

大数据时代隐私权保护研究

李沛儒

新疆财经大学法学院, 新疆 乌鲁木齐

收稿日期: 2024年5月17日; 录用日期: 2024年5月29日; 发布日期: 2024年7月17日

摘要

随着人类社会的发展步入数据时代, 个人隐私权等合法权益受到了极大地威胁。本文将在分析现有法律和执法情况的基础上, 总结大数据时代隐私权保护存在的现行法律的适用性缺陷、行政执法缺乏合力、以及大数据技术安全性的不足。针对当前法律存在的缺陷, 在参考域外隐私权保护做法的基础上, 建议重新界定隐私边界, 充分考虑人格利益和财产利益, 加强监管和执法力度。针对行政执法缺乏合力的问题, 建议加快构建合理高效的行业自律体系, 灵活化的公共管理职能, 以及完善权利救济机制, 形成全方位的执法合力。针对大数据技术存在的安全风险, 建议在全面推广加密存储的基础上, 对公民姓名、身份证号等敏感信息以密钥、算法等方式进行脱敏, 以保障数据的安全传输和存储。通过这些对策建议, 希望能为隐私权保护法律体系的完善和行政执法的有效实施提供参考。

关键词

大数据, 个人隐私, 法律制度

Research on Privacy Protection in Big Data Era

Peiru Li

School of Law, Xinjiang University of Finance and Economics, Urumqi Xinjiang

Received: May 17th, 2024; accepted: May 29th, 2024; published: Jul. 17th, 2024

Abstract

With the development of human society into the data era, personal privacy and other legitimate rights and interests have been greatly threatened. Based on the analysis of existing laws and law enforcement, this paper will summarize the applicability defects of existing laws for privacy protection in the era of big data, the lack of synergy in administrative law enforcement, and the insuf-

文章引用: 李沛儒. 大数据时代隐私权保护研究[J]. 法学, 2024, 12(7): 4400-4406.

DOI: 10.12677/ojs.2024.127625

efficient security of big data technology. In view of the defects in the current law, it is suggested to redefine the privacy boundary, fully consider the interests of personality and property, and strengthen supervision and law enforcement based on the extraterritorial privacy protection practices. In view of the lack of joint force in administrative law enforcement, it is suggested to speed up the construction of a reasonable and efficient industry self-discipline system, flexible public management functions, and improve the rights relief mechanism to form a comprehensive law enforcement joint force. In view of the security risks of big data technology, it is suggested that on the basis of comprehensively promoting encrypted storage, sensitive information such as citizens' names and ID numbers should be desensitized by means of keys and algorithms, so as to ensure the safe transmission and storage of data. Through these countermeasures and suggestions, we hope to provide reference for the improvement of the legal system of privacy protection and the effective implementation of administrative law enforcement.

Keywords

Big Data, Personal Privacy, Legal System

Copyright © 2024 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

随着互联网、社交媒体、移动应用等技术的迅速发展，个人数据的收集、存储和分析能力呈现出前所未有的规模和深度，从而引发了对隐私权保护的需求。在当前的大数据时代，人们在体验数字化带来便利的同时，公民的隐私权也相对地受到前所未有的威胁。隐私权的概念并不是一成不变的，其会随着时代的发展不断丰富，隐私权保护的方式和途径也需要与时俱进[1]。大数据的应用涉及多方面的数据收集、交叉分析和利用，这使得传统法规的适用性变得模糊不清。因此，有必要对现行法律体系进行审视，以适应大数据时代对隐私权保护的新要求。

2. 大数据时代隐私权概述

(一) 大数据时代的内涵

大数据时代是指在当前科技快速发展的背景下，由大量数据的产生、收集、存储、处理和应用所构成的一个全新发展阶段，其主要特征表现为数据量的激增，数据类别的多元化，数据分析的效率以及精准度等。按照目前学界主流观点，大数据时代的内涵可分为三个维度，首先是在数据量方面逐年激增，并且大数据并不仅仅包括传统意义上的结构化数据，还涵盖了传感器数据、媒体数据等非结构化数据，这使得人们面临前所未有的数据量，从而能够进行更全面、深入的分析和预测。其次，数据种类多样，大数据时代所涉及的信息形态日益复杂，包括文本、图像、音频等多媒体数据，这要求人们拥有更强大的处理和分析能力，以从多个维度理解数据。最后，数据处理高效性，大数据技术的应用使得数据的处理速度大幅提升，从而能够实现快速分析和决策。这种高效性为科学研究、商业运营、社会管理等领域提供了更广泛的应用可能性[2]。在大数据时代，数据被认为是一种重要的生产要素，其应用不仅能够各个领域带来创新，同时也带来了隐私权保护等伦理和法律问题的新挑战。

(二) 大数据时代隐私权的内涵

隐私权是个体对其个人信息享有的权利，涵盖了个体对于个人生活、家庭、通信等方面的隐私和私

密信息的保护[3]。隐私权是一种基本的人权，法律体系通常通过隐私法规和相关法律来确保对这些权利的保护，以维护个体的尊严和自由。自2020年《民法典》正式实施之后，我国以成文法的形式对法律层面的隐私权益进行了明确的界定，即任何个人、法人以及非法人性质的组织机构均不得以泄露、盗取、未经允许的公开等方式破坏他人生活秩序或他人主观意愿上不愿为公众或特定群体所知的私密信息或行为。但是需要正视的是，随着大数据技术在社会生产生活中的应用，隐私权的内涵经历了深刻的变革[4]。

3. 大数据时代隐私权保护的立法现状

(一) 立法现状

我国在网络隐私权保护方面尚存在一些不足，目前主要依赖于普通网络监管法规的执法，缺乏完整的网络隐私权保护法律文件。《宪法》作为我国的基础性大法，为隐私权法律制度体系的确立提供了必要的依据，规定公民人格尊严以及通信自由等权益属于法律保护的范畴，这也是网络隐私权法律法规制定的法理基础[5]。2020年之前，作为我国民法法典性质的《民法通则》虽然没有以法律条文的形式对公民的隐私权进行明确的界定，但是最高法出台了相关的司法解释，将隐私权作为公民名誉权的一种具化形式，网络隐私权的侵权及救济适用于名誉权的相关法律规定。我国《个人信息保护法》第6条规定：“处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。”部门规章方面，国务院和公安部发布的相关规定也对网络隐私权的保护提供了基本法律支持。

(二) 大数据时代隐私权保护的新变化

(1) 隐私内容更加广泛和复杂

传统隐私权主要关注个体基本身份信息的保护，然而，随着大数据技术的广泛应用，涉及个体的数据呈现了前所未有的广度和复杂性。大数据时代的信息收集范围扩展到了个体的日常生活、社交网络、健康状况、购物习惯等多个领域，形成了一个庞大而细致入微的数字画像。这使得传统的隐私保护框架难以全面覆盖和应对，迫使法律界重新思考如何保护个体在数字空间中更为广泛和复杂的隐私内容，以确保其信息不受滥用和侵犯[6]。在这一背景下，大数据时代的隐私权保护需要更加全面、灵活的法律机制，以适应不断扩展的隐私内容范围。

(2) 隐私侵权的方式更加隐匿

《民法典》第1034条规定：“自然人的个人信息受法律保护。个人信息中的私密信息适用有关隐私权的规定。”在一定程度上，个人信息与隐私权有着很紧密的联系[7]。《民法典》顺应社会发展，以近年来发生的热点事件为时代背景，采用否定性方式列举了隐私权被侵犯的具体行为类型，如：以电话、短信、即时通讯工具、电子邮件、传单等方式侵扰他人的私人生活安宁。盗摄、窥视、窃听、公开他人的私密活动等。随着科技的不断进步，大数据时代催生了更为隐秘的隐私侵权方式。个人信息的不经意流失、隐蔽的数据跟踪以及复杂的算法分析等手段使得个体难以察觉和抵御隐私侵犯[8]。这种更为隐匿的隐私侵权方式增加了隐私权保护的难度，要求法律体系更具适应性和前瞻性，以有效打击这些隐匿性更强的隐私侵犯手段。随着技术的不断发展，法学领域需要不断创新和完善法律规定，以确保个体在数字化社会中能够更加有效地保护个人隐私权。

(3) 隐私侵权的后果更为严重

《民法典》第1032条规定：“自然人享有隐私权，任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权”。可见公民的隐私权受到侵害会导致其隐私信息在未经本人同意的前提下被第三方公开、泄露，进而使其生活秩序受到破坏[9]。在此过程中，权益人的人格利益或财产权益会受到一定程度的损失。《刑法》第253条规定：“违反国家有关规定，向他人出售或者提供公民个人信息，

情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金”。《民法典》第 1195 条规定：“网络用户利用网络服务实施侵权行为的，权利人有权通知网络服务提供者采取删除、屏蔽、断开链接等必要措施，通知应当包括构成侵权的初步证据及权利人的真实身份信息” [10]。

4. 大数据时代隐私权保护面临的主要困境

（一）现行法律的缺陷

现有的隐私边界界定方法，如：所有权归属、链接控制权等已经不再适应当今数字化社会的复杂情境。控制边界链接的规则因公共场所监控设备的普及而受到挑战，导致了公民在离开家门时无法有效控制个人信息的流出。监控摄像头、购物中心的监视系统等无处不在，公共空间中的信息无法避免地被收集，使得原本自主选择与谁交流的权利受到了削弱。随着技术的发展，信息收集的方式变得越来越隐蔽，个体越发难以了解自己哪些信息被泄露，使得掌握边界渗透的难度大幅增加。明确边界所有权的规则在现实中面临难以确定的难题，法律在界定隐私的具体范围和合法使用之间存在模糊的灰色地带，数据收集者可以通过各种手段找到合理的借口，证明其行为是合规的，形成了法律上的漏洞。

（二）行政执法没有形成合力

随着大数据技术的广泛应用，不同地区和不同行业对隐私权的法规和执法标准呈现出显著的差异，从而导致了执法的不一致性和不协调性。一些发达地区更早关注到隐私权保护，制定了较为严格和先进的法规，而一些相对欠发达的地区在这方面的法规体系相对薄弱。这使得隐私权在不同地区的保护水平存在差异，公民在信息处理中面临的法律环境也参差不齐。此外不同行业在对待隐私权的态度和实践上也存在明显的差异。一些行业尤其是涉及大量个人信息的互联网科技公司，更加注重隐私权的合规保护，制定了相应的隐私政策和操作规范。然而，一些传统行业或者信息采集较为频繁的行业，由于缺乏足够的法规引导或自律机制，对于隐私权的保护相对滞后，容易出现个人信息滥用的情况。这种行业间的差异导致了执法难以形成统一的标准，也使得公民在不同行业间的隐私保护体验存在较大落差。即使是在注重隐私保护的互联网行业，虽然国内互联网行业自律体系已日趋成熟，相继制定并出台了《互联网行业自律公约》、《网站运营公约》等行业规范，但与迅速增长的互联网企业相比，签署和执行这些公约的企业数量相对较少。这导致了自律公约的覆盖面相对狭窄，难以在整个行业范围内形成有效的规范和监督。而且，这些自律公约并非法律法规，因此缺乏法律的强制力。

（三）大数据技术的安全性缺乏保障

由于互联网的通达性，隐私数据的来源较为多元，企业法人、公益性社会组织、政府职能部门以及各类网络平台均有可能以合法方式采集或存储公民隐私信息。而个人隐私权的侵权行为主体也可以是个人或组织机构。而信息技术的发展，使得非法采集、窃取个人隐私数据的方式也趋于多样化，如拷贝、下载、直接购买他人隐私内容等。大数据强大的挖掘技术使得个人隐私能够被轻松获得，这为不法分子提供了滥用数据的机会。

5. 大数据时代隐私权保护的对策建议

（一）完善相关法律规定

在大数据时代，隐私权保护面临着诸多挑战，主要源于现行法律的缺陷和滞后性。传统的隐私概念与数字化社会的复杂情境不相适应，法律框架未能有效定义隐私范围和维护个体权益，导致难以界定合理使用和侵犯隐私之间的法律灰色地带。为了解决这一问题，需要完善相关法律规定，确保隐私权得到有效保护。

(1) 重新界定隐私边界

传统的隐私边界规则已经无法适应当今数字化社会的需求，针对控制边界链接、掌握边界渗透和明确边界所有权等方面的挑战，应该重新界定隐私边界，以应对技术发展带来的挑战。建立更严格的监管机制，限制公共场所监控设备的使用，并规定数据收集者在采集前需获得数据主体的同意或授权；要求数据收集者向个体清晰地披露信息收集行为，并提供个体能够理解和控制的方式。另外，修订法律，明确个体对于自身信息的所有权，并规定数据收集者在使用个人信息时必须遵守相关规定，确保个体信息不被滥用。重新界定隐私边界可以使法律规定更加贴近现实情况，有效保护个体隐私权益。

(2) 充分考虑人格利益和财产利益

《民法典》将人格权独立成编并对隐私权作出了明确规定，这在我国民法发展历程中具有里程碑式的意义。加强对敏感个人信息的保护，针对个人身体状况、健康信息、财务状况等敏感个人信息，采取更加严格的保护措施，限制数据收集者对这些信息的获取和使用，确保个体的人格和财产利益不受侵犯，包括加强对这些信息的安全存储和传输要求，以及对违法获取和使用这些信息的行为进行严厉处罚。此外，在保护个体隐私权益的同时，允许合理的信息共享，促进信息的流动和利用，为此，建立信息共享的法律框架和规范，明确合法的信息共享渠道和方式，并对信息共享过程中可能涉及到的隐私问题进行规范和保护，确保信息的合法、合理使用平衡信息共享和隐私保护之间的关系，允许合理的信息共享，同时保护个体的隐私权益，确保信息的合法、合理使用。

(3) 加强监管和执法力度

当前存在的法律漏洞和灰色地带部分源于监管和执法不力，为了弥补这一缺陷，应加强监管机构的建设与运作，监管机构拥有充足的人力和物力资源，具备对大数据时代隐私权保护问题的专业化、全面化监管能力，并且需要建立有效的监测和检测机制，及时发现和应对隐私权侵权行为。对于涉及隐私权保护的新技术和新业态，监管机构应该及时跟进，确保监管工作的及时性和有效性。针对侵犯隐私权的违法行为，应该采取严厉的处罚措施，提高违法成本，增加违法者的法律风险，包括对数据收集者、数据处理者和数据使用者的处罚，如罚款、行政处罚甚至刑事责任追究，加大处罚力度，有效遏制违法行为的发生，维护个体隐私权益的合法权益。此外，执法机构应该严格执行相关法律法规，对侵犯隐私权的行为进行查处和制止，对于违法行为的举报和投诉，执法机构应该及时受理，并进行调查和处理。同时，执法机构还应该加强与监管机构的协作与配合，形成监管执法合力，确保隐私权保护工作的顺利开展。

(二) 注重行政执法之间的协作

(1) 推动行业自律体系建设

建立行业自律体系可以更好地满足不同行业的特殊需求，制定更为精准的隐私保护标准。相较于以原则性表述为主的法律制度，行业准则以及公约具有更为精细的颗粒度，可以为具体实践提供必要的依据，为企业提供明确的指导和标准。政府可以通过发布相关政策文件，明确支持各行业建立自律机构，并提供必要的支持和资源。鼓励行业组织主动成立自律机构，以参与隐私权的监管和维护。政府的引导和支持有助于加强行业自律的有效性，推动行业在隐私权保护方面迈出更为积极的步伐。行业自律机构可以由行业内的相关方共同组成，包括企业代表、专业从业者、学术界代表等。这种多方参与的机制有助于建立相对独立的监管体系，减少可能存在的利益冲突，提高隐私权监管的公正性和权威性。

(2) 完善权利救济机制

权利救济机制是否完备对权益人的维权具有决定性的影响。就目前现有的隐私权侵权案例而言，类案不同判以及受损权益难以获得充分救济的问题普遍存在，构建完善的权利救济机制可以有效的解决这一问题。政府可以通过公布最高院指导性案例，为司法实践提供指引，促使类案判决更为一致。同时，

设立专门的网络用户维权机构,提供专业化的法律援助和维权服务,增加维权渠道。此外,提高隐私权侵权成本,通过加大对侵权行为的处罚力度,使侵权者付出更高的代价,有助于形成对隐私权的有效威慑。这三方面的措施可以共同构建一个强有力的行政执法合力,有助于在大数据时代更为有效地保护隐私权。

(三) 提高大数据技术安全性

(1) 增强存储数据加密技术

借助于加密算法对数据进行加密是目前应用较为广泛的数据安全防护方式。加密算法可分为对称加密及非对称加密两种类别,二者的区别主要表现为所使用的密钥不同,但均显著加强了数据的安全性。采用这些算法可以有效地防止未经授权的访问和窃取。定期更新密钥是保障存储数据安全性的关键步骤,定期更换密钥可以降低因长时间使用相同密钥而导致的密钥泄露风险。密钥的定期更新可以通过自动化的密钥管理系统来实现,确保密钥始终具备足够的复杂性和安全性。此外,建立完善的密钥管理系统也是不可忽视的一个环节。密钥管理系统需要确保密钥的生成、分发、存储和注销等操作都在受控的环境中进行,以防止密钥被不法分子窃取或滥用。密钥管理系统还应该有足够的监控和报警机制,以便及时发现和应对潜在的安全威胁。

(2) 应对敏感数据进行脱敏处理

脱敏是目前最为有效的敏感数据保护方式之一,《个人信息保护法》中对于敏感信息进行明确解释,提出专门的处理规则。数据脱敏是一种通过特定规则对原始数据进行变形或修改的方法,以在某些不可信的环境中保障数据安全流通。通过脱敏处理,敏感数据失去直接的可识别性,从而减小数据被滥用或恶意利用的潜在风险。采用先进的脱敏算法、建立科学的脱敏规则,并通过技术手段监测和验证脱敏效果,都是确保数据安全性的关键手段。加强对敏感数据的脱敏处理,既可以维护隐私权,也有助于促进大数据的安全应用和合理流通。

6. 结语

在大数据时代,隐私权保护不断面临新的挑战,同时也呈现出一系列的问题。为此,本文主要提出以下三个建议:第一,在法律适用性方面,需要重新界定隐私边界,充分考虑人格利益和财产利益,加强监管和执法力度。第二,为了形成更强有力的行政执法合力,建议推动行业自律体系建设、活用政府行政管理职权,并完善权利救济机制。第三,在技术层面,可以加大对加密技术的研发力度,并鼓励数据使用者对数据进行加密或脱敏,进一步保障数据安全。希望通过本文可以切实帮助我国大数据时代隐私权保护在未来赢得更好的发展。

参考文献

- [1] 郑智婕, 黄子漩. 大数据时代隐私权保护的困境与破解[J]. 法学(汉斯), 2023, 11(4): 3035-3040.
<https://doi.org/10.12677/OJLS.2023.114434>
- [2] 邹开亮, 丁稳. 大数据时代劳动者隐私权保护路径构造[J]. 价格理论与实践, 2022(10): 60-65, 212.
- [3] 陈纯柱, 王唐艳. 大数据时代精准广告投放的隐私权保护研究[J]. 学术探索, 2020(4): 105-112.
- [4] 狄振鹏, 姜士伟. 大数据时代政府数据开放与公民隐私保护问题研究[J]. 情报杂志, 2022, 41(2): 155-159, 118.
- [5] 高志宏. 大数据时代个人信息保护的反思与规则优化[J]. 学术界, 2023(7): 122-137.
- [6] 吴春晓. 大数据环境下隐私权的法律保护——评《大数据时代隐私保护的挑战与思考》[J]. 中国科技论文, 2020, 15(6): I0018.
- [7] 徐璐, 钟涛, 潘禹辰, 卢小宾. 大数据时代招聘平台用户数据隐私保护研究[J]. 情报理论与实践, 2022, 45(12):

68-75.

- [8] 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.
- [9] 董淑芬, 李志祥. 大数据时代信息共享与隐私保护的冲突与平衡[J]. 南京社会科学, 2021(5): 45-5270.
- [10] 刘泽刚. 大数据隐私权的不确定性及其应对机制[J]. 浙江学刊, 2020(6): 48-58.