

数字经济下的数据隐私保护与治理探讨

温家祺

中国传媒大学, 中国·北京 100024

【摘要】目前数字经济已跃升为全球经济增长的新动力。在此浪潮下,数据作为核心生产要素,其价值的深度挖掘与有效利用,对产业升级、资源配置优化及社会治理效率提升发挥着至关重要的作用,不可或缺。基于此,文章结合数字经济概念及治理情况,分析数据在数字经济中的作用,从多方面入手论述数据隐私保护及治理措施。

【关键词】数字经济;数据隐私保护;治理

引言:

随着大数据、云技术、人工智能的广泛运用,数据的收集、储藏、解析及运用愈发便捷,为各行业开辟了前所未有的发展契机。然而,数据量的激增与广泛流通,也加大了数据隐私外泄的风险。数据隐私保护不仅涉及个人权益的保障,更是构筑数字社会信任基石的关键。为应对此次挑战,国际社会和各国政府正强化数据隐私保护法规,企业亦积极探索技术创新,以增强数据安全防护能力。不过,数据隐私的保护与治理非一朝一夕之功,需统筹技术进步、法律约束、行业自律、公众教育等多重因素,构建协同共治的健康生态。

一、数字经济概述

数字经济是数据资源作为关键要素的经济模式,其核心在于依托现代信息网络,并通过信息通信技术的综合集成,促进所有要素的数字化转型。此变迁构成数字经济发展的核心驱动力,优化经济在效率与公平之间的平衡。于数字经济体系内,数据扮演着如同传统经济中石油般的角色,是不可或缺的生产要素。现代信息网络充当数据流通与处理的快速通道,而信息通信技术的综合应用则如同高效引擎,驱动整个经济系统运转,旨在实现全面的数字化要素转型^[1]。

二、数字经济下的数据隐私保护与治理探讨

(一) 现状

在数字经济迅猛崛起的时代背景下,数据作为核心生产要素,对经济社会发展的驱动力日益显著。大数据、云计算、人工智能等技术的广泛渗透,极大增强了数据的采集、存储、处理及分析效能,为各行业开辟了前所未有的发展空间。但随之而来的是数据隐私保护挑战的日益突出,成为制约数字经济持续健康发展的重大障碍。目前,数据泄露、滥用事件频繁发生,对个人隐私构成严重威胁,并影响社会稳定大局。此外,数据治理机制的不健全

还引发了数据权属模糊、流通梗阻等问题,制约了数据价值的深度挖掘与利用。因此,强化数据隐私保护与治理体系,构建一个既安全又高效、秩序井然的数据生态环境,已成为数字经济时代下亟需攻克的重要议题。

(二) 趋势

展望未来,数字经济在应对数据隐私保护与治理的挑战时,将展现以下发展趋势。首要的是,数据隐私保护法律体系将日趋完备,明晰数据所有权、使用准则及追责机制,为数据隐私筑起坚实的法律屏障。同时,技术创新将为数据隐私保护注入新动力,诸如加密技术、数据脱敏等手段的应用,将有效遏制数据泄露的风险。其次,数据治理架构将更趋完善,覆盖从收集、存储、处理到流通的全链条管理,确保数据在遵循法规的前提下高效流通,实现价值最优化。再者,国际合作与交流在数据隐私保护与治理中的作用将愈发凸显,通过构建跨国数据治理框架与合作平台,协同应对跨境数据流带来的复杂挑战。一个由政府、企业及社会各界共治的数据隐私保护与治理体系将逐步形成,促进数字经济在维护个人隐私与社会稳定的前提下,迈向可持续的发展道路。

三、数据在数字经济中的作用

(一) 资源基础

数字经济的基石乃数据,其作为核心资源,对构建数字世界至关重要。在数字经济框架下,数据扮演着如同土地、资本等传统生产要素的角色,成为经济活动不可或缺的基础。数据的庞大体量、多样类型及快速流通特性,为数字经济注入了丰富的素材与宽广的创新领域。企业通过数据的采集、处理与分析,能准确把握市场动态,优化资源分配,提升生产效率,进而在竞争激烈的市场环境中取得优势。数据资源的高效开发与运用,已成为评估国家或地区数字经济发展程度的关键标准。

(二) 创新驱动

数字经济时代下，数据成为技术创新与商业模式革新不可或缺的支撑。它为研发工作供给丰富素材与灵感源泉，推动企业研发更贴合市场需求的产品及服务。借助数据分析技术，企业能精确捕捉消费者需求，实施个性化定制与精确定位营销，拓展新市场领域^[2]。此外，数据驱动跨界融合与协同创新，各行业、各领域数据的交汇融通，孕育出众多新兴业态与商业模式，为数字经济的蓬勃兴盛注入了强劲动力。

（三）决策支持

数字经济环境下，企业决策场景日趋复杂多变，传统依赖经验与直觉的决策模式已难以满足现代管理要求。数据分析技术的应用，为企业决策提供了科学精准的支撑。通过深度挖掘历史数据及动态监测实时数据，企业能精准捕捉市场动态，预测未来走向，进而制定更为合理有效的战略方案。数据驱动的决策模式，既提升了决策效率与质量，又降低了决策风险，为企业稳定发展奠定了坚实基础。

（四）价值增值

在数字经济领域，数据价值不仅体现于直接作为信息载体的功能，更在于经加工、处理及分析后，能挖掘出数据背后隐藏的深层信息与知识，并转化为实际经济效益。企业通过深度发掘与智能利用数据，能发掘新增长机遇，优化业务流程，提升产品及服务的质量与效率，达成价值最大化目标。此外，数据还能作为资产进行交易流通，直接为数据持有者带来经济回报。数据所具备的增值属性，使其在数字经济中地位日益凸显，成为驱动经济社会高质量发展的核心要素。

四、数字经济下的数据隐私保护与治理路径

（一）强化数据分类分级，细化隐私保护标准

当前数字化浪潮汹涌，数据量呈爆炸性增长，已成为核心生产要素。为构建坚实的数据安全屏障并实现隐私保护的精细化，加强数据分类与分级工作至关重要。企业与机构应持科学严谨之态，全面盘点其数据资源^[3]。以金融业为例，该领域业务广泛，涉及储蓄、贷款、投资等多维度，数据复杂多样。首先，依据数据敏感度精确划分：用户身份信息、账户密码及大额交易记录等直接关联资金安全与隐私的数据，应归为绝密级；交易历史、投资偏好等兼具商业价值与隐私特性的数据，划分为机密级；而通用信息、产品介绍等则设为内部公开级。随后，结合业务范畴，对信贷审批、风险评估等各流程特有数据进行分类管理，确保数据体系条理清晰，各岗位人员依据需求与规定访问相应级别数据。同时，细化隐私保护措施刻不容缓。需从法律合规角度出发，深入解析《中华人民共和国个人

信息保护法》《中华人民共和国数据安全法》及行业特定规范，提炼关键要求，制定符合企业实际的数据隐私保护规范。对于大型互联网平台，于用户注册之初即应透明告知信息收集范围、用途及保存期限，确保隐私条款简明易懂；在数据存储环节，严格控制访问权限，实施多因素认证，仅限特定岗位人员接触敏感数据；在数据共享与传输过程中，签订严密的数据保护协议，加密传输路径，全程追踪数据流动，确保接收方遵循同等严格的隐私标准，避免数据外流引发的隐私泄露风险。

（二）实施数据脱敏技术，降低隐私泄露风险

随着数据应用场景的日益丰富，数据在流动、解析与共享过程中，始终面临隐私泄露这一“悬顶之剑”的严峻挑战。高效实施数据脱敏技术，犹如为数据穿戴上一层“隐形盔甲”，成为化解此风险的关键策略。以医疗健康领域为例，医疗机构积累了庞大的病历资料，既包含患者的详细病情、基因信息、治疗历程等高度敏感内容，又承载着医学研究、疾病统计及医保核销等重大社会使命。在科研活动中，数据脱敏技术发挥着重要作用。对于结构化数据，可采用替换、截断、重排等手段，将患者姓名、身份证号等直接标识替换为匿名编码，对住址信息模糊至区县层面，对出生日期进行适度偏移，既保留了疾病特征、检验结果等医学分析所需的关键信息，又有效隐匿了个人身份隐私；针对非结构化数据，如病历描述、影像报告，则利用自然语言处理技术识别并模糊处理隐私词汇。经脱敏处理的数据，可安全输入大数据分析模型，助力医学研究者探索疾病关联、预测流行趋势，而无惧隐私泄露风险。再者，在微政务数据共享中，各部门为提升行政效能、优化公共服务，需频繁交换数据。在此过程中，动态脱敏技术显得尤为重要。例如，基层工作人员在审核社保信息以辅助民政救助决策时，系统会根据其权限，在数据访问瞬间对关键隐私字段进行即时脱敏处理，如部分隐藏身份证号、将家庭收入精确到区间范围，既确保了基层工作的高效进行，又严格守护了民众隐私边界。技术层面，应不断引入先进的加密算法、差分隐私技术等，以优化脱敏效果；同时，定期评估脱敏后数据样本的可用性与隐私保护水平，迭代更新脱敏规则，使数据脱敏成为抵御隐私泄露风险的坚实防线，为数据价值的释放保驾护航。

（三）构建数据跨境流动规则，保障国际隐私安全

鉴于全球数据流动的错综复杂，单一国家的数据保护法规已难以有效应对跨境数据交换中的隐私风险。因此，推动国际共识的形成，构建多边数据保护体系显得尤为迫切，诸如推进《数据保护公约》等国际协议的磋商与签

订,旨在为全球数据流通确立统一的隐私保护基准。在此基础上,应详细制定跨境数据流动的管理细则,涵盖数据出境的审批机制、跨境传输的安全协议以及数据接收国的保护责任等,确保数据跨境传输的每一步均置于严格保护之下。例如,可参考欧盟《通用数据保护条例》(GDPR)的做法,设立数据保护官(DPO)职位,全面负责监督数据跨境流动,确保其合法性。同时,强化国际执法协作,构建跨境数据泄露的应急响应机制,对违法行为实施联合惩戒,以形成强有力的国际威慑效应^[4]。此外,还需关注发展中国家在数据跨境流动中的特殊诉求,通过提供技术支持、能力建设等措施,助力其提升数据保护水平,促进全球数据流动的平衡与可持续发展。

(四) 推广隐私计算应用,实现数据价值与保护双赢

隐私计算,作为一种新兴的数据处理技术,通过精巧的算法设计,确保数据在运算、分析环节中原始信息不被泄露,为数据的共享与利用开辟了全新途径。首要任务是加大对隐私计算技术的研发投入力度,推动高校、科研机构与企业间的协同创新,集中攻克同态加密、安全多方计算、差分隐私等核心技术难题,以期提升隐私计算的效能与效率。以金融业为例,借助隐私计算技术,银行能够在保障客户敏感信息安全的前提下,与其他金融实体共享信用评估模型,从而显著提升信贷审批的精准度与效率。其次,政府应出台一系列激励措施,包括设立专项扶持基金、提供税收减免等,以鼓励企业积极采纳隐私计算技术进行数据处理与共享,有效降低隐私泄露的风险。与此同时,加强隐私计算技术的标准化工作,制定统一的技术规范与评估准则,促进技术间的互操作性和兼容性,为隐私计算技术的广泛普及奠定坚实基础。此外,还需着力加强公众教育与技能培训,提升社会各界对隐私计算技术的认识水平与信任度,从而构建一个健康、积极的技术应用生态环境。

(五) 健全数据监管体系,加大违法惩处力度

当前,数据泄露与滥用事件频发,其根源多在于监管不足与违法成本低。因此,首要之举是健全法律法规框架,清晰界定数据收集、存储、处理、传输等各环节的法律界限,为数据处理活动提供明确的法律指引。例如,可参考欧盟《通用数据保护条例》(GDPR)的严苛条款,对违反数据保护规定的企业施以重罚,以此形成对潜在违法行为的强大震慑。同时,构建跨部门协同监管体系,整合网信办、公安、市场监管等多方资源,形成监管合力,确保对数据全链条的有效监管。此外,还需深化国际合作,联手打击跨境数据犯罪,组建国际数据保护合作机制,保障数据在全球范围内的合法流动。上述举措不仅能显著提升监

管效率,还能有效遏制数据违法行为,切实维护个人与企业的数据隐私权益^[5]。

(六) 提升公众数据素养,增强隐私自我保护能力

数字时代下,每个人都是数据的创造者与利用者,公众的数据素养直接关乎个人隐私安全。故而,教育成为关键切入点,应将数据安全教育融入国民教育体系,自小学至大学,分阶段、分层次地传授数据保护知识,培育公众的数据保护观念与技能。具体而言,可开设数据安全教育专项课程,教导学生识别网络钓鱼、恶意软件等常见风险,并掌握设置复杂密码、定期清理个人信息等基础防护技巧。同时,借助电视、互联网、社交媒体等多元渠道,开展丰富多样的数据保护宣传活动,提升公众对数据隐私风险的警觉性。此外,应鼓励公众运用加密技术、匿名化处理等手段来守护个人数据,增强个人在数据交易中的谈判地位,使公众真正成为自己数据的主导者。通过提升公众的数据素养,不仅能有效减少因个人疏忽引发的数据泄露事件,还能推动全社会形成尊重数据隐私、维护数据安全的良好风尚。

五、结语

数字浪潮以空前之力重塑全球经济版图,数据作为核心动能,在驱动产业升级、激发创新潜能的同时,其隐私安全与治理问题已成为确保经济稳健运行、社会和谐发展的关键要素。从法规体系的健全到技术防护的强化,从促进国际合作到深化公众意识培养,多维度策略交织并进,绘制出一幅协同治理的新图景。这不仅是为了破解当前数据泄露频发、治理失范的紧迫挑战,更是通往数字文明时代、建立可信赖数字生态的必然路径,兼顾了经济持续增长与个人权利保护的双重目标,为数字经济的长远繁荣奠定了坚实基础。

参考文献:

- [1] 胡海波,耿霄.数据跨境流动治理研究:溯源、脉络与动向[J].情报理论与实践,2023,46(07):178-186.
- [2] 刘琳璘.大数据时代背景下数据安全法治问题研究[J].河南警察学院学报,2023,32(05):29-38.
- [3] 盛丹丹.基于大数据分析的隐私信息保护系统设计与实现[J].信息安全研究,2023,9(09):914-920.
- [4] 华劼.人工智能时代的隐私保护——兼论欧盟《通用数据保护条例》条款及相关新规[J].兰州学刊,2023(6):97-108.
- [5] 刘爽岑.数字经济时代下企业数据治理与隐私保护的挑战[J].中外企业文化,2023,(10):127-129.

作者简介:温家祺(2003.11-),男,汉族,云南昆明人,本科,研究方向:数字经济,大数据。