

【社会现象与社会问题研究】

# 大数据背景下公民隐私保护的困境及其对策<sup>\*</sup>

张 铤 程 乐

**摘 要:**大数据技术在给人们带来价值和便利、增进社会进步与福祉的同时,也对公民隐私保护产生巨大挑战,导致公民隐私保护面临一系列现实难题。大数据技术自身存在安全缺陷、新技术条件下隐私保护伦理准则尚未达成以及个人隐私保护立法实践相对滞后是产生公民隐私保护困境的主要原因。对此,要通过加强大数据安全技术研发运用、构建大数据时代隐私保护伦理准则和完善个人隐私保护相关法律法规等系列对策,有效化解大数据时代公民隐私保护的困境。

**关键词:**大数据技术;隐私权;隐私保护

**中图分类号:**G124

**文献标识码:**A

**文章编号:**1003-0751(2021)02-0092-04

随着互联网、物联网和云计算等数字技术的飞速发展,大数据时代已经到来。大数据技术的广泛应用给人们带来了价值和便利,增进了社会进步与福祉。然而,与此同时,大数据技术在信息安全、数据垄断、数字鸿沟和隐私侵害等方面给公民隐私保护构成了巨大挑战。在此背景下,重新审视公民隐私保护这一历久弥新的问题,分析大数据环境下公民隐私保护的困境及其成因,进而提出有效化解策略,不仅具有理论意义,更具实践价值。

## 一、大数据时代公民隐私保护的现实困境

大数据技术在极大促进高新科技发展的同时也加剧了公民隐私保护问题的衍化,给公民隐私保护带来越来越大的挑战。大数据环境下,公民权利保护与隐私泄露的矛盾日益显现,数据垄断与数据鸿沟的扩大危及社会公平正义。然而,无论是政府对大数据行业的监管水平,还是相关企业履行社会责任的程度,都亟待提升。

### 1. 公民权利保护与隐私泄露的矛盾日益显现

根据美国学者沃伦与布兰代斯在《论隐私权》

一文中的界定,隐私就是“免受干扰而独处”的权利。<sup>①</sup>通俗地讲,个人隐私就是指个人不愿与人分享或希望在很有限的范围内分享的信息。隐私权是现代人格权利。由于大数据技术具有数据规模大、处理快、类型多和价值大等特征,私人领域的很多信息被高度数据化,要获取个人隐私,只要掌握大数据就能够实现。这预示着大数据时代个人隐私已无处“躲藏”,随时都有被泄露的风险。在大数据时代,大数据成了重要的资源,能不断被挖掘和二次利用。虽然已出台一些规则要求相关数据经过模糊化、匿名化处理,使用者须履行告知义务,但大数据技术应用的现实情况仍不容乐观。如有国外学者指出:“不管是告知与许可、模糊化还是匿名化,这三大隐私保护策略都失效了。”<sup>②</sup>实际上,即使相关数据经过模糊化、匿名化处理,人们的隐私也可能以另外的方式被泄露,因为在大数据时代,相关关系取代了因果关系。在对庞大数据进行分析的基础上,大数据具有“预测”功能。一些企业利用大数据的这一功能大肆开展“精准营销”,往往不惜侵犯他人隐私。例如,《纽约时报》曾报道美国折扣零售商塔

收稿日期:2020-11-12

<sup>\*</sup> 基金项目:国家社会科学基金重大项目“建立健全我国网络综合治理体系研究”(20ZDA062)。

作者简介:张铤,男,南京大学政府管理学院博士后研究人员(南京 210023)。

程乐,男,浙江大学外国语言文化与国际交流学院副院长,教授,博士生导师(杭州 310018)。

吉特(Target)在不和某位女性面对面对话的前提下成功地预测出了该位女性怀孕的隐私并给她定期寄送相关优惠券。然而,大数据预测产生的巨大价值往往只是被数据搜集者和使用者占有,这是大数据技术的“另类异化”。数据能够不断被二次利用的特点,使我们很难真正守住隐私。<sup>③</sup>总之,大数据的价值实现与公民隐私保护之间存在强大的张力。大数据技术对公民隐私构成巨大威胁,影响技术与社会的和谐生态,导致个人隐私权利保护与隐私泄露的矛盾日益显现。

## 2. 数据垄断与数据鸿沟危及公平正义

大数据技术正在改变政府和企业行为,甚至影响社会结构和全球局势的发展。大数据时代,数据蕴含的巨大价值被进一步释放,尤其是在商业领域。开放共享是大数据技术发展和应用的内在要求,运用大数据技术应对复杂性、预测形势、做出合理决策的前提是数据的开放与共享。打破数据垄断,大数据技术才能实现更好发展。然而,由于社会分工、利益驱使和无序竞争等原因,当前大数据的价值获取、利用仍然存在严重的不平衡,对大数据的占有、分析能力和影响力上的“马太效应”正在形成。在个体层面,仅有少数人能很好地获得和利用大数据资源,造成“数据鸿沟”,导致信息红利分配不公等社会问题。在企业层面,一些互联网巨头垄断大数据资源,不合理地使用和分配大数据,既对公民信息安全造成巨大风险,也影响了市场公平竞争,损害了一些中小企业的利益。在国家层面,不同国家在全球互联网和大数据体系中的地位不同,少数国家聚集和垄断大数据技术平台与资源,导致国家间的数字财富差距越来越大,甚至在一定程度上造成“数据霸权”,危及社会公平正义,也使个人隐私保护处于越来越不利的境况。

## 3. 政府监管与企业社会责任履行效果欠佳

隐私权是重要的人格权利。市场监管是政府的重要经济职能,政府对大数据企业发展具有监管职责,对公民隐私权利有着不可推卸的保护义务。大数据时代,政府应采取有效的监管措施确保大数据企业规范有序发展。但是,由于当前政府监管机构职责分工的不明晰、大数据技术监管体系的不健全和大数据行业运作的特殊性等原因,政府部门对大数据企业监管的效果欠佳。对大数据企业而言,在发展和创新大数据技术的同时本应遵守法律法规,

加强行业自律,履行必要的社会责任。然而,由于大数据技术正处于发展初期,信息安全技术的不完善,制度规范的不健全,再加上政府有效监管的难度大,存在大量管理的“空白地带”,导致一些大数据企业疏于对公民信息安全的维护,加剧了大数据技术的应用风险。例如,当前数据非法交易已形成完整的产业链,“数据黑市”交易泛滥,针对用户信息的非法收集、窃取、贩卖和利用行为猖獗,严重侵犯了公民隐私权利。但是,在一些合法经营的大数据交易平台,数据资源供需矛盾突出,数据有效供给严重不足。某些征信公司在商业利益的驱使下,滥用大数据技术,导致公众信息泄露事件时有发生,对个人隐私造成严重侵犯。

## 二、大数据时代公民隐私保护困境的成因分析

### 1. 大数据技术自身存在安全缺陷

网络搜集和存储数据是大数据技术价值利用的前提。然而,这种广泛搜集数据的行为本身就存在信息泄漏的巨大潜在风险,与个人隐私保护存在很难调和的内在矛盾。即使大数据的使用者都征得数据生产者的同意,经过规范程序采集数据,仍然难以完全避免信息泄露的风险,因为运用网络信息搜索技术在互联网上大肆搜集信息过程本身就存在安全风险,极易造成个人信息和隐私泄漏。可以说,在大数据技术应用的每一阶段,都存在个人信息泄漏的可能。大数据时代,数据安全威胁和风险可谓渗透在大数据产业链的各个环节,这些风险成因复杂交织,既有外部攻击,也有内部泄漏;既有技术漏洞,也有管理缺陷;既有新技术应用带来的新风险,也有传统的网络安全风险。

### 2. 新技术条件下隐私保护伦理准则尚未达成

大数据技术作为一种新兴技术,它的出现改变了人们的日常生活和交往方式,对社会原有的伦理道德规范带来巨大挑战。生产关系是决定社会伦理道德规范产生和发展的主要因素。新的生产力导致生产关系的变化,原有的伦理道德规范应及时改变和调整。如果伦理道德规范与新的生产关系状况不适应,就会产生新的伦理问题。道德伦理准则是大数据技术发展的价值导向,大数据行业须有相应的道德伦理规范。然而,一方面,当前部分大数据企业从业人员不太重视信息道德伦理,信息道德素养不高。例如,某些大数据企业员工缺乏公民隐私保护

责任感,在大数据搜集和利用过程中安全措施不到位,导致公民信息轻易被公开、交易和使用,对公民隐私造成严重侵犯。另一方面,原有的道德伦理准则不能很好地应对新技术条件下隐私保护伦理问题。目前,大数据技术的应用已突破商业领域,在国家安全和军事领域也有很大的发展空间。在大数据技术应用过程中,如果个人隐私权利与国家安全、公共利益发生矛盾和冲突,那么隐私保护伦理问题的产生在所难免。因此,适应大数据技术等新兴技术的发展,赋予原有的道德伦理准则新内涵,构建大数据时代隐私保护新伦理准则,不仅必要,而且紧迫。

### 3. 个人隐私保护立法相对滞后

相对于大数据技术的快速发展,当前我国针对公民隐私保护的立法实践仍显滞后。尽管近些年我国出台了《中华人民共和国网络安全法》等法律法规,在大数据技术发展规范管理等方面发挥了明显作用。但是,由于大数据时代公民隐私保护问题层出不穷,且涉及诸多因素,颇为复杂。因此,公民隐私保护相关立法实践须与时俱进,适应大数据时代的发展要求。例如,大数据技术发展达到一定阶段,必然会鼓励和要求政府部门、科研院所和企业机构等更好地“分享”大数据资源。然而,“分享”大数据资源在产生价值的同时,也存在巨大的数据安全风险,因此需要相关法律法规对数据资源“分享”的要求、程序、范围和责任等做出详细规定,防范大数据“分享”过程中个人信息和隐私的泄漏风险。

## 三、大数据时代保护公民隐私权利的对策建议

当前,我国互联网用户规模已超 8 亿,在数据安全风险日益凸显的当下,保障数据安全、保护个人信息隐私值得高度重视。<sup>④</sup>大数据时代公民隐私保护问题的治理涉及多种因素,是一个复杂的“系统工程”。为此,需要多维并举,综合施策,积极应对。

### 1. 加强大数据安全技术研发运用

面对大数据时代公民隐私安全风险,既要在管理上确保大数据技术安全,也要善于运用技术控制手段提高大数据安全维护能力。因此,加强大数据安全技术的研发和运用至为重要。通过大数据安全技术攻关,可将最新的大大数据安全技术运用于数据的采集、传输、存储和使用等过程,以技术进步促进信息安全,防止公民隐私泄漏,弥补大数据技术自身存在的缺陷。例如,在数据采集阶段,可采用数据类

型、安全等级标注等措施,将数据安全功能提前嵌入到数据管理系统。在数据存储、传输阶段,可采用数据加密、磁盘加密、HDFS 加密等技术保障数据存储和传输安全。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。<sup>⑤</sup>除了传统的数据安全防护技术,账号权限管理、数据脱敏、数据安全域与终端数据防泄露等也是保障大数据安全的有效技术措施。此外,由于个人信息一旦被存储于数据库便难以被彻底删除,因此在数据存储和使用中可采用“到期日设计”技术,防范数据泄漏风险。

### 2. 构建大数据时代公民隐私保护伦理准则

大数据技术发展应体现社会道德伦理准则,承载人类的善和道德价值。大数据时代隐私保护问题折射出技术“双刃”效应背后工具理性与价值理性的断裂。技术发展带来的负面效应根本上是由于相关主体缺乏责任承担的结果,大数据技术引发的隐私保护问题亦是如此。因此,大数据时代公民隐私保护问题的伦理治理关键在于突出责任伦理。具体而言,大数据技术发展应加快构建权利与义务对等、创新与责任一致、个人权利与“公共善”结合等伦理准则。权利与义务对等准则要求大数据的搜集者、使用者在享有大数据带来丰厚利润的同时,承担更大的隐私保护责任。要坚持权责统一,贯彻“谁搜集利用谁负责”原则。大数据搜集者、使用者须对数据生产者履行必要的告知义务,对可能发生的隐私泄漏风险采取安全防护措施。如果隐私确实被泄漏,且造成伤害,那么责任方必须受到追责,承担相应的责任。大数据技术发展应坚持创新与责任一致的伦理准则。“隐私保护既是当代伦理体系中的一般原则,更是大数据技术职业伦理的基本原则。”<sup>⑥</sup>对大数据企业从业人员,必须加强职业伦理教育,增强他们的信息道德伦理意识。需要指出的是,大数据时代在保护公民隐私权的同时,要兼顾社会“公共善”。大数据技术发展应坚持公民权利与“公共善”结合的伦理准则,既要重视个人隐私权利的保护,也要推进大数据的价值共享,增进社会“公共善”。例如,政府部门在确保数据安全的基础上,有责任创建和完善数据开放平台,推进数据开放。政府部门既要重视大数据技术发展的经济政策、产业政策,更要关注社会政策,构建大数据技术社会支持体系,缩小“技术鸿沟”,提升公众对大数据技术的



参与感、体验感和获得感。此外,还要打破少数企业的“数据垄断”,构建大数据交换体系,推动大数据交换正常化。总之,政府部门和相关企业都有责任把大数据的价值延展到更广泛的公众层面。

### 3. 完善公民隐私保护的相关法律法规

由于相关规则的缺失,当前大数据技术正处于“野蛮生长”阶段,亟须完善公民隐私保护的相关法律法规,加强制度供给,构建大数据时代公民隐私保护制度体系,对大数据技术环境下隐私安全风险予以规制。具体而言,一是要求公民隐私保护立法体现制度伦理精神。大数据时代,公民隐私保护的相关法律法规要坚持“善治”的价值目标,坚守社会伦理道德底线,体现制度的正义性。诚如罗尔斯在《正义论》中所指出的:“正义是社会制度的首要价值。”<sup>⑦</sup>二是不断优化公民隐私保护相关法律法规的立法模式。当前,我国没有统一的公民隐私保护法,现有的相关法规制度较为分散,规则过于笼统、空泛,操作性不强。建议采用统一立法与分散立法结合的立法模式,在《中华人民共和国民法典》对隐私权和个人信息进行保护的基础上,加快制定统一的“个人信息保护法”“数据安全法”等法律,通过分散立法,为大数据技术和相关行业规范提供相应的操作细则和行业指南。三是不断细化隐私保护立法内容。要明确大数据时代隐私保护的内容、范围、程度和程序规则,细化数据采集、传输、存储和使用等阶段的信息安全要求,详细规定大数据搜集者、使用者等相关主体的权利和义务,完善大数据隐私侵权行为责任追究和惩处机制,使得大数据时代公民隐私保护真正做到有法可依、有法必依。四是不断完善政府数据监管制度和机制。政府要做好大数据信息

安全顶层设计,要以制度形式明确政府数据监管机构及其监管职责,整合相关部门的数据监管职能,建立公民隐私保护协同执法机制。政府要依法采取多元监管手段,“通过专项报告、不定期抽查、社会监督、电子监察、信用名录等多种方式进行事中事后规制,适时履行监管责任,从过程中阻断,实现公民隐私权保护”<sup>⑧</sup>。

保护大数据背景下的公民隐私,既是政府的职责,也是全社会面临的共同挑战。在加大隐私保护技术的开发与创新、加快隐私保护法治化进程、强化政府各级机关和各类数据公司隐私保护监管职责的基础上,还要高度重视大数据隐私保护高端专业人才的培养和利用,并在全社会开展全方位的道德教育,提升公众道德品质和隐私保护意识,着力构建大数据技术与社会的和谐生态,积极探索大数据时代公民隐私保护的“中国经验”。

### 注释

- ① Warren S. D., Brandeis L. D. The Right to Privacy, *Harvard Law Review*, 1890, Vol.4, No.5, p.193. ② [英]维克托·迈尔-舍恩伯格、肯尼思·库克耶:《大数据时代》,盛杨燕等译,浙江人民出版社,2013年,第200页。③ 陈仕伟、黄欣荣:《大数据时代隐私保护的伦理治理》,《学术界》2016年第1期。④ 杨可欣:《大数据时代的用户数据隐私保护》,人民网, <http://yuqing.people.com.cn/n1/2019/0813/c212888-31292715.html>, 2019年8月13日。⑤ 陆英:《大数据安全防护方法与建议》,《计算机与网络》2019年第7期。⑥ 王勇、王蒲生:《大数据征信的隐私风险与应对策略》,《自然辩证法研究》2016年第7期。⑦ [美]约翰·罗尔斯:《正义论》,何怀宏等译,中国社会科学出版社,1988年,第47页。⑧ 刘筱娟:《大数据监管的政府责任》,《中国行政管理》2017年第7期。

责任编辑:翊 明

## The Dilemma and Countermeasures of Citizen Privacy Protection Under the Background of Big Data

Zhang Ting      Cheng Le

**Abstract:** While big data technology brings value and convenience to people and promotes social progress and well-being, it also poses big challenge to the protection of citizens' privacy, leading to a series of practical problems concerning citizens' privacy protection. The facts that big data technology has security defects in itself, that privacy protection ethics has not been reached under the new technology conditions, and that the practice of personal privacy protection legislation lags behind relatively are the main causes of the dilemma of citizen privacy protection. To deal with this, we should strengthen the research and application of big data security technology, construct the ethical norms of privacy protection in the big data era and perfect the relevant laws and regulations of personal privacy protection, so as to effectively resolve the dilemma of citizen privacy protection in the big data era.

**Key words:** big data technology; privacy right; privacy protection