Open Journal of Legal Science 法学, 2025, 13(5), 871-876
Published Online May 2025 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2025.135124

Hans汉斯

大数据时代下公民隐私权保护研究

汤晶晶

宁波大学马克思主义学院，浙江 宁波

收稿日期：2025年4月2日；录用日期：2025年4月11日；发布日期：2025年5月16日

摘　要

随着大数据技术的快速发展和广泛应用，公民隐私权保护已成为数字时代的重要议题。本研究系统探讨了大数据环境下隐私权概念的新特征及其面临的挑战，包括立法碎片化、司法救济不足和监管效能低下等问题。研究发现，传统隐私权保护机制已难以应对数据聚合分析、算法歧视等新型侵权形态。为此，本文从四个维度提出对策建议：立法上制定专门的《隐私权保护法》，确立数据自主权等新型权利；司法上优化举证责任分配和损害赔偿机制；执法上构建统一权威的智能监管体系；社会层面加强隐私保护宣传教育。研究强调，隐私权保护需要平衡数据利用与权益保障，构建多元协同的治理格局，运用新兴技术提升保护效能，并积极参与国际数字治理规则制定。建议将隐私权保护上升为国家战略，为数字中国建设提供制度保障。本研究为完善大数据时代的隐私权保护体系提供了理论参考和实践路径。

关键词

大数据，隐私权保护，数据治理，法律规制，数字社会

Research on the Protection of Citizens' Privacy Rights in the Era of Big Data

Jingjing Tang

Marxism School of Ningbo University, Ningbo Zhejiang

Received: Apr. 2nd, 2025; accepted: Apr. 11th, 2025; published: May 16th, 2025

Abstract

With the rapid development and widespread application of big data technology, the protection of citizens' privacy rights has become a critical issue in the digital era. This study systematically examines the new characteristics of privacy rights in the big data environment and the challenges they face, including legislative fragmentation, inadequate judicial remedies, and low regulatory efficiency. The research finds that traditional privacy protection mechanisms are insufficient to ad-

文章引用: 汤晶晶. 大数据时代下公民隐私权保护研究[J]. 法学, 2025, 13(5): 871-876.
DOI: 10.12677/ojls.2025.135124

dress new forms of infringement such as data aggregation analysis and algorithmic discrimination. Accordingly, this paper proposes countermeasures from four dimensions: legislatively enacting a specialized "Privacy Rights Protection Law" to establish new rights like data autonomy; judicially optimizing the allocation of burden of proof and damage compensation mechanisms; administratively constructing a unified and authoritative intelligent regulatory system; and socially strengthening privacy protection education. The study emphasizes that privacy protection requires balancing data utilization with rights safeguarding, building a multi-stakeholder collaborative governance framework, leveraging emerging technologies to enhance protection effectiveness, and actively participating in the formulation of international digital governance rules. It is recommended to elevate privacy protection to a national strategy to provide institutional safeguards for the development of Digital China. This research offers theoretical references and practical pathways for improving privacy protection systems in the big data era.

Keywords

Big Data, Privacy Protection, Data Governance, Legal Regulation, Digital Society

1. 引言

2024 年 3 月，国务院下发《推动大规模设备更新和消费品以旧换新行动方案》，将数字化转型、智能化升级作为重点行业设备更新改造的重要方向之一。《方案》中指出在迎接“第四次工业革命”的浪潮中，要牢牢把握数字化、网络化、智能化融合发展的契机，大力推进数字技术与实体经济深度融合，着力推进“数据要素×”和“人工智能+”，通过数字技术为千行百业赋能，发展新质生产力，建设现代化产业体系，以澎湃动力不断开辟经济增长新空间。从客观角度来看，大数据技术的进步已成为国家战略的重要组成部分，这是我国抢占发展机遇、构建国家竞争力的关键技术支撑。

大数据技术在推动社会变革和高新技术发展的同时，关于公民隐私权的保护也被提到议事日程上。由于大数据时代的降临而带来的信息爆炸，使得公民的个人信息存在被贩卖、流通的现象。依法治国是建设中国特色社会主义的本质要求和重要保障，当前如何完善相关法律法规使公民的隐私权得到更好的保护是仍有待研究的重要课题。

2. 大数据及隐私权的概述

2.1. 大数据时代公民隐私权的概念

大数据时代深刻改变了传统隐私的内涵和外延。大数据作为无法通过传统工具处理的海量信息资产，具有数据量大(Volume)、处理速度快(Velocity)、类型多样(Variety)、价值密度低(Value)和真实性(Veracity)的“5V”特征[1]。这些特性使得个人信息在云计算、人工智能等技术的加持下，能够被高效收集、分析和利用，形成具有巨大商业价值和社会价值的数据资源。然而，这种技术便利也带来了前所未有的隐私风险，Facebook、华住酒店等重大数据泄露事件警示我们，在数据价值挖掘与隐私保护之间需要建立新的平衡。

在此背景下，隐私权的定义已从传统的“独处权”演变为对个人信息的全面控制权。它不仅包括个人生活安宁、通信秘密等传统内容，更扩展到对各类数据收集、使用和流转过程的知情权与决定权。现

代隐私权的核心在于确保个人对其私人领域和信息的自主控制，维护数字时代的人格尊严与自由。值得注意的是，随着数据成为关键生产要素，隐私权也呈现出人格权与财产权双重属性并重的特征，这要求我们在保护个人隐私的同时，也要兼顾数据价值的合理开发利用。网络隐私权是在大数据背景下，依据时代的进步而产生的，对于网络隐私权的侵犯往往涉及财产和人身。大数据时代下的公民个人隐私打破了时间和空间的限制，逐渐从传统意义上静态的、封闭的人身隐私、场所隐私，转变为流动的、开放的信息隐私[2]。

2.2. 大数据时代公民隐私权的特点

在大数据技术快速发展的背景下，公民隐私呈现出诸多新特点，这些特点深刻改变了传统隐私保护的理念和方式。首先，隐私数据的边界日益模糊化。传统隐私保护主要针对明确的个人身份信息，如姓名、身份证号等。但在大数据环境下，各类看似无关的行为数据，如浏览记录、购物偏好、位置轨迹等，经过算法分析和关联后都可能成为敏感隐私。这种“非隐私数据转化为隐私”的特性，使得隐私保护的范畴大大扩展。

其次，隐私侵害具有隐蔽性和累积性。单个数据采集行为可能看似无害，但当海量数据被持续收集、聚合分析时，就会产生“量变到质变”的隐私风险[3]。例如，某次购物记录不会暴露个人隐私，但长期积累的消费数据却能精准刻画用户的消费习惯、经济状况等私密信息。这种侵害往往在用户毫无察觉的情况下发生，且损害结果具有滞后性。

第三，隐私权的主体间性特征凸显[4]。在大数据环境下，个人隐私往往涉及多方主体，包括数据主体、数据控制者、数据处理者等多个利益相关方。一个简单的网络行为就可能同时涉及平台运营商、第三方服务商、广告商等多个主体对个人数据的收集和使用。这种多方参与的特性使得隐私保护的责任划分变得异常复杂。

最后，隐私保护面临技术迭代的持续挑战。随着人工智能、物联网等新技术的发展，数据采集的方式和范围不断扩展，从线上行为到线下活动，从主动提供到被动采集，隐私保护始终处于与技术创新赛跑的状态。这就要求隐私保护机制必须具备足够的灵活性和前瞻性，才能应对不断涌现的新挑战。

3. 大数据时代公民隐私权面临挑战

3.1. 大数据时代隐私权法律保护的制度性缺陷

当前我国隐私权法律保护体系在应对大数据技术发展时呈现出明显的滞后性，主要表现在三个方面：首先，立法体系呈现碎片化特征，《民法典》《网络安全法》《个人信息保护法》等法律中的隐私权保护条款缺乏系统协调，导致规范冲突和适用困境。其次，隐私权概念界定未能与时俱进，传统“生活安宁权”和“信息保密权”的界定难以涵盖数据自主权、被遗忘权等新型权利内容，对数据画像、算法歧视等新型侵权形态缺乏有效规制[5]。再次，特殊数据类型保护不足，虽然《个人信息保护法》将生物识别数据等列为敏感信息，但在采集限度、存储要求、使用边界等关键环节缺乏可操作性规定。此外，数据跨境流动监管制度尚不健全，现有规定过于原则化，难以平衡数据安全与流动需求；法律责任体系也存在主体认定困难、赔偿标准模糊等问题，特别是对平台企业的责任认定往往受制于“技术中立”原则。这些制度性缺陷导致现行法律难以为大数据时代的隐私权提供全面保障，亟需通过制定专门法律、建立动态立法机制等途径加以完善。

3.2. 大数据时代隐私权司法保护的现实困境

大数据技术的快速发展使隐私权司法保护面临前所未有的挑战，主要体现在以下方面：首先，侵权

认定标准滞后，传统隐私侵权以“非法公开”为核心要件，但大数据环境下更具危害性的数据聚合分析、用户画像等新型侵权形态往往难以纳入现有认定标准。其次，举证责任分配不合理，根据“谁主张谁举证”原则，受害人需要证明侵权事实、损害结果及因果关系，但大数据环境下数据收集、处理的隐蔽性和技术复杂性使个人举证面临巨大困难。再次，损害赔偿计算缺乏统一标准，现行法律对精神损害赔偿的规定过于原则化，难以应对大数据侵权导致的复合型损害。此外，司法技术能力不足，法官普遍缺乏处理电子证据、理解算法逻辑的专业能力；诉讼效率低下，传统诉讼程序难以适应大数据侵权案件证据量大、涉及面广的特点[6]。更为关键的是，平台责任认定存在困境，算法黑箱导致难以追溯最终责任主体，平台往往以技术中立为由逃避责任。这些困境严重制约了司法救济的有效性，亟需通过建立举证责任倒置规则、完善电子证据规则、引入专家辅助人制度等改革措施加以突破，同时应当探索建立专门的数据法庭或合议庭，提升司法机关处理新型隐私权纠纷的专业能力。

3.3. 大数据时代隐私权行政监管的体系性不足

当前我国隐私权行政监管体系在应对大数据技术带来的挑战时呈现出明显的体系性缺陷，主要表现在以下方面：首先，监管主体权责分散，网信、公安、工信、市场监管等多个部门依据不同法律法规行使监管权，导致职能交叉与监管空白并存。其次，监管标准不统一，各部门对数据收集、存储、使用的合规要求存在差异，企业难以建立统一的合规体系。再次，监管技术手段滞后，面对日新月异的数据处理技术，监管部门普遍缺乏必要的技术能力和专业人才。此外，监管措施缺乏威慑力，现行行政处罚标准与大数据企业的违法收益严重不匹配，难以形成有效震慑；跨区域协作机制不健全，数据流动的跨地域性与监管的属地化管理之间存在矛盾。更为突出的是，对新型业态的监管滞后，云计算、区块链等新技术应用往往游离于现有监管框架之外。同时，行业自律机制不完善，行业协会等社会组织未能充分发挥自律监管作用；国际监管合作不足，在数据跨境流动等全球性问题上缺乏有效的国际合作机制。这些体系性不足严重制约了监管效能，亟需通过建立统一监管机构、制定分级分类监管标准、提升监管科技水平等改革措施加以完善，同时应当探索建立“监管沙盒”等创新机制，在保障隐私安全的前提下促进数据要素有序流动，并加强行政执法与刑事司法的衔接，形成监管合力。

4. 大数据时代公民隐私权保护对策

4.1. 构建系统完备的隐私保护法律体系

在大数据时代背景下，构建系统完备的隐私保护法律体系已成为当务之急。当前我国隐私权法律保护面临的首要挑战是立法体系的碎片化问题。《民法典》《网络安全法》《个人信息保护法》等多部法律中虽然都包含隐私保护条款，但这些规定分散且缺乏协调，导致法律适用时经常出现规范冲突。例如，《民法典》侧重民事权益保护，《网络安全法》强调安全管理，《个人信息保护法》则着重信息处理规范，这种分散立法模式难以应对大数据环境下隐私保护的复杂性。

制定专门的《隐私权保护法》。作为隐私保护领域的基本法，这部法律应当确立隐私权在大数据时代的新内涵，将传统隐私权扩展为包含数据自主权、数据可携权、被遗忘权等新型权利内容的复合型权利[7] (pp. 78-81)。具体而言，数据自主权应赋予个人对其数据的全面控制能力；数据可携权保障个人在不同平台间转移数据的自由；被遗忘权则确保个人可以要求删除不当或过时的个人信息。这部法律还需要明确隐私权与个人信息权益的关系，构建二者协调保护的法律框架。

完善特殊数据类型保护。对于生物识别数据、基因数据、健康医疗数据等敏感信息，现行法律仅作原则性规定，缺乏具体实施细则。建议在专门立法中设立单独章节，对这些特殊数据类型作出特别规定：明确生物识别数据的采集必须遵循“最小必要”原则；规定基因数据只能用于特定目的且必须匿名化处

理；对健康医疗数据的存储提出更高级别的安全要求。同时，应当建立特殊数据使用的备案审查制度，确保其处理过程受到严格监管。

建立动态立法机制。随着数字经济的全球化发展，数据跨境流动日益频繁，但现有法律规定过于原则化。建议在法律中细化数据出境安全评估制度：建立数据分类分级出境管理制度；明确关键数据目录；制定标准化的安全评估流程；规定境外接收方的数据保护义务。同时，要建立数据跨境流动的国际合作机制，通过双边或多边协议协调不同法域的数据保护标准。

通过以上措施，构建起以专门法律为核心、配套法规为支撑、技术标准为补充的立体化隐私保护法律体系，为大数据时代的隐私权提供坚实的制度保障。这一体系应当既坚持保护个人隐私权益的基本原则，又为数据的合法合理利用保留必要空间，实现保护与利用的平衡。

4.2. 隐私权救济机制的优化路径

大数据时代的隐私权司法保护面临诸多困境，亟需构建系统化的救济机制。在实体规则方面，应当突破传统举证责任分配模式，建立以数据控制者为核心的举证责任倒置制度，要求其提供完整的数据处理记录和合规证明[8]。同时完善损害赔偿体系，根据侵权行为性质、持续时间、影响范围等因素建立三级赔偿标准，并将精神损害、社会评价降低等非财产性损害纳入赔偿范围。为应对技术复杂性挑战，建议在法院系统内设立专业数据审判庭，配备具有信息技术背景的法官和专家陪审员，并建立全国性的电子证据鉴定中心和算法审查委员会。

在程序优化方面，需要创新诉讼机制设计。建立电子证据区块链存证平台，实现证据的快速固定和验证；推行全流程在线诉讼模式，降低当事人维权成本。完善示范诉讼制度，通过典型判例确立裁判标准，实现“审理一案、指导一片”的效果[9] (pp. 130-135)。同时强化司法与行政执法的协同，建立案件双向移送机制和信息共享平台，对重大隐私侵权案件实行联合督办。此外，应当优化集体诉讼程序，简化立案条件，完善代表人选任机制，并建立诉讼费用分担制度，切实提升司法救济的可得性和实效性，为公民隐私权提供有力的司法保障。

4.3. 构建协同高效的隐私权行政监管体系

随着大数据技术的快速发展，传统隐私权行政监管模式面临严峻挑战。现行监管体系存在三个突出矛盾：一是数据流动的跨域性与监管的属地化之间的矛盾；二是技术迭代的快速性与监管手段的滞后性之间的矛盾；三是违法行为的隐蔽性与监管能力的有限性之间的矛盾[10] (pp. 185-189)。这些结构性矛盾导致监管效能不足，亟需从制度设计、技术应用和治理模式三个维度进行系统性重构。

在制度设计层面，应当建立统一权威的监管架构。现行多部门分头监管的模式导致监管标准不一、执法尺度差异等问题。借鉴欧盟 GDPR 的实施经验，设立直属国务院的国家数据保护局，整合网信、公安、工信等部门的监管职能，制定全国统一的隐私保护标准和执法规范[7] (pp. 167-171)。该机构应实行垂直管理模式，在省级设立派出机构，建立跨区域执法协作机制，确保监管的一致性和有效性。同时，要完善监管权力清单制度，明确各级监管部门的职责边界，建立监管问责机制，防止监管缺位或越位。

在技术应用层面，需要构建智能化的监管工具体系。大数据时代的隐私侵权往往具有技术性、隐蔽性等特点，传统监管手段难以有效应对。建议重点建设三大技术平台：一是基于区块链的监管信息共享平台，实现监管部门间的数据实时共享和证据固定；二是运用机器学习算法的风险预警系统，通过对海量数据的实时分析，自动识别异常数据处理行为[10]；三是智能合规检查系统，通过自动化手段评估企业的数据合规状况。同时，要建立监管科技(RegTech)研发中心，持续研发适应新技术发展的监管工具，保持监管能力与技术发展的同步性。

在治理模式层面，应当建立多元协同的共治格局。隐私权保护不能仅依靠政府监管，需要调动各方力量形成治理合力。具体而言：第一，强化行业自律，推动相关行业协会制定隐私保护团体标准，建立行业自律公约；第二，完善第三方治理机制，鼓励专业机构开展合规认证和评估，培育专业的隐私保护服务市场；第三，健全公众参与机制，建立便捷的举报投诉平台，完善举报奖励制度[11]；第四，加强国际监管合作，通过双边或多边协议建立跨境监管协作机制，共同应对数据全球化带来的挑战。

通过上述三个维度的系统性重构，可以建立起适应大数据时代要求的现代隐私权监管体系。这一体系具有以下特征：在监管主体上，实现从多头分散到统一权威的转变；在监管手段上，实现从人工检查到智能监管的升级；在治理模式上，实现从政府单方监管到多元协同共治的转型。这种新型监管体系能够有效提升隐私权保护的及时性、精准性和有效性，为数字时代的隐私权提供坚实的制度保障。未来，还需要持续跟踪技术发展动态，不断完善监管制度和手段，保持监管体系的适应性和前瞻性。

5. 结语

大数据技术的迅猛发展在推动社会进步的同时，也对公民隐私权保护提出了前所未有的挑战。本研究系统探讨了大数据时代公民隐私权保护面临的主要困境，并从立法、司法、执法及宣传教育四个维度提出了针对性的对策建议。研究发现，当前隐私权保护体系存在立法碎片化、司法救济不足、监管效能低下等突出问题，亟需构建适应数字时代需求的系统性保护机制。

未来隐私权保护应当坚持以下原则：一是平衡发展，既要保障公民隐私权益，又要促进数据要素合法流动；二是协同治理，构建政府主导、企业自治、行业自律、公众参与的多元共治格局；三是技术赋能，运用区块链、人工智能等新技术提升保护效能；四是国际接轨，积极参与全球数字治理规则制定。建议将隐私权保护上升为国家战略，纳入数字中国建设整体布局，为构建安全可信的数字社会提供制度保障。

本研究仍存在一定局限，如对新兴技术(如联邦学习、隐私计算)的隐私影响分析不够深入，未来可进一步探索技术治理与法律规制的协同路径。随着数字经济的持续发展，隐私权保护将面临更多新课题，需要学界和实务界持续关注与研究。

参考文献

[1] Katal, A., Wazid, M. and Goudar, R.H. (2013) Big Data: Issues, Challenges, Tools and Good Practices. 2013 6*th International Conference on Contemporary Computing* (*IC*3), Noida, 8-10 August 2013, 404-409. https://doi.org/10.1109/ic3.2013.6612229

[2] 杨建国. 大数据时代隐私保护伦理困境的形成机理及其治理[J]. 江苏社会科学, 2021(1): 142-150+243.

[3] 齐爱民. 数据安全与隐私保护研究[J]. 法学研究, 2021(4): 56-69.

[4] 王迁. 知识产权法教程[M]. 北京: 中国人民大学出版社, 2021: 89-102.

[5] 张新宝. 互联网时代的隐私权保护[M]. 北京: 中国人民大学出版社, 2020: 112-115.

[6] 杨立新. 网络隐私权法律保护[M]. 北京: 中国法制出版社, 2021: 105-109.

[7] 周汉华. 个人信息保护法律体系研究[M]. 北京: 法律出版社, 2021: 78-81.

[8] 程啸. 数字经济时代的法律变革[M]. 北京: 法律出版社, 2023: 89-93.

[9] 王利明. 大数据时代的隐私权保护[M]. 北京: 北京大学出版社, 2022: 130-135.

[10] 张平. 大数据法律问题研究[M]. 北京: 北京大学出版社, 2020: 178-182.

[11] 龙卫球. 民法总论[M]. 北京: 中国法制出版社, 2021: 156-160.