

大数据背景下隐私权保护的探讨

孙悦

青岛大学, 山东 青岛

收稿日期: 2022年11月8日; 录用日期: 2022年11月18日; 发布日期: 2023年1月18日

摘要

大数据背景下, 个人信息已经成为信息传播的常态内容, 对于隐私权的侵犯也随处可见, 故对大数据背景下隐私权的保护展开研究是迫切需要的。首先对大数据背景下隐私权的内涵部分进行研究, 分为概念内涵和权利客体两个部分。之后对大数据背景下隐私权的特征进行解读, 特征呈现主体多元化、客体扩张化、侵权方式隐蔽化, 由此为后文的分析奠定理论基础。其次, 探讨目前我国隐私权面临的言论自由对隐私权、公权力对隐私权以及商业发展对隐私权冲击存在的三大问题。最后, 从规范大数据技术建设、完善隐私权监督保护制度以及提高公民个人隐私权保护意识三个方面提出对隐私权保护的建议。

关键词

大数据, 隐私权, 保护

Discussion on Privacy Protection under the Background of Big Data

Yue Sun

Qingdao University, Qingdao Shandong

Received: Nov. 8th, 2022; accepted: Nov. 18th, 2022; published: Jan. 18th, 2023

Abstract

Under the background of big data, personal information has become the norm of communication, and the violation of privacy can be seen everywhere. Therefore, it is urgent to study the protection of privacy under the background of big data. Firstly, the connotation of privacy in the context of big data is studied, which is divided into two parts: connotation and right object. After that, the author interprets the characteristics of privacy rights in the context of big data, showing diversified subjects, expanded objects and concealed infringement modes, thus laying a theoretical foundation for the analysis in the following paper. Secondly, it discusses the three major problems

of the impact of the freedom of speech on the right of privacy, the public power on the right of privacy and the commercial development on the right of privacy. Finally, this paper puts forward some suggestions on privacy protection from three aspects: standardizing the construction of big data technology, improving the privacy supervision and protection system, and enhancing citizens' awareness of privacy protection.

Keywords

Big Data, The Right to Privacy, Protect

Copyright © 2023 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

随着科学技术的完善和全球经济的发展,信息交流成为人们日常生活与工作必不可少的组成部分。大数据、云计算、AI 技术等等已经进入我们的生活,成为了人们习以为常的存在,在购物消费时,人们的消费记录、购买信息会被记录、上传到云端,通过大数据来传送,商家则进一步利用人们的消费数据来推算其兴趣和喜好,进行推销;在人际交往中,人们使用微信、微博、邮箱等聊天、发送文件,聊天记录和文件信息被大数据读取,为我们推送感兴趣的内容和爱好相近的朋友等等。但是大数据为人们带来便利,为商家带来利益的同时,是建立在读取、利用、分析人们的隐私信息之上的。对于目前大数据化的时代,研究分析隐私权的保护是必要且必需的。本文拟以隐私权在大数据背景下的保护为课题,以期可以为隐私权的保护做出一点贡献,促进其完善保护。本文选择以大数据下的隐私权保护为研究课题,主要具有以下几点意义:第一,有助于帮助人们认识到在大数据背景下,隐私权遭到侵犯的事实和程度,促进人们加深隐私权保护的意识。第二,有助于规范商家企业和社会主体的行为,促使其在建立软件,进行商业行为时,完善使用和收集人们隐私信息的行为。第三,有助于总结有关隐私权的相关法律法规,找出法律漏洞,完善法律规范,促进法律的制度体系。

2. 大数据背景下隐私权的内涵

2.1. 隐私权的内涵

大数据背景之下,我们的学习、生活和工作都发生了极大的变化,多种多样的科技产品和软件围绕在我们的身边,记录、收集着我们的信息,形成了一个储存着我们隐私的庞大数据库。大数据的特征就是对于各种信息进行快速、准确、及时的查询、储存、处理,个人隐私在大数据的运行之下必然受到许多方面的挑战和侵害,这就要求我们对隐私权做出更多的研究,解读其内涵。隐私权的概念随着不同的时间和阶段的变化也在不断的发展,并且在不同的国家和地区,其有着不同的解释。大数据背景之下互联网是主要的战地,而互联网维系和运行的中心则是用户个人信息的运转,因此隐私权关注的重点主要是个人信息方面的保护。比如大数据背景下隐私权的泄露情况之一就是商家对于消费者隐私权的侵害,商家为促进商品出售,会利用用户在网上的搜索、购买记录来预测用户和市场的需求。消费者的浏览记录、个人喜好以及生活的习惯都属于个人隐私,却成为商家制定精准营销和广告的工具[1]。

在传统的隐私权概念中,因时代发展的限制,隐私权内涵有所限制。但是随着时代背景的变化和现实情况的发展,隐私权的内涵已经切合时代发展产生了巨大的变化,我国《宪法》第三十八条、三十九

条、四十条,《刑法》第二百四十五条、第二百五十三条,《民法典》第一千零九条、第一千零二十条,《未成年人保护法》第三十九条都是有关于我国隐私权的相关规定。尤其是《民法典》第一千零三十二条对隐私权做出了详细明确的规定,该条第二款对隐私权的内涵做出了明确的界定,即自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。

2.2. 隐私权的权利客体

根据《民法典》第六章有关《隐私权和个人信息保护》的规定,隐私权的权利客体大致可以分为个人信息、私人活动以及私人领域三大方面。在大数据背景以及我国法律新修改的规定下,根据《民法典》第一千零三十二条、第一千零三十三条的以及其他相关法律规定,本文对其作出以下理解。

第一,个人信息。根据《民法典》第一千零三十四条的规定,“个人信息是指以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息,包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。”“个人信息中的私密信息,适用隐私权的规定;没有规定的,适用有关个人信息保护的规定。”具体到目前大数据时代,本文将个人信息的内容归纳为以下几类:其一,个人的交易信息,主要包括个人在各个账户和平台上的消费、投资、交易等记录[2]。其二,个人通讯信息,主要包括个人在生活和工作在微信、短信、邮箱、贴吧等聊天工具上往来的信息。其三,个人位置信息,主要包括个人在日常生活中携带电脑、手机或者使用汽车等交通工具所记录的位置轨迹。其四,个人生活信息,这类信息囊括的内容较为丰富,包括个人在生活中所需要记录的各种电子内容,比如,医疗、社保、住房等各种生活信息。

第二,私人活动,根据《民法典》第一千零三十三条第三款有关私人活动的规定,“除法律另有规定或者权利人明确同意外,任何组织或者个人不得实施下列行为:拍摄、窥视、窃听、公开他人的私密活动。”在大数据背景下,私人活动很容易就被记录、传播,比如,名人、热点事件当事人的活动、生活轨迹等等。私人活动在大数据背景下极易被跟踪、记录和传播,如果不能对人们的私人活动加以保护,那么,每个人都难以保有隐私。

第三,私人领域,在大数据背景之下,私人领域不仅仅限于现实生活中的住宅,还包括在网络之上建立的私人领域性质的储存空间[3]。比如,情侣记录空间、个人网盘内容等等。应该意识到,大数据环境使得私人领域的范围已经从实体边界扩展到虚拟空间。

大数据背景之下,信息技术促进生活质量和方式发展的同时,触犯个人隐私的行为也逐渐加多,现实要求保护个人隐私的呼声也越来越大。公民对于个人隐私的维权意识也随之不断的加强,注重对于个人信息、活动和领域的维护。故明确隐私权的客体,明了隐私权所保护的范围是保护隐私权的重要一步。

3. 大数据背景下侵犯隐私权的特征

3.1. 主体多元化

个人隐私在大数据背景之下受到侵犯的可能,从开始的收集贯穿到之后的储存、分析和使用的全过程。由此,侵犯隐私权的主体也呈现多元化的特点,主要包括互联网用户、互联网提供商、商业公司以及政府部门。

第一,互联网用户。互联网用户是互联网时代的主要支撑,他们既是个人隐私的生产者也可能是个人隐私的侵犯者。其一,互联网用户是互联网的组成部分,数量多,范围广,产生的数据信息巨大,这些密集性强的活动很容易侵犯到他人的隐私。其二,人的本性具有探索未知和秘密的欲望,这种心理会导致互联网用户在日常的网上活动有意或者无意的触犯到他人的隐私。

第二,互联网提供商。互联网提供商是指向互联网用户提供网络信息或者服务的组织机构,主要包

括网络平台提供商、网络内容提供商、网络接入提供商以及网络产品提供商[4]。网络平台提供商是指为互联网用户提供浏览信息、购买商品、发表言论等网络服务平台的提供商,比如京东、淘宝;网络内容提供商是指以网络为媒介,提供信息内容的提供商,比如简书、今日头条;网络接入提供商是指为互联网用户提供网络访问设备、网络访问服务等接入的提供商,比如中国移动、中国电信;网络产品提供商是指为互联网用户提供网络服务的提供商,比如软件公司。各类互联网提供商在其运营之中就是利用为互联网用户搭建信息传输平台所谋利的,其自然掌握着互联网用户的个人信息和网络交流信息。其在大数据的支撑之下,可以通过互联网监控技术毫不费力的获取互联网用户的网络痕迹和网络浏览记录,再从这些信息之中非法利用用户的个人隐私。其利用用户的个人隐私探索爱好习惯,针对用户投放内容和广告或者将用户隐私进行再次贩卖谋取利益。

第三,商业公司。网络时代的数据就是经济价值,个人隐私信息就是金钱[5]。商业公司利用互联网用户的隐私贩卖出售带来利益。比如,之前的美国征信公司 Eqifax 将其 1.6 亿的用户信息贩卖给五万家公司谋取利益¹。商业公司没有经过其征信用户的同意就获取其个人隐私,并将其隐私信息非法出售,属于严重侵犯公民隐私权的行为。

第四,政府部门。政府部门在大数据背景下,其管理方式也随之有所改变。政府部门需要对公民的隐私信息进行收集、储存、分析以及公开和使用,并建立了官方的政府数据库。在数字化社会中,社会治理能力和社会效率的提高必须需要个人信息的支撑,但是如果个人隐私信息不能安全的保护,则容易使得公民受到侵犯。比如,美国“棱镜门”事件²的发生,则是在大数据背景下,为公民隐私权保护敲响的警钟。

3.2. 客体扩张化

在传统社会之中,由于科学技术的限制,隐私权的侵犯客体有限。但是随着科技和社会的发展,大数据使得隐私权的侵犯客体扩大。传统的互联网没有海量数据和大型数据库,个人信息的泄露有限,网上的个人信息通常为身份证号码、家庭住址、身体健康状况、财产状况以及医疗状况等简单的信息。暴露的个人隐私信息少,隐私权所覆盖的客体范围小,则侵犯隐私权的行为则少[6]。但是在大数据背景之下,互联网已经成为人们日常生活中学习和工作不可或缺的一部分,互联网已经渗透到我们生活的方方面面。一方面个人隐私信息的覆盖客体扩大,另一方面随着科技发展,个人隐私信息更容易被收集到。大数据背景下,隐私权的侵犯客体不仅仅局限在简单单调的传统信息,而是上升到了数据库,利用大数据技术收集、分析、挖掘和处理。

3.3. 侵权方式隐蔽化

大数据时代,互联网用户极其容易就可以使用一个虚假的身份进行网上活动,其进行侵权行为很难被找到,这也就使得侵权方式更加隐蔽化。互联网提供商利用其运营过程中获取的用户活动和数据信息来分析得到某个用户的个人隐私,比如,早在 2011 年就有媒体曾爆出可以通过搜索引擎检索到 360 用户的上网浏览记录、用户账号密码以及其他个人隐私信息³。

并且在之后,金山公司由于程序漏洞的原因泄露了大量用户的个人隐私信息⁴。这也暴露了网络公司确实存在私下收集网络用户信息的情况。在这种情况下,网络用户是难以发现自己的个人隐私信息遭到泄露和侵犯,并且用户也往往是在其个人隐私信息被暴露之后在认识到侵权行为的发生[7]。比如,2010

¹https://www.sohu.com/a/329481936_413981.

² 百度百科: <https://baike.baidu.com/item/%E6%A3%B1%E9%95%9C%E9%97%A8/6006333>.

³ 人民资讯: <https://baijiahao.baidu.com/s?id=1689275073662130189&wfr=spider&for=pc>.

⁴<https://www.cantontex.com.cn/jishu/19403.html>.

年 Facebook “泄密门”事件⁵的爆发，超过一亿用户的个人信息被泄露，而大多数人却是在报纸上看到消息才知道自己的隐私被泄露。而曝光这一事件的是一名网络安全咨询师，其表达是借此提醒人们需要重视自己的隐私并且树立保护隐私的态度，因为一个代码就可以收集将近 3 个 G 的隐私信息。大数据背景下，隐私权的侵权行为普遍具有隐蔽性和复杂性，大多数受害者是无法在第一时间知道自己的个人隐私已经受到侵犯。

4. 我国隐私权面临的问题

4.1. 言论自由对隐私权的冲击

言论自由意味着公民享有以语言或者其他方式表达自己思想的权利，每个人都有权自由地发表言论。法律理应保护公民享有获得和传播信息的权利，公民有权发表社会接受的言论，也有权发表不同于社会普遍价值的言论，其中包括引起部分人不快和批评国家的言论。并且在大数据背景之下，人们的言论以更加快捷的方式、更加广泛的传播范围、更强的影响力产生影响。人肉搜索是大数据时代的新产物，是个人发表言论自由与触犯个人隐私信息的冲突。网络用户不仅仅是个人信息的产生者还可能是个人信息的传播者，不仅仅可能是隐私权被侵犯的被害人还可能是侵犯隐私权的主体[8]。我国最初的人肉搜索案件可以追溯到 2007 年的姜岩案，一北京女白领写下一篇遗书博客公之于世后跳楼自杀，其博客记录了丈夫与外遇者的照片以及丈夫的个人信息。网友通过其留下的丈夫个人信息，利用其在网络上的使用轨迹，对其丈夫王某进行人肉搜索。因王某的行为，网友对其进行了搜索和骚扰，甚至严重影响到了王某及其家人的正常工作和生活。之后，王某上訴法庭，法院判决涉事网站承担相应的法律责任，删除王某及相关事件的信息并给予一定的精神损害赔偿。

自 2007 年姜岩案⁶发生之后，随着网络发展的进步，人肉搜索案件的发生与日俱增。目前我国的人肉搜索大致可以分为两种类型，第一种类型是网友对公共人物的搜索，第二种是网友对于公德事件的搜索。人肉搜索对于隐私权的侵犯表现在其将与个人信息密切相关的个人生活安宁、个人隐私信息以及个人活动空间随意搜索、暴露以及传播，影响他人的正常生活[9]。人肉搜索具有两面性，适当的、在法律允许范围内的人肉搜索是公民正当行使言论自由权利、监督权、批评权的体现；但是，过激的、越过合法界限的人肉搜索则是网络暴力的一种、是一种侵犯个人隐私的行为。互联网数据时代犹如一张暗网，在为生活建立便捷通道的同时，也为违法行为披上了一层外衣，降低了网络侵犯隐私权的违法成本。如今，言论自由伴生的人肉搜索已经成为了一个值得重视的社会问题，其带来的对于隐私权的侵犯对于公民的法律权益造成了巨大的威胁[10]。

4.2. 公权力对隐私权的冲击

政府作为国家的掌控者和管理者，对于个人隐私信息的使用和保障方面有着重大的影响，政府通过对于公民个人隐私信息的掌握，为公民提供更加切合的社会服务。同时，政府为了更好地履行职能，会更加积极的探索和收集公民的个人隐私信息。但是，在政府收集公民个人隐私信息带来更好的服务职能的同时，我们也应该注意到其对于保护公民个人隐私信息方面的困难。政府为保障社会的公共利益，会要求网络服务商或者是自己留存一定期限的用户信息，保证在需要的情形下能够调取信息使用[11]。美国联邦调查局一直是公权力与隐私权的争议重点，其调查系统可以从网络数据中识别出认定为犯罪嫌疑人的邮件、轨迹、购买记录等个人信息，并将这些信息上传到美国联邦调查局的数据库中。在某些国家存

⁵ 百度百科: <https://baike.baidu.com/item/%E6%B3%84%E9%9C%B2%E9%97%A8/6386956?fr=aladdin>。

⁶ 百度百科: <https://baijiahao.baidu.com/s?id=1741399609081973019>。

在着法院、警方或者是安全监管机构在案件审理时有权利调查、收集公民、机构信息资料的情况，这种情况下，我们无法确认政府是否只是掌握与案件有关的情况还是掌握公民的所有信息。之后，前美国联邦调查局工作人员斯诺登披露的棱镜计划更是验证了政府对于隐私权侵扰问题的存在，斯诺登暴露美国联邦调查局存在一个计划可以对网络上的即时消息以及现有的数据进行深度的监测，包括使用美国此款服务器的所有人。棱镜计划包括微软、苹果、Youtube、雅虎、Facebook 等互联网巨头参与在内，可以读取到邮件、文件、即时消息、照片、视频、储存信息等个人隐私信息。而此数据库被美国总统每日简报引用一千多次，被国家安全局超过七分之一的报告使用[12]。

4.3. 商业发展对隐私权的冲击

商业发展对于隐私权的冲击可以从两个方面来研究，一方面是万维网对于隐私权的冲击，另一方面是电子商务对于隐私权的冲击。一方面，在大数据背景之下网络服务商通过不为人知的技术实现自动收集用户数据的功能，即使部分软件存在隐私权允许的选项，但在实际中，用户在大意或者知识有限的情况下是难以实现的。万维网在用户使用网络时，会自动的跟踪记录其个人隐私信息，并进行数据的重组合并，并经过精炼提升。另一方面，电子商务的蓬勃发展同时为个人隐私的保护带来了障碍[13]。淘宝、拼多多、京东在内的电子商务平台在用户不知情的情况下，收集用户的浏览记录、消费信息、日常声音，以此数据进行分析评估，并对用户的行为进行预测的问题是在我们日常生活中可以被感知到的。并且现实生活中存在一种常见的个人信息泄露骚扰事件，即电子商务人员拨打用户电话进行推销、讨好评、删差评等行为。对此，美国立法《请勿打我电话法》规定了明示拒绝机制，赋予消费者拒绝的权利。目前我国针对这一问题并没有针对的立法，造成隐私权保护的部分缺失。

5. 我国隐私权保护的建议

5.1. 规范大数据技术建设

大数据背景下对于隐私权的侵犯有部分原因是技术建设的不完善，故本文首先从规范大数据技术建设角度出发进行分析。第一，鼓励保护个人信息软件的推广。目前，网络服务商使用技术追踪用户信息的行为已经被公开并遭到了各方面的谴责抵制，万维网联盟引入网络隐私保护标准，欧盟实施需要经过用户同意的限定跟踪的法案。但是，落实保护隐私法律法规的现实需要就是加强对于大数据的建设，加强保护隐私的措施。保护个人信息软件的功能在于用户使用网络之前可以选择是否允许个人信息被读取、软件告知用户被读取个人信息的范围，用户拥有软件读取个人信息的知情权和选择权。目前这一软件已有部分萌芽，比如 P3P 平台、360 浏览器的反追踪设置，但是其技术不完善和普及不到位问题仍然需要进一步改善。第二，引进信息加密和保护技术。其一，引进安全套接层技术，安全套接层技术是由 Netscape 公司设置的通过公开密钥和对称密钥提供数据保密的安全服务，此技术可以通过密钥和算法对数据进行加密处理，防止违法读取。并包括以秘密共享方式保证个人信息完好、以双向验证技术保证信息安全。其二引进虚拟专用网技术，此技术主要致力于企业信息数据保护。虚拟专用网技术利用密钥管控技术、设备身份辨别技术、隧道技术以及加密解密技术，对发送的数据进行加密和封装，之后利用数据隧道进行传输，再将接受的数据进行解密和复原。并且，其密钥为临时性密钥，对加密数据形成了双层保护。

5.2. 完善隐私权监督保护制度

隐私权的监督保护仅仅靠法律规范是不足的，需要各方面的灵活配合，包括行业内的自律机制。行业内的自律机制可以弥补法律规范的不足，从而建立一种以法律法规为主，行业自律为辅的规范体

系，两者之间可以建立一种良性互动，以更好地保障公民的隐私权益。法律规定是统一的标准，缺乏灵活性，在实际中其往往只能最低限度的保护公民的个人信息。行业内的自律机制则具有灵活性和针对性，可以更加具有实效性地促进行业内的人员规范自身的行为，可以更加充分地保护用户的隐私权。法律规发不能超前或者盲目，其必须给予现实生活以一定的空间实施，而行业内的自律机制则能够更好的在保证法律规范实施的基础上，给予一定的自由。目前，我国的互联网协会存在自律公约，规定自发保障消费者的法定权益、个人隐私，不得利用用户的信息从事没有约定的不相关活动，不得利用其技术或者优势侵害用户权益。虽然，互联网协会的自律公约在一定程度上是关键一步的迈出，但是其在实践中并未对网络服务者起到切实的约束。本文认为行业内自律机制的建立应该联合多方主体，包括但是不限于政府、网络服务商、技术提供商等相关主题，建立专门协会或者机构对此行为进行针对性监督，坚决贯彻落实。

5.3. 提高公民隐私权的保护意识

相对于国外而言，我国公民在传统文化的熏染之下，人是排在社会和国家之后的，个人的独立人格意识较弱，对于个人隐私的保护和重视程度相对较弱。尤其在大数据背景之下，公民在保护隐私权不强烈的意识下，风险更大。本文认为对于公民隐私权意识方面的提高可以在各地区开展公民法制教育，细化到街道切实落实，提高公民对于隐私权的保护意识。可以参考美国专门建立的电子信息中心，此机构专门负责法令的实施以及向公民法律意识的普及。中国也可以建立专门向国家公民传播法律意识的机构，将公民法律意识提高的想法落实到实处。该机构可以针对公民隐私权薄弱的问题，展开隐私权有关的讲座、节目，引导公民树立保护隐私权意识，建立维权守法氛围。公民隐私权维权意识的提高，自然能够约束自我减少侵犯他人隐私权、保护自己隐私权的行为建立。

6. 结语

大数据背景下个人信息是构成互联网数据的基点，由此也造成了个人隐私信息暴露的高风险性质。我国《民法典》第一千零三十二条对隐私权做出了清晰的规定，明确个人隐私包括自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。由此，也反映出隐私权的权利客体包括个人信息、私人活动以及私人领域。不同于传统的工业背景，在大数据快速发展的推动下，个人隐私被侵犯的可能性不断地扩大，范围不断地扩展，强度不断地增加。由此，侵犯隐私权行为也展现出不同以往的特征。从主体、客体以及侵权方式来看，主体更加多元化，从传统的个人更多的扩展到了以主体为代表的互联网提供商、商业公司，甚至是政府部门；客体更加扩张化，从传统的住址、电话扩展到了行动轨迹、医疗或健康状态等；侵权方式更加隐蔽化，从传统的跟踪、偷拍到用户难以发现自己在网络的浏览记录或电子档案被窃取。从问题角度来看，则可以从言论自由、公权力以及商业发展三个维度分析隐私权面临的问题。公民享有言论自由，公平表达自己想法的权利，但是个人的自由如何与他人的隐私相平衡？同时，国家机关利用公权力收集和利用个人隐私来保护公民与如何保护公民隐私权相平衡？以及，商业为谋求发展，收集和使用用户个人信息以达到自我营销和推广的行为如何与保护用户的隐私权相平衡？技术发展、时代进步都是不可避免，如何应对不断出现的问题才是我们应该不断探究的目标。大数据背景下探讨隐私权的保护问题，应该抓住“大数据”和“隐私权”两个要点。就“大数据”而言，用技术来规制技术的发展是必要的，促进保护个人信息软件的推广、引入信息加密和保护技术都可以达到从“大数据”本身发展角度进行不断优化目的。就“隐私权”而言，从国家法制角度和公民意识角度两方面共同努力是可行之路。一方面，完善隐私权监督保护制度，为隐私权的保护树立坚实的后盾；另一方面，提高公民隐私权的保护意识，为隐私权的保护打造锋利的长矛。

参考文献

- [1] 齐鹏飞. 论大数据视角下的隐私权保护模式[J]. 华中科技大学学报, 2019, 33(2): 65-75.
- [2] 程啸. 论大数据时代的个人数据权利[J]. 中国社会科学, 2018(3): 102-122.
- [3] 吴伟光. 从隐私利益的产生和本质来理解中国隐私权制度的特殊性[J]. 当代法学, 2017(4): 50-63.
- [4] 彭支援. 大数据时代隐私权的保护面临的挑战与应对策略[J]. 乐山师范学院学报, 2015(1): 103-107+127.
- [5] 顾理平. 无感伤害: 大数据时代隐私侵权的新特点[J]. 新闻大学, 2019(2): 24-32.
- [6] 徐明. 大数据时代的隐私危机及其侵权法应对[J]. 中国法学, 2017(1): 130-149.
- [7] 范为. 大数据时代个人信息保护的路径重构[J]. 环球法律评论, 2016(5): 92-115.
- [8] 张新宝. 从隐私到个人信息: 利益再衡量的理论与制度安排[J]. 中国法学, 2015(3): 38-59.
- [9] 王利明. 我国侵权责任法的体系构建——以救济法为中心的思考[J]. 中国法学, 2008(4): 3-15.
- [10] 程啸. 民法典编纂视野下的个人信息保护[J]. 中国法学, 2019(4): 26-43.
- [11] 张新宝. 我国隐私权保护法律制度的发展[J]. 国家检察官学院学报, 2010, 18(2): 11-16.
- [12] Boyd, D. and Crawford, K. (2011) Six Provocations for Big Data. Social Science Electronic Publishing, Oxford.
- [13] Organisation for Economic Cooperation & Development (1980) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.