工程与管理科学
Engineering and Management Science
第 8 卷◆第 2 期◆版本 1.0◆2026 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

大数据时代个人信息保护策略探讨

黄明皓
广西诺远科技有限公司　530022

DOI：10.32629/ems.v8i2.18476

［摘　要］大数据技术的发展使个人信息成为数字经济的关键生产要素，其在用户画像构建、市场分析、公共服务优化等领域发挥着重要作用。《个人信息保护法》的实施构建了全方位的法律保障体系，明确了个人信息权益与处理规则。个人信息的合理保护与利用，既是维护人民群众获得感与安全感的基础，也是激发数据要素价值的前提。在此背景下，本文旨在探索系统的个人信息保护策略，对统筹数字经济发展与数据安全具有重要意义。

［关键词］大数据时代；个人信息；保护策略

引言

大数据技术的快速发展为社会生产生活带来诸多便利，其在提升资源配置效率、优化服务体验等方面发挥着重要作用。但在数据价值不断释放的过程中，个人信息作为核心数据资源，其安全保障需求日益凸显。构建科学有效的个人信息保护策略，不仅能维护个人合法权益，还能为数字经济健康发展提供支撑，更能助力国家数据安全体系的完善。因此，明确个人信息保护策略的核心方向与实施路径，成为大数据时代推进数字化建设的重要任务，对实现数据利用与安全保护的平衡具有关键意义。

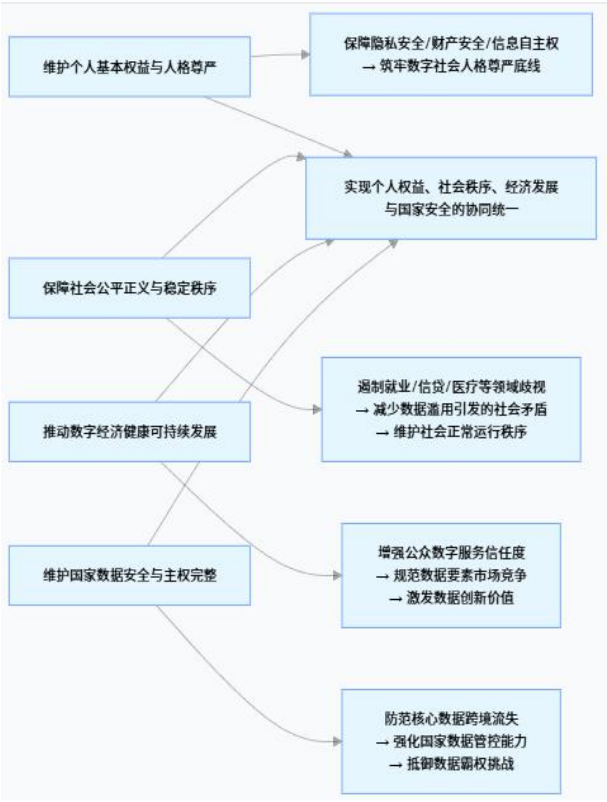
一、大数据时代个人信息保护的重要性

（一）维护个人基本权益与人格尊严的核心保障

个人信息是个人身份、行为、偏好等特征的数字化载体，其完整性与安全性直接关联个人基本权益。在大数据技术的广泛应用中，个人信息被收集、存储、分析的范围不断扩大，若缺乏有效保护，个人信息极易被非法获取、滥用或篡改。这不仅可能导致个人财产安全受到威胁，更会侵犯个人的隐私权与自主权，使个体在数据环境中失去对自身信息的控制能力。当个人信息持续处于暴露状态时，个体的人格尊严将难以得到保障，进而影响个体在社会生活中的安全感与信任感，因此，个人信息保护是维护个人基本权益与人格尊严的核心前提，也是实现个体在数字社会中正常生活的基础[1]。

（二）保障社会公平正义与稳定秩序的重要基石

大数据技术的应用虽提升了社会运行效率，但也可能因个人信息保护缺失引发社会不公问题。在缺乏保护的情况下，部分主体可能利用获取的个人信息实施歧视性行为，如在就业、信贷、医疗等领域，依据个人信息对特定群体设置不公平门槛，破坏社会公平竞争环境。同时，个人信息的大规模泄露或滥用可能引发社会恐慌，扰乱社会正常秩序。此外，个人信息保护机制的完善能够规范数据收集与使用行为，减少因数据滥用引发的社会矛盾，保障社会资源的合理分配，从而为社会公平正义与稳定秩序提供重要支撑。



图一　大数据时代个人信息保护重要性逻辑图

（三）推动数字经济健康可持续发展的必要条件

数字经济的核心在于数据要素的有效流动与合理利用，而个人信息作为重要的数据资源，其保护水平直接影响数字经济的发展质量。若个人信息保护不到位，会降低公众对数字服务的信任度，导致公众对数据共享、数字交易等行为产

生抵触情绪，进而制约数字经济的市场规模与发展速度。同时，缺乏保护的个人信息易引发数据滥用、数据垄断等问题，部分企业可能通过非法收集个人信息获取竞争优势，破坏市场公平竞争格局，阻碍数字经济创新发展。只有建立完善的个人信息保护体系，才能规范数据要素市场秩序，增强公众对数字经济的信任，为数字经济健康可持续发展创造良好环境。

（四）维护国家数据安全与主权完整的关键环节

在全球化背景下，大数据的跨境流动日益频繁，个人信息作为国家数据资源的重要组成部分，其安全保护与国家数据安全、主权完整紧密相关。大量个人信息的跨境泄露可能导致国家核心数据资源流失，被境外势力利用开展情报活动，威胁国家政治安全、经济安全与社会安全。同时，若缺乏有效的个人信息保护机制，国家在数据领域的话语权与主导权将受到削弱，难以应对数据霸权带来的挑战，影响国家数据主权的完整性。

二、大数据时代个人信息保护存在的问题

（一）法律体系存在滞后性与适配性不足

当前个人信息保护相关法律体系未能完全跟上大数据技术的发展速度，法律条款存在一定滞后性。部分法律规定对大数据场景下的个人信息收集、存储、传输、利用等环节的界定不够清晰，对新型数据形态的属性与保护范围缺乏明确规范。同时，不同领域、不同层级的法律规范之间存在衔接不畅的问题，部分条款存在交叉或冲突，导致实践中执法与司法适用标准不统一。此外，法律对个人信息侵权行为的责任认定与处罚力度不足，难以形成有效震慑，无法充分应对大数据时代个人信息被大规模、隐蔽性滥用的情况，使得法律对个人信息的保护作用未能充分发挥。

（二）技术防护能力与数据风险不匹配

大数据技术的快速发展催生了更复杂、更隐蔽的数据安全风险，但当前相关主体的技术防护能力未能与之匹配。部分企业与机构缺乏先进的数据加密、脱敏、访问控制等技术手段，对个人信息的全生命周期安全管理存在漏洞，导致个人信息在收集环节易被过度获取，在存储环节易遭受黑客攻击、内部泄露，在传输环节易被非法拦截。同时，大数据分析技术的广泛应用使得个人信息的关联性挖掘能力大幅提升，即使是看似无关的碎片化信息，也可能通过技术手段整合还原个人完整画像，而现有技术防护措施对这类“间接侵权”行为的识别与阻断能力较弱，无法有效防范数据聚合带来的安全风险。

（三）监管机制存在覆盖不全与协同不足

大数据时代个人信息处理主体呈现多元化、分散化特征，涵盖互联网企业、金融机构、政务部门、第三方数据服务商等，但当前监管机制未能实现对所有处理主体的全面覆盖。部分小型企业、新兴数据服务机构处于监管盲区，缺乏常态化的监管检查，导致这些主体的个人信息保护行为缺乏约束。同时，监管部门之间的协同机制不完善，不同监管机构的职责划分存在交叉模糊地带，在处理跨领域、跨区域的个人信息侵权案件时，容易出现推诿扯皮、响应迟缓的情况[2]。

（四）个人信息保护意识薄弱与维权能力不足

多数个人对大数据时代个人信息的价值与风险认知不足，个人信息保护意识较为薄弱。在日常生活中，个人往往忽视对自身信息的保护，轻易同意各类 APP 的权限申请、签署模糊的用户协议，对个人信息的收集范围、使用目的缺乏主动核查，导致个人信息被过度收集、滥用而不自知。同时，个人在遭遇信息侵权时，面临维权能力不足的问题。个人难以举证证明信息侵权行为的存在、侵权主体的责任以及自身遭受的损失，且维权过程涉及法律程序复杂、时间成本高、经济成本高，多数个人因维权难度大而选择放弃，使得个人作为信息所有者的权益难以通过自身行动得到有效维护，进一步加剧了个人信息被侵权的风险。

三、大数据时代个人信息保护的优化措施

（一）构建动态适配的法律规范体系，夯实制度保障根基

法律体系的完善是个人信息保护的核心支撑，其必须实现与大数据技术发展的同频迭代。立法部门应加快制定《个人信息保护法》配套细则，对“目的限制原则”中的“明确合理”标准、“直接相关”边界及“最小权益影响”尺度做出具体界定，填补新型数据形态保护的规范空白。同时，立法部门需梳理不同领域、层级的法律规范，消除条款交叉与冲突，建立统一的执法与司法适用标准，解决实践中法律适用混乱的问题。

针对个人信息处理全流程，立法部门应明确收集、存储、传输、利用等各环节的操作规范，强化“合法、正当、必要”原则的落地执行，对过度收集、超范围使用等行为做出精准界定。在责任认定与惩戒方面，法律应细化侵权行为的构成要件，提高罚款金额等处罚力度，明确平台、第三方服务商等多方主体的连带责任，形成有效震慑。此外，立法部门需建立法律动态修订机制，定期结合技术发展与实践案例更新条款，同时完善跨境数据流动规则，确保数据跨境传输的安全与合规，从制度层面平衡数据利用与隐私保护的关系。

（二）升级全生命周期技术防护体系，强化风险防控能力

技术防护能力的提升是应对数据安全风险的关键，相关主体需构建覆盖个人信息全生命周期的技术防护架构。技术防护效能评估模型为：

[公式 1：技术防护效能指数]

T=（E+M+A）/3×C

（其中：T 为技术防护效能[0-1]，E 为加密强度[0-1]，M 为脱敏效果[0-1]，A 为访问控制精度[0-1]，C 为系统兼容性[0.8-1.2]）

企业与机构应加大技术研发投入，部署先进的数据加密、脱敏、访问控制技术，对敏感信息实施分级分类保护，确保收集环节仅获取必要信息，存储环节实现安全冗余与泄露预警，传输环节采用加密通道防范拦截。针对数据聚合带来的"间接侵权"风险，技术研发方需开发智能关联分析监测系统，通过算法识别碎片化信息的异常整合行为，实现对潜在风险的提前预警与阻断。

隐私计算技术的应用是平衡数据利用与保护的重要路径，企业应推广联邦学习、差分隐私等技术，在不暴露原始个人信息的前提下实现数据价值挖掘。同时，企业需建立算法透明化机制，公开数据训练来源与算法决策逻辑，打破“数据黑箱”，并为用户提供“算法拒绝权”实现工具。对于人工智能大模型等新技术场景，技术研发方应制定数据安全标准，构建"幻觉数据"识别与过滤机制，从源头防范虚假数据带来的隐私风险。此外，相关主体需定期开展技术防护系统的安全测评与升级，引入第三方机构进行漏洞检测，确保技术能力与数据风险的动态匹配。

（三）建立全域协同的监管治理机制，提升监管执行效能

监管机制的完善需实现从“被动应对”到“主动防控”的转变，构建覆盖全主体、全流程的监管体系。监管部门应扩大监管覆盖范围，将小型企业、新兴数据服务机构纳入监管清单，建立“分级分类+信用评级”的监管模式，对高风险主体实施常态化检查，对低风险主体采用抽查监管，消除监管盲区。在部门协同方面，应建立网信、工信、市场监管、公安等多部门的联席会议制度，明确各部门在个人信息收集、存储、利用等环节的监管职责，避免职责交叉与推诿。

监管技术的升级是提升监管效能的核心手段，监管部门应构建国家级个人信息保护监管平台，整合各领域数据处理动态，通过大数据分析实现对异常处理行为的实时监测与自动预警。针对跨区域案件，应建立全国统一的案件协查机制，实现证据共享与执法协同。同时，监管部门需强化“事前审查—事中监测—事后惩戒”的全链条监管，对 APP 及 SDK 开展常态化合规检测，定期通报违规主体并督促整改，对整改不到位的实施严厉惩戒。此外，监管部门应推动建立国家级 AI 数据交易平台，规范数据共享与定价机制，通过平台化监管实现数据流动的全程可追溯。

（四）强化个人主体的权利保障与能力建设，筑牢基层保护防线

个人保护意识与维权能力的提升是个人信息保护的基础环节，需通过系统性举措实现个人从“被动受害”到“主动维权”的转变。政府与社会组织应开展常态化个人信息保护宣传教育，针对不同群体设计专项课程，重点普及《个人信息保护法》中的知情权、决定权、删除权等权利，提升个人对信息价值与风险的认知能力。针对青少年等重点群体，应建立家校协同教育机制，培养其安全使用数字服务的习惯。

维权渠道的畅通与维权成本的降低是提升维权能力的关键，司法部门应建立个人信息侵权案件的专门审理机制，简化诉讼程序，推行“举证责任倒置”制度，由信息处理者证明自身行为合规，减轻个人举证负担。同时，监管部门应建立便捷的线上投诉举报平台，实现案件快速受理、转办与反馈，并将投诉处理结果纳入企业信用评级[3]。立法部门需进一步完善个人信息权利体系，明确查阅权、复制权、可携带权的实现路径，赋予个人对自动化决策的反对权与解释说明请求权。此外，法律援助机构应扩大服务范围，为经济困难的侵权受害人提供免费法律咨询与代理服务，提升个人维权的可行性。

结语

综上所述，大数据时代个人信息保护策略的构建与实施，是一项系统性工程，其覆盖法律、技术、监管、个人等多个维度。这些策略的落地，能够为个人信息安全提供全方位保障，增强公众对数字环境的信任，进而推动数字经济持续健康发展。同时，策略的不断优化也能提升国家在数据领域的治理能力，为数字社会建设奠定坚实基础。

[参考文献]

[1]李昂.个人金融信息保护中的个人控制模式之检视——基于司法大数据的个人金融信息保护研究[J].法大法律评论，2024，40（02）：23-35.

[2]刘宁.大数据时代网络平台过度收集个人信息行为认定及法律规制策略[J].法制博览，2025，（18）：142-144.

[3]田临儒.个人信息保护在大数据时代下的民法路径探索[J].社会与公益，2025，（12）：74-77.