

新时代背景下个人数据信息安全治理研究

田喜清

(中国互联网络信息中心, 北京 100190)

摘要: 随着信息技术与经济社会的交汇融合, 数据信息翻倍增长。一方面, 数据的收集、共享和使用方便了人们的工作和生活, 另一方面, 导致了大范围、深程度的个人数据信息被侵犯。个人数据信息的侵犯, 不仅危及个人的财产安全和人身安全, 还可能危害到国家政治安全和社会公共利益, 因此个人数据信息的安全治理迫在眉睫。分析发现, 个人数据信息的安全治理包括加快数据信息保护立法进程、明确数据信息权属边界、规范平台数据收集行为等。

关键词: 数据信息; 个人信息; 政治安全; 安全治理

中图分类号: D923 **文献标识码:** A **文章编号:** 1674 - 5639 (2019) 01 - 0054 - 06

DOI: 10. 14091/j. cnki. kmxyxb. 2019. 01. 009

Research on Personal Data Information Security Governance in New Era

TIAN Xiqing

(China Internet Network Information Center, Beijing, China 100190)

Abstract: With the convergence of information technology and economic society, data information has doubled. On one hand, the collection, sharing and use of data facilitates people's work and life; on the other hand, it leads to the violation of a wide range of personal data information. The violation of personal data information not only jeopardizes the property security and personal safety, but also may endanger the political security of the country and the public interest. Therefore, the security management of personal data and information is imminent. The analysis finds that the security management of personal data information includes accelerating the data information legislation process, clarifying the data information ownership boundary, and standardizing the platform data collection behavior etc.

Key words: data information; personal information; political security; security governance

通过信息技术产生的各种大数据, 通过实时的挖掘、分析和计算, 推动着整个社会中知识和价值创造的发展, 培育新产品、新工艺和新市场, 成为了提高经济竞争力, 提升生产效率和调整部门职能的源动力。^[1]当前, 我们已进入信息科技革命的新阶段, 大数据将会彻底融入我们生活的方方面面, 我们的学习方式、出行方式、工作方式, 甚至我们吃的食物等。^[2]正如维克托教授指出的那样, “数据就像一个神奇的钻石矿,

当它的首要价值被发掘后仍能不断给予。它的真实价值就像漂浮在海洋中的冰山, 第一眼只能看到冰山的一角, 而绝大部分都隐藏在表面之下。”^[3]可见, 一个大规模生产、共享、应用数据的时代已经粉墨登场, 一幅崭新的数据世界蓝图正在徐徐显现, 数据日益成为国家的基础性战略资源, 对全球的生产、消费、流通、交换、分配等活动, 对经济社会的运行机制、网络安全以及人们的生产、生活方式和国家的社会治理模式产

收稿日期: 2018 - 07 - 16

基金项目: 国家社科基金青年项目“完善国家网络安全保障体系综合研究”(17CZZ019)。

作者简介: 田喜清 (1983—), 女, 苗族, 湖南怀化人, 副研究员, 法学博士, 主要从事互联网相关法律及政策研究。

生了深刻影响。一方面，数据的收集、共享、交易和使用方便了人们的工作和生活，另一方面也导致了大范围、深程度的个人数据隐私被侵犯。例如，2018年甚嚣尘上的脸书（Facebook）泄密事件，其本质就在于数据信息安全与数据传输流通及数据信息利用之间制度不完善。因此，在当前信息化日新月异、网民规模与日俱增、网络应用推陈出新、互联网极大便利人们工作生活与交互体验的大背景下，数据信息的安全治理刻不容缓。

一、数据信息的概念与数据来源

在现行的相关规定中，对个人信息保护主要集中在《网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的決定》《消费者权益保护法》及《电信和互联网用户个人信息保护规定》等法律和规章中。在《网络安全法》中，将个人信息界定为：“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自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。”换句话说，只要能单独或与其他信息相结合识别出个人身份的各种信息，都受网络安全法的保护。在2017年实施的《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》中，将公民的个人信息界定为：“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身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。”在欧盟《一般数据保护法案》中，将个人数据界定为：“任何指向一个已识别或可识别的自然人（数据主体）的信息。该可识别的自然人能够被直接或间接地识别，尤其是通过参照诸如姓名、身份证件号码、定位数据、在线身份识别这类标识，或者是通过参照针对该自然人一个或多个如物理、生理、遗传、心理、经济、文化或社会身份的要素。”

不难发现，无论是我国的网络安全法，最高人民法院、最高人民检察院的司法解释，还是欧盟的数据保护法案，个人信息的保护范围都包括身份

信息、行为轨迹等。因此，在本文的研究中，将互联网上记录的能够单独或与其他信息结合识别用户个人身份的各种信息、个人的私生活秘密以及网络留痕、行为轨迹产生的各种数据统称为数据信息。随着信息技术的发展，在一定程度上可以说数据信息是多维的、动态的、灵活的，它随着用户的生活经验、上网行为和交互体验而不断丰富，是秘密、安全、道德和伦理概念的重叠。^[4]在信息时代，大数据与信息技术的迅猛发展，用户数据信息财产价值获得了史无前例的关注和提升，海量的数据信息通过采集、加工、分析、挖掘、计算等大数据技术的处理，成为了财富创造的基础。在一定程度上可以说，对于数据信息的收集、存储、整理、交易和使用已经覆盖了人们生活、学习和工作的方方面面，大量涉及数据信息的内容被汇集到大数据之中，被越来越多的互联网企业、数据交易平台用于产品创新、市场营销而获利，成为了具有交换价值的商品，“还越来越多地被直接作为许可使用而获得直接经济利益的客体。”^[5]

当前，网络已经与我们的日常生活、学习、工作如影相随，用户上网的数据在大数据环境下让数据信息的丢失、泄露、滥用、非法交易等侵害数据权属、危害数据主体利益的行为屡见不鲜。那只“看不见的手”随时随刻都在抓取我们的数据信息，例如：京东、淘宝等各大购物网站的购物记录和消费习惯，百度、谷歌等搜索网站的查询记录和兴趣爱好，微博、QQ的聊天记录和社交关系网，滴滴、嘀嗒等打车记录和行程路线，微信、支付宝等手机支付的消费记录和财产状况以及各种App上的注册信息、地理位置信息、通讯录名单，等等。概而言之，这些数据信息的来源主要包括五个方面：一是用户为了办理网络接入、域名注册服务、提供信息发布、即时通讯等服务时与网络运营者签订的用户协议或是确认服务时提供的真实身份信息；二是用户在网上浏览、消费、查询、搜索等各种行为轨迹和网络留痕；三是在未经用户明确同意，在用户不知情或不完全知情的情况下的过度收集；四是在数据存储、传输、使用等过程中利用技术漏洞或是木马的窃取；五是与第三方或是合法获得数据信息的机构或公司进行的不正当交易。企业通

过合法、非法或不道德的手段获取了大量的用户数据信息,并利用这些数据信息挖掘其蕴含的潜在价值,促进企业的发展、业务的拓展、产品的创新、广告的推送、个性化的推荐等,从而获取更大的经济利益和商业价值。

二、数据信息领域的价值与挑战

大数据与物联网、云计算等信息技术的逐步融合和深度应用,把信息、用户、服务、机器等各种本来互无关联的各种元素通过网络联系在一起,利用关联规则、分类聚类算法,从海量不完整、不确定的信息源中挖掘出有价值的信息,并在这些相互关联的信息基础之上预判用户的生活状态、兴趣爱好、消费习惯、消费能力和行为方式等。而数据,作为信息流动的产物,对数据的分析和利用在金融、气象、交通、医疗、通信、农业及新闻资讯等方面已经广泛应用。Facebook 的副总工程师杰伊·帕瑞克说:“如果不利用所收集的数据,那么你所拥有的只是一堆数据,而不是大数据。”同时,由于信息技术和大数据技术本身正如硬币的两面,在服务经济社会发展和便利人们工作、生活的同时,数据信息在存储、分析和传输等各个环节侵犯用户数据信息现象俯拾皆是,用户数据甚至是在毫不察觉或毫不知情的状态下就被他人所掌握和利用,连具体的侵权责任人都难以确定。一些互联网企业通过线上线下的数据整合,将用户的行为习惯、活动规则、消费习惯、兴趣爱好等收集起来,进而形成对用户的精准定位,再把资讯、产品、广告和服务推送给用户消费,利用大数据“杀熟”。此外,由于用户数据信息在收集、存储、使用和交易过程中管理漏洞较多、违法成本较低、追责难度较大、违法手段不断升级等特性,使得大数据时代的数据信息保护面临巨大挑战。具体表现在以下几个方面:

(一) 数据信息的权属尚未确定

大数据时代,数据作为一种重要的战略资源,具有重要的商业价值和研究价值。与此同时,数据的收集、使用、加工、交易和传输还会导致数据信息泄露或滥用,侵害数据权利主体的合法权益和危害社会的公共利益,给用户的人身安全和财产安全

造成严重危害。数据信息的权属问题,如个人原始数据的权属、去标识化的数据权属、与第三共享的数据权属等,已经引起了社会的广泛关注。不过,到目前为止理论界和实务界对数据的权利和数据信息的权属问题尚未达成共识。例如,有学者认为数据权是一种新型人格权,有学者认为数据权是一种著作权,还有学者认为数据权是一种商业秘密权,更多的学者倾向于数据权是一种财产权,而在跨境的数据流通中,还涉及数据的主权问题,因此为了更好地促进数据产业健康、有序的发展,保护用户的数据信息,数据的权属有待进一步厘清。

(二) 数据信息的侵权行为难认定

由于个人数据信息收集的主体较多、收集的范围较广,掌握用户数据信息的企业或机构数据安全意识不强,安全保护技术不完善等多重原因,数据信息被侵害和利用数据信息进行违法犯罪的场景屡禁不止。再加上大数据技术是一把双刃剑,它既可以服务社会,也可以危害社会。网络社会的数据信息侵权行为更多的也是通过大数据技术和网络技术手段,侵犯数据信息的形式和方式不仅难以及时发现而且纷繁复杂。而相对于网络安全知识和技术手段比较贫乏的普通上网用户来说,数据信息受到侵害的场景不仅很难发现,甚至很多时候就算及时发现了也难以采取有效的措施进行权利救济。囿于用户网络安全技术保护能力的欠缺、互联网平台的责任推脱以及跨地区追诉成本较高等因素的多重制约,受害人往往难以取得通过司法途径获得权利救济的相关事实依据和证据材料,甚至更多的时候连侵权行为人都难以确定。

(三) 数据信息的侵权后果很严重

互联网的深入普及和广泛应用,大数据与信息技术打破了地域和时间的限制,数据传输速度快、传播范围广、流通体量大,一旦发生侵害数据权属所有人的行为,有可能给权利人造成的影响和损坏是难以挽回的,很多时候侵害的不仅仅是个人或几个人,而是大批量的用户数据信息泄漏。在一些电商平台、直播平台、社交平台等数亿级用户规模的平台企业中,用户数据信息具有极大的商业价值,侵权行为的发生可能会导致严重的经济损失,例

如：银行账户或密码被盗、信用卡被刷、账户余额被扣等。数据显示，仅2015年下半年到2016年上半年，网民因数据信息泄漏等原因造成的经济损失高达915亿元^[6]。在2016年的山东准大学生“徐玉玉电信诈骗”事件中，除了财产损害以外，还直接导致了被害人的人身伤亡。而在数据的非法跨境流动中，还有可能危害国家的政治安全和社会的公共利益。

此外，为了构建良好的数据生态，构建多维度、动态的、灵活的数据信息保护策略，面临着极大的挑战。我国自从1994年接入国际互联网以来，信息技术的发展极大地拓展了人类生存空间，改变了人们的生活方式，形成了以互联网为介质的网络社会。而与网络社会需求相适应的社会秩序和道德规范尚未真正建立起来，虽然数据信息保护问题首先是一个法律问题，但是法律并非万能，其调整范围也有一定的局限性，它不能解决网络社会中数据信息保护的所有问题，需要伦理道德的约束力予以辅助。因此，在一定意义上可以说，网络用户的数据信息权不仅仅是一项法律权利，而且还是一项道德权利。这些外在的法律、内在的道德，不仅给数据信息的法律保护提出了新的需求和挑战，也彰显了网络伦理道德对于数据信息保护的重要性。同时，网络平台为了提高市场竞争力，为用户提供更精准的服务或是个性化推荐，要求用户在注册时提供包括身份信息在内的多项数据信息，用户为了获得某些服务或便利也被动或不知情的开启了平台获取个人信息的多项权限。因此，当前出台完善的数据信息保护策略、构建良好的数据生态环境迫在眉睫。

三、安全治理：数据信息的前景

近年来，海量的用户数据信息是互联网企业参与市场竞争的砝码。一方面，用户的个人数据信息正变成具有使用价值和交换价值的商品，但是企业因此获得的财富却与用户无关。另一方面，互联网企业除了遵守国内的法律法规，保护国内用户的数据信息以外，在他们积极拓展海外市场的同时，也需遵守外国法律，需要让更加注重数据信息保护的西方消费者放心。因此，保护用户的数据信息不仅是互联网企业需要坚守的法律底线，同时还是应该

遵守的商业伦理和应当承担的企业社会责任，用户数据信息的安全治理势在必行。一方面，政府已经将发展大数据列为国家发展战略，旨在推进大数据的发展和应用；另一方面，政府和企业也需要提升网络安全的治理能力，保护数据信息安全。具体而言，包括以下几个方面的内容：

（一）加快数据信息保护立法进程

“立善法于天下，则天下治；立善法于一国，则一国治。”完善的法律体系，有利于用户数据信息不受信息技术侵犯。目前，我国已颁布的《侵权责任法》《消费者权益保护法》《民法总则》《全国人大常委会关于加强网络信息保护的决定》《电信和互联网用户个人信息保护规定》以及《网络安全法》等数十部法律法规涉及公民个人信息安全的保护。此外，在《刑法》及《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》等相关规定中也有相应的惩治条款。但是，这些法律法规对于电商平台、社交网络、App等大规模收集和抓取用户数据信息的行为约束力尚显不足。因此，需要通过专门立法进一步明确网络运营者和网络服务提供者收集用户信息的原则、程序和范围，并明确其对收集的数据信息进行保密和安全保护的义务，以及对非法使用、保护不力等应当承担的法律责任。同时，国家还要鼓励提高数据信息安全技术创新，对数据信息进行分级分类管理，避免对同一主体的同一信息采集单位过多，推动大数据场景下的数据防窃密、防篡改、防毁损、防泄露等安全技术的研发和部署。

（二）明确数据信息权属边界

大数据时代，原材料的采购、产品的生产加工，商品的消费和客户意见反馈等各个环节都在不断地被数字化，各种数据都在不断地被收集、处理和利用。这不仅有利于对生产的各个环节进行改革和优化，还可以形成新的数据商品和服务，创新供给模式，服务社会发展。数据产业在当前已经首当其冲地成为了最具发展潜力的领域之一，以贵阳大数据交易所等为代表的各个大数据交易所就是数据价值实现的主要平台。而数据的权属问题，是数据产业发展中最重要的基础性制度，数据权属清晰明

了,有利于数据产业的健康有序发展。数据的权属,简而言之就是数据的权利归属,在大多数情况下,数据信息不仅仅是一种人格权,也是一种财产权,尤其是经过匿名化处理的数据,更多的体现是其财产属性。因此,数据信息的权属至少包括两个层面:一是经合法取得的个人数据信息,这里的数据权属毋庸置疑的是属于数据主体本人,本人对于数据信息具有控制权;二是对合法取得的个人数据进行匿名化或去身份化处理的数据信息,数据控制人对数据具有有限的所有权,这里的数据主要体现为一种财产权益,受制于与个人信息主体的合同约定。数据权属问题的研究,有利于为数据交易的正常开展提供法律保障,同时也要重视数据交易过程中的安全风险。

(三) 规范平台数据收集行为

《网络安全法》要求网络运营者在为用户办理网络接入等入网手续或是提供信息发布、即时通讯等服务时提供真实身份信息,但并未明确应该提供哪些真实身份信息,对真实身份信息的范围和种类并未作出界定或限制。因此需要认真研究用户真实身份信息的范围和种类,避免信息收集主体和实名登记事项过多过滥,并创新实名信息收集的方式等。因此,任何互联网平台、网络运营者或网络服务提供者合法收集用户数据信息的前提至少包括三个方面:一是未经用户同意不得收集、使用和处分具有可识别用户身份的数据信息;二是即使在数据收集之前征得了用户的同意,也不得违反法律法规的规定和用户的约定超范围使用,同时在数据收集和使用的整个过程都必须遵守“合法性、正当性和必要性”原则;三是互联网平台无论是在技术上还是在基础规范和基本制度上,都要积极履行和承担平台的主体责任,确保用户充分地、合理地享有对个人数据信息的知情权、选择权、控制权、访问权和删除权(被遗忘权)等。

(四) 加强数据产业的行业自律

随着大数据、人工智能等信息技术的迅猛发展,数据产业方兴未艾。加之当前调整数据产业的法律法规较为滞后,带来了一些新型的数据侵权领域存在法律空白,给数据产业的行业自律提供了施

展才能的舞台。一方面,一些相关的数据行业组织本身处于数据业发展的上游,具有及时、敏锐、便利、高效感知市场发展动态的优势,有责任积极推动数据业的自律建设,尤其是在网络数据认证、个人数据信息的判定、数据保护技术规范等方面形成行业自律规约。积极推动形成全社会数据存储、使用、交易等方面的规范性,并从数据精度处理、去标识化、存储时间、未成年儿童数据特殊保护等方面入手,维护个人数据信息安全。另一方面,由相关行业主管部门指导成立数据信息保护监督社会组织,对企事业单位收集、使用个人信息活动进行监督,组织开展个人数据保护提升行动,对主流移动应用程序的用户隐私政策、服务条款和个人信息的收集使用行为进行评比,并定期向社会公开评比结果,督促各个平台建立健全数据安全保护机制。

(五) 提高用户数据安全意识

数据业的健康有序发展涉及多元社会主体,包括政府、企业和个人。但是当前无论是企业还是个人,甚至是政府部门,都亟待提高数据安全管理意识。一方面,由政府宣传部门组织有关单位利用互联网、电视、广播、报刊、杂志、公共电子屏和广告栏等,加强面向全社会,特别是青少年、老年人的个人数据信息安全方面的宣传教育,提升广大网民的数据安全意识和数据安全技能;网信部门继续办好国家网络安全宣传周,将个人数据信息安全作为重要内容进行广泛宣传。另一方面,要求企业,尤其是用户数量特别大的平台企业建立健全具有针对性和操作性的数据安全管理机制,落实平台企业主体责任,不得违规收集数据、不得滥用数据、不得泄露数据;并建立网络安全工作机构,督促指导网络安全和数据安全,在决策层面设立专门的网络安全或数据安全负责人。此外,还应提高公民依法保护个人数据信息安全的意识,广泛宣传、积极倡导个人合法有度有节制地使用数据信息,安全有效地规避大数据技术发展带来的信息安全风险。

四、结论

一言以蔽之,数据日益成为了国家的基础性战略资源,个人数据信息是国家基础性战略资源

的重要组成部分，个人数据信息安全不仅关乎个人的财产安全和人身安全，还涉及国家的网络安全和社会的公共利益。当前，我国已进入中国特色社会主义新时代，新时代应该有新的作为。个人数据信息的安全治理无疑是我国进入新时代的重要任务。近年来，各国关于个人数据信息保护的法律法规相继出台，例如美国的《隐私权法》，欧盟于2018年5月已经生效的《一般数据保护条例》等，为用户数据信息安全提供了坚实的保障基础。但是，就我国当前的个人数据信息发展现状来说，相关数据信息保护在数据的权属，网络运营者收集用户信息的范围等方面尚不明确，数据交易的流程和规则，对非法使用、保护不力等应当承担的法律责任等方面尚有空白。因此，一方面需要尽快出台个人数据信息安全保护的相关法律法规；另一方面相关执法部门要根据《网络安全法》等现行的法律法规加大对侵犯个人数据信息行为的违法查处力度，规范数据收集、使

用、交易、共享、出境等行为，提升数据产业的行业自律，提高个人数据安全意识，加强个人数据信息的安全治理，保护人民群众的合法权益，保障国家的网络安全和社会公共利益。

[参考文献]

- [1] 经济合作与发展组织. 数据驱动创新：经济增长和社会福利中的大数据 [M]. 张晓，译. 北京：中国工信出版集团，2017：2.
- [2] 史蒂夫·凯斯. 互联网第三次浪潮 [M]. 靳婷婷，译. 北京：中信出版集团，2017：42.
- [3] 维克托·迈尔-舍恩伯格，肯尼思·库克耶. 大数据时代 [M]. 杭州：浙江人民出版社，2013：127.
- [4] 刘雅辉，张铁赢. 大数据时代的个人隐私保护 [J]. 计算机研究与发展，2015（1）：229-247.
- [5] 刘德良. 个人信息的财产权保护 [J]. 法学研究，2007（3）：80-92.
- [6] 惠志斌，覃庆玲. 中国网络空间安全发展报告（2016）[M]. 北京：社会科学文献出版社，2016.

（上接第53页）

[参考文献]

- [1] 国家林业局. 中国林业统计年鉴 2015 [M]. 北京：中国林业出版社，2016：440-444.
- [2] 习近平. 关于《中共中央关于全面深化改革若干重大问题的决定》的说明 [N]. 人民日报，2013-11-16（01）.
- [3] 国家发展改革委有关负责人关于启动新一轮退耕还林还草答记者问 [EB/OL]. [2018-06-03]. http://www.ndrc.gov.cn/zcfb/jd/201409/t20140927_679119.html.
- [4] 中华人民共和国国务院第367号令. 退耕还林条例 [EB/OL]. [2018-06-09]. http://www.gov.cn/gongbao/content/2003/content_62531.htm.

