

大数据时代公民隐私权的法律保护对策研究

洪 衍

宁波大学马克思主义学院, 浙江 宁波

收稿日期: 2025年3月17日; 录用日期: 2025年4月8日; 发布日期: 2025年5月13日

摘 要

大数据时代, 信息技术的飞速发展推动社会的进步与经济增长, 公民的隐私权也面临着泄露风险, 数据在收集、存储和传输过程中有着极大的安全隐患, 而公民的自我保护意识薄弱, 执法监管难度大等现状也给公民的隐私权保护带来了严峻挑战, 为了完善公民隐私权法律保护, 本文提出相应的对策, 寻求信息公开与保护隐私的平衡点, 从而构建一个公正并尊重隐私的社会环境。

关键词

大数据时代, 公民隐私权, 法律保护

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

Yan Hong

School of Marxism, Ningbo University, Ningbo Zhejiang

Received: Mar. 17th, 2025; accepted: Apr. 8th, 2025; published: May 13th, 2025

Abstract

In the era of big data, the rapid development of information technology has promoted social progress and economic growth. However, citizens' privacy rights are also at risk of being leaked. During the collection, storage and transmission of data, there are significant security risks. Moreover, citizens' self-protection awareness is weak, and the difficulty of law enforcement and supervision is high. These current situations have also brought severe challenges to the protection of citizens' privacy rights. In order to improve the legal protection of citizens' privacy rights, this article proposes corresponding countermeasures to seek a balance between information disclosure and privacy

文章引用: 洪衍. 大数据时代公民隐私权的法律保护对策研究[J]. 法学, 2025, 13(5): 866-870.

DOI: 10.12677/ojls.2025.135123

protection, thereby building a fair and privacy-respecting social environment.

Keywords

Big Data Era, Citizen's Privacy Rights, Legal Protection

Copyright © 2025 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 引言

在数字技术革命的浪潮中，大数据已然成为了推动社会进步与经济增长的核心生产要素，数字化浪潮重塑了人类社会发展的运行逻辑，公民的生活已经全方位被数据所渗透与记录。然而当公民的一言一行都被转化为可被储存、分析的数据时，公民的隐私权也遭遇着前所未有的危机。现阶段，我国公民隐私权的法律保护系统还需要不断加强与完善，频繁收到精准投送的广告以及个人信息被肆意贩卖等等都体现了公民的隐私权受到侵犯，严重威胁到公民的人格尊严、财产安全以及社会稳定发展。这种现状下，我们应该要采取一系列保护措施，完善相关的行业规范，加大法治宣传，严格落实现有立法，强化对相关行业的监督管理，提升公民法治素养。

2. 大数据时代公民隐私权面临的挑战

大数据时代，海量的数据可以给我们带来众多便利与价值，但同时，数据的透明化也在一定程度上打破了信息共享与公民隐私保护之间的平衡，公民的隐私权在数据收集环节面临侵权风险，存储与传输中存在安全隐患，严重威胁公民隐私安全。

2.1. 数据收集环节的隐私侵权风险

大数据背景下，对个人数据要素已经不再局限于静态意义上的认识，而更多是从动态角度去衡量它的价值，个人数据要素不仅蕴含着较大的商业价值，而且对于经济组织乃至国家而言，极具战略性意义[1]。诚然，数据收集是各项研究开展的一个基本步骤，但是这种广泛收集数据的行为存在着信息泄露的巨大风险。许多企业和机构在收集数据时，惯用复杂、冗长且晦涩的隐私政策声明，导致普通用户难以理解其中条款。例如，在一些手机应用程序安装时，其要求获取大量的信息位置、通讯录、相册等权限，如果选择不同意，则无法正常使用该应用程序，实际上这就是一种变相的强迫用户同意，使得公民在不得已的情况下，让渡了部分的隐私权。还有电商平台不仅会收集用户所购买的相关商品的信息，还会利用用户的浏览记录、停留时间、搜索关键词等等来深挖用户的潜在爱好、消费偏好、生活习惯等隐私数据，这些都不是正常业务需求的数据收集行为，并且极大地增强了公民泄露隐私的风险。不仅如此，还有很多非法组织也觊觎这些海量数据，他们会通过网络攻击、恶意软件植入等方式，从企业数据库窃取公民个人信息，用于电信诈骗、身份冒用等违法犯罪活动，严重威胁了公民的财产安全。除此之外，还存在不少公民利用大数据作出的侵权行为，例如 2008 年中国的“人肉搜索”司法案例，有公民整合分析并公布他人的数据信息，产生了种种流言蜚语，且对其名誉权及隐私权造成伤害。

2.2. 数据存储与传输中的安全隐患

大数据的发展使得众多机构和平台已经积累了公民的数据信息，但是部分数据存储的场所的安全防

护措施却十分薄弱,单一的服务器防护手段使得黑客能够轻易突破安全防线,将网站中关于用户的隐私信息都窃取。数据在存储过程中,也会由于员工权限设置缺乏严格的细分与监督,导致一些不法分子可能会利用漏洞,获取公民的隐私数据。同时,云计算的广泛运用也使得数据在不同的服务器和云端之间频繁传输,传输的路径也错综复杂,难以做到全面监控,只要某个环节出现问题,公民的隐私数据就会被侵犯。以数据为核心特征的数字技术社会,数据驱动方法的广泛应用及大数据具有的多维度和全面性的特征,能够从大量看似支离破碎的信息中完全复原并了解到此人生活的细节或组织内部的各种信息[2]。这样就给不法分子实施违法犯罪活动有了可乘之机,严重干扰个人的正常生活,甚至危及个人财产安全。

3. 我国公民隐私保护困境成因分析

罗尔斯在《正义论》中指出:“正义是社会制度的首要价值。”[3]在大数据技术蓬勃发展的当下,这句话的意义愈发凸显。大数据技术给我们带来便捷高效的同时,也引发了重重危机,这些危机可能会冲击社会正义的基石。民众在享受数字技术便利的同时,往往忽略自我隐私的保护,对潜在风险缺乏警惕;许多企业由于缺乏相关的规范,导致数据滥用,侵犯公民隐私;而大数据本身也存在难以忽视的缺陷,技术漏洞与管理漏洞相互交织,使得公民隐私暴露在危险之中。

3.1. 民众自我保护意识薄弱

很多公民对个人的个人数据的敏感度不足,在日常生活中随意分享个人信息,比如为了获取小礼品,轻易扫码填写个人的姓名、电话、身份证号等重要信息;在网络上,对各类来路不明的调查问卷毫无戒备,如实填写家庭住址、收入状况等隐私内容;在社交媒体上,将个人动态、位置地址、家庭环境等完全公开,全然不知这些信息可能被不法分子恶意收集与利用。因此,一旦个人隐私遭到侵犯,公民往往因缺乏应对能力,难以采取恰当手段维护自身权益,而当前信息保护形势严峻,面临着内部管理不善与外部恶意侵扰的双重困境。在日常生活里,我们应当审慎判断何时向他人提供个人信息,以此降低隐私泄露风险,规避可能出现的不良后果。

3.2. 行业规范不足导致数据滥用

在如今的数字时代,数据已然成为核心资源,为经济发展、科技创新和社会进步提供强大动力,然而数据滥用的现象屡见不鲜,许多企业在追求利益最大化的驱使下,无视公民的数据权益,肆意收集、挖掘甚至贩卖公民的数据,将公民的隐私当做谋取暴利的工具,从最基础的个人信息,如姓名、身份证号、联系方式,到更为敏感的消费习惯,包括日常消费的品类、频率、金额偏好,以及社交生活中的社交圈子、兴趣爱好、人际关系等内容,无一不被纳入其收集范围。这些敏感隐私数据一旦被泄露和滥用,将会给公民带来极大的危害。对公民个人而言,隐私泄露可能导致骚扰电话、垃圾邮件不断,个人生活被严重干扰;更有甚者,可能会面临诈骗风险,个人财产安全受到威胁,甚至在极端情况下,个人的名誉、人身安全等也会陷入危险境地。此外,这种数据滥用不仅会侵犯公民的隐私权,而且还破坏了市场的公平竞争环境,企业利用非法收集的数据优势进行不正当竞争,运用数据分析对消费者进行差别化定价,或者利用用户进行针对性精准营销等等行为,这些不正当行为不仅不利于消费者的权益,而且还阻碍市场的良性、健康发展。

3.3. 大数据技术自身存在安全缺陷

收集数据的过程本身就存在着泄露公民隐私的潜在风险,大数据采集行为的合规性操作并不能消除隐私泄露的底层风险,即使行业员工是按照一系列规范化流程收集数据,但是仍然无法避免泄露信息的风险。因为互联网收集信息还有大数据技术本身就存在安全风险,这容易导致个人信息泄露和隐私大数

据技术应用的各个阶段都存在个人信息泄露的可能性。在大数据时代，数据安全威胁和风险已经渗透到大数据产业链的每一个环节，这些风险复杂地交织在一起，包括外部攻击和内部泄漏，而技术漏洞和管理漏洞既有新技术应用带来的新风险，也会有传统网络安全风险等等。

4. 完善公民隐私权法律保护的应对策略

完善公民隐私权法律保护策略，能切实保障公民人格尊严与财产安全，规范行业秩序，促进大数据产业健康、有序、可持续发展，因此探讨大数据时代公民隐私权保护的应对策略就显得尤为重要。

4.1. 增强公民的隐私保护意识

大数据环境下，公民更应该提升自身的隐私保护意识，自觉加强个人信息保护的措施，我们可以从以下方面加大对公民的隐私权保护法律知识的宣传力度：在电视、广播等媒体可开设专门的法治节目，邀请法律专家解读隐私权相关法律法规，结合实际案例，深入浅出地剖析隐私侵权行为的特点、危害及法律后果，让观众直观认识到保护隐私权的重要性；报纸、杂志则可设立法治专栏，定期刊登隐私权保护的科普文章、政策解读以及典型案例分析，以文字形式加深读者对相关法律法规的理解。互联网平台更是法治宣传的主阵地，我们需要利用社交媒体的强大传播力，制作生动有趣的短视频、图文漫画等内容，以通俗易懂、诙谐幽默的方式普及隐私权法律知识，吸引大量网民关注和学习。同时，各大网站、论坛可举办线上隐私权保护法律知识讲座、问答活动，鼓励网民积极参与，在互动中提升法律素养。与此同时针对不同的群体，我们也要开展精准化法治宣传教育：学校要将隐私权保护纳入法治教育课程体系，可以通过课堂教学、主题班会、模拟法庭等形式，培养学生的隐私保护意识和法律观念；对于企业的员工，可以开展入职法治培训、定期法律讲座等等，使员工们能够了解企业数据处理中的法律责任，从而避免因工作失误侵犯公民隐私权；深入社区、农村也是必不可少的重要途径，需要组织大量的法律志愿者开展面对面的普法宣传活动，发放宣传手册，现场解答居民关于隐私权保护的疑问，从而提升基层群众的法律意识，全方位拓宽法治宣传教育途径，让隐私权保护法律知识深入人心。

4.2. 加强行业规范

侵犯互联网用户个人隐私的重要渠道之一是通过网络设备，我们应当制定规则和准则来规范相关行业，尤其是针对网络运营商和服务提供商，因为这些实体拥有获取信息的广泛渠道，并能够获取大量个人隐私信息，特别重要的是要加强对这两个领域的管理，从而在问题发生之前加以防范[4]。确立统一且严格的数据收集规范是一个重要的前提条件，每个行业都需要明确规定收集公民数据的目的、范围和方法，因为隐私保护不仅是当代伦理体系中的一个普遍原则，也是大数据技术领域职业道德的基本原则[5]。企业在开发应用程序时，只能收集与应用核心功能直接相关的数据，不得过度索取权限，并且，在收集数据前必须以清晰、易懂的语言告知用户收集目的、用途及存储期限，从而确保用户真正知情并自愿同意。严格规范数据访问权限管理是关键所在，要依据员工工作职能精准分配数据访问级别，杜绝权限滥用现象，对于数据传输这个重要环节，行业应推行高强度加密传输标准，所有涉及公民隐私数据的传输，都必须采用符合安全规范的加密算法，保障数据在传输过程中的保密性与完整性。通过全方位加强行业规范，形成良好的数据治理生态，切实保护公民隐私权，促进行业健康有序发展。

4.3. 提升大数据安全技术研发运用

保护大数据时代公民的隐私安全风险，在技术层面提高大数据安全维护能力也至关重要，这是应对数据隐私风险、保障公民权益的核心举措。通过加强大数据安全技术的研发，鼓励科研机构与相关企业合作，攻克关键技术难题，提高收集者在数据的存储、传输过程中的安全性，从而提高用户在数据使用

中的安全与保障。可以将最新的大数据安全技术能够应用于数据收集、传输、存储和使用的整个过程中，从而通过技术进步来促进信息安全，并防止公民隐私的泄露。数据加密技术犹如给公民的数据穿上了坚固的铠甲，在数据使用过程中，会将传输的数据转化为一串乱码，确保信息的安全传输。此外，还可以强化身份认证技术，大力推广多因素身份认证技术，并结合诸如生物识别技术以及动态验证码等多种方法，为用户登录和数据访问设置多重关卡，在数据使用阶段，可采用防火墙、入侵监测、防病毒、防 DDoS、漏洞扫描等数据安全防护技术[6]。建立大数据安全漏洞检测和修复机制也是必不可少的环节，如此一来便可以通过对大数据系统进行安全检测，从而及时发现并且能够修复技术漏洞，确保新技术在应用前能够有充分的安全测试，这样可以降低数据的收集、存储、运输和共享过程中安全风险，能够大大降低隐私泄露的风险，为个人的数据安全增添了一道坚实的屏障，确保个人数据在使用过程中不会成为隐私泄露的源头。

5. 结语

大数据时代是信息爆炸增长的时代，虽然人们的生活水平得到了极大的提升，但是隐私侵权行为也给人们的生活带来了很大风险。展望未来，平衡法律信息公开与公民的隐私权是需要多方面协同发力、全方位综合措施来保障，共同营造一个更加公正且充分尊重个人隐私权的社会环境，帮助公民了解法律进程，为构建和谐、有序的法治社会添砖加瓦。

参考文献

- [1] 金元浦. 大数据时代个人隐私数据泄露的调研与分析报告[J]. 清华大学学报(哲学社会科学版), 2021, 36(1): 191-201.
- [2] 张媛媛. 论数字社会的个人隐私数据保护——基于技术向善的价值导向[J]. 中国特色社会主义研究, 2022, 36(1): 52-59.
- [3] [美]约翰·罗尔斯. 正义论[M]. 北京: 中国社会科学出版社, 1988: 46-47.
- [4] 王英哲. 大数据时代文献分析与利用[J]. 石家庄职业技术学院学报, 2014, 26(2): 53-56.
- [5] 王勇, 王蒲生. 大数据征信的隐私风险与应对策略[J]. 自然辩证法研究, 2016, 32(7): 118-122.
- [6] 陆英. 大数据安全防护方法与建议[J]. 计算机与网络, 2019, 45(7): 50-51.