



大数据背景下的算法侵权风险问题分析

李或祺

中南财经政法大学司法鉴定技术应用与社会治理学科创新基地，武汉

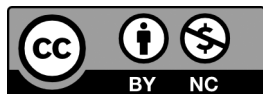
摘 要 | 大数据时代下通过算法可对社会资源实现再分配，极大地提升了社会效率。然而，算法存在的技术偏见、自动关联性与自动化决策等弊端在不同程度对数据主体的法益造成侵害。针对于侵犯数据主体平等权、隐私权以及自由意志被压缩的三种算法侵权类型，本文拟从建立个人数据保护官制度、配置相应对抗的权利以及优化侵权赔偿救济手段三方面提出建议以构建更完善的算法侵权治理体系，保障信息时代下数据主体的权利不被消解。

关键词 | 算法；大数据；技术侵权；法律规制

Copyright © 2021 by author (s) and SciScan Publishing Limited

This article is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](https://creativecommons.org/licenses/by-nc/4.0/).

<https://creativecommons.org/licenses/by-nc/4.0/>



一、问题的提出

近年来，人类社会由传统的工业经济时代迈向数字经济时代，随着技术革新与机器学习理论方兴未艾的深入发展，算法在商业、教育、医疗、行政管理等等领域接管着越来越多被让渡的决策权^[1]。数字经济新产业的蓬勃发展和算法技术的不断更新成熟，给人工智能时代及未来的人类社会生活的发展与进步带来无限可能。从新闻推送的权重配比到手机导航到路线自动优化选择，从犯罪行为相关的治安警务预测到辅助司法工作者定罪量刑，算法基

于海量的数据基础与统计模型对社会资源实现了运算配置，影响、干预、改变了数据主体的行为与判断，辅助甚至取代了传统公权力、商业机关、社会公共部门的决策，即算法决策^[2]。

与之相关为人所诟病的，是诸如“大数据杀熟”、个人信息被泄露等算法衍生问题，广泛的运用同时也使得算法对政府、社会组织及个人等各方群体的影响力日益增强，从而发展为一股新兴的技术权力，即算法权力（algorithmic power）^[3]。算法权力直接催生出监视资本主义（surveillance

[1] 张凌寒. 算法权力的兴起、异化及法律规制[J]. 法商研究, 2019(4): 63-75.

[2] 算法运用于公权力辅助司法决策，如 2017 年 6 月，最高人民检察院通过了《检察机关大数据行动指南（2017—2020 年）》等明确了最高人民检察院提出了“智慧法院”与“智慧检务”建设的行动规划，参见《最高检印发〈检察大数据行动指南（2017—2020 年）〉》，公安部与司法部也有类似大数据与信息化建设的指南。

[3] 姜野. 算法的规训与规训的算法：人工智能时代算法的法律规制[J]. 河北法学, 2018(12): 142-153.

capitalism)^[1]的兴起,也容易在实际运行过程中造成不公平的结果系统性可重复出现,这样的算法偏见(algorithmic bias)堆砌着人们“信息茧房(information cocoons)”^[2]的壁垒,也不可避免地损害了公众群体或特定个体等等的法益。

令人遗憾的是,现行个人信息数据保护模式无法有效规范算法过程。首先,互联网等平台上算法利用所掌握的受众个人信息,针对其兴趣偏好领域进行信息推送,剥夺了大众公平享受信息、社会资源的权利。诚然,基于效益与正义、完全公平的机会分配方式并不存在,但致力于抢占市场份额取得优势的科技寡头们甚至排斥了个体选择更加公平的基本努力^[3]。算法投其所好地抓取受众“想要知道的”资讯内容以取悦并固定用户,势必会导致用户接触到的信息不断窄化,加剧了的信息茧房会进一步引发回声室效应和同质化负效应^[4]。不难想象,公共空间中当获取信息的自由被严重挤压时,多远包容的健康讨论环境被消解,取而代之的可能是不同阶级群体的对立甚至加剧社会的割裂程度。其次,算法自动关联等特性入侵数据主体隐私权利。商业巨头利用技术优势轻易探知用户的操作习惯偏好等并进行精准的画像后形成“监视”^[5]。生活中最常见的商品推送、大数据杀熟无不体现了算法及其背后主体对于个人用户隐私的掌握程度^[6],算法自动决策期间形成算法不透明以及算法黑箱,并通过深度学习进一步演化为“算法权威”挤压数据主体意思自治的空间,对数据主体的行为直接产生控制和影响。

如前所述,传统法律框架下对数据主体的传统保护模式难以适应现实需要。特别是在算法驱动时代下的DT(data technology)社会中,因算法拥有着天然的歧视性、自动关联性以及自动决策性等弊端,上述保护方式无论单独还是结合使用,都难消除算法在数据信息在筛选、分析及加工环节对数据主体带来的权利侵害,造成数据主体无法切身体会对数据信息价值挖掘的意义所在,进而致使其难以积极主动地“分享”数据信息,甚至排斥参与数字经济。因此,法律如何界定算法侵权类型、保护算法过程中的数据主体权利,就成为数字经济社会能否顺利推进和发展的前提,从而预留下继续研究的空间。

二、算法侵权现状及类型分析

(一) 算法的偏见侵犯数据主体平等权

从法理上看,平等在法律层面所追求的价值无外乎相同主体需被平等对待。在当今数字经济时代背景下,法律平等要求社会中每一位主体在人格、权利以及机会等方面都受到相同的对待地位^[7]。事实上,我国现阶段存在的算法导致的侵犯数据主体平等问题,主要原因是由于算法技术运用的标准缺失、运行范畴无法厘清等原因所致。因为算法在数字经济时代不仅决定了数据主体数据资源分配的体现,随时数据作为生产资料重要程度的加深,同时也决定了权利在法律层面的实质性分配,其特征也涉及相关立法面向与要点。现阶段,以算法为

[1] 监视资本主义,最早由肖沙娜·朱伯夫(Shoshana Zuboff)提出,近期网飞公司纪录片《监视资本主义:智能陷阱》重新引发公众对算法技术、公共性及合法性等问题的广泛关注与讨论。

[2] “信息茧房”这一概念最早由凯斯·桑斯坦(Cass R. Sunstein)提出,指网络化虽然能带来更多的资讯选择自由,但公众只会注意到自己选择的东西和是自己愉悦的信息领域,具体参见Cass R. Sunstein. Neither Hayek Nor Habermas [J]. Public Choice, 2008 (134): 87-95.

[3] 刘友华. 算法偏见及其规制路径研究[J]. 法学杂志, 2019 (6): 55-66.

[4] 周文扬, 张天荣. 生成、影响与反思: 聚合类新闻客户端的信息茧房效应研究——以“今日头条”为例[J]. 传媒, 2018 (20): 94-96.

[5] 胡凌. 网络法的政治经济起[M]. 上海: 上海财经大学出版社, 2016: 177.

[6] 算法社会的核心特点是(沿袭于信息社会的)权利和信息失衡——人工智能对我们知晓很多,而我们对其所知甚少,爱因斯坦提出,“我们不能用制造问题的方法去解决问题”。

[7] [美] E. 博登海默. 法理学: 法律哲学与法律方法[M]. 邓正来, 译. 北京: 中国政法大学出版社, 2017: 310-315.

代表的大数据技术、人工智能技术等科技因素发展为“数据”一词添加了较为复杂的内涵,这一复杂影响了数据主体平等权利在立法与法律适用的统一性,并与数据、算法技术因素的无边界性形成了冲突。因此,本就存在天然型的算法歧视所蕴含的偏见对数据主体的平等权造成了巨大的冲击。

具体而言,法的一般性要求法律平等适用于调整对象之上,反对以个别化的方式进行规则建构。从法理上看,算法歧视存在的根本原因在于其产生的“个别规则”突破了法的一般性,尤其是算法在电商平台中的运作过程将这一特点体现得淋漓尽致。此外,先行存在的算法偏见打破了人们常规观念——“算法是中立性且客观的”,表现为算法设计者对算法实现的影响。在算法设计之初所构建的目的和所实现的功能框架便会对算法的客观性造成很大的影响。即使算法设立的目的和所要实现的功能是就不便于携带歧视性的,也难以避免造成侵犯数据主体平等权利的后果。以决定商品售卖的价格为例,平台的算法在利益驱使下针对不同消费者对相同的商品的支付意愿、消费能力与购买习惯等的差异提出不同定价,在这个过程中就形成了价格歧视。同样的形式还有亚马逊给客户推荐的商品更多的和与自己有相关合作的商品,而那些价格更低的商品则没有被推荐,客户没有办法获得更加客观的商品推荐^[1],此外不仅对于个人消费者的平等权利受到侵害,算法偏见还影响到了其他数据主体之间的公平竞争^[2],机器在学习“清洗”数据时,设计何种假设都难以做到完美的“零偏差”^[3]。

(二) 算法的关联性侵蚀数据主体隐私权

早在二十世纪九十年代,以王利明教授为代表的部分学者将隐私权范围划分为个人生活安宁与私人生活信息两部分^[4]。2020年人大通过的《中华人民共和国民法典》中以立法的形式将隐私的定义明确固定为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。而作为抽象的法律概念,隐私权的内涵囿于权利归属的交错复杂以及隐私范围的外延往往具有不确定性^[5]。

在大数据背景下,信息的多样性带来及处理信息源算法的关联性使得数据主体隐私泄露风险大大增加。由于人们的数据的广泛分布,使得多个数据集都有可能存在某个个体或者与他相关联的个体

的数据,这使得数据集之间存在着一定的关联性。在这种情况下,融合之后的数据集的隐私风险相比于单个数据集的隐私风险将增加。算法的高关联性容易形成对于数据主体的“精准画像”,为包括爬取个人数据、寻找数据相关性以及对数据主体特定方面作出相关预测或评估等在内的程序运行打好基础。电子商务平台上的经营者收集存储了一定量的消费者浏览记录、消费记录、存款状况、地理移动位置及信用指数等个人信息,并基于此对了解分析其消费水平、购买能力以及喜好习惯等从而进行差别定价。谷歌公司法律顾问尼克尔提出,当一个对数据整合使用一无所知的用户登录相关网页时,网页中所有的广告背后链接隐藏着相关设计公司的代码以收集用户的个人信息,而远非只是登陆点原始网站拥有搜集信息数据的能力。算法通过将用户数据相关信息关联起来进而发展成关系链乃至关系网络,在一定范围内运用网络爬虫追踪等技术对数据库中的相关信息再处理形成数据画像,以便于更“智能地”反作用于用户本身。

算法自动关联的特性极大程度地扩大了数据挖掘的范围,侵害了数据主体个人信息保密、支配、知情以及维护的隐私权利。从数据挖掘到信用评级、排名,人的主体性被资本化与商品化裹挟,算法平台借此构建出的规范系统与评价体系给每个

[1] 刘友华. 算法偏见及其规制路径研究[J]. 法学杂志, 2019(6): 55-66.

[2] 不同市场主体间由于算法爬去引发的不正当竞争,以新浪微博诉脉脉案、360公司与百度搜索引擎之战为代表,现行的《反不正当竞争法》中设置的“互联网”专条很难实质性解决“算法之战”所引发的具体竞争纠纷案件。

[3] Moses, Lyria, Bennett, et al. Using Big Data for Legal and Law Enforcement Decisions: Testing the New Tools[J]. University of New South Wales Law Journal, 2014, 37(2): 643-678.

[4] 王利明. 人格权法新论[M]. 长春: 吉林人民出版社, 1994: 487.

[5] 学界主流认为,隐私权是个人对其私领域的自主权,即个体自主决定其私生活的形成对个人资料的自主控制,而不受他人非法侵扰、知悉、搜集、利用、公开等等的一种人格权,它蕴涵了自由、自治、尊严以及私人领域不受侵犯的理念。

数据主体“个性化定制”起独一无二的信息茧房。从曾经的斯诺登事件到“脸书-剑桥分析公司”的丑闻,从国内的“P2P网络贷款”、支付宝年度账单事件,到“徐玉玉电信诈骗案”,看似全民免费的数据使用时代换来的数据主体被规训乃至奴役。2020年受新冠疫情的影响,线上教育、网络支付、视频直播等平台蓬勃发展,其中算法自动关联侵蚀数据主体的隐私信息现象更为频繁。在大量信息的表象之下,通过数字渠道源源不断获取的信息实际上被复制、被限制和被控制^[1],无处不在的信息采集与商品推送反映了网络监视的范围与深度,在根本意义上消解了隐私的意义,威胁着数据主体的数据隐私与数据安全,增加了个人信息、隐私数据被不当利用、非法倒卖的风险。

(三) 算法自动化决策权力压缩数据主体意思自治空间

数据主体的意思自治,指主体根据自由、独立的意志在没有非法外力干预的情况下根据自己主观判断进行民事活动。作为私法的核心价值,意思自治旨在为个人提供一种受法律保护的自由,从而使个人获得自主决定的可能性^[2]。“自动化决策”作为与自然人决策相对立的概念,常被认为是利用计算机网络框架与算法程序等替代自然人处理关键数据,并生成对数据主体具有法律效力的决策行为^[3]。也有学者认为算法的权力是信息巨头基于对海量数据的占有与支配,资本权力控制算法设计和研发的过程。

随着数据时代的发展与人工智能的深入学习,算法远超越其设计初衷,被广泛运用于各个领域。从个体行为与决策到商业机关、金融机构的相关借贷、定价、雇佣资格审查等等,算法接替人类手中的权力参与越来越多的公共事务的处理。借鉴了商业领域的模式,算法也逐步成为行政、司法领域中侦查、审批、价值排序、福利资格认定等等公权力决策之中。我国司法系统试推行的智能裁判系统可以高效率地提出裁判、量刑建议,此外犯罪预警系统使传统的事后打击转变为事前预防,其分析结果常直接影响甚至警力的分配调度。算法从不同层面与维度嵌入公共事务的运行与处理,借助架构优势搭建其监管体系,甚至在某些领域成为独立的决策者而取代公权力^[4]。

然而,在当今“微粒社会”之中,算法驱动下人们留下的电子痕迹正在被数据化、碎片化的整合,服务于各个领域的评分、排序与决策之中,算法决策颠覆性地提升了决策效率的同时,却架空了公众参与的传统程序,巨头齐聚,资本介入,压缩了数据主体意思自治的空间。诚如有学者所言,我们的社会运行也许在算法指挥下更加高效,但却否定了我们作为人的重要部分——自由选择的能力与行为责任自负的基础。正如石油公司开采石油一般,社交媒体的算法开采着用户的注意力与精力,并对开采成果进行定向加工——看似浅层的广告投放,本质上是对每个数据主体行为的影响与干预:政治广告的投放影响舆论乃至投票结果;而商业广告则通过影响每个个体的消费行为改变市场。算法提升用户体验的同时看似成为了集体选择的工具却放弃了人之所以为人的自由意志^[5]。一个以代码为符号的社会中权力会越来越集中于算法^[6],甚至有些情况下算法逐渐脱离人的控制与预测,挑战了经济活动和法律关系中“人”的主体地位。

例如,外卖配送员的送餐路线经过算法的计算决策被平台定义为二为地图上的“最优路线”,即使在三维现实世界中这条路线面临着逆行、违规等违反交规的风险,骑手们也往往选择遵循平台的指导路线进行送餐,甚至以他们的生命安全为成本去追求非常苛刻的量化指标的现象。配送平台处于核

[1] [美] 皮埃罗·斯加鲁菲. 智能的本质: 人工智能与机器人领域的64个大问题[M]. 任莉, 张建宇, 译. 北京: 人民邮电出版社, 2017: 170-171.

[2] Dieter. Allgemeiner Teil des BGB [M]. C. F. Müller, 2010: 472.

[3] 唐林垚. “脱离算法自动化决策权”的虚幻承诺[J]. 东方法学, 2020(6): 18-33.

[4] 李文静, 栾群. 人工智能时代算法的法律法规: 现实、理论与进路[J]. 福建师范大学学报(哲学社会科学版), 2020(4): 148-157.

[5] [美] 维克托·迈尔-舍恩伯格, 肯尼思·库克耶. 大数据时代: 生活、工作与思维的大变革[M]. 盛杨燕, 周涛, 译. 杭州: 浙江人民出版社, 2013: 207.

[6] Scott L. Power after Hegemony: Cultural Studies in Mutation [J]. Theory, Culture & Society, 2007, 24(33): 55-78.

心的地位之重,而被“异化”的骑手们放弃了自决自治的选择,仿佛平台算法的一个工具^[1]。从控制受众接触到的信息开始,对数据主体自觉权利不断挤压,算法这一只“无形之手”在决策过程中程序违背了伦理与法制规范的要求。但受到商业秘密的特殊身份的保护,算法的设计逻辑与运行轨迹往往不对大众公开,且算法本身也存在许多控制着无法从外部观察学习到的不透明“黑箱”。

在非商业中的算法的自动化决策行为也存在多方面尚未成熟的问题。司法实践中法官手中的自由裁量权使得法律适应时代的同时司法权力也保持着旺盛的生命力,在许多案件中协调了法律价值的冲突也一定程度地克服了立法的滞后性,因此裁量与决策的模糊性是有重大意义的。但是算法的自动化决策挑战了自由裁量权的设计,甚者,一些旨在避免权力主体在武断时作出的决策并保证其可信度与正当性的传统制度安排,包括了资质要求等声誉机制以及通知、听证、救济、异议等严格的决策法定约束程序,在算法的自动化决策面前均显疲软失灵。当压缩了原本主体自由意志的自治空间时,人主观能动的本质已经丧失。算法的设计初衷不外乎于帮助人类解放生产力,但过于泛滥的权利让渡使得技术凌驾于人类主体之上从而陷入马尔库塞提出的“单向度的人”的逻辑窘境中。

三、算法侵权法律规制路径的选择

(一) 规制的可行性与必要性

在算法规制的可行性方面,规制算法侵权行为的关键在于规制算法设计者的行为,而并非停留于算法这种技术工具。算法妨害横跨公私法领域以及其自身累积形成与不确定的特性,不仅是权利主体救济难以实质发挥的束缚所在,也同样是现阶段立法规制所面临的理论障碍^[2]。立足当下其发展势态与趋势,仅仅从信息保护入手尝试构建人工智能算法的法律规制体系必然收效甚微。于立法者而言,为什么选择标准而不是规则,抑或是选择一个规则而不是标准及其原因是什么,这与标准和规则对立法需求的回应有关。

立法者的这一选择可能纯粹是因为在当前立法背景下,选择其中一种形式会比另一种形式更好地服务于其法律治理目的。其一,立法者选择规则这

一形式,更多地考虑到确定性优先。相较于标准,规则要求法官一致行动,对待事实一视同仁。立法者通过设立规则防止法官在判决时受各方因素影响较大,从而降低了法官自由裁量权过大风险,最大限度保证公平。其二,当立法者选择标准这一形式,更多地考虑到灵活性优先。基于规则的判决抑制了相似性和差异性,而标准允许法官同等对待实质上相似的案件。因此,标准没有规则那么硬性。立法者对于行为尺度做一个大致的判断,找出其中的共通点形成规则,而将具体情形带来的差异化判断留给法官,法官能够更充分的考察个案中的不同因素。此外,根据《通用数据保护条例》(General Data Protection Regulation^[3],下简称“GDPR”)中第35条相关款项提出了数据保护影响评估义务的要求以此确保算法设计者或算法使用主体的意思自治空间,不再受到传统的“命令—控制”型规制中外部压力的影响^[4]。摒弃算法作为新兴技术总是客观中立的刻板印象,压实人工智能算法设计与运营方的主体责任是对于算法侵权的法律规制切入点^[5]。

算法法律规制的必要性一方面在于,标准与规则之间并不是鸿沟,标准与规则之间是连续体而不是分水岭。规则存在异化到与标准具有相似程度的可能,同样地,一个标准可能与其他标准

[1] 2020下半年,一篇名为《外卖骑手,困在系统里》的文章引起舆论热议,其中报道详尽地展示了作为食物链底端的外卖骑手们如何在平台、资本、算法、消费者和监管的夹缝中求生存现状,引人深思。具体参见赖祐萱:《外卖骑手,困在系统里》[EB/OL]. [2021-01-09]. <https://mp.weixin.qq.com/s/Mes1RqI0dp48CMw4pXT-wXw>.

[2] 解正山:《算法决策规制——以算法“解释权”为中心》[J]. 现代法学,2020(1):179-193.

[3] Seeing Council Regulation 2016/679, 2016O. J. (L 119). 2016年通过的《通用数据保护条例》于2018年5月实施,并替代1995年的《数据保护指令》(Data Protection Directive), Council Directive 95/46, 1995O. J. (L 281).

[4] 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(2):3-23.

[5] 孙莹:《人工智能算法规制的原理与方法》[J]. 西南政法大学学报,2020(1):83-95.

或规则相叠加,进而达到与规则相似的确定性。某些规则甚至是标准下反复出现的总结概括,这样看来,我们甚至可以认为“规则是一种已经达到认识论成熟的标准”。并且,标准与规则的混合运用也较为常见,比如我们利用算法控制的自动驾驶汽车时,应与前车保留一定距离以保障行车安全。这样的标准与规则的叠加使用,在保证法律确定性的同时更好的注重到了条文的灵活性,同时也给予了法官一定的自由裁量权。如果没有具体规则作为补足,实际上难以判断什么样的行为才是符合标准的,比如在行车中从车内向外投掷废弃物这一行为,难以事前对该行为是否符合“注意车辆及行车安全”这一标准进行判断,很大程度上依赖法官的自由裁量,此种情形即前文所指的“动态性”和“场景性”。

我国现有的算法及数据技术的法律规范远落后于高速发展的现实需要,如对于算法爬虫导致的破坏公平竞争的相关案件在法院审理时更多倾向适用现行的《反不正当竞争法》第二条的“一般条款”为依据,致使改保留法条被过度使用进而影响了不正当竞争法适用时的谦抑性。《电子商务法》《数据安全管理办法》等法律对于一些社会影响大的算法侵权事件作出了立法层面上的回应,具有明显的滞后性^[1]。对于平台算法作出了部分义务性的条款规定,现阶段能被用于解决算法侵权案件的已生效的法律法规资源相对匮乏,且由于缺乏有效的规制,被运用于商业领域的算法权力可能助长了相关价格垄断及不公平交易的产生,催生的监视资本主义也在威胁着数据主体的人格权利。如现行的《消费者权益保护法》《价格法》等法律无法较好地适用于“价格歧视”的实践规制。应当指出的是,欧盟作为经济与政治共同体与统一主权国家不同,算法技术下造成了个人权利保护相对匮乏,因其宽泛的范围界定能够确 GDPR 的有效实行,但同时正如美国学者所指出的,欧盟的算法规制由于过于宽泛,实际上无法从现行法中直接判断某种具体个人权利是否能够纳入或无法纳入 GDPR 保护范围^[2]。

(二) 建立与完善个人数据保护官制度

算法侵权的类型普遍具有存在的天然性,其

原因在于算法在设计之初便具备歧视性因素。例如,算法研发人员先天的主观因素导致的算法运行时出现的歧视现象,又或者是源于数据输入时的偏差,即“偏见数据进,偏见决策出”、算法模型设计阶段侵害数据主体权益等等。算法在人工智能的技术框架下进行自主学习,其侵权构成的要素复杂,侵权行为往往具有不可逆和难以预测的特性,致使预见性阻碍算法侵权行为的可能性微乎其微,如在个人信息侵权中,执法管理方往往重事后监管而轻事中、事前的审查预警。此外,我国对于数据主体的保护处于监管源“多且乱”的局面。算法的直接作用对象个人信息与隐私数据等等分布在不同的机构,有着复杂的存在形态。对应的监管部门包括了诸如国家工信部、公安部、商务部、等在内的公权力部门,众多且存在监管交叉重复、漏洞死角被忽视等问题。统一管理的缺乏直接导致了监管效率的低下^[3]。

由此可知,只有从源头上对其进行遏制才能最有效遏制算法侵权的存在。个人数据保护管理制度在数据时代快速发展中应运而生。有学者认为通过借鉴 20 世纪初欧美企业中兴起的首席隐私官(CPO, chief privacy officer)^[4]可有效落实数据隐私安全问

[1] 针对算法平台的规制立法,如针对引起热议的“魏则西事件”修订的《电子商务法》第 40 条规定“电子商务平台经营者应当根据商品或者服务的价格、销量、信用等以多种方式向消费者显示商品或者服务的搜索结果;对于竞价排名的商品或者服务,应当显著标明‘广告’。针对人民日报评算法新闻推送事件、朱烨诉百度案等国家互联网信息办公室 2019 年 5 月发布的《数据安全管理办法(征求意见稿)》第 23 条规定“网络运营者利用用户数据和算法推送新闻信息、商业广告等(以下简称‘定向推送’),应当以明显方式标明‘定推’字样,为用户提供停止接收定向推送信息的功能;用户选择停止接收定向推送信息时,应当停止推送,并删除已经收集的设备识别码等用户数据和个人信息。”

[2] Schwartz, et al. The PII problem: Privacy and a new concept of personally identifiable information [J]. New York University Law Review, 2011 (86): 1876.

[3] 周庆山. 完善我国个人信息保护管理制度的思考 [J]. 社会治理, 2018 (1): 34-41.

[4] 宛玲. 国外个人数据保护官的概念、职责与能力素质 [J]. 图书情报工作, 2018 (17): 129-135.

题。就其运行逻辑来看,其本身是一种综合二元的集行政监督、行业自律于一体且旨在增强数据以及算法技术安全性、可解释性的透明化进路的一种职业模式^[1]。我国香港地区在20世纪出台生效的个人信息保护条例中也开创性地设立了亚洲首个个人资料隐私专员公署这一独立的机关^[2]。学界主流探讨的数据保护官制度是由欧盟在2018年发布的GDPR中明确设立的数据保护官一职,即data protection officer,简称DPO,与美国商业公司中隐私保护官、德联邦设立的信息自由专员及香港个人资料隐私专员公署有异曲同工之处。

不仅是掌握了大量用户信息数据的商事企业,公权力部门和其他各种数据控制者、管理者、组织协会等等在涉及GDPR规定的相关个人数据的处理时都需要设立数据保护官。作为掌握着算法权力方、信息安全监管机构与数据主体三方之间的沟通桥梁,数据保护官的身份往往需要具有高独立性与专业性,个人数据保护官这一制度很大程度上可以突破数据使用方与权力主体之间身份的限制,避免数据使用方滥用算法权力侵权的同时一定程度上又可以弥补权利人相关专业知识与技术的欠缺。对于数据主体而言,个人数据官保护制度使其不用再花费冗长的精力与机会成本研读各种隐私政策条文,也不必纠结晦涩难懂的技术说明或专业法律上的繁文缛节。此外,理想的个人数据保护官制度可以规制算法运营商大部分因为算法外部性扩散引发的社会成本向普罗大众或弱势群体不合理转嫁的侵害行为,将抽象的信息数据安全具像化,将直白的生活语言二进制化。与此同时,其专业性与独立性也能防止外部法律与监察机关过度介入、苛责算法运营商的商业行为进而影响其在大数据市场中的竞争力造成因噎废食的局面。

(三) 配置个人权利对抗算法侵权

算法权力与每一个普通数据主体相比力量相差悬殊,算法侵权若未能从源头的解决,那么也应为数据主体配置相应的权利以抵御权力的滥用。针对算法歧视、自动关联及自动化决策三种不同的侵权路径,通过个体赋权的治理模式分别配置数据主体解释请求权、被遗忘权以及拒绝权的权利以对抗算法侵权的发生。

1. 解释请求权的设立

在商业领域算法运行中,多数平台将算法权力背后的程序设计、执行与仲裁等多角色集于一身,使得算法一旦决策错误出现失衡的状况时还会通过负调节等方式进行自我回馈,增强其偏见路径。这样的集权运作从权力分配设计体制上消解了算法权力自我“矫正”的可能性。有学者提出“信息信义义务^[3]”理论,企图从构建特殊行业义务方面着手解决问题,但改框架对于算法平台权利结构的设想过于美好^[4],现实中即使很多商业平台通过内部设置了申诉和处理机制的方式给算法歧视的纠正看似提供了一种可能,但囿于其有关规则等由算法单方制定、修改与执行,既是“当事人”又是“法官”的角色悖论使得用户处于被裁决的弱势地位,面对平等权的侵犯维护和申请救济更是处于绝对被动的状态。为了复杂交错的“算法权力”一个行之有效的外显途径就是增强算法决策的透明度,进而提高技术的可理解性与问责性。

解释权可以分为事前告知权与事后的请求解释权,欧盟2018年正式生效的GDPR的序言中明确指出,个体在遭受算法决策时有获取决策如何做出的解释并质疑的权力,在该条例的第13—14条中提到了数据控制者(算法设计方)对于数据主体有通知义务,且这种事前解释的告知义务先于算法决策的作出。我国《个人信息保护法(草案)》中的相关解释权条款采用的是对于个人权利影响程度的标准,相对于欧盟的《个人数据保护条例》更为广泛。而对于事后算法解释规则的确立,则要求算法的设计者和算法的应用者应当对算法做出决策的过

[1] 程尧,蔡一军. 人工智能背景下算法演进的风险及其法律规制——以域外模式为视角[J]. 山西大同大学学报(社会科学版), 2020(2): 33-39.

[2] 陈美仪,黎智敏,袁焯. 香港个人资料隐私专员公署: 社交媒体与个人资料隐私保障[J]. 全球传媒学刊, 2017(4): 80-86.

[3] 信息信义义务理论, 20世纪90年代早期肯尼思·劳顿(Kenneth Laudon)教授首创该词语,后由杰克·巴尔金(Jack Balkin)教授发展,旨在“一碗水端平”一般用户与搜集、分析、出卖个人信息为业的数据公司之间的关系。

[4] 莉娜·坎,大卫·博森,林少伟,等. 信息信义义务理论之批判[J]. 交大法学, 2021(1): 168-199.

程进行解释,从而使利益相关者的合法权益在遭受算法不当影响时,能够知晓自身合法权益遭受到的损害以及如何寻求救济^[1]。同时,在司法行政领域,考虑由公权力机关提供一定援助以平衡社会个体和算法数据中因为技术能力与理解水平不一带来的严重弱势也值得尝试,向数据主体提供平实易懂的解释以应对如侦查、起诉、审判等活动中中算法权力与公权力可能存在的歧视合谋。

诚然,算法解释权的设立可能影响商业秘密与算法相关的知识产权(如计算概率特定元素权重、比较组等)的保护^[2],也可能因为其解释限度面临可解释程度、与知识产权紧张关系的难题,但应注意的是算法解释权制度初衷所意欲实现的并非“完全透明性”的模型构想,而毋宁一种“适当的透明性”^[3],即算法模型逻辑与关键信息等可视化转化翻译才是解释的关键,而并非要求将算法模型与决策全过程完全公开的苛责。算法模型逻辑与关键信息等可视化转化翻译才是解释的关键,而并非将算法模型与决策全过程完全公开的苛责。通过因果联系与相关性的循环论证,进一步搭建起算法的可责性,防止“赋权失灵”的悲剧发生^[4]。

2. 被遗忘权的设立

算法通过自动关联分析对数据主体形成精准的追踪画像,让人越来越透明化、客体化的同时使得人作为主体附带的产生物“个人信息”变得逐渐商品化。数据互联不可遗忘的特点,加之当下个人信息可以被识别、爬取、篡改、利用甚至贩卖的“保护现状”,彻底改变了人与社会结合方式及其各自属性^[5]。“对于人类而言,遗忘一直是常态,记忆是例外。然而由于数据技术与全球网络的发展,这种平衡已经被打破。往事像刺青一样刺在人们的数字皮肤上。遗忘成了例外而记忆却成了常态”^[6]。鉴于此,作为人们在监视资本主义的焦虑中尝试对抗人格利益在数字化技术与算法中的减损的一种信息自决中新权利建构——被遗忘权则显得十分迫切。

如果说隐私权的出现是旧工业时代下个人私域对于过度干扰的对抗屏障;那么被遗忘权则是当下个人信息过度保存、利用及回收问题的一种弥补的方案。追溯到早期法国针对于刑满释放人员设立的“忘却权(le droit à l'oubli)”,该权力的“出身”说明了隐私保护不仅在于隐私信息特定呵护,更在

于人的主体性与人格自由的发展,对于信息时代中每一个数据主体“网络囚徒”身份困境的保护有重要意义。GDPR 中第 17 条规定了遗忘权,它的设立使得数据主体有权决定是否保留网上公开过的信息和公共空间中的数据痕迹等等,以及是否排除他人不合理的利用行为,进而主动界定和控制个人隐私边界。遗忘权的主动性和积极性与隐私内容保护的被动性、防御性形成互补,共同抵御算法自动关联爬取的侵略性与攻击性。

尽管当下被遗忘权可能被与其他权利诸如言论自由等平衡的困扰,也面临要与算法自动关联的利益直接获得者如各方商业巨头博弈等等的问题,但在法规政策、技术手段等的介入之下,遗忘权与其他利益冲突并不是不可调和,不能因噎废食对其一边倒进行否定。算法运行中自动关联的抓手伸向每一个数据主体的个人信息时,遗忘权的创设对于对抗数字化记忆的可访问性、持久全面等特性提出了一种可行的解决思路,一定程度上打破信息权力与时间的交汇处永久的创造了空间与时间上的圆形监狱“幽灵”困境。我国现行的相关法律条款中有涉及被遗忘权的相关规定,但其立法目的与制度设计更倾向于针对网络运营商收集个人信息的规制,与被遗忘权所要保护的客体、意思表示、抗辩事由及责任划分都有明显不同。被遗忘权的本土化移植可以从阶段性立法入手,借鉴《中华人民共和国

[1] Merle Temme. Algorithms and Transparency in View of the New General Data Protection Regulation [J]. Data Prot L. Rev, 2017 (473) .

[2] 邵国松, 黄琪. 算法伤害和解释权 [J]. 国际新闻界, 2019 (12): 27-43.

[3] Frank Pasquale. The Black Box Society: Secret Algorithms that Control Money and Information [M]. Cambridge, MA: Harvard University Press, 2015: 142.

[4] 张恩典. 大数据时代的算法解释权: 背景、逻辑与构造 [J]. 法学论坛, 2019 (4): 152-160.

[5] 李立丰. 本土化语境下的“被遗忘权”: 个人信息权的程序性建构 [J]. 武汉大学学报(哲学社会科学版), 2019 (3): 145-155.

[6] [美] 维克多·迈尔-舍恩伯格. 删除: 大数据取舍之道 [M]. 袁杰, 译. 杭州: 浙江人民出版社, 2013: 1.

计算机系统安全保护条例》等以地方试点的暂行条例等作为先导措施,再逐渐将被遗忘权引入正在制定中的《个人信息保护法》之中,进一步成熟完善对于数据主体的权利保护。

3. 拒绝权的设立

数字经济时代中,“作为数据生产者 and 使用者参与‘大数据基本循环’的普通公民,对于这里所使用的信息技术基础设施既无法把握又无法施加影响”^[1]。甚者,通过机器优势争夺的决策权力基于架构优势框定了人类的认知与行为模式,并嵌入优势指数的级别扩张影响从而反过来塑造社会运行方式^[2]。除了剥夺每个数据个体平等自决的选择之外,算法权力失控隐患埋藏在了对于个性化主体操控的深处。无论是个性化搜索、倾向性言论还是成瘾性交互设计、定向投放广告,从被吸引到产生黏性,被数据投喂的每一个用户在“睁眼即参与资本主义、开机即参与监视资本主义”的困境中,其面对屏幕的一次双击点赞、一次页面下滑等等的行为剩余价值被算法及其身后的平台方收割与变现。

面对算法的自动化决策,人类应当始终保有主体独立的、最终的决定权,既防止算法缺陷引发无法补救的风险,又在机器面前保有属于人类的自由和尊严。个人应有机会拒绝算法针对其个体的指引、评判或决定,避免人的主体性受到算法的全面侵蚀乃至掌控。拒绝权的前置前提是数据主体有被告知权利,即知情权。用户作为数据主体在其个人信息被行政、商业主体收集使用前有被通知并同意或拒绝的权利,我国2016年发布的《网络安全法》^[3]部分条文体系拒绝权雏形。

根据GDPR中第21条及其他相关条款,拒绝权是指在法律许可的范围内,数据主体有权根据自身情况拒绝授予网络传播等平台收集或处理其个人数据信息的管理。这一权利体现了对于数据主体自身信息绝对控制权以及个人信息自决理念的维护,是保障个体受众主动退出机制的重要保障之一。目前这方面的法律关系变革虽已有萌芽,但远不够成熟到可以匹配现实中算法技术日新月异的高速发展。不同程度的异议权、拒绝权、请求人工干预权等应当在算法应用(尤其是算法裁判或决策)的每一个阶段和场景得到确认,使人在算法面前仍然保留最后的自主性与反思的能力。

(四) 建立算法侵权损害赔偿制度

算法背景下的损害赔偿制度构建主要包含两方面的内容,赔偿主体的厘清以及如何提供救济。首先,算法损害赔偿制度的主体可理解为承担责任的主体,即根据数据主体所受侵害的过程对主体进行判断,以此确定赔偿责任主体是算法使用者还是算法本身。以自动驾驶汽车撞伤行人为例,直接作出撞上行人的这个决定的并不是车上的乘客也不是算法设计者,而是算法本身,单纯将相关责任归于算法这一并不具备真正意义上行为能力的主体,加之目前相关规制法律的缺乏,显然是不可行且不切实际的。然而,把责任推到算法设计者或使用者来说,他们在算法迭代升级和作出决策的过程中没有进行干预的,其原因在于算法在这个过程存在着自主学习的能力。

上述确定损害赔偿主体的解决关键可借鉴国外的学者提出了“场景—制度”的概念,并且国内的学者也提出类似的规制谱系来提供解决问题的方法,算法的种类和应用场景较多,因此我们可以针对不同的情况制定不同的规制的方法,来明确规定责任主体和对被损害利益的一方进行救济。算法在设计和应用的不同阶段,同样也要注意区分责任的主体。当出现侵犯数据主体的平等权时,这些很显然就是设计者在设计过程中对算法训练的数据的不足。被侵权的当事人可以向算法设计者主张算法责任,要求停止侵害和损失赔偿。获得赔偿的救济途径则可以通过上文的个体所提出的民事诉讼和集体诉讼,抑或者是通过向相关部门进行反应和申诉以获得赔偿。

四、结语

在我国从数字经济大国转型数字经济强国的

[1] [德] 罗纳德·巴赫曼, 吉多·肯珀, 等. 大数据时代下半场——数据治理、驱动与变现[M]. 刘志刚, 等译. 北京: 北京联合出版公司, 2017: 20-21.

[2] 张凌寒. 算法权力的兴起、异化及法律规制[J]. 法商研究, 2019(4): 63-75.

[3] 2016年我国发布的《网络安全法》中第41条规定“网络运营商在收集、使用个人信息是需要经过数据主体的许可, 同时要告知数据收集的原因及处理方式”。

大数据时代，算法为技术发展的产物冲击着传统法律模式的运行，也推动着旧法规制的变革。基于现实法律框架与实际情况补充完善算法侵权的权力规制路径、问责渠道与救济方式，以充分利

用好方兴日盛的技术进步更好地服务于人类社会生活的良好发展。

(责任编辑: 何 为)

Analysis of Algorithmic Infringement Risk in the Background of Big Data

Li Yuqi

Innovation Base of Forensic Technology Application and Social Governance, Zhongnan University of Economics and Law, Wuhan

Abstract: In the era of big data, social resources can be redistributed through algorithms, which greatly improves social efficiency. However, the technical bias, automatic relevance, and automatic decision-making of algorithms have infringed on the legal interests of data subjects to varying degrees. Aiming at the three types of algorithmic infringements that infringe on the equality rights of data subjects, the right to privacy, and the autonomy of free will, this article intends to propose three aspects of establishing a personal data protection officer system, configuring corresponding rights of confrontation, and optimizing infringement compensation remedies. A more complete algorithmic infringement governance system ensures that the rights of data subjects in the information age are not eliminated.

Key words: Algorithm; Big data; Technology infringement; Legal regulation