部门法专论

论网络行为数据的法律属性与利用规则

梅夏英　朱开鑫

摘　要: 大数据时代,网络服务提供者对于网络行为数据的商业化利用日益深入,所引发的纠纷亦愈发频繁。信息处理技术的进步与网络商业模式的发展使得网络行为数据具备了对用户身份的间接可识别性,因而网络行为数据应归属于间接个人信息的范畴。网络行为数据的技术特征与商业利用模式决定了其与用户的隐私利益关涉甚微,传统个人信息理论中的"知情同意原则"也不再具备合理性与可行性。在肯定用户对网络行为数据享有所有权的基础上,引入网络著作权利用领域的"选择性排除规则",有望实现保护用户隐私与促进数据经济发展的合理平衡。

关键词: 网络行为数据　间接个人信息　知情同意原则　选择性排除规则

中图分类号: DF529　文献标识码: A　文章编号: 1673 - 8330(2019)02 - 0032 - 10

DOI:10.13893/j.cnki.bffx.2019.02.004

欧盟《通用数据保护条例》(General Data Protection Regulation,简称 GDPR)的施行以及美国《2018 年加州消费者隐私法案》(California Consumer Privacy Act of 2018,简称 CCPA)的颁布,在全球范围内引发了数字信息时代个人信息保护与利用研究的新一轮热潮。历经数十个摩尔定律周期后,人类社会已经正式进入了大数据时代,信息技术的发展使得人们在网络空间中的一举一动都存在被数据化和商业化利用的可能。网络行为数据即在此背景下诞生,并成为数字信息时代个人信息保护与利用研究中一个无法回避的问题。所谓"网络行为数据",是指网络服务提供者通过 cookie 等互联网跟踪记录程序收集的反映用户个人在线行为活动的数据,包括用户的浏览记录、交易记录、检索记录等。[①]近年来,网络服务提供者对于用户网络行为数据的商业利用日趋深入,由此引起的纠纷亦愈发频繁。司法实践中各国对网络行为数据的法律属性以及利用方式都存有误区与困惑,但理论界至今对此鲜有论述。笔者拟就网络行为数据法律属性及利用问题进行探讨,以期从理论角度对现实问题做出回应。

一、网络行为数据法律问题的现实争议

毋庸置疑,我们正面临着一场伟大的时代变革——大数据时代已然来临,正悄然改变着每个人的思维和生活。[②]在大数据时代,最为核心的要素无疑是数据本身,其是大数据得以实现价值的基础。

[作者简介] 梅夏英,对外经济贸易大学法学院教授,博士生导师。朱开鑫,对外经济贸易大学法学院与美国波士顿大学法学院联合培养博士研究生。

① 参见梅夏英《数据的法律属性及其民法定位》,载《中国社会科学》2016 年第 9 期,第 164 页。

② 参见[美]大卫·芬雷布《大数据云图——如何在大数据时代找寻下一个大机遇》,盛杨燕译,浙江人民出版社 2014 年版,第 44 页。

虽然各个国家都在轰轰烈烈地推行大数据战略并如火如荼地开展各项立法，但对于数据的基础理论研究仍处于起步阶段。关于数据的法律属性与利用方式，各国至今尚未达成基本共识。在现实操作层面，数据产业的发展实践更是处于无规制的混乱状态，此问题从各国司法实践之中可见一斑。早在 2012 年 Kevin Low v. LinkedIn Corporation 案中，美国加州地方法院便驳回了用户针对网络服务提供者收集和出售其网络行为数据的侵权诉讼。在该案中，网络服务提供者 LinkedIn 公司利用 cookie 程序大量收集载有用户 ID 信息(包括 LinkedIn ID 和 cookie ID) 、个人主页信息以及在线浏览记录的网络行为数据，并把这些数据提供给了第三方商业机构开发利用。用户据此提出了两项诉讼请求，一是依据加州宪法和普通法(the California Constitution and the Common law) ，服务商的行为构成对其隐私权的侵犯; 二是依据全美广告欺诈法(the False Advertising Law) ，服务商的行为构成对其个人信息中财产性利益的侵害。加州法院在判决中虽然肯定了网络服务提供者利用在线跟踪记录程序收集的用户网络行为数据属于个人信息的范畴，但认为网络行为数据中包含的人身和经济利益远没有达到法律对于隐私权和财产权保护的基本要求，因而驳回了用户的诉讼请求。③ 2015 年在被称为“中国 cookie 侵权第一案”的“朱烨诉北京百度网讯科技公司侵犯隐私权案”中，二审的南京市中级人民法院改变了一审的南京市鼓楼区人民法院有利于原告的判决结论，认定网络行为数据不属于个人信息的范畴，网络服务提供者收集和利用用户网络行为数据的行为不构成对其隐私权的侵犯。二审法院在判决中称被告百度公司个性化推荐服务收集和推送信息的终端是浏览器，没有定向识别使用该浏览器的网络用户身份。百度公司在提供技术服务过程中运用 cookie 等互联网跟踪记录程序收集、利用的用户在线浏览记录、检索记录以及交易记录是未能与用户个人身份对应识别的数据信息，该数据信息的匿名化特征不符合“个人信息”对于可识别性的要求。④

上述案例表明对于网络行为数据的商业化利用，中美两国司法机关都持以开放性的态度并对服务商进行了侵权责任豁免，但二者据以作出上述判决的理由却迥然相异: 美国法院是在承认网络行为数据属于个人信息的基础上，以未造成用户相关权益损害为由拒绝适用隐私权和财产权的保护路径; 中国法院则直接将网络行为数据排除出个人信息的范畴，从而作出用户不享有隐私权保护的判决。虽然中美两国对于网络行为数据的法律认定不尽相同，但都是从个人信息的角度对其进行法律属性和利用规则的分析探讨。不无遗憾的是，2018 年 8 月 31 日全国人大常委会表决通过的《中华人民共和国电子商务法》(下文简称《电子商务法》) 虽然将网络行为数据的保护和利用问题涵摄其中，但却通过“合法权益”的表述避开了对于其法律属性的认定; 而对于网络行为数据的利用规则，《电子商务法》则通过转介条款的方式将其延伸到《广告法》领域。⑤ 数字经济的发展扩展了人们的生存空间，并赋予了我们更大的行动自由，而如何对这些新兴领域进行合理引导和规制则是法律不断发展和创新的动力所在。在数据产业发展日渐兴盛的背景下，对于用户网络行为数据的分析和利用是当前一段时间内数据经济的核心所在，网络行为数据已然成为大数据分析的核心内容。因此我们需要反思，对于网络行为数据的法律属性究竟应如何加以认定，其是否属于个人信息的范畴? 若得出肯定结论，那么在大数据时代的今天，网络行为数据的价值基础与利用规则能否适用传统个人信息保护理论? 笔者试就这些现实问题进行深入的理论探讨。

---

③ See 900 F. Supp. 2d 1010(N. D. Cal. 2012) .

④ 参见江苏省南京市中级人民法院(2014) 宁民终字第 5028 号民事判决书。

⑤ 《电子商务法》第 18 条 “电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务的搜索结果的，应当同时向该消费者提供不针对其个人特征的选项，尊重和平等保护消费者合法权益。电子商务经营者向消费者发送广告的，应当遵守《中华人民共和国广告法》的有关规定。”

二、网络行为数据间接个人信息属性的证成

网络行为数据作为反映用户在线活动轨迹的一类特殊数据，是根据数据记载的信息内容进行的一种类型划分。我们要探讨网络行为数据的法律属性，首先就要厘清数据的法律属性以及其与信息的关系。“信息”和“数据”二概念起源于拉丁文：信息意指“告知”或“指示”，而数据则是“已知”或“事实”的意思。计量和记录一起促进了数据的诞生，它们是数据化最早的基础。⑥ 笔者认为现今人们所称的数据是信息时代的产物，特指网络数据，即可由计算机处理的以 0 和 1 表示的二进制码形式存在的信息体，是内容与形式、信息与代码的结合体。这个结合体的表层是信息，数据的价值就在于其反映的信息内容的价值。这个结合体的内核则是代码，数据是指固定在代码这种特殊载体上的一类信息，即这些有价值的信息都是以 0 和 1 表示的二进制代码的形式存在于计算机硬件设备或网络空间之中。⑦ 代码赋予了数据独特的属性，将其与其他具有信息表达功能的事物相区分，并限定了数据存在的领域与应用的范围。代码本身具有高度的数字化特征，是虚拟空间中的比特流，其只承担一种载体性质的功能，不属于现今民法体系上任何一种权利的客体。就像现实环境中的原子与分子，虽然其组成了物理世界的万千事物，但是其本身并不具备独立的价值与意义。因此，数据应被归为信息的一种特殊表现形式，对于网络行为数据法律属性的探究也就立足于其反映的信息内容的法律属性当中。

中美两国在司法实践中对于网络行为数据作出了截然不同的属性判断，即美国法院肯定了其个人信息的法律属性，而中国法院则持否定态度。笔者认为，在信息时代的今天，美国法院的结论更加符合当前数据经济和信息技术的发展现状。从比较法角度来讲，两大法系国家对于个人信息的法律界定已经达成了基本共识：明确将可识别性作为个人信息判定的依据，并通过直接识别和间接识别二分法将其分为直接个人信息与间接个人信息两类。欧盟《通用数据保护条例》第 4 条规定，“个人数据是指任何指向一个已识别或可识别的自然人的信息，该自然人可被直接或间接识别。”美国《2018 年加州消费者隐私法案》第 1798. 140 条 O 款规定，“个人信息系指直接或间接地识别、关系到、描述、能够相关联或可合理地链接到特定消费者或家庭的信息。”我国虽然尚未颁布专门的“个人信息保护法”，但在 2017 年 6 月正式施行的《中华人民共和国网络安全法》第 76 条第 5 款亦明确规定，“所谓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自然人个人身份的各种信息”。笔者认为，网络行为数据应归属于间接个人信息的范畴，即虽然单一的网络行为数据并不具备用户身份的可识别性，但通过对多渠道收集的网络行为数据集合进行比对分析，便可识别出信息主体的身份。对于网络行为数据的开发利用，早已从网络时代对个人信息的精确收集转向基于大数据样本中数据挖掘产生相关个人信息的关联集成。大数据交叉分析基础之上的二次开发利用，使得那些看似与个人信息无关的数据最终具备了对于信息主体的可识别性。⑧

随着信息技术的不断发展，网络行为数据具备了对用户身份进行识别的条件。近些年来涌现出诸如网站信标（Web Beacons）、深度包检测（Deep Packet Inspection）、cookie 等一大批搜集用户网络行为数据的技术手段，其中最常用的便是 cookie 程序。cookie 是网络服务提供者为了便捷用户的登陆和访问，而存储在用户个人终端中的加密数据。cookie 文件的形成过程是：目标网站的服务器会在用户访问该网站时，向用户的个人电脑生成并发送经过加密且只能由目标网站读取的数据，这些数据负

⑥ 参见［英］维克托·迈尔－舍恩伯格、肯尼斯·库克耶《大数据时代》，盛杨燕、周涛译，浙江人民出版社 2013 年版，第 12 页。

⑦ 参见陈兵《大数据的竞争法属性及规制意义》，载《法学》2018 年第 8 期，第 107 页。

⑧ See Anupam Chander, *How Law Made Silicon Valley*, 63 Emory Law Journal 2004, pp. 639—694.

责记录并上载用户的身份信息和浏览信息。⑨ cookie 文件涵盖了用户浏览的页面和内容、浏览的时间和停留的时长、输入搜索引擎的查询项目等，也能被用来保留用户密码或添加到网络购物车中的商品数据。⑩ 单个的网络服务提供者或许只能收集用户某一领域的网络行为数据，但互联网的本质就在于开放性与共享性，即由多家独立网站组成的数据应用联盟大大增强了其数据的整体收集能力，这使得网络服务提供者建构用户完整的个人信息图谱已不再是难事。⑪ 通过对用户的持续追踪，网络服务提供者建构起日益丰富的数据档案从而具备了对用户身份的识别能力。⑫ 因此，信息技术的发展与网络商业模式的创新使得网络行为数据具备了对用户身份的间接可识别性。

从反证的角度来讲，网络服务提供者在有关数据商业化利用的纠纷中，大都声称自身已经通过匿名化处理技术切断了网络行为数据与用户之间的身份联系。所谓“信息匿名化”，指的是让所有能揭示个人身份的信息都不出现在数据集合之中。这样一来，数据就可以在被分析和应用的同时，不会威胁到信息主体的隐私。⑬ 信息匿名化虽然在小数据时代具有可行性，但在大数据时代伴随数据总量和种类的增多，数据集合体内部的交叉检验使得匿名化处理技术失效了。美国在该领域的两个经典案例——“美国在线案”与“奈飞公司案”，都表明对于用户在线信息的匿名化处理在大数据时代不再奏效。⑭ 总的来讲，网络行为数据匿名化处理失败是由两个因素引起的：一是可供开发利用的数据越来越多，服务商会结合不同来源的数据进行应用分析；二是伴随数据处理技术的不断进步，服务商深度分析数据的能力大大提升。⑮ 美国《基督科学箴言报》曾撰文称“在现有技术条件下，网络服务提供者即使不掌握他人的姓名和 SSN(Social Security Number) ，但只要能够获取出生、性别和邮编这三个数据项，其便可以成功识别全美 87% 的人口。”⑯因此，从数据匿名化处理角度并不能否定网络行为数据具备对信息主体的身份可识别性，这从反面论证了网络行为数据的间接个人信息属性。

从比较法角度来讲，世界各国对于网络行为数据的法律属性都在进行积极的回应，且基本都将其归入个人信息的范畴。早在 2012 年，美国联邦贸易委员会便发布命令要求九大信息服务提供商提供如何收集和使用消费者信息的报告，其在报告附录中将“一项持续的识别符，例如 cookie 用户编号或者处理器序列号”与姓名、地址、邮件地址并列为个人信息。⑰ 《2018 年加州消费者隐私法案》规定，“个人信息包括但不限于因特网或其他电子网络活动信息，包括但不限于浏览历史、搜索历史和关于消费者与因特网网站、应用程序或广告交互的信息”。欧盟《通用数据保护条例》对于网络行为数据

---

⑨ 参见张晓阳《基于 cookie 的精确广告投放技术及其法律边界刍议——以朱烨诉百度公司隐私权纠纷为视角》，载《电子知识产权》2015 年第 9 期，第 81 页。

⑩ 参见朱松林《论行为定向广告中的网络隐私保护》，载《国际新闻界》2013 年第 4 期，第 94 页。

⑪ 前文“朱烨诉北京百度网讯科技公司侵犯隐私权案”中百度广告联盟便是一个典型的例子，被告百度公司通过与新闻、娱乐、游戏、论坛等各领域的网站合作，收集用户在各个成员网站上的浏览信息、检索信息和交易信息并向用户定向发送广告。

⑫ 参见前引⑨。

⑬ 参见金耀《个人信息去身份的法理基础与规范重塑》，载《法学评论》2017 年第 3 期，第 120 页。

⑭ 2006 年 8 月美国最大的因特网服务商“美国在线公司”向社会公布了大量的网络检索数据，希望研究人员据此得出有益的分析结果。虽然“美国在线”声称已经将所有数据进行了严格的匿名化处理，但一个来自佐治亚州的 62 岁的寡妇还是被媒体通过分析“60 岁单身男性”“有益健康的茶叶”“利尔本的园丁”等关键词检索记录识别出来，一时舆论哗然，美国在线公司的高管因此无奈辞职。仅仅时隔两个月，美国在线影片租赁提供商奈飞公司陷入了同样的尴尬境地。在 2006 年度的“Netflix Prize”算法竞赛中，奈飞公司本意希望通过分析经过匿名化处理的电影租赁记录数据来提升自身电影推荐系统的准确性，但一个尚未“出柜”的同性恋母亲的身份信息在比赛过程中被意外公布在网上，随后其愤然起诉了奈飞公司。尽管赛前，奈飞公司也对数据进行了精心的匿名化处理。

⑮ 参见左卫民《迈向大数据法律研究》，载《法学研究》2018 年第 4 期，第 139 页。

⑯ See Mark Clayton, *US Plans Massive Data Sweep*, The Christian Science, February 9, 2006. 转引自徐子沛《大数据》，广西师范大学出版社 2013 年版，第 178 页。

⑰ See Federal Trade Commission, Order to File Special Report, File No. P125404(2012) . 转引自朱芸阳《定向广告中个人信息的法律保护研究——兼评“Cookie 隐私第一案”两审判决》，载《社会科学》2016 年第 1 期，第 103 页。

虽未加以明确规定,但将“在线身份识别信息、个人偏好、兴趣、信度、习性”等网络行为数据的重要组成部分都囊括进了个人数据的范畴。值得注意的是,2017年欧盟委员会通过的《隐私与电子通讯指令》则明确表示网络服务提供者利用cookie技术收集的用户在线数据属于个人数据的范围。我国对于网络行为数据的法律属性没有成文法规定,但最高人民法院在2015年《全国民事审判工作会议纪要》中明确将网络用户的上下线时间、网络浏览日志、网页地址、使用的搜索引擎关键词等网络行为数据纳入个人信息的保护范畴。⑱

三、网络行为数据“知情同意原则”的适用困境

两大法系国家关于个人信息保护理论的相关论证虽多有不同,但基本都是从人格权角度入手。传统个人信息保护理论的核心准则在于让信息主体自主决定是否、如何以及由谁来获取和利用他们的信息,即由权利人牢牢把控个人信息的利用权能。⑲ 在此背景下,两大法系国家对于个人信息的获取和利用都采用了严格的“知情同意原则”(notice and consent)。所谓“知情同意原则”,是指政府机关和其他商事机构只有在明确告知信息主体个人信息的收集和使用状况并获得明确同意的情况下,才可以对其个人信息进行收集和利用。⑳ 大陆法系国家鉴于二战时纳粹集团对于个人信息滥用导致的灾难,故将个人信息权当作公民的一项基本人权来加以保护。以德国为例,个人信息权是一般人格权的一项重要内容,学者大多认为,侵害个人信息实际上等同于对个人自由的侵害,因而需要法律的保护。通过保护公民个人信息不受数据处理技术等手段的侵害,就可以达到保护公民人格尊严和人格自由的效果。㉑ 在此理论背景下,欧盟强调公民个体对与其自身有关的信息拥有绝对的控制权,严格限制公权力组织和商事企业对于公民个人信息的收集和利用。欧盟《通用数据保护条例》这一被称为“史上最严个人信息保护法”的出台便是此种立法倾向的集中体现。但在大数据时代,当个人信息以网络行为数据的形式呈现时,其商业价值不断凸显而相关的人格利益却不断淡化,对于此立法精神的坚守虽然在一定程度上起到了对公民人格权的保护,但无疑阻碍了欧盟数据产业的发展。㉒

英美法系国家受判例法传统影响,没有形成体系化的人格权保护模式。他们采用了“大隐私权”的概念,将个人信息纳入其中,通过隐私权的保护路径对个人信息的开发利用进行规制。英美法系国家学者从社会交往角度审视隐私权,发展出“有限接近自我”理论,对传统隐私权加以阐释。弗瑞德将这种对人际关系的维护和对个人信息的控制联系起来,认为隐私和人际交往密切相关,是我们对自身信息的控制,享有隐私就意味着我们有权允许或者拒绝他人对我们个人信息的获取和使用。㉓ 这一理解迈出了美国通过隐私对个人信息进行保护的重要一步,将消极的防御权利变成了对于个人信息积极支配和利用的权利。㉔ 即使是被称为全美最严厉隐私保护法案的《2018年加州消费者隐私法案》,核心仍旧是立足于数据经济发展的大背景,促进企业对于个人信息的合理化利用。美国肯定个人信息积极利用价值的态度与做法,一定程度上促进了美国数据产业的蓬勃发展。㉕

隶属于大陆法系的中国至今未在立法层面采纳“个人信息权”的概念,理论界和实务界都是从隐

---

⑱ 《最高人民法院2015年度全国民事审判工作会议纪要》第20条规定,能够单独或者相互结合识别特定个人身份及行为隐私的信息构成网络公民个人信息(如网络用户的网络认证账户和密码、IP地址、上下线时间、网络浏览日志、网页地址、使用的搜索引擎关键词,公民个人的姓名、职业、家庭、婚姻、指纹、音频、视频等)。

⑲ 参见张里安、韩旭至《大数据时代下个人信息权的私法属性》,载《法学论坛》2016年第3期,第119页。

⑳ 参见龙卫球《数据新型财产权构建及其体系研究》,载《政法论坛》2017年第4期,第63页。

㉑ 参见杨芳《德国一般人格权中的隐私保护——信息自由原则下对自觉观念的限制》,载《东方法学》2016年第6期,第104页。

㉒ 参见王利明《论个人信息权的法律保护——以个人信息权与隐私权的界分为中心》,载《现代法学》2013年第4期,第62页。

㉓ See Charles Fried, *Privacy*, The Yale Law Journal, Vol. 77, No. 3, 1968, pp. 475—493.

㉔ 参见江海洋《侵犯公民个人信息罪超个人法益之提倡》,载《交大法学》2018年第3期,第139页。

㉕ 参见杨惟钦《价值维度中的个人信息权属模式考察——以利益属性分析切入》,载《法学评论》2016年第4期,第66页。

私权角度论证个人信息保护的合理化基础，对于非隐私性的个人信息则鲜有论述。早先便有学者提出对于个人信息的分类应采纳我国传统理论上“阴私”的概念，将其分为“阴私”类个人信息和除“阴私”以外的个人信息。“阴私”类信息包括裸照以及性行为、性生活、恋爱经历、不为人知的重大疾病和生理缺陷等，对这部分信息采用隐私权的保护模式；[26]非“阴私”类信息包括诸如家庭住址、工作单位、通信号码等，对这部分信息他人可以披露或使用，但不可以滥用。[27] 笔者认为，此观点值得肯定，公民个体对于非“阴私”类的个人信息并无特别的利益需要加以保护。他人在保证不滥用的情况下可以直接对这部分个人信息加以获取和利用。[28] 笔者认为这一理论恰恰可以运用到网络行为数据商业化应用的分析之中。网络行为数据作为对用户在线活动轨迹的反映，主要由用户的交易行为记录、浏览行为记录、搜索行为记录等组成，与上文所述的“阴私”类个人信息相去甚远。笔者认为，网络行为数据虽然在法律属性上归属于个人信息的范畴，但与信息主体的人格利益特别是隐私利益关涉甚微。

在我国《侵权责任法》颁布之前，法律对隐私权的保护采取一种间接保护模式。《中华人民共和国宪法》第 38 条至第 40 条关于公民人格尊严、私人住宅、通信自由和通信秘密的保护规定为其他部门法及司法解释保护公民个人隐私留下了广阔的空间。《侵权责任法》的颁布使得隐私权成为一项独立的人格权，但与生命权、健康权、身体权等绝对权相比，隐私权的定义不够精确，权利范围也不够明晰。因此在侵害隐私权案件中进行违法性判断时，司法机关要求加害人具备主观上的认知并存在侵害故意。[29] 作为隐私权保护最为发达的国家，美国在隐私侵权认定上一个很重要的标准就是被控行为必须构成对他人的“高度冒犯”，从而影响了正常的社会交往活动。[30] 一方面，网络服务提供者收集用户网络行为数据的目的在于对用户在线行为分析结果的商业应用，而非关注数据主体的私密类信息，因此并不存在侵犯数据主体隐私的主观意愿。另一方面，网络行为数据反映的是用户在网络空间中的活动轨迹与行为表现，是用户维持网络社会正常交往所必需的一部分。这部分数据与用户的个人隐私关涉甚微，故而对其进行分析利用无法达到对信息主体“高度冒犯”的标准。只要保证服务商不对网络行为数据加以滥用，其获取和利用网络行为数据便无问题。前文案例中，中美两国司法机关虽然在网络行为数据法律属性的认定上存在分歧，但都认为服务商对于网络行为数据的获取和利用不构成对用户隐私权的侵犯。

按照大陆法系国家传统的个人信息保护理论以及英美法系国家隐私权保护理论，他人想要获取与利用个人信息都必须通过“知情同意原则”来实现。德国作为世界上最早制订个人信息保护法的国家，在《联邦数据保护法》第 4 条第 1 款中明确规定“只有在本法或其他法律允许或规定或数据主体同意时，个人数据的收集、处理和使用才是被许可的。”美国则在其《隐私权法》中针对个人信息披露之同意规定“除非是根据信息相关人的书面请求或事先的书面协议，任何机构不得通过任何方式与其他个人或机构联系，披露信息系统中的任何个人信息……”[31]晚近立法，诸如欧盟《通用数据保护

---

[26] 欧盟《通用数据条例》第 9 条在关于特殊种类的个人数据处理部分中也明确规定“对于揭示种族或民族出身，政治观点、宗教或哲学信仰，工会成员的个人数据，以及唯一识别自然人为目的的基因数据、生物特征数据，健康、自然人的性生活或性取向的数据的处理应当被禁止。”

[27] 参见刘德良《个人信息法律保护的正确观念和做法》，载《中国信息安全》2013 年第 2 期，第 47 页。

[28] 从比较法角度来讲，依据内容的私密程度对个人信息进行类型化界分存在现实依据。美国即将个人信息划分为敏感信息和一般信息，针对敏感个人信息进行专门立法实行更为严格的保护，如针对儿童隐私保护的《儿童在线隐私保护法案》(COPPA) 即为典型代表。

[29] 参见陈聪富主编《侵权违法性与损害赔偿》，北京大学出版社 2012 年版，第 150—159 页。

[30] See Restatement (Second) of Torts, § 652A—D.

[31] 参见任龙龙《论同意不是个人信息处理的正当性基础》，载《政治与法律》2016 年第 1 期，第 126 页。

条例》和美国《2018 年加州消费者隐私法案》,亦都明确规定“知情同意原则”是对于用户个人信息开发利用的前提基础。[32] 尽管我国目前尚未出台专门的“个人信息保护法”,但现行相关立法亦采纳了此种模式。《网络安全法》在第 41 条和 42 条中明确规定,网络运营者收集、使用或向他人提供其收集的个人信息,需经被收集者同意。此外,众多“个人信息保护法学者建议稿”也均对同意基础作了明确的规定。[33] 但在大数据时代,网络行为数据自身所具有的特殊性以及数据产业发展的实际状况决定了其难以简单适用传统个人信息利用领域中的“知情同意原则”。

“知情同意原则”在数据时代不再具有适用上的合理性。一方面,网络行为数据的价值很大一部分体现在“二次开发利用”中,[34]而这些用途会随着社会发展以及技术进步而不断扩张。服务商在收集网络行为数据时并不能预知这些潜在的用途,也就不存在告知用户数据开发用途并获得相关同意的可能性。另一方面,网络行为数据以代码为载体,代码本身的技术性特征决定了网络行为数据产生和存在的方式突破了“知情同意原则”设立的前提条件——信息的最初控制权在信息主体手中。在现有网络架构之下,由于技术性使然,网络行为数据一旦产生便由网络服务提供者而非网络用户自身所直接占有和控制。[35] 网络行为数据的产生过程高度受控于网络服务提供者所提供的技术服务,我们在登录、点击与浏览任何一个网站时,除非服务商主动加以删除,否则产生的全部网上行为记录都会被实时储存在该网站的服务器当中。因此在一定程度上我们甚至可以说,相较于传统的个人信息存在状况,网络服务提供者比我们自身更加熟悉并掌握更多我们自身的网络行为数据。

“知情同意原则”在数据时代亦不再具有适用上的可行性。单个用户通过合同的方式与网络服务提供者进行交易谈判,将自身的网络行为数据以一定的价格授权给服务商使用的可能性并不大。一方面在现实操作层面,网络行为数据的主体——在线用户数量庞大且过于分散,由服务商获得数据个体的许可成本过高,并且单一用户的网络行为数据价值又过低,因而在网络行为数据领域采纳“知情同意原则”不具有经济上的合理性。另一方面在具体实践中,“知情同意原则”的运行效果并不理想,形式大于实质。基于网络服务提供者和普通用户谈判地位的悬殊,服务商完全可以通过格式条款的方式,强迫用户在“用户协议”中接受将自身产生的网络行为数据免费授权给服务商使用。[36] 基于技术上的不对称地位,网络服务提供者亦可以超过用户授权的范围获取和开发其网络行为数据,用户实际上很难发现并对服务商的数据利用行为进行监督。因此,我们需要为网络行为数据的开发利用建构相较于传统的“知情同意原则”更为合理和有效的利用模式。

四、网络行为数据权利配置和利用规则的新建构

从哲学角度看,能量和信息是人类社会赖以存续和发展的两个基本要素,其中能量是人类生存和发展的物质基础,而信息则具有调动和促进能量生产的作用。因此在人类社会发展史上,每一次信息技术的革新,往往都会引发既有物质生产模式乃至整个社会形态的重大变化。伴随大数据时代的到来,人类社会正经历着一场新信息革命的洗礼,在日趋成熟的信息化技术面前,人们行为的一举一动,社会生活的一点一滴,乃至自然环境的一草一木都具有数据化的潜质。在此种技术环境下,对于网络

---

[32] 参见欧盟《通用数据保护条例》第 6 条第 1 款之规定以及美国《2018 年加州消费者隐私法案》1798. 100 条 B 款之规定。

[33] 参见周汉华《中华人民共和国个人信息保护法(专家建议稿)及立法研究报告》,法律出版社 2006 年版;齐爱民《中华人民共和国个人信息保护法示范法草案学者建议稿》,载《河北法学》2005 年第 6 期。

[34] 所谓个人信息的“二次开发利用”,也称价值利用,是指信息控制者将其所搜集掌握的个人信息,通过一定程序算法的分析、筛选、对比、加工等方法,进行整理和重新组合,形成附加值更加突出的个人信息数据库,再对该数据库进行利用的过程。参见张涛:《个人信息权的界定及其民法保护》,吉林大学 2012 年博士学位论文,第 70 页。

[35] 参见梅夏英《虚拟财产的范畴界定和民法保护模式》,载《华东政法大学学报》2017 年第 5 期,第 42 页。

[36] 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》,载《清华法学》2015 年第 3 期,第 94 页。

行为数据的权利配置和利用规则相较于传统个人信息保护理论中的“知情同意”方式必然存在不同之处。

一方面，按照劳动价值理论，谁付出了劳动谁就应对劳动产物获得权利。数据具有高度技术化的特征，服务商提供的在线服务是数据产生和存续的决定性因素。网络行为数据虽然从内容上讲反映的是用户的在线活动轨迹，但从根本上讲若没有服务商架构的网络空间，没有服务商不断的数据收集和处理工作，其便无从而来，也无从存在。[37] 另一方面，我们需要明确信息具有流动性和共享性的特征，信息的价值就在于主体对其流通的垄断性控制权，谁取得了对信息的控制权谁也就在事实上占有了信息的价值。[38] 数据作为一种具备特殊载体的信息亦是如此，谁取得了数据的控制权，谁就实际上掌握数据的使用价值。由于数据以代码的形式存在，其一旦生成就直接存储于在线服务器当中，事实上由网络服务提供者控制和占有，而网络用户并不具备直接获得和控制数据的技术与能力。因此，笔者认为，相较于传统个人信息理论中将信息利用权能赋予用户所有的“知情同意”模式，对于网络行为数据而言将其利用权能赋予网络服务提供者则更具合理性和价值性。[39]

对于网络行为数据的探讨，我们不能脱离数据经济发展的宏观背景。长久以来，传统个人信息理论一直侧重于对信息主体人格利益的保护。但在大数据背景下，面对网络行为数据这一新兴的个人信息表现方式，相关理论规则的探讨就不能再忽视对其经济价值的开发利用。网络行为数据自互联网产生之日起即为客观存在，之所以近年来才引发各界的广泛关注，原因在于数据经济的蓬勃发展导致其商业价值日益凸显。伴随数据产业的崛起与网络用户的激增，网络行为数据的收集与交换有爆炸化发展之趋势。英国著名的行政学家佩里希克斯曾在《个人生活与公共政策》一书中断言：“我们必须承认数据现今已经成为当代经济活动和行政管理运行中的基础动力。”在互联网商业模式下，数据价值的大小取决于其可商业化利用的程度，而数据的商业化利用程度恰恰又取决于其能否反映网络用户实际商业需求的行为习惯、兴趣爱好、个体特征等。一定程度上可以说，对于数据产业发展真正起到推动作用的恰恰就是网络行为数据，其已然成为当前数据开发领域中的重点。在数据商业实践中，网络行为数据已经“为营销之目的而被广泛使用”，上文提到的中美两国案例实际都涉及定向行为广告这一网络行为数据新兴商业化应用领域，并充分体现出其在大数据背景下的经济价值。“网络行为定向广告”(Online Behavioral Advertising)是定向广告的一种特殊形式，它是基于追踪互联网用户的网络浏览行为，根据所追踪的数据分析网络消费者的偏好及个人特性，并向其进行个性化广告推送的一种新型广告模式。[40] 在大数据、智慧营销、移动互联网等时代背景下，网络行为定向广告将会成为未来全球广告业发展的“蓝海”。这就充分表明网络行为数据的价值基础应立足于经济价值的开发，而非过分强调对于信息主体人格利益的保护。

“任何对于互联网的规制都不应阻碍其发展”，这是互联网法律领域的一项基本原则。从整个数据产业的发展角度思考，可以最大程度实现网络行为数据经济价值的主体只能是网络服务提供者。一方面因为单一网络行为数据的商业应用价值基本可以被忽略，可以给用户带来的经济利益极为有限；另一方面即便不存在现实的威胁，用户天然具有对自身隐私泄露的非理性担忧，因而我们可以断言，网络用户在很大程度上会径直将自身掌握的网络行为数据加以删除。在市场化条件下，网络服务

---

[37] 参见程啸《大数据时代的个人数据权利》，载《中国社会科学》2018 年第 3 期，第 102 页。

[38] 参见李延舜《个人信息权保护的法经济学分析及其限制》，载《法学论坛》2015 年第 3 期，第 43 页。

[39] 参见[法]伯纳德·利奥托德、[美]马克·哈蒙德《大数据与商业模式变革：从信息到知识，再到利润》，郑晓舟、胡睿、胡云超译，电子工业出版社 2015 年版，第 5—8 页。

[40] 参见蒋玉石、张红宇、贾佳、杨力《大数据背景下行为定向广告(OBA)与消费者隐私关注问题的研究》，载《管理世界》2015 年第 8 期，第 182 页。

提供者最有能力和条件实现数据的商业价值，因此只有将网络行为数据交由专业的服务商加以开发利用才不会浪费数据本身的价值。[41] 并且根据现行的数据商业化利用模式，服务商将成千上万的网络行为数据收集起来的目的通常并非为了解个体，而是要把若干个具有某种共同特性主体的个人信息按一定的方式创设数据库，以该数据库所反映的某类群体的共性来满足自身或其他数据使用人的需要。[42] 因此，我们无须过分担忧将网络行为数据商业化应用的情况下可能给用户个人隐私带来的威胁。

有鉴于此，笔者认为，在网络行为数据权利配置和利用规则的设计上可以借鉴网络著作权治理领域的“选择排除规则”(Opt-Out Rule)。“选择排除规则”是网络搜索引擎服务商在促进版权数字作品开发和传播的基础上，为降低侵权风险而进行的一项制度创新。[43] “选择排除规则”最早实践于美国谷歌公司的在线图书计划当中：谷歌先行以电子扫描的方式将尽可能多的图书收录进其在线数据库当中，以方便用户在线阅读；著作权人有权在谷歌将自己作品数字化储存后选择将其删除，或者可以选择接受此种收录，并从谷歌图书获得60美元的一次性支付对价以及后续相关利润63%的长期收益。在我国，百度公司在自己的音乐搜索业务中也采纳了“选择排除规则”：音乐著作权人享有充分的自主选择权，其可以要求百度音乐屏蔽盗版歌曲的链接，也可以允许百度音乐使用盗版音乐链接，并从盗版音乐的广告收益中抽取一定比例的分红。

谷歌公司和百度公司各自的著作权“选择排除规则”在具体运作中虽有细节差别，但基本逻辑都是由搜索服务商首先径行利用他人作品，然后允许著作权人选择要求其删除作品，或者选择与其合作并分享利用作品所获得的收益。在网络行为数据利用领域引入“选择排除规则”，可以通过以下思路进行权利配置和制度设计。首先，明确网络行为数据的所有权归属于信息主体即网络用户所有。[44] 其次，采用默示许可的方式，由网络服务提供者直接对用户的网络行为数据进行获取和开发利用。但服务商需要通过“网站说明”等方式告知用户，其会为用户提供哪些免费的增值技术服务或在线体验特权，作为开发利用用户网络行为数据的回馈。[45] 再次，网络用户应当享有实际可行的拒绝网络服务提供者获取和使用其网络行为数据的途径，在此情况下，服务商则有权中止提供给用户的额外技术服务或在线体验特权。

在网络行为数据“选择性排除规则”应用过程中，有两方面的问题需要引起我们足够的重视：

一是网络服务提供者必须为用户提供明确易行的拒绝途径，这是“选择性排除规则”的合理性立基。我们必须保证用户拥有自主选择是否将网络行为数据交由服务商获取和使用的选择自由。[46] 从技术角度来讲，现行网络服务领域的“DNT协议”(Do Not Track)可以有效地解决此问题。所谓“DNT协议”，是指用户有权利和途径通过自己明确的行为向网络服务提供者表明其在线行为不希望受到服务商的追踪和记录，并拒绝后续的商业性开发利用。那些对网络行为数据的开发利用持怀疑否定态度的用户，有权拒绝网络服务提供者的数据开发要求。微软公司于2012年率先宣布在其IE程序中支持“DNT协议”，之后Mozilla的Firefox、苹果的Safari以及Google的Chrome浏览器都开始对“DNT协议”提供兼容支持。国内的360公司也在推广其360浏览器时重点强调其在程序设计中包

---

[41] 参见[美]比尔·弗兰克斯《驾驭大数据》，黄海、车皓阳、王悦等译，人民邮电出版社2013年版，第33页。

[42] 参见洪海林《个人信息财产化及其法律规制研究》，载《四川大学学报(哲学社会科学版)》2006年第5期，第118页。

[43] 参见宋哲《网络服务商注意义务研究》，北京大学出版社2014年版，第165—167页。

[44] “数据财产化”理论创始人美国莱斯格教授称，依据法经济学分析，由网络用户掌握数据所有权才是最有效率的。一方面只有网络用户掌握了数据财产权，才会改变其在数据市场被忽略的境地，迫使服务商在开发利用数据时不得不考虑可能涉及的隐私风险；另一方面若将数据所有权授予服务商，网络用户需要耗费大量成本才能防止其个人信息不被滥用，因为其存在集体行为的困境(collective action problem)。See J Kang, *Information Privacy in Cyberspace Transactions*, 50 Stan. L. R. 1998, p. 1193.

[45] 参见张新宝《“普遍免费+个别付费”：个人信息的一个新思维》，载《比较法研究》2018年第5期，第1页。

[46] 参见余筱兰《信息权在我国民法典编纂中的立法遵从》，载《法学杂志》2017年第4期，第22页。

含了 DNT 服务、清除 cookie 等功能。这在一定程度上表明网络服务提供者在利用网络行为数据的同时，已经对保护用户的隐私利益达成了基本共识，网络行为数据“选择性排除规则”因而具备适用的现实可行性。

二是在鼓励数据经济发展的同时，我们应当建立起对网络行为数据后续开发利用的有效监督管理机制。为了适应大数据时代的新形势，我们在网络行为数据利用领域架构起了不同于传统个人信息保护模式的“选择性排除规则”。在采纳此规则的基础上，我们应当力求实现数据产业发展与用户权益保护的合理平衡，一方面我们为服务商获取、利用用户网络行为数据创造更加便捷可行的途径，另一方面我们应当采取有效措施防止服务商对于网络行为数据的后续滥用。网络服务提供者需要基于其可能对信息主体所造成的影响，对涉及网络行为数据再利用的行为进行安全评测，并依据用户的合理化要求删除可能对其造成伤害的数据信息。[47] 我们所建立的网络行为数据监管机制应当建立在区分数据的属性和用途的基础之上，对于不需要或者只需要适当标准化保护的网络行为数据，可由网络服务提供者自主制定相应的开发和保护规则。但对于一些危险性较大的项目，行政管理机构必须设立规章，规定服务商应如何评估风险、如何规避和减轻对于网络行为数据主体的潜在伤害。这种规则设计将激发服务商对于网络行为数据的创新性再利用，同时也能确保用户免受隐私泄露而造成的损害。

The Legal Nature and Utilization Rule of the Internet Behavior Data

MEI Xia – ying & ZHU Kai – xin

Abstract: In the era of big data, internet service providers have increased the commercial use of network behavior data, which leads to an increasing number of disputes. The progress of information processing technology and the development of internet business model make it possible to identify users´identity through internet behavior data indirectly; therefore internet behavior data should be characterized as personal information. Due to its particular technical features and business model, the internet behavior data has little concern with users´privacy interests, and thus the “Notice and Consent Rule” in traditional personal information theory is no longer reasonable and feasible. On the basis of affirming users´ownership of network behavior data, we should introduce the “Opt – Out Rule” in the online copyright area to balance the protection of users´privacy and the promotion of the development of data economy.

Key words: internet behavior data　indirect personal information　Notice and Consent Rule　Opt – Out Rule

[47] 参见范为《大数据时代个人信息保护的路径重构》，载《环球法律评论》2016 年第 5 期，第 92 页。