数字经济次生风险的全景透视与法治之维

张　媛

摘　要：数字经济次生风险系目前我国数字经济发展面临的理论和实践问题，应通过科学的解析和规范的限制进行回应。鉴于数字经济次生风险的复杂性，采取区分主体的分析框架并实现解析的体系化是恰当的进路：从国家层面来说，全过程数据利用行为的不加规制造成了数据主权之风险；从市场层面来说，外观自由、实际已然接近垄断边缘的数字经济市场当然需要进行矫正；从个人层面来说，数字经济伴随着文化、社会等变化也引发了个人权利陷入不安定的境地。围绕问题进行拆解，国家层面数据主权之风险系数字经济发展和安全之间平衡困难造成的；市场层面贴近垄断系当前技术霸权之现状造成；诸多规律性假定失效使个人信息完整规制方案真空，相关负性影响也随之显现。我国应当基于法治策略确保数字经济的可持续发展，寻求法治保障降低国家安全风险，反对霸权行为；发挥法律激励作用对接市场发展规律，将法治融入市场；适当“过正”矫枉保护个人基本权利，形成文化、氛围与观念。

关键词：数字经济次生风险；数字主权；技术霸权；垄断；基本权利

中图分类号：F49　　**文献标识码：**A　　**文章编号：**1003-0751(2023)12-0031-08

数字经济为推动建设现代化经济体系、建设数字强国发挥重要作用。数字经济发展机遇与挑战并存，加快我国数字经济的体制建设与发展，不仅要抓住数字经济的发展机遇，更要防范数字经济的风险。对于数字经济的风险，目前学界并没有进行系统的分类识别。若从数字经济的兴起和发展来看，企业的数字化构成了数字经济的基础设施建设[1]，在这个意义上，企业可谓是数字经济发展的基石。为了应对经济的数字化发展，企业必须要在技术和数据两大方面抢占先机，而企业据此展开的一系列竞争活动在很大程度上也成为引发数字经济风险的导火索[2]。在一国乃至全球范围内存在着企业不当攫取、过度收集乃至不当处理数据的风险，以及企业利用技术优势对市场进行垄断导致不正当竞争、不公平竞争风险等。企业作为数字经济发展的基础，是构成上述风险的核心要素，文章倾向于将上述风险视为数字经济引发的直接风险，即“原生风险”。而这些原生风险可能会在实践中不断地在政治、经济、法律等领域蔓延，从而引发新的风险。例如，企业在全球范围内对数据的攫取可能会威胁到各国数据主权安全；企业利用技术优势进行的市场垄断可能会进一步加大反垄断的难度以及对消费者权利的侵害；企业在一国范围内对数据的过度挖掘可能会威胁到个人隐私、个人公平获取资源的权利等。本文倾向于将上述由“原生风险”引发的新风险视为数字经济的间接风险，即“次生风险”。

随着数字经济相关产业体量的不断扩大，不可克服的系统性风险积聚，在数字经济原生风险不断升级的同时，数字经济的次生风险也持续发酵，因此有必要意识到数字经济的次生风险是影响数字经济持续健康发展的重要因素。次生风险的规模扩大，将有可能成为未来我国数字经济发展的重要矛盾。研究数字经济的次生风险不仅可以推动构建新发展格局、改造传统产业、建设现代化经济体系，也有助

收稿日期：2023-06-08

作者简介：张媛，女，青岛农业大学人文社科学院教授(山东青岛　266109)。

于保障国家数据主权安全、规范数字经济市场运行、保障公民数据隐私。纵观目前国内对数字经济次生风险的研究，学者们大多从管理学、金融学等学科视角分析数字经济次生风险的成因，而忽视了法治对数字经济蓬勃发展的意义。因此，本文从法治视角解读数字经济次生风险，从认知框架、生成机理与法治策略三个维度展开讨论，欲在法律层面对我国数字经济可持续发展中存在的次生风险进行系统化梳理。

一、框架搭建：基于不同主体的观察视角

数字经济次生风险的表现丰富，与其存在形式、管控框架等存在诸多联系[3]，需要归入特定的框架展开系统性分析。

1.基于国家的观察：数据利用行为与数据主权

数据具有虚拟属性，与传统生产资料所具备的地域属性不同，不同国家与地区在数字资产的产业认知与司法解释上存在巨大偏差，由此而形成的数据主权竞争风险不断在地区和国家间累积，数据主权的概念就是诞生于数据资源不平衡的基础之上。数字经济带来的数据主权安全问题主要表现在以下几方面。

第一，企业间数据跨境流动风险威胁数据主权安全。数据跨境流动安全风险已成为各国关注的主要问题。就数据出境而言，存在两个层面的风险。一是内容层面的风险。数据出境的内容可能涉及到国家安全信息，国家安全信息的外流可能对国家安全产生重大威胁。二是数据出境方式和地点的选择对数据主权安全带来风险。若有相关主体受利益驱使采用非法方式阻碍数据合法出境，必然会威胁国家数据主权。另外，在数据跨境流动过程中必然会经过不同的国家、地区，接受不同的网络服务提供商的服务，如果数据流动经过数据主权重视不足、数据权利保护力度不大的国家或地区，则会对数据主权产生严重威胁。

第二，企业数据的利用威胁数据主权安全。随着云计算和大数据技术的发展，越来越多的数据被存储在跨国的数据中心。企业和个人的数据可能会跨越国界被存储、备份和处理，从而导致数据利用具有跨国性。除跨国企业之外，互联网技术也使得数据可以通过网络在国家之间进行快速和便捷传输。企业可能收集到来自不同国家的客户数据，并进行统一分析和利用。数据流通的跨国性导致数据一旦跨境流通，就有可能成为不法分子的有力武器，数据主权安全便会受到威胁。

第三，企业数字技术控制威胁数据主权安全。数字技术是智慧的治理技术，其通过增量式赋权和重构式创新，实现具体问题与治理主体、解决方案的智能匹配，有效提升治理效能[4]。当前数字经济背景下，一国数字技术的发展能够提升本国在数字经济时代的竞争力和抵御经济风险的能力，如果没有先进的数字技术，就可能陷入潜在的国家数据主权安全风险的包围圈。数字技术的掌握与数据流通渠道紧密相连。先进的数字技术能够确保本国合法有效地管理和掌握数据资源，避免数据被他国或跨国企业所控制，进而丧失对数据的掌控权。拥有先进数字技术的国家可能会利用自身的技术优势，对其他国家进行网络攻击、黑客攻击等。因此，发展先进数字技术的国家也能够有效应对和防范这些攻击，保障国家安全和经济利益不受到损害。另外，数据资源已经成为一种重要的生产要素。如果一国没有先进的数字技术，无法有效地利用和加工数据资源，就会面临技术依赖和竞争劣势。其他先进技术国家可能会通过技术霸权等手段，垄断数据资源，从而限制该国自身的经济发展和市场扩大的可能性。

2.基于市场的观察：市场自由发展与市场垄断

从经济的一般理论出发，无论是农业社会、工业社会还是数字社会，生产要素对经济发展均具有积极的推动作用。与农业时代和工业时代的劳动力等生产要素类似，数字化时代，数据要素的产生改变了传统的基于所有权的分配模式和财产保护模式，推动了经济发展方式的转型[5]。数字化时代，为了实现经济效益最大化，资本往往通过积累形成规模效应，并通过垄断形成技术优势，进而反向加固数据“围栏”[6]。这在阻碍数字要素流通的同时更不利于其经济效用的发挥，在市场层面存在以下两方面的风险。

第一，在数字产业形成规模经济后，数字市场的垄断行为会加大反垄断的难度，对市场的自由竞争产生更强的负面效应。相较于传统行业垄断行为的司法界定，当下由于社会缺乏对数字产业发展的充分认识，对如何衡量以及甄别经济行为中的垄断行为缺乏有效的法理依据以及现实裁定限度。原因在于，我国数字化转型的技术主体更多地依赖于各类企业，其与政府部门相比在数据收集、分析和管理等方面具有明显的技术优势。尤其是随着人们日常生

活的数字化转型,各类企业在总体上拥有越来越多数据的同时,对消费者的细节认知和了解也逐渐渗透进衣食住行等各个领域。与传统企业的市场垄断不同,数字企业不需要将物质资料进行空间上的集中,而是依靠其核心技术收集庞大分散的数据,这加大了资本对数据的统治力度[7]。随着数字化转型的逐步深入,考虑到大数据时代的智能算法特征,企业掌握的数据越多,便越能对市场整体和消费者个人进行准确的把握。为占据产业内部的优势地位,企业将通过横向扩张不断扩大自身的用户覆盖,通过纵向扩张完善自身发展的供应链建设,从而形成企业护城河。如果不对数字要素的垄断加以规制,数字要素垄断的现象将必然发生。一方面,由于数据要素改变了传统物质存在的时空属性,人们无法对其进行直接感知,仅仅通过使用无法得知平台的算法逻辑;另一方面,由于算法的技术特征,即便一般消费者获取了其代码逻辑,也难以就其内容展开实质性审查,种种特征加大了数字垄断的外在监督难度。

第二,对消费者权益的侵犯同样是数字垄断产生的弊端之一。鉴于数字平台垄断势力的不断增强,其损害已经不再局限于价格与经济层面,由于其服务的提供对象往往是消费者,垄断平台所涉及的利益损害更多地涉及隐私和公平维度[8]。一方面,由于数字平台对消费者个体肖像特征的准确把握以及算法的不透明性,垄断平台容易对消费者产生算法歧视,具体表现为不同消费者对相同商品的消费价格不同,或者同一消费者在不同时间、不同地点对同一商品的消费价格不同;另一方面,由于平台经营者具有技术优势,在日常的数据管理、运营规则的建构等方面往往具有更多的话语权,扮演着管理者与仲裁者的双重角色[9]。当垄断平台与消费者产生纠纷时,前者具有的技术优势往往更容易在纠纷中占据主导地位,这不利于保障消费者权益。

3.基于个人的观察:数字经济侵蚀与权利安定

在数字经济的场域中,由于互联网具有联通性,个人不再受制于物理空间意义上的天然屏障,在个人层面的数字经济次生风险集中表现为个人信息安全风险。与财产安全密切相关的信息安全负载于隐私权之上,而数字经济的异化风险则主要来源于其开放化与商业化发展。其一,数字经济的发展要求通过数据开放来实现特定的数字经济目标,但这与个人信息和隐私安全的保障之间存在某种难以调和的张力。对信息安全的保护强调数据的有限开放,以实现数据信息权益保障和合理利用之间的平衡[10]。但基于数字经济的数据开放要求,作为用户的个体在数字经济生活中实施的各项活动都将使关乎其人身和财产安全的数据信息完全暴露于数字平台和社会公众的视野之下。深度参与数字化生活的个体在数字经济各领域中的实践使其原本应处于隐私范围内的数据信息形成体系化联结,个人隐私的整体面貌以及个人的身份、偏好等重要信息外显。其二,数字经济中的各主体基于商业目的而导致隐私性数据信息的非法流通。在逐利动机的驱使下,商业实体或数字平台不仅可能利用个人信息中体现出的个人对特定服务或商品的偏好而谋取利益,还可能通过共享这些数据信息达成垄断性的“商业联盟”。在此情形下,被不当开放的个人数据信息将进一步沦为商业化工具,隐私权的尊严属性被大幅削弱,个人信息安全也无法得到有效保障。

与此同时,算法歧视也会在很大程度上阻碍个人数字资源权利的实现。算法看似具有中立性,但其往往内含着某种价值选择或价值倾向[11]。通过对个人自主选择的干预,这种隐蔽的价值要素使算法发展出(一般意义上的)歧视的衍生态,并严重阻塞了个人获取数字资源的渠道。具体而言,作为算法歧视常见形式的算法推荐,通过获取相对人的数据信息,提炼出个人偏好,并有针对性地为相对人推送相关信息。此种算法推荐模式虽然能够在一定程度上便利人们的生活,但也致使个人的自主决策权受到侵蚀[12]。算法技术所内含的规律模式将形成某种“偏见”,悄无声息地影响人类的实践理性决策,并消弭人类个体的个性与社会生活的偶然性与动态性,使个体只能机械地获取算法所提供的数字资源。在此情形下,个人公平获得数字资源的权利便受到了侵害,个体本应能够为其决策行为构建一个全面、立体的背景性蓝图,却因算法歧视而被困于极其有限的实践范围中。

二、多维透析:基于对照原理的规范讨论

数字经济具有次生风险是客观事实。从历史的维度,国家的数据主权可能会受到威胁;从市场的维度,数字经济可能会导致市场垄断;从伦理的维度,个人的信息与隐私也有安全之虞。数字经济的次生风险会严重损害其持续发展的能力,只有排除这些风险,才能使数字经济迸发前进的力量,从而造福国

家、社会与人民。

1.数据主权对数字经济的桎梏与国家的选择之难

数字经济被誉为“第四次产业革命”[13],要分析其次生风险,我们需要回归到历史的维度看前几次产业革命。蒸汽机的发明促进了第一次产业革命的到来,诞生了全球第一个“日不落帝国”——英国,英国凭借着坚船利炮叩开了清朝的大门,掀起了列强瓜分中国的狂潮;第二次产业革命的标志是内燃机的应用和电动机的诞生,这催发出一系列大军工复合集团,从而引发了两次世界大战,中国也在日本的入侵下面临亡国灭种的危机;第三次产业革命是原子能革命,新中国长期面临着美苏两国的“核讹诈”,我国研究出“两弹”后主权才得到保证。从历史规律就能看出,每一次产业革命都是先发国的狂欢,先发国凭借巨大的科技、经济与军事的优势,将殖民、灾难和战争输出到后发国家[14]。历史证明:想要利用好产业革命成果,必须掌握技术上的主动权[15]。在数字经济勃发的新时代,必须维护好国家的数据主权[16]。当前我国数据主权面临三大隐患。

第一,我国的数字技术基础相对落后。尽管近年来我国数字经济发展迅速,俨然进入发展的第一梯队,涌现了一批世界瞩目的高新企业,诸如阿里巴巴、腾讯、华为等,但是我国的数字技术基础相较于西方国家仍然相对落后。首先,在材料与硬件方面。数字技术仰赖于很多材料与硬件,比如高分子化合物、光纤、芯片等,西方国家在这些技术方面能轻易地卡我国的脖子,造成重大的国家安全隐患[17]。其次,在软件与代码方面。西方国家的计算机科学发展较早,科研成果极其丰富,吸引了全球的专业人才。我国在技术系统开发上仍较为落后,比如ios、安卓、windows等操作系统的源代码始终掌握在西方国家手中[18]。最后,在关联学科配套方面。发展数字经济不仅需要在计算机科学单方面努力,还需要加大对物联网、市场营销、社会学等各关联学科的支持。

第二,我国技术发展面临西方国家的遏制。我国的迅速崛起引起了西方国家的警惕,其对我国技术发展实施了遏制政策,西方的技术封锁拖缓了我国技术发展的节奏[19]。最典型的例子就是近年来异军突起的生成式人工智能技术,美国拥有谷歌、OpenAI等人工智能巨头公司,但我国由于GPU的进口限制,难以大规模开展大语言模型的训练,使我国在人工智能科技的竞争上处于相对不利的位置[20]。

第三,我国的法律与监管处于两难境地。法律与监管是一把双刃剑,一方面,没有系统的法律约束会造成各种失范现象,比如企业的不正当竞争、恶意竞争、损害公益、侵害公民权利等,这些现象是我们要极力避免的;另一方面,如果法律与监管过度,则会抑制科技创新,会使科技人员与公司束手束脚,动辄坠入法网,容易产生“躺平”现象,这对我国参与此轮科技竞争是非常不利的[21]。我国的法律与监管处于两难境地,可能会对我国的数据主权造成潜在的威胁。

2.天然优势对数字垄断的支持与市场的假定失效

第一,垄断行为的认定关键在于特定经营者是否处在市场支配地位,而数字经济的崛起使得这一过程变得极为复杂。一方面,数字经济中“相关市场”的模糊性使得垄断行为的范围难以明确。数字经济的特性使得产品和服务的边界变得模糊,传统的市场界定方法难以准确评估市场结构。另一方面,现有的关于市场支出的单一标准难以全面评估经营者在数字市场中的实际地位。数字经济中的网络效应和数据积累使得市场份额无法全面反映经营者的实际市场影响力。尽管《反垄断法》和《国务院反垄断委员会关于平台经济领域的反垄断指南》提出了一系列认定市场支配地位的指导原则,包括市场贡献、技术优势、经济实力等,但在数字经济中这些因素如何认定仍存在一定难度。执法机构在制定具体认定标准时存在困难,使得数字经济的快速发展与反垄断执法标准不明确之间的矛盾愈发突出。执法机构如果不采取严厉态度,可能导致严重的竞争问题,增加数字市场面临垄断风险的可能性,进一步加剧数字经济市场垄断的风险。

第二,数字经济加大了反垄断立法分歧。关于市场垄断行为,部分学者主张通过政府外部力量及时规制垄断,以维护市场公平;而另一部分学者认为垄断是市场发展的必然阶段,应通过市场自身机制调节,无需制定反垄断法[22]。2022年最新修订的《反垄断法》增加了鼓励创新的立法目的,然而如何处理创新与市场结构的关系,完全竞争和寡头结构哪一种更有利于创新,学界迄今为止尚未达成共识[23]。数字经济的复杂性使得传统经济理论在解释市场行为方面的局限更加显现。数字经济使公平与效率之间的矛盾日益突出,在数字化转型中,市场

结构的动态变化增加了反垄断法立法的复杂性。创新驱动的数字市场可能会因寡头结构而受到阻碍，但完全竞争也极有可能导致公平问题，这种矛盾张力使得法规制定面临巨大挑战，如何平衡创新推动效率提升与维护市场公平的目标，是数字经济背景下推动数字市场健康持续发展亟待解决的问题。

3.规制空白对算法侵害的无知与个人的权利灭失

第一，算法客观性和中立性的偏移激发了算法侵害风险。算法基于数学和逻辑原理而起，是客观而中立的，然而随着数字经济的发展，算法与资本的融合使得算法本身的客观性、中立性产生偏移，在数字消费领域甚至被用来侵害人们的权利。数字经济背景下，算法的设计和使用往往是为了实现特定的目标，这些目标可能与企业利益相关，比如增加销售额或用户参与度，这可能导致算法在作出决策时不考虑甚至侵犯消费者的权益，如在严重的信息不对称的情况下被迫接受“一人一价”[24]。当算法被用来最大化经营者利益时，消费者的权益必然会遭到损害。同样，数字技术并不是在真空中发展的，它们是在特定的社会文化背景下产生和发展的，这意味着这些算法技术反映并加强了现有的社会结构，包括其不平等和偏见。在很多情况下，法律和伦理框架无法完全赶上数字技术的快速发展，这导致了算法歧视和侵犯消费者权利的问题很难通过现有的法律和规章来解决。

第二，“算法黑箱”带来监管挑战。数字经济时代，算法作为数据这一新生产要素的重要推动力对提高社会生产力起到了关键作用，然而算法本身存在的“算法黑箱”问题所带来的法律风险逐渐显现。所谓“算法黑箱”指的是由于技术本身的复杂性以及技术公司实行的排他性商业政策，导致算法的工作原理和目标对用户而言像一个未知的黑箱。由于算法黑箱的存在，当算法引发的行为导致损害时，确定责任主体变得复杂，责任应归咎于算法设计者、使用者还是算法本身？这种不明确的责任归属为法律责任的追究带来了挑战[25]。同时，算法黑箱还导致了算法决策过程的不透明，这影响了使用者的知情权和对算法决策过程的公正性评估。“算法黑箱”的存在不仅增加了保护数据权利的难度，而且还可能为算法侵犯数据权利开启了更多“通道”。当然强调算法透明度和可解释性的同时，也需要考虑到算法创造者的知识产权和商业秘密保护。如何在不侵犯技术公司商业秘密的前提下确保算法的透明度和公平性，是另一个法律难题。

第三，数字准权力引发社会风险。在人类社会的发展史上，权力的源泉从土地演化为劳动力再转移到资本。而在数字经济时代，这个源泉变成了数据，控制数据等同于控制权力。然而，数字准权力并非来源于人民，而是由市场中的运营商收集的数据积累而来，这可能会威胁到社会关系的稳定。一方面，数据权力可能集中在少数大型企业手中，这些企业能够控制信息流动，影响市场竞争和消费者选择，形成数字垄断，加剧社会和经济的不平等，不利于数字经济的良性发展。另一方面，数字技术拥有者可以通过大数据操控公众意见，影响政治决策等。当私营企业掌握大量数据时，可能会影响政府决策，导致公共权力的私有化和政府职能的弱化，侵蚀政府的公共职能。

三、法治路径：基于问题解决的体系展开

数字经济逐步成为中国经济和世界经济增长的重要引擎。习近平总书记在第二届世界互联网大会上强调：“我们愿意同各国加强合作，通过发展跨境电子商务、建设信息经济示范区等，促进世界范围内投资和贸易发展，推动全球数字经济发展。”[26]然而，如何更好地发挥数字经济在经济发展中的助推作用仍是一个未解的课题，因为数字经济既对经济发展和人民生活具有积极作用，同时也伴随着潜在的次生风险。针对这些风险，本文基于法治策略探讨数字经济的可持续发展之路。

1.寻求法治保障，降低国家安全风险

第一，以法治保障下的自主研发技术为根基。在全球科技竞争中，我国的数据技术尚未实现对发达国家的弯道超车，仅仅依赖于技术的引进和学习并不能在全球技术交流中取得优势，自主研发仍然是走向世界科技领域前沿的必然选择。为此，应当迅速建立健全数字基础设施相关法律法规，完善数字监管机制，保障我国数字基础设施的建设；应当加强数据人才的培养，重视培养学生的实际操作能力，加强校企合作，更好地培养适应数字经济时代的人才。

第二，以国际数据市场的法治建构为导向。目前全球科技竞争局势处于全球化趋势不可逆转与西方国家高筑技术壁垒的叠加态，以国际数据市场的法治建构为导向是我国在全球数据领域取得独立地

位的重要途径。一方面,既要重视科学数据的开放共享在科学研究中的重要性,积极参与到全球科学数据开放共享政策的制定与实践合作中[27]。另一方面,我国必须积极参与相关市场规则的制定,推动数据资源的合理利用,使我国在全球数据舞台上发挥更大的作用。成为规则订立者能够有效地防范西方国家在贸易谈判中对我国采取不公平举措,在面对贸易摩擦时可以更有力地进行司法回击,维护我国在数据领域的权益。

第三,以国际性数据平台监管为支撑。数据作为数字经济发展的基石,其只有在流动中才能创造价值,跨境数据流动是跨国公司全球经营得以实现的必要条件[28]。但数据流动和使用也存在潜在风险。例如,技术发达国家和大型跨国公司依据其技术能力能够做到盗用或非法使用其他国家的各类不公开数据,私自收集网络用户的偏好等信息。在全球数据流动的复杂网络中,事前法律难以完全阻止这些不正当的数据使用行为。我国要在全球数据治理中发挥更为积极的作用,就应主导建设国际数据平台监管体系,以保护我国数据主权和各国用户数据权益为目的,打破技术发达国家和大型跨国公司对国际数据交流的不当使用。

第四,以数据技术的产学研结合为动力。我国正处于数据技术发展的关键时期,产学研的结合仍是我国数字技术发展的动力源泉[29]。大数据试验区法治化则是产学研结合的重要抓手,其为产学研合作提供了丰富的信息资源,可以为高校、科研院所以及企业提供研究素材,推动产学研的深度融合。其一,发挥高校学生独具的创新优势,为产学研的合作提供更多的实际案例,推动理论与实践的结合。其二,科研院所作为数字技术研发的核心力量,保障其法律权益有利于拓展其研究的深度和广度,奠定数字技术的产业化基础。其三,通过立法鼓励数据企业拓宽研究领域,注重数字技术在实际应用中的推广。其四,通过法律的协调作用在高校、科研院所与企业之间建立合作机制,推动信息和资源的共享,最大程度地发挥各方的优势。

2.发挥法律激励作用,对接市场发展规律

党的二十大报告指出,必须更好发挥法治固根本、稳预期、利长远的保障作用。诚如上文所述,数字经济的发展滋生了数字垄断等一系列市场风险,需要通过法律制度来指引技术的发展,防止技术垄断,保障市场健康运转。具体而言,可以通过以下路径予以实现。

第一,注重对隐私的保护。平台作为利益主体很可能在利用个人信息的时候对之产生侵犯。基于此,应当将隐私作为一种非价格因素纳入反垄断的框架之中。在数字化时代,隐私权遭受侵害的风险随之增大,必须通过立法对其进行有针对性的规制。可以将该思想体现在我国的《反垄断法》中,即在立法目的条款“维护消费者利益”中增加隐私和数据保护的内容。此外,还可以把《电子商务法》第35条的内容吸收到《反垄断法》中,将平台内经营者改为交易相对人,即可解释为消费者,从而实现对消费者隐私与数据保护的目标。

第二,重塑监管与反垄断的二元治理格局。对守门人在基础平台服务范围内的活动进行监管,明确其对数据监管的法律义务;在基础平台服务范围以外或者虽然在基础平台服务范围内但没有达到标准的平台企业,对守门人的所有经营者集中行为,均通过反垄断机制予以规范[30]。明确监管与反垄断的二元界限,避免两者的相互代替和重叠。此外,还应推动实现监管与反垄断两者之间的良性互动,发挥两者在数据规制方面的作用,促进两者互补,形成制度合力。当然,此二元治理格局的重塑仅靠上述思路的倡导是无济于事的,还需要立法与制度层面的充分供给,故应加快制定数字平台法,细化反垄断实施的相关规定,并推动各项配套措施的改革。

第三,丰富数据监管手段。鉴于数据具有高流动、高渗透等特征,应建立相应的数据流动的动态监管系统,实时掌握数据流动情况,尤其是对大型平台的数据流动情况进行重点与严格的监控,一旦发现失当情况,如妨害市场竞争秩序、损害相关主体利益等,立即开启调查程序。当然,监控的标准并非一概而论,应当针对不同领域的情况进行具体调整,对于涉及到民生福祉的数据应当重点监控,而对于一般领域的数据则应当进行相对宽松的监控。此外,传统的监管方式应紧随时代步伐进行相应更新,特别是面对数据技术这一时代命题,更要立足于技术本身,构建新兴的监管方式。新兴的监管方式有利用大数据进行有效监控、将算法代码中加入数据保护科技、通过人工智能发现问题等,一旦发现不轨之举,可立即向政府监管部门报告。

3.适当“过正”矫枉,保护个人基本权利

构建完善的数据法律制度是防范和化解数据权利风险的关键环节。在构建过程中,可以参考法律关系的基本范式,科学配置不同数据关系主体之间的权利和义务。

第一,完善个人隐私权的立法保护。这是化解数字经济与个人信息权保障之间张力的有效手段。在数字经济时代,数据具有高流通性,数据权利风险也呈现出隐蔽性、复杂性、多发性等特点,严重威胁个人信息安全。因此,通过完善相关立法可以为保护个人隐私权提供规范基础。一方面,应优化知情同意原则的适用条件。个人隐私数据相较于普通信息数据而言,具有高度敏感性和高度重要性。因此,在制定相关法律时,应考虑从告知方式、告知内容、责任后果等方面优化知情同意原则的制度架构,以增强其可操作性和严格性。另一方面,要注意个人隐私权立法与其他法律法规的衔接与融合。可以通过两种模式,即专门立法和分散立法,来完善个人隐私权的规范基础。需要注意与《个人信息保护法》等法律法规的横向衔接与纵向连贯。在保持法律体系的一致性的同时,加强对个人隐私权的全面立法保护。这样可以确保个人隐私权的法律保护得到充分落实,为个人信息在数字经济中的合法使用提供有力支持。

第二,加大对数据权利的保护力度。在宪法的法理逻辑中,国家是基本权利的当然义务主体。在数字经济时代,智能算法的创新对传统社会治理结构和社会组织格局产生了强烈冲击,仅仅依靠公民的力量难以应对这些变化。在新兴的社会治理格局中,技术弱势群体极易受到技术资本的潜在侵蚀,很难确保自身处于对等地位和保障自身的数据权利。虽然宪法文本中规定了国家对公民基本权利的保护义务①,但这并不能涵盖智慧平台与公民个人之间的权利保护的全部路径。因此,应从基本权利的功能体系出发,强化国家的数据权利保护义务。一方面,国家应负有不得侵犯公民个人数据权利的禁止作为义务。在国家公权力的行使过程中,不得侵犯公民的数据权利安全,不得强制公民公开或允许使用数据权利等。另一方面,国家应承担积极义务,通过给付以及其他积极行为等方式促进基本权利的实现。国家可以通过提供有效的制度供给和环境保障,帮助公民对抗大规模、持续化数据处理活动中潜在的人格尊严减损和数据权利侵害的风险[31]。从基本权利的防御权功能和客观法功能两个维度加大国家对个人数据权利的保护力度。

第三,推进数字经济的产业自律。仅仅依靠反垄断执法机构和反不正当竞争执法机构难以有效规制数字市场的垄断行为和不正当竞争行为。为适应新兴社会治理方式的发展需求,要合理界定政府与市场之间的职责边界,并汇聚行业组织、市场主体和政府部门的多元化力量,建立多元化的协同治理机制。在这一过程中,行业自律发挥着重要的作用,既能保护数据权利,又能促进数字经济的发展,同时也有助于转变政府职能。一方面,应建立行业自律组织,构建以保护数据权利和发展数字经济为宗旨的互联网隐私行业自律组织。这样的组织可以制定行业准则和规范,监督行业成员的行为,促进行业的健康发展。另一方面,应适当融入政府监管,完善数据权利保护的事前防御机制和事后保护机制。建立事前的数据权利保护机制,如审查和评估数据处理活动的合规性;建立事后的救济机制,如投诉处理和争议解决机制。这样可以确保数据权利得到全流程的保护。

注释

①个人信息权的宪法规范基础可以追溯至《宪法》第 33 条第 3 款,即“国家尊重和保障人权”。在宪法的规范结构中,国家是基本权利的约束对象,也是基本权利的义务主体。因此,国家原本就有对个人信息权的保护义务,只是在数字经济蓬勃发展的当下,面对较高的数据权利侵犯风险,有必要加大国家的数据保护力度,以国家公权力加强对个人基本权利的保护与救济。

参考文献

[1]任保平,何厚聪.数字经济赋能高质量发展:理论逻辑、路径选择与政策取向[J].财经科学,2022(4):61-75.
[2]汤长安,赵新伟.中国数字经济风险测度研究[J].湖南师范大学社会科学学报,2023(2):55-62.
[3]魏星.共享经济[J].中国科技术语,2017(5):79.
[4]张丙宣.如何运用数字技术提升治理效能[N].学习时报,2020-03-30(5).
[5]张平.数据生产要素性质、知识生产与中国式现代化[J].社会科学战线,2023(10):44-57.
[6]贾利军,郝启晨.基于马克思地租理论的数据生产要素研究[J].经济纵横,2023(8):1-11.
[7]程恩富,余晓爽.数字经济时代的数据垄断与掠夺路径分析[J].理论月刊,2023(9):76-83.
[8]唐要家,王钰.数字经济反垄断消费者福利标准的重构[J].人文杂志,2022(8):46-56.
[9]周文,韩文龙.平台经济发展再审视:垄断与数字税新挑战[J].中国社会科学,2021(3):103-118.
[10]杨建军.数字治理的法治进路[J].比较法研究,2023(5):1-19.
[11]孙伟平.价值哲学视域中的算法歧视与社会公正[J].哲学研究,2023(3):46-55.
[12]邱琳,郭纯.算法歧视:嵌入路径、风险界分与规制构建研究[J].重庆行政,2023(4):59-62.
[13]蓝志勇.第四次工业革命与新公共治理原则[J].清华大学学报(哲学社会科学版),2021(6):195-204.
[14]马奔,叶紫蒙,杨悦兮.中国式现代化与第四次工业革命:风险和应对[J].山东大学学报(哲学社会科学版),2023(1):11-19.

[15]刘妍.数据主权的演进、挑战与层级治理路径[J].中国科技论坛,2023(6):142-152.
[16]李睿.Legitimacy:多义、本义及汉译[J].中国科技术语,2015(1):31-34.
[17]封颖,高芳,徐峰,等.科技政策与产业政策协同关系的再认识[J].中国科技论坛,2020(8):52-59.
[18]汤霞.数据安全与开放之间:数字贸易国际规则构建的中国方案[J].政治与法律,2021(12):26-38.
[19]蓝庆新.中国应对西方国家高技术封锁的历史经验[J].人民论坛,2019(16):28-30.
[20]人工智能 AI 发展可能受限,英伟达称先进的 GPU 受管制,对中国禁售[EB/OL].(2023-10-19)[2023-11-11].https://baijiahao.baidu.com/s?id=1780101878798036236&wfr=spider&for=pc.
[21]黄震,张夏明.中国监管科技的实践探索及其完善路径[J].陕西师范大学学报(哲学社会科学版),2023(4):79-91.
[22]周建军.美国反垄断政策的百年变迁:基于并购重组的考察[J].美国研究,2022(3):111-130.
[23]唐要家,王钰,唐春晖.数字经济、市场结构与创新绩效[J].中国工业经济,2022(10):62-80.
[24]杨雅涵.人工智能时代下算法不当应用的类型化侵害研究与差别化规制路径探索[J].产业科技创新,2022(1):79-82.
[25]王亦菲,韩凯峰.数字经济时代人工智能伦理风险及治理体系研究[J].信息通信技术与政策,2021(2):32-36.
[26]习近平谈治国理政:第 2 卷[M].北京:外交出版社,2017:535.
[27]尤霞光,盛小平.8 个国际组织科学数据开放共享政策的比较与特征分析[J].情报理论与实践,2017(12):40-45.
[28]金晶.欧盟的规则,全球的标准?数据跨境流动监管的"逐顶竞争"[J].中外法学,2023(1):46-65.
[29]王晓红,李娜.数字技术发展、产学研合作与企业创新能力:基于国家级大数据综合试验区的分析[J].科技管理研究,2022(17):1-8.
[30]周汉华.论平台经济反垄断与监管的二元分治[J].中国法学,2023(1):222-240.
[31]王锡锌.个人信息国家保护义务及展开[J].中国法学,2021(1):145-166.

A Panoramic Perspective and the Dimension of Rule of Law on the Secondary Risks of Digital Economy

Zhang Yuan

Abstract:The secondary risks of digital economy are theoretical and practical issues facing the development of digital economy in China, which should be addressed through scientific analysis and normative restrictions. In view of the complexity of the secondary risks of digital economy, it is appropriate to adopt the analysis framework of distinguishing subjects and realize the systematization of analysis. At the national level, the unregulated data utilization behavior in the whole process has caused the risk of data sovereignty; at the market level, the digital economic market that is free in appearance but is actually close to monopoly should be corrected; at the individual level, the digital economy has also led to the instability of individual rights due to cultural and social changes. By breaking down the issues, we can see that the national level data sovereignty risk is caused by the difficulty in balancing the development and security of the digital economy; the market level close to monopoly is caused by the current status of technological hegemony; the failure of many regular assumptions has made the complete regulation scheme of personal information vacuum, and the related negative impacts have also emerged. China should ensure the sustainable development of digital economy based on the rule of law strategy, reduce national security risks by seeking legal protection, and oppose hegemonic behavior; give play to the incentive role of law to connect with the market development law, integrate the rule of law into the market; appropriately "over-correct" to protect the basic rights of individuals, and form a culture, atmosphere and concept.

Key words:secondary risks of digital economy; digital sovereignty; technological hegemony; monopoly; basic rights

责任编辑:刘 一