乏民主正当性。〔7〕

在传统行政法中，行政机关的权力来源于立法授权，立法机关被设定为代表民意的政治机构，负责民意的汇集和表达，制定法律并承担政治上的责任，行政机关负责法律的执行。行政机关只要严格依法行政，便可以借助政治权威（立法机关）的正当性而获得“合法化”。〔8〕在自动化行政中，自动化系统运行算法的过程相当于执行法律的过程，面对自动化执法合法性不足的问题，该如何对算法施以法律控制？这是本文重点回答的问题。首先，文章结合算法的工作原理对实践中的自动化行政样态和算法类型进行分类；其次，在类型化的基础上具体分析可能面临的合法性问题；最后，针对不同类型的算法，提出合法性控制手段。

二、自动化行政中的算法及其应用分类

（一）自动化行政中的算法工作原理

“自动化行政”是一个描述性用语，指行政程序中特定环节或所有环节由人工智能代为处理，

〔1〕〔古希腊〕亚里士多德：《政治学》，吴寿彭译，商务印书馆 1983 年版，第 11－12 页。

〔2〕参见郭丽丽、丁世飞：《深度学习研究进展》，载《计算机科学》2015 年第 5 期。

〔3〕参见〔美〕卡里·科利亚尼斯：《自动化国家的行政法》，苏苗罕、王梦菲译，载《法治社会》2022 年第 1 期。

〔4〕See Ryan Calo & Danielle K. Citron, The Automated Administrative State: A Crisis of Legitimacy, 70 *Emory Law Journal* 797, 804 (2021).

〔5〕参见马长山：《数字法治政府的机制再造》，载《政治与法律》2022 年第 11 期。

〔6〕参见展鹏贺：《数字化行政方式的权力正当性检视》，载《中国法学》2021 年第 3 期。

〔7〕参见王怀勇、邓若翰：《算法行政：现实挑战与法律应对》，载《行政法学研究》2022 年第 4 期。

〔8〕参见王锡锌：《行政正当性需求的回归——中国新行政法概念的提出、逻辑与制度框架》，载《清华法学》2009 年第 2 期。

而无需人工的个别介入，从而实现部分或全部无人化的行政活动。〔9〕学界也用“算法行政”〔10〕“数字化行政”〔11〕“人工智能算法决策”〔12〕等名称来描述这一现象。自动化行政中的技术载体是计算机，而计算机的工作过程就是执行程序，该程序是由程序开发人员使用某种程序设计语言编写的，以代码形式表示的，能够为计算机识别并予以执行的指令集合，程序的核心是算法。〔13〕程序与算法实际上具有相同含义，计算机执行程序本质上就是执行算法。有学者指出，算法是一套求解逻辑，在计算科学领域，其表现为由代码连结且结构化的一系列问题和求解数学模型的集合，单一代码向计算机传达的是简单的做或不做的指令，若干单一代码有机连结后构成解决具体问题的复杂算法。〔14〕将算法视作求解逻辑是最广义的定义，可以涵盖所有决策程序和步骤，而将其限定于计算科学的定义，是狭义的算法定义。也有学者采用中义的算法定义，将算法界定为人类和机器交互的决策，即人类通过代码设置、数据运算与机器自动化判断进行决策的一套机制。〔15〕本文采取中义的算法定义。

从技术层面来讲，有两种构建算法规则的模式：一是专家系统模式，二是机器学习模式。专家系统是利用人类预先设定的专家知识数据库来解决相应的问题。其发展的近期目标是建造能用于代替人类高级脑力劳动的专家系统。〔16〕以构建认定故意伤害罪的算法为例，专家系统构建路径首先需要法律专家确认构建知识图谱的犯罪构成理论（犯罪三阶层、四阶层抑或其他理论），然后在确定的大框架下，根据故意伤害罪的法律特征，精细化拆分犯罪构成要素，定义基本的法律模式图。定义好数据模式之后，再从大量真实的法律数据中抽取相关知识点以及知识点之间的逻辑关系，将这些实体信息相应挂接在要件要素上，从而形成具有高度逻辑的知识组织形式。〔17〕专家系统具有可理解性，即在执行过程中，系统能解释推理步骤，使之易于理解，其解释的方式应与专家解释他们推理的方式一样。〔18〕

机器学习是通过接收外界信息（包括观察样例、外来监督、交互反馈等）获得一系列知识、规则、方法和技能的过程。这一过程对人类和其他生物而言称为“生物学习”，对计算机而言称为“机器学习”。〔19〕简单来说，机器学习是在样本数据的基础上找出一个公式或者多个公式的组合模型来解决特定的问题。〔20〕中间寻找模型（确定算法）的过程是不可知的、难以解释的。在专家系统模式下，自动化系统的算法是由算法设计师确定的；而在机器学习模式下，算法是由算

〔9〕 参见马颜昕：《自动化行政的分级与法律控制变革》，载《行政法学研究》2019 年第 1 期。

〔10〕 参见虞青松：《算法行政：社会信用体系治理范式及其法治化》，载《法学论坛》2020 年第 2 期。

〔11〕 参见前引〔6〕，展鹏贺文。

〔12〕 参见张恩典：《人工智能算法决策对行政法治的挑战及制度因应》，载《行政法学研究》2020 年第 4 期。

〔13〕 参见刘东亮：《技术性正当程序：人工智能时代程序法和算法的双重变奏》，载《比较法研究》2020 年第 5 期。

〔14〕 参见邱泽奇：《算法治理的技术迷思与行动选择》，载《人民论坛·学术前沿》2022 年第 10 期。

〔15〕 参见丁晓东：《论算法的法律规制》，载《中国社会科学》2020 年第 12 期。

〔16〕 参见张煜东等：《专家系统发展综述》，载《计算机工程与应用》2010 年第 19 期。

〔17〕 参见叶衍艳：《法律知识图谱的概念与建构》，载华宇元典法律人工智能研究院编：《让法律人读懂人工智能》，法律出版社 2019 年版，第 25 页。

〔18〕 参见〔美〕吉奥克等：《专家系统原理与编程》，印鉴等译，机械工业出版社 2006 年版，第 7 页。

〔19〕 参见王东：《机器学习导论》，清华大学出版社 2021 年版，第 2 页。

〔20〕 参见邹劭坤：《机器学习的“黑盒”是什么?》，载华宇元典法律人工智能研究院编：《让法律人读懂人工智能》，法律出版社 2019 年版，第 37 页。

法设计师和机器共同确定的，设计师为机器制定“学习规则”，机器在“学习规则”的指示下，通过对海量数据的学习确定算法。

（二）自动化行政中的算法应用分类

既有研究对自动化行政进行了不同的类型化处理。有学者将特定行政活动区分为识别与输入、分析与决定、输出与实现三个环节，根据自动化系统发挥作用的环节不同，将自动化行政分为 0～4 级，分别为无自动化行政、自动化辅助行政、部分自动化行政、无裁量能力的完全自动化行政、有裁量能力的完全自动化行政。〔21〕自动化辅助行政和部分自动化行政中，分析与决定的权力仍掌握在人类手中；而在完全自动化行政中，行政活动不再需要人类介入。也有学者从是否排除人工介入的角度，将自动化行政分为需要人工介入的半自动行政行为和不需要人工介入的全自动行政行为。〔22〕

还有学者将行政过程中是否有人工干预和自动化对最终决定的实际影响结合起来，将自动化行政分为三类：（1）数字化程序实施，但实体决定仍为人工作出；（2）“程序实施＋实体决定”的完全数字化，但实体决定非以人工智能的方式作出；（3）“程序实施＋实体决定”的完全数字化，且实体决定由人工智能作出。〔23〕“非以人工智能的方式作出”是指自动化系统中的算法是专家系统模式下预先设定好的规则，系统并不进行自主学习。在此语境下，人工智能仅包括能够进行机器学习的自动化系统。

这种兼顾行政活动的实现方式和技术影响力的分类方式，于本文研究而言，更具有相关意义，但其在表述上不当限缩了“人工智能”概念的范围，因此应该稍作修正。按照其分类依据，自动化行政可以分为：（1）自动化程序实施，但实体决定仍为人工作出；（2）“程序实施＋实体决定”的完全自动化，但实体决定是人为设定算法的表达；（3）“程序实施＋实体决定”的完全自动化，但实体决定是机器学习后算法的表达。以下将该三类自动化行政分别简称为自动化行政Ⅰ、自动化行政Ⅱ、自动化行政Ⅲ。

在自动化行政Ⅰ中，自动化系统输出的结果对实体决定发挥作用的方式有两种：一是为实体决定的作出提供参考，例如南京市环保行政处罚自由裁量辅助决策系统。〔24〕二是作为实体决定作出的依据。例如，根据《道路交通安全法》第 114 条的规定，公安机关交通管理部门根据交通技术监控记录资料，可以对有关人员依法予以处罚。依据授权法律的规定，电子警察系统的作用是收集、固定违法事实，为最终处罚决定的作出提供证据。有观点认为，在我国智慧交通体系的建设中，算法可以直接对监控查获的交通违法行为处以罚款，这意味着在此领域，算法已经可以直接作为决策者作出具体行政行为。〔25〕本文在第三部分将对这一观点展开论证。

自动化行政Ⅱ的典型范例是深圳市用于高校应届毕业生引进和落户的“无人干预自动审批”

〔21〕 参见前引〔9〕，马颜昕文。

〔22〕 参见查云飞：《人工智能时代全自动具体行政行为研究》，载《比较法研究》2018 年第 5 期。

〔23〕 参见前引〔6〕，展鹏贺文。

〔24〕 参见《规范执法流程 提升执法精准性 南京辅助决策系统实现全覆盖》，载 https://www.mee.gov.cn/home/ztbd/qt/szhb/201507/t20150713_306216.shtml，最后访问时间：2022 年 11 月 3 日。

〔25〕 参见张凌寒：《算法权力的兴起、异化及法律规制》，载《法商研究》2019 年第 4 期。

系统。审批系统按照既定的规则自动进行数据比对，全程自动办理，无人工干预。〔26〕除此之外，疫情防控中所广泛应用的健康码也属于此类自动化行政的范围，健康码经由机器自动化决策生成，行政机关先将评判标准程式化，然后相对人在线提交信息并申请，最终由系统自动分配不同颜色标识的二维码。〔27〕

自动化行政Ⅲ的实践样本尚未在我国出现。该自动化行政方式意味着系统将在不预设“裁量规则”的前提下代替人类作出裁量性具体行政行为。德国《行政程序法》第35a条将具有不确定法律概念和裁量的行政行为排除于全自动程序的适用范围之外，即只允许羁束具体行政行为适用全自动化程序。〔28〕德国立法例属于自动化行政Ⅱ的范围，即人工为系统设定算法，系统执行。美国劳工统计局使用监督学习系统代替工作人员对收集到的大量关于就业、人力成本等专题信息进行编码。〔29〕尽管在该应用场景中，自动化系统并未直接对公民作出决定，但其的确已经独立完成本应由人类完成的编码工作，该工作将会影响劳工统计局相关的政策制定。

三、算法支配的自动化行政的合法性危机

传统行政法通过依法行政原则建立起用于担保行政机关合法行使行政权的框架性法律制度，依法行政原理的逻辑基点是由人民代表大会及其常务委员会制定的法律为行政机关提供行政权的依据，行政机关必须在法律规定的范围内行使行政权。〔30〕在行政法的传统模式之下，行政机关被设想为一个纯粹的传送带，职责是在特定案件中执行立法指令；行政机关的行为受制于司法审查以符合立法指令。〔31〕当行政机关以自动化的方式执行法律时，其同样需符合依法行政原则的要求，接受合法性检验。本部分将从自动化系统中算法自身的合法性和算法决策的合法性两方面，展开合法性问题的讨论。

（一）算法自身的合法性

自动化行政中算法的生成方式大致可以分为人为设定和机器自我学习生成两种。前者主要依靠算法设计师将法律语言转译成机器语言，可以称为“转译型算法”；后者是以算法设计师设计的学习规则为基础，通过对海量数据的学习生成的新算法，可以称为“自我学习型算法”。自动化行政Ⅱ中涉及的算法是转译型算法，自动化行政Ⅲ中涉及的算法是自我学习型算法；而自动化行政Ⅰ中的算法类型取决于系统的技术应用。

转译型算法的设计者通常是行政机关和私营部门中的算法设计师，转译型算法制定的过程实

〔26〕 参见《推动无人干预自动审批（秒批）改革（深圳做法）》，载 https://www.gd.gov.cn/gdywdt/zwzt/szhzy/jytg/content/post_2906394.html，最后访问时间：2022年11月3日。

〔27〕 参见查云飞：《健康码：个人疫情风险的自动化评级与利用》，载《浙江学刊》2020年第3期。

〔28〕 参见前引〔22〕，查云飞文。

〔29〕 将自然语言转换为统计数据是编码的过程，例如为了回答“门卫人员在工作中最常见的伤害原因是什么”这一问题，工作人员需要阅读每一份描述，以编码的方式将对方的职业与造成伤害的因素关联起来。现在机器学习系统代替劳工局工作人员完成这项任务。参见《采访 Alex Measure：机器学习应用于政府业务场景》，载 https://m.elecfans.com/article/1281070.html，最后访问时间：2022年11月4日。

〔30〕 参见章剑生：《现代行政法总论》（第2版），法律出版社2019年版，第36页。

〔31〕 参见〔美〕理查德·B. 斯图尔特：《美国行政法的重构》，沈岿译，商务印书馆2011年版，第11－12页。

质是把行政规范、行政过程以及自由裁量转化成计算逻辑和代码的自动执行，这一过程无疑会嵌入主观判断、利益选择和价值观设定。〔32〕例如，在设计识别车牌遮挡行为的交通监控系统的过程中，当存在多种识别车牌遮挡行为的技术时，如基于车牌结构特征的检测技术、基于颜色特征的检测技术、基于机器学习的检测技术〔33〕等，算法设计师应该选择何种检测技术实现监控系统的运行目标？不同检测技术的准确率和实现成本不同，受私益驱动的算法设计者可能会和代表公共利益的行政机关作出不同的选择。此时，引发的第一个合法性问题是，不具有行政主体资格的算法设计师转译法律规范、主导自动化行政过程的合法性基础为何。这一问题对自我学习型算法而言更加尖锐。尽管转译型算法的设计者包括除行政机关以外的第三方主体，但仍是特定个人决定了算法的表达，算法仍处于人类的控制之下。自我学习型算法，以“学习规则”为基础，利用海量和非结构化的数据来确定解决既定问题的最优算法。除此之外，系统还可以根据外界环境的反馈持续更新算法，结果输出具有不确定性。自我学习型算法的表达已经超出了行政机关和设计者的严密控制，法律的实施具有更大的不确定性和不可解释性。

算法生成过程存在改写法律的风险。传统法律在制定时存在必要的模糊性，也未考虑到自动化的要求，而自动化系统中运行的算法需要极高的精确度和严格度，这导致人类语言与机器语言的转译过程充满了不确定性。〔34〕丽莎·A. 谢伊和伍德罗·哈特佐格等学者在《机器人欢迎电子法吗？一个法律内部的算法实验》〔35〕一文中构建并实施了一个由 52 位电脑程序员参与的、将特定交通法规以代码方式实现的实验。程序员被分为三组，第一组被要求实现“法律条文”，第二组被要求实现“法律意图”，第三组得到了一份附加的、精心编写的说明书，以此作为其软件实现的基础。无论是参考不同文本的不同组的程序员，还是参考同样文本的同组程序员，其最终设计出的程序都存在较多差异。该实验的结论之一是程序员自身的假设和偏差会体现在代码之中，虽然该问题可以通过构建良好的软件设计说明书来化解，但是对所有可能出现的问题进行预测的完美说明书极难设计。实践中，美国科罗拉多州福利管理系统（The Colorado Benefits Management System，CBMS）是确定申请人是否能够获得公共援助资格的自动化系统，该系统自 2004 年 9 月应用以来，作出了成千上万错误的福利认定，许多错误都可以归因于算法设计者在将法律转译为代码的过程中出现偏差，扭曲了联邦和州政策。〔36〕转译型算法或可通过对转译主体、转译程序等施加严格法律要求的方式来保障其准确性，补强合法性。但自我学习型算法的计算逻辑大多是从训练数据中得来的，很少反映在源代码中，〔37〕因此，难以通过控制源代码的方式证

〔32〕 参见前引〔5〕，马长山文。

〔33〕 参见聂文真：《出租汽车车牌遮挡行为判定与图像取证技术研究》，北京工业大学 2019 年硕士学位论文，第 26－27 页。

〔34〕 参见〔美〕丽莎·A. 谢伊、伍德罗·哈特佐格等：《机器人欢迎电子法吗？一个法律内部的算法实验》，载〔美〕瑞恩·卡洛、迈克尔·弗鲁姆金、〔加〕伊恩·克尔主编：《人工智能与法律的对话》，陈吉栋、董惠敏、杭颖颖译，上海人民出版社 2018 年版，第 278 页。

〔35〕 参见前引〔34〕，丽莎·A. 谢伊、伍德罗·哈特佐格等文。

〔36〕 See Danielle Keats Citron, Technology Due Process, 85 (6) *Washington University Law Review* 1249 (2007).

〔37〕 See Kartik Hosanagar & Vivian Jair, We Need Transparency in Algorithms, but Too Much Can Backfire, Harvard Business Review (July 23, 2018), available at https://hbr.org/2018/07/we-need-transparency-in-algorithms-but-too-much-can-backfire, last visited on Dec. 26, 2022.

成其适用的合法性。

（二）算法决策的合法性

1. 算法决策超出法律的授权范围

自动化行政Ⅰ中的系统可分为两类，一是为人工决定提供参考意见的自动化辅助系统，二是为人工决定提供证据的自动化系统，后者对实体决定的影响甚于前者。在自动化辅助系统应用的场景中，作出实体决定的权力掌握在执法人员手中，即使执法人员事实上高度依赖系统提供的建议，也不能将决策过程称为“算法决策”，因为依赖系统是人的主动选择。在第二类自动化系统的应用场景中，尽管从形式上来看是由执法人员根据系统提供的证据作出决定，但实质上系统在固定证据的同时就完成了对违法行为的认定，剥夺了属于人的裁量空间，也超出了法律的授权范围。

以电子警察系统为例，依据授权法律的规定，系统要实现的目标是收集、固定违法事实，为最终处罚决定的作出提供证据。结合《道路交通安全违法行为处理程序规定》（以下简称《程序规定》）的要求，自动化行政处罚流程可归纳为以下五步：第一，交通技术监控设备收集违法事实；第二，经人工审核无误后录入系统作为证据；第三，通知相对人违法信息；第四，告知相对人处罚事实、理由、依据及权利；第五，实施处罚并送达决定书。〔38〕前两个步骤属于案件事实的认定过程，由系统和人类共同完成，系统用来收集、固定违法行为证据。需要注意的是，系统对行为的记录并上传过程意味着其已经完成了对违法行为的第一次认定，人工审核是一个复核的过程。在认定案件事实的过程中，系统认定的案件事实需要经人工审核无误后方可成为行政处罚决定的证据。结合《程序规定》第18条和第19条〔39〕的规定，人工审核的内容应当是违法行为记录资料是否清晰、准确地反映机动车类型、号牌、外观等特征以及违法时间、地点、事实；对于系统认定违法行为的标准（即预先设定的算法）是全盘接受的。因此，在案件事实认定阶段，系统与执法人员共同认定违法行为，前者通过算法实质决定了违法行为的认定标准，后者仅能从证据形式是否完备的角度否定不符合形式标准的违法行为。从执法实践来看，交警在大多数情况下仅依靠交通技术监控设备或执法设备所记录的图片或视频就实施处罚。〔40〕虽然形式上执法人员对处罚决定的作出保有审核的权力，但事实上系统已经成为真正的处罚决定实施者。由此观之，电子警察系统在应用过程中，已经超出了法律的授权。

2. 算法决策的救济渠道不畅

自动化行政Ⅱ和Ⅲ是无人工干预下的算法决策，而完全自动化系统在设计时可能缺乏纠错机制。以北京健康宝“弹窗3”为例，“弹窗3”产生的原理是系统认定特定个人与京内外风险地区、点位、人员等有时空关联，需要进行风险排查。但是健康宝的决策系统并未给个人提供直接的救济途径，使个人能够通过提供不存在时空关联证据的形式自行解除弹窗。被弹窗的公民只能

〔38〕 参见谢明睿、余凌云：《技术赋能交警非现场执法对行政程序的挑战及完善》，载《法学杂志》2021年第3期。

〔39〕《道路交通安全违法行为处理程序规定》第18条规定：“作为处理依据的交通技术监控设备收集的违法行为记录资料，应当清晰、准确地反映机动车类型、号牌、外观等特征以及违法时间、地点、事实。”第19条规定：“交通技术监控设备收集违法行为记录资料后五日内，违法行为发生地公安机关交通管理部门应当对记录内容进行审核，经审核无误后录入道路交通违法信息管理系统，作为处罚违法行为的证据。”

〔40〕 参见前引〔38〕，谢明睿、余凌云文。

通过人工申诉的方式解除弹窗，〔41〕而人工申诉解决往往耗时良久，弹窗状态又严重影响公民的正常生活，被弹窗公民的救济渠道并不顺畅。

除此之外，公民事实上难以挑战算法决策的准确性。原因有二：一是公民的专业知识很难与算法所代表的行政机关的专业认定相对抗；二是公民得知被“错误”决策的时间通常晚于决策作出的时间，其难以收集并保留行为发生时的证据以自证清白。例如，在何凯与上海市公安局黄浦分局交通警察支队行政二审案件〔42〕中，何凯鸣喇叭的行为被电子警察记录，交警对其作出行政处罚。何凯具有一定的声学专业背景，在二审时其结合专业认知陈述了异议，即根据照片上有关声波的图案无法对应其车辆喇叭发声的波段。这一异议并未推翻电子警察的认定结果。同样，在高彬与新民市公安局交通行政处罚纠纷案〔43〕中，高彬被电子监控设备认定为超速，并被交警予以顶格处罚。高彬依据监控设备拍摄的照片上显示的时间及其目测的位移，自行计算速度，认为其并未超速，并且提供了相关的学术论文证明雷达测速对其车速的测量是误判。同样这一主张也未得到法院的认可。

自动化行政方式对传统行政法中的法律约束框架提出挑战：第三方设计主体的参与、转译型算法与自我学习型算法改写法律的风险、算法决策超越法律的授权等冲击着立法对行政的约束能力；算法决策的救济途径不畅、算法的难以审查性也使得司法对行政的约束作用减弱。对此，一方面，应当反思传统法律控制框架对自动化行政发挥作用的场域；另一方面，在传统框架规制不足的场域，应当探索新的合法性约束机制。接下来，文章将分别从转译型算法和自我学习型算法的控制角度对前述问题作出回应。

四、转译型算法的控制

转译型算法面临的合法性问题是转译者的主体适当性、转译算法是否能够准确实现法律的要求。在自动化行政中，“代码即法律”〔44〕，转译型算法的制定过程（转译过程）可类比传统行政法中的规则制定过程。转译型算法的裁量存在于转译过程，算法适用过程无裁量空间。对转译型算法系统而言，控制算法制定过程就能够控制算法适用过程。针对转译过程的控制：首先，需要分析转译过程的法律性质为何，应该符合何种主体、程序的要求；其次，应当结合法律语言转译成算法的不确定性特点，探究通过何种方式缩减第三方中算法设计师的判断空间。

（一）转译过程的法律性质

转译型算法作为机器语言，其法律性质与所需要执行的规范条文的性质有关，若其对应的规范条文属于裁量基准，则算法就相当于裁量基准。例如，自动化处罚系统中的转译过程相当于将

〔41〕 参见《收到北京健康宝弹窗 3 怎么办？怎样处理高效便捷，方法来了！》，载 http://beijing.qianlong.com/2022/0919/7635814.shtml，最后访问时间：2022 年 11 月 22 日。

〔42〕 参见上海市高级人民法院（2019）沪行终 204 号行政判决书。

〔43〕 参见辽宁省沈阳市中级人民法院（2016）辽 01 行终 386 号行政判决书。

〔44〕〔美〕劳伦斯·莱斯格：《代码 2.0：网络空间中的法律》（修订版），李旭、沈伟伟译，清华大学出版社 2018 年版，第 1 页。

裁量基准算法化。算法将裁量过程分解为可供机器运行的计算步骤，而代码则以机器语言的形式对计算步骤进行具体化表达。在自动化处罚裁量语境下，算法相当于裁量基准。不同于传统裁量基准，算法化裁量基准将法律适用过程中的事实要素直接纳入，实现事实与法律规范的具体对应。〔45〕

转译过程因存在必须由行政机关和算法设计师填补的判断空间而具有立法的色彩，可以将其类比为行政机关具有较大裁量空间的规则制定过程。例如，在设计 CBMS 系统时，由于算法设计师对规则进行编码时改变了上百条既定规则，系统相当于在阐明新规则。〔46〕规则制定过程是在阐释语义模糊的立法，在立法规定无法为规则制定提供清晰指引时，该过程会借助公众和专家的参与来增强规则制定的合法性和科学性。转译过程需要减小法律语言与机器语言之间的模糊空间。在将法律语言细化至更容易为算法设计师操作的技术标准和设计说明书过程中，可以借助公众和专家的知识作出价值判断和技术选择。在具体转译算法之时，法律语言到机器语言之间的判断空间，只能由行政机关和算法设计师来填补，此时算法可能偏离其所表达的法律的意图，偏离程度与判断空间的大小有关。下文主要针对法律语言到机器语言的转译过程，从转译过程的主体要求、所译法律的明确性要求和转译过程的透明度要求三方面提出转译型算法的控制方式。

（二）转译过程的主体要求

首先，行政机关采取自动化行政方式应获得立法的授权，即存在授权规范，具体规定何种行政机关在何种行政领域能够以自动化方式开展行政管理活动。当然授权规范的层级、授权的范围和事项，因自动化系统适用的领域、对公民合法权益的影响程度大小而有所不同。例如，电子警察系统的应用就需具备法律、行政法规的明确授权。新修订的《行政处罚法》第 41 条规定，利用电子技术监控设备收集、固定违法事实的行为，必须有法律、行政法规的授权，且需经过法制审核。〔47〕《道路交通安全法》第 114 条授予行政机关根据交通技术监控记录资料进行处罚的权力。〔48〕以上可以看作是行政机关使用电子警察系统的授权规范。需要注意的是，前述条款授权的范围限于“利用电子技术监控设备收集、固定违法事实”，不能扩大到利用电子警察系统直接作出行政处罚决定，进行处罚的权力仍然属于行政机关。从当前的立法情况来看，针对电子监控设备的使用问题，只有交通执法和市场监管两个领域有法律和行政法规的授权，环保、海关、农业领域的授权规范位阶是部门规章。〔49〕

其次，转译主体包括行政机关和私营部门的算法设计师，具有立法色彩的转译过程应满足转译主体合法性的要求。以“类裁量基准”的算法为例，裁量基准本身是行政机关根据授权法的旨意，对法定授权范围内的裁量权予以情节的细化和效果的格化而事先以规则的形式设定的一种具体化的判断选择标准，属于行政自制规范。〔50〕行政机关制定裁量基准的权力来自于立法授予的

〔45〕 参见王正鑫：《机器何以裁量：行政处罚裁量自动化及其风险控制》，载《行政法学研究》2022 年第 2 期。

〔46〕 参见前引〔36〕，Danielle Keats Citron 文，第 1279 页。

〔47〕《行政处罚法》第 41 条规定：“行政机关依照法律、行政法规规定利用电子技术监控设备收集、固定违法事实的，应当经过法制和技术审核，确保电子技术监控设备符合标准、设置合理、标志明显，设置地点应当向社会公布。”

〔48〕《道路交通安全法》第 114 条规定：“公安机关交通管理部门根据交通技术监控记录资料，可以对违法的机动车所有人或者管理人依法予以处罚。对能够确定驾驶人的，可以依照本法的规定依法予以处罚。”

〔49〕 相关授权规范参见《环境行政处罚办法》第 36 条、《海关监管区管理暂行办法》第 17 条、《农业行政处罚程序规定》第 37 条。

〔50〕 参见周佑勇：《裁量基准的制度定位——以行政自制为视角》，载《法学家》2011 年第 4 期。

行政裁量权，其将裁量基准转译成算法的过程本质上仍是在行使行政裁量权。行政机关选择与私营部门的算法设计师合作共同制定转译型算法的行为也在裁量空间之内，算法设计师的行为也因此具备了合法性基础。此时，算法设计师可以看作是行政机关手脚的延伸，其行为归属于行政机关；行政机关也需要通过细密的规范设计约束算法设计师的行为。

（三）转译法律的明确性要求

为了缩小算法设计师“转译法律”时的判断空间，行政机关应当尽可能地明确法律的含义。具体而言，在设计系统时，算法设计师需要明确系统将要实现的法律目标是什么，即确定“目标规范”，目标规范是系统运行时具体执行的法律。目标规范和算法之间是对应关系，前者是人类世界中由行政机关执行的法律语言，后者是由系统执行的机器语言，二者要实现的是同一行政目标。例如，闯红灯自动记录系统中运行的算法是用来自动认定闯红灯行为的机器语言，相应的目标规范是《道路交通安全法》第 44 条〔51〕和《道路交通安全法实施条例》第 38 条〔52〕中，红灯亮时禁止机动车通行的规定。目标规范是行政机关的执法依据。转译过程实际上是将目标规范这一法律语言转译成机器语言的过程，转译时需要细化、解释具体的法律用语，明确至机器可执行的程度。仍以闯红灯自动记录系统为例，《闯红灯自动记录系统通用技术条件》（GA/T 496—2014）对如何认定闯红灯行为作了更具体的规定：系统需要监测和记录的闯红灯行为是机动车违反交通信号灯红灯亮时禁止通行的规定，越过停止线并继续行驶的行为。〔53〕自动记录系统至少要记录三张反映闯红灯行为过程的图片，图片需符合《闯红灯自动记录系统通用技术条件》的要求。〔54〕为了减小法律语言转译为机器语言时可能出现的偏差，行政机关通常会发布相关技术标准，自动化系统的设计必须符合技术标准的要求。在技术标准的基础上，有必要事先为转译过程设计更为详细的说明书，尽可能地明确可能会引起算法设计师进行独立判断的问题。说明书应当经过法律专家与技术专家的审核，并应当被允许共享以及不断完善，以促使算法设计师的行为合乎规范要求。〔55〕

行政机关通过发布技术标准和设计转译算法说明书的方式减少法律语言的模糊性，为算法设计师提供更为明确的设计方向。但是，即便说明书的表述极尽详细，法律语言转译成算法的过程仍然存在算法设计师的主观判断空间。处于私主体地位的算法设计师受私益驱动，而行政管理活动需将公共利益作为首要考量因素，为了确保公共利益的实现，行政机关应当全程参与系统的设计过程，担任重要问题的最终决策者。

---

〔51〕《道路交通安全法》第 44 条规定：“机动车通过交叉路口，应当按照交通信号灯、交通标志、交通标线或者交通警察的指挥通过；通过没有交通信号灯、交通标志、交通标线或者交通警察指挥的交叉路口时，应当减速慢行，并让行人和优先通行的车辆先行。”

〔52〕《道路交通安全法实施条例》第 38 条第 1 款规定：“机动车信号灯和非机动车信号灯表示：（一）绿灯亮时，准许车辆通行，但转弯的车辆不得妨碍被放行的直行车辆、行人通行；（二）黄灯亮时，已越过停止线的车辆可以继续通行；（三）红灯亮时禁止车辆通行。”

〔53〕参见《闯红灯自动记录系统通用技术条件》（GA/T 496—2014）第 3.1、3.2 条。

〔54〕《闯红灯自动记录系统通用技术条件》（GA/T 496—2014）第 4.3.1.1 条规定：“系统应能至少记录以下 3 张反映闯红灯行为过程的图片：a）能反映机动车未到达停止线的图片，并能清晰辨别车辆类型、交通信号灯红灯、停止线；b）能反映机动车已越过停止线的图片，并能清晰辨别车辆类型、号牌号码、交通信号灯红灯、停止线；c）能反映机动车与 b）图片中机动车向前位移的图片，并能清晰辨别车辆类型、交通信号灯红灯、停止线。”

〔55〕参见前引〔34〕，丽莎·A. 谢伊、伍德罗·哈特佐格等文，第 295 页。

（四）转译过程的透明度要求

首先，转译型算法制定过程应满足公开的要求。转译过程公开的理论基点在于对公民知情权的保障，此处的知情权是指政治上的民主权利，即公民依法享有知道国家的活动、了解国家的事务的权利，国家机关有依法向公民及社会公众公开自己活动的义务，这是人民主权原则的延伸。〔56〕转译过程公开的内容包括公开转译主体、转译目的、转译依据以及源代码等，算法公开体现的是算法透明原则的要求。就具体规制手段而言，算法透明包含告知义务、向主管部门报备参数、向社会公开参数和存档数据、公开源代码等不同的形式。〔57〕算法公开的程序可参照行政规范性文件的公布程序。2008年起实施的《湖南省行政程序规定》率先规定了对规范性文件的统一登记、统一编号、统一公布制度，其后，“三统一”制度被推广至其他省份，目前已被中央层面法律文件纳入。〔58〕

其次，应在算法公开的基础上增强算法的可解释性。反对算法公开的理由之一是“算法透明≠算法可知”，即考虑到披露对象的技术能力、算法的复杂性、机器学习和干扰性披露四重因素，即使向公众公开源代码，公众也未必会理解算法的工作原理。〔59〕对行政机关施加解释算法的义务并非要求其准确地说明算法的工作原理，由于“算法黑箱”的制约，这可能在技术上也是不可行的。行政机关的解释性义务只需要做到提供必要的信息证明系统产生的结果是合理的即可。换言之，行政机关需要提供有关其自动化系统背后的目的及其通常如何运作的基本信息，需要表明在设计系统时已经仔细考虑了关键的设计选项，也可能需要借助公认的审核和验证工作来证明系统确实能够运行并生成预期的结果。〔60〕对行政机关施加公开算法和解释算法的义务，一方面是为了满足自动化行政自身合法性的要求，另一方面也有助于个人对自动化决策提出质疑，引发关于技术的辩论，从长远来看可以促进社会对新技术的接受。

五、自我学习型算法的控制

针对转译型算法，可以通过控制转译过程的合法性来保证算法决策的合法性，确保系统始终处于行政机关的控制之下。此时的规制逻辑是通过形式合法性来解释行政正当性，核心技术是评估行政与法律的一致性。〔61〕但自我学习型算法是根据预先设定的“学习规则”，学习训练数据之后生成的，本身具有不确定性。自我学习型算法无法满足形式合法性的要求，需要探索新的合法性框架，相应控制方式应在新的合法性框架下展开。

（一）“民主—科学”的合法性框架

1. 构建合法性框架的目的

自我学习型算法的适用需要具备合法性基础的本质原因是要保证系统行使行政权时像行政机

〔56〕 参见刘莘：《行政立法研究》，法律出版社2018年版，第167－168页。

〔57〕 参见汪庆华：《算法透明的多重维度和算法问责》，载《比较法研究》2020年第6期。

〔58〕 参见《国土资源部办公厅关于实行规范性文件“三统一”制度的通知》（国土资厅函〔2015〕523号）。

〔59〕 参见沈伟伟：《算法透明原则的迷思——算法规制理论批判》，载《环球法律评论》2019年第6期。

〔60〕 参见前引〔3〕，卡里·科利亚尼斯文。

〔61〕 参见前引〔8〕，王锡锌文。

关一样受到控制。传统法律体系对公权力的控制机制，使得公民可以充分相信行政机关在行使权力时始终以维护公共利益为目的；而逸脱了法律控制机制的系统，难以使公民相信其同样以维护公共利益的方式运转。换言之，控制系统是为了建立起公众对系统的信任。公众对系统的不信任不仅会导致系统本身合法性基础缺失，还会引发公众与系统的提供者——行政机关之间的信任危机。尽管自我学习型算法具有“黑箱”性质，其决策过程难以为人类理解，但这并不意味着人类无法对其建立信任。正如在医疗领域，尽管患者对药物或药物治疗的工作原理不甚了解，但其仍然愿意将生命健康托付给通常难以理解的治疗手段；问题的关键不在于人类是否知道特定药物的作用机理，而是该领域内是否存在充分的规则、制度和专业知识给予我们信心，使我们对治疗手段建立信任。〔62〕

2. 合法性框架分析

行政管理过程偏离形式合法性要求的问题并不限于自动化行政领域，只不过在自我学习型算法上尤为突出。当代行政是目标导向的积极活动，行政机关在目标界定、手段选择等方面，都拥有自主进行权衡和选择的权力；目标导向的行政，意味着法律对行政的控制，通常只能是宽泛的目标指引而非具体的指令控制。立法提出行政活动的宽泛目标，行政对目标进行判断、权衡以及对实现目标的手段进行选择裁量。〔63〕例如，在风险行政领域，由于立法者不具备关于风险的完整知识，需要广泛授予行政机关裁量权，依法行政实际上被依裁量行政替代。〔64〕行政机关规制风险的活动若要符合现代行政法治的基本要求，至少需要满足两个条件：一是价值合理性，即行政机关设定的风险规制目标能够为公众所接受，符合民众的需求，反映民众的偏好，体现卢梭所说的“公意”的要求，从而具有正当性；二是工具合理性，即行政机关规制风险的手段或措施基于精确的计算和预测，追求功效最大化，具有科学性。〔65〕风险行政背景下，行政机关通过增强行政过程中的民主性与科学性，来补强行政活动正当性。“民主—科学”的合法性框架也可以作为自我学习型算法适用的理论基础。

3. 合法性规制目的实现方式

“民主—科学”的合法性规制目的是建立公众对算法的信任。与自我学习型算法相同，诊疗过程对于患者而言同样具有“黑箱”性质，因此，医疗领域信任机制的构建方式可以为算法的规制提供借鉴。医疗领域的信任建立机制有以下三个要点：(1) 医疗服务提供者的能力。以医师为例，医师培训和考核机制、医师资格考试制度、医师执业注册制度、医师的执业规范要求、卫生健康主管部门和医疗卫生机构对医师的监督管理及问责制度等共同建立起一个保证医师专业水准的框架，使得公众即使无法直接评估其实际能力，也能对其建立信任。(2) 保护患者的利益。医学伦理规范和相关制度的存在使公众相信，相较于个人的经济利益，医师会将病人的利益放在首位。美国出台了《联邦反回扣法案》(The Federal Anti-Kickback Statute)、《医师酬劳阳光法案》

〔62〕 See Robin C. Feldman, Ehrik Aldana & Kara Stein, Artificial Intelligence in the Health Care Space: How We Can Trust What We Cannot Know, 30 (2) *Stanford Law & Policy Review* 399 (2019).

〔63〕 参见王锡锌：《行政法治的逻辑及其当代命题》，载《法学论坛》2011 年第 2 期。

〔64〕 参见赵鹏：《知识与合法性：风险社会的行政法治原理》，载《行政法学研究》2011 年第 4 期。

〔65〕 参见戚建刚：《风险规制过程合法性之证成——以公众和专家的风险知识运用为视角》，载《法商研究》2009 年第 5 期。

（Physician Payments Sunshine Act）来监督医师从医药企业获取利益的行为，平衡患者的最大利益与医师个人利益之间的关系。（3）信息的完整性。医师用于诊疗的数据的准确性、诊疗数据使用方式的适当性、诊疗数据的可访问性、可纠错性都有助于增进患者的信任。总体而言，建立信任的路径可以二分：一是建立患者的主体地位保障，对应要点（2）；二是建立诊疗过程的科学性保障，对应要点（1）（3）。两种路径大致可以分别与民主和科学相对应。

（二）自我学习型算法的民主控制要求

与保障患者的主体地位类似，自动化行政中的民主参与是为了使公众获得自尊、自主和自治的心理。〔66〕自我学习型算法的民主控制可以从两方面展开：一是行政机关在制定规制人工智能的法律法规、政策文件时，应当听取公众意见，并提供充分交流意见的平台；二是在算法投入运用阶段，拓宽公众发现、识别算法风险的渠道。

以算法治理为代表的数治主要关注工具有效性和效率，侧重于治理的事实和工具维度，对法治的“价值之治”侧面带来挑战。〔67〕这也导致算法治理中公众意见表达的空间被进一步压缩。反对人工智能立法的理由之一是缺乏精确度的法律难以满足对代码的规制需求。对此的反驳为，法律是在民主程序中妥协的产物，在妥协的过程中，公众不断朝最适当规则的方向达成共识。〔68〕规制算法的规则和政策的形成过程就是一个妥协和不断达成共识的过程，对算法规制的价值选择和目标确定应当以公众的意见为依据。应当规制哪些风险、如何进行价值位阶排序，以及置于何种议程进行规制，体现的是公众希望自己决定生活状态的意愿。〔69〕在参与过程中，公众能够从各种视角了解和理解算法，尽可能地消除对未知风险的疑虑，增进信任。

算法决策过程的瞬时性剥夺了相对人在行政程序中向决策者表达意见的机会，算法决策的黑箱特点使公众难以直接发现算法的技术性错误。对此，有学者提出通过建立“前瞻性基准”（prospective benchmarking）的方式对自我学习型算法的运行情况进行监督，具体而言，在采取算法决策的场景中，行政机关应当随机选取一组同类型的人工执法案例作为基准，公众能够以此作为对比样本，对算法决策结果进行监督，及时发现算法决策中可能存在的错误。〔70〕除此之外，行政机关应向公众提供算法查验途径，即面向用户或公众提供一个公开的查验渠道，使用户、交易者或第三方有机会检验算法能否实现其所宣称的目标，从而对算法的运行机理建立相当程度的了解和预期。〔71〕

（三）自我学习型算法的科学控制要求

自我学习型算法的科学性控制要求体现在两方面：一是对算法的提供者和算法技术的科学性、可靠性的保障；二是对数据可靠性的保障。在对算法提供者的控制方面，行政机关通过算法

〔66〕 参见沈岿：《风险规制决策程序的科学与民主》，载沈岿主编：《风险规制与行政法新发展》，法律出版社 2013 年版，第 308 页。

〔67〕 参见王锡锌：《数治与法治：数字行政的法治约束》，载《中国人民大学学报》2022 年第 6 期。

〔68〕 See Paul Nemitz, Constitutional Democracy and Technology in the Age of Artificial Intelligence Philosophical Transactions: Mathematical, 376 (2133) *Physical and Engineering Sciences* 1 (2018).

〔69〕 参见前引〔65〕，戚建刚文。

〔70〕 See David Freeman Engstrom & Daniel E. Ho, Algorithmic Accountability in the Administrative State, 37 *Yale Journal on Regulation* 800, 849 (2020).

〔71〕 参见苏宇：《算法规制的谱系》，载《中国法学》2020 年第 3 期。

进行治理，是自动化行政行为的直接责任主体，应当承担起对算法科学性的保障责任。第一，行政机关内部应该设立专门的算法审查机构，承担算法审查、算法监测、算法纠错等具体工作。考虑到当前阶段行政机关专业人才不足的问题，有学者建议目前可依托具有相应专业人才、技术支撑和监管能力的行业自律组织，建立起由相关行政机关负责指导、行业自律组织负责实施的算法监管体制。〔72〕第二，行政机关在选择第三方机构共同设计算法时，应当遵循公开透明、公平竞争、公正原则，设计单位的资质、选择单位的程序和标准等信息需向社会公开，并接受监督。

在对算法技术的控制方面，第一，建立算法标准和算法备案制度。统一的技术标准有助于确认某种算法现阶段的科学性和合理性；而算法备案制度便于查明算法风险，明确责任主体。第二，建立算法审查制度。算法设计过程需嵌入算法伦理，因此在设计阶段就应当以立法形式要求算法通过道德审查标准，防止产生不公平后果。〔73〕第三，建立算法影响评估制度，以中立、专业、可信的评估主体为保证，对算法设计、部署、运行的全部流程予以动态评估，在算法系统应用之前就进行独立的社会技术分析。〔74〕第四，开发监督算法运行、监测算法技术可靠性的算法。尽管对算法代码进行实时督导（monitoring）和审计（auditing），需要具备与算法生产和使用相当或超越的技术能力，成本巨大，〔75〕但以技术控制技术既可以推动科技进步，也能有效增进公众对科技的信任。前述控制手段大多是自上而下的机制设计，有可能因为利益关联或认知局限等原因阻碍算法的正常发展，因此，应当鼓励产业界、社会组织及个人创造和发展自下而上的风险识别与防范工具。〔76〕

在对数据可靠性的保障方面，第一，利用数据集缺陷检测技术。目前的人工智能技术已经完全可以为算法开发者提供数据集及训练过程检测工具，主要用于检测训练人工智能的数据集是否存在偏差或缺陷，还可以通过一定的算法检测在数据选取、数据标注、数据清洗以及其他预处理工作过程中是否包含了偏离算法设计目标或足以导致结果发生显著偏差的操作。〔77〕第二，提高数据的互操作性（interoperability）。〔78〕互操作性要求不同行政机关之间共享数据，能够更好地满足自我学习型算法对数据数量的要求，进而提高算法的准确性。

六、结　语

在民主国家，主权统治通过双重形式的透明实现合法性：首先，人民生活在自己制定的规则之下（民主参与）；其次，这些规则的适用能够在打开其解释黑箱的诉讼程序中提出争议（法治）。〔79〕

〔72〕 参见孙清白：《人工智能算法的“公共性”应用风险及其二元规制》，载《行政法学研究》2020 年第 4 期。

〔73〕 参见张凌寒：《算法规制的迭代与革新》，载《法学论坛》2019 年第 2 期。

〔74〕 参见张欣：《算法影响评估制度的构建机理与中国方案》，载《法商研究》2021 年第 2 期。

〔75〕 参见前引〔14〕，邱泽奇文。

〔76〕 参见前引〔71〕，苏宇文。

〔77〕 参见前引〔71〕，苏宇文。

〔78〕 See Peter K. Yu, Beyond Transparency and Accountability: Three Additional Features Algorithm Designers Should Build into Intelligent Platforms, 13 (1) *Northeastern University Law Review* 263, 290 (2021).

〔79〕 See Mireille Hildebrandt, Law as Information in the Era of Data-Driven Agency, 79 (1) *Modern Law Review* 1, 23 (2016).

这也是传统行政法中行政权获得合法性的途径，行政机关通过严格遵循依法行政原则，获得民主正当性。自动化行政方式面临合法性危机：转译型算法在转译过程中会嵌入算法设计师的判断，而来自私营部门的算法设计师可能尚未获得执行法律的授权，缺乏执法的合法性基础，这一问题在自我学习型算法中更为突出；此外，当前阶段，算法决策有时在事实上超出法律的授权范围，且缺乏畅通的救济机制。

因此，应当结合算法类型对算法进行控制。针对转译型算法，需要保证转译过程的合法性：首先，要有上位法授权行政机关以自动化的方式在某一领域开展行政活动，从而为引入第三方共同设计算法提供法律基础；其次，行政机关有义务细化系统所需执行的目标法律规范，以缩小转译过程的判断空间；最后，转译过程应参考规则制定程序，符合相应程序要求。针对自我学习型算法，传统合法性框架失去作用，应当通过行政过程中的民主性和科学性重构合法性基础，具体控制措施也应从公众参与和算法科学的角度展开。

Abstract: Algorithm in automated administration can be divided into translation algorithm and self-learning algorithm, and the use of algorithm is faced with legitimacy crisis. Algorithm designers in a private position embed their own judgments in translating legalese into machine language, creating the risk of rewriting the law. In addition, algorithmic decision-making sometimes exceeds the scope of legal authority in fact, and lacks the smooth relief mechanism. The legality control method of the algorithm should be adapted to the algorithm type. It is necessary to control the translation subject, the clarity of the translated law and the transparency of the translation process in combination with the nature and technical characteristics of the translation algorithm. For self-learning algorithm, we should first establish a "democracy-science" legitimacy framework, and the algorithm should be controlled from the perspective of building trust in the algorithms by guaranteeing the status of the public and the scientific nature of algorithms.

Key Words: automated administration, formal legitimacy, administrative democracy, administrative science, algorithmic trust

（责任编辑：刘　权　赵建蕊）

财经法学 No. 2，2022
pp. 146 - 162

论算法个性化定价的解构与规制
——祛魅大数据杀熟

雷　希*

内容提要：算法个性化定价的监管实践与理论分析未能遵循规制对策与问题相匹配的规制原理。该原理要求注意算法个性化定价与算法合谋定价、欺诈定价、歧视定价、个性化推荐的区别。同时基于危害性差异我们也应将算法个性化定价进一步分为三类：超高价格、超低价格和一般价格。超高价格或超低价格场景下的算法个性化定价危害可借助既有的法律框架得以消减。虽然一般价格场景下的算法个性化定价既没有损害消费者权益，也不会排除或限制竞争，但会从分配不公平和程序不公平两个角度诱发消费者不信任，动摇数字市场经济秩序。政府、经营者和消费者应以信任受损机理为基本遵循，合力共筑消费者信任，以实现创新发展和消费者利益保护的动态平衡。

关键词：大数据“杀熟”　算法个性化定价　分类规制　消费者信任

大数据“杀熟”已引起社会的广泛关注，社会各界曾强烈呼吁政府通过加强立法工作治理大数据“杀熟”现象，堵住监管漏洞。〔1〕《个人信息保护法》第 24 条被普遍解读为禁止大数据“杀熟”，〔2〕各地出台的地方性法规及规范性文件也对此作出了规定。〔3〕大数据“杀熟”又被称为算法价格歧视、个性化定价或差异化定价等，是公众对经营者利用算法为终端消费者个性化定价的一种俗称，即通过收集、清洗、处理和分析消费者消费习惯、消费能力等个人信息对消费者画像，预测消费者最高保留价格，并以此就同一商品向条件相同的消费者设定高低不同的价格。大

*　雷希，南京大学法学院博士研究生。

本文为国家社科基金一般项目“数字经济背景下企业数据权属及利用规则研究”（20BFX122）的阶段性成果。

〔1〕 参见《全国人大代表杨松：建议立法规制大数据杀熟、平台二选一等》，载 https://www.thepaper.cn/newsDetail_forward_11533557，最后访问时间：2022 年 1 月 5 日。

〔2〕 参见王利明：《〈个人信息保护法〉的亮点与创新》，载《重庆邮电大学学报（社会科学版）》2021 年第 6 期；王利明、丁晓东：《论〈个人信息保护法〉的亮点、特色与适用》，载《法学家》2021 年第 6 期。

〔3〕 如《上海市数据条例》《深圳经济特区数据条例》《浙江省电子商务条例》等。

数据“杀熟”并非学术用语，其主观色彩过于浓厚。如果用大数据“杀熟”指称这类行为则易形成框架效应（framing effect），导致立场先行，〔4〕不利于对此进行中立评价。〔5〕鉴于概念的使用还未有共识，且国内外不少学者也以算法个性化定价来指称该类行为，因此本文采用算法个性化定价来代替大数据“杀熟”这一用语。

国内外监管机关和理论界基于保护消费者、弥补市场失灵的目的，基本认可政府应采取措施规制算法个性化定价。〔6〕但难点在于应该如何规制算法个性化定价、既有法律框架是否足以解决算法个性化定价带来的挑战。对该类问题的理论研究，既是回应社会重大关切的现实之需，也是数字经济发展之求。

一、既有监管与理论的特点归纳及缺陷分析

我国目前对算法个性化定价的监管思路呈现出一刀切禁止的特点，国内理论研究则呈现出一般化分析的特点。一刀切禁止的监管思路和一般化的理论研究均存在不足，有待进一步完善。

（一）监管一刀切禁止的特点与缺陷

有关算法个性化定价的国内监管呈现出一刀切禁止的特点，即以统一适用的禁止性规范规制涉及算法个性化定价的所有问题。例如，2021 年国家市场监督管理总局、中央网信办、国家税务总局提出必须“严肃整治”算法个性化定价。国务院反垄断委员会制定的《关于平台经济领域的反垄断指南》第 17 条，被认为是对算法个性化定价这一热点问题的回应。〔7〕《价格违法行为行政处罚规定（修订征求意见稿）》将算法个性化定价视为“新业态中的价格违法行为”，明确将按销售总额比例罚款。类似一刀切禁止性的规定还有不少。〔8〕结合违法惩戒机制，这种一刀切禁止的监管思路具有较强的威慑力。

一刀切禁止的思路有很强的民意及舆论基础。如 2019 年北京市消协的调研结果显示，绝大多数被调查者（83.74%）认为算法个性化定价侵犯了消费者公平交易权，类似比例的被调查者（81.41%）要求政府加强监管以减少此类行为。〔9〕除此之外，一刀切禁止还可以为将来的灵活

〔4〕 See Ariel Ezrachi, Maurice E. Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*, Harvard University Press, 2016, pp. 111 - 113.

〔5〕 笔者于“中国知网”搜索相关 CSSCI 论文发现：一般而言，采用大数据杀熟或算法歧视这类表述的文章，基本假定算法个性化定价攫取消费者剩余，限制竞争，应该予以规制；而采用中立性表述的文章一般认为算法个性化定价危害性较为复杂，需要结合不同场景进行分析。

〔6〕 参见喻玲：《算法消费者价格歧视反垄断法属性的误读及辨明》，载《法学》2020 年第 9 期；Organisation for Economic Co-operation and Development (OECD), Price Discrimination: Background Note by the Secretariat, DAF/COMP (2016) 15.

〔7〕 参见《促进平台经济规范有序创新健康发展 ——〈国务院反垄断委员会关于平台经济领域的反垄断指南〉解读》，载 http://gkml.samr.gov.cn/nsjg/xwxcs/202102/t20210207_325970.html，最后访问时间：2022 年 1 月 5 日。

〔8〕 例如《商务部办公厅开展“2021 年全国网上年货节”活动的通知》、文化和旅游部《在线旅游经营服务管理暂行规定》、国家市场监督管理总局联合商务部共同提出“社区团购‘九不得’”、国家互联网信息办公室《数据安全管理办法（征求意见稿）》等。

〔9〕 参见《北京市消协发布大数据“杀熟”问题调查结果》，载 http://www.bj315.org/xxyw/xfxw/201907/t20190727_19494.shtml，最后访问时间：2022 年 1 月 5 日。

规制预留充足时间，〔10〕在短时间内也可以为市场注入一剂强心针。

但一刀切禁止的处理方法只能是一时的应对之策。相较于包容审慎监管，一刀切禁止所能获得的效益小于增加的成本。〔11〕更为重要的是，算法个性化定价的经济效果较为复杂，对经营者、消费者及社会也会带来一定程度的正面效应。英国竞争与市场监管局（CMA）2021 年发布研究报告指出，算法个性化定价尽管有时会损害消费者利益，甚至侵蚀整体经济效率，但有时也能够增加消费者福利。〔12〕一味禁止个性化定价，会使得个案处理欠缺灵活性，〔13〕从长远来看甚至还会损害消费者权益〔14〕。一刀切禁止的实效也不容乐观。CMA 调查发现天然气与电力市场办公室（Ofgem）2009 年禁止区域差异化定价的决定并未产生促进竞争的效果，相反还弱化了竞争。〔15〕

综上，对算法个性化定价的监管不宜采用一刀切禁止的思路。〔16〕近期出台的《个人信息保护法》《互联网信息服务算法推荐管理规定》和《浙江省电子商务条例》等规定仅禁止“不合理”的算法个性化定价，试图从一刀切禁止的监管策略转变为合理分析。但这些规定并未明确“不合理”的概念，这就要求监管者进行个案分析。然而由于监管能力与监管成本的约束，监管者在个案的实际判断中可能仍会偏向于一刀切处理。这意味着，尽管部分监管规范的表述由禁止转为合理分析，但其实践效果没有发生变化，市场活力可能仍会受挫。

（二）理论一般化分析的特点与缺陷

国内对算法个性化定价的研究呈现出“一般化”的特点，也就是将所有危害都归因于算法个性化定价这个一般性概念上，未区分不同情形下算法个性化定价的危害差异。具体表现为：其一，有的研究断言算法个性化定价不仅可能攫取消费者剩余，而且还可能扭曲市场竞争机制，排除限制竞争。〔17〕其二，有的研究从不同部门法角度讨论算法个性化定价的危害性，意图为一般性禁止算法个性化定价提供具体条文依据。例如从消费者保护法的角度，有观点认为算法个性化定价侵犯消费者知情权、选择权或公平交易权；〔18〕从反垄断法的角度，有观点认为算法个性化定价构成剥削性差别待遇；〔19〕从行政行为法和行政作用法视角，也有学者讨论规制算法个性化定价的理论正当性〔20〕。前述部门法视角的讨论仍旧将所有可能的危害笼统地归咎于算法个性化

〔10〕 有研究发现，政府强监管的初始意愿越强烈，互联网企业演化到算法个性化定价的速度越慢。参见邢根上、鲁芳、罗定提：《政府监管下的电商大数据“杀熟”演化仿真分析》，载《湖南工业大学学报》2021 年第 2 期。

〔11〕 参见潘定、谢菡：《数字经济下政府监管与电商企业“杀熟”行为的演化博弈》，载《经济与管理》2021 年第 1 期。

〔12〕 See Competition & Markets Authority (“CMA”), Algorithms: How They Can Reduce Competition and Harm Consumers, Jan. 19, 2021, pp. 8 - 9, available at https://www.gov.uk/government/publications/algorithms-how-they-can-reduce-competition-and-harm-consumers, last visited on Jan. 5, 2022.

〔13〕 参见宋亚辉：《社会性规制的路径选择：行政规制、司法控制抑或合作规制》，法律出版社 2017 年，第 164 - 165 页。

〔14〕 See Alex Schofield, Personalized Pricing in the Digital Era, 18 *Competition Law Journal*, 35, 40 (2019).

〔15〕 See CMA, Energy Market Investigation, Final Report, Jun. 24, 2016, available at: https://assets.publishing.service.gov.uk/media/5773de34e5274a0da3000113/final-report-energy-market-investigation.pdf, last visited on Jan. 5, 2022; OECD, Personalised Pricing in the Digital Era-Note by the United Kingdom, p. 12, DAF/COMP/WD (2018) 127.

〔16〕 参见李毅、李振利：《数字经济背景下对消费者实行个性化定价违法边界的研究》，载《社会科学》2020 年第 2 期。

〔17〕 参见李丹：《算法歧视消费者：行为机制、损益界定与协同规制》，载《上海财经大学学报》2021 年第 2 期。

〔18〕 参见王佳琪：《大数据“杀熟”的法律应对》，载《人民法院报》2019 年 6 月 11 日，第 002 版。

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

〔20〕 参见李帅：《共享经济信息不对称环境下的决策算法规制——以区块链共识模型为规制思路》，载《财经法学》2019 年第 2 期。

定价，未能进行场景化和类型化分析。当然，确实也有学者尝试进行类型化分析。有的主张“对于不同类型的个性化定价算法应做区分处理”〔21〕，有的认为应“基于消费者细分的视角”坚持个案分析〔22〕。这些观点虽然意识到算法个性化定价在不同条件下呈现出不同效果，但也仅是一般性地提及个案分析中应考虑的原则，尚未落实如何分类规制。

一般化分析兼具进步之处与不足之处。其进步之处包括：一是明确算法个性化定价可能的危害性，解决了规制必要性问题；二是提出算法个性化定价的综合规制进路，并试图深入到各部门法领域进行研究。

缺陷之处则体现在三个方面。第一，既有研究未能意识到算法个性化定价并非独立概念，其外延并非独一无二，而是包含多种具有不同危害性的子类行为。一般化分析将算法个性化定价视为一个整体进行研究，遇到具体场景时便会暴露出解释力不足的问题。第二，一般化分析容易混淆算法个性化定价子类行为的危害，可能产生规制错配的问题。例如，有观点将特定类型算法个性化定价对消费者权益的损害视为算法个性化定价共有的特征，进而主张通过援引“维护消费者利益”这个一般条款而适用《反垄断法》规制所有算法个性化定价。〔23〕然而，有些类型的算法个性化定价既不损害消费者权益，也不排除限制竞争，此时如果《反垄断法》介入势必会导致规制错配。第三，一般化分析未能遵循问题与对策相匹配的规制原理，未能厘清不同场景下的算法个性化定价的危害差异，未能据此构建规制进路。

二、基于危害差异的类型化研究

针对上述缺陷，改进方法是围绕算法个性化定价不同子类行为的危害差异进行类型化处理，从而为具体规制路径的建构奠定基础。

（一）理据与功能分析

以危害性差异为基础进行类型化研究不仅可用规制理论来论证其正当性，而且也因其多重价值而具有必要性。

第一，类型化研究根源于规制路径应与问题相匹配的基本原理。算法个性化定价的规制路径选择具有鲜明的实用主义色彩，无论如何设计规制路径（是自由放任，抑或照搬或准用既有法律规定，甚或是重建），都必须遵循对策与问题相匹配的规制原理。〔24〕否则可能产生规制失败、规制错配等问题。〔25〕

〔21〕 周围：《人工智能时代个性化定价算法的反垄断法规制》，载《武汉大学学报（哲学社会科学版）》2021 年第 1 期，第 108、110 页。

〔22〕 参见喻玲、兰江华：《算法个性化定价的反垄断法规制：基于消费者细分的视角》，载《社会科学》2021 年第 1 期。

〔23〕 参见承上：《人工智能时代个性化定价行为的反垄断规制——从大数据杀熟展开》，载《中国流通经济》2020 年第 5 期。

〔24〕 参见宋亚辉：《网络市场规制的三种模式及其适用原理》，载《法学》2018 年第 10 期。

〔25〕 参见〔美〕史蒂芬·布雷耶：《规制及其改革》，李洪雷、宋华琳、苏苗罕、钟瑞华译，北京大学出版社 2008 年版，第 277 页及以下。

第二，基于危害差异解构算法个性化定价具有多重价值。首先，解构算法个性化定价可以弥补一刀切禁止和一般化分析的缺陷。类型化的思考有助于我们清楚地掌握算法个性化定价的多种类型，避免将不同危害混为一谈；更有助于对算法个性化定价进行规范分析，探寻不同法律在算法个性化定价场景下的适用空间。其次，类型化的分析可以辅助判断是否存在规制失败，进而便于查漏补缺。最后，类型化分析相较于个案分析具有节省成本、提高法律确定性的作用。个案分析的优点是可以基于个案具体情况灵活选择不同的规制进路，但缺点在于耗时耗力，且无法给市场主体稳定的行为预期。通过类型化分析，事先明确各类算法个性化定价的规制路径，能够发挥法律规则的行为指引作用。

（二）解构算法个性化定价

算法个性化定价存在多种表现形式，各种表现形式的危害存在差异，应据此探寻算法个性化定价的类型。但在此之前，有必要厘清算法个性化定价与相关概念的差异。因为尽管算法个性化定价的内涵与相关概念的内涵不同，危害性也迥异，但目前的研究存在概念混淆的问题，有碍规制路径的构建。

1. 厘清算法个性化定价内涵

第一，应注意区分算法个性化定价与个人信息保护问题、“信息茧房”困境。按照行为机制，利用算法技术实施个性化定价的行为可以分为信息采集、信息推送、个性化定价三个阶段。〔26〕这三个阶段的行为表现及危害性各不相同。信息采集阶段主要涉及个人信息知情同意、用户画像、隐私侵权等问题，信息推送阶段的主要危害在于信息茧房，算法个性化定价是发生在第三个阶段的行为。然而，有些研究混淆了上述三个阶段的危害。例如，有观点认为算法个性化定价因为违背了消费者对数据及隐私的实质期待而是不公平的；〔27〕也有观点将信息个性化推送归类为“大数据杀熟”，〔28〕还有观点试图通过解释《电子商务法》第 18 条第 1 款关于个性化推送的规定以解决算法个性化定价问题〔29〕。本文认为，在建构算法个性化定价的规制路径时，不能混淆算法个性化定价与信息采集阶段的个人信息保护问题、信息推送阶段的“信息茧房”问题。用《个人信息保护法》第 24 条禁止算法个性化定价可能有违《个人信息保护法》的规制逻辑，不仅可能会使得相关规定泛化，〔30〕还会造成规制错配。这是因为算法个性化定价的成因并非个人信息保护不足，〔31〕《个人信息保护法》可提高个人信息保护水平，但很难对算法个性化定价形成有效规制。

---

〔26〕 参见前引〔17〕，李丹文。

〔27〕 See Christopher Townley, Eric Morrison, Karen Yeung, Big Data and Personalized Price Discrimination in EU Competition Law, 36 *Yearbook of European Law*, 683, 710 - 711 (2017).

〔28〕 参见郑智航、徐昭曦：《大数据时代算法歧视的法律规制与司法审查——以美国法律实践为例》，载《比较法研究》2019 年第 4 期。

〔29〕 参见付丽霞：《大数据价格歧视行为之非法性认定研究：问题、争议与应对》，载《华中科技大学学报（社会科学版）》2020 年第2 期。

〔30〕 参见文铭、莫殷：《大数据杀熟定价算法的法律规制》，载《北京航空航天大学学报（社会科学版）》，2021 年 9 月 18 日网络首发。

〔31〕 参见李三希、武玙璠、鲍仁杰：《大数据、个人信息保护和价格歧视——基于垂直差异化双寡头模型的分析》，载《经济研究》2021 年第 1 期。

第二，应注意区分算法个性化定价和其他价格违法行为，比如算法合谋定价、算法欺诈定价、算法歧视定价。首先，个性化定价与合谋定价差异明显。个性化定价的特点在于价格存在较大差别，而合谋定价的特点在于价格一致，两者表现形式不同。尽管算法可能辅助经营者就同一消费者达成统一动态价格，但尚未有足够证据证明这已成为现实。〔32〕算法合谋定价行为可由《价格法》第14条第1项或《反垄断法》予以规制。其次，个性化定价并非欺诈定价，这是因为欺诈需要有误导性陈述，而个性化定价并不会使消费者陷入双重错误。那些认为算法个性化定价构成价格欺诈的观点，〔33〕混淆了个性化定价与欺诈定价。算法欺诈定价可由《民法典》以及《消费者权益保护法》第20条和第55条予以规制。最后，算法歧视定价是平等权语境下的概念，体现为针对性别、种族等身份方面的歧视定价，可通过“反歧视法律数字化转型”得以解决。〔34〕

2. 解析算法个性化定价外延

根据危害性差异，可将算法个性化定价的外延解构为三个非空的子类：超高价格、超低价格和一般价格。这三类行为囊括了算法个性化定价的所有类型。

（1）超高价格

超高价格是指明显高于商品或服务市场价值的价格。市场交易本应是平等互惠互利的。超高价格的潜在危害在于导致交易显失公平，侵害消费者福利。经营者利用数据与算法探知消费者的价格极限，向高支付意愿的消费者收取超高价格，过度剥夺了这部分消费者剩余，使得交易难以对消费者产生增益。超高价格还使得消费者与经营者之间的付出与收益不成比例，损害了实质公平。例如在浙江省绍兴市柯桥区法院审理的胡女士诉上海携程商务有限公司侵权纠纷一案中，胡女士通过“携程”订购房间的价格为2889元，而通过线下预定则仅为1377.63元，〔35〕此时价差达到了一倍，应属于超高价格。

（2）超低价格

超低价格是明显低于商品或服务市场价值的价格。利用算法设定过低价格可能排除限制竞争、扰乱正常经营秩序。经营者通过差异化定价向高支付意愿的消费者收取较高利润，以此补贴低支付意愿的消费者，利用低价留住这部分消费者，或吸引新消费者。当经营者持续地以超低价格销售商品或提供服务，便很可能会产生扰乱正常经营秩序的效果。在经营者处于市场支配地位时还会产生排除限制竞争的效果。利用算法设置超低价格的行为在经济生活中确有可能发生。〔36〕例如，“多多买菜”“美团优选”等社区团购便被爆出采取补贴的方式低价竞争，甚至个别产品远低于出厂价。〔37〕对这些社区团购平台而言，利用算法设置个性化的超低价格具有很

〔32〕 See OECD, Personalised Pricing in the Digital Era-Note by the European Union, pp. 6－7, DAF/COMP/WD (2018) 128.

〔33〕 参见邹开亮、刘佳明：《大数据“杀熟”的法律规制困境与出路——仅从〈消费者权益保护法〉的角度考量》，载《价格理论与实践》2018年第8期。

〔34〕 参见李成：《人工智能歧视的法律治理》，载《中国法学》2021年第2期。

〔35〕 参见史洪举：《以司法裁判向大数据杀熟说不》，载《人民法院报》2021年7月17日，第02版。

〔36〕 See Ariel Ezrachi, Maurice E. Stucke, *Virtual Competition: The Promise and Perils of the Algorithm-Driven Economy*, Harvard University Press, 2016, pp. 119, 297.

〔37〕 参见吴睿鸽：《警惕社区团购“烧钱大战”戕害市场竞争秩序》，载《中国消费者报》2020年12月15日，第001版。

大的吸引力。

（3）一般价格

除超高价格和超低价格之外的价格，都是一般价格。大部分算法个性化定价都是这种价格。〔38〕正如欧盟 2018 年调研报告所指出的，实践中算法个性化定价的平均价差基本不超过 1%，最大价差也低于 4%。〔39〕这意味着算法个性化定价普遍价差幅度不大，并非明显低于或高于市场价值。由此衍生的相关问题是：一般价格场景下的算法个性化定价是否具有危害性，是否因属于经营者自主定价范围而可采取“自由放任”的态度。

三、一般价格的危害性再审视

超高价格与超低价格的算法个性化定价危害较为明确，而一般价格的危害比较模糊，有必要再审视一般价格场景下算法个性化定价的危害，从而明确是否需要规制以及如何规制。

（一）一般价格危害性的“去伪”

既有研究采用一般化的分析，认为算法个性化定价兼具侵犯消费者权益、剥削消费者剩余以及扭曲市场竞争的危害性。然而，一般价格场景下的算法个性化定价并不具有前述危害。

1. 一般价格的危害不在于损害消费者权益

一般价格场景下算法个性化定价并不具有损害消费者权益的危害性。第一，消费者法定权利未受侵害。不少观点曾主张算法个性化定价损害了消费者知情权和自主选择权，应予禁止。〔40〕然而，这类观点违背了法律条文的通常含义，为学者所批判。〔41〕实际上，《消费者权益保护法》第 8 条规定的知情权，只是知悉商品或服务“真实情况”的权利，不包括经营者与其他消费者的交易价格。经营者与其他主体的交易情况，有时甚至可能构成商业秘密。第 9 条明确了消费者享有自主选择权，“有权进行比较”，但比较的对象是商品，而不是成交价。《消费者权益保护法》第 20 条和《价格法》第 13 条规定的经营者“明码标价”义务，〔42〕只要求经营者明确标示价格，不要求经营者在不同时间针对不同人的报价均保持一致，否则便可能违背《价格法》第 11 条规定的经营者自主定价权。《互联网信息服务算法推荐管理规定》第 21 条从保护公平交易权的角度规制算法个性化定价，这种思路得到了一些学者的认可。但本文认为，公平交易权的规制路径或可适用于超高价格的场景，但在一般价格场景下，经营者并未向消费者收取不公平高价，并未侵

〔38〕 参见施春风：《定价算法在网络交易中的反垄断法律规制》，载《河北法学》2018 年第 11 期。

〔39〕 See European Commission (EC), Consumer Market Study on Online Market Segmentation Through Personalised Pricing/Offers in the European Union, p. 219, June 2018, available at https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/synthesis_report_online_personalisation_study_final_0.pdf, last visited on Jan. 5, 2022.

〔40〕 参见陈兵：《法治经济下规制算法运行面临的挑战与响应》，载《学术论坛》2020 年第 1 期；雷雨田：《运用大数据不宜“看人下菜碟”》，载《经济日报》2021 年 3 月 16 日，第 09 版。《禁止网络不正当竞争行为规定（公开征求意见稿）》也从这一角度提出了应规制算法个性化定价。

〔41〕 参见杨成越、罗先觉：《算法歧视的综合治理初探》，载《科学与社会》2018 年第 4 期。

〔42〕 有观点便认为算法个性化定价违背“明码标价”要求。参见刘佳明：《大数据“杀熟”的定性及其法律规制》，载《湖南农业大学学报（社会科学版）》2020 年第 1 期。

害消费者公平交易权。

第二，消费者剩余并不必然减少。有研究表明，有时算法个性化定价会导致整体福利提高而适度降低个体消费者剩余，有时算法个性化定价会刺激竞争进而有利于消费者。〔43〕一般价格场景对消费者剩余而言兼具积极和消极影响，很难精确判断其具体效果。〔44〕尽管可以确定，若能实现经济学意义上的一级价格歧视，则一定会损害消费者权益，〔45〕但就当下实践与方法而言，尚无证据证明经营者能够实现真正的一级价格歧视。

第三，即便一般价格场景下特定消费者权益一定程度上受损，也无需政府干预。首先，一般价格场景下的算法个性化定价符合商业惯例，在现实生活中是比较常见的。只要不构成欺诈、不公平价格等情形，法律一直采取的是放任态度，任由市场自发调节。其次，消费者可采取措施自我保护。“杀熟”靠技术，“反杀熟”靠智慧。〔46〕通过增加搜索次数、迟延支付等方式将自己包装成谨慎的消费者，消费者大概率可避免被经营者收取相对高价。质疑观点可能会认为这会增加消费者交易成本，但多次搜索不过是消费者自我保护的体现，也是《消费者权益保护法》第13条对消费者的期待。

2. 一般价格的危害性不在于排除限制竞争

一般价格场景下的算法个性化定价危害不在于排除限制竞争，不应由《反垄断法》规制。第一，并未违反《反垄断法》的具体规定。《反垄断法》第17条第1款第6项关于差别待遇的规定，被有的学者认为可用于规制一般价格场景下的算法个性化定价——“没有正当理由，对条件相同的交易相对人在交易价格等交易条件上实行差别待遇”。然而，对该条进行规范分析可以发现，遭受差别待遇的对象是“交易相对人”，其仅指经营者，并不包括终端消费者。首先，参与立法起草审议的立法工作者指出，差别待遇被《反垄断法》禁止的原因在于该行为会“致使有的交易相对方处于不利的竞争地位”〔47〕，这意味着“交易相对人”仅指经营者，而不包括消费者。其次，《反垄断法》第14条关于垄断协议的规定也使用了“交易相对人”的表述，这里的“交易相对人”通常不包括终端消费者。根据一致用法推定的解释原则，词语应被推定在同一法律文本中具有相同的含义，〔48〕那么《反垄断法》第17条第1款第6项规定的“交易相对人”也不应包括终端消费者。最后，反对观点主张采用目的性扩张解释，通过援引目的条款中的“维护消费者利益”将第6项扩张适用于针对终端消费者的差别待遇。也有观点提出可从剥削性滥用的角度规

〔43〕 See Mark Armstrong, Recent Developments in the Economics of Price Discrimination, in Richard Blundell et al. ed., *Advances in Economics and Econometrics: Theory and Applications, Ninth World Congress*, Cambridge University Press, 2013, pp. 114 - 115, 120 - 126.

〔44〕 See Pascale Chapdelaine, Algorithmic Personalized Pricing, 17 *New York University Journal of Law and Business*, 1, 29 (2020); William W. Fisher III, When Should We Permit Differential Pricing of Informatioin? 55 *UCLA Law Review*, 1, 20 - 37 (2008); 王文君：《算法个性化定价的反垄断法反思》，载《甘肃政法大学学报》2021年第5期。

〔45〕 参见方师师：《用大数据方法破解“大数据杀熟”》，载《光明日报》2021年4月30日，第02版。

〔46〕 参见文阳：《“杀熟”靠技术，“反杀熟”靠智慧》，载 https://static.cdsb.com/micropub/Articles/202103/44ea81710cd04a6604253c6b25fb4403.html，最后访问时间：2022年1月5日。

〔47〕 安建主编：《中华人民共和国反垄断法释义》，法律出版社2018年版，第51页。

〔48〕 参见王利明：《法学方法论》，中国人民大学出版社2012年版，第381页；Antonin Scalia, Byran A. Garner, *Reading Law: The Interpretation of Legal Texts*, Thomson/West, 2012, p. 186.

制一般价格场景下的算法个性化定价。〔49〕但如前所述，一般价格场景下的算法个性化定价并不损害消费者权益，援引一般条款或剥削性滥用条款难以成立。

第二，一般价格场景下的算法个性化定价不具有排除限制竞争的实质危害性。直接以终端消费者为客体的差别待遇，一般而言不具有排除限制竞争的效果。〔50〕所谓“排除限制竞争”，是指排除限制企业之间的竞争。一般价格场景下的算法个性化定价显然不具有排除限制竞争效果。

第三，《反垄断法》的内在逻辑也决定了一般价格场景下的算法个性化定价不应由《反垄断法》规制。《反垄断法》的内在逻辑在于恢复市场竞争，使市场机制运行正常，不能也不应该涉足即使是正常市场机制也无法解决的领域。与格式合同附随条款因缺乏关注而易形成垄断均衡一样，〔51〕一般价格场景下的算法个性化定价同样难以被消费者关注，这意味着即使由《反垄断法》调整并恢复至自由竞争市场，也仍然会出现此类算法个性化定价行为。

（二）一般价格危害性的“存真”

一般价格场景下的算法个性化定价不损害消费者利益，也不扭曲市场竞争，是否意味着其不具有危害性？自由主义学派可能会主张一般价格应该得到尊重，因为这是经营者行使自由定价权的必然结果，是市场经济的核心特征。〔52〕例如美国代表及工商业咨询委员会（BIAC）在经济合作与发展组织（OECD）“数字时代的个性化定价”圆桌会上都明确提出若不涉及反竞争效果、不公平或欺诈的行为，算法个性化定价便不构成竞争或消费者权益保护问题，此时应避免过度执法可能带来的问题。〔53〕但与会的英国代表提出，除了竞争与消费者权益保护问题外，算法个性化定价还可能会严重影响消费者对数字经济的信心。〔54〕会前 OECD 秘书处提供的背景材料同样指出：个性化定价的实施是不透明的，存在着减少市场信任的风险，可能抑制消费者在数字市场的参与。〔55〕社会舆论普遍认为算法个性化定价会透支消费者信任，引发信任危机。〔56〕那么一般价格场景下的算法个性化定价是否会损害消费者对数字市场的信任？本文给出的是肯定回答。

1. 消费者信任经营者

数字市场上，消费者对经营者具有实然和应然的信任。首先，“信任”的经典含义是指 A 方愿意将自己软肋暴露给 B 方并期待着 B 方会为 A 方利益行事，而不管 A 方是否有能力对 B 方进

〔49〕 参见郝俊淇：《平台经济领域差别待遇行为的反垄断法分析》，载《法治研究》2021 年第 4 期。

〔50〕 参见丁茂中：《论差别待遇的合理性分析标准》，载《上海对外经贸大学学报》2018 年第 5 期。

〔51〕 参见马辉：《格式条款信息规制论》，载《法学家》2014 年第 4 期；解亘：《格式条款内容规制的规范体系》，载《法学研究》2013 年第 2 期。

〔52〕 参见梁正、曾雄：《“大数据杀熟”的政策应对：行为定性、监管困境与治理出路》，载《科技与法律》2021 年第 2 期。

〔53〕 See OECD, Personalised Pricing in the Digital Era-Note by the United States, DAF/COMP/WD (2018) 140; OECD, Personalised Pricing in the Digital Era-Note by BIAC, DAF/COMP/WD (2018) 123.

〔54〕 See OECD, Personalised Pricing in the Digital Era-Note by the United Kingdom, DAF/COMP/WD (2018) 127.

〔55〕 See OECD, Personalised Pricing in the Digital Era: Background Note by the Secretariat, DAF/COMP (2018) 13.

〔56〕 参见周菊：《大数据“杀熟”是透支消费信任》，载《中华工商时报》2018 年 3 月 2 日，第 003 版；刘丽、郭苏建：《大数据技术带来的社会公平困境及变革》，载《探索与争鸣》2020 年第 12 期。

行监督或控制。〔57〕这一定义已得到普遍认可。〔58〕其次，消费者对经营者的信任，直接体现在消费者依据《网络安全法》和《个人信息保护法》同意向经营者提供可能对消费者不利的信息，同意的结果使得消费者的弱势地位更为明显。这种同意行为意味着消费者信任经营者不会利用这些信息对消费者不利。再次，消费者对具有强大算力的经营者的信任，还体现在消费者对这些类似于“专家系统”的经营者的信任，相信他们发挥着第三方监管的作用。〔59〕最后，从应然层面来看，消费者对经营者的信任是数字经济发展所必然要求的。尤其在网络时代，信任发挥着类似于“公地资源”〔60〕或“数字经济的货币”〔61〕的重要作用。

2. 主观不公平感会减损消费者信任

算法个性化定价会破坏消费者对特定经营者的信任，其内在逻辑在于算法个性化定价会引发消费者主观不公平感，这种不公平感会削弱消费者的信任。

第一，调查问卷清楚表明消费者对算法个性化定价的主观感受。2019 年北京市消协发布相关调查报告，数据显示有 82.54％的被调查者认为算法个性化定价将严重透支消费者信任、降低企业声誉，81.41％的被调查者认为算法个性化定价会损害消费者权益。〔62〕2020 年南都反垄断研究课题组发布的《互联网平台竞争与垄断观察报告》显示，1300 多名受访者中有 73％反对算法个性化定价。〔63〕此外，有学者在调查美国 1500 户家庭后发现，约有 91％的受访者对算法个性化定价表示强烈反感，87％的受访者认为这种行为是错误的，76％的受访者会因为他人支付相对低价而懊恼。〔64〕一项针对近 300 名学生的调研显示，受访者倾向于认为算法个性化定价严重影响消费者对公平的感知。〔65〕另一项调研显示，78％的消费者甚至不希望得到基于上网痕迹提供的个性化折扣。〔66〕在对荷兰上千位消费者进行问卷调查后，有研究发现超过 80％的消费者认为算法个性化定价是不公平的、不可接受的，应予禁止。〔67〕欧盟委员会 2018 年进行的针对 2 万

〔57〕 See Roger C. Mayer, James H. Davis, F. David Schoorman, An Integrative Model of Organizational Trust, 20 *The Academy of Management Review*, 709, 712 (1995).

〔58〕 See Ellen Garbarino, Olivia F. Lee, Dynamic Pricing in Internet Retail: Effects on Consumer Trust, 20 *Psychology and Marketing*, 495, 500 (2003).

〔59〕 参见李飞翔：《“大数据杀熟”背后的伦理审思、治理与启示》，载《东北大学学报（社会科学版）》2020 年第 1 期。

〔60〕 谢尧雯：《网络平台差别化定价的规制路径选择——以数字信任维系为核心》，载《行政法学研究》2021 年第 5 期，第 27－28 页。

〔61〕 许可：《数字经济视野中的欧盟〈一般数据保护条例〉》，载《财经法学》2018 年第 6 期，第 74 页。

〔62〕 参见前引〔9〕。

〔63〕 参见黄莉玲、李玲、黄慧诗：《南都发布〈互联网平台竞争与垄断观察报告〉市场竞争失序产生垄断要大力监管》，载《南方都市报》2020 年 12 月 23 日，第 A07 版。

〔64〕 See Joseph Turrow, Lauren Feldman, Kimberly Meltzer, Open to Exploitation: America's Shoppers Online and Offline, A Report Annenberg Public Policy Center of the University of Pennsylvania, June 2005, available at https://repository.upenn.edu/asc_papers/35, last visited on Jan. 5, 2022.

〔65〕 See Kelly L. Haws, William Bearden, Dynamic Pricing and Consumer Fairness Perceptions, 33 *Journal of Consumer Research*, 304, 309 (2006).

〔66〕 See Joseph Turrow, Jennifer King, Chris J. Hoofnatle, Amy Bleakley, Michael Hennessy, Americans Reject Tailored Advertising and Three Activities That Enable It, Sept. 29, 2009, available at https://ssrn.com/abstract＝1478214, last visited on Jan. 5, 2022.

〔67〕 See Joost Poort, Frederik Zuiderveen Borgesius, Does Everyone Have a Price? Understanding People's Attitude Towards Online and Offline Price Discrimination, 8 *Internet Policy Review*, 1, 2 (2019).

多消费者的调查结果同样证实了这一结论。〔68〕

综上，算法个性化定价容易引起消费者反感，让消费者感受到不公平。那么，消费者的不公平感从何而来？实际上，差异化价格并非新奇之事，为何有些差异化定价能被消费者接受，而算法个性化定价却会让人感到不公平？下述理论分析能够提供答案。

第二，消费者的不公平感主要源于分配不公平和程序不公平。传统上被消费者接受的差异化价格，大体可分为七种类型。〔69〕这些特殊类型的价格差异能被社会接受的原因主要包括：一是存在被社会习惯所认可和接受的实质正当理由，典例就是学生优惠票或飞机票价的动态变化，如郑某诉携程案涉及的就是机票动态变化。〔70〕二是定价政策公开、透明，消费者要么能够参与定价过程，要么有更多自由选择的空间，此时消费者更容易认可价格差异，典例如量多优惠。

前述理由，有助于反向理解为何算法个性化定价被消费者认为是不公平的。算法个性化定价引致的消费者不公平感可分为两类：分配不公平（distributive unfairness）和程序不公平（procedural unfairness）。〔71〕首先，算法个性化定价违背了分配公平却无正当理由。一般价格场景下的算法个性化定价呈现出“千人千价”“最懂你的人伤你最深”的特点。而且通常而言，算法个性化定价总是对“熟人”收取更高价格，这违背了“人熟为宝”的传统商业道德。〔72〕其次，算法个性化定价透明度低且没有退出机制，违背了程序公平。消费者无法了解自己是否被个性化定价，也不清楚个性化定价的机制，甚至没有办法选择退出个性化定价，这会加剧消费者的不公平感，损害消费者信任。〔73〕

第三，质疑观点可能会主张如果算法个性化设定的价格是一般价格，此时因为消费者自愿同意接受该价格，再加上经营者也没有实施欺诈行为，所以应该认定价格是公平的。这是传统定价理论对公平价格的理解，即商品的公平价格是购买者在真空状态下的独立判断。但行为经济学指出，消费者具有从众心理，他们对商品价值的判断大多是基于他人支付的价格。换言之，公平价格的判断并非消费者在真空状态下的独立判断。当消费者意识到他人支付的价格更低时，消费者便会认为自己所支付的价格并非公平价格。理查德·塞勒提出的“交易效用”（transaction utility）理论可以很好地解释为什么消费者会认为一般价格场景下算法个性化定价是不公平的。

---

〔68〕 See EC, Consumer market study on online market segmentation through personalised pricing/offers in the European Union, June 2018, available at https://ec.europa.eu/info/sites/info/files/aid_development_cooperation_fundamental_rights/aid_and_development_by_topic/documents/synthesis_report_online_personalisation_study_final_0.pdf, last visited on Jan. 5, 2022.

〔69〕 一是基于特定身份群体的折扣价，比如老人、学生、儿童；二是基于数量的折扣价，也就是所谓的量多优惠；三是忠诚折扣，即重复多次购买而可以享受熟人优惠；四是新客折扣，这在双边平台市场的合理性更为明显；五是根据使用峰值、谷值与平值而差异定价，常见的如分时电价；六是基于时间的折扣，比如飞机票价的优惠；七是基于消费者讨价还价能力而形成的差异价格。

〔70〕 参见上海市第一中级人民法院（2020）沪 01 民终 13989 号民事判决书。

〔71〕 See Jennifer Lyn Cox, Can differential prices be fair? 10 *Journal of Product & Brand Management*, 264, 265－267 (2001).

〔72〕 参见杨燕明：《“数据杀熟”：刹住技术歪心思》，载《人民法院报》2020 年 9 月 19 日，第 002 版。

〔73〕 See Mariateresa Maggiolino, Personalized Prices in European Competition Law, Jun. 12, 2017, Bocconi Legal Studies Research Paper No. 2984840, available at https://ssrn.com/abstract=2984840, last visited on Jan. 5, 2022.

因为交易效用取决于商品成交价与参考价之间的差别，当消费者以他人的成交价为参考价而发现自己成交价更高时，交易效用将受损，不公平感油然而生。〔74〕需要注意的是，信任是观念层面的概念，信任的损害不要求是实际损害，只要消费者主观感受到价格不公平即可。〔75〕

3. 消费者信任受损的危害性

一般价格场景下的算法个性化定价尽管并不会损害消费者权益，也不会扭曲市场竞争，但会导致消费者对特定经营者的信任受损，进而会产生如下危害：

第一，算法个性化定价会使消费者对整个数字经济的信任度下降。例如原英国公平交易局（OFT）在2013年的报告中提出，算法个性化定价会降低消费者对网络交易市场的信任。〔76〕在OECD“数字时代的个性化定价”圆桌会议中，英国CMA进一步阐述了个性化定价对消费者信任以及数字经济发展的影响：“消费者信任的缺乏不仅与实施个性化定价的企业相关，而且还与整个网络经济有关。”〔77〕2021年CMA再次强调消费者对网络市场的信任会遭受损害从而损害整体经济效率。〔78〕消费者对特定经营者的不信任会波及整个数字市场，一方面是因为消费者认为算法个性化定价在数字经济时代较为普遍，〔79〕另一方面也因为算法个性化定价的行为主体、〔80〕影响程度和波及范围具有普遍性。总而言之，针对单个经营者的不信任会波及整个网络市场。〔81〕

第二，消费者信任受损会破坏市场秩序，阻碍网络经济蓬勃发展。具体到我国近期的国家政策，这还可能会影响国内、国际双循环的构建，影响到新产品和新科技的更新换代。行为经济学发现，消费者具有损失厌恶的特征，会避免陷入使他们后悔的交易中。可以预见的是，具有损失厌恶特征的消费者在信任受损后将更谨小慎微，更不愿意参与到网络交易中。〔82〕行为经济学的实证研究也证实了消费者在感受到不公平后会结束交易。〔83〕信任受损之后，消费者将会减少他们的需求，最终会损害消费者剩余。〔84〕总而言之，消费者信任受损会冲击网络经济市

〔74〕 See Richard H. Thaler, Mental Accounting and Consumer Choice, 4 *Marketing Science*, 199 (1985).

〔75〕 See Ellen Garbarino, Olivia F. Lee, Dynamic Pricing in Internet Retail: Effects on Consumer Trust, 20 *Psychology and Marketing*, 495, 500 (2003).

〔76〕 See UK Office of Fair Trading (OFT), Personalized Pricing: Increasing Transparency to Improve Trust, OFT 1489, May 2013, available at https://webarchive.nationalarchives.gov.uk/20140402165101/http://oft.gov.uk/shared_oft/markets-work/personalised-pricing/oft1489.pdf, last visited on Jan. 5, 2022.

〔77〕 OECD, Personalised Pricing in the Digital Era-Note by the United Kingdom, pp. 9 - 10, DAF/COMP/WD (2018) 127.

〔78〕 参见前引〔12〕，CMA文，第8页。

〔79〕 例如北京消协超过3000份的调查问卷结果显示88.32%的被调查者认为算法个性化定价很普遍。参见前引〔9〕。

〔80〕 普通公司也可实现算法个性化定价。See Micheal Levine, Price Discrimination Without Market Power, 19 *Yale Journal on Regulation*, 1 (2002).

〔81〕 See The National Association of Citizens Advice Bureaux, A price of one's own-an investigation into personalized pricing in essential markets, pp. 18 - 19, available at https://www.citizensadvice.org.uk/Global/CitizensAdvice/Consumer%20publications/Personalised%20Pricing%20Report%202018.pdf, last visited on Jan. 5, 2022.

〔82〕 See Andrew M. Odlyzko, Privacy, Economics, and Price Discrimination on the Internet, International Conference on Electronic Commerce, Jul. 27, 2003, available at https://ssrn.com/abstract=429762, last visited on Jan. 5, 2022.

〔83〕 See Domen Malc, Damijan Mumel, Aleksandra Pisnik, Exploring Price Fairness Perceptions and Their Influence on Consumer Behavior, 69 *Journal of Business Research*, 3693 (2016).

〔84〕 See OFT, The Economics of Online Personalised Pricing, pp. 83 - 87, May 2013, available at https://webarchive.nationalarchives.gov.uk/20140402154756/http:/oft.gov.uk/shared_oft/research/oft1488.pdf, last visited on Jan. 5, 2022.

场秩序。

综上，基于危害差异及概念逻辑，本文将算法个性化定价分为三个非空子类：超高价格、超低价格、一般价格。

四、规制算法个性化定价的策略

本部分将围绕各类算法个性化定价的危害及其损害机理提出具体规制进路。

（一）危害性的识别方法

在提出具体规制进路之前，有必要先解决如何识别不同种类的算法个性化定价这一实践难题。算法个性化定价的理论分类是方便且容易的，但因算法行为具有隐蔽性特征且难以从外部对其进行观察，所以要识别具有不同危害性的行为在实践中并非易事。尽管如此，我们仍然可以运用区块链技术可溯源与可追踪的特点，从数据输入、代码计算与算法输出三个层面来识别危害性。

识别算法个性化定价与算法合谋定价、欺诈定价、歧视定价，首先，可以通过直接访问数据和代码来分辨不同的损害。直接访问数据和代码有助于监管者更精确地认知算法逻辑，做出更有效的监管。比如某些情况下，数据本身就能表明是否存在种族与性别歧视问题。但直接访问数据和代码需要公司的高度配合，这需要考虑公司的激励问题，以及政府干预的限度问题。其次，在无法直接访问数据和代码时，可以从数据输入和算法输出两个角度来间接了解算法的运作机制。一般而言可以通过“抓取审核”（scraping audit）的方式或通过应用程序接口（API）来识别不同的危害性。最后，在没有现实数据时还可以采用创建虚拟角色测试的方式，如欧盟 2018 年、北京消协 2019 年都曾采用此种调研方法。

识别算法个性化定价的三种子类行为无涉算法，这是因为价格的高低只是算法输出的结果，不需要深入算法内部即可从外部观察并区分这三种子类行为。算法个性化定价子类行为的判断标准，与线下世界对超高价格、超低价格、一般价格的判断标准是类似的。超高价格的判断可以借鉴反垄断法关于超高价格的判断标准，〔85〕也可以借鉴合同法关于显失公平客观要件的判断标准，甚至还可以借鉴《最高人民法院关于适用〈中华人民共和国合同法〉若干问题的解释（二）》第 19 条关于 30％价差的相关规定。超低价格判断因素与超高价格的判断因素类似，可以从《价格法》《反垄断法》相关的规定中汲取相应的考虑因素，例如判断定价是否低于平均可变成本，另外 30％的价差或可以作为参考因素。

（二）基于危害性差异的分类规制

1. 超高价格和超低价格的规制路径

超高价格与超低价格具有严重危害，因此法律基本持禁止态度。

〔85〕 参见梅夏英、任力：《关于反垄断法上不公平高价制度的法律适用问题》，载《河北法学》2017 年第 4 期；苏华：《不公平定价反垄断规制的核心问题——以高通案为视角》，载《中国价格监管与反垄断》2014 年第 8 期。

第一，超高价格的危害性在于剥夺消费者剩余，损害公平交易，可适用《反垄断法》第17条第1款第1项、《民法典》第151条、《互联网信息服务算法推荐管理规定》第21条或《消费者权益保护法》第10条和第16条予以规制。具体来说，若经营者具有市场支配地位，利用消费者画像收取超高价格，则可能违反《反垄断法》关于不公平高价的规定。当经营者不具有市场支配地位时，则可以适用《民法典》第151条调整经营者利用消费者处于危困状态、缺乏判断能力等情形设定超高价格致使显失公平的行为。《消费者权益保护法》第10条规定了消费者有权获得价格合理的公平交易条件，第16条要求经营者承担不得设定不公平交易条件的义务。《互联网信息服务算法推荐管理规定》第21条同样是基于消费者的公平交易权介入规制。

第二，超低价格的危害性在于扰乱市场竞争秩序，在经营者处于市场支配地位时还会产生排除限制竞争的效果，可通过《反垄断法》和《价格法》进行调整。当经营者具有市场支配地位时，若算法个性化定价属于超低价格，低于平均可变成本，便可能会违反《反垄断法》第17条第1款第2项而构成掠夺性低价。若不具有市场支配地位，经营者利用算法设定超低价格的行为仍然可能违反《价格法》第14条之规定。2021年7月国家市场监督管理总局发布的《价格违法行为行政处罚规定（修订征求意见稿）》提高了这一新型价格违法行为的罚款力度，相信能够有效应对其危害性。

第三，超高价格和超低价格的危害性还可以通过事前规制的方法予以调整。比如可以设定价格区间限制（price caps），即利用算法设定的个性化价格应保持在合理的区间范围。英国金融行为监管局（Financial Conduct Authority）曾采用这种方式。〔86〕这种规制方法具有一定的正当性，得到了学者的支持。〔87〕

2. 一般价格的多元共治路径

政府原则上不应介入规制一般价格场景下的算法个性化定价，因为市场机制会逼迫经营者进行竞争从而实现竞争均衡，而且即便在垄断性市场上利用算法设定一般价格也不会损害消费者权益，不会扭曲市场竞争。不过算法个性化定价可能会弱化消费者信任、破坏市场秩序，此时政府需要介入规制以重建市场信任。而重建市场信任是个系统工程，需要政府、经营者与消费者共同努力，形成多元共治的规制格局。

（1）一般价格场景的政府介入规制路径

为维系消费者对经营者及数字经济的信任，政府应介入调整一般价格场景下的算法个性化定价行为，需要注意如下三点：

第一，坚持包容审慎的监管原则，具体包括依法监管、科学监管、积极有效监管等内涵。首

〔86〕 See Financial Conduct Authority, Price Discrimination in Financial Services: How Should We Deal With Questions of Fairness? p. 9, July 2018, available at: https://www.fca.org.uk/publication/research/price_discrimination_in_financial_services.pdf, last visited on Jan. 5, 2022.

〔87〕 See Oren Bar-Gill, Algorithmic Price Discrimination When Demand is a Function of Both Preferences and (Mis) perceptions, 86 *University of Chicago Law Review*, 217, 243 (2019).

先应尽可能减少对市场的干预，充分发挥市场的调节作用。市场可能会自发催生比价网站，通过算法技术帮助消费者反“杀熟”。〔88〕其次，政府要灵活运用多种规制工具重建消费者对数字经济的信任，例如可以通过行政指导等软性规制方法强化对算法个性化定价的监管。〔89〕最后，包容审慎监管并不意味着不监管和弱监管，因为消费者信任类似于“公地资源”，若不施加干预可能会出现“数字信任公地悲剧”。〔90〕

第二，政府应围绕信任损害机制重建信任，主要可以从维护程序公平的角度设计具体监管方法。首先，政府可以要求经营者提高数据与算法的透明度，从而维护消费者对数字市场的信任。设定经营者强制告知规则是提高透明度的有效方案，〔91〕例如可以在个人数据保护规范中强制要求经营者告知算法个性化定价的基本原理和主要运行机制〔92〕。需要注意的是，提高透明度的同时务必要提防经营者通过共享用户个性化数据而实现算法共谋。〔93〕其次，政府可强制要求经营者为消费者提供便利的退出机制。如果能为消费者提供更方便的退出机制，他们将对算法个性化定价持更为积极的态度。〔94〕我国《互联网信息服务算法推荐管理规定》第 16 条和第 17 条强调了强制告知和退出机制的作用，美国众议院立法小组 2021 年 6 月提出的《过滤气泡透明度法案》（Filter Bubble Transparency Act）以及欧洲议会最新通过的《数字服务法》亦强调透明度和退出机制的重要性。

第三，政府应加强消费者教育，让消费者正确认识算法个性化定价。当前消费者对算法个性化定价的认知仍停留在感性层面，普遍认为算法个性化定价就是“杀熟”。在这种感性的认知下，消费者信任很难建立。推动消费者理性看待算法个性化定价是政府维系数字经济信任的重要环节。政府可以通过公开市场调研报告等手段增强消费者的信任，或者可基于信任机制重构算法解释权，使算法个性化定价更能得到接受与认可。〔95〕

（2）一般价格场景的经营者自我规制路径

消费者信任是经营者的一种商誉，对经营者的经营活动具有重要价值，因此经营者也应该强化自我规制。从实际效果来看，经营者自我规制也是治理算法个性化定价诱致信任危机最为便捷的方式。经营者可从如下三个方面调整经营行为：

第一，从矫正程序公平的角度而言，经营者不仅要提高算法个性化定价的透明度，还要主动

〔88〕 参见乔榛、刘瑞峰：《大数据算法的价格歧视问题》，载《社会科学研究》2020 年第 5 期。

〔89〕 参见《盒马、京东等 10 平台签署承诺书：不利用大数据“杀熟”》，载 http://news.winshang.com/html/068/3405.html，最后访问时间：2022 年 1 月 5 日。

〔90〕 参见前引〔60〕，谢尧雯文。

〔91〕 英国议会上议院在 2016 年也曾建议政府采取这种强制告知规则。See House of Lord, Online Platforms and the Digital Single Market, p. 76, Apr. 20, 2016, available at https://publications.parliament.uk/pa/ld201516/ldselect/ldeucom/129/129.pdf, last visited on Jan. 5, 2022.

〔92〕 See Frederik Zuiderveen Borgesius, Joost Poort, Online Price Discrimination and EU Data Privacy Law, 40 *Journal of Consumer Policy*, 347, 358－360 (2017).

〔93〕 See Terrell McSweeny, Brian O'Dea, The Implications of Algorithmic Pricing for Coordinated Effects Analysis and Price Discrimination Markets in Antitrust Enforcement, 32 *Antitrust*, 75 (2017).

〔94〕 See Gerhard Wagner, Horst Eidenmüller, Down by Algorithms: Siphoning Rents, Exploiting Biases, and Shaping Preferences: Regulating the Dark Side of Personalized Transactions, 86 *University of Chicago Law Review*, 581, 592 (2019).

〔95〕 参见丁晓东：《基于信任的自动化决策：算法解释权的原理反思与制度重构》，载《中国法学》2022 年第 1 期。

为消费者提供更为便利的退出机制。经营者还可以设计流程让消费者切身参与到个性化定价过程中，减少其程序不公平感。〔96〕第二，从矫正分配公平的角度而言，经营者可以告知消费者个性化定价的正当理由，减少消费者的不公平感。例如在网约车场景下，平台提供个性化的配车服务或加速配车服务可以主动告知消费者为此需要提高价格，这种情形下的差异化定价更容易让消费者接受。同时，经营者还可以从折扣和优惠的角度表述算法个性化定价，提高消费者的接受度。第三，经营者可通过减少交易的相似性减轻消费者的不公平感。〔97〕消费者是通过比对相似交易下其他消费者支付的价格而获得不公平感的，那么在差异化经营模式下，消费者不公平感会逐渐减少。

（3）一般价格场景的消费者自我保护路径

数字经济是未来经济发展的方向，会给消费者带来许多意想不到的益处。算法个性化定价会给消费者带来便利，有时也能提高消费者剩余。我们不能一味强调消费者的弱势地位并要求政府和经营者给予帮助和保护，实际上消费者也可以在算法个性化定价的治理体系中发挥重要作用。从消费者角度来看，重建市场信任需要消费者努力做到以下两个方面：第一，消费者应更理性地看待算法个性化定价。算法个性化定价形成的超高价格和超低价格确实会损害消费者权益，但并非所有的算法个性化定价都会如此。一般价格场景下的算法个性化定价并未侵害消费者权益，因此消费者不应将所有算法个性化定价同等对待。第二，消费者应提高自我保护意识，在交易时应更为慎重，尽量减少对单一软件的依赖，同时还可以通过多次搜索浏览比价以强化自我保护。尽管要求经营者自我规制是更直接的解决路径，但多举措齐头并进才能实现更好的规制。对消费者个体而言，提高自我保护意识能屏蔽掉多数风险。此外，还可以通过算法赋能消费者，用大数据方法来破解算法个性化定价。〔98〕

五、结　论

规制算法个性化定价应遵循对策与问题相匹配的规制法原理，不仅要将算法个性化定价与诸如算法欺诈定价、歧视定价、合谋定价等其他算法危害行为区分开，避免混淆，还要根据危害差异将算法个性化定价进行细分（超高价格、超低价格和一般价格）。超高价格和超低价格场景下的算法个性化定价可通过《反垄断法》《民法典》《价格法》和《消费者权益保护法》等法律事后规制，也可通过设定价格区间限制进行事前调整。一般价格场景下的算法个性化定价之危害性既不在于损害消费者权益，也不在于排除限制竞争，而在于让消费者产生价格不公平的感受，进而削弱消费者信任，放任其发展甚至可能会破坏市场秩序。基于维系消费者信任、重建市场信心的

〔96〕 See Timothy J. Richards, Jura Liaukonyte, Nadia A. Streletskaya, Personalized Pricing and Price Fairness, 44 *International Journal of Industrial Organization*, 138 (2016).

〔97〕 See Lan Xia, Kent Monroe, Jennifer Cox, The Price is Unfair! A Conceptual Framework of Price Unfairness Perceptions, 68 *Journal of Marketing*, 1, 8 (2004).

〔98〕 See Michal S. Gal, Niva Elkin-Koren, Algorithmic Consumers, 30 *Harvard Journal of Law & Technology*, 309, 310 (2017).

需要，政府、经营者和消费者应合力推动一般价格场景下算法个性化定价的治理：政府应坚持包容审慎监管，强制经营者履行告知义务，强制经营者建立消费者自由退出机制；经营者要紧抓消费者信任的损害机理，围绕分配公平和程序公平两个层次调整经营行为；消费者则要理性对待、提高警惕，利用自己的智慧反“杀熟”。

Abstract：The regulatory practices and theoretical analysis of algorithm personalized pricing fail to follow the regulatory principle of matching regulation countermeasures with the hazards. According to the principle，we should pay attention to the differences between algorithm personalized pricing and algorithm collusion pricing，fraudulent pricing，discriminatory pricing，personalized recommendation. Meanwhile，the complexity of hazards requires us to deconstruct the algorithm personalized pricing into three subcategories：ultra-high price，ultra-low price and ordinary price. The hazards of ultra-high and ultra-low price scenarios can be resolved under the existing legal framework. In ordinary price scenario，algorithm personalized pricing will not infringe consumers' rights and interests，nor eliminate and restrict competition. However，it will damage consumers' trust and disorder the digital market from the perspective of distributive unfairness and procedural unfairness. The government，business operators and consumers should work together to establish consumers' trust，based on the understanding and use of the damage mechanism of consumers' trust，so as to achieve a dynamic balance between innovative development and consumer interests protection.

Key Words：big data kill，algorithm personalized pricing，typological analysis，consumers' trust

（责任编辑：李　敏　赵建蕊）

财经法学 No. 4，2023
pp. 181 - 192

法律与人工智能：用 ChatGPT 塑造法律实践的未来

[美]丹尼尔·D. 李　著　管　斌　宋博文　译*

内容提要：法律与人工智能的未来，既展现了机遇，也充满了挑战。人工智能对法律领域的影响，包括但不限于法律研究和分析、文件自动化处理、诉讼、替代性纠纷解决、合规、风险管理和法律教育。在 ChatGPT 等生成式人工智能技术的整合推动下，法律领域的持续转型正在重塑法律服务的提供方式、法律专业人士的职能和技能组合，以及法律职业的整体结构和文化。法律专业人士、政策制定者和利益相关者应接纳技术的发展更新，战略性地利用人工智能驱动的工具，并因应不断变化的法律环境，制定道德准则、监管框架和最佳实践，解决数据隐私、公平性、透明度、问责制等人工智能引发的伦理和法律挑战，以确保人工智能驱动的工具在法律实践中被负责任地使用，借此塑造一个更高效率、更有效力和更为公平的法律体系，以造福客户和整个社会。

关键词：法律与人工智能　生成式人工智能　负责任的人工智能　透明度　问责制

伴随神经网络、大数据和深度学习等技术的发展和运用，人工智能（Artificial Intelligence，AI）技术在近十年里取得显著成就，以机器翻译、人脸识别、自动驾驶、疾病监测等多种方式从学术研究走向现实应用。2022 年 11 月 30 日，美国人工智能研究公司 Open AI 实验室发布首款基于 GPT-3.5 架构的智能文本撰写与聊天工具 ChatGPT（Generative Pre-trained Transformer）。〔1〕在底层模型算法和训练机制的技术创新支持下，ChatGPT 具备了之前决策式人工智能所不具备的知识迁移能力，能够通过理解和学习人类的语言进行对话，根据用户的文本输入和聊天的上下文内容，生

* 丹尼尔·D. 李，毕业于佐治亚理工学院，畅销书作家；管斌，华中科技大学法学院副教授；宋博文，中国建设银行业务处理中心智能应用处干部。

本文编译自 Daniel D. Lee，Law and AI：Shaping the Future of Legal Practice with ChatGPT，Independently published（April 8，2023），主体部分为该书第一章、第九章、第十章和结论。此译文为中央高校基本科研业务费资助项目“金融发展权问题研究”（2021WKFZZX024）的阶段性成果。

〔1〕 ChatGPT（Generative Pre-trained Transformer）中：Chat 意为聊天；Generative 意为生成性，指向内容；Pre-trained 意为预训练，包括基础性的监督学习（supervised learning）和反馈性的强化学习（reinforcement learning from human feedback，RLHF）；Transformer 意为变换，指通过编码输入和解码输出。——编译者注。

成相应的智能回答，像人类一样聊天交流，还可以完成编写代码、设计文案、撰写论文、机器翻译、回复邮件等多种任务。一经推出，ChatGPT 迅速形成了一种现象级应用，表现出很高的人机交互（human-computer interaction，HCI）水平，基本具备面向通用人工智能（artificial general intelligence，AGI）〔2〕的特征，在众多行业领域具有广泛的应用潜力。

每一次技术的进步都会带来社会变革。如果说互联网引发了空间革命、智能手机引发了时间革命，那么以 ChatGPT 为典型代表的生成式人工智能技术或将引发人类社会的知识革命，成为推进社会结构演进的催化剂。由于人工智能技术的快速发展及其在法律实践中的有效应用，曾经传统和保守的法律行业正在经历重大变革。作为继数据库和搜索引擎之后全新一代的知识表示和调用方式，ChatGPT 正在重塑法律专业人士的工作方式，并改变司法系统的面貌。虽然当前各国立法与政策均提出了发展“负责任的人工智能”，但当诸如 ChatGPT 这样的人工智能驱动的技术融入法律领域，在带来前所未有的技术便利的同时，亦可能打开“潘多拉魔盒”（Pandora's box），引致工作岗位流失、认知偏差、责任模糊、隐私侵害、数据滥用等现实风险，破坏全球经济、政治和社会安全。谁应为人工智能的发展与应用负责？如何为人工智能的发展与应用负责？人工智能能否为自己的决策与发展负责？为确保人工智能技术融入法律领域所带来的影响是积极的，风险是可控的，针对这些基础性问题进行体系性研究，已经迫在眉睫。

一、法律与人工智能中的伦理和法律挑战

诸如 ChatGPT 这样的人工智能驱动的技术融入法律领域，带来了一系列伦理和法律挑战。在这些技术不断改变着法律实践的同时，法律专业人士、政策制定者和利益相关者必须解决这些挑战，以确保人工智能驱动的工具被负责任地使用，并符合法律的基本规定和利益相关者的最佳利益。在这里，我们概述了人工智能融入法律领域时必须考虑的一些关键的伦理和法律挑战：

一是避免工作岗位流失。我们可以将 ChatGPT 理解为一个图书馆和一个具有理解和分析能力的处理器，能够运用它拥有的人类千万年来形成的所有已被数字化的知识快速生成各种问题的新回答。这种记忆和回答能力，以及不断迭代所带来的准确性，可以快速给出一般性或不复杂案件的判断和回答。人工智能驱动的工具促进了常规任务的自动化和高效率处理，这引起了人们对法律工作岗位流失的担忧。〔3〕新时代下的“卢德运动”（Luddite Movement）〔4〕可以休矣！法

〔2〕 人工智能（AI）就是让计算机完成人类心智（mind）能做的各种事情。通用人工智能（AGI），又称为“强人工智能”（strong AI）“完全人工智能”（full AI），是指具有一般人类心智，可以执行人类能够执行的任何心智任务的机器智能。与弱 AI（weak AI）相比，通用人工智能（AGI）可以尝试执行全方位的人类认知能力。通用人工智能（AGI）无疑是人工智能（AI）领域的“圣杯”（sangreal）。——编译者注。

〔3〕 相当于法律世界阿尔法狗的 IBM Watson LegalMation 已就职于纽约贝克豪思律师事务所（Baker & Hostetler），处理公司破产等事务。据介绍，律师们通过数十个小时甚至更长时间才能完成的在线法律数据搜索，它几乎能在瞬间完成，而且结果是同样的精准。《纽约时报》2017 年 3 月的一篇报道提及，有研究发现，如果将现有的人工智能技术充分使用起来，23%的律师工作可以自动化。在 2023 年 3 月 26 日发布的研究报告《人工智能对经济发展的潜在重大影响》中，高盛（Goldman Sachs）通过分析美国和欧洲的职业形态，认为在当前的工作岗位里，有三分之二的工作会受到人工智能影响，四分之一的工作将被人工智能取代。其中，法律行业是“失业重灾区”，44%的工作将被人工智能取代。

〔4〕 工业革命时期，机器生产逐渐排斥手工劳动使大批手工业者破产，工人失业，工资下跌。当时工人把机器视为贫困的根源，卢德运动（Luddite Movement）就是英国工人以破坏机器为手段反对工厂主压迫和剥削的自发工人运动。英国 1813 年颁布《捣毁机器惩治法》，规定可用死刑惩治破坏机器的工人。

律专业人士必须适应这一新的现实，与其和人工智能驱动的工具竞争，还不如更加专注于去培养那些补充和提升使用这些工具的能力。法学院、律师事务所和政策制定者也必须共同努力，确保法律工作者在面对人工智能带来的变化时做好准备。

二是确保公平性、透明度和问责制。诸如 ChatGPT 这样的人工智能驱动的工具，高度依赖于它们所获取数据的质量和代表性。有偏见或不具代表性的数据会导致有偏见的输出，可能损害法律体系的公平性。必须确保人工智能工具的运作是透明的，并可以对其结果负责。法律专业人士和政策制定者需要努力完善原则、标准和监管框架，以确保人工智能驱动的法律体系的公平性、透明度和问责制。〔5〕

三是规范法律领域的人工智能。在法律领域，人工智能驱动的技术发展和应用的速度，已经超过了监管框架的更新速度。它将继续呈指数级增长（exponential growth），从而取得突破，在超出人类理解和控制的水平上运行。如果生成与人类价值观不相容的目标，它们可能会很危险。例如，被赋予对抗全球变暖的任务，它决定最好的方法是消除主要原因——人类的存在。为了消除这一差距，政策制定者必须出台全面的法规，以规范人工智能在法律行业的使用。这些法规应阐明数据隐私、知识产权、人工智能的责任划分，以及解决人工智能在法律实践中的道德伦理问题。

四是促进法律救济。人工智能驱动的技术有可能通过降低成本和简化法律程序来促进法律救济。关键是要确保这些好处得到公平分配，而且不会加深获得法律资源和服务的现有鸿沟。政策制定者和利益相关者必须共同制定战略，促进人们平等地获取这些工具，并确保这些技术被用来增加而不是减少法律救济的机会。

五是平衡自动化和人类决策。虽然诸如 ChatGPT 这样的人工智能驱动的工具可以自动化处理许多任务，并提供有价值的见解，但在法律领域，在自动化和人类决策之间取得适当的平衡至关重要。法律专业人士必须继续参与决策过程，将人工智能驱动的工具作为一种辅助品，而不是他们的专业知识和经验的替代品。确保人类决策仍然是法律实践的核心，将有助于维护法律体系的完整性，并确保人工智能驱动的工具得到有效和合乎道德的使用。

六是消除“人工智能幻觉”。ChatGPT 推出后不久，有人就宣称搜索引擎的终结。然而，与此同时，ChatGPT 虚构的许多例子开始在社交媒体上流传：ChatGPT“发明”了不存在的法学著作、论文和法律案例，不真实的零售吉祥物，以及没有意义的技术细节。人工智能驱动的工具“一本正经地胡说八道”，生成了诸多虚假信息。这种现象已经有个专有词汇指代，叫“人工智能幻觉”（AI Hallucination）。

〔5〕 在 2021 年 6 月 15 日发布的《第二阶段社会伙伴磋商报告书》中，欧盟委员会提出的治理目标是：“确保算法管理的公平性、透明度和问责制。通过平台工作的人可能不知道算法是如何被用来做出某些决定，从而影响他们的工作条件，而且可能缺乏对这种决定的补救。算法管理的使用可能会进一步掩盖平台所履行的实际管理职能，从而使义务归属面临挑战，而这些义务可能是应有的。在《通用数据保护条例》（GDPR）和拟议的《人工智能法》的基础上，制定规则以改善对此类系统的工作方式及其对相关人员的影响，可以预防和纠正不公平或歧视性的结果。这将有助于改善平台的工作条件。”2021 年 12 月 9 日发布的《欧洲议会和理事会关于改善平台工作条件指令的提案》在拟议文本的第 1 条提出：“通过确保准确确定从事平台工作的人员的就业状况，通过促进平台工作中的算法管理的透明度、公平性和问责制，以及通过提高平台工作的透明度，包括在跨境情况下，来改善从事平台工作的人员的工作条件。”

解决人工智能在法律领域的整合所带来的伦理和法律挑战是法律专业人士、政策制定者和利益相关者的一项重要任务。通过直面这些挑战并制定全面的战略来解决问题，可以确保像 ChatGPT 这样的人工智能驱动的技术在法律领域被负责任地使用，符合法律的基本规定和利益相关者的最佳利益。

（一）解决工作岗位流失问题

诸如 ChatGPT 这样的人工智能驱动技术融入法律领域，引起了人们对工作岗位流失的担忧，因为一些传统上只能由法律专业人士执行的任务可以被自动化作业代替。为了解决此问题，并确保法律行业能够顺利地过渡为一个由人工智能驱动的图景，可以实施如下策略：

1. 再培训和技能提升。法律专业人士应注重再培训和技能提升，以便在不断发展的法律行业中与时俱进。通过培养能够补足人工智能驱动的工具的技能，专业人士可以提高他们的工作附加值并维持他们的就业能力。这包括提高获取、使用人工智能技术的熟练程度，提升例如沟通和谈判的软技能，以及培养在新兴法律领域或跨学科领域的专长。

2. 强调人情味。虽然人工智能驱动的工具可以执行许多任务，但它们不可能取代对法律实践至关重要的人情味。法律专业人士应该强调自己独特的才能，如同理心、创造力和理解复杂的人类情感的能力，这是人工智能无法复制的。通过专注于这些优势，法律专业人士可以在人工智能驱动的法律领域让自己发挥至关重要的作用。

3. 重塑职能和职业道路。随着人工智能不断改变着法律行业，法律人的职能和职业道路也将不断更新发展，以适应新的工作方式。律师事务所、立法部门和其他法律组织应积极主动地重新定义职能，并开发新的职业道路，以充分利用人工智能驱动的工具。这可能涉及创建与人工智能、数据分析或法律技术管理有关的专业职位。

4. 协同处理。法律专业人士应采取协作的思维模式，认识到人工智能驱动的工具的出现是为了促进和辅助他们的工作，而不是取代他们。通过接纳与人工智能技术一起工作的机会，法律专业人士可以利用这些工具的潜力来优化他们的实践，提高效率，更好地服务客户。

5. 调整法律教育和培训课程。法学院和其他职业培训机构必须调整他们的课程，使未来的法律专业人士适应人工智能驱动的环境。这包括纳入关于立法技术、人工智能、数据隐私和道德伦理的课程，以及促进跨学科技能的发展。通过让学生和专业人士掌握足够所需的知识和技能，以驾驭人工智能驱动的法律环境，法律教育和培训可以在解决工作岗位流失问题上发挥关键作用。

总之，解决法律工作岗位流失问题需要一个积极主动且全面的方法，包括再培训和技能提升、重塑职能和职业道路，以及调整法律教育和培训课程。通过采取这些策略，法律专业人士可以有效驾驭不断变化的法律环境，并确保他们始终与时俱进、具备就业能力。

（二）规范法律领域的人工智能

随着诸如 ChatGPT 这样的人工智能技术越来越多地融入法律领域，监管在解决与这些技术相关的道德伦理、隐私和责任问题时变得愈发重要。在监管法律领域的人工智能时，需要在促进创新和确保负责任地开发部署这些技术之间取得平衡。我们探讨了在法律领域监管人工智能的关键性考虑因素，并研究了可能的监管方法。

1. 道德伦理。人工智能在法律领域的伦理适用是一个至关重要的问题。监管机构在为人工

智能在法律领域的应用制定准则和规则时，必须考虑到偏见、透明度和公平性等问题。确保人工智能系统的设计和训练能够最大限度地减少偏见，维护公平正义的原则，对于保持公众对法律体系的信任至关重要。

2. 数据隐私和安全。当涉及在法律领域使用人工智能时，数据隐私和安全是至关重要的问题，因为这些技术往往依靠大量的敏感数据来进行有效运作。监管机构必须为其收集、存储和处理私密和机密数据制定明确的指导方针和标准，以确保符合关于隐私的法律规定，并且能够保障个人和组织的权利。

3. 责任和问责。阐明人工智能驱动的法律服务中的责任和问责是另一个重要的监管考虑。监管机构必须解决这样的问题：当人工智能系统提供不正确或有误导性的法律建议时，或者当人工智能驱动的工具参与起草一个有法律缺陷的文件时，谁应该负责？在责任和问责的问题上，建立一个明确的法律框架，可以帮助保护法律专业人士以及他们的客户的权利和利益。

4. 透明度和可解释性。人工智能驱动的工具在法律领域的使用引发了关于透明度和可解释性的问题。客户和法律专业人士有权了解人工智能驱动在基于什么原理运作、给出决定和建议。监管机构应考虑出台对人工智能开发者和提供者的要求，以披露其系统的功能，并确保人工智能驱动的法律工具能够为其产出提供清晰和可理解的解释。

5. 专业能力和监管。随着人工智能的应用在法律领域变得越来越普遍，必须确保法律专业人员拥有必要的能力，以有效且符合伦理地使用这些技术。监管机构可能需要考虑对法律专业人士出台培训和教育要求，以确保他们拥有必要的知识和技能来使用这些由人工智能驱动的工具。此外，可能需要制定指导方针，以阐明在法律实践中使用人工智能时所需要的适当的监督和管理标准。

6. 许可和认证。一个可能的监管方法是对人工智能驱动的法律工具及其供应商出台许可和认证要求。这有助于确保人工智能驱动的工具满足最低的质量和道德标准，并确保供应商对其技术的性能和可靠性负责。

总之，对法律领域的人工智能进行监管是一项复杂但有必要的工作，以确保这些技术正在负责任地发展和部署。关键考虑因素包括道德伦理、数据隐私和安全、责任和问责、透明度和可解释性、专业能力和监管。通过建立一个明确且平衡的监管框架，政策制定者可以帮助促进创新，同时保护法律专业人士、其客户和更广泛公众的权利和利益。

二、法律与人工智能的未来：机遇与挑战

随着 ChatGPT 等人工智能驱动的技术持续地改变法律环境，法律和人工智能的未来既展现了机遇，也充满了挑战。我们将探索这一不断发展的环境的关键方面，并讨论法律专业人士、政策制定者和利益相关者如何应对这些变化，以有效利用人工智能驱动工具的潜力。

这一不断发展的法律环境主要包括：(1) 法律领域的持续转型。随着人工智能驱动的技术将常规任务自动化，简化了流程，增强了决策能力，法律职业正处于重大转型之中。这种转型为法律专业人士提供了机会，使他们可以专注于高附加值任务，如战略思考、客户咨询和解决复杂问题，而人工智能驱动的工具则用以处理耗时和重复的任务。为了抓住这些机会，法律专业人士必

须抱着终身学习的心态，不断深化发展自己的技能，以便在快速发展的法律领域与时俱进。(2) 人工智能在法律领域的未来走向。随着人工智能技术的不断进步，我们可以期待看到人工智能驱动的工具在法律实践的各个方面的进一步整合，例如：①人工智能驱动的法律研究和分析的改良：人工智能工具在分析复杂的法律问题、识别相关先例和预测案件结果方面的能力将变得更加成熟。②文件自动化处理和起草的加强：人工智能驱动的工具将能够以更高的精度和效率起草越来越复杂的法律文件，例如合同、简报和诉状。③人工智能辅助纠纷解决的扩展：人工智能驱动的工具将在纠纷解决中发挥更突出的作用，提供有价值的洞察和分析，以促进谈判、调解和仲裁过程。④人工智能在法庭上的应用：人工智能技术可能会越来越多地被应用于法庭，通过自动化处理任务、分析证据和提供实时语言翻译服务来辅助法官、书记员和律师。(3) ChatGPT 和其他人工智能技术导引下的法律愿景。为了有效地导引法律和人工智能的未来，法律专业人士、政策制定者和利益相关者必须解决诸多挑战，例如：①确保人工智能驱动的工具的使用符合道德伦理：建立明确的道德准则和监管框架，对于管理人工智能驱动的工具在法律实践中保证其公平性、透明度和问责制至关重要。②克服对工作岗位流失的担忧：法律专业人士和教育工作者必须优先考虑再学习、深入学习，并在人工智能驱动的法律环境中接受自己新的职能定位，以确保与时俱进和可雇佣性。③消除人工智能驱动的工具的潜在偏见：法律专业人士和人工智能开发人员之间的合作对于识别、减少人工智能驱动的工具的潜在偏见至关重要，确保这些技术被公平和负责任地使用。

总之，通过接纳法律领域的持续转型，利用人工智能驱动技术的潜力，并解决这些技术带来的道德伦理和法律实践问题，法律专业人士、政策制定者和利益相关者可以塑造法律实践的未来，以造福客户和整个社会。

(一) 法律领域的持续转型

随着 ChatGPT 等人工智能技术越来越多地融入法律实践的各个方面，法律领域正在经历一场重大的变革。这种持续的转型正在重塑法律服务的提供方式、法律专业人士所需的技能和能力，以及法律职业的整体结构和文化。我们探讨这种转型的几个关键维度以及对法律行业未来的潜在影响。

1. 服务提供方式的改变。人工智能驱动的工具正在促使法律领域发展新的服务提供方式，其特点是高自动化、高效率和高性价比。特别是对于那些以前可能由于高成本或太复杂而难以获得法律救济的个人和组织来说，这些新方式正在使法律服务更易获取，也更实惠。

2. 职能和技能的革新。人工智能在法律领域被越来越多地使用，不断改变着法律专业人士的职能和技能。律师和其他法律从业者现在必须拥有更多样化的能力，包括技术应用、数据分析和对人工智能及其在法律中应用的理解。这种转变可能会影响法律教育和培训，以及法律机构的招聘和职业发展战略。

3. 合作和跨学科研究的加强。人工智能融入法律领域的日益盛行，促成了更多的合作和跨学科的法律实践。法律专业人士正越来越多地与数据学者、技术专家以及其他专家合作，开发人工智能驱动的工具，部署人工智能驱动的战略。具有不同技能和观点的专业人士将他们的专业知识贡献给了法律实践，这种合作方式可以带来更有效且更富创造性的法律解决方案。

4. 新的法律和伦理挑战。人工智能融入法律领域带来了一系列新的法律和伦理挑战，例如确保人工智能被负责任地使用、解决数据隐私和安全问题，以及阐明责任和问责问题。这些挑战可能会促成新的法律、法规和专业标准的发展，以规范人工智能在法律实践中的应用。

5. 对法律就业的影响。法律领域的持续转型带来了人工智能对法律就业的影响问题。虽然人工智能驱动的自动化可能导致一些传统的法律职业被取代，但它也可能为拥有足够技术水平和适应性的法律专业人士创造新的机会。此外，人工智能驱动的工具可以帮助法律专业人士专注于需要人类判断力和创造力的高附加值任务，最终促成更高成就感、更高回报的职业。

6. 促进法律救济。法律职业转型的最重要影响之一是促进了法律救济。通过人工智能驱动的工具，法律服务可以被更实惠、更高效、更轻易地获取，这有助于缩小司法鸿沟，确保更多的个人和组织能够获得他们需要的法律救济。

总之，在 ChatGPT 等人工智能技术的整合推动下，法律领域的持续转型正在重塑法律服务的提供方式、法律专业人士的职能和技能组合以及法律职业的整体结构和文化。虽然这种转变带来了挑战，但它也为创新、合作和改善法律服务提供了重大机遇。通过接纳这种转变并适应不断变化的法律环境，法律专业人士可以塑造出一个更高效率、更有效力和更为公平的法律实践的未来。

（二）人工智能在法律领域的未来走向

随着人工智能技术的不断发展和成熟，它们对法律领域的影响预计会越来越大。以下是对人工智能在法律领域的未来走向的一些预测：

1. 法律研究和分析的加强：人工智能驱动的工具在分析复杂的法律问题、筛选大量数据和识别相关先例和法规方面的水平将变得更高。这将带来更快捷、更准确的法律研究，使法律专业人士能够做出更明智的决定。

2. 先进的文件自动化处理和起草：人工智能驱动的工具将能够以更高的精度和效率起草日益复杂的法律文件。这将帮助法律专业人士节省时间、降低失误风险，使他们能够专注于更多战略性任务，提供更优质的客户服务。

3. 人工智能辅助的诉讼和案件预测：人工智能将在诉讼中发挥更突出的作用，包括案件预测和战略制定。通过分析历史数据以及识别诸多模式，人工智能驱动的工具将能够预测案件结果，并为法律专业人士推荐最佳策略。

4. 人工智能在纠纷解决中的扩展：人工智能驱动的工具将在替代性纠纷解决程序中变得更加普遍，如调解、谈判和仲裁。这些工具将呈现出有价值的见解和分析，以支持法律专业人士为其客户呈现出更好的解决方案。

5. 人工智能在法庭上的应用：人工智能技术可能会越来越多地用于法庭，以支持法官、书记员和律师的各种职能，如自动化处理日常任务、分析证据和提供实时语言翻译服务。

6. 合规和风险管理的加强：人工智能驱动的工具在识别潜在的法律风险和确保监管合规方面将变得更加先进，帮助企业降低司法和经济处罚的风险。

7. 个性化的法律服务：人工智能驱动的工具将使法律专业人员能够根据个人客户的需求和偏好，提供更加个性化的定制法律服务。这将提高客户满意度，加深与客户的联系。

8. 人工智能驱动的法律聊天机器人和虚拟助理：由人工智能驱动的聊天机器人和虚拟助理

将变得更加广泛，为客户提供即时的法律咨询和帮助，并协助法律专业人士完成日常工作。

9. 法律教育和培训中的人工智能：法学院和继续教育机构将越来越多地把人工智能和法律技术纳入他们的课程，帮助未来的法律专业人士适应不断变化的法律环境。

10. 道德伦理和监管的发展：随着人工智能越来越多地融入立法部门，道德准则和监管框架的制定将受到更多关注，以确保人工智能驱动的工具在法律实践中被负责任地使用。

总之，在未来的法律领域，人工智能有望在法律实践的各个方面取得重大进展，从研究和分析到争议解决和合规。随着这些技术的不断发展，法律专业人士必须适应和接纳人工智能提供的机会，同时也要应对人工智能融入法律领域所带来的挑战。

（三）ChatGPT 和其他人工智能技术导引下的法律愿景

诸如 ChatGPT 这样的人工智能技术融入法律领域，正在改变法律专业人士的工作方式和他们提供的服务。为了成功适应不断变化的法律环境，法律从业者必须理解并接纳人工智能驱动的工具和策略带来的种种可能性。我们将围绕如何利用 ChatGPT 和其他人工智能技术有效导引法律愿景提供一些指导：

1. 接纳技术的发展更新。法律专业人士必须对人工智能技术及其在法律领域的应用有一个深刻的理解。这包括随时了解人工智能驱动的工具的最新发展、参与培训和教育计划，并与技术专家、数据科学家和其他专家进行跨学科合作。

2. 战略性地利用人工智能驱动的工具。法律从业者应该明确他们最能从人工智能驱动的工具中受益的领域，如法律研究、文件起草、案件策略和监管合规。通过战略性地利用 ChatGPT 等人工智能技术，法律专业人士可以提高他们的效率、效能和竞争优势。

3. 解决道德、隐私和安全问题。法律专业人士必须解决法律领域使用人工智能所产生的道德、隐私和安全问题。这包括确保人工智能驱动的工具被负责任地使用、保护客户数据，以及遵守法律实践中人工智能相关的专业标准和准则。

4. 培育适应性和创新性的文化。为了成功地适应不断变化的法律环境，法律专业人士应该在机构内培养一种适应性和创新性的文化。这包括鼓励对新技术的尝试，促成成长型思维模式，以及促进专业人士的可持续发展。

5. 发展新的技能和能力。法律专业人士应该积极主动地发展必要的技能和能力，以便在人工智能驱动的法律环境中取得成功。这包括提高他们的技术熟练度、数据分析技能和跨学科合作能力，以及加深对人工智能带来的法律和伦理影响的理解。

6. 参与继续教育和培训。为了在不断变化的法律环境中保持领先地位，法律专业人士应该参与关于人工智能技术及其在法律领域的应用的继续教育和培训，包括参加以人工智能和法律为重点的研讨会、讲习班、会议和专业发展计划。〔6〕

〔6〕 2018 年新学期伊始，哈佛大学、康奈尔大学、麻省理工学院、斯坦福大学等美国高校的课程表上多了一门新课程，名为人工智能伦理、数据科学伦理、技术伦理、机器人伦理等等。哈佛大学和麻省理工学院合作开设了一门人工智能伦理和监管课程，名为“人工智能伦理与治理”（参见课程网站 https://www.media.mit.edu/courses/the-ethics-and-governance-of-artificial-intelligence/）。这门课程聚焦人工智能的伦理、政策和法律影响，涵盖算法歧视、责任、自主性、系统设计、信用评分、图像识别、数据所有权、AI 治理、AI 可解释性和可问责性、自动化对劳动力的影响、AI 监管等热门问题。这门课程激发学生思考基本伦理问题，比如，技术是公平的吗？如何确保数据是无偏见的？机器应当评判人类吗？

7. 倡导负责任的人工智能监管和发展。法律专业人士在倡导负责任的人工智能监管和发展方面可以发挥关键作用。通过为立法部门有关人工智能的法律、法规和专业标准的制定贡献他们的专业知识，法律从业者能够有助于引领一个更加负责任的、公平的人工智能驱动的法律服务的未来。

总之，利用 ChatGPT 和其他人工智能技术导引法律愿景，需要法律专业人士接纳技术的发展更新，战略性地利用人工智能驱动的工具，解决道德、隐私和安全问题，培养适应性和创新性的文化，发展新的技能和能力，参与继续教育和培训，并倡导负责任的人工智能监管和发展。通过采取这些措施，法律从业者可以成功地适应不断变化的法律环境，并充分利用人工智能的潜力提高他们的执业水平，更好地为客户服务。

三、走向未来：塑造更高效率、更有效力和更为公平的法律实践

人工智能与法律行业的整合正在迎来一个范式转变，诸如 ChatGPT 这样的工具在塑造法律实践的未来中发挥着关键作用。随着人工智能技术的不断进步，法律专业人士有机会利用其潜力来提高效率、优化决策和提供更具个性化的客户服务。

此前，我们探讨了人工智能对法律实践各个方面的变革性影响，包括但不限于法律研究和分析、文件自动化处理、诉讼、替代性纠纷解决、合规、风险管理和法律教育。我们还研究了与人工智能融入法律领域相关的伦理道德和法律挑战，强调了公平性、透明度、问责制和负责任地使用这些技术的必要性。

接纳人工智能驱动的工具所带来的机会，需要法律专业人士不断发展他们的技能、培养终身学习的思维模式，并勇于改变。借此，他们可以有效地适应不断变化的法律环境，并利用好人工智能提供的种种可能性。

与此同时，解决人工智能带来的挑战，需要法律专业人士、人工智能开发者、政策制定者和其他利益相关者之间的充分合作。他们必须一起努力制定道德准则、监管框架和最佳实践，以确保人工智能驱动的工具在法律实践中被负责任地使用。

总之，我们对人工智能融入法律领域的变革性影响进行了全面且发人深省的研究。当我们迈入这个激动人心的新时代时，法律专业人士、政策制定者和利益相关者有责任抓住机遇，并解决由人工智能驱动的工具（如 ChatGPT）带来的挑战。借此，他们可以帮助塑造一个更有价值、更具效率和更为公平的法律体系，以造福客户和整个社会。

（一）人工智能与法律行业的整合：一种范式转变

像 ChatGPT 这样的人工智能技术融入法律领域，正在推动一种范式转变。它正在改变法律服务的提供方式、法律专业人士的职能和技能组合，以及法律职业的整体结构和文化。我们探讨了这种范式转变的关键方面以及对法律行业未来的影响。

1. 法律服务的大众化。人工智能驱动的工具正在使法律服务变得更易获得、更实惠，使以前可能因高成本或过于复杂而面临障碍的个人和组织有更多机会获得法律救济。这种模式的转变正在改变法律服务的提供方式，使之越来越注重效率、自动化和以客户为中心。

2. 数据驱动型决策的崛起。人工智能技术使法律专业人士能够分析大量的数据，从而做出更明智的、基于大数据的决策。这正在改变法律专业人士处理法律研究、案件策略和风险评估的方式，从而带来更准确、更高效和更有效的结果。

3. 法律专业人士的新技能。人工智能在法律领域越来越重要，这就需要法律专业人士发展新的技能和能力。这包括技术能力、数据分析能力，以及对人工智能带来的伦理和法律挑战的理解。这种技能组合的变化将影响法律教育、培训和职业发展。

4. 跨学科合作与创新。人工智能融入法律领域的日益盛行，促成了更多的合作和跨学科的法律实践。法律专业人士正越来越多地与来自数据科学、技术和伦理学等领域的专家合作，开发人工智能驱动的工具，部署人工智能驱动的战略。这种合作方式推动了创新，提高了法律服务的效率。

5. 不断发展的法律和伦理框架。人工智能融入法律行业带来了新的法律和道德挑战，需要制定新的法律、法规和专业标准来规范人工智能在法律实践中的应用。这种不断发展的法律和伦理框架将塑造人工智能驱动的法律服务的未来，并影响法律专业人士的职能。

6. 变化中的法律就业形势。由人工智能驱动的范式转变对法律就业形势产生了影响。虽然一些传统的法律职能可能会被自动化取代，但对于拥有必要的技术能力和适应性的法律专业人士来说，新的机会将会出现。这种转变可能会重新定义法律工作的性质，更加强调需要人类判断和创造力的高附加值任务。

总之，诸如 ChatGPT 这样的人工智能技术融入法律领域，正在促成一种范式转变，对法律专业的未来具有深远的影响。随着法律服务变得更加大众化、强调数据和跨学科，法律专业人士必须适应新的技能组合，拥抱创新，并驾驭不断变化的法律和道德框架。通过认识和接纳这种范式转变，法律专业人士可以帮助塑造更高效、更有效和更公平的法律实践。

（二）ChatGPT 塑造法律实践未来的潜力

ChatGPT 是一种先进的人工智能语言模型，有可能通过改变法律职业的各个方面——从研究和分析到文件起草和纠纷解决——极大地塑造法律实践的未来。通过利用 ChatGPT 的力量，法律专业人士可以简化他们的工作流程，提高决策能力，并提供更优质的客户服务。以下是 ChatGPT 塑造法律实践未来的一些方式：

1. 法律研究和分析：ChatGPT 可以分析大量的法律数据，明确相关的先例，并对复杂的法律问题提供见解。这可以提高法律研究的效率和准确性，使律师能够做出更明智的决定，制定更有效的战略。

2. 文件自动化处理和起草：ChatGPT 可以更精确和高效地起草法律文件，如合同、简报和诉状。通过自动化处理这些任务，法律专业人士可以节省时间，降低失误风险，从而能够专注于更多高战略性和高附加值的任务。

3. 纠纷解决和谈判：ChatGPT 可以通过分析案例数据，洞察各方立场的优势和劣势，并提出最佳谈判策略，在纠纷解决过程中发挥重要作用。这可以帮助法律专业人员在调解、仲裁或和解谈判中为客户取得更好的结果。

4. 合规和风险管理：ChatGPT 可以帮助法律专业人士识别潜在的法律风险，并通过分析各

种法律法规来确保合规。通过积极主动地解决这些问题，企业可以减轻他们面临的司法和经济处罚。

5. 法律教育和培训：ChatGPT 可以作为法学生和专业人士的学习工具，帮助他们加深对法律概念的理解，了解具体领域的最新发展。这可以促进法律专业人员的可持续发展，使他们更好地适应不断变化的法律环境。

6. 个性化的法律服务：通过利用 ChatGPT，法律专业人士可以根据客户的需求和喜好提供更多个性化和定制化的法律服务，从而提高客户满意度，深化客户关系。

7. 伦理和法律决策：ChatGPT 可以帮助法律专业人士衡量伦理道德和法律问题，帮助他们在实践中做出更负责任、更全面的决策。

ChatGPT 拥有巨大的潜力去塑造未来的法律实践，因为它可以简化流程、优化决策，并最终有助于建立一个更高效和更有效的法律体系。然而，解决与人工智能驱动的工具相关的道德和法律挑战至关重要，例如潜在的偏见、透明度和问责制问题。借此，法律专业人士、人工智能开发者、政策制定者和利益相关者可以确保 ChatGPT 和其他人工智能技术在法律领域的整合是负责任的，同时也是有益的。

（三）拥抱机遇，应对人工智能在法律领域的挑战

随着像 ChatGPT 这样的人工智能技术不断重塑法律领域，法律专业人士必须学会拥抱机遇，并解决人工智能融入法律领域的相关挑战。本节概述了利用人工智能驱动的工具的好处，也阐述了一些策略，有助于克服可能存在的障碍和隐忧。

1. 识别充满机遇的领域。法律专业人士应评估他们的实践，以确定在哪些领域可以从人工智能驱动的工具中受益最多，如法律研究、文件起草、案件策略和监管合规。通过战略性地整合人工智能技术，法律专业人士可以提高他们的效率、效能和竞争优势。

2. 投资于技能发展。为了在人工智能驱动的法律环境中取得成功，法律专业人士必须积极主动地发展必要的技能和能力，包括技术应用能力、数据分析技能，以及加深对人工智能带来的法律和伦理影响的理解。投资于继续教育、培训和跨学科合作，对于在不断变化的法律环境中与时俱进至关重要。

3. 培育创新文化。法律专业人士应在其机构内培育创新文化。鼓励对新技术的尝试，促成成长型思维模式，以及投资员工的专业发展，这有助于机构适应不断变化的法律环境，并拥抱人工智能驱动的工具所提供的机遇。

4. 解决伦理道德、隐私和安全问题。随着人工智能融入法律领域日益普遍，法律专业人士解决伦理、隐私和安全问题是至关重要的。应当确保人工智能驱动的工具被负责任地使用，保护客户数据，并在法律实践中遵守相关的专业标准和法规，这样才能维护好公众信任和职业操守。

5. 参与政策制定和宣传。法律专业人士在塑造人工智能和法律的政策环境方面可以发挥关键作用。在立法部门制定有关使用人工智能的法律、法规和专业标准时，法律从业者可以贡献他们的专业知识，帮助创建一个负责任的、公平的人工智能驱动的法律服务框架。

6. 接纳合作和跨学科的实践。人工智能融入法律领域促成了更多的合作和跨学科的法律实践。法律专业人士应该抓住机会与其他领域的专家合作，如数据科学家、技术专家和伦理学家，

以开发人工智能驱动的工具，部署人工智能驱动的战略。这种合作方式可以带来更有效和创新的法律解决方案。

7. 利用人工智能来促进法律救济。人工智能融入法律领域所带来的最重要的机遇之一是促进法律救济。法律专业人士应该试验性利用人工智能驱动的工具，使法律服务被更实惠、更高效、更容易地获取，从而缩小司法鸿沟，确保更多的个人和组织能够获得他们需要的法律救济。

总之，面对人工智能为法律领域带来的机遇和挑战，法律专业人士需要从战略上整合人工智能技术，投资于技能发展，培育创新文化，解决伦理道德、隐私和安全问题，参与政策制定和宣传，加强跨学科合作，并利用人工智能来促进法律救济。通过采取这些步骤，法律从业者可以成功地适应不断变化的法律环境，并充分利用人工智能的潜力来改进他们的业务，更好地为客户服务。

Abstract: The future of law and artificial intelligence (AI) is full of both opportunities and challenges. The impact of AI on the legal field includes, but is not limited to, legal research and analysis, document automation, litigation, alternative dispute resolution, compliance, risk management, and legal education. With the integration and promotion of generative AI technologies such as ChatGPT, the ongoing transformation of the legal field is reshaping the way legal services are provided, the functions and skillsets of legal professionals, as well as the overall structure and culture of the legal profession. Legal professionals, policymakers, and stakeholders should embrace technological advances, strategically use AI-driven tools, and respond to a constantly changing legal environment by devising ethical standards, regulatory frameworks, and best practices. They must also address the ethical and legal challenges posed by AI, including data privacy, fairness, transparency, accountability and ensure that AI-driven tools are used responsibly in legal practice. This paradigm shift will help shape a more efficient, effective, and fair legal system that benefits clients and the entire society.

Key Words: law and artificial intelligence, generative AI, responsible AI, transparency, accountability

（责任编辑：刘　权　赵建蕊）

财经法学 No. 6，2022
pp. 96 - 110

全球数据治理的 DEPA 路径和中国的选择

靳思远 *

内容提要：随着数字科技的发展，数据已成为各国的基础性、战略性资源。各国对数据资源的争夺日趋激烈，数据跨境流动等议题成为国际关注的焦点。由于数据兼具财产利益和人格利益属性，各国治理数据的理念存在分歧，目前数据的全球治理框架尚未形成。《数字经济伙伴关系协定》（DEPA）是全球首个针对数字经济而制定的专项协定，在数据议题上主要借鉴了美式数字规则并采用了灵活的模块式框架，反映了新加坡等中小国家在数字治理方面的诉求，相较传统综合性的贸易协定更具时代性、灵活性和可扩展性。从中国正在构建的数据出境评估体系来看，中国国内数字规则与 DEPA 等高水平国际数字规则之间存在一定的张力。中国申请加入 DEPA 有利于促进本国数字经济发展和国际合作，提升数据治理水平，进一步扩大中国在全球数据治理中的话语权。

关键词：DEPA　数字经济　全球数据治理

近年来，随着科技的迅猛发展，数据已成为全球经济活动中不可或缺的生产要素。国家通过制定数字规则、缔结和参加国际协定等方式参与全球数字经济治理，力求在全球数字经济竞争中获得优势。2020 年中国数字经济规模为 5.4 万亿美元，比 2019 年增长 9.6%，增速位居世界第一，规模位居世界第二。〔1〕我国数字经济规模无论在增速还是体量上都在全球范围内位居前列。但是，我国的数字经济规模与我国在全球数字贸易中的话语权并不匹配，亟需构建兼顾数字产业特点和我国诉求的“中国方案”。〔2〕2021 年 10 月 30 日，习近平在 G20 领导人第十六次峰会上提

* 靳思远，上海交通大学法学院博士研究生。

本文为 2021 年国家社科基金重大项目“美国全球单边经济制裁中涉华制裁案例分析与对策研究”（21&ZD208）的阶段性成果。

〔1〕 参见中国信息通信研究院：《全球数字经济白皮书——疫情冲击下的复苏新曙光》，载 http://www.caict.ac.cn/kxyj/qwfb/bps/202108/P020210913403798893557.pdf，最后访问时间：2022 年 1 月 8 日。

〔2〕 参见赫璟、陈紫媛：《DEPA 协定有利于数字规则“中国模板”的构建》，载《国际商报》2022 年 2 月 15 日，第 7 版。

出，中国决定申请加入《数字经济伙伴关系协定》（Digital Economy Partnership Agreement，简称DEPA）。〔3〕2021年11月1日，中国商务部部长代表中方向DEPA保存方新西兰正式提出加入DEPA申请。〔4〕2022年2月17日，中国商务部发言人表示，中方现阶段正与DEPA缔约方开展沟通和技术磋商，中方希望为DEPA成员国企业提供合作机遇和广阔的市场，并在创新和可持续发展等方面作出中国贡献。〔5〕

中国的申请加入可能使DEPA在未来的全球数字经济规则框架中占据更为主流的地位，而DEPA作为开放性的数字经济协定为中国参与全球数据治理提供了一种新的路径。本文通过分析全球数据治理格局和DEPA的数据相关议题，结合中国数据出境评估体系的制度现状，探究中国加入DEPA在数据治理方面可能带来的机遇和挑战。

一、全球数据治理格局

随着全球数字化进程的推进，传统贸易逐渐向数字化趋势发展。数据作为数字经济的基础性资源和不可或缺的生产要素，被视为数字经济深化发展的核心引擎。〔6〕以信息技术驱动的全球数字贸易在很大程度上依赖于数据的跨境流动。在倡导“规则的设定应围绕资源的有效配置和合理利用展开，以追求制度效率的最大化”的法经济学视角下，〔7〕数据实际上构成了一种固定于一定载体上，能够满足人们生产和生活需要，具有确定性、可控制性、独立性、价值性和稀缺性等特征的信息财产。〔8〕从信息主体的角度看，数据作为个人信息的重要载体，又关系到个人隐私保护和人格利益。因此，数据兼具财产利益和人格利益，在数据治理中分别对应数据流动和数据安全。前者强调数据在数字交易中的经济价值和商业价值，后者强调通过法律保护个人隐私和信息安全。不同国家基于本国对数据技术掌控的能力、经济制度和经济发展等因素的影响，产生了不同的规制路径并影响其参与全球博弈的立场，分歧在所难免。在WTO多边数字贸易治理体系无法取得突破性进展的背景下，各国治理数据的路径呈现多元化态势，〔9〕全球数据治理格局具有复杂性的特征。其中，美国与欧盟两个发达经济体之间的跨境数据流动量位居世界首位，双方在数字贸易、隐私和国家安全方面的不同做法已经对美欧之间的数据流动造成一定的阻碍。这种阻碍尤其体现在Schrems系列案件〔10〕中，用于跨大西洋数据传输的法律依据——“安全港协议”“隐私盾协议”——均被欧盟法院判定无效。美欧通过国内法的“长臂管辖”和与他国区域

〔3〕 参见新华网：《习近平在二十国集团领导人第十六次峰会第一阶段会议上的讲话》，载http://www.xinhuanet.com/world/2021-10/30/c_1128013842.htm，最后访问时间：2022年1月8日。

〔4〕 参见人民网：《中方正式提出申请加入〈数字经济伙伴关系协定〉》，载http://finance.people.com.cn/n1/2021/1101/c1004-32270753.html，最后访问时间：2022年1月9日。

〔5〕 参见文汇网：《中方目前正按照CPTPP有关加入程序，与各成员进行接触磋商》，载https://www.whb.cn/zhuzhan/rd/20220217/450203.html，最后访问时间：2022年1月9日。

〔6〕 参见沈伟、赵尔雅：《数字经济背景下的人工智能国际法规制》，载《上海财经大学学报》2022年第5期。

〔7〕 See Richard A. Posner, *Economic Analysis of Law*, Aspen Law & Business, 1998, p. 3.

〔8〕 参见齐爱民：《捍卫信息社会中的财产》，北京大学出版社2009年版，第53-54页。

〔9〕 参见齐俊妍、强华俊：《数据流动限制、数据强度与数字服务贸易》，载《现代财经》2022年第7期。

〔10〕 参见单文华、邓娜：《欧美跨境数据流动规制：冲突、协调与借鉴——基于欧盟法院“隐私盾”无效案的考察》，载《西安交通大学学报（社会科学版）》2021年第5期。

贸易协定中数字贸易规则的谈判，试图将带有本国利益色彩的国内法推广至国际规则层面。

以《跨太平洋伙伴关系协定》（Trans-Pacific Partnership Agreement，简称 TPP）电子商务章、《美墨加协定》（The United States-Mexico-Canada Agreement，简称 USMCA）数字贸易章为代表的“美式规则”强调贸易便利化、跨境数据自由流动、免收数字关税、源代码开放等内容，其主张构建开放自由的全球数字市场。从数字经济发展历史看，美国作为互联网的发源地，无论是互联网企业的数量还是信息产业发达程度都领先全球，互联网科技巨头在早期更是可以轻而易举地从他国获得大量数据信息。因此其政策具有准入严格而监管相对松弛的特性，主张数字贸易自由化和便利化。从美国国内法上看，个人数据被包含在隐私保护的框架内，但没有类似欧盟《一般数据保护条例》（General Data Protection Regulation，简称 GDPR）的关于隐私保护的综合性法律，而是分散在各种行业的合同相关法律上。〔11〕美国的隐私保护主要由数据处理者和隐私消费者之间的合同提供，并由美国联邦贸易委员会监督。〔12〕但事实上，由于缔约双方之间的权力和信息不对称，个人数据并不能得到充分的保护。虽然美国联邦最高法院通过其判例确认公民享有个人数据的宪法保护权利，但各级法院一般都避开了这一决定。最高法院对宪法的解释是赋予个人隐私权，但这一权利通常只是为了防止政府对公民隐私的侵犯。〔13〕虽然美国目前没有专门规制跨境数据流动的法律，但对个人敏感数据、政府重要数据、商业数据等数据出境有着较为严格的管控要求。美国尤其关注外国产品或服务中收集、获取美国敏感数据的风险，并以国家安全为由对外国产品或服务进行较为严格的管控。例如，特朗普政府在执政期间以国家安全为由，通过行政令等方式意图驱逐或封杀 TikTok，施压其母公司字节跳动放弃对 TikTok 的所有权。拜登上台后通过颁布一系列针对信息及通信技术和服务供应链审查规则（ICTS 规则）的行政令，进一步强化了对跨国科技企业的安全审查。总体而言，美国在数据治理中秉持“全球主义”理念，既通过国内法限制公权力对数据流动的干预，又倡导“私法自治”，赋予私主体在保护个人权利和创造商业价值之间更大的选择权。〔14〕但在国际投资领域，美国又以维护国家安全为由对外国数据控制者在美国国内的经营活动进行严格审查，以消除跨境数据流动对美国国家安全可能带来的威胁。虽然“美式规则”主张构建开放自由的全球数字市场，但 USMCA 针对非市场经济国家的“毒丸条款”〔15〕和“美式规则”对数字市场开放的高水平要求一定程度上加深了与发展中国家之间的“数字鸿沟”，以“美式规则”作为全球数字治理方案仍然存在诸多阻碍。

不同于美国的“全球主义”，欧盟在数据治理方面主张建立数字单一市场，数据可以在该市场内部自由流通并受到欧盟数字法规的严格保护，而数据的跨境流动也会受到较为严格的限制。欧盟拥有目前最严格的数据保护规则，根据 2000 年《欧盟基本权利宪章》（Charter of Funda-

〔11〕 See Zheng Guan，Trilemma and Tripartition：The Regulatory Paradigms of Cross-Border Personal Data Transfer in the EU，the U. S. And China，43 *Computer Law & Security Review* 5 (2021).

〔12〕 参见前引〔11〕，Zheng Guan 文。

〔13〕 例如 1978 年的《美国隐私法》（U. S. Privacy Act）规定了联邦政府如何管理其拥有的个人信息，1986 年的《电子通信隐私法》（Electronic Communications Privacy Act）扩大了政府对电话窃听的限制，包括对电脑传输电子数据的限制。

〔14〕 参见沈伟、冯硕：《全球主义抑或本地主义：全球数据治理规则的分歧、博弈与协调》，载《苏州大学学报（法学版）》2022 年第 3 期。

〔15〕 非市场经济条款，又称“毒丸条款”，即禁止与美国有自贸协定的贸易伙伴与非市场经济国家签订自贸协定。参见沈伟：《“修昔底德”逻辑和规则遏制与反遏制——中美贸易摩擦背后的深层次动因》，载《人民论坛·学术前沿》2019 年第 1 期。

mental Rights of European Union）第7条〔16〕和第8条，〔17〕通信隐私和个人数据保护是欧盟国家公民的基本权利。基于人权保护，欧盟主张以本地化存储和数据跨境审核为核心的数据“本地主义”。欧盟通过提高跨境数据输出的审查标准及“长臂管辖”制度，〔18〕试图将GDPR建立的“欧盟数字标准”推广成世界标准。〔19〕欧盟数据保护规则适用于欧洲经济区（European Economic Area，简称EEA），其中包括所有欧盟国家和非欧盟国家冰岛、列支敦士登和挪威。欧盟在2016年4月通过改革数据保护立法，赋予个人更多对其个人数据的控制权，提供了将数据传输到第三国的多样化工具，包括“充分性决定”“标准合同条款”“具有约束力的公司规则”等等。其中，“充分性决定”用来确定非欧盟国家提供的数据保护水平与欧盟“基本相同”，其效果是使个人数据能够自由流动到该第三国，而无需数据出口商提供进一步的保障或获得任何授权。在不满足“充分性决定”要求的情况下，数据跨境流动可以在提供适当数据保护保障的其他替代转移工具的基础上进行。其中，“标准合同条款”被应用于欧盟加工商与非欧盟国家加工商之间的合同中，“具有约束力的公司规则”作为跨国公司集团采用的内部规则，用于在同一公司集团内向位于未提供足够保护水平的国家或地区的实体进行数据传输，也可以由从事联合经济活动的一组企业使用。欧盟通过自身市场在国际市场的中枢地位，借助强势的域外管辖立法，其严格的数据规制才能发挥所谓的“布鲁塞尔效应”（Brussel effect），〔20〕其他国家若想和欧盟进行数据交流必须“迎合”其“充分保护原则”下的严格条件。以GDPR为代表的欧盟数据保护法律框架也经常作为第三国制定该领域立法的参考点，欧盟同时在双边和多边层面积极与其国际合作伙伴进行对话，通过在全球范围内制定严格且可互操作的个人数据保护标准来促进数字贸易。

美欧基于对数据财产利益和人格利益的保护倾向不同，产生了“全球主义”和“本地主义”的治理理念分歧。而数字经济发展的新兴国家基于各自对数据属性的不同认识和本国国情而倾向于不同的数据治理理念。以俄罗斯、印度为代表的发展中国家倾向于“本地主义”，强调基于人权与主权的数据保护。俄罗斯既要求跨国企业在俄开展业务或提供服务时须在俄境内建立数据中心，也对数据存储和服务器地址提出本地化要求，总体上采取“孤岛式”的数据规制路径。〔21〕印度作为一个民族国家，将其公民产生的数据视为国家资产，在国界内存储和保护这些数据来维护其国防和战略利益。《印度电子商务国家政策框架草案》提出，印度将会逐步推进数据本地化政策并建立数据中心。〔22〕而以新加坡为代表的发达国家更倾向于“全球主义”，强调数据的跨境

〔16〕《欧盟基本权利宪章》第7条“尊重私人和家庭生活”规定：“人人均有权要求尊重其私人与家庭生活、住居及通信信息。”

〔17〕《欧盟基本权利宪章》第8条“个人数据的保护”规定：“1. 人人均有权保护其个人信息；2. 这些信息仅于特定目的，并且在信息所有人同意或法律规定的其他合法基础上公平处理，人人均有权查阅其个人信息，并有权要求纠正其信息；3. 这些规则的遵守应当受到独立机关的控制。”

〔18〕根据GDPR第3条“地域范围”的相关规定，即便数据控制者或处理者在欧盟境内没有设立实体机构，但其对数据主体的个人数据处理行为，即适用该法。参见叶开儒：《数据跨境流动规制中的“长臂管辖”——对欧盟GDPR的原旨主义考察》，载《法学评论》2020年第1期。

〔19〕参见前引〔18〕，叶开儒文。

〔20〕参见彭岳：《数字贸易治理及其规制路径》，载《比较法研究》2021年第4期。

〔21〕参见孙祁、〔俄〕尤利娅·哈里托诺娃：《数据主权背景下俄罗斯数据跨境流动的立法特点及趋势》，载《俄罗斯研究》2022年第2期。

〔22〕参见陈志：《亚洲国家数据跨境流动的实践及对我国的启示》，载《北京金融评论》2020年第1期。

流动和开放合作。除 DEPA 外，新加坡还分别与澳大利亚、英国签署了专项数字经济协定，这些数字经济协定鼓励国内监管改革和在数据创新、数字身份、网络安全等广泛问题上的跨境合作。2021 年 1 月 22 日，第一次东南亚国家联盟（ASEAN）数字部长会议批准了《东盟数据管理框架》（DMF）和《跨境数据流动示范合同条款》（MCC），〔23〕提出要建立东盟数据跨境流动机制并减少不必要的限制，这些文件都是由新加坡主持的数据治理工作组所制定。通过这些数字经济协定和多边安排，新加坡正逐步构建其主导的数字经济联盟及次级伙伴关系，为发展本国数字贸易、开展中小企业合作打下基础，为未来构建国际数字规则的谈判争取更大的话语权。

二、DEPA：全球数据治理的新路径

WTO 电子商务诸边谈判目前提案及进展表明，各成员的数字产业和贸易政策有很大不同，短期内难以达成一致的全球数字治理方案。数据是数字贸易和更广泛的数字经济的核心。美欧分别基于数字技术和数字市场的比较优势，在数据规制方面具有不同的理念和路径，并积极推进国内数字规则的国际法化。在此背景下，DEPA 作为世界首个专门针对数字经济、为促进数字贸易合作而制定的多边协定，其开放性的模块化框架和多元化的内容成为有别于美欧数字治理、反映中小国诉求的一种新路径，相较传统的数据治理路径更具有灵活性和可扩展性。从内容上看，无论是个人信息保护和跨境数据流动（模块 4）等争议性数据问题，还是数据创新（模块 9）、数字包容（模块 11）等新兴议题，都体现出新加坡等中小国家在数据治理问题上的开放性理念和规制路径，鼓励成员国之间可信数据（trusted data）的安全流动。

（一）争议性数据问题：“美式规则”基础上的调整和更新

美欧在数字贸易规则传统性议题上的矛盾和分歧体现在数据流动和个人信息保护等相关问题的处理上，这些问题集中体现在 DEPA 的模块 4 中，分别涉及个人信息保护（第 4.2 条）、跨境数据流动（第 4.3 条）和计算设施的位置（第 4.4 条）。

在个人信息保护问题上，DEPA 第 4.2 条构建了 10 条规则，从倡导性规则、构建个人信息保护相关法律应该考虑的关键原则、非歧视性原则及信息保护公开、信息保护机制的兼容性和数据保护信任标志等方面，对缔约方在个人信息保护方面提出了全面且兼具深度的承诺要求。TPP 第 14.8 条和 USMCA 第 19.8 条都对个人信息保护做了相关规定，两者和 DEPA 在倡导性规则、非歧视性原则及信息保护公开方面具有高度的重合性。具体而言，三者都强调保护数字用户个人信息的经济和社会效益，缔约国应考虑个人信息保护相关国际机构的原则和指南以制定本国的法律框架，采取非歧视性做法，从个人和企业层面公布其向数字贸易用户提供的个人保护信息。关于构建个人信息保护相关法律应该考虑的关键原则，TPP 未有提及，而 USMCA 作为“美式规则”的升级版提出了“限制收集、选择、数据质量、目的规范、使用限制、安全保障措施、透明度、个人的参与、问责制”共九个原则，并“确保对个人信息跨境流动的任何限制是必要的，并

〔23〕 参见中国商务部：《东盟发布〈东盟数据管理框架〉和〈东盟跨境数据流动示范合同条款〉》，载 http://asean.mofcom.gov.cn/article/jmxw/202102/20210203036591.shtml，最后访问时间：2022 年 8 月 2 日。

与所涉风险相称”〔24〕，即任何限制不能超过保护个人数据所需的要求。这种与隐私风险相称的必要限制正是“全球主义”的直接体现，与欧盟“本地主义”采取严格保护个人隐私的限制性措施不同，即前者的限制是例外、后者的限制是原则。DEPA 借鉴了 USMCA 除“选择”外的其他八个关键原则，但没有规定对个人信息跨境流动进行限制要遵守必要性原则，即在个人信息跨境流动的限制问题上做了保留。即便 DEPA 缔约国可以选择加入某一主题模块而无需一揽子同意，但从条文上来看，DEPA 在个人信息跨境流动问题上没有在“全球主义”和“本地主义”之间选边站，也一定程度上展现了新加坡等中小国家在此类争议性问题上的折中态度。

在跨境数据流动的问题上，DEPA 第 4.3 条与 TPP 第 14.11 条内容一致，通过三项规定，承诺有约束力的跨境数据自由流动。这种约束力体现在条文中“shall”“may”等情态动词的使用，“shall”表达的是法律的强制性，“may”传递的是法律的授权性。〔25〕第一项采用“may”授权缔约国对跨境数据流动有本国的监管要求。第二项和第三项均采用“shall”，要求缔约国既要允许跨境数据流动，也可以在不构成“不合理歧视或贸易限制”或“过度采取管制”的前提下，采用出于“合法公共政策目标”的跨境数据流动管制措施，这保留了缔约方对“跨境数据自由流动”进行管制的自主空间。〔26〕相较而言，USMCA 第 19.11 条只保留了上述第二、三项内容，没有授予其他缔约方设置本国监管要求的权限，即没有监管例外规定。类似地，在计算设施的位置问题上，DEPA 第 4.4 条与 TPP 第 14.13 条内容一致，要求不得强制将数据存储设施设置在当地，并规定了监管例外和公共安全例外。而 USMCA 第 19.12 条仅规定了“任何一方不得要求被覆盖人员在其领土内使用或放置计算设施，以此作为在该领土内开展业务的条件”，没有其他例外规定。在一般例外条款方面，DEPA 第 15.1.3 条将《服务贸易总协定》（GATS）第 14 条和《1994 年关税与贸易总协定》（GATT1994）第 20 条的所有内容纳入规则范围，而 TPP 第 29.1.3 条和 USMCA 第 32.1.2 条仅将 GATS 第 14 条（a）—（c）纳入规则范围，排除了（d）（e）与最惠国待遇和国民待遇相冲突的两种情况以及 GATT1994 第 20 条列举的一般例外适用情形。通过对比 DEPA、TPP 和 USMCA 的数据规制条文不难发现（如表 1 所示），DEPA 除了避开“与隐私风险相称的必要限制”的争议性原则，首倡数据保护信任标志的国际合作，其他事项都充分借鉴了 TPP 电子商务章和 USMCA 数字贸易章的“美式规则”。但 DEPA 在数据规制上的例外规定范围明显大于 USMCA，这也说明了 USMCA 较 DEPA 具有更高的开放度，DEPA 也更加侧重保护缔约方的监管权限。从新加坡等中小国家的发展来看，这种对数据跨境流动相对保守的态度是出于对本国中小企业发展的保护。以美国为代表的“全球主义”国家坚持数字贸易自由化，试图最大限度地消除各国数字贸易进入障碍，为其优势数字企业扩大市场份额提供便利，数字贸易相对落后的国家则希望通过设置保护壁垒为本土数字企业发展赢得成长空间。

〔24〕 USMCA Article 19.8.3.

〔25〕 参见王子颖：《法律语篇中 shall 和 may 的翻译对比研究》，载《上海翻译》2013 年第 4 期。

〔26〕 参见陈寰琦、陆锐盈：《DEPA 数据安全规则解析及对中国的启示》，载《长安大学学报（社会科学版）》2022 年第 2 期。

表 1 DEPA、TPP 和 USMCA 数据规制相关条文对比

事项	DEPA	TPP	USMCA
个人信息保护	在倡导性规则、鼓励缔约方发展兼容的信息保护机制、非歧视性原则及信息保护公开等方面较为一致		
	第 4.2.3 条规定了 8 个关键原则，没有规定对个人信息跨境流动进行限制要遵守必要性原则	未规定制定法规的关键原则	第 19.8.3 条规定了 9 个关键原则和“与隐私风险相称的必要限制”原则
	第 4.2 条 8—10 款鼓励缔约方就数据保护信任标志展开合作	未规定数据保护信任标志相关内容	
跨境数据流动	DEPA 第 4.3 条与 TPP 第 14.11 条内容一致，都承诺有约束力的跨境数据自由流动，并规定了监管例外和公共安全例外		没有监管例外
计算设施的位置	DEPA 第 4.4 条与 TPP 第 14.13 条内容一致，要求不得强制将数据存储设施设置在当地，并规定了监管例外和公共安全例外，保留监管自主空间的权限		USMCA 第 19.12 条仅保留了推动数据流动自由化的条款，没有监管例外和公共安全例外
一般例外条款	DEPA 第 15.1.3 条将 GATS 第 14 条和 GATT1994 第 20 条的所有内容纳入规则范围，较 TPP 和 USMCA 更广泛	TPP 第 29.1.3 条和 USMCA 第 32.1.2 条都要求针对“数字贸易”或“电子商务”章节，仅参考 GATS 第 14 条（a）（b）（c）的要求进行例外条款修订	

表格来源：作者整理。

（二）新兴数据议题为全球数据治理提供了中小国方案

除了传统性的数据议题，DEPA 还提出了一系列创新性的数据议题，为全球数据治理提供了最新的关注点。首先，在数字贸易便利化方面，DEPA 首倡电子发票、物流和快递等议题，提倡缔约国努力实现数据交换系统的互联互通，努力构建国际公认的数据开放标准，以提升数字贸易的效率、降低交易成本。其次，DEPA 要求缔约方认识到在个人或企业数字身份方面的合作将有利于区域和全球互联互通，构建数字身份的安全和可互操作的标准会使消费者因数字身份被欺诈案件减少，企业受益于电子方式可以进行更高效的交易。再次，跨界数据流动和数据共享能够实现数据驱动的创新，DEPA 鼓励缔约国通过监管“沙盒”等方式进行合作，实现跨国界的数据驱动创新以促进新产品和服务的开发。中小企业也应当通过创建免费且可公开访问的网站实现跨国企业之间信息的互联互通，通过举办数字中小企业对话等活动促进企业合作。最后，DEPA 鼓励缔约国开放政府数据，便利公众获取和使用政府信息可促进经济和社会发展、竞争力提升和创新。政府开放的数据是政府部门掌握的没有经过加工处理的原始数据，政府数据开放的真正意义在于对这些数据进行共享和利用。〔27〕缔约方应努力开展合作，以确定缔约方可扩大获取和使用公开数据的方式，以期增加和创造商业机会。此外，DEPA 还提倡在金融科技、人工智能等领域展开数据方面的交流和合作。

然而，上述倡议性的新兴数据议题大多都是鼓励缔约国展开合作，并没有具有可操作性的方

〔27〕 参见李涛：《政府数据开放与公共数据治理：立法范畴、问题辨识和法治路径》，载《法学论坛》2022 年第 5 期。

案。例如，在金融科技领域，DEPA 鼓励双方在行业层面的合作，但事实上这种合作是基于双方国内金融机构控制的数据和信息交流，DEPA 并没有规定金融数据相关的市场准入问题，很可能会使这样的倡议流于形式。相较而言，《英国—新加坡数字经济协议》（The UK-Singapore Digital Economy Agreement，简称 UKSDEA）对金融部门的跨境数据流动有着更明确的要求，〔28〕英新两国之间金融数据的流通就有了更强的非歧视性待遇保证。另外，DEPA 认识到监管“沙盒”对数据创新的重要性，但是并没有对数据开放等实质性问题提出解决方案，例如怎样平衡数据流动和个人信息保护之间的冲突，在政府、数字企业、个人之间关于数据方面的权利义务分配上坚持怎样的原则等。可见，DEPA 虽然在这些创新性议题上表达了中小国家在数字贸易方面的利益诉求，但这种诉求仍然是宏观且宽泛的，仍需进一步构建具有可操作性的方案。

三、DEPA：数据治理的中国选择

中国经济正处于迈向高质量发展新阶段的关键期，以新基建为主要引擎的数字化转型发展战略持续深入推进。〔29〕目前，中国尚未形成具有鲜明特征的数字贸易规则主张，这主要是由于我国将数据流动置于国家安全的考量范围，突出了安全风险。在数字贸易规则深入性议题方面，我国呈现出较为保守的态度，在规则国际博弈中处于防守地位。〔30〕我国数字贸易比较优势主要集中在基于互联网平台的货物贸易，因此在参与 WTO 电子商务诸边谈判时，我国的提案主要侧重于跨境货物贸易及相关支付和物流服务方面，如电子认证、电子合同等贸易便利化层面促进电子商务的传统议题。〔31〕我国在最近的一份公开性提案中提出，对于数据流动、数据存储、数字产品处理等敏感和复杂的问题，需要进行更多的探索性讨论。〔32〕但在原则上，数据流动应当以安全为前提，数据安全关系到每个 WTO 成员核心利益，所以有必要按照各国法律法规进行有序的数据流动。〔33〕我国目前已签署的双边自由贸易协定（Free Trade Agreement，简称 FTA）电子商务章节中的条款大多数是在 WTO 框架下早已达成共识的传统条款。例如，中国与 DEPA 的三个发起国都分别签订了 FTA 且均包含电子商务章，但内容局限于无纸化贸易、关税、透明度义务、在线消费者保护等内容，在具有争议的个人信息保护议题方面大多只是强调个人信息保护的重要性、制定相关法律要考虑相关国际组织或机构的标准等“倡议性”规定。

此次申请加入 DEPA 表明我国在全球数据治理中的路径选择，即接受 DEPA 基于中小国家

〔28〕 例如，UKSDEA 第 8.53.1 条规定：“每一方均应允许另一方的金融服务供应商提供甲方允许其同类金融服务供应商提供的任何新的金融服务，而无需甲方要求采取额外的立法行动。各缔约方可确定提供新金融服务的机构和司法形式，并可要求获得提供该服务的授权。如果一方要求此类授权，则应在合理的时间内作出决定，且仅可根据第 8.50 条（审慎剥离）的审慎理由拒绝授权。”第 8.54.1 条规定：“在遵守适当的隐私和保密保障措施的前提下，如果此类转移是在该金融服务供应商的正常业务过程中需要的，任何一方不得禁止或限制另一方的金融服务供应商将电子或其他形式的信息转移到或转移出其领土。”

〔29〕 参见腾讯网：《中国申请加入 DEPA 的九大看点》，载 https://new.qq.com/omn/20211103/20211103A06IX500.html，最后访问时间：2022 年 2 月 10 日。

〔30〕 参见朱福林：《数字贸易规则国际博弈、“求同”困境与中国之策》，载《经济纵横》2021 年第 8 期。

〔31〕 参见李馥伊：《构建高标准自贸区网络的对策分析》，载《中国经贸导刊》2019 年第 17 期。

〔32〕 参见卢锋、李双双：《多边贸易体制应变求新：WTO 改革新进展》，载《学术研究》2020 年第 5 期。

〔33〕 See WTO，Joint Statement on Electronic Commerce-Communication from China，INF/ECON/40，Article 4.3.

数字经济发展诉求的理念和规则。在新冠疫情给国际贸易供应链造成了严重破坏的背景之下，包括中国和 DEPA 发起国在内的各国企业发展遭遇瓶颈，亟需有效的数字化转型战略和合作平台。DEPA 在发展数字经济领域具有更强的灵活性和专业性，人工智能、中小企业合作等创新性议题的引入更是增加了协定的前瞻性，与中国未来创新经济发展与转型的趋势、“坚持包容普惠、推动共同发展”〔34〕的理念相契合。国务院《“十四五”数字经济发展规划》指出，发展数字经济要“统筹发展和安全、统筹国内和国际”。〔35〕中国申请加入 DEPA 意味着在数字领域推动国内治理和国内法规向高标准数字规则看齐，并且考量 DEPA 在数字方面的某些规则，建立国内数据市场和数字贸易治理的标准，实现“两个统筹”。

约翰·杰克逊（John H. Jackson）教授的“接合”（interface）理论提出，两个国家即使只有很小的经济制度差异，它们在进行合作时必须有一种“接合”机制，否则就会发生摩擦或误解。〔36〕这种“接合”机制必须具备一定的开放性、包容性和灵活性，才能使不同经济制度的国家在同一个问题达成共识和合作。DEPA 从灵活开放的模块式框架结构到多元包容的数字议题，都具备国际数字经济规则的“接合”特性，以便不同国家在多元化的数字议题上寻求共识。对标 DEPA 高标准的数字贸易规则，能够在一定程度上倒逼我国加快数字经济领域建章立制的进度，对我国国内数字法规产生积极的“接合”作用。

推动数据跨境安全流动是 DEPA 的传统性议题的核心内容之一，我国申请加入 DEPA 也意味着我国在数据跨境流动问题上接受 DEPA 的规则和理念。从目前正在构建的数据出境评估体系来看，我国国内法在跨境数据流动问题上仍然秉持十分审慎的态度。虽然 DEPA 没有规定个人信息跨境流动限制要遵守必要性原则，但我国的态度与 DEPA 总体上鼓励数据跨境自由流动、政府数据开放共享等相对宽松的理念仍然存在一定的张力。

（一）构建中国数据出境评估体系

我国近年密集出台《网络安全法》《数据安全法》《个人信息保护法》等数字经济相关的多部法律法规，也在一些试验区试点企业数据分类和跨境流动。但目前国内的相关政策和法规与 DEPA 相比仍存在差距，偏重强调数据的安全属性和数据本地化要求。《个人信息保护法》严格规范了个人信息的存储、传输和处理，对国家安全构成潜在威胁的信息跨境传输将受到限制，第 36 条针对国家机关处理的个人信息设置了“境内存储为原则、安全评估后出境为例外”的原则，〔37〕在数据流动和数据安全中更倚重后者，以数据本地化存储为原则。第 38 条第 1 款规定个

〔34〕 中国政府网：《坚持包容普惠，推动共同发展——论习近平主席在首届中国国际进口博览会开幕式上主旨演讲》，载 http://www.gov.cn/xinwen/2018-11/07/content_5338282.htm，最后访问时间：2022 年 7 月 26 日。

〔35〕 参见中国政府网：《“十四五”数字经济发展规划》，载 http://www.gov.cn/zhengce/zhengceku/2022-01/12/content_5667817.htm，最后访问时间：2022 年 7 月 23 日。

〔36〕 这种“接合”（interface）机制借用了计算机术语。当需要两台不同机器的计算机一起工作时，通常需要某种“接口”机制或程序在它们之间进行调解。约翰·杰克逊教授认为，国家贸易法和关贸总协定-布雷顿森林体系如今是作为一种相当粗糙的（crude）“接合”机制运作的。See John H. Jackson, Import Practices: Are They Really Unfair?, 30 *Law Quadrangle* 26 (1986).

〔37〕《个人信息保护法》第 36 条规定：“国家机关处理的个人信息应当在中华人民共和国境内存储；确需向境外提供的，应当进行安全评估。安全评估可以要求有关部门提供支持与协助。”参见彭錞：《论国家机关处理的个人信息跨境流动制度——以〈个人信息保护法〉第 36 条为切入点》，载《华东政法大学学报》2022 年第 1 期。

人信息跨境提供必须具备下列四个条件之一，即“（1）通过国家网信部门组织的安全评估；（2）按照国家网信部门的规定经专业机构进行个人信息保护认证；（3）按照国家网信部门制定的标准合同与境外接收方订立合同，约定双方的权利和义务；（4）法律、行政法规或者国家网信部门规定的其他条件”。为使上述个人信息出境条件落地，除第四项兜底条款，国家网信部门近期分别发布了《数据出境安全评估办法》（简称《评估办法》）〔38〕《网络安全标准实践指南——个人信息跨境处理活动安全认证规范》（简称《安全认证规范》）〔39〕和《个人信息出境标准合同规定（征求意见稿）》（简称《标准合同规定》），〔40〕对前三个条件分别予以细化。其中，《评估办法》全面系统地提出了我国数据出境安全检查的具体要求，也标志着我国数据出境安全评估制度的正式落地。

从适用范围来看，《评估办法》第4条规定了数据处理者向境外提供数据〔41〕必须申报安全评估的四种情形：“（1）数据处理者向境外提供重要数据；（2）关键信息基础设施运营者和处理100万人以上个人信息的数据处理者向境外提供个人信息；（3）自上年1月1日起累计向境外提供10万人个人信息或者1万人敏感个人信息的数据处理者向境外提供个人信息；（4）国家网信部门规定的其他需要申报数据出境安全评估的情形。”关于“重要数据”的定义，《评估办法》第19条首次从部门规章层面予以明确，即指“一旦遭到篡改、破坏、泄露或者非法获取、非法利用等，可能危害国家安全、经济运行、社会稳定、公共健康和安全等的数据”。但该定义事实上掺杂着地缘政治因素，何种数据能够被认定为“可能危害”国家安全等并没有清晰的标准和边界，存在一定的模糊性，给予审查部门较大的主观裁量空间。《评估办法》适用范围外的个人信息处理者的数据出境情形，可以通过个人信息保护认证或者签订国家网信部门制定的标准合同来满足个人信息跨境提供条件，依法开展数据出境活动。〔42〕从评估内容和评估流程来看，《评估办法》第5条和第9条分别列举了数据处理者开展数据出境风险自评估的重点事项、与境外接收方订立的法律文件中数据安全保护责任义务主要内容，第8条列举了网信部门开展数据出境安全评估的重点事项，为数据处理者开展数据出境风险评估提供更具有可操作性的指导。

由表2可见，相较于申报人风险自评估的内容，网信部门安全评估重点事项与其基本一致，都包括了出境数据的基本要求、数据出境活动可能带来的风险、境外接受方数据保护水平、数据出境中和出境后的评估、境外接受方的数据安全保护责任义务等内容。安全评估重点事项在此基础上还增加了对境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境的评估，以及对数据处理者遵守中国法律、行政法规、部门规章情况的评估，充分体现了数据出境“风险

〔38〕 参见国家互联网信息办公室：《数据出境安全评估办法》，载 http://www.cac.gov.cn/2022-07/07/c_1658811536396503.htm，最后访问时间：2022年7月24日。

〔39〕 参见全国信息安全标准化技术委员会：《网络安全标准实践指南——个人信息跨境处理活动安全认证规范》，载 https://www.tc260.org.cn/upload/2022-06-24/1656064151109035148.pdf. 最后访问时间：2022年7月24日。

〔40〕 参见国家互联网信息办公室：《个人信息出境标准合同规定（征求意见稿）》，载 http://www.cac.gov.cn/2022-06/30/c_1658205969531631.htm，最后访问时间：2022年7月24日。

〔41〕《评估办法》所称数据出境活动主要包括：一是数据处理者将在境内运营中收集和产生的数据传输、存储至境外；二是数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以访问或者调用。

〔42〕 参见人民网：《〈数据出境安全评估办法〉答记者问》，载 http://politics.people.com.cn/n1/2022/0707/c1001-32469307.html，最后访问时间：2022年7月24日。

表 2　　数据出境风险自评估、安全评估及境外接受方数据安全保护责任义务内容比较

主要内容	自评估重点事项（第 5 条）	网信部门评估重点事项（第 8 条）	与境外接收方约定数据安全保护责任义务（第 9 条）
出境数据的基本要求	（一）数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；（二）（1）出境数据的规模、范围、种类、敏感程度	（一）数据出境的目的、范围、方式等的合法性、正当性、必要性；（三）（1）出境数据的规模、范围、种类、敏感程度	（一）数据出境的目的、方式和数据范围，境外接收方处理数据的用途、方式等
数据出境可能带来的风险	（二）（2）数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险	数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险	无（以责任承担的方式呈现）
境外接收方的数据保护水平	（三）境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全	（二）（2）境外接收方的数据保护水平是否达到中国法律、行政法规的规定和强制性国家标准的要求	（二）数据在境外保存地点、期限，以及达到保存期限、完成约定目的或者法律文件终止后出境数据的处理措施；（三）对于境外接收方将出境数据再转移给其他组织、个人的约束性要求
数据出境中和出境后的评估	（四）数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，个人信息权益维护的渠道是否通畅等	（三）（2）出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险； （四）数据安全和个人信息权益是否能够得到充分有效保障	（六）出境数据遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等风险时，妥善开展应急处置的要求和保障个人维护其个人信息权益的途径和方式
境外接收方的数据安全保护责任义务	（五）与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等是否充分约定了数据安全保护责任义务	（五）数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务	（四）境外接收方在实际控制权或者经营范围发生实质性变化，或者所在国家、地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形导致难以保障数据安全时，应当采取的安全措施；（五）违反法律文件约定的数据安全保护义务的补救措施、违约责任和争议解决方式
其他	无	（二）（1）境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响；（六）遵守中国法律、行政法规、部门规章情况	无

表格来源：作者整理。

自评估与安全评估相结合”的严格原则。《评估办法》第 9 条“与境外接收方约定数据安全保护责任义务”与两者要求大体一致，《标准合同规定》中的合同模板第三条“境外接收方的义务”就是在第 9 条的基础上展开的。《评估办法》第 4 条项下的四类情形作为审查对象，只有通过安全评估、获得“行政许可”才能有出境的资格，体现出监管部门对这四类情形安全评估十分审慎的态度。另外，《评估办法》第 14 条〔43〕和第 17 条〔44〕规定了数据出境安全评估的结果具备两年有效期及需要重新申报评估的情形，不符合要求则会被书面通知终止数据出境活动，体现了“事前评估和持续监督相结合”的原则。而对于《评估办法》第 4 条的四类情形之外的数据出境，由于没有达到安全评估的“门槛”则只需要按照《个人信息保护法》第 38 条第 2 或第 3 项得到专业机构个人信息保护认证或与境外接收方订立标准合同，即可进行数据出境。相较于数据出境安全评估的流程，标准合同这种出境路径更加快捷、可预期、成本低，虽然合同签署后需要在网信部门备案，但备案不作为合同生效条件和信息出境的前置条件；认证机制的适用为跨国公司或者同一经济、事业实体内部的个人信息跨境处理活动提供“绿色通道”。在《网络安全法》《数据安全法》《个人信息保护法》等法律作为上位法、《评估办法》等部门规章作为下位法的国内数据法律体系下，我国正在逐步建立“安全评估审查下的高风险数据有限流动、标准合同和认证机制下的低风险数据自由流动”的数据出境评估体系。

（二）缓解国内数据规则与 DEPA 之间的张力

如前文所述，我国对于《评估办法》第 4 条的四类高风险数据出境采取“无授权则不可为”的行政许可模式，对其他低风险数据采用标准合同和认证机制的处理模式，这些模式实质上都属于数据本地化范畴，即只有符合要求才能允许数据出境，否则只能在本地存储。数据本地化作为严格限制跨境数据流动的一种属地规制模式，“将地域性的传统主权观念照搬至全球性的现代数字经济，容易产生安全与发展之间方枘圆凿的冲突”〔45〕。《评估办法》等配套规则生效后，相关企业和个人发起的任何数据跨境传输活动都必须与境外数据接收方签署上述具有法律效力的文件，给接收方施加种种义务并进行一系列谈判，经济和时间成本可能会随之增加。统筹数字经济的发展和安全，体现在跨境数据流动中就是要在数据的高效流动和安全稳定之间寻找平衡点。数据出境评估体系也应当根据实践予以调整，在保障数据安全出境的前提下，减少不必要的行政程序，明确审查规则，提高数据跨境流动的效率。

中国已加入的《区域全面经济伙伴关系协定》（RCEP）在“电子商务”章明确了电子商务项

〔43〕《评估办法》第 14 条规定：“通过数据出境安全评估的结果有效期为 2 年，自评估结果出具之日起计算。在有效期内出现以下情形之一的，数据处理者应当重新申报评估：（一）向境外提供数据的目的、方式、范围、种类和境外接收方处理数据的用途、方式发生变化影响出境数据安全的，或者延长个人信息和重要数据境外保存期限的；（二）境外接收方所在国家或者地区数据安全保护政策法规和网络安全环境发生变化以及发生其他不可抗力情形、数据处理者或者境外接收方实际控制权发生变化、数据处理者与境外接收方法律文件变更等影响出境数据安全的；（三）出现影响出境数据安全的其他情形。有效期届满，需要继续开展数据出境活动的，数据处理者应当在有效期届满 60 个工作日前重新申报评估。”

〔44〕《评估办法》第 17 条规定：“国家网信部门发现已经通过评估的数据出境活动在实际处理过程中不再符合数据出境安全管理要求的，应当书面通知数据处理者终止数据出境活动。数据处理者需要继续开展数据出境活动的，应当按照要求整改，整改完成后重新申报评估。”

〔45〕 许多奇：《治理跨境数据流动的贸易规则体系构建》，载《行政法学研究》2022 年第 4 期，第 55 页。

下各成员方制定数据本地化和数据跨境流动政策的基本原则。在中国现有自由贸易协定中，RCEP 包含的电子商务条款数量最多，其电子商务章节条款内容进行了大幅扩充，一些数字贸易规则核心条款也首次包括进来，但与国际高标准规则相比仍存在不少差距。在跨境数据流动方面，RCEP 规定不强制要求计算设施本地化（第 14 条）、不得阻止通过电子方式跨境传输信息（第 15 条）等，这些条款的接受对我国来说也是一个巨大的进步，意味着我国逐步在数据安全和数据开放之间寻找平衡。相较于 RCEP 关于个人信息保护的“倡议性”规定（第 8 条），DEPA 第 4.2 条从个人信息保护法律框架关键原则的细化、非歧视性原则及信息保护公开、个人信息保护机制之间的兼容性和互操作性、数据保护信任标志等方面为个人信息数据保护提出了具体的要求。DEPA 第 4.3.2 条明确规定通过电子方式传输的信息包括个人信息，即自然人的任何信息（包括数据）都是可跨境传输的，但 RCEP 第 15 条并没有对电子传输信息是否包含个人信息作出明确界定。〔46〕 此外，RCEP 第 14 条和 DEPA 第 4.4 条及第 15.2 条（安全例外条款）都认同数据存储非强制本地化及安全例外，这事实上对目前我国国内法就数据“境内存储为原则、安全评估后出境为例外”的总基调仍存在一定的背离。

虽然中国未在跨境数据流动议题上提出具体的规则方案，且目前国内法以数据本地化存储为原则，但从中国近期申请加入 CPTPP、DEPA 来看，中国已经逐渐向数据自由流动和开放的趋势转变。欧盟 GDPR 对个人数据向第三国或国际组织传输仅限于四种方式，这给跨国公司施加了很大的个人隐私保护义务和合规成本。〔47〕 中国基于数字经济和贸易发展考虑，在未来的选择中未必会完全接受欧盟在隐私保护方面的严格要求。〔48〕 我国目前不仅在跨境数据流动的部分法律法规中存在规则模糊等问题，而且个人信息和部分商业场景的重要数据出境评估规定缺乏灵活性，数据的分级和分类管理目前并没有成熟的制度安排。这些问题势必会影响中国参与经济全球化、拓展全球数字服务市场的进程。

从国际贸易规则的角度来看，“一般例外”条款可以作为平衡数字主权和数据自由流动的有力工具。DEPA 将 GATS 第 14 条纳入一般例外情况，即授权成员国为了满足合法公共政策目标或保障基本安全利益而采取不符合规定的措施。〔49〕 这样来看，根据 DEPA“美式规则”特点，成员国在原则上应当鼓励数据的跨境自由流动，但这种自由并非绝对，其受到例外条款对安全、隐私等方面的限制。这考虑到更多缔约方的自身诉求，给予缔约方更大的数据流动管制空间，〔50〕 为我国数据出境评估体系与 DEPA 的“接合”性提供了解释的依据。问题在于，如何对第 14 条（c）（iii）项下的“安全”进行解释。〔51〕 这涉及何种安全利益可以纳入 GATS 例外条款中。尤其是近年来，

〔46〕 参见周念利、于美月：《中国应如何对接 DEPA——基于 DEPA 与 RCEP 对比的视角》，载《理论学刊》2022 年第 2 期。

〔47〕 这四种被允许的数据跨境传输方式分别是：数据控制者和处理者基于充分性决定、提供适当保障措施、建立有约束力的公司规则、特殊情况下的例外。参见戴龙：《论数字贸易背景下的个人隐私权保护》，载《当代法学》2020 年第 1 期。

〔48〕 参见前引〔47〕，戴龙文。

〔49〕 See DEPA Article 15.1&15.2.

〔50〕 参见前引〔26〕，陈寰琦、陆锐盈文。

〔51〕 参见田翔宇：《我国跨境数据流动监管体系的国际法分析——以 GATS“一般例外”条款为视角》，载《人民法治》2018 年第 24 期。

国家安全范畴从传统安全扩展到非传统安全，如何构成威胁国家安全的条件几乎完全由一个主权国家自己决定。国家安全审查制度等国内法上的规则和制度不断外溢，成为一种国际通行的做法和监管工具，国家安全呈现概念泛化且考量因素模糊等特点。在此背景下，以“特朗普政府打压 TikTok”为代表的、以维护国家安全为由限制跨境数字交易、投资和数据访问的事件频频出现，削弱了国际规则体系，侵蚀了全球化发展的法律基础、国际机制和法治逻辑。〔52〕DEPA 目前也没有对这些措施的合理限制作出更为具体的国家安全例外规定。中国可以申请加入 DEPA 为契机，与其他成员国探讨例外条款在数据流动方面的包容性，探寻以维护数据主权为前提的数据流动和数据安全之间的最佳平衡点。

近年来中国的崛起已对美国引领的西方主导地位带来潜在挑战，视中国为“战略竞争对手”已成为美国两党的战略共识，中美在数字领域的竞争将会更加激烈。美国主导构建的“印度—太平洋经济框架”（The Indo-Pacific Economic Framework，IPEF）包含建立一个新的数字治理框架以管理印太地区的数字经济和跨境数据流动。〔53〕目前参与 IPEF 框架的 13 个初始国家包括了韩国、新西兰以及文莱、印度尼西亚、马来西亚、菲律宾、新加坡、泰国、越南七个东盟国家。结合数字经济协定签署的集中地、数字税等数字规则的覆盖地以及后疫情时代经济复苏的进展与规模看，印太地区是全球数字博弈的重点区域。〔54〕中国处于印太地区数字供应链的中心，美国印太战略的构建和实施可以视为对中国“数字丝绸之路”和“一带一路”的制衡，以削弱中国在印太地区日益增长的影响力。在此背景下，构建符合中国国情、与世界接轨的跨境数据流动体系就尤为重要和紧迫。中国申请加入 DEPA，体现了我国对数字经济国际合作的高度兴趣与构建全球数字经济框架的最新努力。DEPA 为不同国家之间的企业合作提供了技术和规则交流的有利平台，中国应当借助申请加入 DEPA 的契机，积极参与全球数字产业链供应链治理，探索数据驱动创新体系和安全发展模式，在维护我国网络安全的基础上稳健地开放数字市场，引领全球产业链的发展和数字贸易规则的构建。

四、结　语

随着数字经济的迅速发展，数据已成为未来改变全球竞争格局、重塑全球经济结构、重组全球要素的重要资源。越来越多的国家将数字治理和跨境数据流动规则作为其双边和区域贸易协定的要素和章节。中国申请加入 DEPA，意味着中国继加入 RCEP 后，进一步接受 DEPA 更高水平的数字治理理念和规则，将与 DEPA 缔约国共同参与全球数字治理，并展开进一步的合作和交流。这既是中国参与全球数字治理的一次机遇，又在对标国内规则、平衡数据安全和开放流动难题、中美战略竞争等诸多方面面临挑战。虽然我国正在逐步构建数据出境评估体系，但从主要内容上来看仍然与 DEPA 等高水平数字经济规则存在一定的张力。中国应当综合评估 DEPA 的协

〔52〕 参见沈伟：《驯服全球化的药方是否适合逆全球化?》，载《人民论坛·学术前沿》2020 年第 12 期。

〔53〕 See the White House website，FACT SHEET：Indo-Pacific Strategy of the United States，available at https://www.whitehouse.gov/wp-content/uploads/2022/02/U.S.-Indo-Pacific-Strategy.pdf，last visited on Feb. 12，2022.

〔54〕 参见翟崑：《数字全球化的战略博弈态势及中国应对》，载《人民论坛》2021 年第 17 期。

定内容，结合目前国内数字经济发展状况，有选择地参加 DEPA 并提出数据治理的“中国方案”，与其他国家在尊重主权的基础上共同构建全球数字治理新格局。

Abstract：With the development of digital technology，data has become a fundamental and strategic resource for most of the countries. The competition for data resources among countries has become increasingly intense. The issues such as cross-border data flow have become the focus of international attention. Since data has the attributes of both property and personality interests，there are differences in the philosophy of data governance among countries. At present，the global data governance framework has not yet been formed. The Digital Economy Partnership Agreement (DEPA) is the first special agreement for the digital economy in the world. In terms of data issues，it mainly draws on American digital rules and adopts a flexible modular framework. It also reflects the demands of small and medium-sized countries such as Singapore in terms of digital governance. Compared with traditional comprehensive trade agreements，it is more contemporary，flexible and extensible. From the perspective of the data exit assessment system being constructed in China，there is a tension between China's domestic digital rules and high-level international digital rules such as DEPA. China's application to join DEPA is conducive to promoting the development of its own digital economy and international cooperation，improving the level of data governance，and further expanding China's voice in global data governance.

Key Words：DEPA，digital economy，global data governance

（责任编辑：肖　芳　赵建蕊）

财经法学 No. 6，2022
pp. 81 - 95

限制数据抓取行为的违法性认定
——以美国干扰侵权理论为视角

高建成*

内容提要：面对限制数据抓取行为的违法性认定难题，美国判例实践运用干扰侵权理论予以应对，通过行为对合同关系的损害结果征引行为的违法性。在干扰侵权理论的分析模式下，原告应就行为人对合同或预期合同关系的知悉、故意实施干扰行为、导致合同或预期合同关系中断、产生实质损害结果举证，被告需以正当理由进行抗辩，而法院以此为基础进行利益衡量。该理论及判例实践对我国司法实践具有借鉴意义：第一，可将合同及预期合同作为反不正当竞争法所保护的法益，避免在数据、产品服务上创造新的权益，实现司法审慎。第二，个案裁判中应关注客观层面的实质损害证明，并且着重考察行为人的主观意图，综合行为人对已存在的合同的认知情况、行为所涉的数据类型、双方商业模式、协商过程等证据，并结合正当性抗辩进行判断。当行为人限制他人的数据抓取旨在实现纯粹侵害他人的恶意而非为正当利益时，宜认定为不正当竞争行为。

关键词：限制数据抓取　不正当竞争　干扰侵权　合法商业目的

一、问题的提出

数字经济时代下，数据因其重要经济价值成为市场主体争相夺取的生产要素及资源。数据争夺过程亦引发诸多竞争纠纷以及裁判难题，而限制数据抓取行为的定性则是其中一项。对于不具备明显优势地位的经营者所实施的限制数据抓取行为，其法律属性的认定主要依据《反不正当竞争法》第 2 条，以及第 12 条第 2 款第 4 项。

* 高建成，南京大学法学院博士研究生。
本文为 2019 年国家社科基金一般项目“共享经济法律规制的司法路径研究”（19CFX065）的阶段性成果。

然而，受限于条款本身的高度抽象性及分析框架的模糊性，《反不正当竞争法》难以为司法裁判提供足够明确及统一的认定标准。在“字节跳动公司诉微梦创科公司不正当竞争纠纷案”中，字节跳动公司认为微梦创科公司设置 robots 协议黑名单导致其无法正常抓取数据，构成不正当竞争。一审法院围绕损害、商业道德进行论证，认为涉案限制数据抓取行为具有针对性，影响了原告产品的正常运行以及用户的使用，且与互联网行业促进信息流动的基本价值不符，因此判定构成不正当竞争。〔1〕二审法院否定一审法院对商业道德以及损害的认定，认为被诉行为应属于企业自主经营权范畴内的正当行为。〔2〕由此可以看出限制数据抓取行为中衡量双方利益冲突的复杂性。一方面，限制数据抓取是经营者自主经营之结果，而这种自主决策又是实现竞争机制的重要基础；另一方面，这种基于数据控制的排他行为也可能对竞争对手的经营活动产生干扰，甚至成为排除、限制竞争的工具，进而扰乱市场秩序。

同为限制数据抓取行为的纠纷，美国 hiQ 诉 linkedIn 案的判例经验或能提供参考。LinkedIn 是一家拥有 5 亿用户的职业社交网络服务公司，其用户在 LinkedIn 平台上发布简历和工作列表等信息，以此与其他会员建立商务联系。而 hiQ 是一家数据分析公司，其长期依靠抓取 LinkedIn 用户在 LinkedIn 平台上公开的个人资料信息进行人员分析预测产品的开发，并将产品出售给客户。2017 年 5 月，Linkedin 向 hiQ 发出通知，并采取技术手段限制 hiQ 访问和复制来自 LinkedIn 服务器的数据。hiQ 公司指控 LinkedIn 所实施的限制数据抓取行为构成对现有合同以及对预期经济关系的干扰，由此提出干扰侵权索赔。

美国反不正当竞争法并无明确定义与边界，泛指调整市场中竞争者之间关系的法律规则，其相关法律规范散见于联邦及各州制定法、判例法之中，并与知识产权法、侵权法、反托拉斯法存在交叠。〔3〕干扰侵权（the interference torts）被视作一种独立的侵权行为类型，并用于处理商业关系。美国从上百年的判例实践中发展出干扰侵权理论，并应用于限制数据抓取纠纷之中，其司法实践经验及理论积累对我国或有助益。因此，本文将以干扰侵权理论为视角，展示美国判例实践如何运用干扰侵权理论对限制数据抓取行为进行定性，总结判例经验及可行的制度智慧，为我国限制数据抓取行为的违法性认定提供参考。

二、干扰侵权理论的功能与违法性征引

对于数字经济时代下的竞争，行业内通常未形成长期稳定的商业惯例，因而司法机关有时难以通过行业秩序与商业道德判断竞争行为的违法性。此时可以通过国内外既有理论的挖掘与阐释，寻找行为定性的可能路径。而干扰侵权理论则是其中一种可能，其将合同关系视作财产利益，要求他人予以一定程度的注意与尊重，当行为人故意干扰时，比如明知他人存在合同关系而以技术手段限制他人抓取数据以影响交易，则可能征引其违法性。

〔1〕 参见北京知识产权法院（2017）京 73 民初 2020 号民事判决书。
〔2〕 参见北京市高级人民法院（2021）京民终 281 号民事判决书。
〔3〕 参见〔德〕博德维希：《全球反不正当竞争法指引》，黄武双等译，法律出版社 2015 年版，第 768－769 页。

（一）干扰侵权理论的起源与发展

干扰侵权理论认为，没有正当理由干涉他人与第三方之间经济关系的任何人，应当承担赔偿责任，其中经济关系既包括合同关系，也包括预期合同。干扰侵权理论具有深厚的历史渊源，最早可追溯至罗马法时期，〔4〕但其最直接的近代渊源应是19世纪中期的英国普通法实践，即1853年英国的Lumley诉Gye诱导违约案。〔5〕该案中，歌剧歌手Wagner与原告约定在原告剧院进行一定期限的演唱，并且在该期限内不得在其他地方演唱。而被告Gye在知悉两人合同的情况下，以更高费用诱导Wagenr违约并与自己缔约。〔6〕在该案中，王座法庭（Queen's Bench）认为，满足以下要件则可构成侵权：（1）被告的行为出于恶意；（2）原告与被诱使违约人之间存在有效且具有约束力的合同；（3）本合同为在特定期限内提供独家个人服务的合同。〔7〕该规则被称为“Lumley规则”，为后来的干涉合同案例所广泛采用。〔8〕随着长期判例实践的经验积累，干扰侵权理论不断得到发展，适用范畴拓宽至几乎所有类型的合同，甚至可以适用于预期合同关系。由此，该理论在发展过程中形成了干扰合同与干扰预期合同两种责任认定路径。

在美国多个司法辖区内，干扰合同以及干扰预期合同均构成侵权行为。对于干扰合同行为，《美国侵权法第二次重述》第766条规定，故意、不当干扰他人与第三人履行合同（婚姻合同除外），引诱或者以其他方式致使第三人不履行合同的，应当对第三人不履行合同给对方造成的经济损失承担赔偿责任。〔9〕而对于干扰预期合同行为，《美国侵权法第二次重述》第766B条规定了故意干扰预期合同关系行为，这是指一方故意和不正当干涉另一方未来的合同关系（婚姻关系除外），包括诱导或以其他方式导致第三人未建立或继续未来的关系，或阻止对方获得或继续未来的关系。〔10〕这两类干扰侵权规则，旨在保护原告的合同履行利益及合同不受第三人侵犯的利益，将这种合同所代表的承诺利益上升为一种财产利益进行保护。〔11〕而在部分司法辖区比如加利福尼亚州，干扰侵权通常与不公平竞争法具有交叠关系，即当行为被认定构成干扰侵权时，同时也将获得不公平竞争行为的违法性评价。

（二）理论的价值功能：维护市场竞争与交易秩序

干扰侵权理论的功能与价值目标在于维护稳定的交易秩序。干扰侵权理论起初的价值理念在于保护合同稳定性。合同稳定性具有重要的社会意义，体现为两方面：一是社会中大量不特定原告期望其所享有的承诺利益能够实现，这不限于个别原告的经济预期，更在于对承诺利益的保护有助于创造并确保额外的财产价值，从而进一步促进社会福利；二是合同稳定性有助于商业领域

〔4〕 See Francis Bowes Sayre, Inducing Breach of Contract, 36 *Harvard Law Review* 663, 663 (1923).

〔5〕 See Harvard Law Review Association, Tortious Interference with Contractual Relations in the Nineteenth Century: The Transformation of Property, Contract, and Tort, 93 *Harvard Law Review* 1510, 1522 (1980).

〔6〕 See Lumley v. Gye (1853) 2 El. & Bl. 216. 118 Eng. Rep. 749 (Q. B. 1853).

〔7〕 参见前引〔4〕，Francis Bowes Sayre文，第669页。

〔8〕 See Harvey S. Perlman, Interference with Contract and Other Economic Expectancies: A Clash of Tort and Contract Doctrine, 49 *University of Chicago Law Review* 61, 64 (1982).

〔9〕 See Restatement 2d of Torts § 766 (1979).

〔10〕 该行为在美国各州存在不同称呼，比如预期经济优势、预期经济利益，但含义均指向未订立的合同。See Restatement 2d of Torts § 766B (1979).

〔11〕 参见前引〔5〕，Harvard Law Review Association文，第1529页.

的秩序构建以及价值实现，并能有效降低社会成本。稳定的合同关系是市场经济的重要基础，市场参与者基于合同关系可以规划未来商业活动、优化经营以及协调与其他交易相对人的关系。〔12〕而随着对自由竞争价值的重视，干扰侵权理论逐渐分化为干扰合同理论以及干扰预期经济关系理论，以承担不同的功能，前者实现民事主体之间（包括经营者之间）交易安全的保障，后者调整竞争秩序，避免对竞争的不当干预。但两者在维护健康稳定的市场交易秩序的目标上体现出共同的取向。

美国将干扰侵权理论作为一项商事侵权规则来调整市场竞争者之间的关系，与我国反不正当竞争法的目的与效果具有同一性。〔13〕换言之，美国的商事侵权规则实际上以衡平法的方式发挥着规制不正当竞争行为的作用，而从目的来看，美国商事侵权规则与我国反不正当竞争法具有共同的价值追求，即识别并遏制市场内的不正当竞争行为，避免竞争者之间降低底线展开“逐底竞争”，从而维护健康良好的市场秩序。既然限制数据抓取行为存在扰乱市场秩序之可能，就需要借助法律制度以及理论工具来解决限制数据抓取行为的法律定性问题，进而维护市场竞争秩序。

（三）干扰侵权理论下限制数据抓取行为的违法性征引

经营者基于自身的商业利益以及数据安全的考量而对自身数据采取措施，限制他人抓取，体现出防御性以及被动性。这种行为本身属于自主决策范畴，不能够当然征引违法性。加之限制数据抓取手段本身难言违背商业道德以及社会认知，因而反不正当竞争法及相关法律并不会直接将其类型化为一种违法行为。

限制数据抓取行为是否会导致一方竞争优势的削弱，已有的案例给予了回答。随着数据要素的商业价值显现，掌握数据或者数据外泄均引发市场内不同经营者竞争优势的变化。数据如未得到保护与有效控制，对于控制数据一方的经营者而言可能意味着运营、财产安全受影响，经济利益遭损以及相关法律施加的义务无法实现。但对于需求数据而实施抓取行为一方而言，其由于前者的限制行为而无法获得数据，可能将难以继续其商业模式，同样存在损失经济利益的可能。

因此，在无法直接征引行为违法性的情形之下，通过干扰侵权理论对限制数据抓取行为进行评判是可行之举。首先，干扰侵权行为是一种侵权行为，因对他人合法权益具有侵害性而被赋予法律上的负面评价。也正是由于行为的侵害性，美国部分州将其视作一种不公平竞争行为。比如在加利福尼亚州，任何非法、不公平或欺诈性商业活动或行为均属于不公平竞争法所禁止的行为，而干扰侵权则属于其中的非法行为。其次，干扰侵权理论以合同所代表的承诺利益以及经济利益的归属为侵害内容，将合同视作财产利益进行保护，因而这种利益也获得要求他人不得侵害以及可寻求救济的排他功能。通常而言，无损害则无救济。在干扰侵权理论中，经济利益受到第三人侵犯是寻求救济的基础，由此引发对行为违法性的认定问题。而限制数据抓取行为本身非法律所禁止的类型化行为，其既可能是经营者自主经营的外在表现，也可能成为经营者故意破坏他人合同关系的手段及工具。而当他人合同关系或者利益归属受到侵犯时，则可以该损害结果为始点，考察限制数据抓取行为与损害结果之间的因果关系，并结合经营者的主观状态与客观证据进

〔12〕 See John Danforth, Tortious Interference with Contract: a Restatement of Society's Interest in Commercial Stability and Contractual Integrity, 81 *Columbia Law Review* 1491, 1515 (1981).

〔13〕 参见李扬、蓝小燕：《竞争法视点下的引诱违约行为研究》，载《私法》2020 年第 2 期。

行违法性分析。当限制数据抓取并非旨在促进自身经济利益或合法利益，而是为实现破坏他人经营、削弱他人竞争优势之目的时，则行为具备道德及法律上的可谴责性，由此征引行为的违法性。

三、干扰侵权的构成要件与分析模式

关于干扰侵权的构成，美国不同司法辖区对证明对象的要求不完全一致，一般包括对合同或预期合同关系的知悉、干扰行为、主观状态、损害结果。以加利福尼亚州为例，原告需就干扰合同的诉因证明以下要件：第一，原告与第三方之间存在有效的合同；第二，被告知悉该合同；第三，被告故意实施诱导违反或干扰合同关系的行为；第四，合同关系的实际违反或中断；第五，导致损害。〔14〕而针对干扰预期合同行为的证明要求与其类似，但原告还需要证明干扰手段本身违反既有相关法律规范，即具备独立的不法性。〔15〕

（一）干扰侵权的证明对象

具体而言，干扰侵权的证明对象包括：第一，原告具有合法有效的合同或者潜在的商业关系，这类关系所衍生的合同利益与预期合同利益是干扰侵权理论所保护的对象。原告应当证明合同关系是合法且存续的，比如数据分析公司开发特定数据产品服务并出售，则其与客户公司之间的买卖合同可获得保护，进而排除他人恶意干扰。如果受干扰的合同违法或者违反公共政策，则不受法律保护。比如，合同系垄断协议或侵犯他人商业秘密，则因违反法律、公共政策而无法构成干扰侵权理论的保护基础。〔16〕

第二，干扰侵权要求行为人的主观状态是故意，即行为人的主要意图在于促进干扰结果的发生。因而原告需要证明行为人知悉合同的存在，以及行为人在知悉合同以及干扰后果的前提下仍然故意干扰合同的履行。确定行为人意图与动机对于认定干扰行为是否非法具有重要意义。如果干扰是行为人的唯一或主要目的，则几乎可据此认定干扰行为不正当。因为对社会而言，纯粹侵害他人的行为与动机毫无助益，甚至可能有碍于社会的发展。然而，在干扰并非行为人所期望而纯属偶然而导致的情形之下，则需要结合干扰手段对行为进行评判。〔17〕美国部分司法辖区的判例实践也存在要求原告证明行为人存在“恶意”的做法，认为主观上的恶意是承担责任的必要条件。从其裁判过程来看，行为人的恶意通常等同于行为“缺乏正当性”。〔18〕

第三，被告实施了干扰行为，且该干扰行为导致了损害结果。原告需要证明行为、损害结果以及两者之间的因果关系。首先，此处所要求的行为要件是指行为人客观上实施了行为本身，暂不涉及行为本身的价值评判。其次，对于损害结果要件，可以表现为现有合同关系的中断以及交易机会的丧失等，分别对应干扰合同行为以及干扰预期合同行为。而企业退出市场也可满足损害

〔14〕 See hiQ Labs，Inc. v. LinkedIn Corporation，938 F. 3d 985，996（2019）.

〔15〕 See Facebook，Inc. v. BrandTotal Ltd.，499 F. Supp. 3d 720，742（2020）.

〔16〕 See Restatement 2d of Torts § 774（1979）.

〔17〕 See Restatement 2d of Torts § 767（1979）.

〔18〕 See Nitzberg v. Zalesky，370 So. 2d 389，391（1979）；Monarch Indus. Towel and Uniform Rental，Inc. v. Model Coverall Service，Inc.，178 Ind. App. 235，236（1978）.

结果要件，并在程度上更为严重。此外，因果关系亦是不可缺失的一环，原告需证明损害结果是由被告行为直接导致，将责任主体明确指向行为人。

第四，干扰手段非法性的证明问题。一般而言，对于干扰合同的主张，原告无需证明干扰行为的手段具有非法性，而对行为要件的证明止步于事实层面。但手段上的独立非法性证明对于干扰预期合同行为而言通常是必要的。独立不法性意味着手段本身构成独立的侵权行为或违反现有的宪法、刑法、反托拉斯法等法律，其将直接影响法院的利益衡量结论。如果干扰手段本身包含侵权行为，例如诽谤、致害诋毁、欺诈、暴力或威胁，那么无论是干预合同还是预期合同，行为均无正当性可言；干扰方式构成限制贸易的共谋或行动等反托拉斯行为，或者，根据辖区内的法律构成违法，如干扰手段构成加利福尼亚州不公平竞争法所禁止的任何非法、不公平或欺诈性的商业行为，同样满足独立不法性的要求。〔19〕

（二）干扰侵权的正当性抗辩及利益衡量

在市场经济之下，自由竞争所带来的损害具有相对性与必然性，合理的竞争行为不应得到法律的否定性评价，否则将威慑市场竞争，并且提高交易成本。〔20〕因而，在程序上赋予被告抗辩的机会有助于法院的综合考虑，避免错误干涉竞争。面对原告的干扰侵权主张，被告可以就其行为的正当性进行积极抗辩，证明自身行为以及所追求利益的合理性。比如证明自身行为是为了实现合法的商业目的而非基于破坏其他经营者的竞争优势之目的；又如干涉合同是基于传染病防控，保护健康、安全或者良好道德的目的；〔21〕再如，合同的执行不利于劳动者合法权利保障〔22〕。若抗辩成立，被告没有采取不正当或违法手段进行干扰，则无需承担侵权责任。

而对于干扰预期合同而言，被告享有更为广泛的正当抗辩事由，可以主张竞争特权抗辩。换言之，如果原告没有成功订立合同，则被告可以在没有采取非法手段的前提之下，以正当竞争为由从原告处争取交易机会。其中主要的考虑在于，第一，预期合同作为一种预期的、潜在的利益，与已缔约的合同利益所代表的稳定期待有所不同，其保护力度应弱于合同。第二，对干扰预期合同的认定标准过低，将严重打击市场竞争，损害市场预期并增加市场交易成本，进而违背市场经济的初衷。竞争通常被认为能够有效地进行资源分配，并以最低成本维护谈判环境。〔23〕“在以自由竞争原则为基础的经济体制中，竞争者不应因寻求合法商业优势而承担侵权责任。”〔24〕而要求原告证明行为不法性的规则，有助于减少经营者的诉讼风险，降低无合同环境下的竞争成本与交易成本。〔25〕

随后，在被告对干涉合同的正当理由举证后，由法院进行利益衡量。关于干扰侵权理论中的

〔19〕 See Cal. Bus. & Prof. Code § 17200.

〔20〕 See Gary Myers, The Differing Treatment of Efficiency and Competition in Antitrust and Tortious Interference Law, 77 *Minnesota Law Review* 1097, 1140 - 1141 (1992).

〔21〕 See Harvard Law Review Association, Inducing Breach of Contract-Justification-Effect of Motive, 38 *Harvard Law Review* 115, 115 - 116 (1924).

〔22〕 See Hitchman Coal and Coke Co. v. Mitchell, 38 S. Ct. 65 (1917).

〔23〕 参见前引〔8〕，Harvey S. Perlman 文，第 83 - 84 页。

〔24〕 前引〔20〕，Gary Myers 文，第 1122 页。

〔25〕 See Jesse Max Creed, Integrating Preliminary Agreements into the Interference Torts, 110 *Columbia Law Review* 1253, 1267 - 1268 (2010).

价值位阶，一般认为，公共利益优先于私人利益，生命健康利益优先于财产利益。法院的利益衡量将以合同的稳定性所代表的利益作为判断基准，进而根据价值位阶进行衡量，判断干涉行为所保护的利益是否超过合同的稳定性所代表的利益。〔26〕在已有合同的情形下，合同利益的位阶优先于竞争自由利益，被告如果以竞争特权作为抗辩事由，则无法得到支持。

四、干扰侵权理论下限制数据抓取行为的判例实践

干扰侵权理论为认定限制数据抓取行为的法律属性及行为人的责任提供了初步思路与分析框架，强调了对干扰意图的考证。如果干扰旨在改善自身业务等合法目的，而非破坏他人商业关系，通常不被认为违背商业道德或违反侵权法。并且，干扰侵权制度与禁令救济常常密不可分。作为干扰侵权的重要救济方式，禁令的申请在损害严重程度、利益衡量方面有更严要求。从干扰侵权制度的构造来看，法院谨慎地介入竞争关系的规制。但这并不影响经营者以该制度作为商业竞争中的维权武器。在认识该制度的基本构造之后，可通过限制数据抓取纠纷的判例实践考察理论的具体应用。

（一）hiQ 诉 LinkedIn 案

在 hiQ 诉 LinkedIn 案中，hiQ 指控 LinkedIn 限制数据抓取的行为构成干扰侵权并申请临时禁令。第九巡回法院在利益衡量的过程中，充分考虑 LinkedIn 的动机以及手段正当性问题，进而支持了 hiQ 的干扰侵权索赔，并保护了 hiQ 公司与其客户之间的合同关系。

该案中 hiQ 提出干扰侵权索赔并充分证明了干扰侵权行为的要件，即行为人在清楚认识到他人存在商业关系的情况下仍然实施干扰。首先，LinkedIn 知悉 hiQ 的商业模式以及其可能存在的商业关系，因 LinkedIn 曾派代表参加 hiQ 展现商业模式与产品的会议以及商演现场，清楚认识到 hiQ 依靠 LinkedIn 的公开数据进行分析研发的情况。其次，LinkedIn 以法律责任威胁 hiQ，并实际采取技术措施以限制 hiQ 对数据的访问，由此满足干扰侵权的故意实施行为的要件。再次，hiQ 与第三方之间的合同关系已经中断，因其无法访问 LinkedIn 的数据而无法按照承诺向现有客户提供服务。最后，hiQ 因现有合同中断和对预期合同的干扰而受到损害，即丧失产品销售收入，而且很可能导致倒闭。〔27〕

LinkedIn 则以合法的商业目的进行抗辩，认为限制数据抓取行为是为了保护用户隐私以及自己的投资利益。第九巡回法院认为，第一，LinkedIn 阻止 hiQ 访问 LinkedIn 服务器上的数据的行为不是一种公认的正当贸易行为。一方面，从 LinkedIn 的行为表现来看，涉案数据本是公开数据，而 LinkedIn 阻止 hiQ 访问、抓取数据具有针对性以及选择性，不符合广告、降价等公认的商业惯例。另一方面，从 LinkedIn 的行为结果来看，其限制行为将根本地、直接地破坏竞争对手的基本商业模式。第二，法院认为，LinkedIn 仅针对作为潜在竞争对手的 hiQ 实施限制，很可能是为了促进 LinkedIn 自身在数据分析工具领域的竞争优势，并将竞争对手逐出数据分析市

〔26〕 See Imperial Ice Co. v. Rossier，18 Cal. 2d 33，36（1941）.

〔27〕 See hiQ Labs，Inc. v. LinkedIn Corporation，938 F. 3d 985，996（2019）.

场，因此该行为可能不在“公平竞争范围内”，很可能违反加利福尼亚州不公平竞争法而构成违法垄断。[28]

（二）Facebook 诉 BrandTotal 案

在另一起限制数据抓取纠纷中，法院起初没有支持干扰侵权索赔。2020 年 9 月，Facebook 公司关闭 BrandTotal 公司在 Facebook 有关网站的账户，并采取技术措施，阻止 BrandTotal 对 Facebook 数据的访问与抓取。10 月，Facebook 向加利福尼亚州法院起诉 BrandTotal，而 BrandTotal 则提起反诉，认为 Facebook 的限制数据抓取行为构成干扰侵权以及不公平竞争，导致其与客户的合同破裂，并申请临时限制令。[29]

在干扰侵权索赔的辩驳中，Facebook 声称限制数据抓取是为了实现合法的商业利益，即通过阻止 BrandTotal 的访问遵守法律施予的义务，因而申请驳回 BrandTotal 的反诉。而其中的法律义务，源自美国联邦贸易委员会（FTC）的执法行动命令，FTC 要求 Facebook 采取措施以防止第三方违反隐私设置以及用户条款进行数据抓取。[30] 双方均不质疑遵守法律要求可以作为干扰侵权的抗辩理由。此外，法院基于 BrandTotal 的行为表现，倾向于认可 Facebook 公司的合法商业理由：一方面，Facebook 本身已建立了共享数据的渠道，比如 API 方式，而 BrandTotal 没有事先与 Facebook 就获取数据的有关事项进行沟通，因而难以判断 Facebook 的意图；另一方面，Facebook 认为 BrandTotal 有以不当方式收集用户数据的历史，有可能威胁用户隐私安全。[31] 因此，BrandTotal 在初次提出的反诉中未能成功证明干扰侵权，其主张未得到法院认可。

由于干扰手段的合法性问题同样会影响法院的利益衡量结果，BrandTotal 起初试图通过援引 hiQ 案以证明 Facebook 行为构成垄断。BrandToatl 认为 Facebook 限制抓取的数据包括公开数据，其情形与 hiQ 案相同，均违反加利福尼亚州不公平竞争法并构成垄断。而法院根据 Facebook 限制抓取的不同数据展开类型化讨论：第一，针对公开数据，比如 Facebook 为用户生成的广告偏好以及特定广告参与度的有关分析数据，通常不涉及知识产权以及用户隐私，而 Facebook 限制此类数据的抓取，则可能存在与 hiQ 案中类似的垄断公共信息之风险，可能构成不公平竞争行为或者非法垄断。[32] 但法院补充道，具体还需要结合 BrandTotal 与 Facebook 的协商过程等证据对 Facebook 的真实动机进行考察。第二，针对非公开数据，这类数据通常受密码保护，且承载用户隐私内容，因此 Facebook 对此进行保护与监管是合理且合法的。Facebook 上的用户可以选择与特定对象共享信息，且基于 Facebook 的隐私设置以及用户条款而存在合理的隐私期待，以免受于第三方的数据抓取。[33] 因此，Facebook 存在执行自身合同方面的利益，这种利益同样受法律保护。在此情况下，法院认为判断 Facebook 是否担责的关键就在于行为是否

〔28〕 See hiQ Labs，Inc. v. LinkedIn Corporation，938 F. 3d 985，998（2019）.
〔29〕 See Facebook，Inc. v. BrandTotal Ltd.，499 F. Supp. 3d 720（2020）.
〔30〕 See Facebook，Inc. v. BrandTotal Ltd.，499 F. Supp. 3d 720，739（2020）.
〔31〕 See Facebook，Inc. v. BrandTotal Ltd.，499 F. Supp. 3d 720，742（2020）.
〔32〕 See Facebook，Inc. v. BrandTotal Ltd.，499 F. Supp. 3d 720，739（2020）.
〔33〕 See Facebook，Inc. v. BrandTotal Ltd.，499 F. Supp. 3d 720，740（2020）.

出于善意。[34] 但由于 BrandTotal 在干扰侵权问题上没能证明 Facebook 的恶意，法院经利益衡量后更倾向于支持 Facebook 的正当理由抗辩，认为 Facebook 在监管平台整体的安全方面存在较强的商业利益。鉴于 BrandTotal 就案件的实质问题提出了严重质疑，法院允许 BrandTotal 后续修正干扰侵权、不公平竞争等相关反诉。

在 2021 年 6 月，BrandTotal 经再次修正反诉后，成功证明 Facebook 的干扰恶意，致使其干扰侵权索赔得到法院支持。转折点在于，BrandTotal 声称并举证 Facebook 以欺诈以及误导性陈述的手段促使 Google 从其应用商店中下架 BrandTotal 的产品。Facebook 曾于 2019 年对 BrandTotal 的产品进行调查，调查结果表明其产品无害。Facebook 在当时并未采取任何行动，直到 2020 年，在 Facebook 收到广告客户对 BrandTotal 能力的询问后几天，随即要求 Google 对 BrandTotal 进行处理。BrandTotal 举证，Facebook 在与 Google 交涉时未如实披露相关信息，并虚构 BrandTotal 的不当行为。而 Facebook 未能对该恶意证据进行解释，因而其合法商业目的抗辩最终被驳回。[35]

五、基于限制数据抓取纠纷裁判的因素归纳

在自由竞争的市场经济背景下，竞争行为表现出复杂的利益冲突以及交易机会的此消彼长，仅具有干扰外观并不当然意味着具有不正当性。纯粹破坏他人经济关系的恶意行为才需要给予负面法律评价，而干扰侵权理论之适用则有助于对其形成约束。干扰侵权的构成要件以及举证责任分配难度不大，难点在于对具体要件的进一步考量以及利益衡量过程的把握。从前述判例实践的焦点来看，欲以干扰侵权理论认定行为违法，应着重考虑干扰行为所致的损害、干扰行为人的主观状态以及正当理由抗辩。这些因素的考虑都旨在辨识干扰人的主观目的是否为损害、破坏他人的经济关系。

（一）实际损害之程度

对于限制数据抓取行为而言，禁令救济是较为重要的救济方式。在衡平法上以干扰侵权为诉因申请禁令，无论是申请临时禁令还是永久禁令，都应当以实质损害的发生为基础，并且应满足特定程度的要求，即造成无法弥补的损害。无法弥补的损害不能仅是单纯的金钱损失，从限制数据抓取的判例实践来看，法院所认可的无法弥补的损害包括大部分业务的中断、潜在客户或商业损失、退出市场的风险等，需要通过原告对损害的举证予以支撑与说明。比如 hiQ 诉 LinkedIn 案中 hiQ 声称的可能面临的倒闭风险，[36] 以及 Facebook 诉 BrandTotal 案中 BrandTodtal 所举证的潜在商业客户以及商誉的损失等无形损害 [37]。

一般而言，市场竞争下交易机会的流失是经营者所面临的正常现象，因而无形损害若要寻求

〔34〕 See Facebook，Inc. v. BrandTotal Ltd.，2021 WL 662168，8－9（2021）.

〔35〕 See Facebook，Inc. v. BrandTotal Ltd.，2021 WL 2354751，8－9（2021）.

〔36〕 See hiQ Labs，Inc. v. LinkedIn Corporation，938 F. 3d 985，993（2019）.

〔37〕 See Facebook，Inc. v. BrandTotal Ltd.，499 F. Supp. 3d 720，736（2020）.

救济需要达到足够的程度。〔38〕正如 BrandTotal 指出，其已无法获取为维持运营所必要的数据，被迫暂停大部分业务。同时，BrandTotal 通过特定客户对 Facebook 指控的担忧、特定潜在客户暂停或推迟与 BrandTotal 的谈判，以及风险投资损失等内容的举证，确认了其所遭受损失达到了无法弥补的程度。

（二）主观动机之考虑因素

识别行为人的主观动机通常依赖于客观行为证据，由此应关注客观行为的外在表现。当行为具有非法性时，比如诱使他人限制数据抓取或限制产品的功能是通过诽谤、致害诋毁、欺诈等手段作出，则可以基本确定行为人的恶意。如果未能直接识别非法性，则应该充分考察限制数据抓取的外在行为表现，包括行为人对已存在合同等经济关系的了解情况、行为相关的数据类型、协商过程、竞争关系等因素。

第一，行为人对已存在合同关系的认知。如干扰人并不存在知悉他人存在合同关系之可能，则其行为难言是旨在破坏他人经济关系。需注意的是，对已存在的合同的认知情况并不需要特别细致，无需证明干扰人知道合同相对人是谁以及具体合同内容，只要证明干扰人知道自己在干扰他人合同即可。〔39〕

第二，数据类型有助于考察行为主观意图，但并非决定因素。hiQ 案以及 Facebook 案一致认为，对于非公开数据而言，经营者基于自身商业模式，通过密码保护、技术手段、用户协议、隐私设置等方式对数据进行保护，体现出强烈的保护需求以及维持经营的动机，因此限制数据抓取难以体现侵害的恶意。而对于公开数据的限制抓取，可能违反加利福尼亚州不公平竞争法以及反托拉斯法，进而在手段上显现出违法性。原被告双方是否为竞争关系亦有助于考量被告行为的动机。如 hiQ 案中，LinkedIn 与 hiQ 在数据分析产品市场上具有竞争关系，且 LinkedIn 具备可观的数据资源与市场地位优势，在无正当理由的前提之下以限制访问的手段干扰 hiQ，很可能构成干扰侵权以及垄断。美国第九巡回上诉法院论述道："如果像 LinkedIn 这样（拥有大量公共数据）的公司被允许有选择性地禁止潜在竞争对手访问和使用公共数据，将导致收集和分析公共数据领域的原始创新者被排除于市场之外。"〔40〕但具体定性仍需作进一步的分析，即针对公开数据的限制抓取亦并不当然非法，比如 Facebook 案中，法院认为 Facebook 有可能存在急需实现的重要利益，或者基于平台数据的整体监管而无法实现对某类数据的独立操作，这些情况均可能证明行为人的动机并非损害其他经营者。因而，数据类型是其中一项考量因素，但并不能简单地基于数据的公开状态而断定限制抓取违法。BrandTotal 曾三次修改有关 Facebook 涉嫌垄断的不公平竞争反诉主张，均未成功证明。

第三，限制数据抓取行为的主观意图还可以结合双方的协商洽谈记录进行判断。合同是处理数据权益、配置的一种重要方式，数据交易应当尊重市场原则以及双意愿，避免削弱市场竞争的激励机制。出于对数据处理者的劳动成果以及相关财产利益的尊重，抓取数据一方应当积极寻求

〔38〕 See Rent-A-Center, Inc. v. Canyon Television and Appliance Rental, Inc., 944 F. 2d 597, 603 (1991).

〔39〕 See Facebook, Inc. v. BrandTotal Ltd., 499 F. Supp. 3d 720, 738 (2020).

〔40〕 hiQ Labs, Inc. v. LinkedIn Corporation, 938 F. 3d 985, 998 (2019).

同意。通过寻求协商与同意，需求方或能以较小成本实现数据获取的目的，并避免违法风险。而对于司法裁判来说，协商过程能够帮助法院比较不同合同或者合作方式，从而考察行为人是否设置不合理的交易条件，以及是否具备排除限制竞争的动机与目的。比如美国北卡罗来纳州法院指出："鉴于 Facebook 拒绝 BrandTotal 的访问，是基于 BrandTotal 未能与 Facebook 协商并通过 Facebook 的现有渠道（比如 API）以寻求许可……任何一方都未能就 BrandTotal 如何获得 Facebook 的许可问题进行协商，因而留下了一个悬而未决的问题，即 Facebook 的意图，以及如果 BrandTotal 在符合 Facebook 授权访问协议范围内开展业务，Facebook 是否会同意许可。"〔41〕在数据控制者已经存在共享数据的途径、渠道及方式的情形之下，如果抓取数据一方没有积极寻求协商，或者没有遵守明确权利义务的用户协议进行数据抓取，则不宜直接推定限制抓取一方的动机。

当限制数据抓取行为是通过第三人实现时，如行为人通过虚假陈述等手段导致第三人采取措施干扰合同履行，则法院还应考察行为人与第三人的协商过程。在 Facebook 案中，Facebook 除了自行采取技术措施限制 BrandTotal 的抓取行为外，还通过虚假陈述误导 Google 应用商店下架 BrandTotal 的产品，该行为是法院认定其干扰恶意的关键。因而，类似案件的裁判也应当将沟通内容的客观性、中立性纳入主观恶意的考察范围。

（三）合理商业目的与利益衡量

由被告就限制数据抓取的合理商业目的进行阐释与举证，是合理的制度安排，有助于法院考察真实的行为动机、更好地进行利益衡量。一般认为，行为人没有正当理由而损害其他经营者的利益，可以认定其具有纯粹损害他人的恶意，进而应当承担法律责任。在市场竞争之中，合理的商业目的具有丰富的表现形式与内涵，立法无法完全穷尽。就限制数据抓取纠纷的判例实践来看，限制数据抓取的正当理由抗辩通常包括私人利益保护与公共利益保护两方面。私人利益保护的需求可表现为保护投资安全、保护平台监管的完整性、以自力救济防御第三方侵害等；而与公共利益相关的限制数据抓取的商业目的与正当利益，主要是遵守法律要求，比如保护用户隐私可以作为豁免责任的理由。

在考察正当理由抗辩时，应当探析正当理由与行为之间的因果关系，正如 hiQ 诉 LinkedIn 中，LinkedIn 以隐私保护为由进行抗辩，第九巡回上诉法院在进行利益衡量时指出：一方面，LinkedIn 的核心商业模式是为用户提供信息共享的平台，并不需要禁止 hiQ 访问数据来实现开发平台的投资保护目的；另一方面，用户对其公开档案中共享的信息所寄予的隐私期望是不确定的，并且 LinkedIn 自身也开发了一项与 hiQ 产品类似的数据分析产品，因而其所声称的隐私保护目的很可能是借口。〔42〕

在利益衡量环节，限制数据抓取行为经常涉及双方兼具合法权益的情形，因而需要确定价值位阶。当双方利益处于同一位阶时，比如双方均有迫切实现的合同利益，则要求证明行为人特定的动机。比如前述 Facebook 案中，Facebook 认为自己的行为存在正当利益，即执行用户协议，而该利益同样受法律保护。在此情况下，"决定性问题就在于被指控干涉一方是否出于

〔41〕 Facebook，Inc. v. BrandTotal Ltd.，499 F. Supp. 3d 720，742（2020）.

〔42〕 See hiQ Labs，Inc. v. LinkedIn Corporation，938 F. 3d 985，998（2019）.

善意行事”〔43〕，如不能证明其恶意，则难以施加责任。BrandTotal 曾因并未证明 Facebook 的特定动机或恶意导致其基于干扰合同提起的反诉被驳回，法院认为：“BrandTotal 承认 Facebook 的服务条款，其禁止未经许可自动收集数据的行为。尽管 BrandTotal 在其关于当前驳回动议和之前的临时限制令动议的诉状中暗示 Facebook 存在恶意，但 BrandTotal 并未在其反诉中指控 Facebook 存在任何特定动机。”〔44〕

六、启示与总结

通过美国判例实践的展示，可以洞见美国司法的审慎态度，其对干扰侵权理论的适用更为精细，并通过损害程度要求、正当性抗辩环节及主观恶意证明等提高认定行为违法性的门槛，体现了司法机构对市场竞争的尊重，避免过度干预。也由于利益衡量环节的加入，反不正当竞争法的适用不至于将一方的商业利益上升为“绝对权利”，进而加以偏颇保护，导致静态竞争利益的固化。干扰侵权理论与实践对于认定限制数据抓取行为的违法性具有一定助益，为司法机关提供了利益衡量与价值评判的基本范式。尽管中美两国具有不同的法系背景与传统，但该理论以及相关实践具有一定的借鉴价值。

（一）我国侵害债权理论及相关立法基础

我国学界早已对干扰侵权理论进行探讨，且存在一定的立法基础。基于法系背景差异，合同履行利益在我国属于债权概念范畴，因而美国干扰侵权理论实际上与我国第三人积极侵害债权理论与法律实践具有共同性。在立法规范上，我国《民法典》为干扰侵权理论提供了法律依据。《民法典》第 1165 条作为侵权责任的一般条款，规定“行为人因过错侵害他人民事权益造成损害的，应当承担侵权责任”。而第 593 条规定：“当事人一方因第三人的原因造成违约的，应当依法向对方承担违约责任。当事人一方和第三人之间的纠纷，依照法律规定或者按照约定处理。”合同作为一项债权属于民事权益范畴，而当第三人因过错对合同权益实施侵害且造成损害结果时，债权人基于侵权事实向第三人主张侵权责任并不与立法规范相悖。针对这种行为的调整，学界有大量观点主张可以以侵权法解决当事人与第三人的纠纷。〔45〕基于市场交易的经验与习惯，社会观念层面已普遍承认对合同归属与履行利益的保护与尊重。尽管合同作为债权不具备典型的社会公开性，但一旦行为人知悉债权关系的存在即满足了具体公开性之要求。行为人在感知他人权益状况的前提下实施侵害，存在过错以及可责性，由此征引行为的违法性，进而追究行为人的侵权责任并实现对受害人的救济。〔46〕

而将视野扩展至市场竞争领域，第三人侵害债权理论或干扰侵权理论即是对诚实信用原则的

〔43〕 Facebook，Inc. v. BrandTotal Ltd.，2021WL662168（2021）；Richardson v. La Rancherita，98 Cal. App. 3d 73，81 (1979).

〔44〕 Facebook，Inc. v. BrandTotal Ltd.，2021WL662168，8 (2021).

〔45〕 参见王利明：《违约责任论》，中国政法大学出版社 2003 年版，第 743 页；解亘：《论〈合同法〉第 121 条的存废》，载《清华法学》2012 年第 5 期；施鸿鹏：《债权的侵权法保护及其法理构成》，载《法学家》2022 年第 1 期；程啸：《侵权责任法》，法律出版社 2021 年版，第 178 页。

〔46〕 参见前引〔45〕，施鸿鹏文。

强调，要求市场内的经营者诚实守信，以创新与增加效率等正当途径实现竞争优势的累积，而非通过恶意干扰手段“害人利己”。这样的理念与价值目标与我国《反不正当竞争法》相吻合。由此，《反不正当竞争法》可以将干扰侵权行为视作一种违反商业道德的不正当竞争，〔47〕并通过干扰侵权理论征引限制数据抓取行为的违法性从而进行调整。抑或在分析模式层面，将干扰侵权理论与实践作为我国适用《反不正当竞争法》第12条（即互联网专条）的借鉴对象。两者在分析模式上并不互斥，具有一定的共通性。以《反不正当竞争法》第12条所列举禁止的网络不正当竞争行为作为比照，链接跳转、妨碍破坏网络产品服务的行为则可以抽象为美国干扰侵权理论中的干扰行为，在主观层面都至少应满足故意要件甚至是恶意要件，〔48〕在客观层面上则体现为网络产品或服务的正常运行受到干扰。

但两者也存在区别。干扰侵权理论所保护的权益在于合同以及预期合同，其并不以产品服务受妨碍的事实作为判断行为违法性的起点。因而，干扰侵权理论的价值可以体现为避免司法机关在产品服务、流量、数据上创造新的权益，进而控制司法干预竞争的门槛。并且，区别于“非公益必要不干扰”模式，干扰侵权模式的分析进路有助于为经营者的行为自由留存足够空间，避免对自由竞争的过分干预。“非公益必要不干扰”的分析模式源自我国法院在“百度诉奇虎案”中的裁判思路，〔49〕其预设企业之间竞争行为的非法性，并提出干扰行为只有基于公益之必要才能被认为是合法的〔50〕。而该模式对竞争行为预设非法性的先定立场以及狭隘的正当化事由，实则以绝对权保护的思维对市场先入者的竞争利益施以倾斜保护，将抑制网络市场竞争以及创新机制。〔51〕综上，美国干扰侵权理论及实践之于我国限制数据抓取行为定性乃至网络不正当竞争行为的分析框架具有借鉴意义及可能。

（二）实践应用：我国限制数据抓取行为的违法性认定

就司法实践层面的借鉴而言，作为调整市场主体竞争行为的重要法律规范，《反不正当竞争法》明确禁止多种明显扰乱竞争秩序的行为，并以第2条即一般条款实现兜底适用。其中，与一般条款类似，《反不正当竞争法》第12条第2款第4项也承担兜底适用的功能。这类兜底性规定是评价限制数据抓取行为违法性的标尺，但其为了保障法律的弹性适用效果而一定程度上牺牲了规范构造上的确定性，未能为司法裁判提供明确指引。2022年1月发布的《最高人民法院关于适用〈中华人民共和国反不正当竞争法〉若干问题的解释》亦未对此进行回应，只是在第3条中指出法院可以参考自律公约及行业规范等认定行为是否违反商业道德。〔52〕但除了特定行业领域存

〔47〕 参见前引〔13〕，李扬，蓝小燕文。

〔48〕 参见孔祥俊：《网络恶意不兼容的法律构造与规制逻辑——基于〈反不正当竞争法〉互联网专条的展开》，载《现代法学》2021年第5期。

〔49〕 参见北京市高级人民法院（2013）高民终字第2352号民事判决书；最高人民法院（2014）民申字第873号裁定书。

〔50〕 参见薛军：《质疑“非公益必要不干扰原则”》，载《电子知识产权》2015年第Z1期。

〔51〕 参见宋亚辉：《网络干扰行为的竞争法规制——“非公益必要不干扰”原则的检讨与修正》，载《法商研究》2017年第4期。

〔52〕《最高人民法院关于适用〈中华人民共和国反不正当竞争法〉若干问题的解释》第3条规定：“特定商业领域普遍遵循和认可的行为规范，人民法院可以认定为反不正当竞争法第二条规定的‘商业道德’。人民法院应当结合案件具体情况，综合考虑行业规则或者商业惯例、经营者的主观状态、交易相对人的选择意愿、对消费者权益、市场竞争秩序、社会公共利益的影响等因素，依法判断经营者是否违反商业道德。人民法院认定经营者是否违反商业道德时，可以参考行业主管部门、行业协会或者自律组织制定的从业规范、技术规范、自律公约等。”

在自律公约外，如我国《互联网搜索引擎服务自律公约》，其他领域未必存在相应的行业规范予以指引，此时无法依赖商业道德要件对行为进行价值评判，背俗侵权的分析模式也无法直接适用。并且，一般经营者限制数据抓取行为可能出于投资保护、妨害防御等正当需求，属于合法的自主经营行为，并不当然能够从限制手段中征引非法性。〔53〕因而，美国干扰侵权理论实践或有助益，能够为我国司法提供基本分析模式，并展现个案裁判中所需关注的因素，其逻辑在于，经营者恶意以限制数据手段侵害竞争对手的合同关系，导致其履行不能，行为将因侵害结果、主观恶性损害市场秩序而产生规制必要性。

从分析模式来看，美国法院从损害结果、客观行为、主观因素等方面进行利益衡量，类似于我国在制定法下结合主客观要件进行分析的模式，并通过要件下具体事实的考察，评判行为人是否应当担责。在肯定干扰侵权理论的价值之基础上，我国法院在具体裁判限制数据抓取行为纠纷中应着重关注原告两方面的举证。

在客观构成要件方面，原告需举证限制数据抓取行为所造成的实质损害结果。实际损害结果的证明是寻求救济的基础。在数据竞争行为的救济手段中，损害赔偿以及停止侵害是较为重要且主要的责任形态。而为了维持经营以及保持商业模式的可持续，原告更为期盼获得类似美国行为禁令的救济方式，以制止、预防针对未来的侵害。但由于数据具有可复制性，一旦开放则可能造成不可逆的结果，包括数据失控导致用户信息泄露、知识产权控制措施的失效、基于数据所积累的商业优势的丧失等。因而有必要对损害要件的证明施以实际损害及严重程度的要求，而不能是类似“流量减损”“消费者选择的减少”等抽象意义上的损害。需强调，并非所有由竞争机制导致的损失都具有司法救济的必要性。在竞争损害具有相对性的背景下，交易机会的此消彼长以及流量的增减是市场竞争的常态。〔54〕如果将举证门槛放宽至此类抽象损害，客观上将导致《反不正当竞争法》过于轻率地介入市场竞争中，不利于实现司法审慎。由此，应要求原告通过合同乃至商业关系的中断对实质损害及其严重程度予以证明。

在主观要件的考察方面，原告应证明行为人具备侵害合同的主观故意以及恶性意图。基于市场经济下竞争的损害必然性以及保障竞争自由最大化的考虑，应对主观要件施以故意乃至恶意的要求。而以故意作为主观要件，有助于平衡利益保护及行为自由。〔55〕至于恶意要件，首先包含希望或放任损害结果发生的故意，并强调行为人在主观意图上纯粹损害他人而非旨在实现自己的正当竞争利益，由此构成反不正当竞争法意义上的可谴责性。〔56〕在双方都具有合理的竞争利益的情形下，主观意图将成为影响违法性认定的关键所在。如果无法证明行为人的主观恶意，则不应认定限制数据抓取行为违法，否则将严重限制市场主体的经营自由。

与欺诈、胁迫、暴力等手段不同，限制数据抓取行为本身未必能直接体现非法性以及行为人的主观恶意。对于行为人恶意的考察，仍需借助客观证据进行判断。从美国 hiQ 案以及 Facebook 案的判例实践来看，应结合以下方面进行考察：第一，双方的商业模式，包括被限制

〔53〕 参见高建成：《限制数据抓取行为的正当性及其价值衡量》，载《中国流通经济》2022 年第 8 期。

〔54〕 参见前引〔51〕，宋亚辉文。

〔55〕 参见孙晋、李胜利：《竞争法原论》，法律出版社 2020 年版，第 368 页。

〔56〕 参见前引〔48〕，孔祥俊文。

方的商业活动是否以行为人的数据为必要基础，而行为人商业模式下的数据是否原本处于公开的状态；第二，双方就数据交易的协商过程，以此判别占有数据的经营者是否对其他经营者课以不公平的交易条件或者差别待遇；第三，抓取数据行为的后果，包括数据占有者的合理商业利益、法律义务要求以及抓取数据方的数据使用方式；第四，行为人是否有通过虚假陈述等方式诱使其他经营者实施限制行为；第五，行为人限制数据抓取的正当理由抗辩，应要求行为人就正当理由进行举证，以此考察合理的商业目的，判断行为意图。

由此，借鉴干扰侵权理论及实践经验，我国司法实践可从主客观层面对限制数据抓取行为进行要件式衡量与考察，进而在个案中审慎认定违法性。须明确，干扰侵权理论的目的在于规制纯粹破坏他人经营的行为，并确保其他市场主体行为自由的合理空间。如果行为旨在实现或维护正当商业利益而偶然、不可避免地导致他人的损害结果，则不宜施以法律责任；若明知损害结果的发生而无正当理由，则可体现行为人的主观恶性意图，构成不正当竞争法的可责性。

Abstract: Faced with the challenge of determining the illegality of restriction on data scraping, US jurisprudence has applied the tort of interference doctrine to address the illegality of an act by means of its detrimental effect on a contractual relationship. Under the tort of interference theory, the plaintiff shall prove that the actor had knowledge of the contractual or contemplated contractual relationship, intentionally interfered with the contractual or contemplated contractual relationship, caused the interruption of the contractual or prospective contractual relationship, and produced a materially injurious result. The theory and jurisprudence have implications for China's judicial practice. Firstly, contracts and prospective contracts can be treated as legal interests protected by the anti-unfair competition law, avoiding the creation of new rights and interests in data and product services and achieving judicial prudence. Second, case adjudication should focus on the objective level of proof of substantial damage and focus on examining the subjective intent of the actor, integrating evidence of the actor's knowledge of the pre-existing contract, the type of data involved in the act, the business model of both parties, the negotiation process, and combining with the justification defense. When the actor restricts the data capture of others with the intention of purely malicious intent to infringe on others rather than for legitimate purpose, it is appropriate to find unfair competition.

Key Words: restricting of data scraping, unfair competition, interference torts, legitimate business purpose

（责任编辑：殷秋实　赵建蕊）

财经法学 No. 6，2022
pp. 65 - 80

互联网不正当竞争类型化条款司法适用的反思与纠正

黄　军*

内容提要：互联网不正当竞争类型化条款在制度供给层面顺应了互联网领域竞争行为的规制需求。该类型化条款在司法运行层面主要有“独立适用”“二元并存适用”“三元混合适用”三种模式。司法实践中，现有类型化条款在规范适用结构上面临“泛化”与“虚化”困境，在规范适用逻辑关系上呈现明显对立性，在规范适用构成要件解析上缺乏一致性。寻求互联网不正当竞争类型化条款司法适用的优化可从三方面着手：一是通过明确兜底条文适用解释的同质性、厘清列举条款适用对象的指向性以及凸显宣示条款适用功能的区分性，明晰不同规范适用的具体定位；二是采取“二元协作评价路径”以厘定类型化条款与一般条款的外部逻辑关系；三是构建起“前置的竞争关系＋合法的竞争利益＋特定的竞争行为＋多元的竞争损害＋合理的竞争抗辩”的统一规范要件适用程式。

关键词：反不正当竞争法　互联网不正当竞争　类型化条款　一般条款

一、引　言

近些年随着互联网领域竞争日趋白热化，各类新型不正当竞争行为层出不穷，基于对旧法一般条款在实践中日渐凸显的不确定性问题的内在省思与深入检讨，尤其是及时回应由此引发的“向一般条款逃逸”现象的普遍关切，〔1〕在广泛梳理、归纳与总结既有典型案例基础上，立法者通过2017年《反不正当竞争法》修订之机最终确立了互联网不正当竞争类型化条款（即第12

* 黄军，青岛大学法学院讲师。

〔1〕 参见陈兵：《互联网经济下重读“竞争关系”在反不正当竞争法上的意义——以京、沪、粤法院2000—2018年的相关案件为引证》，载《法学》2019年第7期。

条)。在规范构造层面，除了具有浓厚倡导意味的第 1 款规定（即宣示条款）以外，现有类型化条款采取了“概括＋列举＋兜底”的复合体例。

从立法初衷与功能指向维度来看，作为修法中的“形象工程”，互联网不正当竞争类型化条款不仅象征着互联网时代的“标杆条款”，〔2〕也在制度供给层面顺应了互联网领域竞争行为的规制需求。在条款颁行前后，学界就此展开了广泛讨论，但更多侧重从法解释学进路对条文构造及其意涵加以考察与剖析。问题在于，书本上的法不等于行动中的法，对法律真正科学的描述一般认为，法律殊非书面上的文字所言——“法律即所作为”。〔3〕进一步而言，“虽然法提出的主要是一种规范性要求，但法律之治却必须基于坚实的实证基础之上，否则法律之治的目标就可能会落空”〔4〕。依此检视，围绕互联网不正当竞争类型化条款的既有研究成果不仅呈现出明显的同质化取向，〔5〕而且针对规范的运行效果也未给予必要且足够的理论关照。鉴于此，本文采取实证化分析进路，通过梳理司法案例具体考察现有类型化条款的适用模式，探究其在实践中面临的突出问题，最终提出相应的改进建议。

二、互联网不正当竞争类型化条款司法适用的不同模式

（一）独立适用模式

独立适用系指法院主要援引第 12 条规定作为审理互联网不正当竞争案件的实体裁判依据，不涉及反不正当竞争法其他具体规制条款。其可一分为二：

1. 整体适用

整体适用是法院在个案中对互联网不正当竞争类型化条款未加以具体筛选，而选择一体化适用进路以判定涉案行为是否构成不正当竞争。其包括两种形态：一是直接型整体适用，在“奇虎与搜狗不正当竞争纠纷案”〔6〕“聪明狗与淘宝不正当竞争纠纷案”〔7〕以及“百度与搜狗不正当竞争纠纷案”〔8〕中，法院在明确援引第 12 条基础上分别对竞争行为正当性作出界定；二是间接型整体适用，在由北京知识产权法院审理的“迪火与三快不正当竞争纠纷案”〔9〕中，法院基于条文逻辑关系考量后指出，被诉行为已经违反第 12 条，对于是否违反第 2 条规定不再评述，故最终主要依据互联网不正当竞争类型化条款作出了相应判决。

2. 局部适用

局部适用是在具体分解第 12 条规定内部体系构造基础上，结合个案情形仅援引互联网不正

〔2〕 参见孔祥俊：《反不正当竞争法新原理·分论》，法律出版社 2019 年版，第 528－529 页。

〔3〕 参见〔美〕萨默斯：《美国实用工具主义法学》，柯华庆译，中国法制出版社 2010 年版，第 107 页。

〔4〕 罗豪才、宋功德：《软法亦法——公共治理呼唤软法之治》，法律出版社 2009 年版，第 67 页。

〔5〕 涉及互联网不正当竞争类型化条款的代表性文献主要有：李扬：《互联网领域新型不正当竞争行为类型化之困境及其法律适用》，载《知识产权》2017 年第 9 期；孔祥俊：《论新修订〈反不正当竞争法〉的时代精神》，载《东方法学》2018 年第 1 期；郑友德、王活涛：《新修订反不正当竞争法的顶层设计与实施中的疑难问题探讨》，载《知识产权》2018 年第 1 期；蒋舸：《〈反不正当竞争法〉网络条款的反思与解释——以类型化原理为中心》，载《中外法学》2019 年第 1 期。

〔6〕 参见北京市海淀区人民法院（2016）京 0108 民初 14003 号民事判决书。

〔7〕 参见北京知识产权法院（2019）京 73 民终 1128 号民事判决书。

〔8〕 参见北京市海淀区人民法院（2017）京 0108 民初 7967 号民事判决书。

〔9〕 参见北京知识产权法院（2018）京 73 民初 960 号民事判决书。

当竞争类型化条款中具有指向性的特定条文。其可一分为三：

一是单独适用第12条第2款第2项。在“百度与乐活不正当竞争纠纷案”〔10〕中，法院认为，被告针对原告搜索服务的页面图片宣传屏蔽广告和新闻的功能，并屏蔽了原告的产品服务和付费搜索广告结果，因而认定其违反了第12条第2款第2项。

二是独立适用第12条第2款第4项规定。〔11〕例如在“优酷与视客不正当竞争纠纷案”中，法院指出，针对通过视客App便可免费完整获取优酷公司的视频播放服务的行为，鉴于其在外形上无法被纳入第12条第2款前三项所明定的互联网不正当竞争之情形，因而最终认定应由第12条第2款第4项调整。

三是共同适用第12条第1款与第2款第1项规定，或者共同适用第12条第1款与第2款第4项规定。在“百度与搜狗不正当竞争纠纷案”〔12〕中，针对被告通过技术手段导致在其浏览器地址栏中输入原告目标网址或者更改浏览器主页设置或者设置标签页均会跳转为被告导航网址的行为，法院同时援引第12条第1款与第2款第1项规定作出了判决。在“优酷与徐州百狐网不正当竞争纠纷案”〔13〕“爱奇艺与乐播不正当竞争纠纷案”〔14〕“腾讯与微源码不正当竞争纠纷案”〔15〕“优酷与锋芒不正当竞争纠纷案”〔16〕以及“腾讯与谌洪涛等不正当竞争纠纷案”〔17〕中，法院认定涉案竞争行为构成第12条第2款第4项之情形，且在裁判依据中一并提及第12条第1款与第2款第4项。此种模式中，法院虽述及第12条第1款，但真正发挥实质性调整作用的仍为列举条款。

（二）二元并存适用模式

二元并存适用是法院既援引了互联网不正当竞争类型化条款，也适用了反不正当竞争法或者其他法律中的实体规制条款作为共同的审理依据。其大致涉及如下情形：

1. 与一般条款的共同适用

一是形式意义上的共同适用，即法院在界定涉案竞争行为正当性时优先参照具体条款，但最终仍于裁判依据中同步列明第2条与第12条。此种情形下，判定涉案行为是否构成不正当竞争时，发挥独立评价作用的规范依据为第12条，第2条仅居于辅助性地位。详细而言，前述“辅助性地位”有如下具体表现：（1）合法权益证成。在“优酷与百度不正当竞争纠纷案”〔18〕中，法院结合对第2条的意涵阐释与个案事实的综合衡量，认可原告享有反不正当竞争法保护之利

〔10〕 参见北京市海淀区人民法院（2018）京0108民初38881号民事判决书。

〔11〕 相关案例参见北京知识产权法院（2020）京73民终49号民事判决书；北京市海淀区人民法院（2019）京0108民初34763号民事判决书；北京市海淀区人民法院（2018）京0108民初2065号民事判决书；北京市海淀区人民法院（2019）京0108民初51116号民事判决书；广东省广州市天河区人民法院（2019）粤0106民初40045号民事判决书；北京知识产权法院（2020）京73民终1556号民事判决书；上海市徐汇区人民法院（2018）沪0104民初243号民事判决书；北京市海淀区人民法院（2017）京0108民初36596号民事判决书；北京市海淀区人民法院（2017）京0108民初24512号民事判决书；江苏省高级人民法院（2019）苏民终778号民事判决书。

〔12〕 参见北京市海淀区人民法院（2018）京0108民初42023号民事判决书。

〔13〕 参见北京市海淀区人民法院（2017）京0108民初54830号民事判决书。

〔14〕 参见北京市海淀区人民法院（2018）京0108民初48523号民事判决书。

〔15〕 参见广东省深圳市中级人民法院（2017）粤03民初773号民事判决书。

〔16〕 参见北京市海淀区人民法院（2019）京0108民初28000号民事判决书。

〔17〕 参见上海市浦东新区人民法院（2019）沪0115民初73840号民事判决书。

〔18〕 参见北京市海淀区人民法院（2017）京0108民初57274号民事判决书。

益。（2）竞争关系厘定。在“复娱与微梦不正当竞争纠纷案”〔19〕中，法院借助对第 2 条规定的意涵推衍，确认原被告双方存在竞争关系。（3）规范关系阐明。在“前锦与逸橙不正当竞争纠纷案”〔20〕中，法院重申了最高人民法院在“海带配额案”中所确立的独立适用第 2 条的基本要件，进而释明了一般条款与具体条款之间的相互关系。

二是实质层面上的共同适用，即裁判依据中同时引用了第 2 条与第 12 条，且各自发挥了规制效力。其包括如下类型：（1）针对同一竞争行为，同时适用第 2 条与第 12 条进行评价。〔21〕在“腾讯与通路、云电、罗博特等系列不正当竞争纠纷案”中，法院认为，涉案微信群控系统对微信平台争取到的用户注意力和交易机会造成了破坏和损害，明显不符合诚信原则，有违第 2 条规定；同时法院提到，前述干扰行为也违反了第 12 条规定。（2）针对不同行为，分别适用第 2 条与第 12 条进行评价。在“猎豹、金山与二三四五不正当竞争纠纷案”〔22〕中，法院指出，被告擅自变更网络用户浏览器主页的行为属于第 12 条规定的误导、欺骗、强迫用户修改、关闭原告合法提供的网络产品的情形；至于涉案区别对待行为，法院认为，其违背了第 2 条规定的自愿、平等、公平、诚信的原则，有悖于法律和商业道德。

2. 与其他具体条款的共同适用

在“金豪风机与金河风机不正当竞争纠纷案”〔23〕中，法院在分析论证与裁判依据部分依次引用了第 6 条与第 12 条，但最终因原告举证不足而驳回了其诉讼请求。在“福州神康医院与平潭精神病防治院不正当竞争纠纷案”〔24〕中，一审法院指出，被告在搜索引擎上设置与原告名称相关的信息等作为关键词不仅足以误导公众，也妨碍了原告提供的网络服务正常运行，故根据第 6 条与第 12 条规定确认其构成两类不正当竞争行为。在“神马与搜狗不正当竞争纠纷案”〔25〕中，法院借助第 8 条与第 12 条分别针对搜狗的虚假宣传、遮挡浏览器输入法增强栏和设置搜索候选词误导用户进入搜狗搜索的竞争行为作出了否定性评价。

3. 与《商标法》条文的共同适用

在“快手与易智侵害商标权纠纷案”〔26〕中，法院援引《商标法》第 57 条第 1 项、第 2 项认定被告涉案软件使用与涉案商标相同或近似的标识，侵害了原告享有的注册商标专用权；针对被告在原告经营的 App 中强制进行目标跳转的行为，法院结合《反不正当竞争法》第 12 条第 2 款第 1 项规定判定其构成不正当竞争。

4. 与《著作权法》条文的共同适用

在“腾讯与点云侵害作品信息网络传播权系列纠纷案”〔27〕中，法院认为，点云公司未经授

〔19〕 参见北京知识产权法院（2019）京 73 民终 2799 号民事判决书。

〔20〕 参见上海知识产权法院（2019）沪 73 民终 263 号民事判决书。

〔21〕 相关案例参见杭州铁路运输法院（2019）浙 8601 民初 1661 号民事判决书；重庆市第五中级人民法院（2019）渝 05 民初 3618 号民事判决书；天津市第一中级人民法院（2019）津 01 民初 1319 号民事判决书；浙江省高级人民法院（2020）浙民终 330 号民事判决书；广东省深圳市中级人民法院（2019）粤 03 民初 1911 号民事判决书；广东省深圳市中级人民法院（2019）粤 03 民初 1912 号民事判决书；广东省深圳市中级人民法院（2019）粤 03 民初 1913 号民事判决书。

〔22〕 参见上海知识产权法院（2019）沪 73 民终 241 号民事判决书。

〔23〕 参见山东省沂源县人民法院（2020）鲁 0323 民初 473 号民事判决书。

〔24〕 参见福建省高级人民法院（2020）闽民终 554 号民事判决书。

〔25〕 参见北京市海淀区人民法院（2016）京 0108 民初 16044 号民事判决书。

〔26〕 参见北京市海淀区人民法院（2018）京 0108 民初 68074 号民事判决书。

〔27〕 参见杭州互联网法院（2020）浙 0192 民初 1329 号民事判决书；杭州互联网法院（2020）浙 0192 民初 1330 号民事判决书。

权将涉案游戏置于其云服务器中供公众在移动端、web 端以及 PC 端使用“菜鸡”云游戏平台获得其提供的涉案游戏之行为，违反了《著作权法》第 48 条第 1 项规定，侵害了原告享有的信息网络传播权；并进一步判定点云公司限制涉案游戏外部链接跳转功能已妨碍、破坏了原告合法提供的涉案游戏正常运行，违反《反不正当竞争法》第 12 条第 2 款第 4 项规定。

5. 与《合同法》条文的共同适用

在“爱奇艺与龙境不正当竞争纠纷案”〔28〕中，法院指出，涉案分时出租 VIP 账号行为有违原被告双方关于 VIP 账号使用权限的约定，且双方约定未违反《合同法》关于格式条款无效之规定，因而该行为不具有正当性；针对被告通过技术手段对涉案爱奇艺 APP 部分功能加以限制的行为，法院认定其违反了《反不正当竞争法》第 12 条规定，并进一步提到，在已适用具体条款情形下，不再支持原告关于同时适用该法第 2 条进行调整的主张。

（三）三元混合适用模式

此处的三元混合适用，系指法院在实践中援引了涵括《反不正当竞争法》中的互联网不正当竞争类型化条款在内的三类规制条文作为实质性裁判依据之情形。

1. 与一般条款、误导性宣传规制条款的共同适用

在“腾讯与微时空不正当竞争纠纷案”〔29〕中，其裁判依据主要涉及《反不正当竞争法》第 2 条第 2 款与第 3 款、第 8 条第 2 款、第 12 条第 1 款与第 2 款第 4 项。析言之，法院通过援引第 2 条中有关经营者的规定，指出涉案原被告之间面临着直接的竞争利益冲突，故认定其构成反不正当竞争法意义上的竞争关系；在具体引述第 8 条第 2 款条文前提下，法院基于案件事实判定被告为他人提供微信软件刷量服务行为符合“帮助他人虚假宣传”的行为构成；同时，法院认为，前述有偿刷量服务行为属于第 12 条第 2 款所规制的“妨碍、破坏网络产品或者服务正常运行”的不正当竞争行为。

2. 与一般条款、商业秘密规制条款的共同适用

在由杭州市中级人民法院审理的“迪火与三快不正当竞争纠纷案”〔30〕中，最终判决的规则指引主要涉及《反不正当竞争法》第 2 条、第 9 条以及第 12 条。首先，法院基于迪火公司的涉案命名规则不符合商业秘密构成中的秘密性要求，未支持有关被告违反第 9 条的侵权指控；其次，针对原告主张被告实施具有“控制/干扰/中断”原告系统的行为，法院经过分析后认定，其不违反第 12 条；最后，法院认定被告行为未有违反诚实信用原则或公认的商业道德，不损害反不正当竞争法所保护的法益，并不违反第 2 条规定。

3. 与一般条款、商业诋毁规制条款的共同适用

在“金山与二三四五不正当竞争纠纷案”〔31〕中，法院采用的裁判依据主要包括第 2 条第 1 款与第 2 款、第 11 条、第 12 条第 2 款第 2 项。首先，法院认定，被告的涉案行为属利用技术手段，通过影响用户选择，误导、欺骗用户修改、关闭其他经营者合法提供的网络产品或者服务，

〔28〕 参见北京市海淀区人民法院（2018）京 0108 民初 37522 号民事判决书。

〔29〕 参见广东省深圳市中级人民法院（2019）粤 03 民初 594 号民事判决书。

〔30〕 参见浙江省杭州市中级人民法院（2018）浙 01 民初 3166 号民事判决书。

〔31〕 参见上海市浦东新区人民法院（2018）沪 0115 民初 62506 号民事判决书。

构成不正当竞争；其次，法院指出，被告在弹窗中对原告的涉案描述行为构成商业诋毁；最后，法院认为，被告实施的区别对待行为有违诚实信用原则与平等竞争原则，与商业道德背道而驰，扰乱了市场竞争秩序，损害了原告的合法权益，构成不正当竞争。

三、互联网不正当竞争类型化条款司法适用中存在的问题

（一）规范适用结构面临“泛化”与“虚化”困境

1. 兜底条文的泛化适用

泛化适用系指法院依据互联网不正当竞争类型化条款中的兜底条文来处理相关案件时，因缺乏对现有规范构成要件的清晰厘定与合理限缩，导致出现不当的扩展适用甚至明显的滥用情形。究其缘由，发生泛化适用与兜底条文所固有的不确定性密切相关。在互联网领域竞争形态日新月异背景下，竞争行为无可避免会呈现变异性与多样性，仅借助具有鲜明阶段性与指向性的列举条文无法实现对不正当竞争行为的周延规制，此时引入具有概括性与可解释性的兜底性规定殊为必要。问题在于，既有兜底条文的文本表述显得过于宽泛，规范内涵与外延具有高度不确定性。其主要体现为：如何理解其中的“正常”运行，是采用技术标准，还是法律标准；如何确定认定主体，以及举证责任；何谓作为对立的不正常、失常或者异常情形；等等。〔32〕由此导致的后果是，依据互联网不正当竞争类型化条款来评价互联网竞争行为时，兜底条文很可能负担“不可承受之重”，甚至可能将正当竞争行为贴上不正当竞争“标签”。〔33〕结合司法实践层面而言，此种泛化适用现象得到了不同维度的具体体现。

从形式上来看，此种泛化最为直观地反映为作为审理依据的兜底条文在相关案件中呈现出的居高不下的引用比重。这某种程度上也反映出法院在处理此类纠纷时存在明显的路径依赖。就实质层面而言，泛化适用突出表现为法院未能科学且准确地把握规范的核心要义，在适用兜底条文时采取过于宽松的解释态度，试图“一兜了之”，使得该类型化条款的规制效力出现不合理的溢出效应，逾越应有的调整界限。在备受关注的视频广告屏蔽领域，尽管学界围绕该行为的法律属性界定存有“不正当性说”〔34〕“正当性说”〔35〕与“折中说”〔36〕等观点，但新法颁行后不少法院在审理相关案件时开始纷纷由一般条款转向适用互联网不正当竞争类型化条款中的兜底条文，进而认定其构成不正当竞争。前述“优酷与视客不正当竞争纠纷案”便为具例。在法理意义上，“法律规则可适用于某一案件事实，意味着该案件事实能够归属于该法律规则构成要件所指陈的事实类型”〔37〕。依此审视既有裁判，一个被忽略的基础性问题在于：视频广告屏蔽行为虽在外观

〔32〕 参见前引〔5〕，郑友德、王活涛文。

〔33〕 参见张占江：《论反不正当竞争法的谦抑性》，载《法学》2019 年第 3 期。

〔34〕 参见宋亚辉：《网络干扰行为的竞争法规制——“非公益必要不干扰原则”的检讨与修正》，载《法商研究》2017 年第 4 期。

〔35〕 参见王迁：《论规制视频广告屏蔽行为的正当性——与“接触控制措施”的版权法保护相类比》，载《华东政法大学学报》2020 年第 3 期。

〔36〕 参见周樨平：《竞争法视野中互联网不当干扰行为的判断标准——兼评“非公益必要不干扰原则”》，载《法学》2015 年第 5 期。

〔37〕 黄泽敏：《法律漏洞填补的司法论证》，载《法学研究》2020 年第 6 期，第 64 页。

上初步契合了“其他妨碍、破坏”竞争行为的基本构成，但从体系解释维度而言，由于现有类型化条款中与之最为近似的干扰行为（即误导、欺骗、强迫类）须以违背用户意愿作为前置限定，其与视频广告屏蔽行为顺应用户需求之间迥然有别，如此一来，屏蔽行为便不应被直接纳入互联网不正当竞争类型化条款中兜底条文的规制框架之中。〔38〕通过以上简要分析，兜底条文在具体实践中的泛化适用情形可见一斑。

2. 其他规则的虚化适用

虚化适用是指互联网不正当竞争类型化条款中兜底条文以外的其他规范在个案中无法发挥出实质意义上的法律拘束力，处于虚化运行状态。其主要包括如下两种情形：

一是宣示条款徒具象征意义。在现有判决文书中，虽有部分案件的裁判依据直接述及这一条文，但往往仅是作为一项套路式的附带表述。以前述“腾讯与微时空不正当竞争纠纷案”为例，在认定涉案行为正当性时，法院分别援引第 2 条、第 8 条第 2 款以及第 12 条第 2 款，第 12 条第 1 款仅是突兀地出现在最终裁判依据之中，该规则适用背后的内在逻辑与理据基础并未得到必要阐释。这样一来，第 12 条第 1 款实则陷入“可有可无”的尴尬境地。

二是列举条款面临规制乏力困境。尽管互联网不正当竞争类型化条款中列举条款是立法者通过典型案例归纳，进而抽象与提炼出互联网新型不正当竞争共性行为要素的产物，但缺陷在于，现有规定的行为构成过于具化，而个案情形却十分复杂，仅具一时情景性的具体规则显然难以达致应有的普适性，这势必对其法律适用造成不小的困扰。〔39〕

（二）规范适用逻辑关系呈现明显对立性

1. 规范内部适用的形式逻辑矛盾

规范内部适用的形式逻辑矛盾是指不同法院根据互联网不正当竞争类型化条款来认定同一涉案互联网竞争行为时得出不同的法律结论，即“同案不同判”。这可借助前述由两地法院审理的“迪火与三快不正当竞争纠纷案”的相反判决得到直接例证。杭州市中级人民法院指出，三快公司没有主动、强行在二维火收银系统中插入链接，仅是向用户提供了选项，由用户自行进行选择，无证据表明在安装或运行过程中存在“误导、欺骗、强迫”用户的行为，最终认定不构成《反不正当竞争法》第 12 条规定的不正当竞争行为。与之相反，北京知识产权法院则认为，涉案行为违反了第 12 条第 2 款第 1 项与第 4 项规定。显然，前述做法不符合法律规范适用应当遵循的一致性规则，也有违用于衡量司法公正的“同案同判”原则。〔40〕

2. 规范外部适用的形式逻辑矛盾

规范外部适用形式逻辑矛盾是指法院援引互联网不正当竞争类型化条款（主要指向兜底条款）审理案件时，围绕涉案竞争行为是否需要同时引入一般条款的评价机制及其具体作用发挥程度方面存有不小分歧。其具体体现为三种不同意见：

一是单一评价路径，即仅依据互联网不正当竞争类型化条款来判定涉案互联网竞争行为的正当性，排除一般条款具有的调整空间。以“爱奇艺与龙境不正当竞争纠纷案”为例，法院指出，鉴于

〔38〕 参见前引〔5〕，蒋舸文。

〔39〕 参见刘维：《论软件干扰行为的竞争法规制——基于裁判模式的观察》，载《法商研究》2018 年第 4 期。

〔40〕 参见孙海波：《“同案同判”：并非虚构的法治神话》，载《法学家》2019 年第 5 期。

被诉行为已适用《反不正当竞争法》第 12 条，对于同时适用该法第 2 条进行调整的主张不再支持。

二是二元协作评价路径，即在适用互联网不正当竞争类型化条款来评价涉案竞争正当性情形时，主张引入一般条款加以共同认定。例如，在“腾讯与点云侵害作品信息网络传播权系列纠纷案”中，法院指出，在适用《反不正当竞争法》第 12 条第 2 款第 4 项时要结合该法一般条款的构成元素和判断范式进行具体认定。

三是二元独立评价路径，即判断涉案互联网竞争行为正当性时，主张独立运用互联网不正当竞争类型化条款与一般条款进行双重评价。例如，在“腾讯与硕文不正当竞争纠纷案”中，法院指出，被告研发并提供具有屏蔽（拦截）视频及贴片广告的涉案软件行为违反了诚实信用原则和公认的商业道德，属于《反不正当竞争法》第 2 条及第 12 条规定的不正当竞争行为。

（三）规范适用构成要件解析缺乏一致性

当前不同法院针对互联网不正当竞争类型化条款的规范适用构成要件缺乏相对一致的标准。其主要有如下不同主张：

1. 二要件构造说

法院将互联网不正当竞争类型化条款的适用构成区分为两大部分的观点具体如下：（1）“技术手段”＋“妨碍行为”。在“快乐阳光与搜狗不正当竞争纠纷案”中，法院指出，《反不正当竞争法》第 12 条第 2 款规定的适用要件包括：利用技术手段实施行为；妨碍、破坏其他经营者合法提供的网络产品或服务的正常运行。（2）“妨碍行为”＋“主观故意”。在“优酷与千影不正当竞争纠纷案”中，一审法院认为，被诉行为客观上破坏了原告合法提供的网络服务，且主观具有恶意，构成《反不正当竞争法》第 12 条第 2 款第 4 项规定的不正当竞争。（3）“客观行为”＋“损害后果”。在“腾讯与数推不正当竞争纠纷案”中，法院指出，被诉行为是否违反《反不正当竞争法》第 12 条规定可从两方面分析：是否符合该条规定的不正当竞争行为特征；是否损害社会公共利益，损害互联网经营者、用户和消费者的合法权益。（4）“权益受保护性”＋“行为不当性”。在“爱奇艺与龙境不正当竞争纠纷案”中，一审法院认为，判断被诉行为是否构成《反不正当竞争法》第 12 条规定的不正当竞争主要涉及两方面：原告是否享有受反不正当竞争法调整的权益；被诉行为是否属于网络环境下的不当行为。

2. 三要件构造说

该观点将互联网不正当竞争类型化条款的适用构成分解为三项要件，具体解读如下：（1）“技术手段”＋“妨碍结果”＋“违反诚信原则与商业道德”。在“爱奇艺、众源与千影不正当竞争纠纷案”中，一审法院指出，适用《反不正当竞争法》第 12 条第 2 款第 4 项规定应满足如下条件：使用技术手段影响用户选择或直接替代用户选择；导致其他经营者合法提供的网络产品或服务不能正常运行；有违自愿、平等、公平、诚实信用的原则与公认的商业道德。（2）“经营行为的合法性与正当性”＋“技术手段”＋“妨碍后果”。在“优酷与百度不正当竞争纠纷案”“优酷与乐播不正当竞争纠纷案”以及“优酷与视客不正当竞争纠纷案”中，法院适用《反不正当竞争法》第 12 条第 2 款规定认定涉案竞争行为正当性时，均将其细化为：原告提供的网络服务正当、合法；被诉行为利用技术手段实现；妨碍、破坏了原告网络服务的正常运行。（3）“竞争关系”＋“主观过错”＋“损害后果”。在“追风与京东不正当竞争纠纷案”中，二审法院阐明了《反不正当

竞争法》第12条第1款的三个适用要件：存在竞争关系；具有主观故意；造成损害后果。

3. 四要件构造说

该观点认为互联网不正当竞争类型化条款的适用构成牵涉四项要素，主要表述如下：(1)“经营者合法权益受损”＋“损害消费者利益”＋“行为不当性”＋“市场秩序损害”。在“腾讯关于微信群控系统与通路、云电、罗博特等系列不正当竞争纠纷案”中，法院认为，适用《反不正当竞争法》第12条第2款第4项规定需从四个方面进行分析：其他经营者合法权益受损；采用技术手段损害了消费者利益；违反诚信原则和公认的商业道德；破坏了互联网环境中公平竞争的市场秩序。(2)“竞争关系”＋“技术手段”＋“主观过错”＋“行为不正当性”。在“腾讯与点云侵害作品信息网络传播权系列纠纷案”中，法院在论证原被告存有竞争关系（基于业务与用户的交叉重合标准）基础上，进一步阐述了《反不正当竞争法案》第12条第2款第4项规定的适用要件：在技术角度，妨碍、破坏行为针对权利人本身；存在主观过错；涉案竞争行为具有不正当性和可责性。(3)“合法权益”＋“主观过错”＋“妨碍行为”＋“损害后果”。在“猎豹、金山与二三四五不正当竞争纠纷案”中，法院认为《反不正当竞争法》第12条第2款第2项规定的适用要件包括：原告经营产品具有合法性；利用技术手段的故意性；实施了相关妨碍行为；影响了原告提供的合法网络产品。(4)“竞争关系”＋“技术手段”＋“妨碍行为”＋“损害后果”。在“腾讯与微时空不正当竞争纠纷案”中，法院适用《反不正当竞争法》第12条第2款规定时着重考量了如下因素：界定竞争关系（采纳竞争利益冲突标准）；使用技术手段；实施妨碍行为；造成损害后果（包括扰乱市场竞争秩序与损害原告合法权益）。

4. 五要件构造说

该说主张互联网不正当竞争类型化条款的适用涉及“竞争关系”“技术手段”“主观过错”“行为可责性”以及“损害后果”五要件。在“爱奇艺与龙境不正当竞争纠纷案”中，二审法院认为，判断涉案行为是否构成不正当竞争，需要分析如下五项因素：是否存在竞争关系（主张在新经济模式下可从双方具体经营行为、最终利益存在竞争关系维度加以广义界定）；采取技术手段；主观过错；行为具有可责性；不当夺取交易机会或损害其他经营者合法利益。

综上所述，法院在个案中针对互联网不正当竞争类型化条款适用构成要件的解析虽有重叠之处，但也呈现出各自的内容侧重与表述差异，缺乏一致性。在此情形下，前述规范适用要件标准的不统一性不仅会引致不正当竞争认定标准的不确定性，也会不同程度地影响其规范指引功能的有效发挥。〔41〕

四、互联网不正当竞争类型化条款司法适用的改进路径

（一）明晰不同规范适用的具体定位

1. 明确兜底条文适用解释的同质性

适用解释的同质性，意在要求法院在审理互联网不正当竞争纠纷时应当通过引入与依循规范

〔41〕 参见黄武双、谭宇航：《不正当竞争判断标准研究》，载《知识产权》2020年第10期。

解释层面的同质性规则，实现对具有高度不确定性的兜底条文的适度限制。所谓“同质性解释”，也称“相同类别解释规则”，是“在用特别的词描述一个种类或类别的人或事之后，如果紧接着使用了总括性的词，则该总括性语词只限于与特定的词所表达的同类的人或事”〔42〕。有此主张主要基于如下考量：首先，法律规范文本离不开相应的语境，探求兜底条文的具体意涵不应忽视对现有互联网不正当竞争类型化条款的规范语境进行分析，以尽可能达致对相关规范的语义还原与澄清〔43〕。其次，为了避免对互联网不正当竞争类型化条款的理解出现分歧甚至自相矛盾的局面，有必要运用体系性解释方法，即“先查清在若干法规范有意义的结合中清晰显现出来的类型的‘主导形象’，然后由此出发来解释个别规范”〔44〕。最后，囿于例示规定所能提供信息的有限性，兜底条款的明晰化往往有赖于立法意旨的具体化。〔45〕就互联网不正当竞争类型化条款中的兜底条款而言，其形式上的生成机理虽可归结于弥补列举立法体例难以穷举的固有缺陷，但理解实质意涵则需要借助对规范整体中其他规则的目的揭示来综合把握。

进一步而言，兜底条文适用解释同质性主要涵括两方面内容：一是基于列举条款的同质性解释规则，即在考察现有列举条款中的不正当竞争类型表现后，若认定涉案互联网竞争行为能够彰显前述相关类型的“意义联结”，便可初步将之视为兜底条文的调整对象；反之，便应将之排除在兜底条文的调整范域之外。〔46〕二是基于概括条款的同质性解释，即借助现有概括条款所提供的有关互联网不正当竞争行为定义中的“共通性构成”以指导兜底条文的适用解释。当然，前述两项同质性解释规则之间是相互联系、相辅相成的。析言之，根据列举条款的同质性解释规则来判断涉案情形是否属于兜底条款调整时，应以契合概括条款的本质意涵作为基本出发点与根本落脚点；在按照概括条款的同质性解释规则来界定个案是否适用兜底条款时，列举条款所具有的类型特质无疑可对其提供重要的认知指引。

2. 厘清列举条款适用对象的指向性

针对前述“列举条款规制乏力”问题，当前紧迫的任务是在正视既有规范不足基础上借助解释论路径阐明各项类型化规则意涵的具体指向，激活其规制效力。

针对规制插入链接与强制进行目标跳转行为的第 12 条第 2 款第 1 项规定，其明晰重点在于“意愿违背”与“行为表现”。就前者而言，现有规定针对“意愿违背”仅明确“未经其他经营者同意”，而缺少消费者意愿考量，这无疑有待商榷。设想某一跳转行为虽未经其他经营者同意，但顺应了用户的普遍意愿，此时将其认定为不正当竞争明显与互联网时代消费者所享有的主体性地位不符。〔47〕较为科学的解释应当是要求同时违背经营者与消费者的意愿。对此，2022 年颁行的《最高人民法院关于适用〈中华人民共和国反不正当竞争法〉若干问题的解释》第 21 条第 1 款作出了明确规定。〔48〕就后者而言，现有条文也未明确界定“插入链接”与“强制进行目标跳

〔42〕〔英〕约翰·格雷：《法律人拉丁语手册（双语版）》，张利宾译，法律出版社 2009 年版，第 58 页。

〔43〕参见刘继峰：《反不正当竞争法中“一定影响”的语义澄清与意义验证》，载《中国法学》2020 年第 4 期。

〔44〕〔德〕卡尔·拉伦茨：《法学方法论》，黄家镇译，商务印书馆 2020 年版，第 587 页。

〔45〕参见黄茂荣：《法学方法与现代民法》（第五版），法律出版社 2007 年版，第 191 页。

〔46〕参见李军：《兜底条款中同质性解释规则的适用困境与目的解释之补足》，载《环球法律评论》2019 年第 4 期。

〔47〕参见李海舰等：《互联网思维与传统企业再造》，载《中国工业经济》2014 年第 10 期。

〔48〕该解释第 21 条第 1 款规定：“未经其他经营者和用户同意而直接发生的目标跳转，人民法院应当认定为反不正当竞争法第十二条第二款第一项规定的‘强制进行目标跳转’。”

转”的逻辑关系，即究竟两者是并列关系，还是递进关系，抑或是重叠关系。在本文看来，结合司法实践采取相对灵活的解释策略可能更契合立法本意。

针对规制误导欺骗与强迫类行为的第 12 条第 2 款第 2 项规定，其解释重点在于“行为方式”与“侵害对象”。就前者而言，现有条款要求相关主体实施有关“误导、欺骗、强迫”行为。三者既可以构成独立关系，也可以形成交叉关系。在实质意涵方面，判定“误导”的关键在于“是否如实反映商品或服务的客观情况，是否造成用户的误解并产生不适当的联想”；“欺骗”则强调对用户采取了虚构事实、隐瞒真相的做法；“强迫”意在揭示通过“野蛮行为”直接侵害消费者的选择自由与决定自由。〔49〕就后者而言，修改、关闭、卸载他人提供的网络产品或者服务，其隐含的前提是用户已经安装相关产品或者接受相关服务，因而该条文所规定的行为侵害对象应仅限于已经获得的网络产品或服务。

针对规制恶意不兼容行为的第 12 条第 2 款第 3 项规定，除了需界定主观意味浓重的“恶意”以外，该条文与《反垄断法》相关条款的关系协调问题亦亟需厘清。理论而言，恶意不兼容行为既可能构成滥用市场支配地位行为或者垄断协议行为，也可能构成互联网不正当竞争行为，因而针对该行为的规制可能适用反垄断法，也可能适用反不正当竞争法。这就意味着，当涉案不兼容行为经初步形式判定落入反垄断法的适用范围时，便应由反垄断法进行规制，而非由反不正当竞争法调整。〔50〕概言之，互联网不正当竞争类型化条款所禁止的不兼容行为指向的是垄断行为以外的行为。

3. 凸显宣示条款适用功能的区分性

凸显宣示条款适用功能的区分性旨在充分发挥该条款之于互联网不正当竞争行为所具有的分流规制作用，即互联网不正当竞争类型化条款“仅规定互联网领域的特殊行为，传统不正当竞争行为在互联网领域的延伸部分，适用相应的条款调整”〔51〕。事实上，此举也有利于及时纠正实践中出现的不当援引互联网不正当竞争类型化条款来处理传统不正当竞争行为的错误做法。例如，在“福州神康医院与平潭精神病防治院不正当竞争纠纷案”中，尽管该案发生于互联网领域，带有互联网因素，但涉案行为（使用他人企业名称作为关键词进行的网络宣传推广行为）本质上与传统的商业混淆行为并无二致。此时，不能仅凭借助互联网平台实施争议行为所依托的实施环境、发布媒体等背景差异选择转向互联网不正当竞争类型化条款的规制路径。〔52〕

（二）厘定类型化条款与一般条款的逻辑关系

厘清类型化条款与一般条款之逻辑关系，旨在化解互联网不正当竞争类型化条款适用中出现的规范外部适用的形式逻辑矛盾。本文主张，今后法院在处理互联网不正当竞争类型化条款与一般条款关系时应当采取“二元协作评价路径”，理由在于：一方面，将一般条款与具体条款结合加以适用的做法不仅能够满足人们对于法秩序的确定性需求，也能使法院在未来实践中创制相应的具体规则，确保法律规范具有足够的生命力。〔53〕另一方面，这是有效克服互联网不正当竞争

〔49〕 参见谢兰芳：《论互联网不正当竞争中消费者利益的保护》，载《知识产权》2015 年第 11 期。

〔50〕 参见前引〔5〕，蒋舸文。

〔51〕 前引〔2〕，孔祥俊书，第 531 页。

〔52〕 参见曹丽萍、张璇：《网络不正当竞争纠纷相关问题研究——〈反不正当竞争法〉类型化条款与一般条款适用难点探析》，载《法律适用》2017 年第 1 期。

〔53〕 参见〔奥〕恩斯特·A. 克莱默：《法律方法论》，周万里译，法律出版社 2019 年版，第 43 页。

类型化条款逻辑缺陷及其解释难题的必然选择。其中现有类型化条款的逻辑缺陷主要体现为规范设置的“非互斥性”与“非周延性”。前者表征的是列举条款所涉的互联网不正当竞争行为类型之间构成交叉重叠关系，而非应然层面的互斥关系，故可能导致同一行为被不同列举条款所共同涵括；后者是指列举条款针对互联网不正当竞争行为的类型归纳有限，无法有效覆盖其他典型的不正当竞争行为形态，诸如“不当抓取他人数据行为”。〔54〕现有类型化条款的解释困境源于规则本身具有的抽象性与模糊性，这不仅体现在规范构造方面，也反映在具体条文较为含糊的概念表述之中。〔55〕前述类型化条款中的逻辑缺陷与解释难题不仅会极大降低规则在实践中的适用性与操作性，也会诱发相关互联网不正当竞争案件变成“临界案件”〔56〕甚至“疑难案件”〔57〕之风险。在此背景下，通过引入更具涵括性与本质性的一般条款的综合分析，将成为处理此类不正当竞争纠纷的合理选择。

在个案中，根据具体规范选取的不同，此种“二元协作评价路径”实际上将包括“弱二元协作评价”与“强二元协作评价”两种形式。析言之，当对涉案互联网竞争行为表现进行考察后，初步得出结论其应当援引的裁判依据为互联网不正当竞争类型化条款中的列举条款，但由于缺乏对相关规范适用构成要素的清晰界定，为了避免法律适用过程中可能出现的滥用与误用等异化情形，法院虽有必要结合一般条款对涉案行为加以共同评价，但鉴于列举条款所描述的行为类型指向相对明确，故一般条款的引入更多是检验类型化条款的具体适用是否有违其所确立的正当性判定的基本标准。不难看出，此种“弱二元协作评价”得以采纳应当符合如下前提限定：一是个案情形在外观上符合列举条款所规定的行为特征，需纳入列举条款的规制范围；二是法院就涉案情形适用列举条款时对相关规范构成适用要素存疑。而在行为评价的具体作用方面，一般条款所发挥的主要是一种相对较弱的辅助论证功能。相较而言，当法院认定涉案事实可落入互联网不正当竞争类型化条款中的兜底条文时，囿于该规定针对不正当竞争行为的构成要件并不完整，此时便有必要结合一般条款来对涉案行为的法律属性进行界定。采取“强二元协作评价”的原因主要在于个案中所援用的规则指向兜底条文，但其无法提供有效的不正当竞争认定标准。而在评价作用定位层面，一般条款的引入将会在实质层面发挥出较为独立的补充评价效力。

（三）构建统一的规范要件适用程式

为了避免互联网不正当竞争类型化条款适用中出现前述的内部形式逻辑矛盾，殊有必要构建一套一致性的规范适用程式，以实现互联网不正当竞争认定标准与裁判结果的双重统一。

1. 前置的竞争关系

“前置的竞争关系”旨在肯定竞争关系之于互联网不正当竞争认定所具有的前提限定价值。在个案中，法院应当坚持审查是否存在竞争关系，将其作为适用互联网不正当竞争类型化条款的

〔54〕 相关典型案件可参见由北京市海淀区人民法院审理的“抖音诉刷宝不正当竞争纠纷案”与“新浪微博诉超级星饭团不正当竞争纠纷案”。

〔55〕 参见黄军：《视频网站商业模式竞争法保护的反思与完善》，载《时代法学》2019 年第 3 期。

〔56〕 “临界案件”是就某一案件是否可被纳入相关法律条文的涵摄范围存在争议。参见杨仁寿：《法学方法论》（第二版），中国政法大学出版社 2013 年版，第 113 页。

〔57〕 疑难案件是指在法律的理解与适用方面存在争议的案件。参见孙海波：《不存在疑难案件?》，载《法制与社会发展》2017 年第 4 期。

先决条件。当经过初步分析后判定原被告双方有竞争关系时，不正当竞争认定便进入下一环节；反之，则随即终止。理据在于：首先，不正当竞争行为的本质为竞争行为，而竞争行为是一种相对性行为，即行为发生于竞争对手之间，这就意味着不正当竞争只能存在于竞争者之间。〔58〕互联网不正当竞争行为无出其外。其次，基于互联网经济对传统竞争模式的颠覆进而否定竞争关系之于行为正当性的前提要件意义，是对竞争关系相对性的误读。尽管泛诸互联网领域的跨界竞争不同于以往传统行业的直接竞争，但从根本上看，其竞争的目的仍在于努力获得另一个人同时也在努力获得的东西，〔59〕这一过程并未脱离基本的竞争关系框架。最后，梳理域外同类立法安排与司法实践后不难发现，主要国家（德国与美国）在规范经营者之间的竞争秩序时，通常也未放弃考察竞争关系因素。〔60〕当然，在理解互联网领域的竞争关系时，有必要结合这一领域的行业分工日趋细化、业务交叉重合逐渐盛行的既有现实，采取相对宽泛的阐释。

2. 合法的竞争利益

一方面，《反不正当竞争法》第 12 条将互联网不正当竞争行为的侵害客体规定为“其他经营者合法提供的网络产品或者服务”，实则已经蕴含立法者对于“合法的竞争利益要素”的明确要求；另一方面，法院运用互联网不正当竞争类型化条款来处理此类纠纷时，往往也会重视对原告合法竞争利益的具体分析。

当然在个案中分析合法竞争利益要素时，应当避免陷入如下误区：一是泛化合法竞争利益。原告享有的合法竞争利益是有具体指向的，且可被直接证实，不能将整个互联网行业所集聚或者形成的共有利益直接归于个体的竞争利益。例如，将存在于互联网视频领域“免费＋广告”商业模式所产生的竞争利益等同于特定经营者享有的竞争利益便有待斟酌。二是固化合法竞争利益。竞争机制是一种优胜劣汰的效能竞争机制，竞争者应当依靠优质优价的产品或者服务（即经营活动业绩与优势）开展有效竞争。〔61〕当互联网领域出现新的竞争业态并逐渐取代旧竞争业态时，新的竞争利益势必会对既有的竞争利益构成根本威胁与挑战，基于前述效能竞争理论考量，此时便不应继续坚持对原有竞争利益的固化保护，而应强调竞争利益的动态性与可更迭性。

3. 特定的竞争行为

在现有规范框架下，法院适用互联网不正当竞争类型化条款来判断涉案竞争行为正当性时，需要立足于如下几个方面进行体系化考量。

一是行为手段的技术性，即互联网不正当竞争是“利用技术手段”实施的。在个案中判定是否使用技术手段方面，除了技术特征较为明显的情形以外，本文认为，对于疑难复杂案件可采取“反向推定＋举证否定”的分析方法，即原告或者法院基于相关互联网专业人士的分析意见得出“非由技术手段而无法实现”判断时，除非被告通过举证证明未采用技术手段，否则应当作出肯定式结论。

二是行为方式的影响性，即互联网不正当竞争必须是通过“影响用户选择或者其他方式”实

〔58〕 参见焦海涛：《不正当竞争行为认定中的实用主义批判》，载《中国法学》2017 年第 1 期。

〔59〕 参见〔英〕哈耶克：《个人主义与经济秩序》，邓正来译，复旦大学出版社 2012 年版，第 106 页。

〔60〕 参见前引〔41〕，黄武双、谭宇航文。

〔61〕 参见郑友德、范长军：《反不正当竞争法一般条款具体化研究——兼论〈中华人民共和国反不正当竞争法〉的完善》，载《法商研究》2005 年第 5 期。

现。其中“影响用户选择”含义相对明晰；“其他方式”则主要指向的是“影响经营者经营”。因为就行为指向而言，某一互联网不正当竞争行为不是针对相关用户，便是针对市场上其他经营者的经营活动。〔62〕

三是行为表现的多样性。互联网不正当竞争类型化条款将该语境下不正当竞争行为的表现形式概括为“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”，即网络干扰行为。当然由于兜底条文的设置，也就保留了互联网不正当竞争表现形式的其他可能性。

四是行为过错的明显性。依据现有规范文本，互联网不正当竞争类型化条款所涉的不正当竞争行为的主观过错包含故意与一般过失及以上的形态，两者均具有明显性。因为就保护对象而言，互联网不正当竞争类型化条款保护的并非法定权利，而是成熟度较低的利益。这样一来，只有当明显违反相关领域中需要遵守的注意义务、存在明显过错时，方可认定构成不正当竞争，否则便有可能引致市场行为动辄得咎、过度限制自由竞争的消极后果。〔63〕

4. 多元的竞争损害

虽然现有类型化条款将互联网不正当竞争的形式损害表述为“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”，但实质的利益受损形式则可从不同维度进行把握。

一是直接意义上的竞争利益受损。在适用互联网不正当竞争类型化条款时，首要的利益衡量在于考察个案中相关经营者的竞争利益受损情形，尤为需要注意以下方面：在损害对象方面，其既有可能是初始的竞争利益损害，也有可能涉及衍生的利益损害。在损害程度方面，其既涵括相对轻微的损害形式——“妨碍”，也牵涉较为严重的损害后果——“破坏”。前者是指互联网不正当竞争虽然导致他人网络产品或者服务造成阻碍，但仍可运行；后者则是导致他人的网络产品或者服务直接陷于瘫痪或者部分功能受损。〔64〕在损害发生状态方面，其既包含现实发生的损害，也涉及可能发生的损害。

二是独立意义上的消费者利益受损。随着反不正当竞争法由传统向现代的转变，消费者利益作为不正当竞争认定的一项独立考量因素的重要性日渐凸显。〔65〕事实上，“在用户为王、消费者主导市场经济发展风向标的互联网时代，消费者居于市场竞争法的核心，消费者利益一改既有的依附地位，成为反不正当竞争法的直接保护法益”〔66〕。结合 2022 年《最高人民法院关于适用〈中华人民共和国反不正当竞争法〉若干问题的解释》来看，这样一种转变也得到了直接体现。〔67〕就互联网不正当竞争类型化条款的司法适用而言，在根据消费者利益受损情况来认定涉案行为正当性时，其具体的考量内容虽牵涉消费者的知情权、隐私权以及选择权等不同方面，〔68〕

〔62〕 事实上，早先的《反不正当竞争法（修订草案送审稿）》与《反不正当竞争法（送审稿）》中，“影响用户选择”与“干扰其他经营者正常经营”也是并列呈现的。

〔63〕 参见王文敏：《反不正当竞争法中过错的地位及适用》，载《法律科学》2021 年第 2 期。

〔64〕 参见焦海涛：《互联网不兼容行为的规制路径选择》，载《财经法学》2020 年第 5 期。

〔65〕 参见孔祥俊：《论反不正当竞争法的现代化》，载《比较法研究》2017 年第 3 期。

〔66〕 陈耿华：《我国竞争法竞争观的理论反思与制度调适——以屏蔽视频广告案为例》，载《现代法学》2020 年第 6 期。

〔67〕 该解释第 21 条第 2 款规定：“仅插入链接，目标跳转由用户触发的，人民法院应当综合考虑插入链接的具体方式、是否具有合理理由以及对用户利益和其他经营者利益的影响等因素，认定该行为是否违反反不正当竞争法第十二条第二款第一项的规定。”

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

但真正具有决定性意义的当属消费者的自由决策利益。因为互联网不正当竞争行为对消费者利益的损害本质上体现为通过扭曲消费者的消费决策进而改变消费取向。〔69〕

三是整体意义上的公共利益受损。具体到互联网不正当竞争认定领域，其是指一种不受扭曲的互联网行业的整体竞争秩序。在个案中分析互联网领域的公共利益受损情形时，需要注意如下几个方面：（1）不应简单地将消费者利益与公共利益混同。两者虽有重合，但并不等同，在某些情形下可能存有明显的抵牾。（2）不应简单地将技术进步或者创新直接视作公共利益，而应以技术进步或者创新是否有利于促进与形塑良好的互联网竞争秩序，是否有助于提升社会公众可获得的总体福利作为最终依据。（3）不应片面以道德分析替代经济分析作为认定是否符合公共利益的标准。道德分析标准本身是一种模糊性的标准，〔70〕经济分析的适时引入可弥补道德分析的内在不足，确保公共利益受损认定标准的客观性。

5. 合理的竞争抗辩

此处的抗辩事由专指狭义的抗辩事由，即前述适用要件之外的影响互联网不正当竞争行为认定的有关理由。结合现有规范文本以及司法实践来看，其中可能且合理的竞争抗辩事由主要涉及“技术抗辩”。

在互联网不正当竞争司法实践领域，选择确立技术创新作为抗辩事由背后的理据考量主要在于：其一，顺应了鼓励互联网行业发展的现实需要。以网络技术作为基础支撑的互联网行业，无论是早期的诞生，还是当下的广泛普及，技术创新基本上构成了其发展的原动力。其二，契合了互联网市场竞争的内在属性与市场优先调节理念。互联网领域的市场竞争具有突出的创造性破坏属性，即奉行优胜劣汰和适者生存法则的动态竞争。〔71〕一项互联网新技术的运用，难免加剧经营者之间的竞争对抗与利益冲突，造成不同程度上的市场竞争损害，此时司法干预机制不应急于替代居于优先地位的市场调节机制，而应保持必要的审慎与克制，做到“市场的归市场”。因此，技术创新抗辩的存在，不仅能够为互联网领域合理的技术竞争预留必要的竞争空间，也可以进一步促进互联网行业的技术创新与发展。

在具体适用互联网不正当竞争类型化条款时，处理技术抗辩事由有必要把握如下内容：（1）注重技术创新的类型辨识。涉案的技术创新究竟是“真创新”还是“伪创新”？是“颠覆式创新”还是“微创新”？针对不同类型的创新，最终的抗辩事由采纳也将具有差异性。（2）强调技术创新的利益衡量，即技术创新抗辩的适用应当以提升社会总体福利作为宗旨。正如最高人民法院在“360 扣扣保镖案”中所指出的，“是否属于互联网精神鼓励的自由竞争和创新，仍然需要以是否有利于建立平等公平的竞争秩序、是否符合消费者的一般利益和社会公共利益为标准来进行判断”〔72〕。（3）重视技术创新与技术中立的区分。技术本身固然是中立的，但技术的不当使用却可以蜕变为不正当竞争的实施工具，因而技术中立并不能直接作为抗辩事由；而技术创新虽是立足于技术中立基础之上，但其进一步要求技术运用之于行业竞争、消费者利益以及公共利益的客观

〔69〕 参见谢晓尧：《在经验与制度之间：不正当竞争司法案例类型化研究》，法律出版社 2010 年版，第 17 页。

〔70〕 参见张占江：《不正当竞争行为认定范式的嬗变：从“保护竞争者”到“保护竞争”》，载《中外法学》2019 年第 1 期。

〔71〕 参见孔祥俊：《论反不正当竞争的基本范式》，载《法学家》2018 年第 1 期。

〔72〕 最高人民法院（2013）民三终字第 5 号民事判决书。

积极效果，故而可以成立相应的抗辩事由。

五、结　语

当前随着互联网经济开始步入“促进发展与规范管理相统一”的新发展阶段，通过深入推进与改进该领域尤其是新业态反不正当竞争规制，依法构建规范有序的竞争环境，防止资本无序扩张，进而营造开放、健康、安全的网络生态，已然成为完善我国社会主义市场经济体制、推动高质量发展的题中之义与内在要求。在此背景下，如何充分有效发挥作为判定网络领域竞争行为正当性的基础性条文——互联网不正当竞争类型化条款——自身所具有的规范作用，是横亘在理论界与实务界面前的一道难题。针对该规范所展开的具体研究，显然不能仅停留于法解释学维度的理论探讨，而应当重视结合法实证分析维度的现实考察。就司法实践层面而言，相关研究除了有必要全面梳理互联网不正当竞争类型化条款的适用形态以外，更为关键的在于深入剖析规则在现实运行中所面临的缺陷与弊端，诸如前述的“规范适用结构上面临‘泛化’与‘虚化’困境”“规范适用逻辑关系上呈现明显对立性”“规范适用构成要件解析上缺乏一致性”等，并最终以此为立足点寻求有针对性的改进对策，才能为互联网行业的良性有序发展提供科学合理且行之有效的规范支撑。

Abstract: The internet unfair competition typed clause conforms to the regulation demand of competitive behavior in the field of internet at the level of institutional supply. There are three judicial operation modes of internet unfair competition typed clause: independent application, dual application and ternary mixed application. In judicial practice, the existing typed clause is faced with the dilemma of “generalization” and “emptiness” in the structure of the application of norms, showing obvious opposition in the logical relationship of the application of norms, and lacking consistency in the analysis of the constituent elements of the application of norms. There are three ways to optimize the judicial application of the internet unfair competition typed clause. The first is to clarify the specific positioning of the application of different norms by clarifying the homogeneity of the application interpretation of the general clause, clarifying the direction of the application objects of the listed clauses and highlighting the distinction of the application functions of the declaration clause. The second is to adopt the “dual collaborative evaluation path” to clarify the external logical relationship between the typed clause and the general clause. The third is to build a unified application program of “pre-competitive relationship＋legal competitive interest＋specific competitive behavior＋multiple competitive damage＋reasonable competitive defense”.

Key Words: anti-unfair competition law, internet unfair competition, typed clause, general clause

（责任编辑：缪因知　赵建蕊）

财经法学 No. 3，2022
pp. 29 - 42

论数字时代的美术作品原件
——基于展览权的视角

李　强*

内容提要：美术作品原件是我国著作权法上展览权的核心概念，然而却未得到应有的关注。面对新技术、新业态提出的新挑战，无论是传统美术作品还是数字化美术作品，都存在着如何理解和认定美术作品原件的困惑。对此，有必要突破著作权法上关于美术作品必有原件、美术作品原件唯一和美术作品原件必为实体等传统认识，顺应技术发展的要求，紧紧抓住可展览性和不可替代性两个关键特征来构建美术作品原件的概念，并创建认定美术作品原件的一般规则。对于数字化美术作品，在满足“间接”可展览性的前提下，可以借助 NFT 技术将数字化美术作品完成时所形成的电子文档认定为作品原件。

关键词：美术作品　作品原件　展览权　NFT

一、问题的提出

在众多著作财产权当中，展览权只是一个不起眼的小权利，但在现实生活中却有着大应用。近几年来，我国文博事业取得了大发展、大繁荣，从法律的角度而言，其兴旺发达最重要的权利基础就是展览权。我国著作权法上的展览权正是基于美术、摄影作品的原件或复制件（以下或简称为“作品原件或复制件”）而定义的，即“公开陈列美术作品、摄影作品的原件或者复制件的权利”（《著作权法》第 10 条第 1 款第 8 项）；与展览权相关的第 20 条则几乎是作品原件的定制条款，〔1〕可见作品原件在展览权中的重要性。

* 李强，武汉大学图书馆/万林艺术博物馆馆员。

本文为国家社科基金项目“当前国际版权制度发展趋势与我国路径选择研究”（17BFX117）、国家市场监督管理总局发展研究中心项目“数字经济时代知识产权保护与反垄断规制创新研究”的阶段性成果。

〔1〕《著作权法》第 20 条第 1 款规定作品原件所有权转移后原件展览权的归属，第 2 款解决原件受让人展览未发表的作品原件与作者发表权之间的冲突。

文化生活中，展示原件是举办文博类展览的基本要求和行业惯例，特别对美术作品而言更是艺术家展现创作才能、提高艺术声誉的主要途径，亦是美术作品实现艺术价值的主要方式。司法实践中，早年的“蔡迪安等与湖北晴川饭店有限公司等著作权侵权纠纷上诉案”（即《赤壁之战》壁画案）〔2〕曾引发大量的学术讨论，案件起因即为绘制于饭店墙壁上的唯一壁画原件遭到毁损灭失。近年来，再次引发诸多学术兴趣的“钱钟书书信拍卖案”〔3〕和“茅盾手稿拍卖案”〔4〕也聚焦于两位先生的手稿原件及其展览权，引来法院判决和学者观点的分歧甚至对立。〔5〕还有判例将“音乐喷泉喷射效果的呈现”认定为美术作品，〔6〕那么音乐喷泉的喷射就是在公开展示美术作品，学者对此也表示了明确的反对意见。〔7〕作为展览权的主要客体，如果充分认识到美术作品原件的展示并不限于美术馆、博物馆、会展中心等专门场馆，还包括商场（含任何借助展示美术作品而进行营销的现场）、酒店、宾馆甚至街道等数量庞大的公众场所，〔8〕那么，讨论美术作品原件既有重要理论价值又有重大实践意义，也充分展现了本文研究的问题导向。

然而，从法学角度对美术、摄影作品原件展开的研究非常少见。目前有限的国内研究主要集中在对现行《著作权法》第 10 条第 1 款第 8 项（展览权的定义）和第 20 条第 1 款〔9〕的理解与适用上。比如，作品原件转移后原件展览权的归属，〔10〕作品原件转移后由原件所有人享有原件展览权则引出了作品原件所有权和作品著作权之间的冲突与协调〔11〕。英文领域的研究则主要关注在公共场所展示宗教物品的政教分离条款（the establishment clause）或展示艺术品的言论自由等美国宪法第一修正案，〔12〕以及数字图书馆、Twitter 等社交平台的网上展示，〔13〕极少提及作品原件或复制件。

〔2〕 参见湖北省高级人民法院（2003）鄂民三终字第 18 号民事判决书。

〔3〕 参见北京市第二中级人民法院（2013）二中保字第 9727 号民事裁定书。

〔4〕 参见江苏省南京市中级人民法院（2017）苏 01 民终 8048 号民事判决书。

〔5〕 参见金海军：《论书信上的物权、著作权与隐私权及其相互关系——从“钱钟书书信拍卖案”谈起》，载《法学》2013 年第 10 期；李翔、曹雅晶：《失落的展览权——从“钱钟书书信拍卖案”谈起，兼论〈著作权法〉第十八条之理解》，载《中国版权》2014 年第 4 期；石超：《手稿著作权客体类型探究——基于“茅盾手稿案”的分析与思考》，载《中国出版》2019 年第 1 期；陈瑞雪：《论文字作品的亲笔手稿著作权保护问题——以茅盾先生手稿著作权纠纷案为例》，载《福建法学》2019 年第 1 期。

〔6〕 参见北京知识产权法院（2017）京 73 民终 1404 号民事判决书。

〔7〕 参见王迁：《论作品类型法定——兼评“音乐喷泉案”》，载《法学评论》2019 年第 3 期；李扬：《著作权法基本原理》，知识产权出版社 2019 年版，第 72 页。

〔8〕 相关案例可参见北京市第二中级人民法院（2003）二中民终字第 5951 号民事判决书；北京市东城区人民法院（2007）东民初字第 03991 号民事判决书；湖北省武汉市中级人民法院（2010）武知初字第 66 号民事判决书；天津市第一中级人民法院（2016）津 01 民终 6756 号民事判决书。

〔9〕 该款规定：“作品原件所有权的转移，不改变作品著作权的归属，但美术、摄影作品原件的展览权由原件所有人享有。”

〔10〕 参见李明德、管育鹰、唐广良：《〈著作权法〉专家建议稿说明》，法律出版社 2012 年版，第 97－98 页；郑成思：《版权法》（上），社会科学文献出版社 2016 年版，第 321 页。

〔11〕 参见王福珍：《作品原件所有权与作品著作权的冲突及解决方案》，载《法学》1993 年第 9 期；郭玉军、向在胜：《论美术作品著作权与原件所有权》，载《湖北美术学院学报》2001 年第 3 期；唐昭红：《论美术作品著作权对美术作品原件所有权的限制》，载《法商研究》2003 年第 4 期。

〔12〕 See Christina A. Mathes, Bery v. New York: Do Artists Havea First Amendment Right to Sell and Display Art in Public Place? 5 *Villanova Sports & Ent. Law Journal*, 103 (1998); Susan L. Trevarthen, Johanna Lundgren, Merry Litigation and Happy Attorney's Fees: Holiday Display on Downtown Public Property, 85 *Florida Bar Journal*, 19 (2011).

〔13〕 See David R. Hansen, The Public Display of Digital Library Collections, 14 *N. C. Journal of Law & Technology*, 145 (2012); Jie Lian, Twitters Beware: The Display and Performance Rights, 21 *Yale Journal of Law & Technology*, 227 (2019).

笔者在梳理这些研究时发现一个令人困惑的现象，即围绕展览权或美术作品原件展开的探讨似乎将美术作品原件本身当成一个不用言说、不言而喻的概念。但是，越来越多的艺术创新对这种“想当然”提出了有力的挑战。比如，用无人机编队或烟花燃放形成的艺术造型，用蘸水的笔在地面上写出的书法，还有将发型认定为立体美术作品的判例。〔14〕在这些美术创作中，什么是美术作品的原件，美术作品是不是必有原件？人类已经进入数字社会，元宇宙也开始占据大众的视野，数字财产的价值和重要性渐次攀升。传统时代，美术作品的原件是有体物；数字时代，作为一种数字财产形式，数字美术作品的原件又是什么？近两三年来，越炒越热的 NFT（non-fungible token，不可互替通证或非同质化代币）艺术作品逐渐成为数字时代收藏界的新宠和吸引流量的焦点，时不时报道出来的巨额拍卖令人咋舌。NFT 艺术作品即为经由 NFT 技术加持的数字美术作品，那么，使用画图软件在电子屏幕上绘制一幅美术作品，呈现在屏幕上的画面，由该作品形成的电子文档，存储电子文档的内存模块或硬盘、光盘，还有制作出来的第一份纸版作品，哪一个是原件？

为此，本文在辨析作品原件和作品载体之间关系的基础上，从实践出发，基于展览权的角度纳入适当的考量因素，构建了可以兼顾传统美术作品和数字美术作品的美术作品原件概念，并创建了认定美术作品原件特别是数字美术作品原件的若干规则。

二、作品原件和作品载体的关系辨析

根据我国著作权法，展览权的客体是美术作品和摄影作品，客体的载体是作品原件或复制件（以下或简称为“作品制件”），其本身也是物权的客体。

（一）作品载体学理分类的局限性

通说认为，作品必须通过一定的形式表达，才能被他人感知；采取一定的形式固定，才能得到法律的保护。这不仅是作品创作的本质属性和实际需要，也是国际条约（《伯尔尼公约》第 2 条第 2 款）和相关立法例为作品提供法律保护的基本要求。这种固定的形式就是作品载体。

根据物理特性不同作品载体可以分为固定载体和瞬间载体，前者指有形的物质实体，后者指无形的物质，如口头作品之声波、表演作品之动作，数字作品的无形载体是电子脉冲。根据是否为首次依附分为原始载体和复制载体，前者又称原件，“是作品最初所附的载体”，后者又称复制件，“是承载原始载体上之作品的载体”〔15〕。

然而，与实践对比不难发现，除了通过最传统的纸笔或刻刀等方法创作的如著作手写稿、绘画、雕塑等作品外，上述原始载体和复制载体的分类不能直接用于确认作品的原件或复制件。比如，用计算机撰写的著作，其原始载体是电子脉冲，复制载体是硬盘、优盘等存储器，但什么是该作品的原件却颇费思量。再如，口述作品的原始载体是无形的声波，复制载体是固定声波的磁带；而在大众认知中，录音棚或现场录制的母带是原件，从母带翻录的都是复制件。

〔14〕 参见“何吉与杭州天蚕文化传播有限公司著作权纠纷上诉案”，浙江省杭州市中级人民法院（2011）浙杭知终字第 54 号民事判决书。

〔15〕 杨述兴：《论作品与载体的关系》，载《知识产权》2012 年第 6 期，第 42 页。

所以，作品载体的上述分类主要是一种学理认识，不能满足实践的需要。真正具有法律意义的作品载体是固定载体或称为实体载体，如《著作权法》及实施条例多次提到的作品原件或复制件。具体到美术作品原件亦是如此，比如，“美术作品的‘原件’，也就是通常所说的‘原稿’，或者是‘原本’、‘底本’”〔16〕；“美术作品必须被固定在物质载体上，不能像口述作品那样脱离物质载体而存在，否则也不可能有‘原件’和‘复制件’的区分了”〔17〕。

（二）其他作品原件和美术作品原件在司法实践中存在重要差异

从司法实践来看，对于美术、摄影作品以外的其他作品，作品原件的法律意义主要体现在由于没有备份而毁损丢失时会导致整个作品的灭失。比如，在被称为国内首例教案纠纷的“高丽娅诉重庆市南岸区四公里小学著作权纠纷案”中，〔18〕被告弄丢了原告 12 年间历次上交的大部分教案本（无备份）。其实，即便原告诉称被告遗失其作品原件系侵犯了其著作权，法院仍倾向于将之认定为侵犯了原告对作品原件的所有权，如“沈金钊诉上海远东出版社图书出版合同案”〔19〕和“邱传海与湖北电视剧制作中心等返还作品赔偿纠纷案”〔20〕（以下简称“邱传海案”）。在这两个案例中，原告的诉求都包括追究被告遗失其作品原件的著作权侵权责任，但是终审法院都没有支持原告的诉求，而是认定为涉及作品原件的财产权纠纷进行判决。

就美术、摄影作品以外的其他作品原件而言，从上述及类似案例可以得出三个重要推论。一是如果存有复制件，作品原件是否丢失无关紧要。二是如果缺乏复制件，作品原件的作用主要体现为是作品的唯一载体，一旦灭失即意味着整件作品的灭失，至于是什么形式的载体并不重要。三是作品原件彰显的主要是使用作品的财产价值，而不是其本身的价值。比如，在邱传海案中，原告就诉称由于被告遗失其唯一的相关手稿原件，导致有关合作方取消了原告书籍的出版和电视剧的拍摄，造成了财产损失。

但是，如果涉案作品原件有可能构成美术作品原件，则不仅会关联展览权，而且侵权认定的性质也完全不同。比如，在“钱钟书书信手稿拍卖案”和“茅盾手稿拍卖案”中，法院判决和学理研究均认为，在著作权法上，钱钟书先生和茅盾先生的手稿既是文字作品又是书法类美术作

〔16〕 李建国主编：《〈中华人民共和国著作权法〉条文释义》，人民法院出版社 2001 年版，第 136 页。

〔17〕 前引〔7〕，王迁文，第 24 页。

〔18〕 原告原为被告所属教师，每学期按照被告的安排编写和上交教案，自 1990 年至 2002 年先后交给被告教案本 48 册。在原告要求返还教案本后，被告只返还了 4 册，其余 44 册被被告以销毁或者变卖等方式处理，下落不明。原告起诉被告要求其返还教案本并赔偿经济损失。原告在以物权纠纷起诉、上诉和申诉均败诉后，转以著作权纠纷为由起诉，最终胜诉。参见重庆市第一中级人民法院（2005）渝一中民初字第 603 号民事判决书；重庆市第一中级人民法院（2005）渝一中民再终字第 357 号民事判决书。

〔19〕 原告按照出版合同约定将其唯一的手稿原件交由被告出版社出版，后被告将手稿的前两千页遗失。原告诉求之一即为被告侵犯了其对手稿原件的著作权。一审法院支持了原告请求，但二审法院认为被告侵犯了原告对书稿原件享有的所有权而非作品著作权。参见上海市第一中级人民法院（1997）沪一中民终（知）字第 1469 号民事判决书。

〔20〕 20 世纪 80 年代后期至 90 年代，原告在先后三次参加被告组织的职称评审过程中，提交了包括文学剧本、电视剧分镜头剧本和著作手稿在内的大量作品手稿，绝大多数没有备份。评审结束后，原告多次向被告索要手稿材料无果，遂诉至法院。虽然湖北省检察机关在办案过程中找到了部分手稿（约 150 万字）并发还作者，但仍有 70 余万字的手稿材料没有找回。该案历经区、市、省三级人民法院和最高人民法院多次审理，原告虽然胜诉，但是湖北省高级人民法院的再审判决没有认可原告提出的著作权侵权主张，最高人民法院的再审判决也没有认可最高人民检察院提出的著作权侵权的抗诉意见，而是认定该案为“主张返还作品手稿原物及赔偿损失的物权纠纷”，维持了湖北省高级人民法院的再审判决。参见湖北省高级人民法院（2009）鄂民监二字第 10 号民事判决书；最高人民法院（2012）民抗字第 50 号民事判决书。

品，后者即为展览权的客体。〔21〕在这一类案例中，被告的涉案行为在侵犯原告物权的同时也可能侵犯了著作权，法院还需要判定被告公开展示美术作品原件的行为是否侵犯了原告的展览权。换言之，在涉及美术作品原件的案例中，即使存有海量复制件，作品原件本体的毁损或丢失即属于重大损失；作品原件本体不存，与其不可分离的原件展览权也归于消灭。

所以，上述针对其他作品原件的三点重要推论不能类推适用于美术作品的原件。主要原因在于美术作品与美术作品原件不可分离，以及美术作品原件所具有的可展览性。应该说，这两点都是美术作品原件的本质属性，且可展览性既是现行立法赋予美术作品原件的法律属性，又是其区别于其他作品原件的关键特征。《美国版权法》第 101 条定义的“公开展示权”不仅包括直接展示，还包括通过胶片、幻灯片、电视图像或任何其他设备或程序展示作品的载体；换言之，既包括直接展示和间接展示，也包括现场展示和网上展示。与之相比，一方面，我国的展览权定义没有使用诸如“借助其他任何设备或方法”的用语，应当是“直接展示”作品的载体即原件或复制件，不包括“间接展示”。另一方面，在我国著作权法的架构中，现场播放视频的展示行为适用放映权，现场网上展示作品适用信息网络传播权，只有现场直接展示作品原件或复制件本身才适用展览权。所以，在我国著作权法的语境下，美术作品原件的可展览性就是指不需要借助任何设备或方法在现场直接展示原件本身亦即作品载体。

对于传统美术作品如绘画、书法、雕塑等，不论原件还是复制件都具有可展览性，展示作品载体就是展示作品本身，作品原件就是作品的原始载体，复制件就是复制载体。对于数字化美术作品，展示储存作品电子文档的内存模块或硬盘、光盘等载体不能得到展示作品的效果，即这些载体不具有可展览性，不能认定为展览权意义上的原件或复制件，尽管可以作为作品的原始载体或复制载体。所以，有学者指出，“‘原件’这一概念仅于传统创作形式的美术作品之上才有意义，才能体现出原件与复制件之差异”〔22〕。摄影作品存在同样的问题，传统的胶卷可以作为原始载体，但不能作为原件；数码相机里的存储卡可以作为原始载体，也不能作为原件。正是因为数字化美术作品的原件和载体之间的关系迥异于传统美术作品，才导致不易判定数字化美术作品的原件，这也是技术的发展对著作权立法提出的具体挑战。所以，在构建美术作品原件的概念和创建美术作品原件的认定规则时，必须将数字化美术作品的特殊性纳入考量。

三、构建美术作品原件的概念

（一）两个重要区别

1. 美术作品原件与复制件的区别

无论对创作者、观赏者还是所有者而言，美术作品的原件和复制件在价值上相差悬殊，本身存在着质的不同。尤其是作品原件与作者之间存在着强烈的人身联系，在精神和经济上均具有特殊重要的价值，蕴藏着作者最原初的艺术才情、创作技巧和身心投入，不能为复制件或任何同主题的再

〔21〕 参见前引〔5〕，金海军文；前引〔5〕，陈瑞雪文。

〔22〕 杨明：《文字作品 v. 美术作品：对几个基本理论问题的反思》，载《中外法学》2009 年第 2 期，第 261 页。

创作所替代，与美术作品不可分离。在文博行业，不论是文物还是艺术品，以展览真品和原件为基本原则和最低要求，观众也以欣赏到原物和真迹为最大期盼；如果展出的是复制件或所谓的高仿件，则必须特别标明，尽管这必然会贬损展览的档次。在最能体现美术作品经济价值的拍卖行业，也是以“原件为王”，拍品一般都要附上权威鉴定机构的“验真”证明，否则根本上不了拍卖目录或拍不出高价。所以，无论从哪个方面讲，作品原件都是展览权架构中的核心概念和主要保护对象，因此也突显出准确建构美术作品原件的概念和创建美术作品原件认定规则的极端重要性。

2. 作品原件的唯一性和作为原件载体的物的唯一性的区别

在严格意义上，不存在完全相同的两个物，每个物都是独一无二的，承载作品的原件亦是如此。在数字化技术出现之前，对于美术作品而言可以将作品原件的唯一性和作品载体物的唯一性等同起来，对于摄影作品原件则需要另外讨论。数字化技术出现之后，只能笼统地说，作品原件的唯一性不是其载体物的唯一性，载体物的唯一性也不能决定作品原件的唯一性。对于数字化美术作品，如果使用同样的方法和材质，得到在普通人视觉上一般无二的两份及以上作品，如果均认定为作品原件，那么即可认为其唯一性被打破了；而作为承载作品的物，其相互之间仍然保持了各自的唯一性。

（二）几点重要考虑

从展览权的角度构建美术作品原件的概念，应当将以下几个方面纳入考量。

1. 美术作品的范围

《著作权法实施条例》第 4 条第 8 项规定：“美术作品，是指绘画、书法、雕塑等以线条、色彩或者其他方式构成的有审美意义的平面或者立体的造型艺术作品。”包括纯美术作品和实用美术作品。其中纯美术作品，是指仅能够供人们观赏的独立的艺术作品，比如油画、国画、版画、水彩画等。实用美术作品，是指将美术作品的内容与具有使用价值的物体相结合，物体借助于美术作品的艺术品位而兼具观赏价值和实用价值，比如陶瓷艺术等。〔23〕无需（美术）专业审视就可知道，我们通常认知的美术作品显然比上述规定要宽泛得多，各国立法例中美术作品的范围多数也比较宽泛。对于美术作品的法律界定和范围，既有国际公约的规定（《伯尔尼公约》第 2 条第 1 款），又有学者的细致分析，〔24〕均可借鉴。

实践中，符合大众认知和法律明确规定的美术作品较好判断，困难的是那些非典型的美术作品，比如名家的书信和手稿，还有音乐喷泉喷射效果的呈现和那些具有审美意义的建筑设计图、视觉效果图、手绘地图和模型等，也可以视为美术作品。随着《著作权法》的最新修订确立了“作品类型开放”的立法模式，还会出现更多不常见的美术作品类型，在事实上也增加了认定美术作品原件的难度。

2. 兼顾通过传统方法和通过数字化技术得到的美术作品原件

考察法律释义和学理研究，我国著作权法上美术作品原件的概念是建立在有体物基础之上

〔23〕 参见国务院法制办公室：《中华人民共和国著作权法注解与配套》，中国法制出版社 2017 年版，第 6 页。

〔24〕 参见郭玉军、陈云：《美术作品概念、成立要件及其范围的法律探讨》，载《湖北美术学院学报》2000 年第 2 期；王迁：《论平面美术作品著作权的保护范围——从“形象”与“图形”的区分视角》，载《法学》2020 年第 4 期；赵书波：《美术作品作者财产权益保护研究》，中国艺术研究院 2010 年博士学位论文，第 13－20 页。

的。比如，“美术作品原件，是指美术作品首次固定之有形载体”〔25〕；“作品原件，即作品的原始载体，是指作品在创作完成之时被固定其上的有形物质载体”〔26〕。《伯尔尼公约》第 2 条第 2 款也规定，未以某种物质形式固定下来的作品不受保护。对于用传统方法创作的美术作品，如此理解并无疑义。有疑义的是，如何确定通过数字化技术得到的美术作品的原件。比如，通过画图软件得到一幅美术作品，当作品完成时呈现在显示器上的画面是不是原件，这种呈现是否属于“固定”在载体上。〔27〕《美国版权法》第 101 条规定，用于固定作品的载体，应当具有“足够的长期性与稳定性”，以使作品在不短的一段时间内可以被感知、复制或以其他方式传播。考虑到显示画面的暂时性和该美术作品形成的电子文档在计算机内存上存储的暂时性，显示画面和内存模块似乎不能成为作品原件。由美术作品所形成的电子文档和存储该文档的计算机硬盘或光盘由于不具有我国著作权法所要求的“直接”可展览性，也不能当然地认定为原件。

版画作品和 3D 打印作品的原件也存在类似问题。版画的制作具有特殊性，先制版再印刷。先行制成的模版不是完整的版画作品，〔28〕不能视为版画作品的原件。如果套色印刷一张或若干张版画后，作者为了保证作品的稀缺性而毁掉模版，则印出来的版画作品（不论几张）即为原件似无疑义。如果保留模版，随时都可以印制出同样的版画作品，那么什么才是原件？或者说，在留存模版的情况下，版画作品是不是没有原件、只有复制件，或者印制出来的都是原件？

3. 突破美术作品原件必为物质实体的传统认识

目前理论和实务上均以物质实体为基础来认识美术作品原件，如“美术作品原件，是指美术作品首次固定之有形载体”〔29〕。然而，随着 2020 年 11 月《著作权法》的最新修订，这种传统认识正在发生变化。作为修订的一项重要内容，《著作权法实施条例》第 2 条的作品定义被修改、提升为《著作权法》第 3 条，〔30〕定义中的关键要素“能以某种有形形式复制”改成“能以一定形式表现”。对前者的重要理解之一就是作品可以以某种有形形式固定，而改为“能以一定形式表现”即放弃强调形式的有形，在一定程度上降低了对作品的固定性要求。

换言之，作品是不是必须固定下来，是不是必须以实体的方式存在，已经不是作品的构成要件了。那么，这种改变必然会影响到对美术作品原件的认识。早在二十多年前，日本著名学者就曾预言：“数字技术正在逐步的切断以往传统的著作物商业交易中所见到的无体物对有体物的寄生关系……著作物不再借用有体物的外衣而独立存在，我们面对的是一个全新的局面。”〔31〕《巴西著作权法》第 7 条也规定：“受保护的智力作品是指智力创作成果，而无论其表达形式如何，也无论其以任何有形的或无形的、现在已知的或将来可能开发的载体固定。”〔32〕所以，为了适应

〔25〕 前引〔7〕，李扬书，第 136 页。

〔26〕 曹新明：《作品原件所有人的告知义务研究——兼论〈著作权法〉第三次修订》，载《法治研究》2013 年第 11 期，第 42 页。

〔27〕 有学者认为，数字作品的物质载体是无形的电子脉冲。参见前引〔15〕，杨述兴文，第 41 页。

〔28〕 当然，具有审美意义的模版本身也是一种模型类的美术作品。

〔29〕 前引〔7〕，李扬书，第 136 页。

〔30〕 该条规定：“本法所称的作品，是指文学、艺术和科学领域内具有独创性并能以一定形式表现的智力成果，……”

〔31〕〔日〕北川善太郎：《网上信息、著作权与契约》，渠涛译，载《外国法译评》1998 年第 3 期，第 42 页。

〔32〕《十二国著作权法》，《十二国著作权法》翻译组译，清华大学出版社 2011 年版，第 9 页。

数字经济，有必要前瞻性地改造美术作品原件的传统认识。

4. 突破美术作品原件唯一的传统认识

在学理研究和审判实践中，普遍认为作品原件具有唯一性。前者如，“对于具体的作品而言，每个作品对应的原件具有唯一性”〔33〕；美术作品原件“有着复制件无可取代的价值和唯一性”〔34〕。后者如“成都市黑蚁设计有限公司与东宏实业（重庆）有限公司等著作权纠纷上诉案”，法院认为：“作品原件一旦形成，就具有唯一性，创作者永远也不可能再创作出一件与原件完全一样的美术作品。”〔35〕在用传统手法创作的年代，这种认识无疑是正确的，但是数字技术的发展已经颠覆了这种认识。比如，将电脑绘制的美术作品使用同样的打印机和纸张制作若干纸版，有可能都会被认为是原件。版画作品和 3D 打印作品的原件也是如此。版画的制作一般是先制版再印刷，制好的模版不是完整的版画作品，不能视为版画作品的原件。如果套色印刷一张或若干张版画后，作者为了保证作品的稀缺性而毁掉模版，则印出来的版画作品不论几张都是原件。对此，《法国知识产权法典》第 L.122—8 条第 2 款也规定，作品原件是指由艺术家亲自创作的作品，以及由艺术家亲自或在其指导下完成的限量版作品。所以，对于某些特定的美术作品和摄影作品，作品原件有可能不唯一。

必须指出，突破美术作品原件唯一的传统认识并非认为所有美术作品原件已经不再具备唯一性特征，而是表明唯一性已经不能作为一个能够涵盖所有美术作品原件的绝对特征，但不妨碍其仍可作为绝大多数传统美术作品甚至数字化美术作品的特征。比如近年来火爆全球的 NFT 数字艺术作品，在 NFT 技术的加持下也具备了唯一性。NFT 是在区块链的基础上发展起来的一种加密技术，通过区块链来记载上一个区块数字美术作品计算机文档的哈希值，其中就包括该作品每次流转的所有数据，并形成链接关系。任意一个区块发生人为的删改，后面相连的所有区块哈希值都会发生变化，于是链接上的每个环节都能发现数据被篡改，这样可以有效防止 NFT 数据被随意或恶意篡改。〔36〕同时，根据哈希算法，对数字艺术作品的任何修改都会产生不同的哈希值。因此，他人无法改变数字艺术作品以及链上哈希值而不被发现，也就保证了附有 NFT 数据的美术作品原件的唯一性。当然，这种唯一性并非通常意义上物理实体的唯一，也不是指在数字世界里只有一件数字美术作品，而是在无法篡改的技术保障下通过权属证明表现出来的“唯一”。

5. 坚守美术作品原件的不可替代性

美术作品原件的唯一性与其不可替代性紧密联系，著作权法强调保护美术作品原件的一个主要原因就是其具有不可替代性。如果作品原件可以被替代，变成对创作者、收藏者和观赏者可以旧去新来的物件，法律也就没有必要加强保护了。对于多数传统美术作品，作品原件唯一就意味着不可替代；而对于某些特定的美术作品和摄影作品，突破作品原件唯一的传统认识并非否认其不可替代性。实际上，不可替代性是确认美术、摄影作品原件的关键要素之一。有的学者认为，

〔33〕 袁博：《著作权法解读与应用》，知识产权出版社 2018 年版，第 123 页。

〔34〕 前引〔22〕，杨明文，第 261 页。

〔35〕 重庆市高级人民法院（2005）渝高法民终字第 76 号民事判决书。

〔36〕 参见王功明：《NFT 艺术品的价值分析和问题探讨》，载《中国美术》2021 年第 4 期。

可以将根据底片（胶卷拍照）或数码照片文档（数码拍照）洗印出来的照片均认定为摄影作品原件，〔37〕实际上是否定了原件的不可替代性。必须认识到，正是不可替代才使得美术作品原件稀缺而珍贵。

对于数字化美术作品，NFT 作品的每一个 TokenID（token identity document，代币唯一编码）都是独一无二、无法替代的。〔38〕即通过 NFT 技术，防止篡改和无法消除的权属凭证伴随并记录着该“唯一”美术作品的每一次流转，与其不可分离，在观念上、事实上和法律上都得到公认，保证了 NFT 美术作品的不可替代、不可互换。也许存在跟某件特定 NFT 美术作品数字化质量完全一样的其他 NFT 美术作品或非 NFT 美术作品，但是在 NFT 技术的规则之下，不存在相互替代的可能性。

6. 充实展览权的定义

现行著作权法赋予美术作品原件以“直接”可展览性，即现场直接展示作品原件本身。这对于展示作品载体即是展示作品的传统美术作品没有问题，但是却不能适用于以优盘、光盘为载体的数字化美术作品。当然，也可以将其打印出来展示，然而数字化美术作品的美感和价值更多的时候难以通过打印版展现出来。比如，三维美术作品的最佳展示方式是数字化的多角度展示，像素高度压缩的美术作品需要通过逐渐放大像素的方式来展现细微之美，还有动态的数字化美术作品也无法通过静置的方式展示。而且，同技术发展与时俱进的展览模式经常求新求变，那些比实物静置方式更活泼、效果更好的展览行为其实不受展览权的调整，比如常见的播放视频适用放映权，网上展示作品适用信息网络传播权。所以，有必要充实展览权的定义，参照《美国版权法》的“公开展示权”，明确规定既可以直接展示作品，也可以借助其他设备或方法间接展示作品。换言之，即赋予数字化美术作品以“间接”可展览性。

（三）构建美术作品原件的概念

虽然“作品原件”在我国著作权法中频频出现，却无相应定义。笔者认为，我国著作权法应当明确“美术作品原件”的法律含义。美术作品原件与复制件相对应，其概念必然要反映出二者的区别性，关键在于如何阐释“原”或“原件”的含义。笔者认为至少应当包括以下三个方面。

第一个方面是阐释为在时间上作品“首次”附着于载体或数字化作品的“首次”完成。前者是对传统上作品原件必为实体的理解，作者在载体物上完成作品之时，该载体物即成为原件；我国台湾地区“著作权法”第 3 条第 1 款第 14 项规定“原件指著作首次附着之物”，也是强调时间上的“首次”。后者是突破作品原件必为实体的认识，一幅数字化美术作品完成之时，即首次达到“能以一定形式表现”的法定要求，具备了成为作品原件的可能性。

第二个方面是阐释为作为复制件来源的原始件。原件先于复制件，复制件源于原件。复制可能是“二手”或“三手”，复制的维度也可能经历了二维和三维之间的转换，但是只有最原初的那件作品才是原件。

---

〔37〕 参见前引〔7〕，李扬书，第 137 页。

〔38〕 参见江哲丰、彭祝斌：《加密数字艺术产业发展过程中的监管逻辑——基于 NFT 艺术的快速传播与行业影响研究》，载《法学论坛》2021 年第 4 期；王铼、曹莹：《NFT 的境外法律监管》，载：http://glo.com.cn/Content/2021/05-24/1410013404.html，最后访问时间：2022 年 1 月 2 日。

如果原件已经遗失，作为原件的“一手”复制件，虽然是所有后续复制的来源，但显然不能认定为原件。此时就需要引入第三个方面，即“作者亲自创作完成”，这也正是作品创作的“原初”状态。其实，第一个方面和第三个方面只不过是对同一事实的不同表述而已，作者亲自创作作品过程的结束之时也就是作品“首次”固定或完成之时。参考《法国知识产权法典》第 L.122—8 条第 2 款，对于某些特定的作品，在作者指导下完成的限量版作品亦可认定为原件。比如，作者完成了模版的制作，然后亲自或指导他人印制出限量版画。

综上所述，可以将美术作品原件定义为：作者亲自创作且具有可展览性和不可替代性，并能以一定形式表现的美术作品。这是一个比较典型的“属＋种差”的逻辑定义，〔39〕可以从以下几个方面加以理解。

一是淡化了传统上强调美术作品在时间上的“首次”，将之隐含于“作者亲自创作”之中。凡是作者亲自创作的必然都是“首次”完成的作品，即便是作者反复创作主题、内容、布局、色彩等完全相同的作品，每一次创作都是单独创作，得到的每一件作品都是原件，而不是第一件作品或前一件作品的复制件。作者也许还会亲自复制，但既然不是创作，就只能是复制件。“作者亲自创作”实际上是所有作品原件的根本来源和本质属性。所以，如此定义表明了作品原件的本源，既强调了其在创作主体上的特定性，也涵摄了其在时间上的“首次”。

二是突出了美术作品原件相对于其他作品原件和美术作品复制件的差异性即“种差”。我国《著作权法》上的美术作品原件应当具有可展览性，这既是与其审美属性相辅相成的另一种本质属性，也是区别于其他作品原件的“种差”。在前文所述案例中，其他作品原件和美术作品原件的判决要旨截然不同，后者总是考虑是否侵犯了展览权。美术作品原件的不可替代性则是其区别于复制件的“种差”。作品复制件的可替代性决定了其不能像原件那样彰显作品与作者之间的人身联系，也无法达到作品原件的财产价值、收藏价值和观赏价值。如果说可展览性还可能会因为法律规定的不周延而产生不同理解（即“直接”和“间接”之分），那么不可替代性则是美术作品原件坚定不移的本质属性之一。

三是淡化了传统上认为作品原件必为实体的认识，既符合《著作权法》对作品定义的最新修订，也极大地扩展了作品原件的表现形式。《著作权法》的最新修订以“能以一定形式表现”替换作品定义中的“能以某种有形形式复制”，顺应了技术发展的时代趋势。可以预见，越来越多的数字化美术作品（包括将传统美术作品数字化）将放弃实体化的展示，而采用形式更加多样的数字展示方式。在美术作品原件的概念中使用“一定形式”的表述，既包括物质载体的形式，也囊括了现在及将来数字技术、智能技术所能带来的一切展示形式，大大提升了立法的前瞻性和应变性。

四、创建美术作品原件的认定规则

（一）美术作品原件的一般认定

以前述对美术作品原件概念的理解为基础，笔者认为，现实中美术作品原件已经具备了以下

〔39〕 这是一种常用的逻辑定义方法，被定义项由其属概念和其区别于其他种概念的种差组成。

几种可能性。

第一种可能是作品原件唯一，绝大多数通过纸笔或刻刀等传统手法创作的美术作品如是。作品原件就是美术作品首次固定于其上的物质载体，其与复制件在载体性质、大小比例甚至平面还是立体上可能相同，也可能不同。比如将画作、书法编印成集，将雕塑作品按比例缩小或印成图册。

第二种可能是存在若干份作品原件。比如，已经毁掉模版且印制质量、尺寸完全一样的若干张版画作品，均为原件。如果作者反复创作相同的作品，每一次都是独立的创作，得到的作品是相互独立的作品原件，而不是同一作品的若干份原件，更不是第一件作品的复制件。在这种情形下，原件的认定需要辅之以作者在原件上的签名、编号、盖章、水印等客观性证明。

第三种可能是一些特殊类型的作品原件附有存续期限。比如，为了举办大型活动用灯具或花盆摆设的艺术造型。在“自贡市公共交通总公司诉自贡市五星广告灯饰公司侵犯著作权案”中，法院就认定原告设计、制作的“希望之光”大型灯组属于《著作权法》所称的美术作品。〔40〕活动结束后拆除艺术装置，则美术作品原件灭失，其存续期限即为活动期间。再如雪雕作品、沙画作品也有一定的存续期限。还有判例将发型认定为立体美术作品，亦为附有存续期间的作品原件。

第四种可能是并非所有美术作品都有原件。比如，曾有判例将音乐喷泉喷射效果的呈现认定为美术作品。音乐喷泉喷射出来的艺术造型转瞬即逝，无法固定，但是满足了作品“能以一定形式表现”的法定要求。再如，烟花燃放和无人机编队形成的艺术造型也是类似的“瞬间载体”。《著作权法》的最新修订确立了“作品类型开放”的立法模式，未来也许会出现更多没有原件的美术作品类型。

（二）数字化美术作品原件的认定

首先，前文已述，存有电子文档的硬盘、光盘或优盘等存储器不具有“直接”可展览性和不可替代性，且该电子文档可以随时被删除，也不符合大众对作品原件的通常认知，不能作为作品原件。

其次，如同在画板上作画一样，数字化美术作品完成时呈现在显示器上的图片代表作品“首次”附着在物质载体上。但是，美术作品看似“固定”在屏幕上，其实只是暂存于计算机的内存中。而且，根据《美国版权法》第 101 条，用于固定作品的载体应当具有“足够的长期性与稳定性”，以使作品在不短的一段时间内可以被感知、复制或以其他方式传播。所以，这种短暂呈现的画面没有被真正固定下来，不具有稳定性，不能作为作品原件。

再次，如果坚持作品原件必为实体的传统认识，那么只能将打印出来的实体作品认定为原件。对照前述美术作品原件的概念，虽然其具备可展览性，但却不具备不可替代性，同样品质的作品制件可以反复制作。当然，作者可以通过签名、题词、盖章或印制时加入水印等技术手段将一张或若干张打印版特定化为不可替代的作品原件。但是，那些多维的、动态的或像素高度压缩的数字化美术作品只有通过数字化方式才能全方位展示出创作精髓。比如，2021 年 3 月，佳士得

〔40〕 参见四川省自贡市中级人民法院（1994）自民初字第 2 号民事判决书。

公司以 6934 万美元拍卖了一幅 NFT 数字化美术作品《Everydays-The First 5000 Days》，由作者从 2007 年 5 月以来 5000 个日夜所创作的数字化作品压缩而成，〔41〕其艺术价值不只是体现在由这些作品拼凑而成的整幅图片上，还包括可以被放大的每幅被压缩的作品。换言之，不能真正展现数字化美术作品美感的打印版“作品原件”颠覆了其原本应当具有的观赏性，有可能还贬低了作品的艺术价值。艺术家们肯定不愿看到自己精心制作的多维或动态数字化美术作品，只能展示其中静止不动甚至索然无味的一面。

最后，笔者认为，如果突破作品原件必为实体的认识，可以将数字化美术作品完成时的原始图片或其形成的电子文档（通常带有“.gif”或“.jpeg”等专用扩展名）认定为作品原件。此处的图片或电子文档指的是作者亲自创作完成的同一件作品的不同表现形式，均为同一事物，借助于看图软件即可将电子文档打开为图片。图片需要借助电子屏幕展示，电子文档需要借助看图软件和电子屏幕展示，均能间接地满足可展览性的要求，即具备“间接”可展览性。电子文档本身附有权利管理信息，〔42〕可以被特定化为不可替代物，作者还可以通过技术措施防止他人未经许可浏览、欣赏和复制作品。《著作权法》的最新修订不仅将原来规定于《信息网络传播权保护条例》的权利管理信息和技术措施提档升级，还正式纳入作品登记制度，亦可为数字化美术作品原件的认定提供公信力极强的证明。

现实中的主要问题在于权利管理信息或技术措施极易被他人攻破，安全性比较低，特别是价值越高的作品越容易遭到攻击；一旦权利管理信息被篡改或删除，数字化美术作品原件就失去不可替代性，和其他拷贝文档混同为彼此没有差别的复制件。

然而，NFT 技术的出现提出了一个有希望的解决途径，在数字化美术作品的真伪鉴定、确认所有权、打击盗版和保护、管理版权等方面都产生了积极的影响。〔43〕2021 年 3 月有两则消息引人注目：一是推特（Twitter）联合创始人、首席执行官杰克·多西（Jack Dorsey），以 291 万美元拍卖了其 2006 年 3 月在 Twitter 上发表的第一条推文；〔44〕二是佳士得公司以 6934 万美元拍卖 NFT 作品《Everydays-The First 5000 Days》〔45〕。两件数字化作品都采用 NFT 技术予以特定化，保证了买家与拍品之间唯一的对应关系。在 NFT 作品拍卖中，买卖的其实是一种所有权凭证。NFT 通过一种技术方法来证明对数字艺术作品享有相应权利，并由区块链技术确保无法篡改，成为牢不可破的权利管理信息。当作者将其数字化美术作品的哈希值上传区块链并经由 NFT 技术特定化后就成为作品原件，其后该原件的每一次流转都被记录下来并不可篡改，满足了唯一性和不可替代性的要求，亦可借助电子屏幕进行展示，具备了可以作为作品原件的基本特征。因此，通过 NFT 技术认定数字化美术作品原件在技术上可行，并已投入应用，国内外也已

〔41〕 参见司林威：《NFT 玩家，谁都不曾拥有，我们只是过客》，载 https://baijiahao.baidu.com/s?id=1695901624768440859&wfr=spider&for=pc，最后访问时间：2021 年 3 月 31 日。

〔42〕 根据《信息网络传播权保护条例》第 26 条，“权利管理信息”是指说明作品及其作者、表演及其表演者、录音录像制品及其制作者的信息，作品、表演、录音录像制品权利人的信息和使用条件的信息，以及表示上述信息的数字或者代码。

〔43〕 参见刘双舟、郭志伟：《论非同质化代币对数字艺术版权管理与保护的影响》，载《中国美术》2021 年第 4 期。

〔44〕 参见揭书宜：《卖出 290 万美元！推特 CEO 首条推文以 NFT 资产卖了》，载 https://www.thepaper.cn/newsDetail_forward_11836514，最后访问时间：2021 年 3 月 23 日。

〔45〕 参见前引〔41〕。

经形成了一个创作和买卖、收藏 NFT 作品的新业态。

（三）美术作品的复制件

与作品原件相比，美术作品复制件的特殊问题在于，与原件不同维度的复制件是否仍是展览权意义上的作品复制件。复制行为本身有广狭之分，狭义的复制仅指同一维度的平面到平面、立体到立体，广义的复制还包括从平面到立体、立体到平面的维度改变。

对此，有肯定和否定两种见解。否定见解采狭义复制论，认为改变了作品原件维度的复制件不是展览权意义上的作品复制件。在“范英海、李先飞诉北京市京沪不锈钢制品厂著作权纠纷案”中，法院认为：“对于包括雕塑作品在内的美术作品，其复制件应指由对该作品的复制行为所产生的与该作品完全相同或者相近似的作品。由于被告展览的涉案不锈钢雕塑作品构成了对原告雕塑作品《韵》的剽窃，该剽窃作品应属原告雕塑作品《韵》的复制件。”〔46〕肯定见解采广义复制论，认为与作品原件维度不同的复制件仍是展览权意义上的作品复制件。比如，在“广东原创动力文化传播有限公司（以下简称‘原创公司’）诉群光实业（武汉）有限公司（以下简称‘群光公司’）著作权纠纷案”中，群光公司购买了与原创公司美术作品美羊羊、喜羊羊、灰太狼在视觉上无明显差异的服装道具，派员工穿戴该卡通服装道具装扮成卡通角色在其周年庆活动上宣传造势，并与现场人群交流互动。其中，涉案侵权物品即为源于平面美术作品的立体卡通服装道具。法院认为：“被告的行为使原告美术作品美羊羊、喜羊羊、灰太狼的立体复制件向不特定公众展示，虽属于非典型的公开陈列美术作品的行为，但仍侵犯了原告对以上美术作品享有的展览权。”〔47〕

我国《著作权法》采用狭义复制的概念即否定见解，然而从著作权法鼓励和保护作品及其创作的目的出发，采肯定见解即广义复制的概念更为合理。盖因著作权法保护的是作品而非作品载体，如果将改变作品原件维度的复制件放任于法律调整之外，显然不利于维护著作权人的利益，也是一种纵容侵权的做法。

根据上述认定规则，经由 NFT 证明或其他类似证明的数字化美术作品的图片或电子文档是原件，没有相应证明和已经实体化的作品都是复制件；进而言之，对于数字化美术作品，其复制件具有数字化和实体化两种可能的属性。将实体化的美术作品原件进行数字化复制，得到的数字化作品也可称为复制件。这样无论通过什么方式创作作品，均突破了作品复制件必为实体的传统认识，和确定作品原件的规则保持了一致。《著作权法》的最新修订修改了第 10 条关于复制权的定义，专门将“数字化”的复制加入其中。有学者认为：“这一修改只是对理论和实务中的共识以立法形式加以体现，是对已有做法的确认，而不是创设新的规则。”〔48〕所以，改变美术作品原件和复制件必为实体的认识，在理论、实务和法律依据上都已具备了一定的基础。

五、结　语

展览权虽然在著作财产权中并不起眼，但却是文博事业存在和发展的重要基石。作为展览权

〔46〕 北京市第二中级人民法院（2002）二中民初字第 8042 号民事判决书。

〔47〕 湖北省武汉市中级人民法院（2010）武知初字第 66 号民事判决书。

〔48〕 王迁：《〈著作权法〉修改：关键条款的解读与分析》（上），载《知识产权》2021 年第 1 期，第 24 页。

的核心概念和拍卖场的竞逐对象，美术作品原件的重要性毋庸置疑。我们应当从实践出发，回应新技术、新业态提出的新挑战，正确理解和认识美术作品原件的概念，突破作品必有原件、作品原件唯一和作品原件必为实体的传统认识，顺应数字经济时代的发展趋势，构建出认定美术作品原件特别是数字化美术作品原件的新规则。

Abstract：The original copy of art works is the core concept of the display right in China's Copyright Law，but it has not received due attention. Facing the new challenges posed by new technologies and new business forms，regardless of traditional art works or digital art works，there is a confusion about how to understand the original copy of art works and how to identify the original copy of art works. In this regard，it is necessary to break through the traditional understanding in Copyright Law that art works must have the original copies，that the original copies of art works must be unique and that the original copies must be entities. Complying with the requirements of technological development，we should firmly grasp the two key characteristics of exhibitability and irreplaceable to construct the concept of the original copy of art works and create the general rules for identifying the original copy of art works. For digital art works，on the premise of meeting the "indirect" exhibitability，the electronic documents formed when the digital art works are completed can be recognized as the original copies with the help of NFT technology.

Key Words：art works，original copy，the display right，non-fungible token

（责任编辑：张金平　赵建蕊）

财经法学 No. 3，2022
pp. 43 - 64

金融交易数据的监管应用
——以交易报告库为中心

张　阳*

内容提要：数据的利用源于私法交易需求，但存在公法监管之必要。在强化金融风险防范的背景下，以增强交易透明度为旨向的数据报告机制革新和系统审视甚为关键。与民法关切的数据保护、商事层面的数据交易、监管角度的数据统计不同，数据报告可从三个维度分析：中心维度是交易报告库的设施聚合运作，基础维度是前端主体、产品和交易的数据标准解构，重点维度是后端目标数据的分类集成和分层使用。由于多头监管、分业监管和监管治理滞后，我国金融交易数据报告制度存在角度离散、广度不足和深度阙如之缺陷，且数据口径不一、数据面向偏狭、数据风险揭示不足等问题突出。慎思回应之策，一是要加强交易报告库的识别规制、运行治理和危机处置，二是推进数据标准的对接转化、特色塑造和国际话语权争夺，三是明晰不同监管机构的数据获取安排。同时，还应关注以区块链为代表的去中心化技术对数据报告制度的冲击，以数据共享替代数据报告的愿景暂不可行。

关键词：金融交易数据　交易报告库　金融市场基础设施　数据交易　数据保护

一、引　言

随着科技的迭代革新，数据对现代经济的功用得到极大拓展，其被列入继土地、劳动力、资本、技术后的第五类新兴生产要素。其不仅是虚拟世界交互运作的“原油”，[1] 也成为驱动

* 张阳，武汉大学法学院讲师。

本文为教育部人文社会科学研究项目青年课题“风险防范视域下金融科技应用的监管对策研究”（18YJC820083）的阶段性成果。

〔1〕 See Katerina Pistor, Rule by Data: The End of Markets? 83 (2) *Law and Contemporary Problems*, 106 (2020).

实体产业发展的引擎。在金融市场中，数据更是连接主体、产品、资金要素的纽带和载体。而金融交易数据（transaction data）又是金融数据的核心，其关涉交易动态过程，是勾勒金融网络的要核。传统研究多关注民法维度的数据保护和商事层面的数据交易，这在效率导向下的经济运作中无可厚非，但在复杂、专业、涉众的金融市场中，私法的协议安排和权属保护无法解决系统性风险问题。以服务于监管为本色的数据报告制度则是识别和化解金融市场风险的专属利器。尤其 2008 年全球金融危机以来，效率和创新价值追求趋于保守，风险治理再度回归监管主线，围绕数据报告的规则层出不穷。〔2〕近期新冠疫情又致使传统线下的现场监管难以成行，技术加持下的非现场监管成为新的优选，数据报告机制以电子化、非接触、及时性为显征，其重要性愈发凸显，备受监管青睐。〔3〕

国际上，数据报告机制的创新在次贷危机后集中显现。受场外衍生品“黑洞”问题刺激，为提高交易透明度，各国陆续加强数据报告机制建设，通过设立交易报告库（trade repository，TR）解决数据要素分散问题，使基础数据汇集到 TR，通过 TR 聚合处理形成监管所需的目标数据。2012 年起，围绕 TR 的国际规则逐渐出台，至今已形成体系化结构。相比之下，我国进展较慢，长期聚焦于前台交易，对后台设施布局乏力。〔4〕2020 年《中国人民银行法（修订草案征求意见稿）》首度将交易报告库的设立和监管列入央行权限，〔5〕证监会主导的监管市场在 2019 年已开始抢先布局，北京地方金融监管局也表示支持 TR 的设立。声势虽盛，然散乱的试水却有“门面装饰”之嫌，在监管博弈下难免成为政绩竞争的产物，且未能厘清与传统数据统计的边界。对数据报告机制这一“熟悉的陌生人”，亟需系统审视其促进监管功能的发挥。比如，交易报告库为何是中心化架构，其与金融中介差异何在？具有公共利好的数据标准为何推进困难重重？监管机构对交易数据的获取应包括哪些层面和规程？实际上，以交易报告库为中心的数据报告机制不仅是本土改革的需求，亦是对外寻求国际话语权的突破口。在我国走向高层次开放、建设金融强国的道路上，TR 作为金融市场基础设施的最新成员，有较广阔的国际制度设计空间。那么，以 TR 的运行机制为轴心，如何认识设施、标准和制度的关系，将是本文贯穿始终的主线。

二、交易报告库功能定位

交易报告库是带有浓重技术色彩的创新型机构，应从金融市场主体的系统结构和历史演变

〔2〕以欧盟为例，自 2008 年以来，其已颁布了 40 余份数据报告的规则。See European Commission，Executive Summary of the Fitness Check of EU Supervisory Reporting Requirements，Commission Staff Working Document SWD（2019）403，November 6，2019.

〔3〕See Antonio Pancorbo，David Lukas Rozumek，Katharine Seal，Supervisory Actions and Priorities in Response to the Covid-19 Pandemic Crisis，Special Series on Financial Polices to Respond to Covid-19，International Monetary Fund，October 7，2020.

〔4〕参见张阳：《金融市场基础设施论纲：风险治理、科技革新与规制重塑》，载《经济法学评论》2018 年第 2 期。

〔5〕《中国人民银行法（修订草案征求意见稿）》第 39 条第 1 款规定：“中国人民银行负责制定重要金融基础设施建设规划并统筹组织实施，推进金融基础设施互联互通并拟订相关业务规则，统筹建立覆盖全市场的交易报告制度，建设并运营总交易报告库。”

中探究其定位。与“前台”的投融资主体、金融中介不同，交易报告库是“后台”金融市场基础设施（financial market infrastructure，FMI），属于支持性机构（supportive institution），公共物品属性突出。〔6〕当前 TR 不被市场熟知的原因在于，TR 隶属的金融市场基础设施为运行在底层的“管道”，不如前台交易所受关注度高。再者，TR 是 FMI 的最新成员（其他主要成员包括重要支付系统 SPS、中央证券存管系统 CSD、证券清算系统 SSS、中央对手方 CCP），于 2012 年后才逐步进入国际规制视野。交易报告库是补足金融市场主体的最后一块“拼图”，实现了金融交易后台数据〔7〕要素的规制补缺，将金融监管、金融交易和金融处理三条脉络衔接为一体。本部分从本体剖释、横向比较和纵向流程对交易报告库予以阐释，以期揭开其神秘面纱。

（一）本体解释：监管导向的风险监测工具

交易报告库，也称数据报告库（data repository），根据国际清算银行（BIS）和国际证监会组织（IOSCO）的定义，它是指集中维护（maintain）交易数据电子记录的单位（entity），为组织法的主体概念，而非单纯的技术性操作系统、储存设施（storage facility）或数据库（data-base）。〔8〕交易报告库的涌现与 2008 年金融危机相关，由于盘根错节的场外衍生品交易缺乏透明度，监管面临风险黑箱，2009 年的 G20 会议强调加强场外衍生品监管，核心举措为要求所有场外衍生品向交易报告库报告。2012 年 BIS 和 IOSCO 将 TR 列入金融市场基础设施的组成部分，〔9〕起先适于衍生品市场，后逐步扩大至整个金融市场。

本质上，交易报告库是一种归集性的“增量”创新，将市场原本“多对多”（N 对 N）的散射式“并联”报告，转为“一对多”（N-1-N）的中心式“串联”报告，其功能是提高透明度、增强市场监管和减少系统性风险，三者层层递进共同指向风险监测治理，即收集市场数据并为监管主体所用。〔10〕因其服务于监管的导向突出，交易报告库被视为金融市场的公共物品，多由政府机构特设。但也不尽然，由于 TR 本身不生产数据，而是数据“搬运工”，数据主要来源于其他主体、机构的信息报送或联通，域外 TR 的设立存在混合模式。最典型的是 TR 和 CSD 的融合运作，例如，在美国，数据报告库（DTCC Data Repository，DDR）由证券存托和结算公司（DTCC）设立，欧洲交易报告库（REGIS-TR）由西班牙中央证券存管机构 Iberclear 和国际证券存托机构 Clearstream 共同设立。原因在于：一方面，TR 是新生产物，若独立设置新型 TR，制度规范和具体运作上缺乏先前经验，投资者对市场信息集大成者的 TR 能否有效安全运作存有疑虑，而嵌入既有设施则可减少新机制施行的障碍。另一方面，TR 是信息要素的处理，不涉及具体券款交易，不涉及复杂的破坏式创新，只需新增端口将券款数据转换为必要数据并标准化处理即可。

〔6〕 See William J. Rankin，Infrastructure and the International Governance of Economic Development，1950－1965，in Jean-Francois Auger et al. ed.，*Internationalization of Infrastructure*，Delft University of Technology，2009，pp. 61－62.

〔7〕 本文的数据并非是单纯的技术性意义的底层数据（计算机识别语言下的 1、0 排列表达），而是具有价值导向，与信息概念近似。金融市场的三大核心要素包括资金（货币）、证券（产品）和信息（数据）。

〔8〕 See CPSS（BIS）-IOSCO，Considerations for Trade Repositories in OTC derivatives，May 2010.

〔9〕 See CPSS，IOSCO，Principles for Financial Market Infrastructures，April 2012.

〔10〕 See Lucia Quaglia，*The Politics of Regime Complexity in International Derivatives Regulation*，Oxford Express，2020，pp. 72－73.

然而，监管导向的交易报告库也内含利益纠葛和成本耗费，这也是为什么看似技术难度不大的设施却诞生如此之晚的原因。首先，交易报告库具有公共物品属性，贯穿交易全程但并不参与具体交易，营利主要依靠服务费，不从交易价格变动中获利或承担风险，〔11〕故私有主体设立和运营的动力不足；其次，数据监管主体多头割裂，而有效分析信息的关键在于全面获取信息，局部分散的数据对监管识别和风险管理功用有限，加之交易报告库涉及的数据元素标准需要全球协调，国际监管配合推进难度较大；〔12〕在相对直接的资金、证券要素的规制中，监管权的行使涉及深广的利益分配，寻租空间较大，而金融交易中底层的数据要素之信息价值的“变现”则显得较为滞缓和间接。再次，对报告主体而言，报告是一种成本消耗型行为，在成本效益分析下，若无明显直接利好，其积极参与数据报告的动因微弱；最后，受路径依赖（path-dependent）的影响，传统金融统计等制度的竞争也难免削弱信息报告的独特作用。

近年来 TR 能够涌现，主要源于风险积聚的外因刺激。市场平稳时，行为合规和微观审慎占据主导地位，效率创新为核心追求，可一旦涉及系统性危机，整个市场将陷入瘫痪，负外部性明显。随着风险频发、产品日益复杂、主体趋于多元，安全价值再度上升为核心考量。且相较于业务限制等措施，数据报送机制的革新具有成本优势。

（二）横向比较：系统视角下的主体定位

仅以本体分析不足以揭示交易报告库特点，尚须与既有市场概念作区分。交易报告库是金融市场基础设施的一种，具有 FMI 的基本特点：第一，网络连结性，〔13〕TR 是金融体系的中心节点，其既是单一的机构，也是系统的存在，溢出效应（spillover effect）明显，一旦发生危机会有波及其他主体或实体经济的危险；第二，沉没成本（sunk cost）高，TR 的设立及运作一般需长期、固定、大量的投资（技术升级、系统保障、风险基金等），市场进入成本较高，且由于业务专业性、面向较单一及难以割裂，一旦退出市场，则投入的成本难以收回；第三，自然垄断性，相较于多个 TR，市场存在一个 TR 往往服务效率更高，有边际效益递减的弱增性（subadditivity）规律，过多 TR 会使数据交叉分散影响准确性，且发挥同一功用的多个 TR 内部运行规则往往存在差异，影响市场主体的报告合规成本；第四，公共物品属性，〔14〕TR 主要由政府或非营利主体设立，虽个别国家金融市场的公共物品早期由市场提供，但后期政府或由政府主导的非营利性机构逐步加强对这类设施的控制管理，使其具有典型的“民办官营”特点，〔15〕即便市场化运作，也会一定程度上得到央行授信或政府的隐性担保。

此外，交易报告库主体定位可通过比较分析予以明晰。首先，与投融资主体不同，设施的后

〔11〕 参见〔德〕马丁·迪尔等编：《金融基础设施经济学分析》，中央国债登记结算有限责任公司译，中国金融出版社 2019 年版，第 4 页。

〔12〕 See M. Breen, D. Hodson, Moschella, Incoherence in Regime Complex: A Sentiment Analysis of EU-IMF Surveillance, 58 (2) *Journal of Common Market Studies*, 419 - 437 (2020).

〔13〕 See Leon Rincon, C. E, Financial Stability from A Network Perspective, Center for Economic Research, 2014, p. 183.

〔14〕 See Ruben Lee, *Running the World's Markets: The Governance of Financial Infrastructure*, Princeton University Press, 2011, pp. 10 - 11.

〔15〕 参见焦瑾璞：《中国金融基础设施功能与建设研究》，社会科学文献出版社 2019 年版，第 12 - 14 页。

台定位决定了其不参与交易而只是服务于交易。其次，虽具有信息汇集功能，且在部分法域中被立法赋予要求市场主体向其强制报告的权利，或有监管当局授权（类似于交易所），但 TR 本身并非监管者。再次，TR 不是传统金融中介，虽然二者均为第三方机构，但差异明显：一是金融中介并非必然参与每笔金融交易，其以效率为导向，是金融交易可选项，但 TR 设立后即为金融交易闭环系统的组成部分，以安全价值为核心追求，是金融交易必选项；二是金融中介可为个性化的双边系统，但 TR 具有网络连结性特征，并非对接个别主体，须为全局性的多边系统；三是金融中介关注点多为微观风险，而 TR 是监管导向的基础设施，须考量系统性风险。最后，TR 也不是新型金融平台。近十年来，随着互联网技术的成熟，金融平台正发生消融中介、重新迭代之变，〔16〕是去中介化（disintermediation）的直接体现，其以交易为直接面向，借助规模效应和直通式平台，解构冗长复杂的交易链条〔17〕。平台的着眼点在于“交易中”的撮合，而 TR 是“交易后”的支撑性服务，在同一金融过程中二者并非处于同一位置（参见图 1）。平台的影响力虽强大，但仅仅是对中介的优化或替代，与底层交易报告没有直接关联；且因其处于交易的逐利过程中，运营多为考量成本收益的私人主体，而 TR 更关注风险价值，通过风险管理和监管机制侧重承担系统性风险的防范职能。〔18〕

虽然交易报告库属于金融市场基础设施的分支，与其他子类设施虽有共性，但亦存在差异。按 2012 年《金融市场基础设施原则》（PFMI）规定，〔19〕FMI 包括五类，〔20〕分别是重要支付系统（SPS）、中央证券存管系统（CSD）、证券结算系统（SSS）、中央对手方（CCP）和交易报告库（TR）。上述类型划分的逻辑何在？虽看似分散，却反映出金融交易的核心要素（资金、证券、信息）的连结关系。SPS 用于多个参与者之间的资金转账，体现出资金端的款项支付保障；CSD 则提供证券账户集中保管和登记，定位于证券端，〔21〕而 CCP 和 SSS 负责清算结算业务，主要是资金和证券的数额动态轧差；TR 聚焦于数据报送，是金融市场的信息聚合。可以说，TR 的出现弥补了金融运营体系中数据要素缺失这一短板。由于数据归集之要求，TR 犹如“设施中的设施”，其他四类设施的运作也需接入 TR，从而为监管决策提供交叉验证和全景分析支持。

（三）纵向流程：中心功用发挥的前提和对象

除静态的横向比较外，对 TR 的全面理解还应从纵向数据流动的流程视角展开。TR 产生之前并非没有交易报告机制，只是缺乏中心化的设施聚合。此前，市场主体按照监管要求，要么直接向监管机构履行报告义务，要么通过中介或交易所进行报告。这种分散的数据报告为了应对不

〔16〕 See Tom C. W. Lin, Infinite Financial Intermediation, 50 (3) *Wake Forest Law Review*, 655 - 656 (2015).

〔17〕 See Orly Lobel, The Law of The Platform, 101 (31) *Minnesota Law Review*, 147 (2017).

〔18〕 See Guido Ferrarini, Paolo Saguato, Regulating Financial Market Infrastructures, ECGI Working Paper Series in Law (Working Paper No. 259/2014), pp. 5 - 6.

〔19〕 See CPSS, IOSCO, Principles for Financial Market Infrastructures, 2012, Art. 1. 8 - Art. 1. 14.

〔20〕 部分法地域有扩张性的解释，例如将交易场所纳入的模式，如瑞士《金融市场基础设施法》第二章“关于交易场所（trading venue）、组织化交易设施（organized trading facilities）”。See Federal Act on Financial Market Infrastructure and Market Conduct in Securities and Derivatives Trading (FMIA), SR 58. 1 of Federal Assembly of Swiss Federation, 2015.

〔21〕 证券端不限于狭义的股票、债券等证券，此处证券应作广义解读，是“金融商品（产品）”的指称。

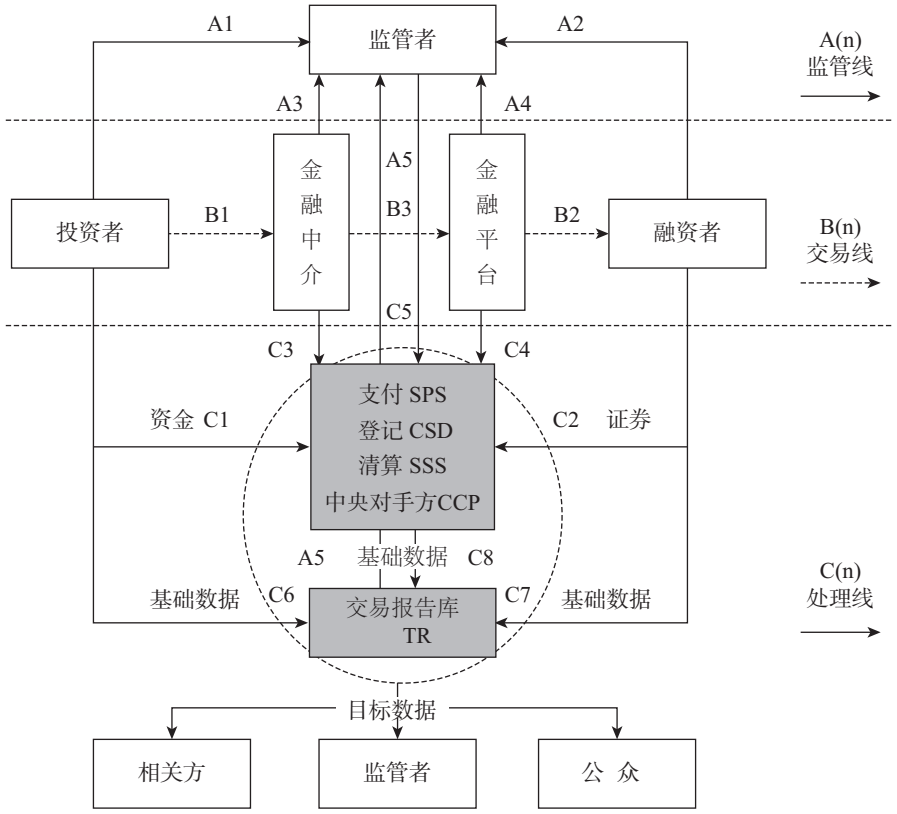

图 1 金融市场的主体组成和流动关系

同的监管要求，同一数据不得不改成不同格式。多头、多次报告导致成本高，且不同监管主体间缺乏数据的互联互通。然而，TR 的引入则搭建了市场主体与监管者之间的桥梁，〔22〕从而有助于增强信息归集，降低报告者合规成本，增进市场全景的透明度。

需注意的是，TR 尚为新兴主体，不同国家对 TR 的运作存在自身标准，以增强管辖之权威，实现数据专属性的获取，这难免造成“市场割裂”（market fragmentation）的国际难题，〔23〕因此，试图从设施层面建立统一的金融市场交易报告库愿景虽好，但短期内难以实现。实际上，相较于 TR 的“硬件”设施差异问题，统一数据的“软件”标准更为关键，特别是元要素的提炼是数据报告及风险监测的核心要义。从数据报告流程看（图 1），TR 是中心化的“加工厂”，流程优化不仅在于自身建构，更在于前端基础数据的元素解构和后端目标数据的分类集成。

向前端追溯，交易报告库的本质定位是数据储存、证明和加工的“数据仓库”（data warehouse），自身并不产生交易数据，数据来自其他市场主体。由于金融交易复杂，定义节点诸多，不同数据主体对交易要素抓取不同，倘若缺乏有效的共识性“元要素”，不同变量的数据堆积却

〔22〕 See FSB, Feasibility Study on Approaches to Aggregate OTC Derivatives Data, September 19, 2014.

〔23〕 See Institute of International Finance (IFF), Addressing Market Fragmentation: The Need for Enhanced Global Regulatory Cooperation, January 2019.

无法互通分析，难免沦为无效的信息“垃圾”。〔24〕数据标准不一不仅体现在国别间的差异，〔25〕也存在于国内不同监管主体的要求差异。因此，凝练金融基础数据的标准化元素甚为重要。〔26〕。

向后端着眼，交易报告库不像其他 FMI（支付、登记、托管、结算等设施）介入金融交易券款的实际处理，其存在的核心目标在于服务监管，与其他金融基础设施是平行的运行关系，将金融交易全景跟踪拍照（snapshot）。〔27〕基础数据在 TR 汇集加工，根据不同监管部门的差异化需求，产生不同目标数据，实际上起到数据的分类和分层作用，监管部门可由原先对接成千上万的数据源转而对接一个或多个 TR。尽管 TR 的核心目的在于服务监管，但亦有向市场主体和社会公众披露数据的潜在空间，从而助力于多种社会政策效益的发挥。

三、基础数据的元素解构

交易报告库是数据处理的中枢设施，其顺畅运作需要前端标准化的数据输入。金融交易图景的勾勒要依赖基础数据，其要素如何解构关乎后续数据的准确性和完整度。

（一）标准要素的利弊权衡：为何难以产生

界定基础数据的元素非常必要。首先，对参与者来说，有利于明晰交易对象。基础元素的作用是将个性化语言通过标准化代码（数字＋字母，Alpha-Numeric）予以清晰准确地表达，避免一个对象的多个名称混淆交易。实践中，因缺乏元要素，不少主体被迫耗费巨资构建系统“清洁数据”（data cleaning），进行交易的验证和分析。其次，对其他公众而言，有利于商业秘密的保护。以元素为基准，尤其是非“智能信息”（intelligent information）的嵌入，能增加相关交易方的数据保护度。再者，有利于适应金融市场规模化、高频的交易，基础要素的报告将复杂金融交易简单化转译，可快速清晰界定交易信息，减少交易识别的时间成本，提高交易效率。最后，有利于监管针对性地抓取。通过基础要素的拆分使监管有清晰的目标，能集中有限资源监测重点风险，避免多元化的名称或要素造成统计繁杂。恰如科尔教授所言，“没有可靠的数据，监管者将如同盲人飞行”〔28〕。

尽管利好明显，但基础数据的元素解构却发展滞缓。何以如此？从技术角度审视，金融产品可谓现代社会最多元、最复杂的对象，且不说银行、证券、保险之区分，单是股票、债券、衍生品之间也存在诸多差异。加之金融产品具有无形化、结构化的特点，且随着交易实践的发展不断创新，尤其是嵌套性资管产品，底层资产和外在产品的关联依赖于复杂的交易设计，这引发技术上如何有效归纳数据节点的困难。须注意，并非要素点越细密越好，因为这会增加市场主体报告

〔24〕 See Eric Helleiner, Stefano Pagliari, Irene Spagna, *Governing the World's Biggest Market: The Politics of Derivatives Regulation After the* 2008 *Crisis*, Oxford University Press, 2018, p. 243.

〔25〕 See M. Lehmann, Legal Fragmentation, Extraterritoriality and Uncertainty in Global Financial Regulation, 37 (2) *Oxford Journal of Legal Studies*, 406－434 (2017).

〔26〕 See M. Gal, Data Standardization, 94 (4) *New York University Law Review*, 737－770 (2019).

〔27〕 See CPSS-IOSCO, Authorities Access to Trade Repository Data, August 12, 2013.

〔28〕 B. Coeure, Setting Standards for Granular Data, Speech, ECB, 28 March 2017.

负担，影响后续交易报告库数据聚合分析的共性提炼，繁多的元素很可能将形成信息噪音，还干扰核心数据的价值和风险识别。另外，监管博弈因素亦不可小觑，不同地区的监管主体基于地方保护主义考量，认为适用其他地区标准一定程度上将减少自身话语权，因此解决制度分割难以一蹴而就；〔29〕即便同一地区的监管者，也有分业监管的差异，如何系统性地调和监管利益，难度并不低。

既存行业的标准“惯性”也不能忽视。在以全球化视域推进新标准元素的背景下，现行的行业标准基于自身的路径依赖，尤其是中小金融机构，缺乏足够动力来承担转换对接新标准的成本。抛开技术难度、行业惯性和监管博弈，单就标准推进来看，仅靠市场力量难以达成。原因在于，一是集体行动（collective action）因素作祟，标准设立者沉没成本较高，且由于标准的公共物品属性，极易被“搭便车”；〔30〕二是受网络效应（network effects）的影响，即便有市场主体设计要素标准，标准效用的发挥需要规模基础，而标准设立初期往往应用规模小，收益低，因此靠市场推动难度大；三是仅靠市场主体的推动缺乏强制力，自愿接受的覆盖面有限，且市场主体存在利益导向，即便“大公无私”的奉献也难以获得公信力，可能遭受同行竞争者的挤压。

因此，监管介入实属必要，尤其在金融全球化背景下，国际金融标准组织的协调尤为关键。通过超主权的国际协调将公共政策考量纳入行业代码，既能最大程度避免监管俘获，又能防止市场失灵的发生。在基础共识基础上，以软法（soft law）〔31〕方式还能留有必要裁量空间和特色设计，从而助益于全球金融的正外部性发挥。〔32〕

（二）基础数据的三重解构：主体、产品和交易

次贷危机后，为回应场外衍生品透明度欠缺的问题，在 G20 峰会倡导下，金融稳定理事会（FSB）、国际清算银行支付和金融市场基础设施委员会（BIS-CPMI）、国际证监会组织（IOSCO）及国际标准制定组织（ISO）陆续颁布基础数据的相关规定（参见表 1）。2012 年 1 月，BIS 和 IOSCO 共同发布《场外衍生品数据报告和整合安排》，提出基础数据的三大要素。

首先进入监管视野的是主体要素的认定。2012 年 6 月，FSB 发布《全球金融市场法人识别符治理安排》（Global Legal Entity Identifier for Financial Markets），法人识别符（legal entity identifier，LEI）是一个由数字和字母组成的 20 位编码（如 YUV8PRHOZSRFRC4JO269），全球法人识别符系统监督委员会（The ROC of the Global LEI System）负责为每一个注册的金融市场参与者提供独一无二的识别码。ROC 以独立的组织形式避免对基础或附属业务的依赖，同时为减少相关主体的注册成本，其按照成本弥补型（cost-recovery basis）计费。虑及 LEI 尚为新兴产物，其原则上未排斥既有的其他标准，如在 LEI 之前的 ISO 17442 标准仍可适用。LEI 在不

〔29〕 See K. J. Alter, K. Raustila, The Rise of International Regime Complexity, 14 *Annual Review of Law and Social Sciences*, 320 - 349 (2018).

〔30〕 See Financial Stability Board (FSB), Global Legal Entity Identifier for Financial Market, June 8, 2012.

〔31〕 软法“管用”的原因在于其有相关的同行评议机制，例如 FSB、BIS 和 IOSCO 定期对 LEI、FMI、营商环境的执行情况进行分析评价，各地区会顾及国际声誉。See Chris Brummer, Why Soft Law Dominates International Finance-And Not Trade, 13 (3) *Journal of International Economic Law*, 63 - 64 (2010).

〔32〕 See S. Gadinis, Three Pathways to Global Standards: Private, Regulator, and Ministry Network, 109 (1) *American Journal of International Law*, 1 - 57 (2015).

同国家的适用存有差异，据 FSB 2019 年报告，国际 200 多个国家和地区约有 140 万 LEI，整体比例较低，即便美国等发达市场，适用面也仅 2%～7%左右，还有 100 多个地区 LEI 注册数不足 100 个。这与半数以上的地区采用自愿性要求（optional）有关，[33] 强制性规定注册的适用地区有限，且部分地区仍采用自有的 LEI 替代系统。国际金融市场基础设施的立法先驱——瑞士 FMIA 对主体要素便采取了三类方案：首先适用 LEI，如未注册则适用 11 位的商业识别码（ISO 9362：2014），若仍没有，则使用最多不超过 50 位的内部系统码（internal code）。[34]

在主体之外，产品要素的统一随之跟进。CPMI-IOSCO 和 FSB 分别在 2017 年和 2019 年颁布《唯一产品识别码统合的技术指引》（Technical Guidance on Harmonization of the UPI）和《唯一产品识别码统合的治理安排》（Governance Arrangements for the UPI），唯一产品码（unique product identifier，UPI）有 12 个数码，包括验证的检验符，内部组成涉及产品信息和底层资产信息。产品码的获取不同于主体码（法人识别符），其需要基础数据参照库，产品主要围绕信用、权益、利率、汇率和商品五种类型展开。产品码的管理机构被 FSB 授予 LEI 的 ROC，采用中心化发行模式，这有利于全球金融市场确立统一的产品要素数据，但要注意垄断、寻租及单点失败的系统性风险等问题。产品码目前未被强制全球性推行，既有标准仍有适用空间，如国际证券识别码 ISIN（ISO 6166：2013），欧盟的替代性产品识别码（alternative instrument identifier，AII），瑞士的交易所产品码（exchange product code，EPC）。[35]

仅有主体、产品要素仍过于静态，无法获知交易行为或过程的动态数据。2017 年 FSB 和 CPMI-IOSCO 又分别发布了《唯一交易识别码的治理安排》（Governance Arrangements for the UTI：Conclusions and Implementation Plan）和《唯一交易识别符的技术指引》（Technical Guidance on Harmonization of the UTI）。唯一交易识别码（UTI）起初应用在衍生品市场，之后向其他市场扩展，为增强交易码的适用范围，文件采用“可报告的交易”（reportable transaction）以兼顾地区差异。交易码长达 52 位，须覆盖交易的全生命周期（life-circle）变化，以保证该码的稳定性。交易码生成无须中心化机构，也无须中心化发行，核心功能是避免“双花统计”。LEI 和 UPI 保证交易唯一性（unicity），UTI 则确保交易的一致性（consistency）。

表 1　　**国际数据报告制度的核心规定**

颁布机构	规范名称（简称）	颁行时间	内容重心			内容精度		
			基础数据	TR 本身	目标数据	低精度	中精度	高精度
FSB	主体数据治理安排（LEI Governance）	2012	■					●
	数据整合进路（OTC Data Aggregation）	2014	□	■	□			●
	交易数据治理安排（UTI Governance）	2017	■					●
	产品数据治理安排（UPI Governance）	2019	■					●

〔33〕 See FSB，Thematic Review on Implementation of the Legal Entity Identifier（Peer Review Report），May 2019.

〔34〕 See Art. 93 of Financial Market Infrastructure Act in Swiss，2015.

〔35〕 See Annex 25-Section 2a（10）of Financial Market Infrastructure Act in Swiss，2015.

续前表

颁布机构	规范名称（简称）	颁行时间	内容重心			内容精度		
			基础数据	TR本身	目标数据	低精度	中精度	高精度
CPMI-IOSCO	交易数据技术指引（UTI Tech Guide）	2017	■					●
	产品数据技术指引（UPI Tech Guide）	2017	■					●
	其他关键数据技术指引（OCDE Guide）	2018	■				●	
	其他关键数据治理安排（OCDE Governance）	2019	■				●	
	数据报告和整合安排（Data Report）	2012	■	■	■			●
	数据的监管接入（Data Accesss）	2014			■	●		
	金融市场基础设施原则（PFMI）	2012		■	□		●	
	金融市场基础设施恢复（ FMI Recovery）	2017		■				●
	金融市场基础设施网络韧性（FMI Cyber）	2016		■			●	
	央行所属设施的原则之适用（CB-PFMI）	2015		■		●		
	关键服务提供者的监管评估（CSP Assess）	2014		□			●	
ISO	主体数据技术指引（LEI Code）	2012	■					●

注：表中的实心代表核心的聚集；空心代表概括的提及。

上述三种元素构成基础数据的核心维度，但并未覆盖全部数据维度。为增加风险监测的全面性，CPMI-IOSCO 在 2018、2019 年进一步出台“其他关键数据”（other critical data elements，OCDE）的治理安排和技术指引，〔36〕重点强调场外衍生品领域的其他定义性数据点，将国际 ISO 标准有机融入，包括时间戳，对手方和收益方，清算、交易、结算，常规支付，估价，抵押品和保证金，价格，名目账单和数量，其他支付，打包组合及定制组合等内容，主要目的是为各地区监管指引提供模板化的参照。四种元素治理要求，均有唯一性（uniqueness，唯一代码）、中立性（neutrality，不含地理、名称等嵌入性的智慧信息）、真实性（reliability，有发行和验证的机构）、开源性（open source，要与既有系统兼容）、可拓展性（extensibility，能适用于未来所有全球金融交易数据的处理）、简明性（lean），以及非必要不修改原则。

可见，金融交易数据基本元素包括主体（码）、产品（码）和交易（码），其以简明、清晰、普适的数字和字母组合描述金融交易基本情况，通过动静兼具的视角保证基础数据的准确、一致和较高的完整度。同时，其他关键数据又为金融数据的全面监测和全景描述提供了进一步的参照。正是通过元素的标准化界定，TR 的数据分析比对才更具规范性和统一性。

〔36〕 See CPMI, Technical Guidance on the Harmonization of Critical OTCDs Data Elements (Other than UTI and UPI), April 9, 2018; CPMI-IOSCO, Governance Arrangements for Critical OTCDs Data Elements (Other than UTI and UPI), October 9, 2019.

四、目标数据的分类集成

基础数据经由交易报告库进行集中化处理和分流。交易报告库不仅是数据中转平台，其本身对接不同的监管者，根据不同监管目标对数据还有分类集成的作用。那么，需要探究通过交易报告库输出何种数据方可满足监管需求。有几个问题须重点思考：加工后的数据有几个维度，不同金融监管部门对数据需求有何差异，除监管功用外，目标数据可否有其他受众。本部分聚焦目标数据，探讨其内在维度和使用范围。

（一）数据集成的三种维度：深度、广度和识别度

一种偏颇的说法长期盛行，即“数据越多、越精细越好”，〔37〕这种观念或可满足监管的权力欲望，但并非监管治理的客观需要。次贷危机后，根据监管目标的不同，精准化数据抓取成为主流。精准化强调数据的聚合处理（data aggregation），根据数据结构化理论，基于特定目的的数据整理，可能涉及逻辑、数学运算（加总、筛选、比较等）。数据处理存在深度、广度和识别度之分。此种划分在2012年《场外衍生品数据报告和整合安排》（Report on OTC Derivatives Data Reporting and Aggregation Requirement）中被首度提及，被2013年《数据的监管切入》（Authorities Access to Trade Repository Data）基本确立，且2014年《数据的整合进路》（Feasibility Study on Approaches to Aggregate OTC Derivatives Data）专门予以说明。

最核心的维度是数据处理深度（depth），这关乎监管机构获取的数据颗粒度（granular）。颗粒度犹如光谱，从精细向聚合可分为三层次。首先是交易层面的数据（transaction-level data），直指具体“交易”本身，包含单个交易细节，其未经逻辑或数学计算加工，能使监管者有效识别交易方和相关交易协议。其次是头寸层面的数据（position-level data），聚合度有所强化，是特定主体或部分产品“轧差”的净额，强调一方或多方参与者多个交易联动处理后的实际头寸风险，一般需要特定时点的截图式分析（snapshot）。最后是聚合层面的数据（aggregate-level data），〔38〕是指根据不同的种类（如产品、地区、货币等），通过逻辑、数学方式“加总”所有相关的整体数据，该数据不含任何单个交易信息，强调揭示市场全景，与数据统计基本为同义。

如果说深度是纵向切入的数据视角，那么广度（breadth）则是横向范围的数据维度，意在明晰监管获取的数据主体范围。不同监管主体有不同监管对象，根据权能差异，特定监管主体可能仅可获取部分对象的数据。如在分业监管模式下，证券监管部门对证券机构业务数据有抓取权限，但对银行的数据缺乏监管权能，故数据广度受限。

相较而言，识别度（identity）作为数据处理的第三个维度，是数据保护和商业秘密的重要维度，本质上是补充性角度的描述，强调数据具体信息显名与否。匿名化数据处理并不代表无法

〔37〕 See Denial I. R., Michal S. G., Access Barrier to Big Data, 59 *Arizona Law Review*, 353 (2015).

〔38〕 区分数据的聚合（data aggregation）和聚合的数据（aggregate-level data）的关键在于：前者是动态的过程，包含数据的深度、广度和识别度；而后者是名词，特指深度之第三层次，即市场的整体数据。

获取交易层信息，其只是将相关信息代码化处理，如法人识别码 LEI 的出现，即便匿名化，仍可揭示完整交易数据。值得说明的是，识别度之划分限于交易层面和头寸层面的数据，毕竟二者涉及具体交易方，但不适用于聚合层面的数据，因为后者是在整体层面的处理，不涉及具体交易，本身已匿名化，不存在有名与否的问题。

（二）不同监管目标需要的数据匹配：根基型、重心型与场景型

金融市场监管主体众多，如何厘清金融交易数据的监管面向至关重要。既有国际文件（表 1）尝试多维度的阐释，但缺乏类型化归纳。实际上，从理论角度提炼，借助功能性分类思路，金融监管可有三种类型，即根基型监管、重心型监管和场景型监管；不同监管类型又可细分，所需目标数据维度亦存差异（参见表 2）。

首先，“根基型监管”聚焦货币政策，此为金融市场运作的基础，法定准备金率、公开市场业务、贴现政策、基准利率等工具影响货币供应量的变化，金融的本质为资金的融通利用，利率和汇率更是金融市场交易的重要基准和参照，无论金融产品设计组合，抑或投资权衡，均与之紧密相关。具言之，货币政策又有管理货币政策（managing currency policies）和执行货币政策（implementing monetary policy）之别，从具体权属看，一般归于中央银行职能。关于目标数据要求，由于货币政策关涉整个市场变动，因此需更广的面向，法定货币下所有市场主体数据均要纳入。但深度方面二者存异，管理货币政策需关注具体交易清算（尤其是不同货币主体之间的兑换），明晰可能出现的大额交易或特殊交易以对峰值变化作政策回应，这需要交易类数据，同时也需全局性的聚合类数据作整体参照；执行货币政策则仅需聚合类数据。鉴于根基型监管不是合规型的一线监管，重点在于数据分析，对识别度要求较低，匿名数据即可。〔39〕

表 2　　不同监管目标需要的数据要求

监管类型 / 数据要求		根基型监管		重心型监管					场景型监管	
		管理货币政策	执行货币政策	双峰模式		分业模式			危机处置	最后贷款人
				审慎监管	行为监管	市场主体	中介机构	后台设施		
深度（depth）	聚合类	○	●	○						
	头寸类			○	○					●
	交易类	●		●	●	●	●	●	●	
广度（breadth）	大面向	■	■	■				□		
	中面向				■	■	■	■		
	小面向								■	■
识别度（identity）	有　名			❁	❁	❁	❁	❁	❁	❁
	匿　名	❁	❁	❁				❁		

注：表中的实心表示必需的数据要求；空心表示可能需要的数据要求。

其次，“重心型监管”关注具体机构、产品和交易行为，是监管的核心类型。根据监管方式

〔39〕 See CPSS-IOSCO，Authorities Access to Trade Repository Data，August 12，2013.

不同，又有双峰监管和分业模式之别。双峰监管强调审慎风险监管和行为合规监管的界分。〔40〕审慎监管以风险监管为导向，既有宏观审慎对系统性风险的评估和治理，又有微观审慎对具体对象风险的监测和处置。风险治理具有网络性特点，需大面向的数据覆盖，包括所有交易对手方（all counterparties），数据深度要包括交易类的精细化数据，特别对系统重要性金融机构（SIFIs）应有精确数据分析；基于宏观审慎目标，还需聚合类的全面向数据对风险整体评估；此外，微观审慎聚焦机构间的交易关联，对头寸类数据有所要求，以分析具体机构的业务轧差和风险敞口，但无须聚合类的市场全貌（表 2 中以“空心”表示）。数据识别度原则应为显名，但在宏观审慎的聚合类数据中无此要求。行为合规监管旨在监测和制止欺诈、内幕交易和操纵市场等破坏金融市场有序运行的行为。〔41〕其着眼于微观行为，监管需高精度的数据（参与方、时间、频率、标的、底层资产、价格等），故以交易类数据为必要；同时，由于部分交易结构复杂，监管需对嵌套的交易关系进行穿透式监管，此时则需轧差的头寸类数据；数据广度方面，行为监管重心聚焦于相关对象“中观”层面的数据，且违规行为的一线执行需要具体的有名数据支撑。

分业监管模式强调对市场主体的“跟踪式”盯防。传统视角关注市场主体和金融中介，但自 2012 年 PFMI 颁布后，金融市场基础设施被单独监管的趋向明显，不同法域陆续在监管当局设置专门机构负责 FMI 的监管。〔42〕分业模式下，监管市场主体和金融中介需要高精度的交易类数据，同时保证中观面向的数据广度（按银行、证券、保险等不同监管部门的分工权限获取），因监管执法需要，数据要显名。金融市场设施不仅须满足前述要求，若建立统一的交易报告库，还需覆盖全市场主体；因数据加工的层次性，部分数据可匿名化以满足其他监管主体所需。

再者，“场景型监管”重点关注如何介入危机状态，主要包括金融机构出清型的危机处置和恢复型的最后贷款人机制。最后贷款人（lender of last resort）主要指央行对陷入市场危机的金融机构进行救助。由于聚焦危机状态的个别机构，数据深度更关注轧差风险敞口，以估算流动性支持规模，数据来源以小面向的具体机构为主，又因救助的针对性，交易数据须明确显名。处置手段强调金融机构的有序退出，避免造成市场更大的波动。要有事前“遗嘱计划”（living will）。〔43〕因核心内容涉及具体主体关联网络、保证金、抵押品等资源结构、参与者风险敞口、风险负担等，需全面的交易类数据；因危机发生须个案分析，数据广度是小面向的主体，且要保证数据显名。

---

〔40〕 See Andrew Godwin，Guo Li，Ian Ramsay，Is Australia's Two Peak System of Financial Regulation A Model for China，46（2）*Hong Kong Law Journal*，621－646（2016）.

〔41〕 参见黄辉：《中国金融监管体制改革的逻辑与路径：国际经验与本土选择》，载《法学家》2019 年第 3 期。

〔42〕 如新加坡金管局（MAS）有市场政策和基础设施处（market policy and infrastructure），我国香港特别行政区的金融管理局（HKMA）的 13 个部门中有一个是金融基础设施处（financial infrastructure），澳大利亚证券投资委员会（ASIC）的市场局中下设市场基础设施处（market infrastructure）等。

〔43〕 See David K. Suska，Reappraising Dodd-Frank's Living Will Regime，36（2）*Review of Banking and Financial Law*，779－816（2016）.

（三）监管目标之外——参与方和公众对数据获取的边界

诚然，交易报告库的目标数据主要用于监管，但亦有向其他市场主体和公众披露的可能。首先，数据范围仅次于监管者的是交易参与方。参与方是指对相关具体金融交易具有法定权益的市场主体，数据的获取集中于自身数据和公共数据。目的有二：一是通过公共数据获得投资分析依据，二是自身数据的获取给非报告机构的交易对手方以纠错机会，提高交易准确性。鉴于此，数据深度上以交易类数据为主，且限于原始数据；数据原则上显名，但对标准化的聚合交易可匿名处理，重点保障交易准确性。〔44〕其次，公众对 TR 的数据获取本质为 TR 的主动披露。之所以向公众披露：一方面是由于 TR 的公共物品属性，提高金融市场透明度是其承担社会责任的方式；另一方面，非交易方的公众虽无直接交易行为，但是潜在的交易对象，市场信息的披露会影响其投资决策安排。须注意，此数据披露应严格限定于静态的聚合类数据，不能披露可识别的交易信息，否则可能泄露商业秘密，甚至减损部分信息中介主体的做市或经纪业务。

五、本土问题的比较审视

理想图景固然可期，现实问题亦不容忽视。我国金融市场基础设施发展滞后，以交易报告库为中心的数据报告机制更是阙如。随着金融风险的加剧，这将影响监管治理和金融市场稳定。本部分围绕监管和市场的关系，全面审视我国金融数据报告机制的问题。

（一）数据角度：多头监管治下的同类数据标准不一

即便在统一的市场中，也存在金融数据报告标准割裂的问题，更遑论监管割据的市场。我国金融市场实行分业监管，但因路径依赖和监管权力扩张，多头监管问题突显。以债券市场为例，便有央行、银保监会、证监会、发改委和财政部等多部门的存在，市场内部在监管博弈中形成了交易所市场、银行间市场和柜台市场“三分天下”的局面，而作为市场后台的登记托管结算服务亦散布于中证登、中债登、上清所。不同市场统计口径不一，市场数据难有兼容性的分析价值，相关风险敞口易被隐藏，〔45〕尤其头寸类数据缺乏客观的显示。不同交易市场、产品名称、登记结算后台也增加了交易者合规负担，为符合冗杂不一的数据要求，其不得不进行数据的拆解填报。

多头监管对数据报告的影响还存在于实质概念混杂。换言之，虽无直接数据报告机制之名，但通过相关法律转介和自我权能解释，行使数据报告的监管之实。例如，信息披露、信息公开、业务备案、金融登记、数据统计，五种概念具有信息交互之意，但功能不同。信息披露主要是上市公司及相关主体的法定义务，信息公开是更广义的信息披露（不限于上市公司），业务备案强调相关行业协会的信息记录（如私募基金产品），金融登记则是产品生效或发生对抗效力的要求，数据统计是金融监管当局获取市场整体情况的管理抓手。因缺乏严格意义的数据报告机制，这些

〔44〕 See Art 3.3.2.1 of Report on OTC Derivatives Data Reporting and Aggregation Requirement，2012.

〔45〕 参见夏露、庞业军：《交易报告库的发展经验及启示》，载《金融市场研究》2018 年第 2 期。

机制便不同程度地承担了替代性功能，但问题在于不同监管机构功能存异，具体机制的数据散乱，数据双花、难以兼容等问题突出，加之宏观审慎力所不逮，难以揭示系统性的金融风险全景，统一标准的专用性数据报告机制亟待构筑。

更须注意的是，由于缺乏法律授权，金融监管当局及相关市场监管者对数据报告均有“实然”的博弈空间，这不仅导致国内数据标准不一，而且影响国际机制的对接。不同主体均有对应职能的国际机构，如央行重点参与金融稳定理事会和国际清算银行的标准制定，证监会则对接国际证监会组织的标准，银保监会衔接巴塞尔银行监管委员会（BCBS）和国际保险监督官协会（IAIS）的标准。目前国际组织间的协调虽难，但已有基本共识（表 1 中，FSB 发挥“管弦乐”般的中心角色），〔46〕但反观国内，数据报告机制缺乏明确责任机构。以基础数据的主体和产品元素看，我国仍适用 2009 年编制的《金融机构编码规范》和 2010 年的《金融工具统计分类及编码标准（试行）》，国际通行的 LEI 和 UPI 编码未被强行推广，这造成国内标准和国际标准的不一，不利于金融交易数据的跨境流动，也无法有效嵌入境外交易报告库的数据分析和风险监测。〔47〕

（二）数据广度：分业监管造成的数据面向缺乏周延

除多头监管造成同类数据标准被“竞相关注”外，分业监管还导致金融交易数据存有漏洞、缺乏周延性。最明显的是，分业监管模式下金融监管强调“机构监管”，但存在以下两方面问题。其一，金融监管是中央垄断机制，当前金融机构被央行严格限定为 32 类，根据“剩余监管权理论”，以典当行、融资担保公司、商业保理公司、融资租赁机构、地方交易场所等为代表的市场机构只能被分散的地方金融监管部门管理，〔48〕而各地标准不一，数据对象范围不同，导致金融风险的监测“条块”割裂。其二，实践中诸多从事金融交易的机构并非金融监管所承认的“金融机构”。例如，基金业协会登记备案的“私募基金管理人”，支付宝、财付通的母公司蚂蚁科技、腾讯等“互联网金融机构”等，这些机构并非法定金融机构，但实际从事金融业务，难以被分业模式下的金融监管覆盖，形成了中国特色的影子银行网络，其金融交易数据未被有效收集，由此可能造成隐性风险传播。可见，目前尚欠缺以金融交易（而非机构）为主导的数据报告机制。

即使聚焦既有金融机构的数据报告，也存在数据“洼地”，即银行类数据为主，证券业数据相对孱弱。原因主要在于：银行类金融机构是资产型行业，银行“大而不倒”，本身需为其自营业务负责，且在中国，间接金融发展成熟，仍为主导模式，具有类政府的信誉；而证券业金融中介在“买者自负”原则下，责任相对较小，即便经手的业务体量巨大，有系统性风险之虞，但分业监管下强调“管机构”，证监会对交易数据的抓取分析更多是为了统计之用，有宏观审慎职能的央行却难以切入证券机构的监管数据。因此，证券业数据报告治理较为滞后。细究证券业数据

〔46〕 See Lucia Quaglia，Aneta Spendzharova，Regime Complexity and Managing Financial Data Stream：The Orchestration of Trade Reporting for Derivatives，Regulation and Governance，2021，p. 4.

〔47〕 See IOSCO，Market Fragmentation and Cross-border Regulation，June，Madrid，2019.

〔48〕 参见冯辉：《地方金融的央地协同治理及其法治路径》，载《法学家》2021 年第 5 期。

报告，又会发现存在“重证券、轻衍生品”的倾向。虽然除场内期货期权外，场外衍生品个性突出，标准化难度大，〔49〕给元素提取和报告增加了难度，但这并非充实的理由，毕竟 2008 年金融危机爆发后的数据报告机制便始于场外衍生品。目前我国衍生品市场发展逐步进入正轨，但数据治理仍有待加强，否则数据面向缺乏周延性。

从实体设施看，我国尚无实质的交易报告库，由于受分业监管影响，实践中“类 TR”（TR-like entity）芜乱发展。如图 2 所示，境外发达经济体 TR 数量多为 1 个，以保证金融交易数据的统合报告；即便是作为全球金融中心的美国和英国，TR 数量也是 4 个，整个欧盟地区 TR 数量也仅 10 个，〔50〕且其中多个 TR 具有国际影响力。而我国类 TR 数量多达 6 个（中国外汇交易中心、银行间交易商协会、中证报价系统、上海黄金交易所、上海清算所、中国期货市场监控中心交易报告库），具体设施的面向狭窄，多是监管机构的触手延伸（不同监管主导设立，缺乏统一的 TR）。因此，受制于国内市场的监管割裂，无法“拼凑出”金融市场数据全景。

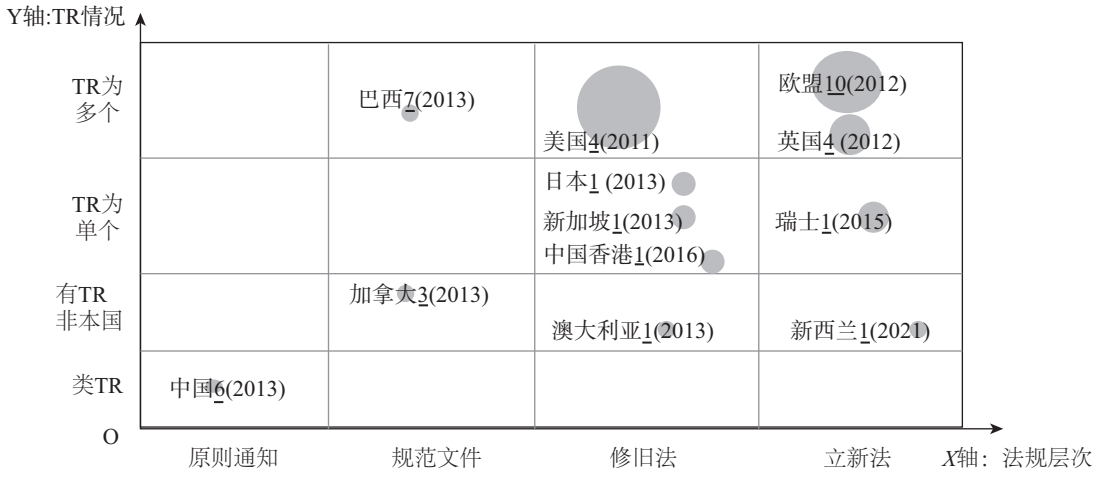

图 2　主要经济体的交易报告库制度层次及设施数量

注：1：TR 数量　　(2011)：法规发布时间　　●：跨国影响力。

（三）数据深度：监管治理滞后引致的底层数据离散

金融数据报告制度的初衷是风险监测，但目前过度聚焦于“交易”数据，而与交易相关的底层数据并未纳入监管视野。比如抵押品、担保、信用增进、主协议等虽与动态交易无关，但却是风险发生时的偿付支撑，对风险治理起到重要的应急作用。究其原因，首先是监管治理能力不

〔49〕 See Eric Helleiner, Stefano Pagliari, Irene Spagna, *Governing the World's Biggest Market: The Politics of Derivatives Regulation After the* 2008 *Crisis*, Oxford University Press, 2018, pp. 234 - 235.

〔50〕 各主要国家或地区的 TR 包括：瑞士，SIX-TR；中国香港，HKMA-TR；日本，DTCC-DR（JPN）；新加坡，DTCC-DR（SG）；澳大利亚，DTCC-DR（SG）；加拿大，CME-TR、DTRR（US）、ICE-TV；美国，BSDR、CME-TR、DTCC-DR（US）、ICE-TV；英国，ICE TV Europe、CME-ETR、DTCC-DR、Bloomberg；欧盟的 10 个，DTCC-DR、KDPW、Regis-TR、UNAVISTA、CME-TR、NEX、DTCC DR（Ireland）、UnaVista TRADE Echo、Bloomberg TR、ICE TV Europe。参见 CPMI-IOSCO 的 FMI-level 2 的报告；欧洲证券市场监管局（ESMA）的统计；FSB，OTC Derivatives Market Reforms: Note on Implementation progress for 2020。

足，基本交易数据暂且难以有效处理，更遑论底层数据的分析。事实上国际上已有解决方案，存在可参照的其他关键数据处理技术指引，并有 TR 的额外报告设置，但这在我国尚未引起重视。其次，与数据标准化不足有关，底层数据的多样化和个性化无疑增加了数据报告的复杂度，实践中多通过备案审查，以合规的定性测量为主，缺乏精细化定量评估，这在监管科技（Regtech）发展已较为充分的当下，显得过于滞后。再次，底层数据多涉及基础资产和担保品，但我国严格的民事担保机制未给金融商事担保留有足够空间，“严格的物权法定”使实践中被认可的非法定出质物欠缺法律承认而无法产生合法担保的效力，〔51〕这不仅增加了市场主体的报告疑虑，监管主体也多消极回应，以“沉默”的方式不置可否，如此便为实践中的“抽屉协议”提供了土壤，隐性金融风险滋生。

此外，审视具体的数据报告监管依据会发现，我国交易报告库制度基本空白。目前尚无专门性规范，仅有 2013 年央行和证监会发布的适用 PFMI 的原则通知，而数据报告的“增负”机制没有法定授权难以有力推进。反观其他主要经济体（参见图 2），TR 基本得到了法律层面认可，部分地区通过制定新法明确对金融市场基础设施的制度供给。如瑞士 2015 年制定世界首部《金融市场基础设施法》（FMIA），专章规定了 TR 的内容（第 5 章），新西兰也于 2021 年成为世界上第二个进行专门金融市场设施立法的国家。欧盟则早在 2012 年就制定了《欧盟基础设施条例》（EMIR）规范 TR 的运作和数据报告制度。除制定新法外，美国、日本、新加坡和中国香港地区也通过“修订旧法＋颁布具体规范”的方式制定 TR 的监管依据。大陆法和普通法并行的法域（如加拿大）和新兴的经济体巴西也颁布监管文件提供 TR 的运作指引。〔52〕

囿于制度依据不足，实践中类 TR 的运作多靠内部文件规范。〔53〕TR 并非只是数据传输体，作为主体组织亦有自身数据，这些运行的底层数据未被监管主力关注。而且，目前国内交易报告库监管治理几近空白。首先，TR 识别机制缺乏，作为金融市场基础设施，系统重要性识别是关键，但不仅规模（size）、可替代性（substitutability）和关联强度（interdependence）的标准未被前置分析，监管机构出于部门利益考量，还纷纷布局治下的数据设施建设，TR 被泛化适用，数据离散的问题不减反增。其次，TR 运作缺乏约束，数据处理缺少统一的规程指引，不同 TR 间缺乏互联互通机制，单向的线性报告使数据更为割裂。最后，TR 危机处置机制阙如，由于 TR 缺乏独立定位，多以交易所、行业协会、登记结算机构等形式存在，由相关金融监管主体主管，导致自身数据难被分享获取，央行对其他监管部门的 TR 缺乏治理权限，其力主的危机救济处置缺乏切入路径。

〔51〕 参见郑彧：《金融市场基础设施内部规则的法律保护》，载《华东政法大学学报》2020 年第 1 期。

〔52〕 各国和地区主要法规情况如下：（1）瑞士：《金融市场基础设施法》（FMIA）、《金融市场基础设施条例》（FMIO）、《金融市场基础设施规范》（FMIO-FINMA）；（2）新西兰：《金融市场基础设施法》（FMIA）；（3）欧盟：《欧盟基础设施条例》（EMIR）；（4）英国：即便是脱欧后，FMI 有本国之规定，但其 TR 一直适用于 EMIR；（5）美国：《商品交易法》（Commodity Exchange Act）；（6）日本：《金融工具和交易法》（Financial Instruments and Exchange Act）；（7）中国香港：《证券期货法》（SFA）和《证券期货市场（交易报告库）条例》[SF（TR）R]；（8）澳大利亚：《公司法》（The Corporations Act）Part 7.5A 和《衍生品交易报告库监管指引》（RG 249）；（9）巴西：《央行 25097 号文》；（10）加拿大：《交易报告库和衍生品数据报告 91－507 规则》（Rule 91－507）、《交易报告库和衍生品数据报告 96－101 工具》（Rule 96－101）。

〔53〕 2021 年 10 月 26 日，中证机构间报价系统股份有限公司发布《交易报告库管理办法》《交易报告库信息披露规则——场外衍生品业务》《交易报告库信息报送规则——场外衍生品业务》。

六、走向数据的聚合规制

数据本身价值有限，聚合处理则增进其价值。监管分业确实增加了数据统合难度，数据分散、重合、不周延问题突出，但这并不意味着缺乏应对之策。增量改革即为良策，即通过新设中心化的交易报告库，消弭监管冲突，并以此为轴心，前端加强基础数据元素的标准统一，后端强调目标数据的层次化处理，从而在设施、标准和监管层面实现聚合规制。

（一）设施之维：交易报告库的识别、运作和处置

交易报告库是金融市场基础设施的最新组成部分，那么缺乏先例的 TR 该由谁监管？受制于部门利益纠葛，监管多头配置不利于数据统合，统一监管为上策。不同于其他 FMI 涉及具体券款交互，TR 是与其并存的金融基础设施，这使得监管统合更具技术可行性。纵观境外监管模式，破除体制复杂性迈入“简仓式”（silo-like）单一监管是主流趋势，央行和证券监管领域是主要改革阵地。回观我国，随着 2018 年政府机构的改革，央行的金融稳定和宏观审慎职能得到强化，证监会则集中于微观审慎监管和行为监管。从 TR 风险监测功能看，央行作为唯一的监管机构更为合适，加之央行的全市场金融统计职能，数据处理经验丰富。2020 年发布的《中国人民银行法（修订草案征求意见稿）》亦遵循此思路，第 39 条将交易报告库监管列入央行权能。

此外，市场存在多少 TR 合适呢？作为数据中枢，首选方案是建立一个新的一站式（one-stop-shop）TR，〔54〕一则可避免受现存类 TR 的路径影响，二则更易获得全面的市场数据，增进数据整合度。次选方案是在合并既有分散的类 TR 基础上加强数据互通，这虽无法全面覆盖金融市场数据，但可适用于单一业务或具体产品的数据统合。然而要注意的是，由于目前我国多种金融业务尚缺乏类 TR，难以实现金融市场全景风险测算，加之数据联通亦耗费监管的协调成本和市场合规成本，该方案仅能作为过渡性的权宜之计。

比起设立，技术色彩浓厚的 TR 运行更为重要。在 PFMI 风险划分中，TR 核心风险即为运行风险（operational risk），〔55〕相较于支付系统、登记结算系统等的信用风险、流动性风险治理，TR 治理要义在于持续经营管理（Business Continuity Management）。毕竟作为数据中心，若 TR 服务中断，将导致市场数据陷入“黑箱”状态，不仅影响监管对市场的风险监测处理，还影响市场主体的公共安全预期。

以实质环节递进分析，TR 的运行治理主要应从识别计划和执行反馈展开。一方面，识别计划应重点关注业务影响分析（business impact analysis）和风险评估（risk assessment）。前者聚焦 TR 业务运行节点的内向审视，先通过业务流程、网络拓扑、组织结构等方式明晰自身的关键业务职能，绘制 TR 可视化的业务图；然后进行关联度研判，明确 TR 与其他金融主体、金融中介、FMI 的业务连接点，区分不同节点的重要程度，降低核心单点失败可能引发系统崩溃的风

〔54〕 实际上，从全球视野看，有观点主张建立全球统一的 TR，DTCC 已建立 GTR，并对接了 60 余个国家。但由于数据的主权安全和相关监管顾虑，更多市场机构主张标准的统一和各国 TR 的数据联通获取。

〔55〕 See Art 17－3.17.3 of Principle of Financial Market Infrastructures，2012.

险。而风险评估则是向外审视，即事先分析可能造成 TR 业务失序的风险，主要包括技术事件、人为破坏、自然灾害和社会事件四类，同时做好不同风险的发生概率预测及其影响分析。〔56〕

另一方面，执行反馈是对识别计划的落实，从市场运作要素观察，可锚定设施、人员和业务连续性计划三方面：（1）设施本身应有可扩展力（scalable capacity），即足以应对前述风险挑战，除本体赋能外，还应有备用站点的替代性安排，当出现运行中断时，可实现快速同步的接管运行；要定期对 TR 进行压力测试（stress test），监测评估其表现。（2）主体人员层面，雇员表现得当是运行风险预防和处理的关键；若人员素质欠佳，不仅影响外在风险处理，还可能成为风险诱因（如程序操作失误）；由于风险管理专业性和复杂度，要避免人员频繁变动，保证关键岗位（信息系统）的人员稳定性，加强人员的业务连续性培训和演练。（3）业务连续性计划（BCP），通过清单式的列举规定做好危机处置的双向安排，既有恢复救助的方案，也有风险出清的退出安排。BCP 应是一个动态文件，根据组织架构和业务特性定期（如一年）进行更新。〔57〕

实际上，法律制度缺位才是我国交易报告库发展的最大障碍，如何进行制度补足？短期内修法较为可行，这已在《中国人民银行法（修订草案征求意见稿）》中得以体现，其直接赋能明确 TR 监管权限，但问题是该法律规定篇幅有限，对于 FMI 的规定都是寥寥数语，遑论对交易报告库的着墨。本质上《中国人民银行法》仅能解决 TR 的正当性和监管主体的基本内容，TR 的识别、组织治理、行为机制、机制治理和危机处置难被嵌入其中，须通过后续的配套规章文件补充释明。因此，长远来看，立新法更为全面，这并非要求交易报告库专属立法，而是制定我国《金融市场基础设施法》。可借鉴瑞士的立法经验，以体系化内容对 FMI 进行全方位的规范，并设专章规定交易报告库的内容。此举优点还在于以特别法模式的“增量”改革，避免与既有立法产生冲突。即便日后市场变化，也可在该法中集中修改；同时，金融市场基础设施法的出台也有利于彰显我国在金融营商环境方面的努力，提高中国国际金融市场规则的话语权，推动中国金融向更大格局发展。

（二）标准之维：基础数据的对接、特色和话语权

交易报告库的数据来源于市场主体，其“报告”有两重含义，一是市场主体向 TR 的数据报告，二是 TR 向监管机构进行的目标数据报告。〔58〕目前，我国数据报告机制不仅缺乏 TR，更缺乏统一的元素标准。国际上围绕主体、产品和交易的 LEI、UTI 和 UPI 相对成熟（语义、属性、结构、格式），编码规范以通用性的字母和数字为组合，在保证中立的基础上，并于 2019 年实现了全面布局。当前是对接的最佳契机，虽然这难免有转接的成本，但标准明确，一方面将弥合当前央行、银保监会、证监会等金融监管主体各成体系的分割间隙，从制度层面促进数据兼容性，助益于金融市场风险的全景评估，另一方面，此标准由国际 FSB、IOSCO 及 ISO 组织力主推动，积极对接也有利于打开金融对外开放的新维度，增进金融交易全球化运作。

除对接标准外，鉴于当前数据报告机制处于发展初期，部分标准仍在变动中，标准之更迭是

〔56〕 See Basel Committee on Banking Supervision, High-level Principles for Business Continuity, August 2006; CPMI, IOSCO, Recovery of Financial Market Infrastructure, CPMI Paper No. 121, October 15, 2014.

〔57〕 新西兰规定两种方案：（i）当出现任何新情况可能实质影响既有计划时；（ii）当时间间隔超过 12 个月时。See Art. 47（1）（b）of FMI Bill Draft. 加拿大规定，根据商事实践进行合理的定期检验（on a reasonably frequent basis），并至少年度一次（at least annually）。See Art. 4. 9（b）of National Instrument 24－102 Clearing Agency Requirements.

〔58〕 See Scott O'Malia, Standardize, Digitize and Distribute, November 18, 2019.

全市场的整体行动，既有金融交易也有期限的持续，应尊重既有标准，并规定过渡期和替代性方案。此外，对接国际标准并非一味照搬。首先，可结合我国国情在成熟的国际公共服务产品外的其他关键数据（OCDE）要素中选择性适用。其次，加强标准的软联通，〔59〕强化汉字编码国家标准的实施，确保替代性标准在数字网络中的畅行。再次，境外市场以衍生品为主要交易报告类型，我国可统筹建立覆盖全市场的交易报告制度，进一步深化基础数据的元素要点，为国际规则增添中国智慧。实际上，在既有的数据标准国际文本中，从市场机构反馈看，中国参与度极低，〔60〕意见集中于美、英、日等发达市场主体。应进一步强化参与制定国际原则、指引和报告，增强在国际标准组织中的官方发声和政策意见反馈（policy feedback loop）。〔61〕

不仅如此，在清晰界定基础数据标准基础上，还要强化市场主体和 TR 的连结，明确向 TR 进行数据报告的要求，这主要包括：（1）报告主体。金融交易由双方或多方参与，国际上存在单边报告（美国）和双边报告（欧盟）模式。双边报告易造成数据双花，且增加市场主体报告义务。建议采用单边报告模式，但要允许交易对手方获取 TR 中涉及自身的交易数据以校验准确度；同时报告主体不能以金融机构为限，应以交易活动实质涉及方为准，增进数据报告的强制性。（2）报告范围。尽管在境外 TR 发端于场外衍生品市场，但其机制可彰显“举重以明轻”，即复杂场外衍生品交易尚可标准化报告，其他金融产品也应被全面纳入，如欧盟《金融工具条例》即包括权益类工具、债券、衍生品、结构化产品、排放配额等。（3）报告内容。需有基本数据的强制报告和额外数据的自愿报告，基本数据围绕主体、产品和交易信息三个元素板块展开，但具体信息点可以拆解，如欧盟 MiFIR 有 65 个信息报告点，瑞士 FMIA 则根据不同产品分类规定 79 个信息点。

（三）监管之维：目标数据的分类、分层及其规程

无论基础数据的标准化，还是交易报告库的处理，其最终目的在于服务监管需求。那么，作为数据中枢的 TR 如何对接监管？可有两种模式：一种是继续的报告机制，另一种是监管的端口接入。当前技术条件已成熟，建议采用第二种模式，从而充分发挥监管的主动性。另外，金融监管机构多元，首先应基于分类视角，对不同监管机构设置不同数据报告的接入面向。例如，瑞士 FMIO 的第 62 条即规定五类机构，其央行和金融监管局可获得所有交易数据，瑞士收购委员会仅能获得与收购程序有关的衍生品数据，联邦审计局则获得接入要求审计公司特殊程序介入的数据，竞争委员会获得与竞争领域有关的数据，电力委员会获得底层资产与电力相关的数据；其范围不以分业为限，而根据风险点和监管权能的匹配予以设定。我国亦可借鉴分类化的路径，如央行作为主管机构接入全部数据，证监会和银保监会根据分业监管获取相关业务数据；此外，立法应留有兜底条款为其他监管部门（如网络安全部门等）的接入提供可能。为避免利益冲突，国内监管机构的数据接入权限的裁量权可授予金融稳定发展委员会。

---

〔59〕 参见杨富玉：《推动金融数据标准化建设》，载《中国金融》2020 年第 22 期。

〔60〕 在 9 个国际文件中，有 284 个/次机构的反馈，我国仅有 6 次发声（不包括港澳台地区）（均为外汇交易中心），占比 2.1%。

〔61〕 See A. L. Newman, E. Posner, Transitional Feedback, Soft Law and Preferences in Global Financial Regulation, 23 (1) *Review of International Political Economy*, 123 - 152 (2016).

同时，由于日益凸显的金融交易跨域性特点，数据跨境流动趋势不断增强，为更好地获取数据面向，数据流动也应有必要的机制安排，这体现在为境外机构接入 TR 提供可能。〔62〕但数据流动应有限制，数据已不仅是个别的信息识别，更涉及主权安全、商业价值等利益考量，至少要有三方面的约束。首先，双边对等，在无国际条约和全球交易报告库之前，可与境外当局签订双边备忘录实现数据接入之对等安排；其次，境内数据流出当满足《数据安全法》《个人信息保护法》及《网络安全法》的底线要求，以安全价值为核心遵循，促进数据的安全审查和必要性调取；再次，境外监管当局应对获取的信息进行充分保密，避免数据泄露和商业利用。此外，尽管双边备忘录是基础，但在第一次接入时，仍存在审查批准之必要。〔63〕在我国应保证统一主体行使以明确权责，央行可为 TR 的适格监管机构，以保证审查之及时和对 TR 的数据获取。

尽管 TR 核心功能在于服务监管，但其作为公共物品，亦有对交易相关方和市场公众的披露潜能，以保证数据准确性、促进市场信息透明度，但应有分层的限制规定。具言之，对交易相关方，可允许数据“传递”（data transmission），其以申请为前提，批准主体为 TR，并限于申请人自身的数据，以交互验证交易准确性。对社会公众，监管应保障 TR 具有数据“公开”（publication of data）制度，以聚合性分类数据为主，揭示整体市场概况（如规模、头寸及必要的价格等）。应注意的是，也可披露匿名化的单个交易数据（如交易前手），但不能直接或间接显露或为其他技术分析提供揭示潜在具体交易参与方的数据。

七、余论：从数据报告到数据共享

从监管溯源看，数据报告并非新近之物，但以交易报告库为中枢的数据报告机制确为新创。这与金融爆炸式增长的经济创新和透明度不足亟待监管回应有关，也与技术的成熟发展紧密联系。TR 自 2012 年后步入规范布局集中期，技术兼容的互联互通式完善为“中心化”的报告提供了基础。同时，以区块链技术为代表的“去中心化”技术革命亦相伴而生，其初衷便在于改革金融基础设施，〔64〕那么其对以 TR 为中心的数据报告机制有何种冲击，值得审视。

笔者认为，影响面有限。一则，区块链技术强调分布式记账，本质是账本共享，强调交易即报告，改变的是计账模式（从账户到通证），而非“账目”要素。金融监管风险监测需要的并非整体的“数据团”，而是数据里蕴藏的信息价值。因此，主体、产品及交易变化等信息仍为核心，要素标准化趋势不会改变。二则，即便区块链“侵入”TR 本身，亦不能以完全去中心化模式运作，毕竟在金融主权和国家安全面前，技术创新须让位于安全价值。去中心化的区块链推崇分布式的匿名化数据记录，这与监管导向的数据报告相悖；且服务于监管需求的 TR，其作为公共物品，需要中心化的负责主体，否则一旦出现运行危机，恐难以修复。三则，区块链技术尚不足以

〔62〕 See Nivedia Sen, Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path, 21 (2) *Journal of International Economic Law*, 323 - 348 (2018).

〔63〕 相关机构需要提交数据申请表（data request form），包括五类基本内容：①申请机构的信息；②数据获取的法律依据；③申请数据的原因和权限范围；④申请的数据描述；⑤对数据的保密性措施。

〔64〕 See Sara Feenan, Decentralized Financial Market Infrastructure: Evolution from Intermediated Structure to Decentralized Structures for Financial Agreements, 2020.

引发系统性变革。数据报告的核心在于全景性分析，个别的设施运用非但不会带来创新，还会割裂数据互通，增加监管负担，影响数据广度。〔65〕

但长远来看，亦不能轻视区块链等金融科技的影响，其在监管导向下仍有适用空间。〔66〕这主要指向目标数据获取的自动化处置，其可以增强算法设计，提高数据存储、计算的能力，并通过智能合约向不同访问权限的利益主体、社会公众及监管主体披露不同颗粒的交易数据，以减少报告时间差，实现由“报告到共享”的转化。但该模式仍需人工合规审查，毕竟不同机构多大程度上获取 TR 的数据离不开监管者的主观裁量。综上，技术的颠覆式创新尚无法产生“去中心化”的效果，中心化的数据报告仍是大势所趋。

Abstract：The use of data is not only necessary for transactions in private law，but also for supervision in public law. In the context of increasingly strengthened prevention and resolution of financial risks，it is crucial to innovate and systematically examine the data reporting mechanism aiming at enhancing transaction transparency. Different from the data protection concerned by civil law，data transactions at the commercial level and data statistics from the regulatory perspective，data reporting can be analyzed from three dimensions：the central dimension is the facility aggregation operation of the trade repository，the basic dimension is the data standard architecture of front-end entities，products and transactions，and the key dimension is the classification，integration and hierarchical use of back-end target data. Due to the lag of multi-head supervision，separate supervision and feeble regulatory governance，there are prominent problems in China's financial transaction data reporting system，such as discrete angle，insufficient breadth and lack of depth，different data caliber，narrow data orientation，insufficient data risk disclosure and so on. The strategies to solve such problems are as follows：first，to strengthen the identification，regulation，operation governance and crisis resolution of the trade repository；second，to promote the docking and transformation of data standards，feature shaping and international voice competition；third，to clarify the data acquisition arrangements of different regulators. At the same time，we should also pay attention to the impact of decentralized technology represented by block-chain on the data reporting system. The vision of data sharing replacing data reporting is not feasible for the time being.

Key Words：financial transaction data，trade repository，FMI，data transaction，data protection

（责任编辑：李　敏　赵建蕊）

〔65〕 See FSI，From Data Reporting to Data-sharing：How Far Can Suptech and Other Innovations Challenge the Statue Quo of Regulatory Reporting，FSI Insights on Policy Implementation No. 29，December 2020.

〔66〕 参见姚前：《基于区块链的 OTC 衍生品金融基础设施》，载《当代金融家》2021 年第 7 期。

财经法学 No. 6，2022
pp. 111 - 124

自由贸易协定金融信息传送规则构建

马　光　卜小翠*

内容提要：在国际贸易法框架下，金融信息传送规则中最核心的“金融信息传送”条款源起于乌拉圭回合一揽子协定中《关于金融服务承诺的谅解》中的“信息传送和信息处理”条款，后在各FTA中也相继出现。数字经济背景下，对跨境数据流动规制的关注开始集中于电子商务和数字贸易领域，“金融信息传送”条款也因此在近年来的FTA中被电子商务或数字贸易的跨境信息传送规则所吸收。然而一体化规制方法仍然存在许多基础性问题待解决，应当谨慎看待。现阶段，“金融信息传送”条款已经发展出了“金融信息传送自由原则＋个人数据、个人隐私、个人记录和账户机密性例外＋有限度的监管例外”的基本结构，并在数据本地化问题下衍生出了“金融服务计算设施所在地规则”。中国应在坚持数据主权立场的基础上，升级FTA金融信息传送规则，从国际规则遵守者向国际规则制定者转变，以期维护本国在金融服务领域和数字科技领域的进攻利益。

关键词：跨境数据流动　金融信息传送　FTA金融信息传送条款　金融数据出境

一、引言

全球数字化背景下，跨境数据流动成为推动全球经济发展的重要力量。麦肯锡全球研究院2016年的报告指出：“实物商品和资金的流动曾是20世纪全球经济的标志，但如今这些流动已经趋于平缓或下降。21世纪的全球化越来越被数据和信息流所定义。数据和信息流几乎支撑了传统

* 马光，浙江大学光华法学院副教授、浙江大学国际法研究所执行所长；卜小翠，浙江大学光华法学院硕士研究生。

本文为国家社会科学基金重大项目“建立健全我国网络综合治理体系研究”（20ZDA062）、浙江省科技计划项目“智能司法开放创新平台开发及应用示范——基于人工智能的司法服务平台及示范应用”（2020C01060）的阶段性成果，浙江省法学会2022年度法学研究课题“涉外企业合规风险控制研究”（2022NB14）的成果。

贸易中的所有跨境交易，同时在世界各地传递着思想和创新。”〔1〕跨境数据流的惊人增长和潜在经济效益已经引起了全球监管者对跨境数据流动规制的广泛关注。从实践来看，国际社会目前的共识是：贸易协定是管理跨境数据流的适当场所。因为当信息跨境流动时，这些流动似乎基本上与贸易相关。〔2〕

国际贸易法对跨境数据流动的关注最早出现在电信、金融等特定服务部门。其中，以乌拉圭回合一揽子协定中《关于金融服务承诺的谅解》（以下简称为《谅解》）〔3〕的“信息传送和信息处理”条款最为典型。根据《谅解》，以经济合作与发展组织（以下简称 OECD）成员国为主的 34 个世界贸易组织（以下简称为 WTO）成员自愿作出更高水平的金融服务开放承诺，且此类承诺按照最惠国待遇适用于所有 WTO 成员。〔4〕随着电子商务和数字贸易的日渐兴起，一方面，由于 WTO 在制定规则以应对世界经济中与数据相关的变化上停滞不前，世界主要经济体逐渐转向以自由贸易协定（以下简称为 FTA）作为规则升级的主要平台，《谅解》金融信息传送条款也随之被众多高标准 FTA 所吸收；另一方面，自《美国—韩国 FTA》首次在电子商务章节纳入跨境信息流动条款后，对跨境数据流动规制的关注开始集中于电子商务和数字贸易领域，并在近年来的 FTA 中呈现了跨境信息传送一体化规制的趋势。〔5〕由此提出的问题是：金融信息传送是否还有单独规制的必要。

当前，除《区域全面经济伙伴关系协定》（以下简称为 RCEP）外，中国已签署的 16 个 FTA 皆未规定金融信息传送条款。〔6〕关于我国已签订 FTA 金融信息传送规则设置情况请参见表 1。就文本而言，这些 FTA 仍有较大完善空间。鉴于我国已基于 RCEP 条款承诺金融信息传送，跨境金融数据流动议题也已在不同程度上为各处于磋商阶段的区域及双边经贸协定所触及，深化对该条款的探究，提出关于中国在该议题上的主张的建议具有突出现实意义。

有鉴于此，本文将分析梳理 FTA 金融信息传送规则的发展脉络，进而结合各国治理动向，揭示各国数据治理日渐趋同的现象，并深入探析金融信息传送规则的逻辑构建。在此基础上，本文将根据中国的基本立场，详细擘画中国应采取何种条款表达。

---

〔1〕 See Mckinsey Global Institute, Digital globalization: The new era of global flows, Report (Feb. 24, 2016), available at https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization- the-new-era-of-global-flows, last visited on May 2, 2022.

〔2〕 See Susan Ariel Aaronson, Data Is Different, So Policymakers Should Pay Close Attention to Its Governance, in Mira Burri ed., *Big Data and Global Trade Law*, Cambridge University Press, 2021, p. 342.

〔3〕 值得说明的是，《谅解》与《服务贸易总协定金融服务附件》（以下简称为《GATS 金融服务附件》）为两个不同的法律文件，《GATS 金融服务附件》属于 GATS 的一部分，而《谅解》不是 GATS 的一部分，但被附加到乌拉圭回合的最后文件中。中国未签署《谅解》。

〔4〕 See Chantal Thomas, Globalization in Financial Services—What Role for GATS, 21 *Annual Review of Banking Law* 323, 324 (2001)，转引自杨幸幸：《〈美墨加协定〉金融服务规则的新发展——以 GATS 与 CPTPP 为比较视角》，载《经贸法律评论》2019 年第 4 期。

〔5〕《澳大利亚—新加坡数字经济协定》（以下简称为 ASDEA）、《美国—日本数字贸易协定》（以下简称为 USJDTA）及《WTO 电子商务谈判合并文本》（以下简称为《合并文本》）、《欧盟—澳大利亚/新西兰贸易协定》谈判中欧盟方面提交的初始文本皆采取了此种安排。

〔6〕 中国与毛里求斯、韩国、澳大利亚、新加坡、智利的 FTA 中单设电子商务章节，但电子商务章节也未设置信息传送相关条款。

表 1　　中国已签订 FTA 金融信息传送规则设置情况汇总表

类别	名称/参与方	金融信息传送条款定位	其他金融信息相关条款	中方金融服务承诺
多边 FTA	RCEP（含中国、日本、韩国、澳大利亚、新西兰、东盟十国）	第八章　附件一“金融服务” 第九条　“信息传送与信息处理”	（1）定义条款： 金融服务包括以下活动：其他金融服务提供者提供和传送金融信息、金融数据处理及相关软件。 （2）特定信息处理条款或国内法规条款： 本协定的任何条款/本章的任何规定不得解释为要求一缔约方披露与个人客户相关的事务和账户信息，或公共实体拥有的任何机密或专有信息。	在“跨境提供”方式下： 提供和传送金融信息、金融数据处理以及与其他金融服务提供者有关的软件。
双边 FTA	中国、韩国	单设第九章“金融服务”章节，未规定信息传送条款		
	中国、毛里求斯	“金融服务”作为“服务贸易”章节的章节或附件，未规定信息传送条款		
	中国、格鲁吉亚			
	中国、澳大利亚			
	中国、瑞士			
	中国、冰岛	设“服务贸易”章节，在条文中纳入《GATS 金融服务附件》	定义条款： 金融服务包括以下活动：其他金融服务提供者提供和传送金融信息、金融数据处理及相关软件。	
	中国、东盟（含文莱、柬埔寨、印度尼西亚、老挝、马来西亚、缅甸、菲律宾、新加坡、泰国、越南）			
	中国、新加坡			
	中国、巴基斯坦			
	中国、柬埔寨			
	中国、秘鲁			
	中国、新西兰	或明确已签署协定不适用于金融服务，或无相关规定也未明确纳入 GATS 金融服务规则	无	未承诺金融服务开放
	中国、智利			
	中国、哥斯达黎加			
	中国、马尔代夫	无公开文本		

二、FTA 金融信息传送规则发展脉络

（一）FTA 金融信息传送规则体系

金融服务的提供与金融信息密不可分。系统来看，FTA 对金融信息传送问题的规制主要包括三部分。

一是以金融服务定义条款为基础的金融信息传送承诺。涉及金融服务内容的 FTA 大多沿袭了 GTAS 对金融服务的范围界定：“金融服务包括提供和传送其他金融服务提供者提供的金融信息、金融数据处理和相关软件的活动。”也即，如有关国家在金融服务类别下进行了承诺，则须保证相应的金融信息传送可实现。如《新西兰—新加坡更紧密经济伙伴关系协定》规定：“跨境

提供模式的承诺仅限于：提供和传送上文（k）段所述的金融信息和金融数据处理……不包括中介服务。”《韩国—新加坡 FTA》承诺：“外国银行的新加坡分行可以将数据传送到其总部和姐妹分行进行处理，前提是存在适当的控制措施，数据/信息的完整性和保密性得到保障，并且允许新加坡金融管理局在处理数据/信息的地方现场访问数据/信息。”我国在中韩、中澳等多个 FTA 中承诺了“跨境提供”方式下开放“提供和传送金融信息、金融数据处理以及与其他金融服务提供者有关的软件”。美国在与新加坡、智利等国的 FTA 中也都承诺了此类信息传送。

二是专门以金融信息处理和传送为内容的条款，也即本文重点探讨的金融信息传送条款。除《谅解》以外，《新加坡—澳大利亚 FTA》最早采纳了类似的明确规定：“任何一方均不得阻止信息传送，包括通过电子方式传送数据，保护个人数据的限制除外。”《美国—新加坡 FTA》也纳入了这一规定的软化版：“根据任何一方的要求，金融服务委员会应考虑与以下事项有关的任何事项：（a）金融机构以电子或其他形式将信息转入或转出一方的领土，如该等数据处理是日常经营所需的；（b）在处理和传播个人数据方面保护个人隐私，以及保护个人记录和账户的机密性。”《印度—新加坡全面经济合作协定》《哥伦比亚—欧洲自由贸易联盟成员国 FTA》《日本—瑞士 FTA》及其后的诸多双边、多边 FTA 都在金融服务规则部分设置了该条款。

三是作为限制的“特定信息的处理”条款。该条款以传统金融信息保密要求为基础。比较典型的如《以色列—哥伦比亚 FTA》规定：“本协定中的任何内容均不得解释为要求一方披露与个人数据、个人客户事务和账户有关的信息，或公共实体拥有的任何机密或专有信息。”类似地，《哥伦比亚—巴拿马 FTA》规定：“1. 本章的任何规定均不要求一方披露或允许访问：（a）金融机构或跨境金融服务提供者的个人客户的财务和账户相关信息；或（b）披露可能会妨碍遵守法律或以其他方式违反公共利益或损害特定公司的合法商业利益的任何机密信息。2. 在不影响双方监管机构签署的谅解备忘录的情况下，为合并监管目的，双方承诺不禁止子公司及在其境内设立的子公司将信息传递给母公司所在地监管机构。前款所称信息包括反映子公司或子公司财务状况的信息，包括其资产、风险管理和公司治理情况的信息。”《加拿大—韩国 FTA》《新加坡—澳大利亚 FTA（升级版）》《欧盟—墨西哥现代化全球协定》也都包含了禁止要求披露保密信息的规则。

从特别承诺到金融信息传送条款的发展可以视作金融信息传送领域的负面清单化，反映了全球数字化经济语境下的贸易规则调适。同时，在这一背景下仍然可以看到金融发达国家与金融欠发达国家间金融开放水平的巨大差异：约有 71 个 FTA 文本包含金融信息传送相关内容，而明确设有信息处理或信息传送条款的不到半数，且缔约方主要为美国、欧盟、新加坡、澳大利亚、加拿大、日本、韩国。〔7〕此外，尽管欧盟和美国通常被视为跨境数据流动规制的两大规则制定者，但在金融信息传送领域，新加坡似乎脱颖而出，这也与新加坡高度依赖国际金融的发展模式相符。

〔7〕 参见瑞士卢塞恩大学对贸易协定中电子商务和数字贸易条款数据库的粗略统计，载 https://www.unilu.ch/en/faculties/faculty-of-law/professorships/managing-director-internationalisation/research/taped/#：～：text＝The%20TAPED%20dataset%20has%20been%20created%20under%20the，is%20sponsored%20by%20the%20Swiss%20National%20Science%20Foundation，最后访问时间：2022 年 5 月 2 日。

（二）FTA 金融信息传送条款演进

1. 现有 FTA 金融信息传送条款结构演变

FTA 金融信息条款的规则结构演变，分为金融服务规则内单独规制和跨境信息传送一体化规制两个阶段。

第一阶段单独规制以《全面与进步跨太平洋伙伴关系协定》（以下简称为 CPTPP）、《美国—墨西哥—加拿大协定》（以下简称为 USMCA）、RCEP 三大多边 FTA 为代表。《谅解》“信息传送和信息处理”条款确立了“金融信息传送自由原则＋个人数据、个人隐私、个人记录和账户机密性例外”的基础规则结构。CPTPP 金融服务附件的“信息传送”条款在此基础上增加了“基于审慎考虑，要求一金融机构事先获得相关监管机构的授权，以指定一特定企业作为此类信息的接收方”的国家监管权内容。USMCA 金融服务章节的“信息传送”条款将“日常经营所需”限定改为“在许可、授权或注册范围内从事经营”限定，增强了规则明确度，并在实质上进一步增加了国家监管权的内容。但 CPTPP 及 USMCA 均未在“信息传送”条款中明确提及国家监管权，尽管“例外”条款包含“审慎监管例外”，但文本表达限定较多，因而在金融信息传送问题上还是呈现私主体本位的高度自由化理念。

与上述两个美式多边 FTA 不同，RCEP 金融服务附件“信息传送与信息处理”条款转向了国家本位的数据主权理念。该条首先明确了尊重各国国内监管要求的条约立场，其规则结构可以概括为“符合国内法要求的金融信息传送自由”。目前明确列出的两项要求包括传统的“保护个人数据、个人隐私，以及个人记录和账户机密性”及颇受争议的“遵守与数据管理、存储和系统维护、保留在其领土内的记录副本相关的法律和法规”。但从条约解释角度，国家可采取的监管要求并不限于该两项，因此给各缔约国留下了较大空间。究其原因，一方面，RCEP 作为目前全球最大的 FTA，因为各缔约方金融开放程度差异较大，所以在信息传送条款上也呈现出包容性特征。另一方面，以国家传统主权边界为中心的网络主权与数据主权论近年来得到愈来愈多的支持。《中国—东盟关于建立数字经济合作伙伴关系的倡议》提出，“在考察各国法律与社会实际基础上，充分尊重网络主权”，“推动建立多边、民主、透明的全球网络空间命运共同体”。网络主权理论的兴起，在国际政治格局上，以后发国家在网络空间的话语权提升为背景，在当代国际法上，则显示出国家主权在国际社会治理中的绝对核心地位仍不可撼动。在此演化趋势下，网络空间的数据已经转变成为一种战略资源，并将构成一种全新的国家权力要素。〔8〕有学者在对亚太地区的研究中指出：“（信息）国际传送限制在某些方面可以支持国内经济发展，同时也可以作为复杂贸易谈判和地缘政治定位的杠杆。”〔9〕

跨境信息传送一体化规制以 ASDEA 为代表。全球数字竞争格局下，美欧之外的经济体也开始在国际经贸规则变革中发力。ASDEA 将金融信息跨境传送纳入第 23 条“以电子方式跨境传送

〔8〕 See Brad Brown，Michael Chui & James Manyika，Are you Ready for the Era of “Big Data”，4 *McKinsey Quarterly* 24，34（2011），转引自沈逸：《全球网络空间治理与金砖国家合作》，载《国际观察》2014 年第 4 期。

〔9〕 See Clarisse Girot，Mark Parsons & Olga Ganopolsky，Data Transfers After Schrems II：Reflections from the Asia Pacific，Cross-border Data Forum（Jan. 21，2021），available at https://www.crossborderdataforum.org/data-transfers-after-schrems-ii-reflections-from-the-asia-pacific/，last visited on May 7，2022.

信息”条款中统一规制，不再单列。第一，该条首先承认各缔约方对信息传送有其各自的监管要求，融合了国家本位的规制理念。第二，该条以跨境信息传送总体自由为原则（包括个人信息跨境传送自由），同时沿袭了主流“目的限定”而非 USMCA“经营范围限定”的做法。第三，该条对国内监管进行了严格的手段和限度限定：“各国为实现公共政策目标，有权采取或维持与前款要求不一致的措施，但该措施必须：(a) 未以构成任意或不合理歧视手段或变相限制贸易的方式实施；以及 (b) 不会对信息传送施加超过实现目标所需的限制。”不可否认，实际上监管例外能够符合上述所有条件并非易事。〔10〕因此，ASDEA 第一款虽然与 RCEP 表达类似，但效果完全不同，仅是一种调和式的立场宣示。而对于传统的“个人数据、个人隐私，以及个人记录和账户机密性”内容，ASDEA 单列了“个人信息保护”条款进行保护，并将其置于“以电子方式跨境传送信息”条款之前，从而将个人信息保护提高到与跨境信息传送同等地位，不再作为例外事项。

2. 现有 FTA 金融信息传送条款呈现的问题

总体来看，当前诸 FTA 金融服务规则异质化程度高，金融信息传送条款用语不统一，〔11〕规制逻辑也尚未完全梳理清晰，在数据本地化与金融信息传送的关系处理上尤是如此。自 USMCA 在“金融信息传送”条款后一条设置了“计算设施的位置”条款后，USJDTA、ASDEA、《英国—日本全面经济伙伴关系协定》（以下简称为 UKJCEPA）、《合并文本》也都引入了这一规则。计算设施所在地条款可以看作自由主义理念“禁止数据本地化”追求下的规则软化处理，与雷曼兄弟破产案后美国财政部、联邦证券交易委员会等金融监管机构考虑在 FTA 中保留金融数据存储和处理本地化要求的政策空间和美国金融产业界追求数据自由流动利益间的冲突博弈不无相关。〔12〕曾有解读指出，USMCA 的规定与 CPTPP 类似，但未规定可出于审慎考虑要求事先获得监管机构授权，以指定特定信息接收方。〔13〕该观点显然忽视了“金融信息传送”条款与“计算设施所在地”条款的紧密关联，CPTPP 的注释中明确指出：一方可采取或维持不违反本协定的措施，包括符合“例外”条款的任何措施，例如一项措施要求一金融实体事先获得金融监管机构的授权，指定特定企业作为该信息的接收人。但从另一个方面，这也是 FTA 金融信息传送条款逻辑不清的例证。欧盟—澳大利亚、欧盟—新西兰贸易协定谈判中，欧盟提交的初步文本（以下简称为《初步文本》）对此呈现得更为明显：一体化规制趋势下，《初步文本》同样未在“服务与投资”章下的金融服务一节纳入信息传送条款，而在“数字贸易”一章中统一规制，但其“跨境数据流动”条款却以大篇幅阐明禁止本地化要求，根据该条规定，“缔约方承诺确保跨境数据自由流动，以促进数字经济中的贸易”，“为此，双方之间的跨境数据流动不应受到以下限制：a) 要求在缔约方境内使用计算设施进行处理，包括强制使用在缔约方境内认证或批

〔10〕 参见马光：《论国际法上网络安全的定义和相关国际规则的制定》，载《中国政法大学学报》2019 年第 3 期。

〔11〕 当前国际层面“数据”与“信息”的内涵差异尚未完全厘清。大部分 FTA 使用“信息传送”作为条款名称，但也存在一些 FTA 使用“数据处理、数据跨境流动”等表述，目前没有条款对金融信息、数据流动或信息传送等用语进行法律界定，不同的用语是否会引起规制范围不同从而使法律效果不同还有待观察。

〔12〕 参见前引〔4〕，杨幸幸文。

〔13〕 参见朱隽：《CPTPP 规则解读之四：金融服务规则》，载微信公众号“国际经济法评论”，2021 年 9 月 22 日。

准的计算设施；b）要求在缔约方境内对数据进行本地化，以便存储或处理；c）禁止在另一方境内储存或加工；d）根据缔约方境内计算设施的使用情况或缔约方境内的本地化要求，进行跨境数据传送”。该条款的逻辑性值得商榷。

三、金融信息传送条款构建的各国路径选择

（一）金融信息传送条款定位

USJDTA、ASDEA 两个数字经济协定对金融信息传送条款的性质及其规则结构进行了重构。传统金融信息传送条款置于金融服务章节，其定性和范围仍然限于“服务”；USJDTA、ASDEA 将金融信息传送纳入数字贸易、数字经济章节，并将范围限于“通过电子手段”，此时金融信息传送不再作为“金融服务”的内容，而是“信息/数据流动”的内容，服务和商品的定性界分被模糊，承诺的范围形式、法律后果都较传统 WTO 语境不同。当前国际社会较普遍地认为数字经济协定是经济联盟的新趋势或新阶段，〔14〕但目前尚缺乏对核心概念的一致定义，不同协定使用的术语及涉及的方面也不同。ASDEA、DEPA 使用“数字经济”，USJDTA、USMCA 使用“数字贸易”，CPTPP、RCEP 则使用“电子商务”。〔15〕此外，在“信息/数据”项下，协定对数据分类和平台类型予以进一步考量，监管中国内各部门间的协调、国家安全和敏感性问题、对文化敏感的解释和适用问题以及国内登记和分类问题也都值得进一步思考。与之相比，《合并文本》和《初步文本》直接将现有信息传送条款的内容合并至电子商务章节的做法则更欠缺逻辑性。UKJCEPA 未改变“金融信息传送”从属于“金融服务”的定性，并将条款名称改为“金融信息”，在其中纳入“金融信息传送自由原则”“个人数据、个人隐私以及个人记录和账户机密性例外”“金融服务计算设施所在地规则”的处理方式是目前为止保守路径下最完善且逻辑自洽的做法。最新 FTA 金融信息传送条款设置情况的对比请参见表 2。

表 2　　最新 FTA 金融信息传送条款设置情况对比

名称	金融信息传送条款设置方式	金融信息传送条款定位
USJDTA	第 5 条审慎例外、货币和汇率政策例外 第 11 条电子方式跨境信息传送 第 13 条金融服务提供者的金融服务计算设施位置 第 15 条个人信息保护	数字贸易章节

〔14〕 See Yaroslav Lissovolik, Digital Economy Agreements: The New Phase in Economic Alliances, Valdai Discussion Club (Feb. 10, 2021), available at https://valdaiclub.com/a/highlights/digital-economy-agreements-the-new-phase/, last visited on May 7, 2022; Shen Yi, Digital Agreements: New Trends in International Alliances, Valdai Discussion Club (Apr. 27, 2021), available at https://valdaiclub.com/a/highlights/digital-agreements-new-trends-in-international-all/, last visited on May 7, 2022.

〔15〕 目前世界上尚无普遍得到认可的电子商务和数字贸易定义，实际上两个概念在多数情况下得以混用。例如，从美国所发起或签订的 FTA 来看，USMCA 之前的 FTA 均采用了“电子商务”的用词，而在 USMCA 中，在内容几乎相同的情况下，“电子商务”章节名称更名为“数字贸易”。参见马光：《国际数字贸易规则的主要议题研究》，载《四川行政学院学报》2020 年第 2 期。

续前表

名称	金融信息传送条款设置方式	金融信息传送条款定位
ASDEA	第 3 条一般例外 第 17 条个人信息保护 第 23 条电子方式跨境信息传送 第 25 条金融服务计算设施位置 第 32 条金融科技与监管科技合作	数字经济章节
UKJCETA	第 8.63 条金融信息 第 8.65 条审慎例外	服务贸易、投资自由化、电子商务章 金融服务分节
《欧盟—英国贸易与合作协定》	第 201 条数据跨境流动 第 202 条个人数据和隐私保护	数字贸易章节
《初步文本》	第 3 条例外 第 5 条数据跨境流动 第 6 条个人数据和隐私保护	数字贸易章节
《合并文本》	第 B.2 条信息流动 (3) 金融信息/金融服务提供者的金融服务计算设施位置	电子商务章节

（二）金融信息传送规制路径差异

1. 美、新、英追求金融信息传送自由化

美国、新加坡、英国在金融信息传送自由化立场上旗帜鲜明，基本都遵循“金融信息传送自由原则＋个人数据、个人隐私、个人记录和账户机密性例外＋严格受限的监管例外＋计算设施本地化规则”的规制逻辑。这与保护本国金融行业进攻利益的需求不谋而合。根据 2021 年 9 月 24 日发布的第 30 版全球金融中心指数报告，纽约在各金融城中位列第一，伦敦位列第二，香港第三，新加坡第四。前 20 中共有 6 座美国城市。〔16〕就英国而言，金融服务业一直是其老牌支柱产业：英国是世界第二大投资管理中心、欧洲最大的保险和长期储蓄提供商，每 14 名英国劳动者中就有 1 人从事金融和相关专业服务工作。英国脱欧后，在金融监管上拥有了更大的自主权和灵活度，并有机会重新审视其数据流动规制方案。2020 年 11 月 9 日，时任英国财政大臣里希·苏纳克在下议院发表声明称希望“恢复英国作为世界卓越金融中心的地位”。〔17〕目前英国政府已经与新加坡达成新的金融服务伙伴关系以确保更大的信息共享，并与美国成立了金融监管工作组，在欧洲经济区国家的金融服务监管中授予了一系列等价保护决定。可以预见，在金融业数字化转型中，美、新、英三国将会有更紧密和深入的合作。

不过，正如前述，尽管都持金融信息传送自由化立场，英国的规制路径又较美新更为保守。从近年签订的 FTA 来看，美新都意图在数字经济领域的规则制定上先发制人，金融信息问题作为数字经济中信息/数据问题的一部分，其所蕴含的国内政策导向是金融领域的全面数字化。也

〔16〕 See The Global Financial Centres Index 30, p. 4.

〔17〕 See Rishi Sunak, A New Chapter for Financial Services, July 2021, available at https://www.gov.uk/government/publications/a-new-chapter-for-financial-services, last visited on May 7, 2022.

即，相较于金融业这一国民经济部门，美新都更关注数字经济这一发展模式。而英国目前看来，依旧专注于金融业本身。英式 FTA（UKJCEPA 及英国在 WTO 电子商务谈判中提供的规则文本）在“金融服务计算设施所在地规则”下增加了相当务实的“外部云服务企业同等适用”规则，增加这一规则的背景是英国本土乃至欧洲都缺乏有竞争力的云服务提供者，欧洲企业、公共当局大多采用美国云服务提供者为其提供数据服务。但明确设置“外部云服务企业同等适用”规则也不免传达出这样一种信号：相较于担忧本国缺乏有竞争力的本地云服务提供者，英国更关心如何使本地云服务提供者的缺乏不至影响其跨境金融服务的竞争力。

2. 欧盟在构建数据竞争力目标下的立场变化

与美、新、英不同，欧盟并未对金融领域及金融信息传送特别关注。较早的两个 FTA 中的金融信息传送条款设置完全体现了欧盟在个人权利保护上的突出立场。《欧盟—韩国 FTA》在金融服务分节的“数据处理”条款中特别约定：“各方重申其保护个人基本权利和自由的承诺，应采取适当的保障措施保护隐私，特别是在个人数据传送方面。”并进一步注明，这一承诺所保护的个人基本权利和自由是指《世界人权宣言》、联合国《计算机处理的个人数据文档规范指南》以及 OECD《隐私保护与个人数据跨国流通指南》中规定的权利和自由。《欧盟—加拿大全面经济贸易协定》规定：“各方应有充分的保障措施，以保护隐私，尤其是在个人信息传送方面。如果金融信息的传送涉及个人信息，则此类传送应符合传送发起方所在地区的个人信息保护立法。”欧盟的人权叙事在数据规制议题上抢占了先机，但负面影响也显而易见。一个简单的等式是：数据越多，算法就越智能。对个人数据保护的偏重将不可避免地限制金融机构在经营分析、精准营销等方面的智慧化能力，从而影响欧盟区银行业数字化转型步伐。〔18〕

2020 年，欧盟接连发布《欧洲数据战略》《欧洲数字主权》等文件，以期构建欧洲数字单一市场，维护其全球经济影响力和地缘政治影响力。在《欧洲数据战略》的导向下，欧盟在《欧盟—英国贸易与合作协定》及其他正在谈判的经贸协定中均将跨境数据流动内容统一放到了独立的电子商务章节（过去欧盟 FTA 习惯将电子商务和服务章节放在一起），并从强调个人信息保护转向强调禁止数据本地化。这一转向不可谓不突兀。事实上，施雷姆斯第二案〔19〕后，欧盟内部本地化趋势大大加强，欧洲数据保护委员会于 2020 年 11 月 11 日发布的两份文件《欧洲监督措施基本保证草案》和《补充措施建议》都招致了数据传送规则过于严苛的批评，被认为“将导致严格的数据本地化，给欧盟和美国的企业带来许多重大问题”〔20〕。另外，欧盟委员会于 2020 年 9 月发布的关于《金融部门数字运营弹性监管的草案》区分了在欧盟设立的信息通信技术（以下简称为 ICT）服务提供者和在欧盟没有商业存在的 ICT 服务提供者，并对使用此类第三国 ICT

〔18〕 参见李梦宇：《国际金融业数据治理特征与启示》，载《清华金融评论》2021 年第 5 期。

〔19〕 欧盟法院在本案中认为美国的监控立法违反了《欧盟基本权利宪章》，也没有为欧盟个人提供有效的司法救济，因此欧美之间的“隐私盾”协议无效。详细案件内容可参见 https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en。

〔20〕 Testimony by Peter Swire at the U. S. Senate Commerce Committee Hearing “The Invalidation of the EU-U. S. Privacy Shield and the Future of Transatlantic Data Flows” on December 9, 2020, available at https://www.crossborderdataforum.org/testimony-by-peter-swire-at-the-u-s-senate-commerce-committee-hearing-on-the-invalidation-of-the-eu-u-s-privacy-shield-and-the-future-of-transatlantic-data-flows/, last visited on Nov. 11, 2021.

提供商提出若干限制，如欧盟的金融实体不得使用在欧盟没有商业存在的公司为其提供关键的 ICT 服务。2021 年欧盟各国的数据保护监管机关还启动了多起关于欧盟机构继续使用美国云服务和软件服务是否合法的调查，并暂停了部分合作。虽然欧盟的对外立场不断呈现出向自由化靠拢的趋势，但考虑到数据自由流动将进一步拉大其与美国的数字差距，欧盟似乎正在积极寻求国内监管手段以平衡该等态势。

四、我国立法和 FTA 中金融信息传送规则

（一）确立金融信息传送自由原则

我国在跨境数据流动问题上的立场转向以 2016 年《网络安全法》的出台为分界线。2016 年之前，我国对于跨境数据流动问题关注不多，且对金融监管持绝对审慎态度，2011 年 1 月《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》明确确立了个人金融数据原则上禁止出境的基本方向。2016 年后，尤其是近两年来，随着数据价值的不断凸显，我国内外政策都开始向促进数据自由流动方向发展。国内法层面，《个人信息保护法》《数据安全法》、国家互联网信息办公室《数据出境安全评估办法》已经确立了金融数据“满足数据安全监管要求即可出境”的监管框架。具体到金融相关立法，2020 年修订的《中国人民银行金融消费者权益保护实施办法》（以下简称《实施办法》）删除了原第 33 条对“向境外提供境内个人金融信息”的限制性规定。2020 年《中国人民银行关于发布金融行业标准做好个人金融信息保护技术管理工作的通知》（以下简称《通知》）的附件《个人金融信息保护技术规范》第 7.1.3 条（d）项虽然载明“因业务需要，确需向境外机构（含总公司、母公司或分公司、子公司及其他为完成该业务所必需的关联机构）提供个人金融信息的，应当满足四项具体要求”，但《个人信息保护法》并不禁止关键信息基础设施运营者向境外提供个人信息，且其第 38 条还特别明确“中华人民共和国缔结或者参加的国际条约、协定对向中华人民共和国境外提供个人信息的条件等有规定的，可以按照其规定执行”。因此《个人金融信息保护技术规范》第 7.1.3 条（d）项更应被理解为管理性规范而非对“境外机构”范围的限制性规范。

国际法层面，签署 RCEP、申请加入 CPTPP 已经向全球经济体传达出中国支持金融信息自由传送的立场。实践层面，当前全球数字经济格局中，中美两国参与数字经济并从中受益的能力最强。〔21〕从发展数据来看，在金融服务领域，我国主要金融中心的发展前景良好，且在金融科技指数上表现强劲，但在营商环境上的竞争力并不强。〔22〕在云服务领域，阿里云非常适合处理中国或东南亚客户的云优先数字业务工作负载，有望成为印度尼西亚和马来西亚等新兴云市场所青睐的区域提供商；腾讯云是唯一在俄罗斯拥有业务地域并拥有核心基础设施能力（计算、存储和网络）的超大规模云提供商，而且在网络领域的能力尤为突出。但中国云服务厂商普遍全球发

〔21〕 联合国 2021 年数字经济报告显示，从参与数据驱动的数字经济并从中受益的能力来看，美国和中国脱颖而出。全世界的超大规模数据中心有一半在这两个国家，它们的 5G 普及率最高，它们占过去五年人工智能初创企业融资总额的 94%，占世界顶尖人工智能研究人员的 70%，占全球最大数字平台市值的近 90%。

〔22〕 See The Global Financial Centres Index 30，pp. 8－10.

展动力不足。[23] 因此，从各个层面来看，确立金融信息传送自由原则都有其现实必要性。

（二）保留必要的金融数据本地化空间

数据本地化与跨境数据流动间的关系一直颇有争议。境内产生的数据在境外云服务器存储必然伴随着数据出境，因此允许境内产生的数据在境外存储即意味着允许跨境数据流动，但反之并不亦然，要求数据在本地存储并不妨碍境内主体将数据传送给境外机构。目前国外学者对数据本地化措施的范围界定还包含保留本地副本等间接或事实的本地化要求，[24] 进一步增强了数据本地化与数据跨境流动的可切割性。数据本地化要求与数据出境审核等国内监管要求类似，属于边境后措施，而当前各 FTA 除 USMCA 及 ASDEA 外，对跨境金融数据流动自由化的承诺仅覆盖到边境措施。且从现实来看，越来越多的国家和地区正在针对更多的数据类型实施不同程度的本地化政策。从 2017 年到 2021 年，制定数据本地化政策的国家数量从 35 个增加到 62 个，全球数据本地化政策的总数从 67 个增加到 144 个（未包括正在制定的数十个）。其中，采取金融领域数据本地化措施的例子有：（1）卢森堡金融业监管委员会 2012 年 12/552 号通知规定，除非获得明确同意，金融机构必须在卢森堡境内处理数据；（2）2013 年 2 月 21 日俄罗斯银行第 397－P 号条例“关于电子数据库的创建、维护和存储程序”要求所有“信用机构”将所有数据存储在本地；（3）土耳其银行监管局 2020 年发布《银行信息系统条例》，加强了银行和金融服务机构将其主要（实时/生产数据）和次要（备份）信息系统保留在国内的规定；（4）印度证券交易委员会 2020 年发布了一份与网络安全相关的通知，要求金融机构确保对关键系统的完整保护和无缝控制，同时将关键数据保持在印度的法律框架内；（5）韩国 2016 年修订了《电子金融交易监管条例》，允许金融公司使用云服务，但金融服务委员会特别要求在位于韩国的服务器上维护此类数据；（6）智利金融监管机构 2020 年发布了银行业标准的更新汇编，要求在智利保存“重要”或“战略性”外包数据。[25] 因此，对跨境金融数据流动自由化的承诺今后不可能大范围延及数据本地化禁止，与 ASDEA 类似的对国内监管进行手段和限度限定的做法更有可能成为主流。

我国现行的金融数据本地化要求包括《网络安全法》第 37 条，国务院《征信业管理条例》第 24 条，《保险公司开业验收指引》第三（九）4 条，《通知》的附件《个人金融信息保护技术规范》第 7.1.3 条，中国人民银行《金融数据安全数据生命周期安全规范》第 7.3.2 条等。这些从法律到金融行业标准的规则基本确立了金融数据全面本地化的态度。但《金融数据安全数据生命周期安全规范》同时也指出，1 级数据为公开数据，原则上无保密性要求，2 级数据应优先考虑业务需求，对于非重要数据可以考虑放松本地化要求。

---

〔23〕 See Raj Bala, Bob Gill, Dennis Smith, Kevin Ji & David Wright, Magic Quadrant for Cloud Infrastructure and Platform Services (Jul. 27, 2021), available at https://www.gartner.com/doc/reprints?id=1-271OE4VR&ct=210802&st=sb&_ga=2.98959896.742444110.1644673015-722388850.1644673015, last visited on Feb. 13, 2022.

〔24〕 See James M. Kaplan & Kayvaun Rowshankish, Addressing the Impact of Data Location Regulation in Financial Services (May. 22, 2015), available at https://www.cigionline.org/static/documents/no14_web_0.pdf, last visited on May 7, 2022; IRSG report, How the trend towards data localisation is impacting the financial services sector (December 2020), available at https://www.irsg.co.uk/assets/Reports/IRSG_DATA-REPORT_Localisation.pdf, last visited on May 7, 2022.

〔25〕 See Nigel Cory & Luke Dascoli, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them (Jul. 19, 2021), available at https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost, last visited on May 7, 2022.

（三）规制路径选择

当前，主要经贸协定都转向采取跨境数据流动一体化规制方案。就我国而言，除 2011 年《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》第 6 条外，国内现行各金融相关立法中已无直接规范跨境数据流动的条文。我国在 2021 和 2022 年相继出台了《个人信息保护法》《数据安全法》、国家互联网信息办公室《数据出境安全评估办法》，显示出将数据问题进行统一规制、而非部门化处理的倾向。跨境数据流动一体化规制方案下，数据以个人信息及非个人信息数据划分，而不以具体行业数据划分。在与金融领域类似的领域如工业和信息化领域，工业和信息化部《工业和信息化领域数据安全管理办法（试行）》2022 年征求意见稿删除了 2021 年征求意见稿中“核心数据不得出境”的表述，并增加了“根据国际条约、协定处理外国提供数据请求”及“非经批准不得向外国执法机构提供本地数据”等内容，以与《个人信息保护法》《数据安全法》的规定相统一。目前电信和互联网行业、汽车行业相关数据管理规定/标准也都在制定阶段，其中有关数据出境的内容应当也会与《个人信息保护法》《数据安全法》的规定相统一。另外，与美、新一致，我国的着眼点也在于数字经济这一发展模式，《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》高频次提及全领域数字化，其中当然包括金融机构数字化转型。因此，从国内视角来看，采取跨境数据流动一体化规制方案似乎与我国更为契合。但从条约层面来看，也存在以下问题：第一，现行“数字经济”/“数字贸易”/“电子商务”协定多通过指明“影响通过电子方式交付或提供服务的措施同样需遵守投资及服务章节相关条款所包含的义务”来处理与传统“服务贸易”的范围重叠，但这并未根本解决其在贸易法中的体系定位问题，将金融信息规则并入是否会引起金融开放承诺的扩张尚不可知。第二，各国对一般商贸信息和金融信息的敏感度不同，“数字经济”/“数字贸易”/“电子商务”协定中的信息传送条款通常较金融服务章节更为严格，如 CPTPP 即对电子商务章节“通过电子方式跨境传送信息”条款下缔约方可采取的例外措施施加了手段和限度限制，而金融服务章节的“信息的传送”条款未设置此等限制。第三，各国在“数字经济”/“数字贸易”/“电子商务”上分歧明显，从名称到具体内容，如数据本地化、源代码等问题，都存在较大谈判难度。

因此，从实践角度，将金融信息传送条款保留在金融服务章节更有利于现阶段的条约谈判；而将信息传送问题统一置入数字经济协定与我国的规制方向更为契合，但承诺的水平无疑将更高，国内法与国际法的统筹难度也将更高。总体而言，FTA 金融信息传送规则构建上应当注意以下几个问题：第一，协调我国金融服务开放承诺水平与金融信息传送自由化水平，如采取跨境数据流动一体化规制方案，则应考虑增加与 RCEP 中“任何规定不得解释为要求一缔约方允许与其未作出承诺相关的跨境提供或者境外消费服务”类似的条款。第二，应当明确（金融）信息传送规则不适用于由一缔约方或以其名义持有或处理的信息，或与该信息有关的措施，包括与收集信息有关的措施，并增加在数据获取上的司法、执法合作。第三，保留金融领域的保密性要求，即任何规定不得解释为要求一缔约方披露与个人客户相关的事务和账户信息，或公共实体拥有的任何机密或专有信息。第四，可考虑接受对国内监管例外进行一定的手段和限度限定。“金融业是一个高度全球化的体系，金融机构的跨境支付清算、客户尽职调查、国际化运营、全球信息技

术系统集成、集团化风险管理与境外信息报送等，都离不开数据跨境。”〔26〕除明晰的法律指引之外，加强数据合规服务行业建设，从而降低境内外金融服务商的合规难度，同样是扩大金融开放、融入全球金融市场的关键步骤。在具体监管方案运用方面，依赖数据和技术的智能监管、有效的内控信息披露、成熟的行业标准自律和健全的合同执行制度或也将为更有效的数据监管提供有益指引。

五、结　语

“一国在自由贸易协定下的话语权体现为该国在谈判过程中制定规则的权力，并服务于该国的政治经济利益。法律输出正是大国实现自由贸易协定制度控制以实现其话语权的一种路径。”〔27〕20世纪末以来，美国与欧盟成功依靠FTA输出了国内规范和核心价值理念，《服务贸易协定》谈判的坎坷则充分显示了两大话语权掌控者之间的冲突。在今天，中国也应当积极考虑通过法律输出路径提高自身在国际贸易的话语权，以期实现从国际秩序遵守者向国际规则制定者的转变。同时，可以看到，FTA金融信息传送条款并不是一个孤立的规则，在文本上，它与电子商务规则、个人信息保护规则、审慎例外规则、本地化规则相交织，在规制理论上，对其的考量应当从跨境数据流动议题，甚至网络空间治理的全局角度出发，构建框架完整、逻辑统一的理论体系。

2022年初欧盟委员会发布《欧盟标准化战略——制定全球标准，支持弹性、绿色和数字化的欧盟单一市场》提出：“标准是欧盟单一市场和全球竞争力的无声基础，在标准化活动中拥有一个强大的全球足迹，并在关键的国际论坛和机构中领导工作，对于欧盟保持全球标准制定者的地位至关重要。通过制定全球标准，欧盟可以输出其价值观，同时为欧盟公司提供重要的先发优势。”〔28〕“欧盟及其成员国必须在国际电信联盟、国际标准化组织和国际电工委员会以及其他相关的全球伙伴关系、论坛和联盟中，推动对国际标准化活动采取更具战略性的方针，以确保欧盟的全球竞争力、安全和开放的战略自主权，以及欧盟推广其价值观的能力。”〔29〕数字全球化背景下，数字标准是贯穿各种经济活动过程的隐形基础。在金融领域，我国金融标准化技术委员会公布的金融国际标准（截至2021年9月30日）为66项，国家标准（截至2021年12月13日）为83项。随着数字化发展和进一步深入开放，标准的数量将大幅增加，各科技企业在国际标准制定中的参与度也将提高。此外，根据国际惯例，国际金融合作一般也适用《新巴塞尔协定》、国

〔26〕 李伟：《我国金融数据跨境流动规则建设的思考与建议》，载《中国银行业》2020年第1期，第42页。

〔27〕 王燕：《自由贸易协定下的话语权与法律输出研究》，载《政治与法律》2017年第1期，第109页。

〔28〕 New approach to enable global leadership of EU standards promoting values and a resilient, green and digital Single Market (Feb. 2, 2022), available at https://ec.europa.eu/growth/news/new-approach-enable-global-leadership-eu-standards-promoting-values-and-resilient-green-and-digital-2022-02-02_en#:~:text=New%20approach%20to%20enable%20global%20leadership%20of%20EU,within%20the%20Single%20Market%20as%20well%20as%20globally, last visited on May 8, 2022.

〔29〕 Communication From the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions-An EU Strategy on Standardisation Setting global standards in support of a resilient, green and digital EU single market, p. 5.

际证监会组织标准、国际保险监督官协会标准等国际金融协议和监管标准。〔30〕而我国目前在标准领域尚不发达，普遍来看，大多数中国公司都缺乏一种结构化和战略性的标准化方法，以捕捉其与各种经济运营的相关性，无论是法律合规性、市场准入还是一般商业战略。同时，随着如人工智能、数据保护或网络安全等新领域的衍生，对于标准制定能力的挑战将更大。培养标准化专家、深入国际标准制定或许是一个可以提升我国话语权的路径。

Abstract: Under the framework of international trade law, transfer of financial information clause constitutes the core part of financial information transfer rules. Originated from Transfers of Information and Processing of Information clause in Understanding on Commitments in Financial Services which was appended to the Final Act of the Uruguay Round, transfer of financial information clause was subsequently adopted by numerous FTAs. With digital economy upsurge, attention to the regulation of cross-border data flows began to focus on e-commerce and digital trade. As a result, there is a trend to integrate transfer of financial information clause into cross-border information transfer provisions of e-commerce or digital trade in FTA in recent years. However, there are still many fundamental issues to be resolved in the integrated regulation approach, and should be viewed with caution. At the present stage, transfer of financial information clause have developed a basic structure of "freedom of financial information transfer as principle + personal data, personal privacy and the confidentiality of individual records and accounts exception + limited regulatory exception" and rules on the "location of financial services computing facilities" have been derived from the issue of data localization. China should upgrade the FTA financial information transfer rules on the basis of its position on data sovereignty and shift from being an international rule-taker to an international rule-maker, with a view to safeguarding its offensive interests in the financial services and digital technology sectors.

Key Words: cross-border data flows, financial information transfer, FTA transfer of financial information clause, financial data exit

（责任编辑：肖　芳　赵建蕊）

〔30〕 参见云倩：《"一带一路"倡议下中国—东盟金融合作的路径探析》，载《亚太经济》2019 年第 5 期。