

Doi:10.11835/j.issn.1008-5831.fx.2019.06.001

欢迎按以下格式引用:胡朝阳.大数据背景下个人信息处理行为的法律规制——以个人信息处理行为的双重外部性为分析视角[J].重庆大学学报(社会科学版),2020(1):131-145.Do:10.11835/j.issn.1008-5831.fx.2019.06.001.

Citation Format: HU Chaoyang. Legal regulation of personal information processing action in the background of big data: From the perspective of dual externalities of personal information processing[J]. Journal of Chongqing University(Social Science Edition), 2020(1):131-145. Do:10.11835/j.issn.1008-5831. fx. 2019.06.001.

大数据背景下个人信息 处理行为的法律规制 ——以个人信息处理行为的双重外部性为分析视角

胡朝阳

(东南大学 法学院,江苏 南京 210096)

摘要:大数据背景下个人信息处理行为既引发数据安全风险等负外部性,也会带来分享经济价值实现等正外部性,“大数据悖论”现象揭示了双重外部性成因。基于“外部性内在化”原理赋予信息主体以个人信息权并赋予数据控制者以大数据财产权虽有助分别规制其双重外部性,但网络大数据背景下其双重外部性规制彼此交互影响而面临两难困境。法经济学关于“损害之相互性”理论证立了基于“风险导向理念”规制个人信息处理以破解其两难困境的经济逻辑。大数据产业发展有赖个人信息处理的“外部性外部化”而实现分享经济。法经济学关于“公地悲剧”理论证立了基于“外部性外部化”规制个人信息处理而满足大数据产业发展需要的经济逻辑。大数据背景下个人信息处理的规制有赖从“压制型法”到兼及“回应型法”的理念转换,从“外部性内在化”兼及“外部性外部化”的机制并举,从数据资源权利配置兼及数字技术权力干预的措施协同,实现大数据产业创新与个人信息安全的有机平衡。

关键词:大数据;个人信息处理;双重外部性;大数据悖论;法律规制

中图分类号:D922.8 **文献标志码:**A **文章编号:**1008-5831(2020)01-0131-15

随着大数据、人工智能与移动网络等信息网络技术的发展,个人信息被大量采集转移使用,网络数据生成及大数据分析正深刻揭示个人信息及其数据处理所潜藏的巨大价值。用户个人信息与网络运营商大数据集在其全生命周期中面临客体交织与利益交叉,用户与大数据企业之间及大数

修回日期:2019-05-15

基金项目:中央高校基本科研业务费专项资金资助项目(2242015S20060)

作者简介:胡朝阳,男,法学博士,东南大学法学院教授,江苏高校区域法治发展协同创新中心、东南大学科技法与知识产权研究所研究员,主要从事知识产权法研究,Email: hucy1221@hotmail.com。

据企业相互之间围绕用户信息处理及大数据挖掘利用所衍生数据利益产生剧烈角力与争夺。近年来围绕网络空间数据取用出现了系列纠纷^①。美国今年3月Facebook信息泄露事件表面上源自互联网平台基于“信息流广告”^②采集用户信息进行大数据分析所致,深层上折射出消费者对Cambridge Analytica 数据公司滥用数据的担忧与恐惧。值此背景,美国2018年6月28日通过的《2018加州消费者隐私法案》(CCPA)与欧盟2018年5月25日实施《一般数据保护条例》(GDPR)相比,两者虽殊途同归但宗旨与价值取向不同,CCPA旨在规范数据的商业化利用,GDPR意在保护基本人权,在对个人信息的使用上,CCPA“原则上允许,有条件禁止”,GDPR“原则上禁止,有合法授权时允许”。在我国着力加强个人信息保护又大力促进大数据产业发展背景下^③,协调两者关系亟待合理规制个人信息处理行为。

目前,学界针对个人信息处理行为规制的探讨涉及个人信息与大数据的属性、权属及其保护与利用的冲突化解。为此,一方面基于权利规制进路展开。例如,Lessig认为,“个人必须具有针对隐私进行协商的能力”,随着互联网信息技术的发展,将数据作为财产并赋予用户以财产权的财产规则保护个人信息相对侵权责任规则的传统法律架构更具优势^[1]。国内学界围绕个人信息权构造与大数据权配置展开探讨^[2],指出大数据时代个人数据权扩张妨碍数据产业发展,主张数据企业享有其合法收集、存储和利用个人数据的绝对权,强调个人只享有消极防御的信息自决权以应对其数据收集和利用不当所致人格与财产侵害^[3]。另一研究进路则基于行为规制展开。例如,Mayer-Schönberger认为,大数据时代告知同意、模糊化或匿名化处理等隐私政策均告失效,主张“从个人同意到让数据使用者承担责任”,实现责任与自由并举的信息管理^[4]。倡导风险导向^[5]与场景导向^[6]的隐私管理新理念。国内学界检讨个人信息处理适用“告知同意”规则的正当性^[7],探索其适用“去身份”规则的行业标准^[8],提出其基于场景的风险理念规制的可行性^[9]。鉴于大数据时代信息控制者在个人信息利用上强激励与其保护上弱激励而去探索建立激励相容的个人数据治理体系^[10]。此外,还有基于“卡-梅框架”及其“规则菜单”组合保护模式,分析数据法益在其产生者与使用者间优化配置及财产规则与责任规则对不同类型数据及其不同处理阶段的适用选择^[11]。

针对大数据时代个人信息的私权属性^[12],有研究提出质疑并强调个人信息为公共物品而非稀缺资源,不存在“公地悲剧”问题,其适用财产规则保护面临低效,主张施以公权规制^[13]或社会控制^[14],分析指出个人信息兼有隐私自主价值和在社会交往中获取一定经济利益及某种社会评价与服务的使用价值^[15]。但值得注意的是,大数据背景下个人信息处理与数据资源开发利用互为表里,大数据分析价值挖掘有赖个人信息生态系统海量集成的大数据资源及其数据“喂养”优化算法的“公地喜剧”^④式效应,从而促进其共享经济实现。其个人信息处理既引发数据安全风险,也带来分

①例如,新浪微博诉脉脉(京73民终[2016]588号)、大众点评诉百度(沪73民终[2016]242号)、深圳谷米诉武汉元光(粤03民初[2017]822号)、淘宝(中国)诉安徽美景(浙8601民初[2017]4034号)等不正当竞争案均涉及用户信息数据之争;此外还有,顺丰与菜鸟互相关闭数据接口争议(国家邮政局调解),华为与腾讯关于华为荣耀Magic手机侵害微信用户数据争议(工信部调解),江苏省消保委诉百度民事公益诉讼案,美国HiQ Labs对LinkedIn领英的数据抓取纠纷案,美国Facebook信息泄露事件等。

②一种依据社交群体属性对用户喜好和特点进行智能推广的商业模式,由网络平台汇聚整合用户各种行为大数据而由广告公司进行数据分析并实现定向投放,类似国内的今日头条、微博等平台运营模式。

③工业和信息化部颁布《大数据产业发展规划(2016—2020年)》将大数据产业界定为“以数据生产、采集、储存、加工、分析、服务为主的相关经济活动”。

④“公地喜剧”概念由耶鲁大学法学院教授Carol Rose首次提出,公地问题上既有“公地悲剧”也有“公地喜剧”,结果是随着不同的制度、文化等情境而产生的“公地戏剧”。See Carol Rose. The Comedy of the Commons: Custom, Commerce, and Inherently Public Property. University of Chicago Law Review, 1986, 53(3): 711-781.

享经济价值收益,即其溢出效应具正负双重外部性且呈交互影响格局^⑤。因而,规制其个人信息处理行为不应仅以负外部性视角或限于“外部性内在化”^⑥规制方式,而应以个人信息处理全生命周期为观察对象,以其正负双重外部性及交互影响为切入视角,基于多元进路探寻其法律规制可能的破局。

一、大数据背景下个人信息处理行为的双重外部性

大数据背景下个人信息处理既可能施加信息主体以隐私披露不当或施加信息控制者以数据泄露他用等数据安全风险成本的负外部性,也可能带给信息主体以服务质量提升或带给信息控制者以算法设计优化等分享经济价值收益的正外部性,其双重外部性交互影响。

(一) 大数据背景下个人信息处理行为的负外部性

大数据背景下个人信息来源极其复杂^⑦,其在网络空间的存在形式与取用方式变动不居。例如,网络平台用户注册身份信息、运营商通过 Cookies 工具抓取用户日志及业务与位置等行为信息、政务管理部门主动采集、网络爬虫 iworm 从系统窃取、第三方开发者通过 OpenAPI 接口协议从开放平台间接共享或挖掘分析原生数据推测所得,既有用户输入点击行为而记录存储的原生数据,也有基于原生数据经算法加工与聚合生成的衍生数据。我国 2018 年 5 月 1 日启用的信息安全技术标准《个人信息安全规范》具体界分了个人信息与个人敏感信息并以附录对其范围和类型进行列举,个人信息如用户操作记录、IMEI 信息、设备 MAC 地址等;个人敏感信息如指纹、网页浏览记录和精准定位信息等。

随着信息数字化程度的提升,各类先进传感技术与高科技身份识别技术发展,个体行为触发包括语言、地理位置,甚至味觉、触觉、情绪等直接或间接承载身份属性的信息都能转化为数字形态存储并具备其可用性,个人信息内涵外延不断丰富发展并随其使用环境、使用主体及信息主体性质的不同而持续变化,以往基于一元论的共性描述与静态描述界定个人信息内涵则面临现实挑战。大数据背景下个人信息处理会带来信息泄露、隐私侵害、数据不当采集转移与使用乃至数据垄断或数据滥用等负外部性。在美国 Facebook 信息泄露事件中, Cambridge Analytica 数据挖掘公司被指利用来自第三方 App 收集转移 Facebook 用户 5 000 万点赞信息,据此分析其用户性格和政治倾向而人为制造“信息茧房”^⑧以定向推送信息影响选民政治立场,引发公众对个人信息处理行为负外部性的广泛关注。大数据信息平台的开放共享性及计算机代码的可破解性使个人信息面临被窃取他用风险,

^⑤外部性问题由阿尔弗莱德·马歇尔在其《经济学原理》中首先提出,后由庇古充实完善,最终形成了外部性理论。参见:[美] 格里高利·曼昆《经济学原理》(梁小民、梁砾译,北京大学出版社,2014年版201页)。外部性体现为某经济主体未经市场交易对另一经济主体施加的成本(负外部性)或是收益(正外部性)。

^⑥以庇古为代表的新福利经济学主张对负外部性以征税或对正外部性以补贴的政府干预规制, See A. C. Pigou, *The Economics of Welfare* 134(4th ed. 1932); See T. Scitovsky, *Two Concepts of External Economics*, *J. Pol. Econ.* 143(1954)。以科斯为代表的制度经济学主张对负外部性以科责或对正外部性以赋权的产权交易规制, See R. H. Coase, *The Firm, the Market, and the Law*, Chicago, The University of Chicago Press, 1988, p. 28。科斯《社会成本问题》侧重负外部性角度指出外部性的相互性。“公地悲剧”效应则显示正外部性的相互性存在。

^⑦关于大数据概念有以 IBM 为代表的技术型界定或以 Gartner 等代表的非技术型界定,包括本体论、工具论与资源论等。笔者认为,大数据是基于“4V”特征的海量数据集以分析挖掘彼此勾连“目的信息”(Boyd, 2012)的技术工具,也是基于多渠道海量数据而快速分析以产生可用于行动“知识流”(Kalyvas, 2016)的信息资源。

^⑧凯斯·桑斯坦考察互联网信息传播指出,公众对信息的需求是个性化的而非全方位的,往往只注意选择使自身愉悦的信息领域,久而久之将自身桎梏于像蚕茧一般的“茧房”中,信息茧房(Information Cocoons)概念由此而生。参见:凯斯·桑斯坦《信息乌托邦——众人如何生产知识》(法律出版社,2008年版6-10页)。

其数据交易与数据共享面临隐私合规与数据权属等挑战,其数据分析与数据产品开发面临算法偏差与去标识后再识别风险。大数据开发利用与价值挖掘赖以继的数据生态系统倘若呈现数据垄断、数据滥用、数据歧视等,围绕其信息主体的个人信息处理行为便呈现负外部性。

鉴于个人信息处理的负外部性,我国《民法总则》第111条规定个人信息须依法收集、使用、加工、传输并受法律保护。《网络安全法》专章规定网络用户数据信息取用行为不仅要遵循“合法、正当、必要”与目的限定原则,还要遵从向用户“告知同意”程序规范和对用户信息转移“去身份化”要求。《个人信息安全规范》从信息的收集、保存、使用、共享、转让、公开披露等方面详细规定了个人信息处理行为规范^⑨。规定个人信息控制者(指有权决定个人信息处理目的、方式等组织或者个人)开展个人信息处理活动时应遵循权责一致、目的明确、选择同意、最小够用、公开透明、确保安全、主体参与等基本原则,对个人信息的委托处理及共享、转让作出相关规定。相对于欧盟《一般数据保护条例》(GDPR)规定数据可携权^⑩、被遗忘权^⑪、算法可解释权^⑫(The Right to Explanation of Automated Decision)等权利配置,我国现行制度设计虽然为规制个人信息处理的负外部性提供了支撑,但其在适应大数据产业基于个人信息处理的创新发展趋势上的合理有效性尚待观察。

(二)大数据背景下个人信息处理行为的正外部性

大数据背景下的个人信息处理行为也会带来所谓“正外部性”。一方面,数据中间商大量收集如用户自愿提供、电脑记录测量、挖掘分析推测等行为信息并为其正外部性创造条件^{[16]40-44};另一方面,大数据分析将传统结构化数据与非结构化数据的价值结合,如社交网络生成内容、图片、视频、监测、传感器、位置、搜索日志等非结构化数据占全球数据逾95%,其极具商业情报价值,挖掘其相关性与数据模式可掌控市场趋势与消费行为^{[17]8}。

首先,大数据背景下个人信息处理行为的网络外部性具有促进分享经济实现的正效应。传统的“公地悲剧”理论揭示了过度使用权属不明的公地会导致资源枯竭现象。不过在互联网背景下,“消费者从技术应用中所获价值与使用该技术的人数正相关。这增加了新技术的市场需求,进而又提升了研究者的创新激励”^{[18]1-2}。其实,大数据资源的价值挖掘基础正在于其信息共享及其关联利用。大数据背景下某个体对信息的使用并不影响其他个体使用该信息,无数个体可同时共享同样的信息,那些使用者少、兼容性低的孤立数据或技术未必有利用户。数据控制者取用以个人信息为客体的信息品数量愈多、愈广,其数据分析挖掘的网络外部性效应发挥愈可靠、精准,形成所谓“公地喜剧”现象^[19]。从平台用户(顾客、商户)采集而来的消费模式、驾驭行为、可靠程度、购物习惯等个人数据,其采集与处理过程往往彼此关联,“因采集何种数据的决定本身就依赖于关于未来如何利用这些数据的创新性思考”^{[18]380-381}。大数据分析可使网络中众多个人信息之间相互关联,大数据产业中个人信息网络每个节点都有较强关联度,而网络外部性(network externalities)的强弱与网络的规模及其关联度息息相关^[20]。可见,大数据背景下个人信息处理行为通过提供“喂养”大数据

⑨我国《个人信息安全规范》作为国家推荐标准的软法规制工具,为保护大数据产业发展起见,将匿名化后不可恢复识别的信息及出于公共利益或学术研究而采取去标识化的个人信息作为同意规则的例外。

⑩又称数据转移权,即用户可自主将个人数据以机器可读格式畅通无阻地直接迁移至新的网络运营商。这使Google、Facebook等数据挖掘巨头面临因用户转移而丢失大量数据的挑战。

⑪又称被删除权,即数据主体有权要求数据控制者删除个人数据,数据控制者对此有遵从义务且不能过分延长数据留存时间。这使以cookie形式收集数据、从定向投放广告中获益的技术巨头面临莫大损失。

⑫又称算法公平性,即数据主体有权要求算法自动决策者给出解释,不满意算法决策时有权选择退出。如贷款申请人被算法决策拒绝时有权寻求合理解释。此权利设置难免深度制约乃至延缓AI智能技术发展。

分析及其智能算法的“饲料”,发挥其促进个人信息开发利用与开放共享的“网络外部性”正效应。

其次,大数据背景下个人信息处理行为的网络外部性正效应发挥有赖其产业运作模式下的规模收益递增(边际成本递减)。在互联网领域,规模收益递增(边际成本递减)是“公地悲剧”现象产生的必要条件,网络外部性外部化(共享经济)是“公地悲剧”现象产生的充分条件,相对宽松而又恰当的竞争政策对互联网领域“公地悲剧”的持续形成十分重要。“公地悲剧理论”(Theory of Comedy of The Commons)建立在如下八组基础概念基础上^[21]:争用性与限用性(竞争性与排他性)、传统公地品与信息品、普通外部性与网络外部性、外部性内部化与外部性外部化、有形网与无形网、“右版权”与“左版权”、公地与公地品、公地悲剧与公地喜剧。基于“公地悲剧理论”,大数据形态下的原生信息不满足“争用性”(Rivalrous)却有一定的“限用性”(Excludable)^⑬。在大数据背景下,若将原生态的个人信息划归私人物品范畴而让其成为私人财产权客体,将私人财产属性赋予个人信息主体,则对充分激发其“网络外部性”正效应释放却未必有利。基于信息生态系统的数据信息规模化集成与数字技术交互式兼容而进行个人信息处理行为,有其推动共享经济实现并产生“公地悲剧”现象的正效应^⑭,由此揭示了基于“网络外部性”之外部化而实现共享经济模式的经济逻辑。

(三) 基于“大数据三重悖论”的双重外部性成因探析

大数据具有透明化悖论、身份悖论与权力悖论等三重悖论(Three Paradoxes)^⑮,这使大数据背景下个人信息处理面临正负效应并存的双重外部性^⑯。

首先,信息透明化要求与信息搜集秘密进行的透明化悖论使个人信息处理呈正负外部性。大数据背景下个人信息处理需遵循告知、选择、访问规则等透明化要求^{[17]54-57}。告知即明确数据采集的实体、用途、性质、方式及其潜在接收方;选择即信息主体对数据二次使用或超原初目的使用或与第三方共享时有权选择加入(opt in)或退出(opt out);访问即信息主体可及时、便捷地访问数据控制者掌握的信息,质疑不准确信息,更正或删除其不需要及存储不当信息。美国《2018 加州消费者隐私法案》(CCPA)除赋予消费者上述权利外,还规定企业可为个人信息的收集、出售或者删除提供财务激励,包括根据消费者的数据在合理范围内向其提供差异化费率或价格的商品或服务甚至向其支付赔偿金^⑰。事实上,透明化要求可以扭转用户与数据控制者的信息不对称进而给用户个人信息安全保障,促进其信息的开放共享以及基于“网络外部性”的外部化而实现“公地悲剧”式的开发利用,激发大数据分析挖掘的正效应溢出,促进共享经济发展。不过,基于透明化悖论其信息搜集秘密进行又使个人信息面临着潜在的安全威胁,可能导致企业过度采集用户信息甚至数据滥用等负外部性。

其次,大数据开发利用识别个人身份与其识别个人身份中牺牲个人或者群体身份隐私的身份悖论使其信息处理呈正负外部性。一方面,大数据开发利用有赖采集海量个人信息包括原生数据

^⑬“争用性”即你用别人便不能用,“限用性”即可限制别人使用。两者兼具的是私人物品(Private Goods);两者皆不具的是公共物品(Public Goods)。后者面临市场失灵而前者不会。不具“争用性”但具“限用性”的是俱乐部物品或曰共享品(Club Goods),其通过赋权(例如信息产权)等权利配置解决市场失灵问题。

^⑭例如,API(Application Programming Interface)作为应用程序编程接口可应用于所有计算机平台和操作系统,这些API以不同格式连接数据,每种数据格式要求以不同的数据命令和参数实现正确的数据通信。

^⑮Neil M. Richards & Jonathan King. Three Paradoxes of Big Data. 66 Stanford Law Review Online 41 (2013).

^⑯悖论是表面上同一命题或推理中隐含两个对立结论却又不能自圆其说。逻辑学上指可同时推导或证明两个互相矛盾命题的命题或理论体系。抽象公式是“如事件A发生,则推导出非A,非A发生则推导出A”。

^⑰See CCPA, <https://www.jdsupra.com/legalnews/the-california-consumer-privacy-act-of-25374/> (2018-9-1 访问)。

和衍生数据(推测数据),以预测特定行为发生的可能性^{[16]41-53},据此发现其关联事物间的相关关系^[22]。另一方面,随着“数据中间商”大量运用 Cookie[®] 收集用户信息甚至从以社交网络服务 SNS 为主的数据源中任意获取包括关注热点、兴趣爱好、居住地址、出入场所、消费习惯、购买记录等数据,网络运营商不仅秘密收集用户信息用于对其记分并施以差别对待,还据此开发出独特的“记分制度”并用于商品化销售^{[16]52},导致社会被等级化。例如,网约车平台司机给用户贴上属性标签(Tag),其识别用户身份有助赋予司机以接单激励而提升约车效率,有益其信息处理的正外部性实现,但倘若司机给用户贴上不良属性标签(如性暗示或差评),便有牺牲用户隐私而影响信息安全甚至引发数据歧视的负外部性。

再次,大数据资源作为社会改造强大工具与其以牺牲个人权利为代价而实现独享数据特权之间产生权力悖论,这使个人信息处理面临正负外部性。一方面,大数据背景下信息主体以让渡个人权利为代价使大数据开发利用产生“公地悲剧”式的正外部性。个人信息处理行为的网络外部性效应与其取用信息数量、网络规模和技术兼容性密切相关。对数据控制者而言,其数据价值往往取决于数据的数量规模^[23]。随着大数据产业规模化收集个人信息,网络储量巨大的用户信息为其产业创新发展及其信息处理释放正外部性创造了条件。另一方面,大数据作为社会改造工具以牺牲个人权利为代价又有沦为数据控制者专享特权趋势,导致信息处理的数据集中垄断甚至滥用等负外部性。网络用户存在消费“粘性”,权力悖论造成信息控制者相互竞争态势下的赢者通吃及其信息资源的寡头独占,妨碍其他网络运营商对信息资源的数据共享及其规模化开发利用,不利众多信息主体在权利让渡下分享网络外部性的正效应,削弱了大数据创新活力及其对用户体验的改进,妨碍共享经济发展。

二、双重外部性下个人信息处理行为规制的两难困境

科斯在《社会成本问题》中以工厂甲排出烟尘给邻近居民乙带来有害影响为例指出,“人们一般将该问题视为甲给乙造成损害,所考虑的是:如何制止甲?但这是错误的。我们正在分析的问题具有相互性,即避免对乙的损害将会使甲遭受损害。必须决定的真正问题是,是允许甲损害乙,还是允许乙损害甲?关键在于避免较严重的损害”,据此提出“损害具有相互性本质”^⑩。在网络空间,数据控制者与其信息主体也会因基于大数据运用的个人信息处理行为而产生所谓“损害的相互性”问题,造成其双重外部性规制的两难困境,规制其负外部性可能制约其正外部性实现,规制其正外部性可能激励其负外部性溢出。

(一) 个人信息处理负外部性规制对其正外部性实现的制约

规制个人信息处理的负外部性往往通过赋予其信息主体以个人信息控制权,相应科以其个人信息处理者保护个人信息之义务,使大数据产业损害信息主体的隐私安全、人格尊严等负外部性得以由其生成者加以内在化地负担。在大数据背景下,个人信息处理行为负外部性规制会成为约束其正外部性实现的影响因素。

首先,适用告知同意规则规制个人信息处理的负外部性可能对其正外部性实现构成约束。适用告知同意规则意味着赋予信息主体以信息自决权而遏制其信息处理负外部性。不过个人信息自

^⑩Cookie 中包含可以识别浏览器的识别子,在访问网站的时候会记录用户的浏览信息,网站的合作公司也会收到该相关记录。

^⑪R. H. Coase, The Problem of Social Cost, 3 J. L&Econ. 1(1960), in The Firm, the Market and the Law 95-156(1988).

决权并非对任何可识别的个人信息收集、处理和利用均享决定与控制权的承认和保护,而是对自动化处理给人格或财产带来加害危险的事先防御或前置保护机制^[24]。随着大数据技术的发展,个人信息交换领域不再限于商品市场,信息智能处理机制也将成为其交换的新场所^[13]。大数据时代个人信息生态系统的去中心化重构使用户信息处理面临网络服务商、数据中间商及后续开发利用者等多元主体,其价值创造源泉取决其信息的后续多方流转与比对挖掘开发。共享经济模式下“信息最小化”原则的合理性以及大数据背景下基于告知同意规则限定个人信息权属的有效性往往令人质疑。基于“反公地悲剧”理论^②,赋予作为大数据客体的个人信息以分散的数据控制权将极为不利于大数据商业价值的发掘。将个人信息关在密室中永远见不到阳光,排斥其商业正当利用必然归于落后^[25]。大数据开发利用有赖产业创新激励,既要加强个人信息保护更要积极探讨如何促进其有效利用。大数据背景下个人信息处理的规制原则应是防止滥用,而非严格保护,故个人信息处理行为正当与否宜基于责任规则及事后判断方式,不应仅以同意作为个人信息处理的正当性基础^[7]。相对于事后适用内在化补偿机制(责任规则)的规制模式,严格遵循事前告知同意规则(财产规则)恐有碍个人信息处理的正外部性实现,不利于充分激发大数据产业创新活力与促进分享经济发展。

其次,适用去身份化规则规制个人信息处理的负外部性可能对其正外部性实现构成制约。如今大数据已成为最炙手可热的交易商品,也是众多公司、行业、非营利组织和政府部门渴望获得的资产,它在很大程度上是经由线上活动留下一种易被追踪并能透露出个体身份、交易、去向的数字印迹等信息构成。个人信息一旦被收集,则其信息主体便难以控制数据被谁使用抑或被如何使用^[26]。为避免未经授权的个人信息处理行为所致外部性风险,法律科以大数据开发利用者对其所处理个人信息进行去身份标识化等义务,要求对其进行脱敏处理后使其成为无法识别特定个人且不能复原的信息,据此将数据隐私属性与资产属性剥离以确保其数据流通的信息安全。不过,为提高匿名化后数据的可用性,需采取适当的数据匿名化算法,以降低实行匿名保护隐私安全时概化处理所带来的信息损失。但是,大数据开发的共享经济特性有赖于对网络空间信息资源的有效掌握与使用并对其信息内容的充分挖掘与整理。因而,若是采取过高标准而严格遵从去身份标识规则对个人信息进行脱敏处理与数据清洗以规制其负外部性,难免大为削弱其原始数据的潜在挖掘价值,妨碍大数据开发利用的商业目标实现甚至动摇其产业创新发展的经济基础。

(二) 个人信息处理正外部性规制对其负外部性溢出的激励

大数据背景下个人信息处理也有正外部性,基于“公地悲剧”理论通过法律拟制方式进行产权配置,赋予数据控制者对其数据资源拥有向社会公众“征税”的权利,据此规制个人信息处理的正外部性,有可能对其个人信息处理的负外部性溢出产生激励效应。

基于“公地悲剧”理论,如财产资源因权属不明而沦为人人皆可任意使用的公地,往往因个体行为的边际收益大于等于边际成本,却又不负担其行为外部性的社会成本,个人被无限制赋予对公地的过度使用权,进而导致资源枯竭甚至经济系统崩溃。就大数据背景下个人信息处理而言,有研究认为,除了用户初始数据上配置人格权与财产权外,还需在数据经营者层面配置数据经营权与数据资产权,并对其原生数据与衍生数据开发提供权益保障^[2]。当然,“卡—梅框架”下对法授权利

^②Michael A. Heller, Tragedy of the Anticommons: Property in the Transition from Marx to Markets, Harvard Law Review, Vol.111. 1998. pp. 621-688.

(entitlement)的保护有“财产规则、责任规则、禁易规则”三种路径^②。据此有研究主张,将数据法益配置给数据产生者,并适用财产规则是一条相对优选的路径^[11]。值得注意的是,个人信息处理中的数据红利与数据安全往往此消彼长。若是赋予数据控制者对大数据资源尤其是原生数据以绝对财产权,网络运营商出于机会主义倾向便有适用告知同意规则以“一揽子协议”概括授权模式籍由用户点击而过度收集甚至恣意圈存用户信息的内在激励,以致其规避遵从去身份规则甚至回避遵从“防止身份再识别”义务。可见,对数据控制者掌握海量用户信息的大数据集赋予财产权以规制其信息处理的正外部性,难免对个人信息处理的负外部性溢出产生某种潜在激励。

例如,美国 hiQ 诉 LinkedIn 爬虫案中,原告对抓取和复制数据进行开发而产生有别于领英公司产品却又方便用户的使用功能,领英却禁止原告抓取和复制其平台数据,原告遂向法院申请禁令,要求领英解除技术措施,加州北部地区法院认定领英的行为构成数据垄断,裁决领英解除限制并允许其抓取数据。实际上,为提升用户使用体验,个人信息处理往往会基于 API 协议允许网络运营商对入网数据彼此进行合理抓取或复制以实现信息共享。但在微博诉脉脉案中,我国法院判决脉脉对微博注册用户个人数据抓取构成不正当竞争,借助反不正当竞争法一般条款上之行为规范进路以保护用户数据权益。对此有研究认为数据财产化的权利进路可实现与个人信息权的折冲调和^[27],但值得注意的是,数据财产权化与个人信息权利化之间存在外部溢出效应的交互影响。网络外部性的数据集聚效应虽会激发个人信息处理的正外部性,不过若是不受限制地赋予大数据集等信息资源以财产权来规制其个人信息处理的正外部性,反而会对其负外部性溢出产生潜在的激励预期。大数据作为信息资源或技术工具均面临滥用风险。例如,提供独特产品与服务的数据运营商独占获得特定数据控制权,第三方开发者未经用户再授权而擅自抓取、使用网络平台上用户信息,数据控制者拒绝开放共享其收集的用户数据导致数据市场的单寡头垄断等。再如,处优势地位的数据运营商利用大数据技术定向追踪竞争对手行为乃至与其明示或默示达成价格垄断共谋,通过分析潜在用户的支付意愿价格而给特定用户以歧视性垄断定价。可见,基于数据财产化的权利进路规制大数据背景下个人信息处理的正外部性也会潜在地激发其负外部性溢出。

(三) 大数据背景下个人信息处理行为规制的价值取向分析

科斯认为,明晰产权有助市场交易,经由市场交易可基于外部性内部化实现社会产值最大化,但现实世界的交易成本过高而妨碍交易,为促进交易达成并实现效率最优,宜将其产权配置给使用价值最高者。但是,大数据背景下个人信息处理行为规制除了要实现其自由与效率价值,还需维护其安全与公平价值,面临着价值冲突取舍问题。

以在线行为广告(OBA)^②为例,其通过网络隐秘追踪和概括网页浏览等访问用户,利用 cookie 数据记录其访问的日志站点、点开的链接等,依据用户网络活动特点与偏好为其建档并悄然完成其数据采集与分析。在线行为广告商通过秘密追踪与监视为用户建档并在非透明化下对其进行信息

^①Guido Calabresi and A. Douglas Melamed. Property Rules, Liability Rules, and Inalienability: One View of the Cathedra. Harvard Law Review. Volume 85. April 1972 Number 6. pp. 1089-1128. 财产规则强调除非是自愿交易否则产权不得转移,责任规则强调如发生非自愿交易由损害方按第三方估价向被害方补偿损失。

^②美国数字广告联盟(Digital Advertising Alliance,简称DAA)对其定义是:“长期从某台电脑或设备上收集有关用户在各种非关联网站上的网页浏览行为的数据,目的是利用这类数据预测用户的喜好或兴趣,以便根据从这些网页浏览行为中推断出来的喜好或兴趣,向那台电脑或设备发送广告。”参见:[美]詹姆斯.R.卡利瓦斯《大数据商业应用风险规避与法律指南》(人民邮电出版社,2016年版68-69页)。

处理,且基于某种算法筛选机制向其追踪用户定向推送个性化服务,上述行为具有潜在危及用户人身(隐私)财产安全的负外部性。不过,若是立法“禁止追踪”以规制其负外部性,可能对在线行为广告商的个人信息处理行为构成自由限制,抑制其基于大数据分析以提升网络服务质量的正外部效应溢出,进而影响网络用户据此享受便捷服务的自由。可见,在线行为广告商的个人信息处理面临正负双重外部性,保障信息主体的信息安全可能与维护在线行为广告商的信息追踪与推送自由产生价值冲突,而且对在线行为广告商基于信息追踪与推送自由的营运效率及其产业发展产生所谓“损害之相互性”。不过,基于将产权配置给使用价值最高者的效率优化原理,赋予用户以个人信息控制权,有助其自主决定信息安全价值并基于市场交易需要参与在线行为广告商的大数据资源优化配置。欧盟《一般数据保护条例》(GDPR)赋予用户“数据可携权”和“被遗忘权”,其规制个人信息处理行为的价值取向便是用户的信息安全优于在线行为广告商的数据自由,此种规制的经济逻辑在于为避免后者对前者的更大损害,宜将数据可携权、被遗忘权等配置给用户。

再以基于算法决策的智能分析评估系统为例,网络运营者与用户在大数据分析计算中的数据结构安排与算法选择上存在“透明化悖论”所致信息不对称,算法“黑箱”(Black box)面临透明化困境。长期以来人们受“数学清洗”^{②③}思维方式影响,甚少质疑算法决策公平性,殊不知算法作为技术面临工具理性与价值理性的张力^{②④}。算法设计将交易或服务规则代码化后倘若信息披露不足,基于算法决策的选择自由却潜藏了算法监管缺失的危机,不仅难以趋向公平正义甚至有呈现算法歧视的极大可能。美国 North pointe 公司开发的犯罪风险评估算法 COMPAS 在使用中出现系统地歧视黑人现象,更多将白人错误地评估为低犯罪风险的群体,显示了其算法偏见^[28]。大数据的“身份悖论”与“权力悖论”使其数据占有使用一旦沦为数据控制者专享特权,网络运营商在工具理性驱使下便有基于算法设计对用户实行记分化追踪并依各类信息识别社会主体身份的内在激励。据此构筑的“信息茧房”又强力维系用户网络化生存空间秩序,用户受“透明化悖论”所限却对其构筑的“理性铁笼”^{②⑤}了无体悟,对算法差错甚至数据失当所致正义价值迷失鲜有觉察。随着智能决策愈益投射于现实社会空间参与其秩序再造,算法及其代码设计日益主宰着公共决策并对个体权益产生广泛影响。若欲“通过设计实现公平”(Fairness by Design)还需前瞻构建技术公平规则^[29]。欧盟《一般数据保护条例》赋予用户对智能决策的“可解释权”(The Right to Explanation)^{②⑥},其规制个人信息处理行为的价值取向便是算法设计的技术正义实现优于其智能决策的秩序再造,其规制的经济逻辑则是为避免后者对前者的更大损害,需赋予用户对智能算法的可解释权。

三、大数据背景下个人信息处理行为的双重外部性规制

大数据背景下个人信息处理的双重外部性规制面临所谓“损害的相互性”选择问题,解决其双

^{②③}自孔德以降的社会实证主义兴起以来,逐渐出现了一种利用数学将人类社会事务量化、客观化的思潮,Fred Benenson 将这种对数据的崇拜称之为数学清洗(Math washing),特别是随着计算机网络技术的迅猛发展,人们更倾向利用算法、模型、机器学习等数学方法重塑一个更加客观的现实世界。

^{②④}工具理性基于功利导向关注目的与结果,与基于某些重要信念(义务、尊严、美、规训等)作为行动指引的价值理性不同。参见:马克斯·韦伯《经济与社会(上卷)》(林荣远译,商务印书馆,1997年版57页)。

^{②⑤}马克斯·韦伯认为,随着工具理性对价值理性的替代,工具理性对人类生存状况造成了新的束缚,即所谓“理性的铁笼”(iron cage)。参见:马克斯·韦伯《新教伦理与资本主义兴起》(广西师范大学出版社,2010年版)。

^{②⑥}经合组织(OECD)2017年发布《算法与合谋》报告指出,完全的算法透明度并非仅公开或向管制部门披露其源代码,而要解释特定算法的结果如何得出,实践中强制性的算法透明度与可问责性可能面临很大挑战,尤其黑箱算法恐难实现更高透明度要求。目前各国对算法监管的执法实践与理论研究尚存分歧。

重外部性规制的两难困境需实现其规制理念、规制机理与规制机制的调整。

(一) 规制理念上实现从“压制型法”到兼及“回应型法”转换

在法社会学看来,“回应型法”作为法律进化的理想类型缓解了“压制型法”被动适应环境与“自治型法”为保持机构完整而自我隔离的紧张关系,它“把社会压力理解为认识的来源与自我校正的机会”,呈现“由一种对成本与收益的合理评估证明为正当”以及“对公共秩序危机采取一种以问题为中心的态度”^[30]。为解决大数据背景下个人信息处理行为双重外部性规制的两难困境,引入“回应型法”规制理念,有助于平衡大数据产业创新发展与个人信息合理利用、数据脱敏开发与信息安全保障的利益紧张关系并实现有关立法的规制缓和。

我国为遏制个人信息非法交易及电信网络诈骗漫延,对个人信息处理规制一度呈现先刑后民态势。刑法修正案(九)率先规定侵犯公民个人信息的罪名、罪状与罪责,司法解释明确其适用条件并确立“识别性+关联性”的个人信息标准,区分了“敏感、重要和一般”信息类别并据此量化设定差异化入罪门槛,但其刚性、静态界定“个人信息”^②,在对大数据产业创新背景下个人信息处理行为方式变动不居情势的适应上,显示了“压制型法”的被动性而欠缺“回应型法”的灵活性。我国《民法总则》除了规范个人信息保护与处理,其第127条还规定法律对数据的保护有规定的依其规定,这意味着未来相关立法需充分考虑大数据产业创新与个人信息安全的协同规制关系。对创新行业若采取“全有全无”(all-or-nothing)的规制策略,将其纳入既有规制框架或界定为非规制行业而任其“野蛮生长”^③,均宽严失当。从域外立法看,借鉴美国有效平衡个人利益与商业利益的隐私权保护模式功能,吸纳欧盟有效赋予个人信息自决权的基本人权保护模式价值,可为我国有效协调促进大数据产业创新发展与加强个人信息处理安全保障之间利益冲突提供政策立法参照。

近年来,为应对大数据下个人信息处理行为规制难题,学界基于美国《消费者隐私权利法案(草案)》及欧盟《一般数据保护条例》吸纳“风险与场景导向”的国际主流新理念,提出变信息处理前的静态合规遵循为信息使用中的动态风险控制,以此促进个人信息“合理使用”并重点规制其“不合理使用”,提升个人信息保护的有效性及其实质性,大幅减轻企业不必要的合规负担,协调隐私保护与数据价值开发^[9]。也有研究强调,个人信息保护的治理结构设计必须考虑其实施环节的“激励相容机制”实现,“个人信息从最内核的隐私信息到通常理解的敏感信息再到最外围的大数据意义上的非敏感个人信息,呈现一个放射状扇形结构。对于不同的个人信息,执行机制就要进行区分,采用不同强度的保护标准,界定信息控制者不同的责任”^[10]。其实,无论以“风险与场景导向”规制个人信息处理,还是以“激励相容机制”设计数据治理结构,其规制逻辑正是法经济学有关“损害之相互性本质”。为避免大数据产业创新与个人信息安全保障产生“相互损害”,宜将双方视为互有约束性的变量因素,并依其(敏感、重要或一般)个人信息处理不同场景的外部性大小,匹配适用用户(积极或消极)同意标准并据此确立规制强度,使规制的制度供给与制度需求相均衡并保持两者间的动态回

②参见“两高”《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》(2017年6月1日施行)有关规定将“公民个人信息”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”。

③See Gillian Hadfield, Legal Barriers to Innovation: The Growing Economic Cost of Professional Control over Corporate Legal Markets, 60 Stan. L. Rev. 1689, 1695 (2007).

应,增强用户与数据控制者间的私权自治,实现个人信息处理的“帕累托效率”^②。

(二) 规制机制上实行“外部性内在化”与“外部性外部化”并举

法经济学关于“外部性的内在化”^[31]规制模式认为,当某种行为带来社会损害等负外部性时予以适当惩戒或由其生成者向受损者进行补偿,当某种行为带来社会收益等正外部性时予以适当补贴或由其受益者向生成者进行付费。

一方面,大数据背景下个人信息处理的负外部性需要加以内在化规制。大数据形态下的原生信息不具有“争用性”而有其特定条件下的“限用性”。大数据中未去身份处理的个人信息兼具人身与财产属性,因其人身属性而有一定的“限用性”。大数据背景下个人信息处理存在危及信息主体的信息安全和挑战信息控制者的限用性能力等负外部效应。以外外部性内在化的自愿协商规制为例,纵然“卡—梅框架”揭示“财产规则、责任规则、不可让渡规则”具有内在对称性,当市场的交易费用低于法院的交易费用时,财产规则优于责任规则;当市场的交易费用相对较高时,则与此相反^[32]。但财产规则与责任规则的优选适用存在界分歧义^③,所谓价高者得的权利配置忽视了“管理财产权制度的成本”,产权界定要考虑“管理(主要是信息)成本”^[33]。大数据背景下的个人信息同样面临权利界定及其隐私利益协商定价的交易成本难题。在信息处理问题上,适用财产规则有可能面临制度定价成本更高的复杂局面。即便适用责任规则的市场交易成本更低,但正确适用责任规则有赖第三方定价者(例如法院)拥有更强的信息搜集与判定能力。因而基于制度供给与制度需求相均衡实现效率最优的经济学原理,外部性规制作为制度供给应视其外部性的具体情形采取相应的规制模式与强度。规制大数据背景下个人信息处理行为需完备其信息分类并辨明其外部性的具体样态,针对原生数据与衍生数据、个人核心数据与非核心数据等各类信息特性,依信息处理行为的外部性差异采取不同规制措施。对于极端敏感的核心信息若是收集使用不当可能造成难以挽回的损失,需经由“财产规则”甚至“不可转让规则”予以特别保护,对于非敏感的普通信息可以适当容许适用“责任规则”来解决个人信息处理行为的规制问题。通过构建数据使用者责任机制并籍以“卡尔多—希克斯”效率标准,基于外部性内在化规制对数据处理行为实施可能面临利益受损的信息主体予以经济补偿,从而实现其数据处理行为的效率增长。

另一方面,蕴藏海量信息的大数据集作为信息资源呈俱乐部物品(共享品)属性,有赖基于“外部性内在化”解决其开发利用中权属不明所致的市场失灵问题,基于“外部性外部化”解决其数据价值挖掘中开放共享不足所致的资源配置低效与竞争妨碍问题,籍以促进大数据产业创新并实现其个人信息处理的正外部性。由于数据产品开发需要采集海量的个人信息,经脱敏处理后作为“喂食”并优化其算法设计的信息资源,但由海量的个人信息集成的大数据资源有别于公共物品之处在于其固定成本很高而边际成本很低甚至趋于零。大数据的网络外部性使众多网络用户集聚在需求侧对信息品进行争相使用并给公众带来相当可观的规模化的网络外部正效应,满足了共享经济需要。网络经济或数字经济实行“免费+增值服务”的运营模式便源于其规模经济上和边际收益上的递增趋势,网络平台使用者越多其网络外部性正效应越大,具有满足“外部性外部化”(共享经济)的“公地喜剧”色彩,从而实现其规模收益递增(边际成本递减)以充分激发其分享经济功能。大数据

^②帕累托效率指所谓“除非损人便不能利己”的资源配置均衡状态,而“卡—希”效率要求由损人利己者向受损者提供合理补偿。参见: [美]波斯纳《法律的经济分析》(中国大百科全书出版社,1997年版40页)。

^③Carol Rose, The Shadow of the Cathedral, 106 Yale Law Journal 2175(1997).

不具“争用性”但具“限用性”属性使大数据产业面临数据集中而有导致数据垄断甚至数据滥用的趋势。随着智能算法大力提升市场透明度,即便竞争者间并无明确协议,默示合谋(tacit collusion)仍有可能^[34]。这增添了反垄断执法在评估与算法相关的协议、协同行为等反竞争风险上的挑战^[35]。为避免大数据开发利用与个人信息处理在双重外部性规制上的“相互损害”,除借助“外部性内在化”规制其信息处理的数据不当侵占,还要借助“外部性外部化”规制其信息处理的数据垄断集中^⑩。若是数据控制者拥有数据占市场支配地位,无正当理由拒绝数据分享而有排除、限制竞争行为,结合本国大数据产业发展应适用反垄断法对此予以规制^⑪。

(三) 规制措施上施行数据资源权利配置与数字技术权力干预协同

大数据背景下个人信息处理离不开数据选择及算法设计。算法设计以数据结构为基础,针对实际问题待处理数据选择恰当的存储结构,基于选定的存储结构而优化算法设计,机器学习中的算法优化有赖可靠的数据资源,否则会导致算法偏差。因而,规制其信息处理行为既要基于信息资源取用的数据权利配置以利信息主体的自主规制,也要基于算法优化与代码设计的数字“权力”干预以利数据控制者的协同规制。

首先,大数据背景下的个人信息作为数据资源有待恰当的权利配置。一方面,赋予信息主体对其个人信息以知情与同意权、选择与变更权、删除与撤回权等,有助信息主体对数据控制者取用个人信息及其处理行为进行自主规制。欧美政府近年来主导的“消费者授权政策”强化用户权限,英国政府推行的 Midata Project 与美国政府推行的 Smart Disclosure 旨在实现个人数据由机构掌控转向用户自行掌控^{[16]192-209}。包括由网络平台开发“数据盒子”(Data Box)为信息主体自我管理、储存、交易、转移个人信息提供技术支撑^⑫,完善反爬虫机制,为用户提供一站式撤回与关闭授权。当然,若赋予信息主体以算法解释权,则会扭转“透明化悖论”所致数据控制者对信息主体的信息强势地位,以及“身份悖论”所致数据控制者对信息主体的数据歧视威胁。另一方面,赋予数据控制者基于大数据原生信息开发的衍生数据产品以产权配置,有助数据控制者协同规制第三方的个人信息处理行为。对数据控制者而言,相对于遵从告知同意规则取用人个信息,其适用去身份规则的成本付出更高且面临反向工程被再识别风险,若对处于粗放状态的原生数据赋予绝对权的产权配置,反而助长其基于告知同意规则的概括授权随意取用个人信息。若是数据控制者通过云计算、大数据分析将原本单一且价值有限的碎片化原生数据进行提炼整合生成有使用价值的产品,对此赋予相应产权则有助激励大数据产业创新,也有助促使数据控制者积极规制第三方因擅自使用其数据产品而不当进行其信息处理行为。因而,立法赋予何种类型与强度的个人信息权与数据资源产权往往彰显了保障个人信息安全与促进大数据产业创新的不同价值取向。

其次,大数据背景下个人信息处理作为数字技术运用有赖权力干预。去身份是个人信息有序

⑩前者参阅新浪微博诉脉脉抓取使用微博用户信息案(京73民终[2016]588号);后者参阅美国 HiQ Labs 诉 LinkedIn 拒绝数据抓取纠纷案,HiQ Labs, Inc. v. LinkedIn Corporation, No.3:17-cv-03301(N.D. Cal.2017)。

⑫各国对数据分享的反垄断执法尚存分歧,数据作为信息资源既可作为企业的竞争优势也会构成相关市场的进入壁垒,关键是数据是否构成反垄断法上的必要设施(Essential Facility)并合理界定适用领域。参见:孙晋、钟原《大数据时代下数据构成必要设施的反垄断法分析》(《电子知识产权》,2018年第5期)。

⑬如此,网络平台商便有义务利用“数据盒子”整合个人信息并完备其数据库,为信息主体与信息买家建立商谈平台并基于平台对话使信息主体获得满意的对价。See Hamed Haddadi, Richard Mortier, Derek McAuley, Jon Crowcroft, “Human-data interaction”, Cambridge Computer Laboratory, No.837, (Jun, 2015)。

流通与再利用之前提,分离数据中隐私与资产属性可降低数据流通中的隐私风险^[8]。不过集中于人格隐私保护的大数据研究面临局限^[36]。数据脱敏处理若过于彻底去除大数据所涉个人身份信息的直接标识符或改变其准标识符的判断,虽有助于保障个人信息安全,但却削弱了其潜在挖掘价值。数据控制者为减少数据匿名化后的信息损失并提高其可用性,往往有基于代码设计降低去身份标识标准甚至变相追踪、识别用户身份的机会主义倾向。因法律无法介入互联网信息传输的技术过程直接规制虚拟空间的生成和运作,代码构筑了网络空间并具有“隐形法”的功能^④。代码设计者基于理性人机会主义倾向面临效率性的违法的经济激励^⑤。因而规制个人信息处理既要运用市场手段确保个人信息权自主行使,又要科以数据控制者在算法决策中保障信息安全义务并将其转化为程序代码设计要求,在信息处理合规边界内为促进大数据产业创新寻求制度适用选择空间。设计出验证、证实、知情同意、透明性、可责性、救济、责任等机制以削弱或避免机器歧视、确保公平正义^[29]。为此,鼓励信息安全技术开发,基于元数据标签绑定技术提升用户控制权行使及其信息处理透明度,运用加密算法实现信息密文传输以防被窃听或篡改,引用安全认证、数字水印、电子签名、区块链确保原始信息真实。基于信息运行数据流建立个人信息泄露溯源机制^[37]。同时,在制度设计上基于用户与数据控制者双重授权机制制止数据滥用,辅以数据登记及溯源监管、网络运营备案审查、代码设计合法评估与算法决策审计监督等数字技术运用的权力干预措施。

四、结语

大数据产业面临个人信息的提供者、收集者、分析者、中间商、使用者、第三方开发者及监督者等多元主体基于人格与财产、公权与私权之博弈,这使大数据产业创新与个人信息处理规制面临内在张力。我国“十三五”规划提出实施国家大数据战略,工业和信息化部为落实《促进大数据发展行动纲要》发布的《大数据产业发展规划》指出,大数据产业发展面临“数据所有权、隐私权等相关法律法规和信息安全、开放共享等标准规范不健全,尚未建立起兼顾安全与发展的数据开放、管理和信息安全保障体系”等支撑体系不完善的问题,并提出其政策法制完善措施^⑥。然而,数据的法律属性与权利归属在理论上尚未廓清,其司法实践中尚在探索^⑦。大数据产业往往以欧盟与中美对比观察认为,过严的个人信息保护会限制其产业发展甚至削弱其竞争力。值得注意的是,数据共享开发利用以相关主体间的信任机制为基础,有效规制个人信息处理行为能强化其信任机制并为大数据产业创新发展增添信息资源流通活力。全面揭示大数据背景下个人信息处理的双重外部性及其规制的交互影响,以系统性的整体视角把握大数据产业发展与个人信息保护的共生关系,基于“损害之相互性”理论并借鉴“公地悲剧”理论探寻其双重外部性规制的经济逻辑,有助于深入探明其政策法

^④美国学者莱斯格就互联网规制问题指出,法律、社会规范、市场、代码等任何单一规制手段都有局限性,应充分发挥代码规制的应有作用。参见:[美]劳伦斯·莱斯格《代码2.0——网络空间中的法律》(李旭、沈伟伟译,清华大学出版社,2009年第4版98页)。

^⑤例如2018年4月“今日头条”因智能推送内容问题受到监管部门责令其永久关停“内涵段子”客户端软件及公众号的处罚,随后发布声明称要全面纠正算法与机器审核的缺陷,将正确的价值观融入技术和产品。

^⑥除现行立法及尚待制订个人信息保护法外,还包括《大数据服务安全能力要求》《个人信息安全规范》《大数据安全管理指南》(征求意见稿)等国家推荐标准及《大数据行业自律公约》等软法规制措施。

^⑦2018年8月16日杭州互联网法院在淘宝(中国)诉安徽美景不正当竞争案中认定,如无法定或约定,用户对提供网络运营者的单个用户信息尚无独立的财产权或财产性权益;网络运营者对由用户信息数字化记录转换而来的原始网络数据依其与用户约定享有使用权;对其深度开发与系统整合的大数据产品“生意参谋”,因其内容是源于却又独立于用户信息、原始网络数据的衍生数据,网络运营者应享有独立的财产性权益。

制完善之路。

参考文献:

- [1] 劳伦斯·莱斯格.代码——塑造网络空间的法律[M].李旭,译.北京:中信出版社,2004:197.
- [2] 龙卫球.数据新型财产权构建及其体系研究[J].政法论坛,2017,35(4):63-77.
- [3] 程啸.论大数据时代的个人数据权利[J].中国社会科学,2018(3):102-122,207-208.
- [4] 维克托·迈尔·舍恩伯格.大数据时代[M].盛杨燕,周涛,译.杭州:浙江人民出版社,2013:220-221.
- [5] KUNER C, CATE F H, MILLARD C, et al. Risk management in data protection[J]. International Data Privacy Law, 2015, 5(2):95-98.
- [6] TENE O, POLONETSKY J. Big data for all; Privacy and user control in the age of analytics[M]. Social Science Electronic Publishing, 2013.
- [7] 任龙龙.论同意不是个人信息处理的正当性基础[J].政治与法律,2016(1):126-134.
- [8] 金耀.个人信息去身份的法理基础与规范重塑[J].法学评论,2017,35(3):120-130.
- [9] 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,2016,38(5):92-115.
- [10] 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[J].法学研究,2018,40(2):3-23.
- [11] 肖冬梅,文禹衡.法经济学视野下数据保护的规则适用与选择[J].法律科学(西北政法大学学报),2016,34(6):119-127.
- [12] 张里安,韩旭至.大数据时代下个人信息权的私法属性[J].法学论坛,2016,31(3):119-129.
- [13] 吴伟光.大数据技术下个人数据信息私权保护论批判[J].政治与法律,2016(7):116-132.
- [14] 高富平.个人信息保护:从个人控制到社会控制[J].法学研究,2018,40(3):84-101.
- [15] 谢远扬.信息论视角下个人信息价值——兼对隐私权保护模式的检讨[J].清华法学,2015,9(3):94-110.
- [16] 城田真琴.数据中间商[M].邓一多,译.北京:北京联合出版公司,2016.
- [17] 詹姆斯.R.卡利瓦斯,迈克尔.R.奥弗利.大数据商业应用风险规避与法律指南[M].陈婷,译.北京:人民邮电出版社,2016:8.
- [18] 让·梯若尔.创新、竞争与平台经济——诺贝尔经济学奖得主论文集[M].寇宗来,张艳华,译.北京:法律出版社,2017:1-2.
- [19] ROSE C. The comedy of the commons: Custom, commerce, and inherently public property[J]. The University of Chicago Law Review, 1986, 53(3):711-781.
- [20] 喻炜,王凤生.我国大数据产业政策研究——基于网络外部性与异质信息产品视角[J].当代经济科学,2016,38(3):72-79.
- [21] 于立.“公地悲剧理论”与互联网竞争政策[EB/OL].[2018-08-17].http://www.sohu.com/a/223927338_455313.
- [22] 维克托·迈尔·舍恩伯格,肯尼思·库克耶.大数据时代[M].盛杨燕,周涛,译.杭州:浙江人民出版社,2013:67-71.
- [23] SHELANSKI H A. Information, innovation, and competition policy for the internet[J]. University of Pennsylvania Law Review, 2013, 161(6):1663-1705.
- [24] 杨芳.个人信息自决权理论及其检讨——兼论个人信息保护法之保护客体[J].比较法研究,2015(6):22-33.
- [25] 郭瑜.个人数据保护法研究[M].北京:北京大学出版社,2012:111.
- [26] 特伦斯·克雷格,玛丽.E.卢德洛芙.大数据与隐私[M].赵亮,武青,译.沈阳:东北大学出版社,2016.
- [27] 许可.数据保护的三重进路——评新浪微博诉脉脉不正当竞争案[J].上海大学学报(社会科学版),2017,34(6):15-27.
- [28] 曹建峰.人工智能:机器歧视及应对之策[J].信息安全与通信保密,2016,14(12):15-19.
- [29] CITRON D K. Technological due process[J]. Washington University Law Review, 2008, 85:1249-1312.
- [30] P.诺内特,P.塞尔兹尼克.转变中的法律与社会:迈向回应型法[M].季卫东,张志铭,译.北京:中国政法大学出版社,2004.
- [31] 杰弗里.L.哈里森.法与经济学[M].2版.北京:法律出版社,2004:43-44.
- [32] CALABRESI G, MELAMED A D. Property rules, liability rules, and inalienability: One view of the cathedral[J]. Harvard Law Review, 1972, 85(6):1089-1128.

- [33] 理查德·A·波斯纳. 法律的经济分析[M]. 蒋兆康, 译. 北京: 中国大百科全书出版社, 1997: 64-65.
- [34] EZRACHI A, STUCKE M E. Virtual competition: The promise and perils of the algorithm-driven economy [M]. Harvard University Press, 2016: 17.
- [35] 韩伟. 算法合谋反垄断初探: OECD《算法与合谋》报告介评(下)[J]. 竞争政策研究, 2017(6): 68-77.
- [36] HELVESTION M N. Consumer protection in the age of big data [J]. Washington University Law Review, 2016 (4): 859-917.
- [37] 王忠. 大数据时代个人数据隐私规制[M]. 北京: 社会科学文献出版社, 2014: 28.

Legal regulation of personal information processing action in the background of big data:

From the perspective of dual externalities of personal information processing

HU Chaoyang

(School of Law, Southeast University, Nanjing 210096, P. R. China)

Abstract: Personal information processing not only causes negative externalities such as data security risks, but also brings positive externalities such as the realization of sharing economy in the background of big data. The causes of double externalities can be revealed by the phenomenon of “Three Paradoxes of Big Data”. Based on the theory of “internalization of externalities”, both the negative externalities and the positive externalities from personal information processing will be regulated if the information subject is empowered with the rights to personal information, and the data controller is empowered with the rights to big data property. However, in the background of network big data, dual externalities of personal information processing are interacted with each other and faced with some dilemmas. The theory of “mutuality of damage” in law and economics provides an economic logical explanation for regulating personal information processing behavior based on the “risk-based approach”. The development of big data industry depends on the “externalization of externalities” of personal information processing to realize its sharing economy. The theory of “comedy of the commons” in law and economics provides the economic logic proof for regulating personal information processing behavior based on the “externalization of externalities” in order to meet the needs of big data industry development. For the regulation of personal information processing in the background of big data, we should enforce the transformation from the “repressive law” to the “responsive law” on ideas, the coexistence of both the “internalization of externalities” and the “externalization of externalities” on mechanisms, the coordination of both the data resources rights allocation and the digital technology power intervention on measures, so that the organic balance between big data industry innovation and personal information security can be achieved.

Key words: big data; personal information processing; dual externalities; paradoxes of big data; legal regulation

(责任编辑 胡志平)