Dispute Settlement 争议解决, 2026, 12(4), 1-9
Published Online April 2026 in Hans. https://www.hanspub.org/journal/ds
https://doi.org/10.12677/ds.2026.124094

Hans汉斯

人工智能数据垄断与数据安全保护的双重审视

梁志鹏

青岛科技大学法学院，山东 青岛

收稿日期：2026年2月23日；录用日期：2026年3月16日；发布日期：2026年3月25日

摘　要

在人工智能快速发展的背景下，数据作为重要资源的独占问题和安全保护受到广泛关注，数据独占不仅破坏市场公平竞争还打击创新积极性，同时严重危害数据安全体系。本研究详细分析人工智能领域数据独占的具体表现、形成原因和安全风险传递方式，并且说明数据安全保护遇到的多种困难，然后从法律改进、加强监督、建立共享平台、提升技术防护和加强国际合作等方面给出解决办法，努力建立有效管理框架来确保数字经济稳定发展。平台企业在数据独占形成过程中利用技术优势和算法不透明获取数据，这种独占方式不但阻碍数据自由流动反而加重数字差距。跨境数据流动管理不足和隐私计算技术落后是安全保护的主要难题，不过动态反垄断机制设计可能带来新的管理思路。

关键词

人工智能，数据垄断，数据安全保护，反垄断规制，数字经济

A Dual Perspective on Data Monopolization and Data Security Protection in Artificial Intelligence

Zhipeng Liang

Law School, Qingdao University of Science and Technology, Qingdao Shandong

Received: February 23, 2026; accepted: March 16, 2026; published: March 25, 2026

Abstract

Against the backdrop of the rapid development of artificial intelligence, the monopolization of data as a critical resource and the protection of data security have attracted widespread attention. Data monopolization not only undermines the fair competition of the market and dampens the enthusiasm for innovation, but also severely endangers the data security system. This study conducts an

文章引用: 梁志鹏. 人工智能数据垄断与数据安全保护的双重审视[J]. 争议解决, 2026, 12(4): 1-9.
DOI: 10.12677/ds.2026.124094

in-depth analysis of the specific manifestations, formative causes and transmission modes of security risks of data monopolization in the field of artificial intelligence, and expounds the various challenges faced in data security protection. It then proposes solutions from the aspects of legal improvement, strengthened supervision, establishment of sharing platforms, enhancement of technical protection and reinforcement of international cooperation, striving to construct an effective governance framework to ensure the steady development of the digital economy. Platform enterprises exploit technological advantages and algorithmic opacity to obtain data in the process of forming data monopolization, which not only hinders the free flow of data but also widens the digital divide. Inadequate governance of cross-border data flow and the backwardness of privacy computing technology are the major challenges for data security protection, yet the design of a dynamic anti-monopoly mechanism may bring forth new governance ideas.

Keywords

Artificial Intelligence, Data Monopolization, Data Security Protection, Anti-Monopoly Regulation, Digital Economy

1. 问题的提出

人工智能技术推动数字经济快速成长，数据作为关键资源不仅帮助优化算法还催生了新商业模式和经济热点，虽然数据集中化趋势带来垄断问题已经影响市场竞争并造成安全威胁，少数企业凭借数据收集和分析优势占据市场主导地位然后实施限制竞争等不当行为，比方说用户敏感信息过度集中在这些企业手中会大大增加泄露风险，2018 年 Facebook 事件中 8700 万用户数据被盗就暴露出这类安全问题。

数据垄断既体现在企业利用资源优势阻碍技术创新也表现为隐私保护机制失效导致权益受损，问题核心在于数据控制权过于集中与安全防护体系薄弱之间的矛盾[1]，数字经济生态中生产要素配置失衡不但压制市场活力而且直接危及公民个人信息安全，这就要求监管部门必须建立数据流通与风险防控的平衡机制[2]。

在数字经济发展过程中需要同时关注人工智能数据垄断和安全保护问题，研究数据垄断有助于改进反垄断法规并保持市场公平，推动创新经济发展，加强数据安全研究可以建立更好防护系统，保护用户利益并增强社会安全感，这种双重关注是应对数字经济挑战的必然要求[3]，促进人工智能技术健康发展的重要基础，通过一起解决数据垄断和安全体系建设问题，既能满足当前数字治理的紧急需要，为技术发展提供长期保障。

2. 人工智能数据垄断的内涵与表现形式

(一) 数据垄断的定义与特征

数字经济发展使得数据成为重要资源并改变企业竞争方式，同时影响市场格局且带来数据垄断问题，企业或组织通过掌握大量数据限制竞争并赚取高额利润，虽然数据垄断与传统垄断不同且具有自身特点，但是破坏市场公平并关系到经济和社会稳定，现在数据垄断依靠控制大量数据占据市场优势，这种垄断形式不但隐蔽性强而且扩展速度快，运作方式不仅降低市场效率还涉及社会资源分配不公平。

关于数据垄断的特征，主要是以下两点：第一、数据具有非竞争性和部分排他性。数据具有非排他

性，多个主体可同时使用且不会因使用而损耗，能大幅提升数据利用价值，助力企业扩大市场。同时，数据又具备部分排他性，可通过加密、权限管控等手段限制他人访问，帮助企业维持数据优势与市场地位[4]。两种特性结合，使数据垄断平台能低成本扩张，凭借海量用户数据形成核心竞争力，不断巩固市场壁垒，让竞争对手难以抗衡。第二、数据垄断往往呈现出隐蔽性，这给监管和防范带来了极大的挑战。企业在内部完成数据采集、存储、分析，常通过模糊用户协议、后台静默获取等隐性手段收集用户信息，外部难以知晓[5]。数据垄断企业还利用算法实施价格歧视、差异化定价等行为，算法复杂且被视为商业机密，传统监管难以识别与有效监管。

(二) 人工智能数据垄断的具体表现形式

1) 数据封锁与拒绝交易是数据垄断的常见手段。

掌握海量数据的企业为维持竞争优势，常通过信息屏蔽限制甚至拒绝数据共享。大型地图服务商则掌握道路、地形、路况等关键地理数据，却不愿向新兴地图开发商开放接口，导致新企业难以获取充足基础数据，产品易出现路径不准、定位缺失等问题，无法与头部企业竞争。信息屏蔽严重阻碍数据流通与共享，制约产业技术创新发展。数据如同数字时代的“石油”，对其封锁等同于垄断核心资源，使中小市场主体缺乏发展动力，破坏市场公平竞争环境。

2) 滥用市场支配地位是人工智能数据垄断的突出表现。

数据垄断者往往利用自己的数据优势，采取各种限制竞争的手段。差异化对待就是一种典型的表现形式，即企业依据客户的消费习惯、购买力、使用频率等信息，向不同的用户提供不同的交易条件[6]。在线旅行平台利用大数据分析用户出行偏好与消费能力，对高频、高消费商旅用户上调酒店价格、减少优惠，对价格敏感的年轻用户则给予优惠，实施差别定价。这种区别对待违背公平交易原则，损害部分消费者权益，扰乱市场公平竞争秩序。此类数据驱动的差别定价并非基于成本差异，而是企业谋取高额利润的垄断手段，导致消费者无法以合理价格进行消费选择。

同时，搭售也是数据垄断企业滥用市场优势的常见手段。部分企业将优势信息产品与其他产品捆绑销售，强制用户购买。例如办公软件行业，一些企业在销售电子表格、文档编辑等核心数据处理软件时，强制用户搭配购买绘图、项目管理等非必需辅助软件，用户需额外付费，增加了使用成本。这种捆绑销售极大地限制了专注单一功能产品企业的发展，用户受捆绑模式影响倾向“一站式”采购，导致中小软件厂商难以获得用户，逐渐丧失市场竞争力，破坏了市场公平竞争的环境。

3) 数据驱动的并购与集中加剧了数据垄断的趋势。

在目前的技术产业中，越来越多的企业通过并购获取海量数据，以此扩大数据规模、抢占更大市场份额，最终形成更强的竞争优势。很多大的科技企业都在不断地进行并购，他们的目标不是为了获得他们的技术和业务，而是因为他们的数据[7]。这类新兴企业因其自身的特点与定位，拥有特定的用户群，并已积累了丰富的数据，如特定兴趣人群的社交关系、特定区域的用户行为等。此次并购之后，该数据将被纳入超大型平台企业的数据库，从而使超大型平台企业在社会网络中的位置更加稳固。

数据驱动型企业合并会带来诸多不利影响。它会快速提高行业集中度，减少市场竞争主体。初创企业本可凭借创新模式与技术打破现有格局、推动产业创新，但被大企业并购后，创新动力明显减弱。大企业并购后更注重整合数据以巩固自身地位，初创企业的创新项目易被搁置、团队被解散，削弱行业整体创新活力。从数据垄断角度看，数据高度集中会加剧垄断风险，其他企业尤其是新兴企业难以获取数据，无法与数据垄断企业竞争，进而破坏产业创新生态，不利于行业健康发展。

(三) 人工智能时代数据垄断与合法竞争的判断标准

结合我国《反垄断法》《平台经济领域反垄断指南》《数据安全法》《个人信息保护法》等现行法律

法规，立足人工智能技术的发展特征与数据资源的属性，构建人工智能时代数据垄断与合法竞争的具体判断标准主要是以下三个方面：第一是相关市场界定：采用“商品 + 数据 + 技术 + 地域”多元标准，分别依据 AI 产品功能、数据类型与获取难度、技术壁垒与替代性、服务覆盖范围及数据跨域特征，界定对应相关市场，其中数据相关市场为核心。第二是市场支配地位认定：以数据资源为核心指标，结合技术能力、市场份额、市场进入壁垒综合判断。企业掌握不可替代的核心数据，且技术领先、市场份额超50%、相关市场壁垒高，可认定其具有支配地位。第三是垄断行为判定：核心是看行为的反竞争性与无正当理由性。具有支配地位的企业，无正当理由实施数据封锁、非成本导向的差异化定价、强制性搭售，或开展以数据为核心且排除竞争的未审并购，均构成垄断；基于数据安全、成本差异等合理理由的行为，属合法竞争。

3. 人工智能数据垄断的形成原因

(一) 技术壁垒与网络效应

数据垄断企业拥有雄厚的资本、人力资源等资源，在技术研究上进行了大量投资，并对其进行了深入研究。例如，基于深度学习的方法，企业可以通过对大数据的分析，从中发现有价值的信息，进而对产品和服务进行优化。而新入行的企业，由于没有足够的经验，难以在短期内将其掌握。比如，在语音识别、影像识别等方面，业界龙头企业经过长期的研究与开发，已在精度与表现上遥遥领先于同行。即使新企业将大量的资源投入到研发之中，短时间内也很难与之相匹配，这就导致了新进入者在市场竞争中的不利地位，很难将已有的大型数字平台企业的市场模式给打破[8]。

网络效应也是信息垄断形成的重要原因。用户规模扩大带动平台数据呈指数增长，平台可依托用户行为数据优化推荐算法、提升服务质量。以短视频平台为例，头部平台能采集海量行为数据优化服务，而新兴平台因用户与数据不足，推荐效果差、用户体验不佳，难以吸引用户与积累数据，陷入恶性循环。这种正向反馈机制不断巩固头部平台的市场地位，形成赢者通吃的效应，最终催生信息垄断。

(二) 数据的规模经济与范围经济

这些数据有明显的规模效益。当数据规模越来越大时，在其价值不断提高的同时，每一单元数据的处理代价也将越来越低[9]。大型电商平台积累了大量的用户消费数据，在此基础上，平台能够更加精确地掌握用户的消费偏好、购买频率等情况，实现精准营销，提升营销效率，减少营销费用。同时，通过对这些数据的分析，对供应链进行优化，从而达到减少库存费用、提升运作效率的目的。与此形成鲜明对比的是，小规模的电商平台因其数据规模受限，不能对其进行深度挖掘，很难做到准确的营销与有效的供应链管理，从而在市场上处于不利地位。

数据的规模经济效应也促使了信息垄断的出现。企业可利用同一数据开展多元业务，挖掘数据价值、节约成本、提升收益。例如金融科技公司可借助用户交易数据评估资信、提供信用服务，辅助银行进行风控管理，并通过合作拓展商机。但中小企业因数据储量不足、技术能力有限，难以实现数据多元化利用，在市场竞争中处于弱势边缘地位。

(三) 法律法规的滞后性

面对飞速发展的数字经济，我国现行的法律、法规已经出现了严重的滞后，很难有效地解决“人工智能”所带来的“数据垄断”问题。传统的反垄断法对相关市场的定义多以商品或服务的物理属性和地域范围为依据，而随着数字经济的发展，数据的跨行业、跨地域的流动，相关市场的定义也变得异常复杂。例如，传统的反垄断法律仅仅从搜索服务的角度对其进行定义，而现实生活中，搜索引擎企业通过搜集用户的搜索信息，把自己的业务扩展到了广告、电商等多个行业。由于互联网上各种数据驱动的服务之间存在着一定的关联性，因此，目前的反垄断法很难对其进行有效的规制[10]。

我国现行立法尚未对数据所有权、使用、共享等问题作出明确的规定。企业常常通过格式条款获取用户信息，用户难以掌控自身信息使用与共享。因法律依据缺失，个人信息被过度开发利用、权益易受侵害；数据共享缺乏统一标准与管理，易引发泄露和滥用。立法空白给企业不正当数据竞争留下漏洞，也为数据垄断提供了条件。

(四) 典型案例分析

1) 案例一：深圳市腾讯计算机系统有限公司等诉浙江搜道网络技术有限公司等不正当竞争纠纷案

腾讯公司运营的微信平台，凭借多年深耕社交领域的积累，汇聚了海量用户账号、好友关系链、用户操作行为等原始数据，通过持续的技术研发、资金投入和管理维护，将分散的单一数据整合形成具有商业价值和竞争优势的数据资源整体，这一数据资源也是微信平台维持用户粘性、实现商业价值的核心基础。而浙江搜道公司、杭州聚客通公司开发的“聚客通群控软件”，通过外挂技术非法嵌套于微信平台运行，在未经腾讯公司授权、也未获得用户明确同意的情况下，大量抓取微信用户相关数据，用于商业营销活动，严重干扰微信平台的正常运营[1]。腾讯公司为维护自身合法权益，诉至法院请求认定二被告构成不正当竞争，法院一审依法认定被告行为构成不正当竞争，判决其停止侵权并赔偿 260 万元，二审法院审理后裁定维持原判。该案中，法院确立了数据权属二元界定规则，明确用户对单一原始数据享有核心权利，平台对聚合后的整体数据享有合法的竞争性利益，这一认定既契合《反不正当竞争法》公平诚信、诚实信用的基本原则，又有效填补了当前数据权属界定的司法空白。同时，法院认定被告的非法抓取行为违反“合法、适度、用户同意”的数据使用原则，危及用户信息安全，明确否定其“技术中立”的抗辩理由，精准界定其不正当竞争行为的性质，为同类数据竞争案件提供了重要司法参照。此外，被告的寄生式竞争行为未付出数据采集、管理的必要成本，却掠夺腾讯平台的竞争优势，破坏市场正常的投入–回报机制，抑制平台优化数据服务的创新动力，降低行业整体竞争效率；其非法抓取行为还导致数据流向低效使用场景，无法发挥数据的协同价值，扭曲资源配置并造成社会资源浪费；同时促使腾讯进一步强化反爬技术、收紧数据开放权限，抬高行业数据流通门槛，最终形成“非法抓取–强化保护–壁垒固化”的恶性循环。

2) 案例二：北京链某房地产经纪有限公司等诉上海幻某信息科技有限公司等不正当竞争纠纷案

链某方投入大量人力、物力和技术资源，构建起包含 2.26 亿套房屋信息的“楼盘字典”数据库，为保护自身数据权益，还采取了水印、反爬取等一系列技术和管理措施。而上海幻某公司、北京同某公司运营的“开某宝”产品，通过“房源读取”“批量采集”等功能，在未经链某方及贝某找房网授权的情况下，非法抓取平台房源数据，自动去除原有水印并替换经纪人联系方式，供非贝某系经纪人发布虚假房源以实现引流目的，该产品累计用户已超 23 万名。为此，链某方诉至法院，请求判令二被告赔偿经济损失 528 万元，法院经审理认定被告行为构成不正当竞争，判决赔偿 178 万元，二审法院裁定维持原判[2]。本案判决中法院明确了商业数据的保护标准，认定“楼盘字典”数据符合集合性、合法性、价值性、管理性特征，属于《反不正当竞争法》保护的商业数据，认可链某方通过合法采集、专业拍摄、脱敏处理等投入形成的竞争优势应受法律保护，厘清了商业数据的司法保护边界；同时界定被告行为本质是数据垄断的隐性表现，其掠夺性使用核心数据、打破合理数据控制的行为，既割裂数据与原始权利人的关联，又催生虚假房源，损害消费者权益与市场竞争秩序；在责任裁量上，法院综合被告用户规模、行为持续时间、主观过错等因素酌定赔偿，体现“损害程度与责任相匹配”原则，对遏制数据滥用、防范数据垄断具有震慑作用。并且被告的非法抓取行为扭曲了市场成本收益结构，其边际成本仅为服务器维护与软件运

[1]杭州铁路运输法院。(2019)浙 8601 民初 1987 号民事判决书[Z]。杭州：杭州铁路运输法院，2020-06-02。
[2]上海知识产权法院。(2024)沪 73 民终 225 号民事判决书[Z]。上海：上海知识产权法院，2025-04-24。

营成本，却能通过用户服务费获得高额边际收益，这种失衡激励了不正当竞争；同时，被告的免费掠夺使链某方的巨额投入无法获得合理回报，削弱行业创新动力，挤压中小房产信息平台的创新空间，不利于行业技术升级与多元化发展；此外，虚假房源泛滥增加消费者信息辨别成本，链某方升级反爬技术提高数据维护成本，行业信任度下降推高交易谈判与风险成本，整体增加社会交易成本，违背数字经济“降本增效”的核心价值。

4. 人工智能数据垄断对数据安全保护的影响

(一) 数据滥用与隐私侵犯

数据垄断公司通常拥有大量的用户隐私，包括用户的基本信息、消费习惯和浏览记录等。受经济利益的驱动，很多企业对其进行了不当利用和分享，从而导致了用户个人信息的侵害。为了获得更大的经济效益，有些公司会把自己的用户信息卖给第三方广告主进行精准的广告投放。用户在使用有关的程序和服务时，只是出于对平台的基本功能的需要，并没有同意为其它商业用途而使用这些数据。但是，一些数据垄断公司在用户不知道的时候，就已经将这些数据进行了秘密的共享，从而造成了用户的隐私泄漏[11]。更重要的是，数据垄断企业凭借技术优势深挖分析用户数据，可从中获取健康、财务、心理等隐私，致用户的个人信息权益严重受损。

(二) 数据泄露风险的增加

由于数据垄断公司拥有海量的数据，因此数据泄漏事故的发生将会造成比一般企业更大的损失。数据泄露不但会造成使用者的个人信息泄露和滥用，给使用者造成巨大的经济损失，而且还会引起信任危机，给产业带来巨大的影响。2017 年，美国一家名叫 Equifax 的征信公司出现了一起数据泄漏案，涉及到了 1470 万用户的隐私，这些隐私包括姓名、社保号、生日等。一旦用户的个人信息被窃取，那么他们将会面临被盗用、被盗刷等危险，很多人因此而蒙受巨大的经济损失。为了维持自身的垄断地位，数据垄断公司常常过分重视数据的隐私性，在数据泄漏防范等表层工作中投入更多的资源，而忽略了对数据安全保障的实质性投入与有效管理。在数据存储、传输、使用等环节，由于缺少有效的安全手段和风险评价机制，造成了数据泄漏的风险增大。与此同时，数据垄断企业因其内部管理繁琐，对员工权限的管控不严，极易发生因员工违规操作而造成的数据泄漏。

(三) 阻碍数据安全技术的创新

此外，资料垄断也会妨碍资料安全科技革新。为了维持自己在数据空间中的支配地位，垄断公司通常采取禁运、限制等手段，不愿与其它公司共享或共同研发有关的技术。一些大的科技企业在数据保密方面采用了一系列的专利保护措施，形成了一道专利壁垒，以此来限制其它公司的应用[12]。其他的企业因担心侵权，不敢深入开展数据安全技术研发，产业内技术交流与合作受阻，难以形成协同创新环境。企业对数据安全投入不足、创新动力缺乏，中小企业更是忙于生存，无力投入财力人力。这导致行业数据安全技术发展滞后，难以应对日益增长的数据规模与安全威胁。在人工智能发展下，新型黑客攻击与恶意软件不断出现，安全技术无法有效应对，数据安全隐患愈发严重。

5. 数据安全保护面临的挑战

(一) 数据权属界定模糊

在“数字经济”背景下，数据的生成与利用由用户、数据收集者、数据处理者等多方参与，而当前对数据所有权的界定尚不明确[13]。以社会化媒体为例，用户通过其发布内容和交互形成海量的数据。从使用者的观点来看，这些资料是他们的个人表现与社会行为的纪录，应该拥有某种程度的控制权；但是，作为数据收集者和处理者的平台，在对数据进行存储、管理和使用的过程中，往往会对数据提出相应的

要求。比如前文所说的杭州互联网法院审理的腾讯诉浙江搜道网络不正当竞争案，微信用户的账号数据、好友关系链数据等原始数据由用户生成，但腾讯作为平台投入大量资源完成数据的聚合与管理，双方就数据权益归属产生激烈争议——被告主张数据归用户所有，腾讯无权主张权利，而腾讯则主张对数据资源整体享有权益，该案的核心争议正是数据权属界定模糊的直接体现。这样的所有权不清晰，导致了在数据的采集、使用和共享的过程中，双方的权利和责任都不清楚，很有可能会引起数据争议和安全方面的问题。正如该案中，被告的“聚客通群控软件”擅自抓取微信数据，既涉及未经不知情用户同意使用其数据的权益侵害，又引发平台数据经营生态受损的竞争纠纷，充分印证了权属模糊会滋生数据滥用、侵权竞争等连锁问题。在特定的应用中，用户通过应用授权获取个人信息时，权属与使用情况难以有效监管。部分软件在用户不知情时过度采集信息用于商业牟利，侵害用户权益。数据处理者受利益驱动忽视安全防护，进一步加剧数据安全风险。

(二) 技术漏洞与攻击威胁

随着人工智能的普及，数据面临着更多的技术缺陷与安全攻击。AI 系统存在技术漏洞，易被黑客利用窃取、篡改数据；机器学习若使用污染数据训练，会降低模型准确性与可信度。安全机制漏洞可能被突破，导致重要数据泄露。恶意软件、勒索病毒、间谍软件等同样威胁数据安全，造成数据丢失、损毁或被窃取。此外，AI 还存在算法偏见与数据中毒风险，前者引发不公，后者破坏数据真实性。2016 年美国某知名银行 AI 系统遭入侵，用户信息泄露并造成巨额经济损失，凸显技术缺陷与网络攻击对数据安全的严重危害。

(三) 跨国数据流动的监管难题

经济全球化背景下，数据跨境流动日趋频繁，各国及区域间数据安全保障标准及相关法律规定不尽相同，使得跨境数据流监管面临严峻挑战。部分国家或地区在数据安全方面采取了更为严厉的措施，如数据存储本地化、跨国界传输等；而其他的国家或地区，对资料的跨国界流动的限制比较宽松。这一差别，使企业在跨国界的数据流通过程中，面临着高的合规成本和高度的管理不确定性[14]。由于跨国企业在全球经营中需跨境传输数据，部分企业为降低成本，将数据存放在监管宽松地区，易引发泄露与滥用风险。跨境数据流动关乎着国家的数据安全，涉及国家机密、公民敏感信息，一旦失控将危害国家安全。如何在保障安全与隐私的前提下实现数据自由流通、促进全球经济合作，已成为各国共同课题。当前国际缺乏统一监管标准与协作机制，监管分散，难以有效管控跨境数据，进一步加剧安全挑战。

6. 应对人工智能数据垄断与加强数据安全保护的策略

(一) 完善反垄断法律体系与监管执法

法治完善与监管强化是治理人工智能数据垄断、保障数据安全的根本保障。一方面需补齐法律制度空白，结合人工智能技术特征修订《反垄断法》，增设数据垄断专门条款，明确界定标准、认定程序与法律责任，细化平台经济反垄断指南并制定生成式 AI、数据处理等细分领域专项指引，同时完善《数据安全法》《个人信息保护法》，明确数据权属与各主体权责，制定大模型训练数据使用规范，平衡版权保护与技术创新[15]。另一方面要加大违法惩戒力度，将罚款与企业违法所得、营业额挂钩，对情节严重者采取停业、拆分等处罚，建立失信惩戒机制限制违法企业市场准入与融资。此外，整合监管资源设立专门数字经济监管机构，构建“技术监管 + 人工监管”体系，借助可解释 AI、大数据等技术穿透算法黑箱、搭建数据安全监测预警体系，实现监管的专业化、精细化与协同化。

(二) 构建技术与机制体系

技术创新与机制构建是打破数据垄断、强化数据安全的核心支撑，需从数据共享、算法监管、技术防护三方面发力。一是建立数据分类分级共享机制，按类型将数据分为公共、企业、个人数据，按敏感

程度划分为非敏感、一般敏感、核心敏感数据，制定差异化共享规则，公共数据应开尽开、企业数据安全流通、个人数据授权使用，同时搭建“政府开放 + 行业交易 + 企业共享”三级平台体系，依托区块链实现数据交易可追溯。二是实施算法全生命周期监管，依托可解释 AI、全生命周期追溯、生成式 AI 专项审核技术破解算法黑箱，按安全风险将算法分为三级实施差异化审查，建立算法透明度报告制度，培育第三方审查机构保障监管专业性。三是打造一体化数据安全技术体系，政府设立专项基金支持加密、隐私计算、数据脱敏等核心技术研发，推动产学研协同创新，加快技术产业化落地并融入企业全流程运营，由国家标准化管理委员会牵头制定数据安全技术国标与行标，推动标准国际化。

(三) 深化国际协同治理，平衡数据流动与安全保护

加强国际间的合作与协作，通过积极地参与到国际数据治理中来，我们才能更好地保护自己的利益，更好地保护自己的数据安全。这就要求我们要建立跨国监管协作机制，与主要经济体搭建信息交流、执法合作与风险联防联控体系，设立跨国数据安全事件应急处置机制，联合开展泄露、网络攻击等事件的调查与处置。最后推动国际技术交流合作，与各国开展数据安全、人工智能技术的联合研发、学术交流与技术培训，共享研发成果与经验，鼓励我国数据安全企业“走出去”参与国际市场竞争，推动我国技术的国际化应用，实现全球范围内数据流动与安全保护的平衡发展。

7. 结语

随着人工智能技术的快速发展，数据隐私保护已成为我国重要课题。数据垄断严重扰乱市场竞争秩序，抑制技术创新，危害数据安全。垄断企业凭借数据优势实施数据封锁、滥用市场地位，损害其他企业利益；基于数据的并购行为，削弱创业企业创新动力与能力。同时，数据垄断加剧安全隐患，企业不当使用个人信息，一旦泄露将造成重大损失。

当前数据安全保障存在着数据产权界定不清，采集、使用、共享等环节纠纷与风险频发等问题，用户合法权益难以得到保障。人工智能系统漏洞、恶意程序攻击、算法安全缺陷等，则进一步威胁着数据安全。各国数据保护标准不一，跨境数据流动监管复杂，也加大了安全管理难度。对此，需要明确数据相关界定与认定规则，提高违法处罚力度；强化数据监管与执法，设立专门监管机构，构建技术与机制体系，深化国际合作；建立安全规范的数据共享机制，推动数据合法高效利用。

随着人工智能发展，数据垄断与安全问题不断演变。未来需持续深化研究，完善政策制度，强化技术创新与国际协同，切实维护国家数据安全，保障数字经济健康可持续发展。

参考文献

[1] 刘妍, 陈天雨, 陈烨, 等. 互联网平台数据垄断主要表现及治理路径[J]. 情报理论与实践, 2023(11): 52-59.

[2] 王德正. 人工智能背景下隐私数据侵权责任的认定困境[J]. 法治论坛, 2023(4): 35-53.

[3] 曾田. 人工智能时代内容数据集中反垄断风险与公私合作治理[J]. 中国出版, 2024(15): 46-52.

[4] 曹胜亮, 张晓萌. 人工智能时代数据竞争的法律规制[J]. 学习与实践, 2019(10): 83-91.

[5] 李勇坚, 张海汝. 数字平台行为垄断与反垄断研究[J]. 中国社会科学院大学学报, 2023(5): 41-51.

[6] 顾尧舜. 数据垄断场景下滥用市场支配地位认定标准的完善[J]. 天府新论, 2024(6): 1-11.

[7] 贺惠章, 李锋森. 数字经济新型垄断: 成因探析、典型形式及法律规制——兼论金融科技风险防控[J]. 金融理论与实践, 2023(1): 25-34.

[8] 丁国峰. 大数据运用视角下互联网反垄断规制的完善进路[J]. 商业经济与管理, 2023(10): 79-89.

[9] 程华, 武玥璠, 李三希. 数据交易与数据垄断: 基于个性化定价视角[J]. 世界经济, 2023(3): 161-178.

[10] 胡晓红. 反垄断法视域下我国平台经济领域“守门人”义务之构造[J]. 学海, 2023(2): 164-172.

[11] 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[J]. 中国流通经济, 2020(5): 121-128.

[12] 孙海涛, 周奇锜. 平台数据垄断的监管困境与共享机制探析[J]. 江苏社会科学, 2023(3): 131-139.

[13] 闫夏秋, 孙瑜. 开放平台数据共享的制度困境与法律应对[J]. 西南金融, 2023(3): 96-108.

[14] 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.

[15] 刘奕麟. 论大数据商业模式反垄断规制的困境与出路——以滥用市场支配地位为研究视角[J]. 大连理工大学学报(社会科学版), 2024(3): 80-86.