·学科前沿·

《学术界》(月刊)
总第242期,2018.7
ACADEMICS
No.7 Jul. 2018

互联网平台企业的网络垄断与公民隐私权保护
——兼论互联网时代公民隐私权的新发展与维权困境

○ 陈剩勇,卢志朋
(浙江工商大学 公共管理学院,浙江 杭州 310018)

〔摘 要〕移动互联网和信息技术的飞速发展为消费者提供了更便捷和舒适的网络服务,也增加了公民隐私权被侵犯的风险。近年来,以BAT为代表的互联网平台企业的兴起和扩张对公民隐私权构成了巨大威胁,具体表现为互联网平台在个人信息数据收集、使用、保护过程中对公民隐私权的种种侵权行为。互联网平台企业的网络垄断与公民隐私权保护之间的张力,主要表现为数据收集阶段互联网服务功能与信息供给之间的张力、数据使用阶段强大掌控者与弱小社会个体之间的张力、数据保护阶段立法规制滞后性与信息技术发展迅猛之间的张力,使传统公民隐私权的保护制度形同虚设。为应对互联网时代公民权利面临的新挑战,需要通过国家立法和市场监管,从扩充数据收集中用户主体的权利范围,加强互联网平台数据使用的内外监管,构建数据安全保护的技术与制度协同机制等方面,对互联网平台巨头的网络垄断和扩张行为加以必要的限制、规范和监控,以防范"数字利维坦"对公民隐私权带来的威胁和风险。

〔关键词〕互联网平台企业;网络垄断;数字利维坦;公民隐私权保护;限权与监管
DOI:10.3969/j.issn.1002-1698.2018.07.004

一、问题的提出与文献回顾

进入21世纪以来,随着信息技术和移动互联网的高速发展,各行各业都被卷入到互联网"跨界革命"的浪潮之中,谷歌、亚马逊、面簿等不同领域的互联网创新企业巨头在全球范围内迅速崛起。在中国,根据中国互联网络信息中心

作者简介:陈剩勇,浙江工商大学公共管理学院教授,浙江大学地方政府与社会治理研究中心主任;卢志朋,浙江工商大学公共管理学院行政管理专业硕士研究生。

(CNNIC)在京发布的第41次《中国互联网络发展状况统计报告》,截至2017年12月,我国境内外上市互联网企业数量达到102家,总体市值为8.97万亿元人民币,[1]业务主要涉及网络游戏、电子商务、文化传媒、网络金融和软件工具等领域,服务范围几乎覆盖了普罗大众"衣、食、住、行"和社会生活的方方面面。因此,互联网企业的一举一动都深刻地影响着消费者的行为模式。其中,百度、阿里巴巴、腾讯(通常简称BAT)三大互联网企业巨头,在引擎搜索、电子商务、即时通信等领域所占的市场份额都超过50%以上,三家企业的市值之和占了互联网企业总体市值的73.9%,[2]形成了互联网经济的垄断格局。近年来,三大互联网企业寡头通过地毯式的并购、山寨、参股等形式进行业务扩张和资源延伸,使得当前我国估值前30名未上市的互联网创业公司都充斥着它们的身影,[3]BAT俨然成了互联网经济和网络时代的"利维坦",即"数字利维坦"。

以BAT为代表的互联网平台巨头的兴起、发展和扩张过程,固然促进了互联网经济的大发展,为消费者带来了诸多便利,但其网络垄断的形成也为公民隐私权保护和维权埋下了巨大的隐患。一方面,信息化时代大数据、云计算和人工智能等技术的进步,使得互联网企业获取消费者隐私信息变得尤为容易;另一方面,网络信息传播的快速化和广泛性的特征以及网络行为的匿名化,使得网络侵权行为的后果远远超出了传统法律的管辖和控制。普通人在网络空间犹如"裸奔",不知不觉之间已把隐私权主动交出,网络侵权无所不在,网络维权困难重重。

2018年以来,BAT等互联网企业巨头相继陷入一场涉及侵害用户隐私的社会舆论旋窝之中。1月1日,吉利控股集团有限公司董事长李书福在公开场合谈及信息安全时,质疑"马化腾天天在看我们的微信",引起社会公众对自身隐私权的担忧。[4]1月3日,在朋友圈疯传的支付宝年度账单中,《芝麻服务协议》以极不显眼的方式诱导用户默认了对芝麻信用的授权,被质疑侵犯隐私权。[5]1月5日,百度因涉嫌侵害消费者个人信息安全而被江苏省消费者权益保障委员会提起公益民事诉讼。[6]实际上,这只是互联网企业侵犯公民隐私权的冰山一角。多起涉及互联网平台巨头侵犯公民隐私权的事件在同一时段密集发生,凸现出整个互联网行业在用户隐私保护方面令人堪忧的事实。

虽然腾讯、阿里巴巴和百度等三大巨头迅速对这三起纠纷都做出了积极回应,但由此引发的关于互联网企业巨头权力扩张与公民隐私权保护的社会舆论表明,互联网技术的迅猛发展不再只是一个科学技术和互联网行业发展的新现象,同时也是一个涉及到人类社会的经济形态、交往模式和法律规则等诸多方面的重要问题。在当前和未来可预期的一段时间里,随着物联网、大数据和人工智能三者的技术叠加,我们将会面临一个生活在"无隐私的社会"[7]中的厄运。面对信息时代日新月异的变革,如何应对互联网技术快速发展和"数字利维坦"市场垄断所带来的各种关于侵害公民隐私权的法律、政策和伦理风险,是当下社会各界包括公民、企业、政府关注的热点话题,也是政治学界无法回避的重大课题。

有关互联网企业对公民隐私权产生威胁的现象,近年来也逐渐进入了国内

外学者的研究视野。Subashini 和 Kavitha、Samson、Xu Heng 等众多国外学者都认为当前互联网企业发展面临的最大挑战在于如何有效地保护消费者个人隐私信息。[8]一些学者分别基于社会认知、利益及保护激励等理论模型的构建,或者通过调查互联网用户进一步讨论消费者隐私权保护行为的影响因素,发现消费者对隐私权保护的知晓[9]、逐利动机[10]、网络使用者对自己个人数据被收集的关注程度[11]、个人对被收集信息的控制能力[12]、对公司保护个人信息的能力评价[13]等因素会显著影响消费者的网络隐私权保护行为。此外,更多的学者着眼于解决实际问题,从技术角度设计了诸如 CSI 工事法[14]、K – 匿名法[15]、PE 三工具[16]、综合算法[17]等个人敏感数据加密的方式来保护消费者的个人隐私信息;从制度性监管层面提出了构建第三方公开审计[18]、完善消费者隐私权保护的框架与法规[19],以及建立消费者数据保护标准[20]等措施来防止互联网企业对公民隐私权的侵犯。

国内学者对互联网时代公民隐私权保护等相关问题的探讨,更多的是围绕政府这一主体而展开,涉及互联网企业巨头垄断侵权与公民隐私权保护的研究则相对较少,且以规范分析居多。王锐从公民信息保护与互联网企业利益平衡的视角出发,研究了当前我国个人信息隐私权保护法律存在的不足。[21]张茂月认为企业会利用互联网时代信息获取的便利性有意识地收集和分析个人信息数据以实现精准化营销,从而造成“信息收集知情权”“信息安宁权”“信息处分权”和“个人信息数据泄露”等四方面的“网络侵权”风险。[22]郑戈强调互联网技术的广泛应用对整个法律体系运作的重塑,掌握大数据的国家机关和商业机构与公民个人之间的权力关系也会因此而改变,个人会变得越来越透明,而数据权力行使者却变得越来越隐秘。[23]谢远扬和金耀等指出,当前我国互联网发展采取的是以同意规则为中心的消费者信息保护模式,这种模式对于公民隐私权的保护存在着诸多局限性,学者们提出了通过将知情理论嵌入到消费者与经营者关系之中,限制和缩小同意规则的适用范围,采用场景风险规则等建议,促使消费者权利规范向数据收集者的行为规范转变。[24]此外,方兴东、张静、刘国辉考察和分析了全球知名的互联网企业谷歌产品与用户隐私问题,指出随着谷歌企业用户数量的增长、创新领域的拓展、新隐私政策的出台以及产品智能化水平的提升,将会扩大用户个人隐私泄露的风险,因而需要政府和社会从政策、技术、用户等层面加以防范。[25]

以上学者的研究为互联网发展与公民信息隐私权关系的研究提供了基础,但对于互联网企业如何威胁公民隐私权以及信息技术对公民隐私权保护的冲击力度等方面的探讨显得有所不足。本文将围绕互联网平台巨头的兴起对公民隐私权的威胁这一主题,考察互联网时代公民隐私权保护面临的新形势,分析互联网平台在个人隐私数据收集、使用、保护过程中对公民隐私权的侵害及其深层次原因,探讨如何避免互联网平台的企业巨头在获取数据、使用数据和保护数据过程中对公民隐私权的威胁,以构建一个安全可信的信息消费环境。

二、从传统隐私权到信息隐私权:技术与社会互构中公民隐私权的演变

1890 年,美国学者沃伦和布兰蒂斯在《哈佛法律评论》上发表的《The Right to Privacy》一文中提出隐私权概念,认为隐私(privacy)是一种个人免于被陪伴和观察的状态,其对应的隐私权(right to privacy)表现为不得随意将与社会无合法关联之事项泄漏于公众和个人不受干扰的权利。[26]到了 1960 年代,威廉·普洛塞(William Prosser)系统梳理了 300 多起关于公民隐私权被侵犯的案例,将侵犯隐私权概括为侵扰私人生活安宁、盗用他人姓名或肖像、公开揭露他人私生活秘密、以公开的方式发布容易使公众产生误解的他人扭曲形象四种类型。[27]普洛塞的这些观点后来成为了《美国侵权法重述(二)》的基础,为美国侵犯隐私权的司法审判提供了标准。

经过 100 多年的发展与演化,尽管法律界和学术界对于隐私概念的界定尚存争议,但不可否认的是,传统的隐私权作为一种独立的民事权利在法律实践中已经达成基本共识。例如,在美国社会中,个人隐私权的正当性往往来源于“个人自由”这种公民最为重要的基本权利和核心价值的引申,[28]为了避免公民被他人压迫或操控,维护公民个人隐私成为了必要的选择,美国国会先后制定实施了《信息自由法》《隐私权法》《电子通信隐私法》等有关隐私权保护的相关法律,逐渐确立了隐私权的宪法地位。[29]相比于美国,欧盟似乎更重视人的基本权利和人类核心价值意识,其隐私权概念首先涉及的是个人的荣誉与尊严等人权要素,早在 1953 年颁布的《欧洲人权公约》,就明确规定了每个人有权在其私人事务、家庭、居所和通信等方面受到尊重。之后,欧盟又制定和出台了《欧盟基本权利宪章》等一系列隐私权保护的法律条例,进一步加强对公民隐私权的保护。当代中国对隐私权的法律规定相对较晚。1982 年制定的《民事诉讼法》(试行)是最初提及隐私的相关法律文件,2005 年修改的《妇女权益保障法》首次明确隐私权,2009 年出台的《侵权责任法》,全面确认了隐私权作为一项独立的权利规定,当今中国的隐私权前后历时二十多年而逐渐完善。由此观之,依照各个国家立法的发展变迁历程,作为公民基本权利重要内容之一的个人隐私权逐步取得了世界大多数国家的法律认同,成为一项超越民事权利的宪法性权利。

作为一种随着技术发展而变迁的开放性与扩充性的权利赋予,[30]公民隐私权是在技术与社会互构过程中不断加以改变的。随着互联网时代的到来,由于个人资料的电子化存储以及信息收集的简单化、低成本、高商业价值,使得公民隐私权遭受侵害的威胁日益凸显,传统的四分法隐私权理论面临着巨大的冲击。因此,出现了 Jerry Kang 所提倡的空间性、自治性和信息性三类的新型隐私权理论,[31]将强调个人不被打扰的消极性的防御型基本权利扩张到能够个人自我控制并决定信息的使用范围及其正确性、完整性的积极性的主动型人身权利。[32]此后,技术伦理学家塔瓦尼进一步将公民隐私权归纳为物理隐私、决策隐私、心理隐私与信息隐私四种类型,[33]推动了隐私权在理论层面上从传统隐私权向信

息隐私权演变的进程。

无论是隐私权的自我扩张,还是权利的补充,随着个人隐私边界和隐私权内涵的变化,人们不得不对信息化时代个人的隐私权益进行价值层面的反思、伦理层面的规范以及法律层面的规制,进而在社会管理实践和学术理论研究中审慎地思考和探寻互联网企业巨头的网络权力扩张与公民隐私权保护的应对之道。为此,各个国家都在探索对个人数据和信息隐私的保护措施以维护信息时代公民的基本权利和自由,防止政府机关和商业机构以违背公民意愿的方式滥用其掌握的信息资源谋取私利。

三、互联网平台网络垄断与公民隐私权面临的威胁及其表现

相比于传统企业自利性与服务性的特性,互联网平台企业为消费者带来便利化的服务以促进社会经济发展的同时,也会出于企业利益最大化的考虑,凭借云计算技术过度挖掘其掌握的个人数据背后所蕴藏的商业价值。与此同时,由于互联网平台企业的市场行为具有虚拟性、互动性、广域性和即时性等特点,加之互联网领域的市场垄断效应,使得消费者的信息往往被少数的互联网商业巨头所掌握。因此,信息时代互联网企业侵犯公民隐私的风险显著增大,其侵权行为远远超过了传统意义上隐私权侵害的共性特征,而更具有隐蔽性、复杂性,主要表现为数据收集过程中对消费者免受外界打扰的威胁、数据使用过程中对公民决策隐私权的威胁、数据保护过程中对个人数据处分权的威胁等新内容。

(一)互联网平台数据收集过程对消费者隐私权的威胁

免受外界打扰作为公民隐私权最原始的内涵,表明个人拥有在生活空间和心理空间免受打扰或干预的权利。但是,信息时代政府机关和商业机构可能会通过无所不在的摄像头、无孔不入的监听器、无处可逃的定位系统等高科技对公民个人生活空间造成干扰。判断使用此类技术是否侵犯公民隐私权往往以公共场所和私人场所作为界限依据,而现代科技早已突破社会生活场域的“围墙”“房屋”等传统的物理空间界限,[34]“公”“私”场所的界限也不再那么清晰,大量使用监控技术不可避免会给普通公民的日常生活造成干扰。例如,很多 APP 软件在提供服务的同时,基本都要求消费者出让读取识别码、调用摄像头、允许开启定位、打开运动数据等权限,如果拒绝的话可能无法正常使用该 APP 的功能。虽然,也有部分 APP 没有强制性要求用户同意调用请求,但如果用户选择跳过调用权限,下次再使用手机 APP 时,依旧会弹出调用权限的提示,反复提示直到用户同意调用权限为止。[35]这种近乎于霸王条款式的权限设定,特别是对于定位系统的权限要求,使得消费者受缚于互联网平台,自身活动空间不被干扰的隐私权利受到威胁。除了对 APP 使用者数据的收集之外,互联网企业也会收集非用户资料,例如,Facebook 总裁扎克伯格在接受美国国会听证会质询时,首次公开承认 Facebook 平台会以安全理由收集未注册的非用户者的相关信息。[36]不仅如此,频频发生的互联网企业之间进行的赤裸裸的数据交易现象,更使得数据

收集的合法性变得脆弱。此外,大型互联网平台还可以通过隐秘方式变相处理手中的信息资源,最典型的就是企业之间的数据共享合作和并购行为,当诸如阿里巴巴与高德公司合作建立海量的基础地图和生活服务数据库、美团公司正式将摩拜单车收归门下等新闻接踵而来时,也意味着消费者在 A 平台所留下的数据信息可以不经过权利主体的认可与授权转移到 B 公司。因此,互联网平台通过以上种种直接或变通的方式收集消费者信息数据的同时,也给公民隐私权带来了显著的威胁。

(二)互联网平台在数据使用过程中对消费者隐私权的威胁

在大数据时代,除了给消费者造成直接身心受害的侵权行为之外,互联网企业在数据使用过程中还能够悄无声息地支配或侵害消费者决策隐私权利。这里所说的决策隐私权是指个人在作出涉及教育、健康、职业、婚姻、政治观点等方面的选择与决定时拥有免于他人干预的权益。[37] 在现实生活中,每当我们享受网上购物、时政阅览、信息通讯、搜索引擎、电子交易等网络服务之后,都会间接性表达了自身的某些消费需求,进而被互联网平台识别并加以利用,出现很多与之相关的广告推送,这些广告作为互联网企业精准营销的一种手段也许能为消费者提供个性化产品信息,但是,更多的往往表现为互联网企业因逐利性推送虚假或误导性的信息干扰消费者决策,导致对消费者隐私权利的间接侵害,其中,饱受争议的就是互联网企业的竞价排名和推送虚假广告的不正当行为。最典型的案例莫过于 2016 年发生的魏则西事件,此次事件直指诟病已久的百度竞价排名的盈利模式,百度公司通过竞价排名的方式将没有与斯坦福大学医院合作且不具备相应技术的北京武警二院“高捧”为“放心医院”,网民魏则西正是在这种误导性的医疗信息的影响下,接受了不当治疗并最终病逝。[38] 最近,今日头条也出现了类似现象,为了规避一线城市严厉的监管措施,他们有选择性地向二三线城市推送虚假广告,给消费者的决策隐私权造成了威胁。在欧美国家,一些互联网商业机构凭借自身的数据掌控能力试图影响国家政治,如通过信息技术了解选民的偏好,在特定人群中传播、曝光很多虚假信息,潜移默化地影响人们的价值判断,进而支配选民的政治行为,使得公民在信息的狂轰滥炸下失去自身的判断,最终导致整个社会秩序被资本所驱动。近期曝光的有关 Facebook 公司泄露用户信息的事件,甚至涉嫌操纵美国大选,剑桥分析公司在 2016 年美国大选期间运用人工智能技术针对潜在选民的政治倾向、情绪表达以及易受影响的程度等特征投放付费政治广告,试图影响总统选举的结果。此外,英国脱欧公投结果在此次“隐私门”中也遭到了公众的质疑。

(三)互联网平台在数据安全保护阶段对消费者隐私权的威胁

当互联网平台收集了数据,保护数据安全就是其重要责任。正如隐私权控制论学说所强调的,公民个人拥有自主决定他人获取或披露与自身相关信息的范围与场合的权利。然而,在网络空间中,个人只是在自愿公开信息的环节拥有处分权,网络供应商可以通过隐私权保护“告知条款”以及信息公开“同意协议”

的方式,[39]借助互联网技术传播速度快、传播范围广、传播渠道多的特有属性,将消费者信息永久记载在网络存储空间之中,使得信息的传播、挖掘、分析等环节的处分权基本超出了消费者的控制范围,从而将权利主体的数据处分权转移到自己手中。在失去数据处分权之后,第三方可以肆意传播利用消费者置于互联网之中的相关信息,甚至不用承担侵权责任。[40]例如,2017 年曝光的现金贷平台向数据公司购买所谓的"数据产品",再通过爬虫技术获得用户在移动通信运营商、淘宝等知名电商网站、微信支付宝等社交网络上的行为轨迹,以及包括央行征信报告、水电煤使用等在内的生活信息,作为平台放贷前评估用户风险的"风控奇招"。[41]此外,网络虚拟空间的信息泄露、谣言传播等行为也会威胁到消费者的身心安全,特别是电信诈骗、电话骚扰、信息恐吓等方式在现实生活中已经给普通民众造成巨大干扰和惨痛代价。更有甚者,互联网企业利用大数据反向识别技术,能够挖掘和揭露消费者个人不愿意向他人展示的诸如悲伤、痛苦、肉体创伤、精神创伤等生理或情感层面的敏感信息,一旦这些信息被披露,势必会引起人们的尴尬和羞耻感,降低个人的人格尊严,也会给受害人带来巨大的心理压力和精神创伤。[42]多年前,美国塔吉特公司通过"怀孕指数"发现一名在校女生妊娠的隐私信息造成纠纷,[43]就是互联网企业披露个人敏感信息影响公民正常生活的最好例证。由于网络信息存储的长期存在,这种心理干扰具有长期性、不确定性,更加剧了互联网企业泄露消费者敏感信息所带来的社会风险。

四、互联网时代公民隐私权保障不力的原因分析

如上所述,互联网平台尤其是网络巨头在收集、使用和保护消费者数据的过程中,都或多或少存在侵犯消费者隐私的冲动,公民隐私权无时无地都面临遭受侵害的风险。究其原因,我们认为,互联网企业发展和扩张与公民隐私权保护之间的冲突,主要根源于互联网企业在收集数据、使用数据和保护数据三个阶段存在的紧张,即数据收集阶段互联网服务功能与信息供给之间的张力、数据使用阶段强大掌控者与弱小社会个体之间的张力、数据保护阶段立法规制滞后性与信息技术发展迅猛之间的张力。

(一)数据收集过程中互联网服务功能与信息供给之间的张力

对于普通消费者而言,最大的效用需求是享受互联网企业提供的便利化服务,比如,在微信朋友圈、QQ 空间转发动态,在淘宝、京东购物,在百度、搜狗信息咨询,利用网易新闻、今日头条阅读时事等等。但是,这些普通行为都会在互联网平台上留下痕迹,会被动地为互联网企业提供了各种数据信息,这些数据将会成为互联网企业赖以发展的重要资源,能够为企业产品研发、定制和精准营销提供关键的数据基础。[44]因此,对于互联网企业来说,通过对海量信息的掌握,利用大数据和云计算技术,将这些看似零散的碎片化信息进行加工处理并加以分析,就能够挖掘出消费者的消费偏好,从而进行个性化产品的定制。如果互联网企业的市场行为就此止步,那么用户隐私权被侵犯的可能性会大大降低,因为

用户的隐私权是否被破坏并不完全取决于是否透露自己的个人信息，而取决于信息在被透露给其他人或机构之后，被用作何种场合、何种用途以及信息的使用方式，[45]只要企业保护消费者信息安全，那么消费者和企业都能实现共赢。

然而，一旦商业机构的信息平台不受法律规制、道德约束和技术控制，在强大的商业动机诱惑面前，企业往往会不惜冒着风险，擅自把消费者的相关数据用于其他用途或出售给第三方，通过滥用数据资源谋取高额的利润，这就很难保证公民个人信息不被泄露，公民个人隐私权也非常容易被侵害。最近，美国社交平台公司 Facebook 就面临着这样的危机，在未经许可的情况下将用户个人信息泄露给第三方即剑桥分析公司，以用于非正当目的，并且允许第三方 APP 开发者提取用户的个人信息，使得互联网空间中的个人隐私权成为了国际笑话。[46]

由此可知，消费者为了获取便利化服务自愿提供私人信息，但随着个人相关信息被存储在网络之中，消费者辨别个人信息将会被用于何种用途变得越来越困难，当公众无法了解个人数据的最终使用情况，就为互联网企业有意识地收集和分析个人信息数据提供了机会，公民隐私权也面临着被侵害的风险，从而陷入互联网服务与数据收集的紧张关系之中。

（二）数据使用过程中大数据掌控者与弱小社会个体之间的张力

如今，大部分互联网企业，特别是以 BAT 为代表的商业巨头，往往都掌握了大数据、云计算以及人工智能应用技术，具备收集、处理、分析消费者个人信息数据的能力，成为信息时代大数据的实际掌控者。这种强大的信息库往往会催生集权效应，当企业与消费者之间未建立可信的信息伦理规范以保证双方的利益平衡时，大数据掌控者能够毫不遮掩地植入商家的特定利益需求，进而隐秘地、不受控制地利用个人数据，[47]使得社会可能陷入乔治·奥威尔在《1984》中所描述的“老大哥在看着你”的全面侵掠个人隐私权的生存状态，[48]有所不同的是在这个大数据时代的权力来源不再局限于传统的政府公权力，更包含一些互联网商业机构的数据掌控权力。

此外，互联网技术的门槛效益势必会强化一部分人的能力，造成信息资源配置的不对称、不平等的现象，[49]在互联网企业海量数据和技术壁垒的压倒性优势下，互联网平台企业能够主导舆论以及消费者的各种偏好，使得公民在隐私权被侵犯的时候，一直处于不利地位，甚至无法发声，普通消费者几乎没有力量来抵抗，越来越多的人成为无法维护自身隐私和自由的弱者。[50]例如，互联网企业可能为了掩饰自己的行为或其他影响自身权益的事证，可以通过对掌控的信息资源加以利用、销毁、篡改的方式，让消费者难以追诉责任和主张权利。[51]因此，互联网企业作为数据掌控者与消费者作为弱小的社会个体之间的张力，一定程度上会带来“电子歧视”和“数字鸿沟”效应，使得越来越少的人享有越来越大的自由，越来越多的人受到越来越强的必然性的束缚。[52]

（三）数据保护过程中立法规制滞后性与信息技术迅猛发展的张力

在任何一个时代，法律的调整与完善都是基于对现实社会经济生活的回应，

通过不断的修改、补充来填补空白、漏洞,是一个循环推进的缓慢演变过程。在早期工业文明时期,公民隐私权保护的相关法律的被动调整进程能够适应当时公民个人自由发展的需要。但是,在互联网产业蓬勃发展的信息文明和人工智能时代,程序繁复、耗时冗长的立法程序显然远远滞后于互联网技术"摩尔定律"[53]的更新换代效应。高科技的更新周期大约在两年左右,甚至不超过两年,而在法律制定、颁布、执行的过程中,两年时间显得较短,即使对于事关公民隐私权侵犯的相关纠纷案件,其诉讼周期往往也比较长,经过旷日持久的审理之后,又会陷入新的一轮技术风波之中,使得原有的案件可能已经失去了价值。[54]特别是对于我们这个非判例法的国家,法律制定者只有发现问题才去解决问题,法律的制定实施具有相对稳定性,在互联网企业飞速发展过程中,难以保证对公民隐私权事项进行一种相对静态的保护。就像任甲玉与百度公司被遗忘权案以及百度在 BBS 贴吧恶意攻击、诬陷等侵犯他人隐私权的案件尚未结束,又出现了百度公司利用新技术侵害公民隐私权的案例,越界收集、过度获取公民个人隐私信息,各种侵害方式和手段也层出不穷,使得现有的法律体系防不胜防。但法律又不能对信息技术创新过于限制,不然会导致部分有助于社会进步的科技创新夭折,因而技术发展与法律滞后的张力始终存在,必然严重制约互联网行业的管制效果,由此而产生的侵权风险越来越复杂,几乎远远超出了我们的想象。

五、限制互联网企业巨头网络垄断和市场扩张,保障信息社会的公民隐私权

互联网企业巨头的兴起和市场权力的扩张,一定程度上是建立在消费者个人信息数据不断被获取的基础之上。在如何有效规范和防范互联网技术对人类自由权利侵害的整体性法律框架尚未成熟的当下,网络上的数据收集、使用和数据安全方面存在的张力,会进一步扩大互联网企业巨头的网络垄断和市场扩张与公民隐私权保护之间的冲突。因此,我们在为信息时代的到来而欢呼之际,更需要警惕"数字利维坦"对公民隐私权的侵害,对人类自由空间的剥夺,同时应探讨和提出应对之道,对互联网技术和信息产业高速发展带来的商业机构强大的数据控制力作出必要的规范和制衡,限制互联网企业巨头的网络垄断和市场扩张,保障公民的隐私权利,达成信息技术和互联网经济发展与个人隐私权保护的平衡。

从当前信息产业发展状况来看,在大数据、云计算、人工智能技术和互联网经济高速发展过程中呈现的寡头垄断格局,对公民隐私权的保护和法律监管能力提出了严峻挑战。当下亟需全国人大启动网络立法和修法进程,制定并完善相关法律,从法律层面严格规范互联网巨头的商业行为,结合公民个人信息隐私保护相关法律和反垄断法的有关内容,将大型互联网平台,特别是 BAT 这样具有垄断地位的互联网企业巨头纳入国家法律监管框架之内,规范并限制互联网平台的网络垄断和市场扩张,保护消费者的隐私权利。在国家立法规范、限制和防范互联网企业巨头侵权风险的基础上,拥有地方立法权的各级政府还应采取

以下行政和市场监管措施,规范互联网企业在数据收集、使用、保护等三个方面的市场行为,把互联网经济发展和企业扩张对公民隐私权利侵害的风险降至可控的范围内,实现互联网企业发展与公民隐私权保护的平衡。

第一,扩充数据收集过程中用户主体的权利范围。我国现有的《消费者权益保护法》和《网络安全法》关于用户数据收集的相关法律条文,大多是基于同意规则而制定,且没有具体细化消费者作为数据主体地位的权利范围,由于企业与用户双方信息掌控能力的不平等,使得这种流于形式的知情同意规则往往成为互联网平台后续可能涉及侵权行为的"挡箭牌"。[55]而消费者数据权利范围作为影响公民隐私权保护效果的重要变量,数据主体权利的补充和完善都会起着难以替代的作用。因此,在数据收集过程中,需要基于原有用户数据权利保护不断细化和完善数据主体的权利保护范围。例如,我国可以结合实际情况借鉴欧盟最新制定的《统一数据保护条例》,强化或赋予现有数据主体的知情权、访问权、拒绝权和被遗忘权等相应权利,也就是说,通过建立包括处理目的、数据类别、数据接收者情况说明、储存期限等内容的相关数据收集清单以强化用户信息知情权;通过简化消费者访问自身信息数据的程序保障数据主体的访问权;通过更具操作性的方式明确数据主体基于自身特殊情况随时拒绝使用个人信息的情形以补充消费者的拒绝权;通过授予数据主体更正和清除与自身有关的错误信息的权力以维护数据收集过程中数据主体的更正权和被遗忘权。此外,消费者对隐私权保护的知晓程度、对个人数据被收集的关注程度等隐私意识的强弱也具有巨大影响力,公众追求安全保障的网络信息服务成为互联网企业市场竞争的关键要素,也能从侧面激发互联网企业开发更高标准的隐私保密系统以满足消费者的需求,让企业自觉采纳以"告知"和"选择"为基础的合理的隐私政策。[56]

因此,在法律层面强化数据主体权利的同时,还要唤醒广大社会公众在数据收集过程中的信息隐私权保护意识,即用户在使用网络软件前需要树立起明确的信息隐私观念。一方面,当互联网企业以非法要求获取和使用公民个人信息时,能够主动拒绝其不合理要求和权限设定,构筑起防止网络平台侵害个人信息隐私的第一道篱笆;另一方面,在互联网平台非法或违背自身意愿收集相关数据资料和敏感信息时,公民也需要勇于发声、勇于维权,及时向有关政府部门反映,甚至斥之于法律机构。[57]通过扩充数据主体的权利范围,激发用户自身数据安全保护敏感度,从权利主体的角度防止公民隐私权被侵害。

第二,加强互联网平台数据使用的内外监管。从当前我国对消费者隐私保护的政策措施来看,政府层面的外部规制还比较弱,互联网平台自身的行业规范也相对缺失。因此,未来亟需在消费者信息隐私保护的规制架构之中加强互联网平台数据使用的内外监管。一方面,从政府层面建立具有威慑力的外部监管机制。在我国现行体制下,可以探索设立类似于数据监督管理局的执法机构,在整合市场监管、网信办、公安局等部门数据执法相关职能的同时,保证监管机构

的独立性、透明性、合法性,[58]负责对互联网企业使用消费者信息数据进行常态化、机制化的调查、评估以及风险警告,并且定期向社会公众发布互联网平台数据使用状况的年度报告。另一方面,强化互联网企业及其从业者保护用户隐私的内部治理规范。首先,在用户数据日益掌握在网络供应商手中的背景下,通过社会舆论和行业规则促使互联网平台履行及时更新、修正、处理数据并通知消费者相关情况的义务和责任,确保公民隐私保护从消费者权利规范走向网络平台行为规范。在消费者数据保护过程中更加突出互联网平台作为信息控制者的社会责任和法定义务,并通过建立企业数据保护官的强制性措施,完善互联网平台的内部治理机制,从而调动信息控制者参与消费者信息安全保护的积极性。[59]其次,发挥互联网行业组织在互联网技术应用规范方面的作用,建立互联网平台自律规范以保护消费者隐私权。其中,互联网行业自律组织在制定隐私政策时应该包括三个层次:一是能够清楚地罗列隐私政策,让互联网公司能够明确自身收集数据的合法内容、正当手段以及数据用途的合理范畴;二是网络供应商将收集到的可识别的个人数据向其他网站或组织出售之前必须获得授权;三是保障消费者检查和更正敏感数据的权利。[60]如此,在法律规制滞后于信息技术发展,很多新形式的隐私侵权行为难以找到相关法律规定之时,可以通过有效发挥行业自律的灵活性优势以填补网络平台侵权的漏洞。

第三,构建数据安全保护的技术与制度协同机制。就现实状况而言,消费者隐私保护既是一个技术性问题,也是一个制度性问题,技术防范与制度规制是保护公民隐私权的“两只手”,缺一不可。然而,由于政府部门的“公共性”和私人部门的“竞争逐利性”的组织属性差异,政府部门通常更侧重于法律法规等制度性措施保护公民隐私权,商业机构则偏向于技术性措施以维护消费者数据安全,“两只手”在现实生活中并未形成有效的整合作用和协同效应。因此,未来我们亟待建立健全技术与制度协同运作的隐私保护机制。一方面,需要加大保护个人隐私的技术研发,通过网络数据安全防护技术的不断创新以制约大数据技术的负面效应,凭借用户匿名程序、数据加密传输、分布式访问控制等技术保护手段应对互联网企业对公民隐私权的威胁,从技术层面保护消费者数据信息安全,类似于一些互联网科技公司对骚扰短信和诈骗电话的提示拦截,就是技术性防范思路的实际应用。另一方面,需要完善消费者隐私保护的法规政策体系。首先,借鉴欧盟《统一数据保护条例》的相关经验,从国家整体的法律制度层面明确信息时代隐私权的权利属性、内容范畴、维权方式以及商业机构非法收集、滥用、侵害公民隐私信息的法律责任和赔偿原则,[61]通过整合《消费者权益保护法》《网络安全法》《刑法》等相关法律对个人数据信息保护的措施,进一步强化网络隐私保护的专门立法,出台类似于个人信息保护法的法律文件及配套条例,解决当前互联网发展过程中消费者隐私权保护存在的法律内容碎片化、侵权途径间接化、维权渠道脆弱化、司法救济薄弱化等问题。其次,在公民隐私权保护的整体性制度框架下,逐步细化网络侵权的监管措施,补充或增加特定领域的特

定主体隐私保护的原则和办法,特别是对一些互联网企业擦边球式的侵权行为进行更具针对性的专项治理,通过常规化法律法规建设和专项化网络治理措施给公民隐私权和网络通信自由加上“双保险”。通过技术防范与制度规制相结合的方式,最大限度地发挥政府部门和企业机构维护消费者隐私权的合力。

六、结　语

移动互联网、大数据、云计算和人工智能等信息技术的飞速发展,互联网平台企业巨头的崛起为消费者的日常生活提供了便捷舒适的网络服务,从根本上影响甚至改变了当代人的生活方式、交往方式和行为习惯。与此同时,移动互联网时代和信息社会的公民隐私权被侵犯的风险显著增加,公民的自由空间也被空前压缩。近年来崛起的互联网平台企业,在大数据技术精准营销和自利性市场行为的驱动之下,无形中给消费者戴上了“电子枷锁”,个人数据成了普通公众享受快捷便利的网络服务的代价。在移动互联网和信息技术高速发展的信息社会,如何控制“数字利维坦”的网络权力和市场扩张,有效保障公民的隐私权,是世界各国面临的世纪性难题。需要指出的是,信息时代公民隐私权的维护和保障,是一项涉及到信息技术、公民隐私保护意识、行业自律和法律规范等诸多层面的系统工程,并非一朝一夕所能解决。随着智能革命和文明社会的发展,未来需要从长远的角度整合法律规范、政府的制度性监管和企业技术性防范的合力,在强化政府监管的同时,加强互联网行业自律并激活公民的自我保护意识,对互联网企业巨头的网络垄断权力加以全方位的限制、规范和监控,限制并逐步消解“数字利维坦”企业的网络垄断,遏制互联网平台巨头的无限制扩张,防范垄断和扩张给公民隐私权带来的威胁和风险,有效保障信息时代的公民隐私权。

注释:

〔1〕〔2〕中国互联网络信息中心:《中国互联网络发展状况统计报告》,2018 年 1 月 31 日。

〔3〕相关资料参见中华网、中商情报网、凤凰财经、搜狐新闻、新华网等国内主流媒体公开报道;孙宝文、荆文君、何毅:《互联网行业反垄断管制必要性的再判断》,《经济学动态》2017 年第 7 期。

〔4〕杜峰:《网络隐私门频频引爆舆论 信息安全保护焦虑渐增》,《通信信息报》2018 年 1 月 10 日。

〔5〕方海平、王俊丹、包慧:《支付宝年度账单捆绑推广芝麻信用遭质疑,个人隐私保护规范待解》,《21 世纪经济报道》2018 年 1 月 5 日。

〔6〕薛庆元:《百度涉嫌侵害消费者个人信息安全被起诉 法院已立案》,《中国消费者报》2018 年 1 月 5 日。

〔7〕吴军:《智能时代:大数据与智能革命重新定义未来》,北京:中信出版集团,2016 年。

〔8〕相关研究成果请参见 S Subashini, V Kavitha, “A Survey on Security Issues in Service Delivery Models of Cloud Computing”, *Journal of Network and Computer Applications*, 2011, 34(1), pp. 1 – 11; Samson Yoseph Esayas, “A Walk in to the Cloud and Cloudy It Remains: The Challenges and Prospects of ‘Processing’ and ‘Transferring’ Personal Data”, *Computer Law & Security Review*, 2012, 28(3), pp. 662 – 678; Xu Heng, “A Value Sensitive Design Investigation of Privacy Enhancing Tools in Web Browsers”, *Decision Support Systems*, 2012, 54(1), pp. 424 – 433.

〔9〕JP Yong, SW Campbell, N Kwak, “Affect, Cognition and Reward: Predictors of Privacy Protection on-

line", *Computers in Human Behavior*, 2012, 28(3), pp. 1019 – 1027.

〔10〕W Heirman, M Walrave, K Ponnet, "Predicting Adolescents' Disclosure of Personal Information in Exchange for Commercial Incentives: An Application of an Extended Theory of Planned Behavior", *Cyberpsychology, Behavior, and Social Networking*, 2013, 16(2), pp. 81 – 87.

〔11〕A Beldad, MD Jong, M Steehouder, "I Trust not Therefore It must be Risky: Determinants of the Perceived Risks of Disclosing Personal Data for E – government Transactions", *Computers in Human Behavior*, 2011, 27(6), pp. 2233 – 2242.

〔12〕JJV Chen, AH Huang, A Muzzerall, "Privacy Concerns and Expectation of Control", *Human System Management*, 2012, 31(2), pp. 123 – 131.

〔13〕KS Schwaig, AH Segars, V Grover, KD Fiedler, "A Model of Consumers' Perception of the Invasion of Information Privacy", *Information&Management*, 2013, 50(1), pp. 1 – 12.

〔14〕J Herranz, J Nin, M Solé, "More Hybrid and Secure Protection of Statistical Data Sets", *IEEE Transactions on Dependable and Secure Computing*, 2012, 9(5), pp. 727 – 740.

〔15〕G Zhang, Y Yang, J Chen, "A Historical Probability based Noise Generation Strategy for Privacy Protection in Cloud Computing", *Journal of Computer and System Sciences*, 2012, 78(5), pp. 1374 – 1381.

〔16〕Xu Heng, "A Value Sensitive Design Investigation of Privacy Enhancing Tools in Web Browsers", *Decision Support Systems*, 2012, 54(1), pp. 424 – 433.

〔17〕相关研究成果请参见 M Yuan, L Chen, PS Yu, T Yu, "Protecting Sensitive Labels in Social Network Data Anonymization", *IEEE Transactions on Knowledge and Data Engineering*, 2013, 25(3), pp. 633 – 647.

〔18〕C Wang, SSM Chow, Q Wang, K Ren, W Lou, "Privacy – Preserving Public Auditing for Secure Cloud Storage", *IEEE Transactions on Computers*, 2013, 62(2), pp. 362 – 375.

〔19〕M Desai, M Drobac, M Gates, G Louer, "The FTC privacy Report and the White House Consumer Privacy Bill of Rights: Policymaking Trends and What You Need to Know in 2013", *Mobile Marketing Association*, 2012, 7(3), pp. 66 – 81.

〔20〕Alexander Dix, "Built – in Privacy——No Panacea, but a Necessary Condition for Effective Privacy Protection", *Identity In the Information Society*, 2010, 3(2), pp. 257 – 265.

〔21〕王锐:《云产业发展与消费者隐私权保护的平衡机制研究——基于成本—收益视角》,《商业经济与管理》2014 年第 3 期。

〔22〕张茂月:《大数据时代公民个人信息数据面临的风险及应对》,《情报理论与实践》2015 年第 6 期。

〔23〕〔50〕郑戈:《在鼓励创新与保护人权之间——法律如何回应大数据技术革新的挑战》,《探索与争鸣》2016 年第 7 期。

〔24〕相关研究成果请参见谢远扬:《信息论视角下个人信息的价值——兼对隐私权保护模式的检讨》,《清华法学》2015 年第 3 期;金耀:《消费者个人信息保护规则之检讨与重塑——以隐私控制理论为基础》,《浙江社会科学》2017 年第 11 期。

〔25〕方兴东、张静、刘国辉:《谷歌产品对用户个人隐私的影响——表现、趋势与对策》,《新闻界》2014 年第 11 期。

〔26〕Samuel Warren & Louis Brandeis, "The Right to Privacy", *Harvard Law Review*, 1890, 4(5), December 15.

〔27〕William L. Prosser, "Privacy", *California Law Review*, 1960, 48(3), p. 389.

〔28〕〔60〕〔美〕理查德·斯皮内洛:《铁笼还是乌托邦——网络空间的道德与法律》,李伦等译,北京:北京大学出版社,2007 年,第 143、148 页。

〔29〕陈璞:《大数据、隐私权与自由》,《中共中央党校学报》2016 年第 5 期。

〔30〕〔37〕段伟文、纪长霖:《网络与大数据时代的隐私权》,《科学与社会》2014 年第 2 期。

〔31〕Jerry Kang,"Information Privacy in Cyberspace Transactions", *Stan L Rev* ,1998(50).

〔32〕Charles Fried, "Privacy", *Yale L. J* ,1968(77).

〔33〕Himma,Kenneth E. ,Tavani,Herman T. (eds.) , *The Handbook of Information and Computer Ethics* , John Wiley & Sons,Inc. 2008,pp. 135 – 156.

〔34〕徐明:《大数据时代的隐私危机及其侵权法应对》,《中国法学》2017 年第 1 期。

〔35〕赵思茵、李静:《APP"疯狂"调用权限背后 用户隐私或暴露无遗》,《中国经营报》2017 年 3 月 18 日。

〔36〕《扎克伯格承认面簿也收集非用户资料》,《联合早报》2018 年 4 月 13 日。

〔38〕房雅楠:《百度该取消医疗广告竞价排名吗?》,《中国商报》2016 年 5 月 10 日。

〔39〕〔49〕周佳念:《信息技术的发展与隐私权的保护》,《法商研究》2003 年第 1 期。

〔40〕张融:《试探互联网时代的隐私权保护路径》,《电子政务》2017 年第 9 期。

〔41〕李玲:《个人信息买卖黑链:淘宝 25 页和京东 3 年数据仅需 1 元》,http://tech. sina. com. cn/i/2017 – 11 – 23/doc – ifypacti7108636. shtml。

〔42〕Anital. Allen,"Lying to Protect Privacy", *VILL. L. Rev* ,1999(2),pp. 161 – 177.

〔43〕Somini Sengupta,"Risk and Riches in User Data for Facebook", *The New York Times* , 2012 – 12 – 16.

〔44〕王君晖:《不要让隐私在网络时代"裸奔"》,《证券时报》2018 年 1 月 6 日。

〔45〕丁楠、潘有能:《数据挖掘中的隐私保护:法律与技术》,《情报理论与实践》2007 年第 6 期。

〔46〕孙兴杰:《Facebook 泄密门:大数据、班农主义与"通俄门"》,http://tech. sina. com. cn/i/2018 – 03 – 25/doc – ifysnevm8758676. shtml。

〔47〕〔52〕郑戈:《人工智能与法律的未来》,《探索与争鸣》2017 年第 10 期。

〔48〕〔英〕乔治·奥威尔:《1984》,刘绍铭译,北京:北京十月文艺出版社,2013 年。

〔51〕高波:《大数据:电子数据证据的挑战与机遇》,《重庆大学学报(社会科学版)》2014 年第 3 期。

〔53〕孙泉:《解读摩尔定律》,《集成电路应用》2004 年第 8 期。

〔54〕吴志攀:《"互联网 +"的兴起与法律的滞后性》,《国家行政学院学报》2015 年第 3 期。

〔55〕范为:《大数据时代个人信息保护的路径重构》,《环球法律评论》2016 年第 5 期。

〔56〕王菲:《互联网精准营销的隐私权保护:法律、市场、技术》,《国际新闻界》2011 年第 12 期。

〔57〕安宝洋、翁建定:《大数据时代网络信息的伦理缺失及应对策略》,《自然辩证法研究》2015 年第 12 期。

〔58〕周汉华:《探索激励相容的个人数据治理之道——中国个人信息保护法的立法方向》,《法学研究》2018 年第 2 期。

〔59〕Miguel Recio,"Data Protection Officer:The Key Figure to Ensure Data Protection and Accountability", *Eur. Data Prot. L. Rev* ,2017,p. 114.

〔61〕王丽萍、刘鹏:《发展与挑战:信息社会中的隐私权保护》,《山东大学学报(哲学社会科学版)》2009 年第 3 期。

〔责任编辑:刘姝媛〕