

# 论我国信息治理的信任建构及其路径选择

姚力博

**摘要：**我国围绕信息治理形成了三重规制方案：基于民法人格权进路的信息分级规制论、强调公权介入的行政规制论和行为主义治理论。这三重方案表现出从信息控制范式到信息沟通范式的发展趋势。在数字社会，个人信息利用与保护的平衡在于信息流通中的信任建构。信任机制具有稳定规范性期待、确保将来合作的功能，但因社会时势不同，而呈现出从伦理保障信任到法律保障信任的机理差异。通过法律建立信任是科技革命背景下信息技术发展和社会治理模式转型的共同结果，反映了现代社会的开放性、沟通性和共享性等特征。信息治理的信任建构适应了数字社会强交互—弱竞争、强介入—软强制、强预期—弱共识的结构要求，有助于形成协作型、沟通型治理模式，平衡信息流通与保护。我国数字法治建设应当聚焦信任关系的基础性、程序性、过程性、群际性和语境性，将信息信任分化于信息处理的安全、透明、公平、反歧视、整全等原则。这一信任规制结构的形成应当以民主化立法为开端，形成科技、法律、伦理、市场的耦合机制。

**关键词：**信息治理 信息信任 程序原则 实质原则 数字法治

## 一、引 言

自 20 世纪 90 年代以来，我国进入数字时代，大数据、人工智能驱动信息经济蓬勃发展，信息流通和治理的体系日趋复杂。2022 年 12 月印发的《中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见》，明确提出“激活数据要素潜能，做强做优做大数字经济”的战略部署。<sup>①</sup>2023 年，习近平总书记强调发展“新质生产力”<sup>②</sup>，推进经济发展在新一轮技术革命和产业转型中生产力的跃迁突变。这些举措既为我国科技产业和数字市场的蓬勃发展形成了助推力量，也对信息保护体系提出了更高要求。在此背景下，我国《民法典》《个人信息保护法》《数据安全法》等基础性法律相

〔作者简介〕姚力博，清华大学法学院博士研究生，研究方向：比较法、数字法。 北京 100084

〔收稿日期〕2024-10-19

〔基金项目〕清华大学自主科研项目“信息社会法治研究”（编号：2019THZWJC01）

①《中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见（2022 年 12 月 2 日）》，《人民日报》2022 年 12 月 20 日，第 1 版。

②《加快发展新质生产力 扎实推进高质量发展》，《人民日报》2024 年 2 月 2 日，第 1 版。

继出台,标志着我国个人信息保护进入体系化、法治化新阶段。在数字能量释放的背景下,如何更好地兼容信息流通利用的发展和保护诉求,成为信息治理方案中的重要考量。这一治理难题具有深刻的时代背景。在全球各大经济体中,信息流动和权益保护之间的张力始终存在。在我国信息立法进程中,关于数字立法的立法目标、保护手段和治理方式等基础性问题就曾引发学界广泛讨论。<sup>①</sup>目前学界形成了三大主流信息治理范式:基于民法人格权进路的信息分级规制论、强调公权介入的行政规制论和行为主义信息治理理论。但这三者均在平衡信息利用和保护中存有缺陷,难以完全适应数字社会高度流动、开放的本质特征。

本文通过系统检视我国既有的治理范式,提出应当将数字信任作为信息治理的核心建构要素。这一主张的提出顺应了现代社会科技革命和复杂性科学的发展趋势,是数字社会流动、开放、沟通的必然要求。通过法律建立信息信任有助于匹配数字社会强交互—弱竞争、强介入—软强制、强预期—弱共识的社会结构。应当通过程序信任和实质信任的设计,将信息信任内化为信息处理的安全、透明、公平、反歧视、整全各原则。在我国,信息信任的建立应以立法民主化为起点,构建技术标准、法律规范、伦理准则与信任机制耦合作用的治理体系。

## 二、我国信息治理方案的反思

当前我国学界和立法界大体形成了三重信息治理和保护方案,各有利弊。

第一,人格权分级规制论。这一方案认为,个人信息保护的核心法益是民事权益中的人格权益,法律保护的是信息主体的人格。因此,法律规制应以人格权为中心,以私法—侵权进路为主导,根据被损害的法益与人格规范的远近,区分个人信息的基础性权能和工具性权能,进行信息的分级管理和利用。<sup>②</sup>人格权进路为我国多数民法学者所赞成,它兼具权利宣示效果。不过,这一方案也有不足。(1)就权利内容来看,人格权的强规范色彩可以论证个人的核心信息如生物基因、身份信息的保护,但也使得其余不属于人格权的核心范畴但同样重要的个人信息,如个人行踪、通信信息、金融消费等信息无法获得有效保护。这些信息才是如今互联网商业利用的主要对象,并因其财产属性与其他信息形成冲突。(2)就治理模式来看,人格权进路将“知情—同意”原则视为个人信息处理的核心原则,同时将个人信息保护定位于私法范畴,适用侵权法救济。面对知识、技术、资源更优的数字侵权方,普通用户面临认知能力弱、维权难度高、维权周期漫长等劣势,权利的有效行使和救济难以实现。<sup>③</sup>(3)“具体列举+分级管理”的规制模式更适于为数据处理者提供行为指南,具有浓厚的技术性,但在执法实践中,对从事具体判断的法官施加了过重的技术负担,难以实现法律效果与社会效果的统一。

第二,公法规制进路。这一方案主张,个人信息存有权法益,但更具社会集体利益和公共利益。因此,信息治理应当公私法兼用,以公法特别是行政规制为主导。这一方案为我国多数公法学者所赞成,可进一步具体化为个人信息“集体/社会控制”<sup>④</sup>、“国家保护”<sup>⑤</sup>等方案。此观点的理据在于,信息保护与信息利用之间的冲突在于“个人信息个人控制”的私权理念,它建立于对数字社会

① 具体来看,学界围绕个人信息权性质的讨论,表现为权益论与权利论、民法保护与公法保护、个人控制与社会控制之间的争论,最后大体形成“公私协同”的法律体系,更多是出于实用主义考虑。相关总结参见张翔:《个人信息权的宪法(学)证成:基于对区分保护论和支配权论的反思》,《环球法律评论》2022年第1期。

② 程啸:《论个人信息权益》,《华东政法大学学报》2023年第1期。

③⑤ 王锡锌:《国家保护视野中的个人信息权利束》,《中国社会科学》2021年第11期。

④ 高富平:《个人信息保护:从个人控制到社会控制》,《网络信息法学研究》2018年第2期。

原子论的想象，忽视个人信息的公共性本质，阻碍了信息的流通和利用。同时，公权规制有助于弥补私权救济的不足。然而，这一方案也存在问题。(1) 就权利主体来看，个人信息—社会控制的权责主体并不明确，容易陷入个人信息—国家所有/持有的困境，陷入个人权利与国家义务的直接对等。(2) 就治理主体来看，个人信息—国家保护强调国家机关履行信息规制的主体责任，倾向以行政管理关系取代用户—商家之间的横向交易关系，挤压了私法自治空间，容易陷入否定个体权利的悖论。同时，信息规制由事后救济到事前规则制定的转变，赋予行政机构庞大权限，带来权力寻租、行政越权的合法性风险。(3) 就规制模式来看，个人信息集体控制对信息的理解仍然固守于信息的客体化、所有化想象，将信息控制与流通对立起来，无法适应现代社会开放、共享的流动需求。

第三，行为主义规制。不同于前两种进路，行为主义方案倾向于打破部门法的界限，认为个人信息同时蕴含着个体利益和社会利益，围绕信息利用产生多重法律关系，但多元权属和利益格局无碍信息利用，法律可以在个人信息流通的各环节合理介入，通过规制模式的创新，建立信息利用的宏观结构，同时场景化、分类化、比例化处理个人信息流通中的保护。行为主义立基于 20 世纪 70 年代的美国信息法律实践，秉持实用逻辑，以信息流通为前提，场景化信息保护。这一方案在我国以丁晓东、戴昕等学者为代表，主张行为主义在企业数据利用、数据市场构建的领域应用。<sup>①</sup> 行为主义进路在承认法律权属争议的前提下积极推进信息的商业化利用，有助于实现数字经济发展的最大化。然而，这一方案也有其缺陷。(1) 从权益内容来看，行为主义模式不承认个人信息的“本权”存在，所以在对信息权益内容、范围和效力上论证不足，无从说明个人信息权作为私权的规范性和正当性。(2) 从规制模式来看，行为主义保护走向了对个人权益保护的高度场景化，陷入标准的相对主义，在统一规则空缺的情况下，容易形成规则冲突，导致法律体系的碎片化、地域化。(3) 在个人信息流通、处理和保护之间的场景化权衡中，信息保护的私人利益通常不敌信息流通的公共利益和信息使用的商业利益，导致对个人的保护不足。总体来看，奉行行为主义规制模式的美国信息治理的确存在统一立法难以形成、信息侵犯事件频发、个人权益保护孱弱的缺陷，证实了如上论断。

不过，行为主义规制模式洞察到，无论是个人信息的人格权防御还是公私法兼容的国家保护范式，都建立在个人信息“排他性”的基础上，无法适应现代数字社会的沟通趋势。<sup>②</sup> 故而，行为主义将重点置于个人信息利用相关的多元法律主体，施以类型化责任。这一方案确有助于促进信息流通，提供多方主体激励。然而，行为主义所追求的信息治理却包含了以矮化信息“本权”为代价便利信息流通、贬损个人权益的后果。那么，如何在信息流通和信息利用之间的平衡中，寻得权益保护的更优解？特别是，在我国推动数据市场建设、发展信息用益权属的建设历程中，如何在行为主义方案的基础上强化个人权益保护，成为数字法治的重要难题。

本文认为，我国的信息规制方案必须充分认识到信任对现代社会的建构性作用，积极推动信任要素的原则约束与规则应用。这一主张源自数字社会发展的多元性、复杂性与开放性特征。当前，我国信息规制与治理方案可以从以下四个方面进行完善：(1) 在承认现存信息权属争议的基础上，积极鼓励信息流通和利用；(2) 在信息治理环节聚焦信息利用过程，强化过程规制、程序规制、市场规制与伦理规制的协同作用，构建协作规制系统；(3) 推进多方主体参与，实现信息共治；(4) 提升规制合法性与合理性，降低规制成本，增强规制实效。这些措施对信息治理的有效性与合法性提出了更高要求，依赖基于信任的法治框架的建设。

<sup>①</sup> 丁晓东：《个人信息的双重属性与行为主义规制》，《法学家》2020 年第 1 期。

<sup>②</sup> 余成峰：《数字时代隐私权的社会理论重构》，《中国法学》2023 年第 2 期。



### 三、信息法律关系的信任约束

#### （一）理论源起：信任作为复杂社会的应对方案

信息法专家阿里·埃斯拉·瓦尔德曼（Ari Ezra Waldman）指出，英美信息法中的信任机制源于道德传统和普通法上的忠诚义务，在鼓励信息流通的同时，强调建立信息收集和处理的责任制，以适应共享经济的发展需求。<sup>①</sup> 因此，隐私法和数字法治应侧重保护和修复信任关系。这一看法展现了社会信任与法律制度相互建构的特征。从社会学视角看，信任既是个体心理的主观感受，也是社会秩序的建构性产物，是维持期望、延续沟通、促进合作的重要前提。信任机制在不同社会呈现出不同特征：前现代社会的信任秩序主要依赖社群伦理、阶层权威和个人声望等传统资源，具有实质性、特殊性、集体性和强制性特征；现代陌生人社会高速流动和跨域合作的需求则改变了秩序维持与社会互动的客观条件，<sup>②</sup> 使得现代信任更具未来取向，强调其在复杂社会未来预期和沟通面向的塑造作用，具有更强的适应性与演化性。

在数字时代，第四次科技革命的发展带来了复杂性的增长。生命科学、认知科学和信息科学的研究表明，生命世界乃至人类社会的秩序表征为混沌涌现的特征，如果蝇繁殖、水流汹涌和意识苗生，无法为线性近似法所解释。<sup>③</sup> 这意味着，传统预设的因果链条常常是不准确甚至是错误的，“种种现象的相互纠结、迷雾、不确定性和矛盾”，形成了现代社会多元、连接、充足、特殊、开放、无序的关系图景。<sup>④</sup> 社会学界提出“黑箱理论”，作为对这种难以观测和解密的社会互动的描述。计算机技术的发展推动大数据和人工智能的迭代，加速了传统社会伦理强制所带来的信任保障机制的式微，强化了数字社会的开放性和不确定性。针对这一局面，学界提出了两种重建数字时代社会信任的方案。

第一种方案主张通过技术手段解决异议风险。这一方案预设，技术带来的不确定性源于对技术的无知，因此可以通过知识学习来应对技术风险。我国学界提出的“打开技术黑箱”“揭开无知之幕”等主张反映了这一思路。然而，风险社会专家乌尔里希·贝克（Ulrich Beck）指出，在现代社会，风险与科技表现出共生形态，科学本身已被卷入风险诞生和成长的过程。<sup>⑤</sup> 技术的发展往往会制造更多问题，并以难以察觉的系统性方式呈现，倾向于增加无知而非知识、带来风险而非确定性。因此，单纯依靠技术本身难以有效解决不确定性问题。另外，技术黑箱现象也催生了专家信任机制。<sup>⑥</sup> 凭借专业技术和知识优势，专家成为联结行业发展与公众知情的重要桥梁。但专家监管也容易受到不公正和人为操纵的质疑，特别是当大型企业滥用权力时，公众对专家机构的信任度往往会降低，继而削弱专家信任机制的效力。

第二种方案主张通过法律建立预期信任机制。该方案认为，即便技术完全透明难以实现、专家预测存有偏差，法律规范仍可提供制度性信任保障。其理论依据在于，虽然技术发展具有不确定性，但法律主体具有有责性、技术手段具有可控性、法律结果具有预测性，这为人为建构信任提供了制度空间。相较于技术判准，法律能够为风险与未知提供制度保障。在法学界，这一主张表现为要求法律建立可信性沟通机制，在人机交互的“黑箱”环境中构建半透明的“白箱”系统，从而简化沟通复杂

① 阿里·埃斯拉·瓦尔德曼：《隐私即信任：大数据时代的信息隐私》，张璐译，法律出版社，2022年，第89页。

② 陆宽宽、王润稼：《信与任的双重变奏：信任的道德逻辑》，《湖北社会科学》2022年第6期。

③ 米歇尔·沃尔德罗普：《复杂：诞生于秩序与混沌边缘的科学》，陈玲译，生活·读书·新知三联书店，1997年，第80—81页。

④ 埃德加·莫兰：《复杂性思想导论》，陈一壮译，华东师范大学出版社，2008年，第8—9页。

⑤ 乌尔里希·贝克：《风险社会》，何博文译，译林出版社，2004年，第28页。

⑥ 参见吴新慧：《算法之下：数字信任还是专家信任？》，《学习与实践》2022年第12期。

性，稳定规模合作的预期。<sup>①</sup>相应地，这也对法律系统本身提出了更高的中立性要求和论证要求。

20 世纪下半叶以来，建立法律信任的法理依据逐步明晰。现代结构功能主义理论奠基人塔尔科特·帕森斯（Talcott Parson）提出，现代社会根据功能原则分化为 AGIL 四结构，<sup>②</sup>其中法律系统承担整合功能，作为现代社会的信托系统（fiduciary system）发挥作用。法律植根于社会共同体系统，连接着社会中的文化、政治和经济部门，既从文化系统获取正当性支持以形成共识性制度规范，又作为经济与政治系统的组织手段，促进社会功能的稳定运作。这一思路为德国沟通论学者所继承。例如，尤尔根·哈贝马斯（Jürgen Habermas）认为，法律植根于日常生活世界，依赖个人的认知和验证能力、文化的确定性实践以及通过价值规范整合的群体团结，保障了简单互动的“毋庸置疑”。<sup>③</sup>面对大型社会的复杂互动，法律机制借助语言媒介，在全社会范围内充当系统和生活世界之间的转换器，促进分化世界的整合。<sup>④</sup>系统论学者尼克拉斯·卢曼（Niklas Luhmann，又译为鲁曼）则将“稳定规范性期待”视为法律系统的核心功能，认为法律系统通过认知开放、规范封闭的运作原则，借助系统的记忆与学习能力、法/不法的二分符码对司法个案进行决断式处理，从而维护社会的规范性期待，确保沟通的持续性。<sup>⑤</sup>由此可见，通过法律建构信任，是现代法治的功能之维。

在数字时代，信任关系表现为整合个体心理、技术适用和法律规范的动态过程。<sup>⑥</sup>通过建立法律信任机制，数字法治能够充分发挥信息媒介的功能特性，在促进信息流通的同时，构建具有约束力的信任共识，实现权利保护的目标。法律信任所蕴含的强交互性、强社会性和强开放性特征，顺应了数字社会开放共享、主体多元、利益多维的结构特点，回应了现代技术与秩序建构的沟通转向。

## （二）强交互—弱竞争：法律信任的协作优势

数字社会的治理要求法律构建“强交互—弱竞争”的协作体系，通过多元治理手段塑造理想的网络秩序。网络法专家劳伦斯·莱斯格（Lawrence Lessig）指出，网络秩序的构建依赖四种基本力量：技术架构（architect/code）、市场、法律和规范。<sup>⑦</sup>面对现代社会的复杂多元境况，任何单一维度的秩序保障都显得力有不逮。（1）伦理信任的“地方性”失灵。信息技术极大地扩展了人际交往的时空范围，创造了前所未有的陌生人互动环境，这使得基于特定社群的伦理信任机制面临失效风险。伦理信任作为社群文化的有机组成部分，其价值的特殊性天然地与信息的流动性在本质上存在内在张力。因此，强伦理导向的规制模式不仅会降低信息流通效率，而且会损害信息共享所带来的社会福利。（2）市场机制具有自利性缺陷。个人信息作为现代社会的“微粒”，不仅是重要的经济生产要素，而且关涉社会信任维系、公共空间构建、国家安全与风险防控等重大公共利益。然而，市场机制固有的“丛林法则”与“负外部性”等弊端，使其难以全面地保障这些多元价值，必须突破传统私法自治的局限，构建公私法协同的立体规制结构。（3）代码规制的合法性遭受质疑。尽管技术专家在网络架构设计中发挥着关键作用，但数字时代的治理民主化诉求要求打破技术精英的垄断地位。无论是行为主义模式推动的市场自治，还是公权监管主导下的行政规制，其技术架构设计都必须通过民

① 余成峰：《从马的法律到黑箱之法》，《读书》2019年第3期。

② AGIL 指的是模式维持（pattern maintain）、整合（integration）、目标实现（goal attainment）与适应（adaption），分别为文化系统、社会系统、政治系统与经济系统所拥有。参见 Talcott Parsons, *The System of Modern Societies*, Englewood Cliffs, NJ: Prentice Hall, 1971, p. 11.

③ Jürgen Habermas, *The Theory of Communicative Action, Volume II: Lifeworld and System: A Critique of Functionalist Reason*, Beacon Press, 1981, pp. 221–222.

④ 参见尤尔根·哈贝马斯：《在事实与规范之间：关于法律和民主法治的商谈理论》，童世骏译，生活·读书·新知三联书店，2003年，第98页。

⑤ 尼克拉斯·鲁曼：《社会系统：一个一般理论的大纲》，鲁贵显、汤志杰译，暖暖书屋，2021年，第381—383页。

⑥ 张成岗、阿柔娜：《智慧治理场景下的数字信任构建：机制、挑战及趋向》，《社会治理》2024年第1期。

⑦ 劳伦斯·莱斯格：《代码 2.0：网络空间中的法律》，李旭、沈伟伟译，清华大学出版社，2009年，第138页。

主程序的检验,实现“独立”与“问责”的平衡。(4)“危险”与“风险”叠加,亟须可信的社会环境。现代社会风险的全球化、制度化和反身性特征使得潜在风险演变为实害的概率显著提升。<sup>①</sup>数据泄露事件频发、“黑天鹅”乱飞的环境严重削弱了社会主体的合作意愿与投资信心,进而损害信息流通的整体福利。这种风险环境使得安全保障成为信息治理的核心考量。总体而言,信息法规制必须妥善处理价值的普遍性与地方性、法益的私人性和公共性、治理的精英化与大众化、法律的现实需求与未来发展之间的张力。在这些关系中,信任机制发挥着关键的调和作用。

全球隐私保护实践表明,信任要素正通过多种路径融入技术、市场、伦理与法律的协同框架。例如,欧盟竭力推进“隐私设计”(privacy by design)的立法应用,强调技术发展必须从产品和服务开发环节就将特定价值(信任、隐私)纳入发展框架。2010年以来,欧洲数据保护委员会(European Data Protection Board, EDPB)持续推进科技立法的伦理评估,通过不断嵌入市场伦理、科技伦理和社群伦理,规制数字市场运营,通过赋能科技、治理科技、合规科技的开发应对平台的“暗黑模式”(dark pattern)。<sup>②</sup>美国则对新自由主义进行适应性调整,通过行为主义的法律干预明晰数据权责,借助行为主义的法律介入,助推数据产权与保护责任的明晰,借助公平信息实践(fair information practices),创造良好的信息市场生态。

### (三) 强介入—软强制:信任规范的治理优势

在当代多元社会,法规范的治理应秉持“强介入—软强制”原则,尊重多元主体参与,实现数字社会自治与他治的结合。自20世纪下半叶以来,以信息法为代表的“第三法域”兴起,<sup>③</sup>反映了社会治理模式的现代转型。它要求规制者既要充分认识市场失灵和私法不足的弊端,又要避免陷入全权管控的规制困境,推进国家、行业、企业、个人等多方治理主体的共治。其中,国家治理的有效性在于提供包含立法、司法和行政裁量权的公共规制权,形成与公民权利、组织权利/权力的多向制约,保障个人经济与社会权利。特别是借助新型行政手段,将核心价值和政策目标嵌入数字法治关系,实现法律管理、促进、保护和干预等不同功能。<sup>④</sup>

法律之“强介入”源自现代社会的复杂性和治理难度,要求国家更为积极主动地适应经济社会的发展需要。为此,必须通过行政监管、行政强制、行政指导等手段,深度介入和调节失衡的私人关系。“软强制”则是指,法律在贯彻自身命令的同时,也要尊重功能分化时代的社会自治诉求。现代经济社会运行的高度专业化、组织化和精密化特征,对传统的强制性命令形成了天然抵制。因此,法规范的形成不仅需要国家立法机关自上而下的权威确认,也要得到社会共同体自下而上的自发认同。此外,鉴于技术发展的黑箱性难以完全破解,法律规制应当尊重技术领域的有限自治,尊重技术发展的客观规律。所以,这一模式不同于传统规制,它借助于国家立法、信息技术和社会相关利益主体之间的紧密结合,形成复合、多元的治理模式。

当今全球各主要信息经济体均致力于寻求信息主体的自治与法律规制的平衡,但各有偏颇。美国信息法模式颇为依赖经济市场的自律,国家只提供基础性立法、政策和机构监管框架,鲜少对私营部门做出统一规制。这种“节俭监管”模式放纵了市场失灵,薄弱的行业自律也无法提供有效的个人权利保护。<sup>⑤</sup>更严重的是,这一模式纵容了资本对立法的游说,导致了公共立法权的腐败。相较之下,欧盟以《欧盟通用数据保护条例》(General Data Protection Regulation, GDPR)为代表的强监管模式,通过基本权利确认、公法介入和伦理引导实施统一规制。但这种模式也存在将道德论证直接转化

① 彼得·什托姆普卡:《信任:一种社会学理论》,程胜利译,中华书局,2005年,第49页。

② 朱悦:《立法过程所见的欧盟平台治理——兼论比较法研究的过程视角》,《数字法治》2023年第3期。

③ 吴文芳:《个人信息保护法的社会法属性及其法律意义》,《法治研究》2022年第5期。

④ 王锡锌:《国家保护视野中的个人信息权利束》,《中国社会科学》2021年第11期。

⑤ Siona Listokin, “Does Industry Self-Regulation of Consumer Data Privacy Work?” *Sociotechnical Security and Privacy*, March/April, 2017.



为法律规则、滋生官僚主义、抑制技术创新等缺陷。

构建国家与社会之间的信任纽带，成为突破信息规制单边困境的关键出路。信任作为社会共同体的团结纽带，产生于主体间长期互动的文化积淀，具有人为建构性。通过法律机制强化信息处理过程中的信任关系，能够建立稳定的意义联结，为数字沟通提供安全基础。同时，信任机制具有情境适应性，可以分化为经济交易中的互利信任、权力运行中的合法信任，作为经济和政治社会的运行支持，成为法与社会沟通的纽带。

#### （四）强预期—弱共识：信任预期的沟通优势

将信任纳入数字法治框架，有助于形成数字社会“强预期—弱共识”的新型沟通模式。数字社会带来了陌生人之间的交往革命，重构了人际信任的建构逻辑。<sup>①</sup> 传统基于宗教、血缘和业缘的统一性瓦解，人与人之间的大型互动只能通过即时性、流动性的交互来实现，呈现出去中心、语境性色彩。<sup>②</sup> 可以说，“社会生活中人们之间的休戚与共、息息相关的‘共同感’也随之消退”<sup>③</sup>，基于宗教、伦理的“厚”共识大为削弱，基于沟通的“薄”信任成为确保合作进行的必要条件。反思性社会的共同秩序，只能通过信任要素建立起来。不过，不同于熟人社会的实质信任，一方面，数字社会要求一种抽象的、可普遍化的一般信任机制；另一方面，凭借与线下世界的嵌入，数字社会本身具有极高的情境性，呈现出形态多样、规范多元、关系分殊的特征，这要求信任机制必须兼容灵活、动态的情境，能够进行多维转换。

在现代数字社会，信息治理表现出从排他性封闭进路到共享性沟通进路的转型。传统隐私权以物理空间的公共—私人二分为原则，建立在所有权—控制权范式的基础上，以私密、秘密为要件，<sup>④</sup> 强调信息的静态保护。而在数字社会，虚拟空间的发展使得物理边界的公私二分逐渐模糊，社会关系呈现流行、开放、共享的特征，信息关系也不仅仅是控制—访问关系，而是凭借其信息便捷、低廉的复制成本与关联使用，在流通中产生方方面面的利益关系，对居民生活、企业经营乃至政务管理影响甚巨。信息法律关系的形成可能基于网站与用户之间的服务协议、公共部门所获得的法定许可、劳动雇佣关系等基础法律关系，但在信息市场，信息处理者和主体之间可能并无直接关联。这一流通结构使得信息流动被置于现实和虚拟环境交错的网络结构：个人在数字社会中遭遇的是“事件”，形成的是“际遇”，无法消弭的是“风险”。<sup>⑤</sup> 随着信息本身成为社会关系生产的重要媒介，信息利用和保护也在维护私人利益、公共利益和集体福利之间灵活转换。因此，在数字时代重塑社会秩序的努力，必须确保沟通的敞开，着眼于可能的法律关系。

## 四、构建信息信任的程序原则与实质原则

我国学界已经逐步形成共识，信息治理的方向应从“信息控制”转向“沟通信任”，通过完善信息处理程序、健全主体机制、优化组织架构等方式，推进信任塑造。<sup>⑥</sup> 本文认为，在强交互性进路下，信息法律关系的构建不应局限于侵权救济或者公权指令模式，而应通过多重法律手段，形成信息治理的灵活约束，较之行为主义提供更强保护。在强社会性的进路下，信息信任的建立应强化主体参与，充分考虑多元利益，较之公权规制进路提供更强的灵活性。在强开放性的进路下，信息信任的建

① 张成岗、阿柔娜：《智慧治理场景下的数字信任构建：机制、挑战及趋向》，《社会治理》2024年第1期。

② 余成峰：《数字时代隐私权的社会理论重构》，《中国法学》2023年第2期。

③ 贺来：《“关系理性”与真实的“共同体”》，《中国社会科学》2015年第6期。

④ 余成峰：《信息隐私权的宪法时刻规范基础与体系重构》，《中外法学》2021年第1期。

⑤ 程关松：《个人信息保护的中国权利话语》，《法学家》2019年第5期。

⑥ 参见杨建军：《可信人工智能发展与法律制度的构建》，《东方法学》2024年第9期。

立应着眼于未来法律关系，鼓励信息利用，避免传统隐私权的封闭困境。<sup>①</sup> 具体来看，信息信任应当嵌入信息处理的法治框架，表现为信息处理的程序原则与实质原则，具体化为安全原则、透明原则、公平原则、反歧视原则与整全原则，弥散化为信息处理的基础信任、程序信任、过程信任、群际信任和语境信任，实现对信息处理的过程约束和结果约束。

### （一）安全原则建立基础信任

作为信息秩序的核心支柱，信息安全涵盖保密性、完整性、真实性与可靠性四个维度，直接关涉隐私权等基本权利的实现。当前我国信息安全面临的挑战日益严峻。在技术层面，随着现代科学技术和信息全球化的发展，信息的脱域性、流动性和可再组织性加剧了信息储存与流动的风险。在社会层面，我国正处于数字化社会转型期，私人与公共部门对数据的依赖性持续加深，新技术的应用与适用加剧了安全挑战。特别是，随着技术发展的日新月异，对信息安全的保障要兼顾互联网技术的发展特点，不仅要处理信息侵害的实在破坏，而且要应对信息侵害的潜在风险，使得风险控制进路在比较法上广为遵循。<sup>②</sup> 不过，信息安全的风险往往是多重的，同时包含了技术风险、背景风险（background risk）和剩余风险（residual risk）三种，共同构成对信息安全的挑战。<sup>③</sup> 技术风险主要指的是信息处理技术本身不成熟而带来的安全隐患，它特别出现于信息储存与流通环节的信息安全保障措施与加固不足导致的信息泄漏情况中。背景风险指的是信息控制者作为信息处理的主体，进行信息安全保护所采取的方案与其目的息息相关，故而具有适用的局限性。而剩余风险指的是，经过特殊化处理后的信息（如匿名信息、假名信息等）仍有被再度破解的可能，可结合其他信息还原机密内容。

尽管我国目前已经构建了以《数据安全法》《网络安全法》《电子签名法》为核心的法律保障体系，仍应持续关注信息流通中的风险防控。（1）应强化风险管控进路，进行信息保护技术的安全评估。我国《个人信息保护法》第55条规定了高风险行为的个人信息保护影响评估制度，应当建立全过程的风险管理，识别和有效评估未来风险，完善安全应对措施，强化模拟应急处理系统。在基本技术风险评估之外，针对背景风险和剩余风险，应结合信息处理的过程，对相关背景元素，如信息性质、现行监管机制、可用信息来源、接收信息的可能第三方、可能遭受的安全攻击等进行综合考量。同时，不能一劳永逸地认为信息安全处理后就不再面临新的破解和滥用可能，仍要评估当前保护手段是否对已经识别的风险有效并作出调整，定期评估是否存在新的风险。（2）明确信息安全审查的责任分配。我国当前立法将网络安全维护责任下放至各级政府和相关机构（网信、电信、公安与国家安全部门）。2020年，《网络安全审查办法》规定了关键信息基础设施运营者和网络平台运营者的网络安全审查义务。在现有分级监管框架下，应进一步厘清相关主体的责任，强化重点领域保护。（3）完善数据分级分类管理制度。针对事关国家安全、经济命脉和重要民生等重要和敏感个人信息，立法部门应尽快出台统一法律或指导意见，制定更具操作性的分级标准与保护规范，避免因立法碎片化导致的安全漏洞。

### （二）透明原则建立程序信任

透明原则要求信息处理者向用户说明信息处理的内在逻辑，特别是在自动化决策场景下，需要阐明“特定因素对算法决策的具体影响”<sup>④</sup>。这一原则与算法公开原则、可解释性密切相关，其产生源于对“算法黑箱”“数字霸权”的普遍担忧。<sup>⑤</sup> 一方面，计算机科技的快速发展使得普通人在认知能力上与机器存在显著差距，难以充分理解隐私选择及其后果；另一方面，信息技术架构使个人的议价

① 高富平：《可信数据流通制度论——治理范式经济秩序的形成》，《交大法学》2024年第5期。

② 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》，《环球法律评论》2022年第1期。

③ 张涛：《欧盟个人数据匿名化治理：法律、技术与风险》，《图书馆论坛》2019年第12期。

④ 苏宁：《优化算法可解释性及透明度义务之诠释与展开》，《法律科学（西北政法大學學報）》2022年第1期。

⑤ 董青岭：《人工智能时代的算法黑箱与信任重建》，《人民论坛·学术前沿》2014年第16期。



与决策能力沦为形式化“同意”，难以确保决策的充分有效性。然而，在商业交易、网络参与、行为选择等日常生活领域，人们都深受信息决策的影响。自动化算法与市场竞争的结合，使得个人信息的自动化处理不仅关涉消费公平和竞争秩序，更因其在公共部门的运用而具有维系社会正义、减少算法操纵的重要公共意义。

不过，算法处理的透明度本身具有层次性，包含了决策机理解释、决策结果解释和算法方法论解释三个维度，涉及市场主体、竞争者、监管者与消费者多方利益。在法律关系层面，算法透明既与安全、尊严、平等实体性价值相连，又关涉国家安全、隐私保护、商业秘密和知识产权竞争等多重考量。因此，简单要求完全公开算法既不现实，也无助于商业发展。<sup>①</sup> 算法透明不应等同于强监管，而应根据技术的可解释性水平，根据比例原则，推行不同强度的透明规范。

私营部门的信息处理透明原则在实质上发挥着“正当程序”的功能，与“可解释性”相伴相成，并以问责制为依托。经济合作与发展组织（Organization for Economic Co-operation and Development, OECD）在2002年发布的《隐私保护和跨境个人数据流动指南》中，明确规定了目的明确、公开等原则，并施以问责制原则的约束。<sup>②</sup> 继GDPR之后，欧盟又于2022年末通过《数字市场法案》（Digital Market Act）与《数字服务法案》（Digital Service Act），通过加强市场监管、规制“守门人”（gatekeeper）制度来推进数字市场算法透明。我国《个人信息保护法》第7条、第24条规定了决策透明的一般要求，《关于加强互联网信息服务算法综合治理的指导意见》《互联网信息服务算法推荐管理规定》等部门规章也鼓励“经由设计的透明”，就算法解释权、算法参数备案、影响评估、合规审计层面做出原则性规定。比较而言，我国对算法透明的法律要求属于中等强度，介于美国的宽松要求与欧盟的严格规定之间。在当前数据流动进一步推进的情况下，为更好促进数字竞争和保护个人信息，精确化信息处理的透明要求仍有作为空间。

### （三）公平原则建立过程信任

公平原则在狭义上指信息处理者与被处理者之间的交易公平，旨在保证消费者利益。这一原则同时包含主观公平与客观公平两个维度。主观公平强调消费者个体的心理信任状态，依赖于“自动化偏见”这一技术中立预设：人们倾向于相信信息处理结果是合理、公平且无偏见的。<sup>③</sup> 这种预设维持着日常交易的基本信任。然而，一旦技术公平被证伪，如出现歧视性个案或群体事件，将引发广泛的社会信任危机。例如，大数据杀熟、用户画像定向广告等商业实践引发消费者抵触情绪，导致其消费意愿降低。不过，值得注意的是，主观公平不一定以完全的客观公平为前提，它具有感受性、情境性和主观性，体现了信息关系中的柔性一面，可以通过完全“知情—同意”政策、有效的信息撤回权等程序设计予以实现。在多数情况下，客观公平倒是会对主观信任产生破坏性影响。

客观公平着眼于信息处理结果的分配结果，涵盖福利公平与能力公平两个方面。福利公平直接调节信息处理者与用户双方的交易关系，要求双方处于理性对等、平等的地位，基于诚信、公平、必要原则处理个人信息。能力公平则指向信息处理的“长尾”效应，要求不得基于个人信息处理的结果产生价格歧视、偏见标签、拒绝服务等负面影响。面对自动化决策的幽灵，人们尤其担忧算法偏见通过数据输入—决策作出—执行监督等链条被放大，特别是在公私部门数据共享背景下，可能加剧信贷金融、福利分配等领域的既有歧视。<sup>④</sup> 故而，能力公平原则特别强调信息处理的公正性、准确性与真实性，要求每次数据处理必须“如其所是”地反映当前情况，杜绝历史偏见的延续。

① 沈伟伟：《算法透明原则的迷思——算法规制理论的批判》，《环球法律评论》2019年第6期。

② See OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 2002-02-12, [https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-012021-examples-regarding-data-breach\\_en](https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-012021-examples-regarding-data-breach_en), visited on 2024-04-01.

③ 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》，《比较法研究》2020年第5期。

④ 曹博：《算法歧视的类型界分与规制范式重构》，《现代法学》2021年第4期。

信息公平原则的实现依赖市场规则的完善。(1) 应以维护交易公平为基准。可借鉴美国市场行为主义的规制模式,借鉴“公平信息实践原则”,通过市场监督管理部门对违反市场秩序的行为进行执法监管,合理引入诚信原则,减少并消除数字平台的“暗黑模式”、数字操纵、不当诱导(deceptive)、价格欺诈(fraud)等行为,避免经济社会的“丛林法则”。(2) 矫正交易双方的权力不对称。数字经济关系必须关注信息处理中的权力关系,特别是消费者的弱势地位。通过强化立法规定、公益诉讼等司法救济机制,确保信息主体的“权利行使有效”“数字参与有可能”“决定有意义”“失权有救济”。(3) 协调信息处理关系与竞争秩序之间的关系。随着信息平台向3.0演进,需要厘清信息处理关系与不正当竞争、市场垄断的界限,加强对大型平台的规制。

#### (四) 反歧视原则维系群际信任

反歧视原则关注个人信息处理的社会效应,旨在防止数字时代的“系统性排斥”。不同于狭义公平原则聚焦交易公平,反歧视原则禁止决策者基于个体所属群体的差别对待,<sup>①</sup> 强调自动化信息处理的系统性、群体性影响。一般来说,歧视性数据往往来源于现实生活对特定群体的偏见,技术逻辑耦合了歧视形成的社会规律<sup>②</sup>,进一步常态化、制度化了基于性别、种族、宗教、地域、年龄、健康状况等先天禀赋的歧视。尤其是在权重排名、分类评价、预测分析和信息过滤等算法应用中,自动化决策对平等原则构成严峻挑战,不仅影响公民医疗、消费、信贷、保险等领域的权益实现,而且贬损公民尊严,背离了人格平等。

不过,信息处理的反歧视问题面临特殊困难。这主要因为,技术黑箱使得污染数据难以及时发现和纠正,个案救济机制如删除权也多适用于信息明显错误的环节,且需要权利人主动主张。为减少群体性歧视事件的发生,应建立重点领域、重点行业的常态化纠偏机制。(1) 实施信息分级保护,对敏感信息特殊对待,施行与其他非敏感信息不同流通与保护方式。<sup>③</sup> 我国《个人信息保护法》专设“敏感个人信息的处理规则”,但目前单行立法层面多以效力层级较低、体系化较弱的行政规章和国家标准为主,如《征信业管理条例》《信息安全技术—个人信息安全规范》单独规制。仍应借鉴比较法上的经验,强化个人生物信息、银行金融等领域的立法,建立敏感信息全面覆盖、重点保护模式。(2) 建立算法审计和个人信息保护评估制度,引入技术专家监督。算法审计可平衡商业秘密与合规需求。从比较法来看,英美等国家均设立官方机构如信息专员办公室(Information Commissioner's Office)、联邦贸易委员会对涉及个人照片等生物特征的数据处理行为展开审计,以算法正义联盟(Algorithmic Justice League)为代表的第三方审计部门的参与对美国刑事司法算法反歧视的应用做出了重要贡献。<sup>④</sup> 当前我国个人信息保护评估制度处于发展期,应继续加强算法影响评估制度建设,强化制度监管。(3) 完善信息清洁制度,推进数据匿名化。个人人身、医疗等信息通常关涉人格尊严,应通过“被遗忘权”、儿童信息保护部门、专职受理部门等方案,推进错误信息、歧视性信息的个例纠正。同时,在数据市场,匿名数据是数据利用的重要来源。当前我国数据匿名化标准模糊、可操作性较低,应当明晰立法标准,为“不可识别”“不可逆转”等原则提供细致说明与操作指南,推进匿名化后的信息利用,强化流通中的保护。

#### (五) 整全性原则维护语境信任

整全性原则始自网络安全和网络机密的考虑,强调信息处理的安全、稳定与可控性,如今则被认

① 张欣:《算法公平的类型构建与制度实现》,《中外法学》2024年第4期。

② 李成:《人工智能歧视的法律治理》,《中国法学》2021年第2期。

③ 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》,《环球法律评论》2022年第2期。

④ 转引自张欣、宋雨鑫:《算法审计的制度逻辑和本土化构建》,《郑州大学学报(哲学社会科学版)》2022年第6期。

为是信息流通的较高要求，关注宏观信息流通的认知效应，聚焦信息整全对统计结果的影响，<sup>①</sup> 要求信息完整、准确并及时更新。20 世纪以来，由互联网商业化开启的信息技术发展已然由样本采集的小数据时代过渡到大数据算法时代。其中，数据的质量（data quality）来自其完整性。一般认为，相关数据越完整，越趋向于“全数据”（all data），数据的效果就会越“自然”，越能客观真实地反映被处理者的实际情况。<sup>②</sup> 然而，在实践中，信息整全性常常受到挑战。在以信息第三方共享为主的数据池的建设中，专司分类处理、自动生成内容的计算系统广为应用，使得信息的再处理更容易，碎片化信息加总即可产生新的内容。因此，信息处理者不仅是个人信息的收集者和利用者，也是个人信息的再生产者，作为被处理的对象则面临人格去真、异化乃至伪造的困境。

在当前信息保护中，整全性原则以英美法的“场景性隐私”（contextual privacy）为代表，侧重隐私保护的整体语境的衡量，关注获取信息的妥当性、信息的分布、情景完整性/整全性等价值，并以数字正义为最终调节。<sup>③</sup> 在具体规则中，GDPR 第 5 条规定了“整全性与诚信原则”（integrity and confidentiality），并陆续发布《数据泄露通知指南》<sup>④</sup>《执法活动人脸识别技术应用指南》<sup>⑤</sup>，致力于穷尽各场景不同的保护标准。OECD 则将“质量原则”列入数据处理八大原则，要求关注数据的相关性、完整性和准确性。<sup>⑥</sup> 我国《个人信息保护法》第 8 条同样规定了信息质量条款，但仍需细化情境标准。总体来看，信息整全性可通过如下方案推进：（1）立法明确信息处理整全性原则，完善信息准确性、妥当性、目的限制的保护标准，推进稳妥、可信的信息流通；（2）提高数字技术处理的门槛，将数据处理整全性纳入市场竞争要素，推进优势信息处理技术的应用；（3）制定情境性标准，细化不同场景如劳动环境、公务场景、弱势群体的信息处理规则；（4）审慎推进信息可携带权的发展，平衡权利行使与信息质量保障。

## 五、我国数字法治信任的耦合路径

信任原则的法律建构进入数字法治的结构设置、规则完善和程序安排，也对法秩序提出了更高的中立性、论证性和整合性要求。同时，法律也必须认清其介入限度，与技术、规范、市场等协调，形成交互支持的系统性信任框架。在我国，信息信任的法治建立应当以提升立法的民主参与为开端，实现与科技、市场、现代伦理的耦合。

其一，强化立法信任，推进信息立法的民主化与科学化。我国当前信息规制呈现行政为主的规制倾向，以网信办和市场监督管理局为代表的信息规制机构获得了主导地位，权限涵盖事前规制，包括设定新技术、新应用的准入标准等，接近于行政立法。这一做法极大提升了我国立法的回应性和专业性，但仍有不足。一方面，当前信息规制的行政文件效力层级较低，立法技术不成熟，在信息跨境流通、信息匿名化等领域呈现碎片化、地域化的特征，降低了规制效力；另一方面，复杂社会政府权力

① See Richard Y. Wang, Diane M. Strong, “Beyond Accuracy: What Data Quality Means to Data Consumers,” *Journal of Management Information Systems*, Vol. 12, No. 4, 1996.

② 王天恩：《大数据的规模整全性及其重要哲学意蕴》，《江汉论坛》2022 年第 4 期。

③ See Helen Nissenbaum, “Privacy as Contextual Integrity,” *Washington Law Review*, Vol. 79, 2004.

④ See EDPB, *Guidelines 01/2021 on Examples Regarding Data Breach Notification*, 2021-01-19, [https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-012021-examples-regarding-data-breach\\_en](https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidelines-012021-examples-regarding-data-breach_en), visited on 2024-04-01.

⑤ See EDPB, *Guidelines 05/2022 on the Use of Facial Recognition Technology in the Area of Law Enforcement*, 2022-05-16, [https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area\\_en](https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_en), visited on 2024-04-01.

⑥ See OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 2002-12-12, [https://www.oecd.org/publications/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data\\_9789264196391-en.html](https://www.oecd.org/publications/oecd-guidelines-on-the-protection-of-privacy-and-transborder-flows-of-personal-data_9789264196391-en.html), visited on 2024-04-01.



扩张，行政规章由于空白授权在事实上发挥着“立法形成”的功能，潜藏了合法性风险。同时，广泛的行政裁量权和规制的专业化加剧了政府结构的集中，导致行政权力的自我赋权。如此，强监管—强专家的治理模式可能提高企业合规成本，同时增加权力寻租空间，降低行政规制的合法性。因此，必须提升行政规制的合法、科学和民主化。这就要求强化立法约束，提升法律、规章制定中的民主商谈。(1) 立法商谈环节应扩大并落实法律、规章的公开征询过程，广泛吸收公众和专家商谈的意见、共识与关切，使得法律形成经过技术专家的专业论证、商业和公民代表的审议表达、社会公众和舆论的公开监督，<sup>①</sup> 确保利益相关方的有效、透明、切实参与。(2) 行政规章制定环节也应符合法定和民主要求。行政部门的内部审查应坚持规制手段的可行性、合理性与合法性，涉及公民（与企业）基本权利义务的规章应当通过立法机构的合法性审查，行政手段的调用须符合法治原则和比例原则，推进执法效率提升与执法合法性的共同实现。

其二，实现信任对科技发展的结构嵌入。“法律即代码，代码即法律”的主张忽视了法律作为社会科学区别于自然科学的本质，即法律作为社会生活交往的产物，受制于社会关系建构的妥当性和正当性要求。因此，必须正确看待法律与科技之间的互动关系，理解法律“白箱”为“技术黑箱”提供的负责环境。(1) 尊重科技发展的有限自治。承认技术在一定程度上的不可解释性，不能“一刀切”，要求算法技术绝对、事前、完全透明，但以其目的正当、程序正当为限，强化算法技术负责制。(2) 助推“经由设计的信任”。技术发展具有一定的建构性，应通过立法要求，强化技术开发端、说理端和救济端的信任建设，提高架构可信度，弱化对社会的负面影响。(3) 鼓励技术共同体的内部反思。知识共同体具有争鸣性、开放性，应当允许并鼓励技术专家争鸣，通过“赋权个人”与“赋能企业”展开抗衡，推动科技产品升级，促进用户权益保护。(4) 强化技术说明和信任程序的建构。信息技术决策具有自动性，应强化信息处理和利用过程中的整体安全性、可解释性和完整性，完善决策影响评估，以合法性、必要性为底线，推进信息法的知情—同意原则、目的限制原则、数据最小化原则、数据参与原则的落实，合理引入诚信原则。

其三，鼓励市场信任，营造良好竞争环境。信息流通是自发市场行为，具有规模合作的动力，但也易产生“丛林法则”的天然弊端。在鼓励信息开发的同时，应加强市场秩序建设，通过设定公平基准，推动交易信任，营造良好竞争秩序。(1) 建立健全数据用益制度，将开发者权益保护明细化，尊重知识产权和劳动投入，推进信息利己和利他并行，完善公开“数据池”的建设，探索数据信托制度，建立数字使用和开发信任机制。(2) 提升行业自治，推动市场交易诚信环境的塑造，通过行业准则、技术门槛、企业黑/白名单等自治监督，促进市场互信。(3) 建立健全信息处理行业准入门槛，强化算法审计评估。除对国家安全、经济市场和社会与公共利益的影响外，仍要评估特定技术应用对信息主体的自由与尊严的潜在威胁，鼓励企业良性竞争。(4) 加大消费者保护与信息市场的衔接力度，尊重消费者权益，鼓励通过消费者公益诉讼等方式，激活社会能量，培育权利文化，发挥社会法的自我纠偏效力。(5) 完善执法工具，通过各地市监局监管工具的改进，推进反不正当竞争与反垄断法的完善，及时识别、监管不当竞争行为，促进信息市场开放，发挥信息流通的良好功用。

其四，完整认识现代伦理信任的形式性、程序性。在数字时代，市场行为和技术开发具有较高的自发性、不可解释性，基于实质伦理的注入很可能徒劳无功。同时，伦理活性减弱的现代社会往往呈现主体多元、利益分殊的多元格局，强伦理导向的强监管未必收益良好，甚至可能破坏信任预期，扰乱数字市场。(1) 信息伦理的建设必须认识法律规制的限度，推进信任建构的多主体性、交互性、多边性，鼓励利害关系方在立法、执法和自律中发挥作用。这些利害关系方包括但不限于数据收集者、数据处理者、行业自律部门、普通用户、国家监管部门、社会公益组织，分别建立维系交易的市

<sup>①</sup> 马剑银：《通过公共领域的立法民主——商谈论视角下的立法过程模型》，高鸿钧、何增科主编：《清华法治论衡》第十一辑，清华大学出版社，2009年。

场信任、促进团结的伦理信任、保障权利的执法信任和推动创新的科技信任，推进信任模式的弥散化、共识化、规模化。(2) 在法律信任的模式下，处理好形式与实质、一般与情境的关系，正确认识数字信任的弱共识性和强预期性，通过信息信任的程序条件与实质条件的合作，吸纳风险异议。这不仅要求行政部门内部的灵活执法，也要求一种科学、谦抑的立法伦理。借助立法焊定最低信任共识，并与经济系统、政治系统、科技系统进行有限的意义兑换。

## 六、结 语

数字社会的开放性、流动性和大规模性使得信息进一步的流通和利用不可避免。个人信息治理方案既要求符合信息流通的功能发挥，也必须内嵌共识性的意义结构，提供信息保护的有力约束。当前，我国个人信息保护与流通的多重方案，要么陷入对权利本体论、封闭论、原子论的误解，忽视信息利用的潜能，要么容易走向纯粹实用主义的误区，贬损个人信息保护的价值。现代数字立法应将焦点置于信息信任的构建，特别是信息处理过程中的信任维护。信任具有稳定规范性期待、确保将来合作的功能，必须作为数字法治的核心来对待。借助其“软强制—强介入”，信息立法可以将来自社会共同体的信任资源带入国家法的建构，实现法律与社会的协奏；借助其“弱共识—强预期”，信息立法有助于应对现代沟通社会信息关系的即时性、过程性和生成性，强化信息流通中的保护；最后，法律必须认识到自身规制的限度，与技术、规范、市场等协作，形成系统性信任框架。通过信任原则的安全、透明、公正、反歧视、整全的法治纳入，形成信息处理的程序与实质约束。

当前我国数字立法已经将信任要素纳入平台治理<sup>①</sup>等局部设置，但仍可继续完善。信任建构应以立法为开端，通过强化立法的民主参与，为信息规制权注入信任要素。信任经由民主化的立法嵌入法律系统，实现与科技、市场、现代伦理的耦合，推进信任、法律、技术和市场的合奏，实现信息流通中的保护和保护下的利用。

(责任编辑：武素迁)

<sup>①</sup> 戴昕：《平台责任与社会信任》，《法律科学（西北政法大学学报）》2023年第2期。