大数据环境下个人信息保护与数据安全问题探析

卢健平
惠州市水利综合事务中心　广东　惠州　516003

摘　要：在数字经济快速发展背景下，大数据作为核心生产要素广泛应用于各领域，但其海量性、多样性等特征也加剧了个人信息保护与数据安全风险。本文界定相关核心概念，梳理当前个人信息过度收集、数据泄露等突出问题，从法律、技术、管理、社会个人四个层面剖析深层成因，提出完善法律法规、强化技术防护、健全监管机制、提升全民防护能力的优化路径，为平衡大数据价值释放与个人信息安全保障提供理论与实践参考。

关键词：大数据环境；个人信息保护；数据安全问题

引言：随着大数据技术与政务、金融、医疗等领域深度融合，数据价值持续释放，极大提升了社会运行效率与决策科学性。但与此同时，个人信息过度收集、滥用、泄露等问题频发，数据存储传输漏洞、跨境流动隐患等安全挑战凸显，既侵犯个人合法权益，也阻碍数字经济健康发展。基于此，本文聚焦大数据环境下个人信息保护与数据安全问题，探析问题成因与优化策略，助力构建安全有序的数字空间。

1 相关概念与理论基础

1.1 大数据相关概念界定

（1）大数据的定义与特征：大数据是指无法在一定时间范围内用常规软件工具进行捕捉、管理和处理的数据集合，核心特征为海量性、高速性、多样性、价值性和真实性，是数字时代的核心生产要素。（2）大数据的应用场景：广泛覆盖各领域，包括政务服务优化、金融风险防控、医疗精准诊疗、电商个性化推荐等，助力提升效率、优化决策。

1.2 个人信息与数据安全核心概念

（1）个人信息的定义、分类与价值：指以电子或其他方式记录的可识别特定自然人的信息，分为高度敏感、敏感和一般信息三类，是数字经济发展的重要资源，兼具个人权益属性和商业价值。（2）数据安全的内涵与核心要求：内涵是保障数据处于有效保护和合法利用的状态，核心要求包括保密性、完整性、可用性，需符合《数据安全法》相关规定。（3）个人信息保护与数据安全的关联性：个人信息保护是数据安全的核心组成部分，数据安全是个人信息保护的重要保障，二者协同维护数字空间秩序。

1.3 相关理论支撑

（1）隐私保护理论：核心是保障个人对自身信息的自主控制权，通过技术和制度手段防止信息泄露、滥用，兼顾隐私保护与数据利用的平衡。（2）数据治理理论：通过制度、标准和技术，对数据全生命周期进行管理，确保数据质量、安全与合规，推动数据价值释放。（3）网络安全理论：以CIA三元组为核心，通过多层防护措施，保护网络系统和数据免受攻击，为大数据应用和个人信息保护提供基础保障。

2 大数据环境下个人信息保护与数据安全的现状及问题

2.1 大数据环境下个人信息保护与数据安全现状

（1）政策法规逐步完善：我国已构建起以《个人信息保护法》《数据安全法》为核心的法律法规体系，明确个人信息保护边界和数据安全责任，细化监管要求，为行业发展划定合规红线。（2）技术防护初步落地：大数据加密、脱敏、访问控制等防护技术逐步应用，多数企业搭建了基础数据安全防护体系，有效降低了部分常规信息泄露风险，提升了数据安全保障能力。（3）行业自律意识逐步提升：行业协会牵头制定自律规范，重点领域企业主动完善数据管理制度、开展合规培训，逐步形成“合规经营、重视安全”的行业共识。

2.2 个人信息保护存在的核心问题

（1）个人信息过度收集与滥用问题突出：部分企业超出业务需求，强制收集用户非必要个人信息，甚至将收集的信息用于精准营销、利益交换，侵犯用户信息自主权。（2）个人信息泄露风险频发且溯源困难：大数据汇聚导致信息集中化，数据存储、共享环节易出现泄露，且泄露渠道隐蔽、链条复杂，事后溯源取证难度大，难以追责。（3）个人信息主体维权成本高、渠道不畅：用户发现信息被泄露或滥用后，面临取证难、流程繁琐、维权成本高的问题，部分维权渠道不够便捷，导致用户维权意愿偏低[1]。

2.3 数据安全面临的主要挑战

（1）数据存储与传输过程中的安全漏洞：部分企业存储设备防护不足、传输协议不规范，易被黑客攻击窃取数据，且海量数据存储增加了安全管理难度。（2）大数据技术应用带来的安全风险：大数据分析、人工智能等技术的普及，可能引发数据挖掘过度、算法歧视等问题，同时技术迭代加快也导致安全防护难以同步跟进。（3）跨境数据流动中的安全隐患：全球化背景下，数据跨境传输日益频繁，不同国家和地区数据安全规则差异较大，易出现数据泄露、滥用，且跨境监管难度较大。

2.4 问题产生的表层原因

（1）技术应用与安全防护脱节：部分企业重技术应用、轻安全防护，投入不足，导致安全技术与大数据应用发展不同步，无法有效抵御新型安全风险。（2）企业主体责任落实不到位：部分企业缺乏合规意识，未建立完善的数据安全管理制度，未落实信息收集、存储、使用等环节的安全责任，违规操作频发。（3）个人信息保护意识薄弱：部分用户对个人信息重视不足，随意泄露个人信息、点击不明链接，缺乏自我保护意识，间接加剧了信息泄露和滥用风险。

3 大数据环境下个人信息保护与数据安全问题的深层成因分析

3.1 法律层面成因

（1）相关法律法规存在滞后性与不完善性：大数据技术迭代速度快，新型数据应用场景不断涌现，现有法律法规难以全面覆盖数据收集、共享、销毁等全生命周期，对算法滥用、隐性信息泄露等新型问题缺乏明确界定，存在监管空白。（2）法律责任界定模糊、处罚力度不足：部分条款对企业、平台等主体的责任划分不够清晰，对违规收集、泄露个人信息等行为的处罚标准偏低，违法成本远低于违法收益，难以形成有效震慑，导致部分主体铤而走险。（3）跨境数据监管法律体系不健全：目前跨境数据流动的法律规范较为零散，缺乏统一的监管标准和协作机制，难以应对数据跨境传输中的安全风险，且不同国家法律差异较大，增加了跨境监管的难度和复杂度。

3.2 技术层面成因

（1）大数据技术自身的复杂性带来安全漏洞：大数据具有海量性、多样性特征，数据汇聚、分析、存储过程涉及多环节、多技术，技术架构复杂，易出现数据脱敏不彻底、访问权限混乱等安全漏洞，给非法获取数据提供可乘之机。（2）安全防护技术研发与应用滞后：相较于大数据应用技术的快速发展，安全防护技术研发投入不足，核心技术仍有短板，部分企业沿用传统防护手段，无法抵御新型网络攻击和数据泄露风险，防护能力与应用需求脱节。（3）技术标准不统一导致防护效果参差不齐：目前大数据安全防护缺乏统一的技术标准和规范，不同企业、行业采用的防护技术和手段差异较大，部分企业的防护措施流于形式，难以形成系统、有效的安全防护体系[2]。

3.3 管理与监管层面成因

（1）监管体系不健全，多头监管与监管真空并存：大数据涉及多行业、多领域，现有监管体系存在部门分工不明确、协调机制不完善等问题，部分领域出现多头监管、权责交叉，而部分新兴领域则存在监管真空，监管效率低下。（2）监管技术与手段落后于大数据发展速度：监管部门的技术装备和监管手段较为传统，缺乏智能化、精准化的监管工具，难以实现对海量数据的实时监测、预警和溯源，无法及时发现和处置安全隐患。（3）企业内部数据管理制度缺失：部分企业缺乏完善的数据安全管理制度，未建立数据全生命周期管理流程，缺乏专业的安全管理团队，员工违规操作、内部泄露等问题频发，进一步加剧数据安全风险。

3.4 社会与个人层面成因

（1）社会层面：个人信息保护氛围尚未形成，部分媒体对个人信息保护的宣传引导不足，行业内违规行为曝光力度不够，社会公众对个人信息泄露的危害认知不深，尚未形成“人人重视信息安全”的社会氛围。（2）个人层面：信息安全意识与维权能力不足，部分用户对个人信息的重要性认识不足，随意填写、泄露个人信息，缺乏自我保护意识；同时，用户面临取证难、维权流程繁琐等问题，维权能力薄弱，难以有效维护自身合法权益。

4 大数据环境下个人信息保护与数据安全的优化路径

4.1 完善相关法律法规体系

（1）健全个人信息保护与数据安全专项立法：结合大数据时代数据处理的多元化、复杂化、智能化特点，细化个人信息收集、存储、使用、传输、销毁、共享等全流程法律规范，弥补现有法律在算法推荐、数据脱敏、跨境传输等新兴场景下的监管空白，明确个人信息与公共数据、商业数据的边界，实现立法与技术发展同频同步，为数据安全保护和个人信息权益保障提供坚实的法律支撑。（2）明确法律责任，加大处罚力度：清晰界定企业、平台、监管部门及相关责任人的法律责任，区分民事、行政、刑事责任边界，针对违规收集、泄露、滥用个人信息等行为，提高罚款金额、加大处罚力度，将违法成本提高至远超违法收益，同时建立失信惩

戒机制，对严重违规主体实施市场禁入，形成强有力的法律震慑[3]。（3）完善跨境数据流动监管法律规范：结合国际规则，制定统一的跨境数据流动监管标准，明确数据出境安全评估流程、条件和责任，建立跨境数据流动协同监管机制，加强与其他国家和地区的法律协作，推动形成兼容互通的跨境数据监管体系，防范跨境数据安全风险。

4.2 强化技术防护体系建设

（1）推进隐私增强技术（PETs）研发与应用：加大对隐私增强技术的研发投入，重点突破差分隐私、联邦学习、同态加密等核心技术，推动其在大数据分析、数据共享等场景的广泛应用，实现“数据可用不可见”，在保障数据价值释放的同时，有效保护个人信息安全。（2）完善数据加密、访问控制等核心防护技术：优化数据加密技术，对敏感个人信息实行全流程加密存储和传输，升级访问控制机制，建立基于角色的分级授权体系，严格控制数据访问权限，防范内部泄露和非法访问；同时引入入侵检测、漏洞扫描等技术，实现安全隐患实时监测和预警[4]。（3）建立统一的技术标准与安全评估体系：由行业主管部门牵头，联合企业、科研机构，制定统一的大数据安全防护技术标准和规范，明确防护技术要求、实施流程和评估标准；建立常态化安全评估机制，定期对企业数据安全防护体系进行评估，督促企业及时整改安全隐患，提升整体防护水平。

4.3 健全管理与监管机制

（1）构建协同高效的监管体系，明确监管职责：整合监管资源，明确各监管部门的职责分工，建立跨部门协同监管机制，打破监管壁垒，避免多头监管和监管真空；明确监管重点领域和关键环节，聚焦高频违规场景，提升监管针对性和效率。（2）提升监管技术水平，实现精准监管：加大监管技术研发投入，引入大数据、人工智能等技术，搭建智能化监管平台，实现对海量数据的实时监测、分析和溯源，精准识别违规行为，提升监管的智能化、精准化水平，做到早发现、早预警、早处置[5]。（3）强化企业主体责任，完善内部管理制度：督促企业建立健全数据安全管理制度，明确数据安全负责人和管理团队，制定数据全生命周期管理流程；加强企业合规培训，提升员工数据安全意识和合规素养，建立内部审计和问责机制，对违规操作行为严肃追责，推动企业落实主体责任。

4.4 提升社会与个人防护能力

（1）加强宣传教育，营造良好社会氛围：通过媒体、社区、学校等多种渠道，开展个人信息保护和数据安全宣传教育活动，普及相关法律法规和安全知识，曝光典型违规案例，提升社会公众对个人信息安全的重视程度，营造“人人关注信息安全、人人参与信息保护”的良好社会氛围。（2）提升个人信息安全意识与维权能力：引导用户树立个人信息保护意识，规范个人信息使用行为，避免随意泄露个人信息、点击不明链接；简化维权流程，畅通维权渠道，为用户提供便捷的取证、投诉、维权指导服务，提升用户的维权能力，保障用户合法权益。（3）发挥行业协会作用，强化行业自律：支持行业协会牵头制定行业自律规范，引导企业主动履行社会责任，开展合规承诺和自查自纠；建立行业信用评价体系，对合规企业予以表彰，对违规企业进行通报批评，推动行业形成自我约束、良性发展的格局。

结束语

大数据时代，个人信息保护与数据安全是数字经济高质量发展的重要前提，二者相辅相成、不可割裂。解决当前存在的各类问题，需凝聚法律、技术、管理、社会个人的多方合力，补齐立法短板、强化技术支撑、健全监管体系、提升全民素养。唯有如此，才能实现个人信息权益保障与大数据价值释放的双向共赢，推动数字空间持续健康发展，为数字经济可持续发展筑牢安全屏障。

参考文献

[1]张少峰.大数据时代个人信息保护浅议[J].合作经济与科技,2021,20(14):174-175.

[2]崔梦雪.人工智能时代隐私权保护问题研究[J].科技创新与应用,2021,9(17):71-73.

[3]黄岱.大数据与云计算环境下个人信息安全协同保护研究[J].信息与电脑(理论版),2023,15(06):193-195.

[4]王鹏.基于大数据与云计算环境的个人信息安全协同保护研究[J].信息与电脑,2021,10(22):204-205.

[5]代琪怡,刘维.大数据与云计算环境下个人信息安全协同保护研究[J].电脑知识与技术,2023,13(18):57-58.