DOI: 10.11817/j.issn. 1672-3104. 2024. 01. 007

商业机构用户画像应用的政府治理责任研究

吴亮

(华东理工大学法学院，上海，200237)

摘要：商业机构的用户画像目前在人工智能系统、智能预测、场景识别等方面得到广泛应用，其“监控式”信息汇集方式带来的个人信息侵权风险、算法决策带来的过滤泡效应与差别对待风险，对政府的用户画像治理形成新挑战。我国已初步形成用户画像发展与治理的政策体系，相应法律框架也逐渐成型。在国际上，用户画像治理的政府责任包括个人信息治理和智能算法治理两种不同的模式，政府的用户画像治理责任应当在宪法的国家保护义务框架下，实现发展促进与风险预防的价值协调。我国应通过顶层设计对治理模式进行延伸迭代，推进个人信息治理与智能算法治理的协同，并且将预警原则和国家担保责任原则作为治理责任的分配原则。

关键词：用户画像治理；政府责任；个人信息治理；智能算法治理

中图分类号：D922.1 **文献标识码：**A **文章编号：**1672-3104(2024)01−0063−13

随着人工智能掀起新的技术革命，用户画像作为一种数据分析工具获得广泛应用。所谓“用户画像”(user portrait)，是指通过收集、汇聚、分析个人信息，对特定自然人的职业、经济、健康、教育、喜好、信用、行为等做出分析或预测，形成个人特征模型的过程[1]。无论是国家层面的公共治理还是私人层面的精准营销，都通过用户画像收集、挖掘和分析公民个人信息，描绘人格轮廓或群体概貌，进而预测使用者的特质或需求。在国外，剑桥分析公司利用脸书(Facebook)使用者的网络活动记录建立用户图像，对社会公众精准投放政治宣传广告，预测和影响总统选举活动。谷歌、微软等商业机构结合用户在搜索引擎和网站的浏览与交易记录，分析其潜在消费需求与消费能力，使其个性化推荐和广告投放更加精准。在国内，政府部门汇聚低保、残疾人、优抚等保障对象的数据，制作困难群众的个人画像，为疫情防控、社会救助与精准扶贫提供支持。人民银行征信系统、百行征信等机构收集、处理和共享源于金融机构、互联网金融的信用数据，依法合规向社会提供公民的个人信用画像，为普惠金融服务提供良好助力。然而，用户画像在增加消费者便利、促进产业创新与社会管理而受到青睐的同时，也带来网络社会治理的新挑战。“北京大生知行科技有限公司与罗懿个人信息保护案”“王某诉每日优鲜公司隐私侵权案”等都表明，某些商业机构忽略了个人信息不当收集和使用、算法决策带来的过滤泡效应与差别对待风险等问题。由于用户画像引起的法律问题具有复杂性，目前的法律治理框架难以彻底解决。政府应当顺应用户画像自身的逻辑和规律进行治理，在借鉴国内外经验的基础上探索改良创新的路径。囿于篇幅，本文的讨论以商业机构的用户画像应用为主，不涉及公共部门的用户画像应用。

收稿日期：2022−12−29；**修回日期：**2023−07−26

基金项目：教育部人文社科规划基金项目“公共数据授权运营的行政法规制研究”(23YJA820028)；上海市浦江人才计划项目“公共数据开放的行政法问题研究”(21PJC027)；上海市教育科学研究一般项目“学生网络欺凌的法律防治与网德教育研究”(C2021013)

作者简介：吴亮，男，安徽池州人，法学博士，华东理工大学法学院副教授，主要研究方向：行政法学、数字政府建设，联系邮箱：wlwulaw@ecust.edu.cn

一、用户画像的广泛应用及对政府治理的挑战

(一) 用户画像的广泛应用及其特征

“现代信息社会是由资讯网络形成的社会结构，并被不断创新的高科技所推动。”[1]用户画像的法律规范虽然是制度构建问题，但是首先要面对的是技术认知问题。用户画像的理念最早是由交互设计之父库柏(Alan Cooper)于 1999 年提出的，指“通过真实数据分析得出标签化的目标用户模型”[2]。换言之，给个体或者群体用户贴上多维度、提炼化的标签，加以综合就能勾勒整体特质的画像，例如健康画像、信用画像等。用户画像的数据内容广泛，涉及人口属性、兴趣特征、消费特征、位置特征、设备属性等。网络服务提供者、社会治理机构在大数据与人工智能技术的基础上，依托聚类分析、关联规则等算法比对和分析用户的行为记录，全面描述和剖析其特征，合理预测其心理和行为。在技术上，用户画像需要经过“数据收集—数据清洗(聚类分析)—细分假设—算法建模—构建画像—场景应用”的流程[3]。在功能上，用户画像可以挖掘用户的个性化特质，洞察未来趋势和人群差异，提升管理精细度、营销精准度与服务匹配度。迄今为止，用户画像已经广泛应用于人工智能系统、智能预测、场景识别等领域。

1. 人工智能系统的应用

用户画像借助由深度学习、智能算法、类神经网络与大数据分析组成的人工智能系统的预测功能，对数据实现语义层、服务层的融合，提高行为预测与决策回应的科学性与客观性。首先，嵌入深度学习技术的人工智能是人工智能的第四级——最高级类型。与设计者给予特征的机器学习不同，深度学习是由机器自己创造特征，提升了人工智能感知的自动化程度。基于深度学习的智能算法配合类神经网络(CNN)的使用，使机器得以模仿人脑进行函数演算和非监督式学习，分析与辨识出海量数据蕴藏的潜在规律，进而达到预测效果[4]。其次，类神经网络是深度学习的技术基础，模拟生物神经系统网络进行信息处理的数学模型，其运作分为依据演算法对输入数据进行运算的学习阶段，以及通过神经元输出计算结果和进行可靠性验证的回想阶段[5]。最后，大数据技术也是用户画像的重要技术依赖，可以针对海量数据进行比对和预测，在数据分析阶段发挥关键作用。

2. 智能预测的应用

随着人工智能系统的自动化，各领域的用户画像应用均在不断拓展智能预测的探索。在商业营销与金融领域，用户画像模型通过挖掘和剖析用户的静态和动态数据，勾勒产品服务的供需情况，进而精准预测消费者的潜在需求，挖掘用户的偏好与情绪需求。在社会安保领域，基于用户画像的安保防控措施颇为常见，精准锁定安全保卫热点和维护社会治安。欧盟的乘客姓名记录系统(PNR)的用户画像模型已能通过乘客的航空活动信息预测其社会关系、精神状态和行动意图，从而甄别可疑的恐怖分子[6]。不过，基于人格尊严、个人隐私及相关监管政策的限制，通过用户画像来预测个人行为的活动很大程度上处于被限制或禁止的状态。

3. 场景识别的应用

用户画像有助于建立完善的用户洞察模型，以行为区别用户，提高社会管理者或者商业机构的场景识别能力。目前，用户画像的场景识别应用主要有以下两种[7]：一是行为模式剖析，即为了研究行为模式以及既有行为的意义，通过归纳法、演绎法发现固定模式与解释偏好规律。最常见的是利用网络浏览记录来追踪在线消费者的活动，或者通过智能穿戴设备的手势、行动、睡眠等资讯，推测消费者的个性特质、社交偏好等个人信息。二是定位剖析，即商业机构通过位置服务(LBS)、打卡记录等来定位某区域内的大规模人群，推测其行程安排、导航路线、消费地点等，并用于精准营销和广告投放。不过，场景识别应用的生态仍然有待改善，用户隐私安全与信任、多类型数据的使用、多维度数据的融合、行为预测的准确度等关键性瓶颈均有待突破[8]，用户画像带来的网络社会治理风险也未被充分理

解，这些都对场景识别应用的扩展形成阻碍。

(二) 用户画像的政府治理挑战

用户画像的应用蕴含巨大的社会与经济利益，但是也带来延伸性、渗透性的法律风险，需要依托政府、社会的多元协同治理才能有效应对。对于政府端而言，用户画像应用给政府促进发展与预防风险的治理能力提出了如下挑战：

其一，用户画像所依托的“监控式”信息汇集方式极大削弱了用户的个人信息控制能力，加剧了网络社会中数据处理者与用户之间的权力失衡，而个人信息保护制度缺乏有效应对机制。用户画像的第一个步骤就是汇整与统合不同来源的个人信息，发现其关联性并且建立联结，具体举措包括：一是不对称的秘密监视，用户持续处于完全可见的透明状态而数据处理者则不可见。二是对人群的全面检查，通过分类识别、评价预测、赏罚奖惩等机制有效地引导用户的行为模式。据调查显示，一些商业 APP 暗中通过“擅自收集”“超范围收集”等违规方式，精准且长久记录完整的消费者图像，用以预测、调控和独占用户的未来消费决策①。这种“监控式”信息汇集方式会造成新型个人信息侵权风险。信息处理者将用户累积的数据提炼成零成本、高价值的资产——行为盈余(behavior surplus)，通过向用户索取、主动收集等方式萃取和重组描绘个体样貌的数据。这种秘密监视方式持续时间长、分布区域广，难以被觉察。个人信息的使用和流通由大数据与人工智能自动完成，用户根本无从知晓和介入，从而侵犯到公民不受干扰和审查的信息自决权。

公私部门运用大数据技术系统、全面地收集用户的个人信息，进而形成以信息监控为特征的监控社会。大量个人信息被汇整而成的特征描绘(profiling)使信息处理者能够贴近观察与监视用户的一举一动，甚至从中推敲出未经揭露但是更具敏感性、私密性的个人信息。用户对其个人信息的控制程度逐渐降低，导致个人特质遭受他人详尽观察的“累积效应”[9]。美国法的“马赛克理论”详细描述了这种信息累加整合而产生的加权效果。随着技术的进步，累积效应导致信息资料的可识别性标准出现相对化、流动化趋势，弱化去识别化措施的保护效果[10]。任何不具有识别性的信息都可能通过与其他信息资料的交叉比对，转变成为可识别的个人信息。这类信息资料由于已经公开或者被使用，导致无法再以个人信息的名义加以保护，由此产生个人信息保护的法律难题[11]。而且在整个监控的过程中，用户毫不知情，甚至在追求消费便利的过程中自愿参加和主动接受规训。后续的用户画像大多属于超出收集目的的“目的外使用”情形，不仅复杂难测，而且欠缺透明度，用户对其自身信息收集、使用的认知有限，甚至被排除在外而无法有效应对。“监控式”信息汇集方式造成事前告知同意程序失去意义，个体对个人信息的控制能力降低。

进一步而言，用户画像是依托高科技建构的“人际互动之虚拟形象”，识别、监视乃至塑造着个人在真实空间的消费主体面貌，蕴含着对社会成员产生自我规训与隐形约束的权力效应。用户画像的全面检查方式提高了商业机构对消费者的控制效率，使其沦为被观察的档案和被权力宰制的对象。其重点不是用户的自我决定与发展轨迹，而是其行为模式必须受到商业机构的检查，以及受到积分、评等、排名等奖罚机制的矫正和引导。商业机构通过用户画像来检查和控制普通人的状态，占据观察和检查的优势地位，它和社会公众之间产生“观察者”与“被观察者”的不平等权力关系，“深刻介入个人的内心与行动，根据人们的过去塑造人们的现在与将来”。

其二，依赖智能算法的标签分类会嵌入程序设计者、决策者的主观价值偏见，或者在关联性分析中融入不符合社会价值观的判断，明显扭曲决策的合理性，增加过滤泡效应与差别对待风险。用户画像的应用并非仅仅是取得用户人格、喜好的特征描绘，更重要的是辅助决策。信息处理者运用智能算法对用户数据进行关联性分析，比对与预测用户不为常人所知的人格特质，衍生个人并未直接提供的新数据，用以预测、调控和独占用户的未来消费或者行为决策，个性化推荐、行为定向广告、智能安保设施就是典型案例。但是，这种用户画像应用虽然满足用户的个性化要求，但是也造成个体成员隔离于整体社会的影响人们对周围环境正确认知的“过滤泡效应”。

用户画像一旦分析出个人的心理偏好、消费倾向、行为模式，就会根据预测结果层层过滤，量身打造令其满意的信息内容，隐藏不符合其意向的内容[12]。这种做法势必导致个人接触的信息同质化，容易窄化个人的认知范围，进而影响到思想和行为自主性，减少人们对新理念、新行为或者社会互动的尝试，侵害和限制人格的自由发展。

除了过滤泡效应之外，程序设计者、决策者在通过基于特征描绘的关联性分析对用户进行标签分类时，在算法中可能会融入强烈的个人主观偏见，导致差别对待的扭曲结果。这包括两类情形：一是数据不当联结，将人脸特征、声音联结到人格特质、性格取向、智力缺陷等，可能对特定群体造成严重的刻板印象与歧视对待。如根据现有的罪犯人脸数据库辨识出具有某项特定人脸特征的公民，将其作为潜在罪犯予以重点防范，这种做法超越道德判断与人格尊严保护的法律底线。“算法运算过程的不透明性，并不客观完整的数据样本，以及人类对人工智能技术的滥用和对算法决策结果的盲目自信，导致算法错误被进一步放大。”[13]二是数据偏差引起的歧视。由于数据输入的不准确、不完整、不及时，或者目标对象本身由于贫困、偏僻、漏报而影响了数据的精准性，都可能造成用户画像扭曲决策者对特定群体的正确印象，进而导致决策的不公正[14]。以刷单炒信现象为例，个人信息或者用户评价的失真导致用户画像数据在收集阶段就有严重瑕疵，并且影响到贷款、授信、交易等决策的客观准确。

二、我国用户画像政府治理的政策立场与法律框架

自 2018 年以来，我国开始对用户画像相关活动进行法律监管。2018 年 5 月，国家标准化管理委员会发布推荐性国家标准——《信息安全技术个人信息安全规范》(GB/T 35273—2017)，标志着用户画像风险规制工作被纳入政府治理的轨道。迄今为止，我国针对用户画像政府治理领域的政策立场日益清晰，法律框架也逐渐成形。

(一) 用户画像政府治理的政策立场

1. 对智能预测应用的积极支持

基于用户画像的智能预测应用是促进我国全面数字化转型的重要举措，得到了数字经济、数字政府等领域的政策认可。在数字经济领域，中央全面深化改革委员会《关于深化新一代信息技术与制造业融合发展的指导意见》以及上海市委、市政府《关于全面推进上海城市数字化转型的意见》等地方性政策，均将基于用户画像的智能预测应用纳入数据服务产业扶持政策体系中，强调要以挖掘社会数据要素价值为导向，统筹规划、系统构建产品智能化与数据驱动的新兴服务业态，促进相关的组织架构、算法规制、标准制定、安全评估等能力建设。《广东省人民政府关于加快数字化发展的意见》提出大力发展数据清洗、建模、可视化、用户画像、行业分析、信用评价等数据服务产业[15]。在数字政府领域，《国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》提出“加强数字社会、数字政府建设，提升公共服务、社会治理等数字化智能化水平”的目标，为智能预测应用在公共服务、文化消费、小额信贷等领域的推广奠定了政策基础[16]。国务院《关于进一步优化营商环境降低市场主体制度性交易成本的意见》提出“对企业进行分类画像，推动惠企政策智能匹配、快速兑现”。这些规定为政府促进用户画像与数字治理应用场景的结合，提供了有力支持。

2. 对场景识别应用的严格监管

自 2018 年起，我国对场景识别应用的政府治理日趋严格。以基于用户画像的定向推送服务为例，《信息安全技术个人信息安全规范》限制个人信息收集的明确身份指向性，避免用户画像精确定位到特定个人，如推送商业广告不得直接使用基于特定自然人个人信息的用户画像[17]。《关于开展 APP 违法违规收集使用个人信息专项治理的公告》倡导 APP 运营者在定向推送新闻、时政、广告时，为用户提供拒绝接受定向推送的选项。《信息安全技术个人信息安全规范》新设用户画像的使用限制条款：个人特征描述不得包含恐怖迷信，危害国家安全、荣誉和利益等违法内容；

用途也不得侵害公民、法人和其他组织的合法权益，不能危害国家安全、荣誉和利益。《互联网信息服务算法推荐管理规定》要求加强用户模型和用户标签管理，不得将违法和不良信息关键词作为用户标签并据以推送信息。

3. 对不当处理个人信息行为的强力约束

《信息安全技术个人信息安全规范》确立了用户画像对个人信息收集的“最小够用原则”，并要求个人信息处理者的隐私政策应当涵盖收集、使用用户画像的目的及各个业务功能。《互联网个人信息安全保护指南》依据用户画像的增值应用为用户所带来的法律后果的不同，将其区分为“不经用户授权”和“经用户授权”两种形式，并强调用户有反对或者拒绝的权利。《APP违法违规手机使用个人信息自评估指南》规定，如果APP经营者将个人信息用于用户画像、个性化展示等，隐私政策中应说明其应用场景和可能影响。《互联网个人信息安全保护指南》以是否可能为用户带来法律后果作为标准，划分用户画像的用户授权同意机制。《信息安全技术个人信息安全规范》首次规定对信息系统自动决策的安全影响评估要求，以及对涉及申诉的决策结果增加人工复核的要求。《个人金融信息保护技术规范》明确将用户画像、特征标签等加工后的信息纳入个人信息或者个人敏感信息的范畴，强调整合个人信息须经本人授权同意。

(二) 用户画像政府治理的法律框架

法律是“体现时代特征并与公共政策保持密切亲缘关系的规则体系”[18]。分析用户画像治理的政府责任、总结政策得失，离不开解读既有的法律框架。尽管我国尚未针对用户画像的政府治理出台专门性法规，但是治理的法律框架却有迹可循。我国已经建立起一系列法律规范，既赋权政府预防与惩治犯罪、防范网络风险、保障公民合法权利等多项责任，也授权政府实施多项举措以促进大数据产业与推动数字治理的发展。这些法律规范为用户画像政府治理提供制度支撑，构成政府部门的责任界限。

1. 引导用户画像相关产业发展的法律框架

《数据安全法》确立了以数据开发利用与产业发展促进数据安全的统筹发展理念，对不同领域的专门性立法提供方针指引。这些专门性立法包括交通管理、公共安全、民生服务等方面的地方性法规、规章和规范性文件。如国务院出台放管服改革优化营商环境法规，在信用信息的归集共享基础上形成完善的小微企业风险画像，引导金融机构的普惠小微金融服务[19]。上海市施行“一网统管+精准救助”法规体系，汇聚多部门数据形成个人和家庭属性标签，从社区、家庭、个人三个维度对社区居民进行民生画像，提高社会救助服务能级。上述法律规范已经为政府推动用户画像的发展提供了基本框架。用户画像的发展面临着裁量措施的合理性、创新激励的有效性、财政优惠的合法性等问题，在制定相关法律政策时需要加以回应，为政府发展用户画像的法定责任提供规范指引。

2. 防范用户画像风险的法律框架

在风险预防方面，基于既有的个人信息保护、数据安全、算法应用的监管实践，有关政府责任的法律框架比较清晰。这包括以下两方面内容：

一是有关个人信息保护与数据安全的法律规定，在用户画像政府治理方面具有价值导向作用。《数据安全法》对用户画像虽未直接涉及，但是对数据处理者确立了“合法、正当、促进经济社会发展，增进人民福祉，符合社会公德和伦理”的原则。《个人信息保护法》强调涉及用户画像的自动化决策若可能对个人权益造成重大影响，个人对其信息的收集与处理拥有反对权与拒绝权；在通过自动化决策方式进行商业营销、信息推送时，应当提供不针对其个人特征的选项。《数据安全管理办法》要求网络运营者不得以改善服务质量、提升用户体验、定向推送信息、研发新产品等为由，以默认授权、功能捆绑等形式强迫、误导个人同意收集其信息。《深圳经济特区数据条例》也规定了数据处理者对用户画像的规则与用途的明示义务，且个人拥有拒绝用户画像与个性化推荐的权利。另外，金融、社交平台、健康防疫等专业领域涉及用户画像的个人信息保护也逐步加强，如《个人金融信息保护技术规范》新增用户画像对个人特征描述的限制、个性化展示

与数据汇聚融合的限制等要求。

二是有关算法应用的法律规定。《关于加强互联网信息服务算法综合治理的指导意见》明确了商业机构对算法应用结果的主体责任，对检索过滤类算法强化特征库和标签库的有效性评估，对调度决策类算法加强对不合理差别待遇的治理。《互联网信息服务算法推荐管理规定》要求算法推荐服务提供者向用户提供选择或者删除针对其个人特征的用户标签的功能。《上海市网络交易平台网络营销活动算法应用指引》规定网络交易平台经营者应当确保消费者画像依据来源合法，尊重消费者人格尊严，避免使用有违社会公德、歧视性、偏见性的用户标签。政府责任全面渗透到用户画像治理的各领域，成为行政执法的重要依据。

三、域外用户画像政府治理责任的两种模式

用户画像的兴起伴随着商业机构数据监控权力的不断加强，基于特征描绘的算法决策也蕴含着过滤泡效应与差别对待风险。这种风险难以通过市场力量加以化解，需要由政府介入实施规制，消除用户的侵权风险与维系市场主体的创新动力。从国外实践来看，用户画像政府治理责任具有“以信息主体信任为中心的个人信息治理模式”和“以算法主体责任为中心的智能算法治理模式”两种不同的模式。

(一) 以促进用户信任为中心的个人信息治理模式

个人信息治理模式已经成为欧美政府治理责任的主流模式，如《欧盟一般信息保护规范》(GDPR)、《英国信息保护法》(DPA)、《美国统一个人数据保护法》(UPDPA)、《美国加州隐私权法案》(CPRA)等。正如美国学者拜尔金(Balkin)在《隐私的受托模式》一文中所指出的，将信托关系下规范契约当事人之间法律关系的做法引入个人信息保护领域，建立基于信任关系脉络的信息受托人模式，强化数据处理者依据信任关系所承担的忠诚义务是用户画像政府治理的发展趋势①。相对于用户而言，数据处理者是居于个人信息控制和专业知识的优势一方，因此应当善尽基于委托的双重忠实义务：第一，在数据处理者与用户之间，用户将其个人信息通过合意转让给数据处理者，数据处理者应当为了维护用户的最佳利益而利用数据，协助其有效行使自主权能，并担保人格尊严等权益不因数据滥用而产生侵害风险。第二，在数据处理者与国家、社会之间，国家、社会基于信任将个人信息的利用权限委托给特定的数据处理者，数据处理者应对其活动的合法、公平承担担保责任，并遵守监管规则。为了确保数据处理者履行信息受托人义务，法律应不断强化公民同意其个人信息用于用户画像的各项权利，保障其掌握个人信息流动的范围，同时通过高额罚金、司法救济和信息安全机制，课予信息处理者管理个人信息的各项责任。主要的制度设计包括：

其一，强调数据处理者向用户的充分告知义务。为了消除“监控式”信息汇集方式带来的危险，世界各国均将充分告知机制作为个人信息保护的基本要求，如《欧盟一般信息保护规范》针对用户画像的告知义务向数据处理者提出两项合法标准：一是告知内容应当具有实质意义，包括数据处理者会收集和利用何种个人信息，用户画像的分类标签逻辑等；二是用户画像及其后续决策对数据来源主体可能造成的法律后果应予告知。

其二，强化信息主体的自主性与反制“捆绑式同意”的用户同意权强化机制。如《欧盟一般信息保护规范》(GDPR)规定，除了基于重大公益目的或者履行用户和信息处理者之间的协议所必需，用户画像对个人信息的收集和利用应当具备用户“自主、具体、知情、明确、明示”的授权同意[20]。只要用户反对或后续申请撤回，则与其相关的信息收集与用户画像服务行为须立即停止。对于涉及宗教信仰、生物识别特征等敏感性个人信息的用户画像，优先保护个人信息权益，原则上不得利用此类信息进行自动化决策。

但是，个人信息治理模式仍然存在着诸多不足：第一，混合资料(bastard data)的出现动摇了

以个人信息保护为基点的用户画像政府治理框架[21]。随着大数据分析、机器学习促成的“数据累积效应”，个人信息的可识别性标准遭遇严重挑战，信息处理者可以从非个人信息中轻易获取相当于个人信息的混合资料，并且逃脱法律的监管。第二，以告知同意规则作为获取个人信息合法权源的制度设计不适应实际需要。在告知层面，隐私政策冗长、不明确，用户受限于认知偏差、信息不对称而不能完全理解隐私政策，或误解隐私风险[22]。在同意层面，用户画像如果不涉及跨网络运营者使用或者不产生法律结果，就可不经用户授权使用其个人信息。然而，“不经本人授权”由于欠缺必要的配套机制，面临着个人信息易遭滥用的质疑。法律虽在免于用户事前授权的条款中内置了用户反对或拒绝权，对于其内涵外延、落实机制却没有详细表述。这种缺位导致立法和实践难有大的作为，只能停留在象征意义的宏观话语。另外，第三方接受个人信息处理者的转让，对个人信息的增值应用虽然需要履行告知同意程序，却无法回应“个人即使同意交出信息也仍有隐私权保障之必要”的法理质疑[23]。第三，当前的法律聚焦于规范对个人的信息收集和特征描绘，却忽略了特定群体的信息收集和特征描绘。在实践中，很多信息处理者利用机器学习技术先建立不同资料组的特征，在此基础上概率性剖析特定个人属于何种群体，同样可以实现对个人的特征描绘。第四，用户画像使用者与不同用户之间从点到点的线性关系演化成由多点组成的个面关系，难以准确界定侵权范围。如在剑桥分析公司丑闻事件中，不良企业通过平台媒体的订阅者向外散布政治广告，误导更多人的投票决策，实际受害者难以估量。而且，用户画像造成的侵害是个人信息收集、处理和数字身份决策共同加成的结果，人们的自我认同、人格特质都会受此影响，具体的侵害效果难以量化评估。

(二) 以正当程序约束为中心的智能算法治理模式

智能算法治理模式着眼于强化算法主体的课责性，通过创造出符合正当程序原则的算法管制规则，弥补个人信息治理模式对用户画像的规范缺失。围绕正当程序约束来强化用户画像的法律监管是发达国家的重要经验[24]。2021 年《欧盟人工智能法》、2019 年《欧盟人工智能伦理准则》、2020 年《美国人工智能倡议法》、2019 年《美国人工智能增长研究法案》(GRAITR)及其配套的《美国人工智能政府法案》均主张参考正当程序逻辑约束用户画像与算法分析决策，排除公私部门“算法黑匣”的恣意操控，保障个人得到公平公正对待，并且满足公众对政府决策的安定性、可预测性需求。有学者归纳了正当法律程序对自动化决策的管制要求，即“规范应事先制定以减少恣意裁量的可能；规范应平等适用于同类个案且得出近似的结果；确保规范的随机适用不会被任何利益团体操控”[25]。迄今为止，学界和实务界对基于用户画像的自动化决策进行程序规范的认知，主要是围绕人为介入搭配算法透明两项义务来开展程序管制的，具体包括两项内容。

其一，算法决策的人为介入义务，即在分配智能算法与自然人在决策执行中的互动关系时，以自然人而非机器作为最终课责对象，内容包括“算法只能辅助自然人作出决策”和“自然人保留事后推翻算法决策的权利”。这是由于，智能算法的运作具有不可预测的特征，可能在关联性分析中形成歧视性、不公正的推论与评价结果，并导致公民由于担心受到差别对待而有意无意地改变内在思想与外在言行，对人格尊严和人性自主造成影响。人为介入义务的具体要求包括：在算法建构阶段应由自然人判断数据选择和算法应用的适当性；在基于算法的决策阶段应由自然人审查基于算法的自动化决策逻辑是否合理，并据此决定采纳、修正或者推翻。

其二，算法应用的透明化义务，即通过算法相关资讯的披露打破智能算法的黑箱，提升自然人对智能算法的掌握度与信任度。由于算法决策的正当性取决于自然人对算法内容的掌握程度与信任程度，因此，人为介入义务需要以“算法具备说明能力”作为人机良性互动、避免算法出错的主要规制手段。换言之，通过一定的透明化手段让社会公众得以理解数据、算法及其各种判断的过程，降低智能算法的不可预测性，提升人

们对其的信任程度。这里的透明化手段具体包括两种：一是“形式透明化型”，即将算法程序代码向社会进行披露和公示，方便监管部门进行静态分析。如《美国人工智能政府法案》规定商业机构运用用户画像时应当将其算法程序、训练数据交由权威的第三方专业机构审核，确保其符合安全、合理标准。但是，算法程序代码本身的复杂性、无序性，仅有静态分析可能误导社会忽略其潜在的关键弊端，同时静态分析难以追踪算法程序与环境互动的实际过程，难以完全消除算法偏差。二是“实质透明化型”，即要求商业机构在运用用户画像时实现全过程公开透明，确保数据输入、算法模型、逻辑决策、信息筛选、动态展示等全过程信息的动态汇集与公开披露，避免决策者借助“算法黑箱”逃脱法律规范和社会监督。典型的如《欧盟人工智能法》《美国人工智能倡议法》等。

但是，智能算法治理模式也会遭遇一些疑难问题：第一，透明化错觉问题，即大量的资讯披露会给社会公众带来透明化明升暗降的错觉，未必代表更有效的透明化[26]。数据处理者可能会通过控制算法披露的时间、增加算法理解的难度、延时更新数据库、以多重披露制造理解混乱等方法，误导社会公众的认知和降低外部监督的成效。第二，系统漏洞问题，即算法公开会泄露自动化决策机制中的代理变数，导致社会公众知晓某些非直接测量结果的评估因素，比如测量履约风险的薪资、人格特质、信用记录要求，并且采取规避应对措施[27]。随机变数的产生方式如果为人所知，或者在不确认变数是否真的随机而有可能存在规律的情况下，就会影响算法的预测与评价功能，易造成自动化决策的不公平或失真。第三，私人部门透明化的正当性质疑。要求私人部门的特定信息向社会公开透明，在很多情况下未必经得起利益平衡原则的考验[28]。如果不存在超越商业秘密、知识产权、经营自主权等私人利益的公益保护之必要，则不宜向私人部门课以公开义务。因此，如何适应技术的发展加强对上述问题的应对，是进一步制度设计要认真对待的问题。

四、我国用户画像政府治理责任的重构与配置

(一) 用户画像政府治理责任的理念重构

用户画像应用既有正面意义，也存在技术风险，运用政府规制实现市场因素与国家任务的协调是一条可行途径。政府对用户画像风险的治理责任可以回溯到宪法上的国家保护义务理论。国家保护义务源于基本权客观规范体系，在德国法上是指国家负有保护公民生命、健康、自由与财产等法益的作为义务，在“具有危险防御功能的法治国”“社会国”原则下，积极排除来自第三方主体的侵害或危险行为[29]。我国宪法制度虽然与德国有别，也无法简单套用法治国、社会国概念来诠释国家任务，但是在处理发展促进与风险预防的关系方面，国家保护义务理论具有借鉴意义。国家在实施宪法第十四、二十条规定的“发展、促进和推广科学技术以及发展社会生产力”任务时，也要从维护人性尊严与人格自由发展的角度出发，为用户画像确立清晰合法的行为价值标准。有学者整理国家针对七种宪法风险的预防义务，并指出该义务对基本权利的保护程度与方式，随着现代社会风险的高度不确定而呈现出动态扩张的趋势[30]。

在宪法的国家保护义务框架下，为实现发展促进与风险预防的价值协调，实现用户画像政府治理的目标协同，需要实现不同价值趋向的动态平衡。以风险预防为导向的国家保护义务不限于消极排除侵犯公民个人信息犯罪等现实损害，更包括积极防范用户画像的数据安全、差别对待等风险，在其未对公民权利造成严重且不可恢复的损害之前，进行有效管控。但是，风险预防的目标并不是零风险，而是通过成本效益分析建构适当的保护标准，实现社会公共利益与风险预防之间的最大净收益。数字革命是社会进步与经济发展的动力，政府应当适度容忍伴随其而生的“剩余风险”合理存在，对危害后果是否发生、发生时间与范围难以确定的危险不必一概干预[31]。“国家不宜漠视人们对风险的恐惧，忽略人类理

性局限而采取过度避险的措施。”[32]政府如果贸然采取积极干预措施，可能拘束第三人的行动自由、财产权、经营自由、商业秘密而造成权利冲突。因此，国家干预措施的选择应当保留灵活性，不宜将所有用户画像的应用一概纳入高风险治理框架，而要根据其涉及的信息安全风险程度、关联性分析涉及的违法性与不当性、可能影响的范围、受害权利的性质等因素，在“禁止过度侵害”的最高限度与“禁止保护不足”的最低限度之间作出最佳判断，设计分级规制体系。

(二) 用户画像政府治理责任的模式重构

我国的用户画像政府治理虽然跻身世界前列，但是仍然主要停留在传统的个人信息治理模式层面，偏重个人信息收集阶段的信息安全保障，对基于特征描述之算法决策阶段的技术治理不足，偏重监管信息但是监管算法尚不充分，信息与算法分而治之且未形成有机统一。依据不同风险的分类管理是技术治理的普遍做法，有助于根据不同的场景实现规制精细化。用户画像是个人信息、算法及一系列判断的组合，因此，技术治理体系理应将个人信息和算法作为两大分类标准，从单一管控走向多元统筹，推进本土化制度建设与规范引领，形成在全球更有影响力的用户画像治理政府责任体系。

第一，推进政府对个人信息治理模式的全链条责任治理。当前，我国政府的用户画像治理责任主要聚焦于信息安全导向下的信息服务规范和用户个人信息保护，尽管已经在个人信息治理的基础上作出诸多细化与创新，但是仍然需要进一步优化。用户画像在应用过程中造成扩散性风险与危害，传统的告知同意机制远不足以应对情势考量与案件裁判之需要。首先，需要强化现有的告知同意机制，并由政府进行监督，进一步落实《个人信息保护法》的公开透明原则，提高告知内容的清晰、全面、准确程度，确保用户同意是建立在充分考虑和正确认知风险的基础上的[33]。其次，将全链条责任治理的重心从个人信息收集阶段转向利用阶段，减轻用户基于同意而自担侵权风险的责任，加重数据处理者作为信息受托人的信息安全责任。应当以数据处理者为中心来设计责任承担规则：一是明确商业机构的“个人信息担保义务”，包括不得超出法定范围与限度利用个人信息，对个人信息处理的全过程进行告知、通知与公示，保障信息质量，进行来源合法性审查、敏感信息校验等。二是确立商业机构对配合行政规制和公民请求救济的严格协助义务，如履行风险监测、数据认证、算法审查、资料申报等手续，为公民设立程序参与、撤回退出、赔偿请求、违规举报等机制。强化数据处理者对用户受托责任的制度设计，有利于督促其认真协助公民妥善行使知情、访问、更正、删除等权利，对《信息安全技术个人信息安全规范》等法律中有关用户画像限制使用、组织信息安全管理要求等也应作出相应调整。

第二，促进政府对智能算法治理模式的监管升级。2022 年《互联网信息服务算法推荐管理规定》标志着我国用户画像政府治理开始并重对待个人信息治理模式与智能算法治理模式，将规制重点延伸到算法技术支持者。这是对技术风险发展的因应性制度调整。用户画像治理超越个人信息治理模式，为用户画像的每个阶段都制定规则，符合国际发展趋势。智能算法治理模式能够有效克服个人信息治理模式对用户画像的规范缺失：其一，在告知同意规则难以充分发挥功效的情况下，该模式直接将规制对象从个人信息转向用户画像的应用活动即自动化决策本身，有效防范用户画像所产生的新型风险。其二，算法程序通过比较两组相似而敏感程度不同的数据，有效避免机器学习间接使用个人敏感信息作出决策的可能，从而杜绝混合资料所造成的“个人敏感信息不当成为自动化决策的关键因素”的风险。因此，应当围绕用户画像应用的全流程来设计制度，在整体立法框架下统筹协调信息、算法的规制，将个人信息治理模式、智能算法治理模式统一纳入未来的用户画像基础性立法。不过，现有立法的一些具体措施还难以满足实践需求。例如，由于立法没有“用户标签”概念，以及“选择或删除用户标签”的具体实现路径与效果衡量缺乏明确规定，导致用户无法自主控制希望接收到的个性化内容推荐信息的标签、画像维度，用

户调控个性化内容推荐展示相关性程度的能力实际上仍十分受限。又如，当前的规制聚焦于算法机制机理、特征库、标签制度备案说明等透明性规制，缺乏围绕算法公平性的人为介入义务规制。需要在保证算法分析系统的透明化之外，探索强化算法决策结果的可责性，确保设计者、执行者和监督者彼此之间的独立性与相互制衡，避免算法决策的自我增强与自我回馈效应陷入无人察觉、难以矫正的风险。

(三) 用户画像政府治理责任的配置原则

1. 预警原则

预警原则(the precautionary principle)，即行政规制领域处理不确定风险的法律原则，是指“对具有规制所需事实的不确定性、科学实验的不确定性等风险议题，在缺乏证据证明损害的情形下应尽早实施规制”[34]。依据启动规制的门槛差异，预警原则又分为两类：一是强的预警原则，即政府在面临特定风险时，即便无法证明因果关系，也要立即采取预警措施。二是弱的预警原则，即仅仅要求政府针对程度严重且不可恢复的风险，才需要承担主动预警的义务[35]。随着人们风险认知的深化，预警原则不再限于“强调不确定性条件不得成为延缓规制的正当理由，要求尽早应对风险”的传统含义，逐渐从降低规制启动门槛的指导原则转换成审查规制程序能否有效评估、处理与应对不确定性风险的程序性要求。预警原则绝非对不确定性风险的单纯回应，而是涉及社会不同群体间如何整合评估与应对风险的决策过程，风险规制从“专家评估—行政规制—群体沟通”的线性模式转化为三者融合于同一程序的环形模式[36]。以往由特定专家独占的风险伤害几率和严重性诠释机制逐渐松动，这就为其他领域专家与普通民众参与规制标准制定、风险评估提供了契机，信息公开、正当程序、公共参与等成为风险规制的重要举措。由于不确定性风险的存在，政府对用户画像治理的责任离不开预警原则的支撑与指引。

首先，用户画像政府治理应采取弱的预警原则。只有当用户画像对公民权利、社会公共利益的潜在或者现实危险达到严重且不可恢复的程度时，政府才能启动规制。在某些利用大数据定向推送个性化服务、智能社交推荐、企业营销与运营推送活动中，用户画像的个人信息侵权、差别对待、资料独裁风险发生的盖然性较低，损害程度与范围较小，政府若是为了确保过程安全，一概要求用户画像使用者举证证明其行为的合法性，则既不符合成本效益要求，也无法达到兼顾促进发展与风险预防的效果。对于这类不具有重大风险但具备发展潜力的技术应用与产业发展，政府应当宽容对待。

其次，用户画像政府治理应当构建一套弹性健全的规制程序。社会各界对个人信息侵权、差别对待、资料独裁风险的认知经历着由浅入深的变化，预警原则提倡风险认知的社会生成过程从规制程序角度不断调整风险规制的社会属性与价值选择，促进政府更加稳健、理性地作出决策。具体的程序机制包括：一是跨领域的专家参与。用户画像为大数据、人工智能技术的使用带来规制的新挑战，凸显出风险规制带有多元利益平衡的特征，因此，规制程序应当整合各领域专业意见，提供跨领域沟通机会的参与模式，吸纳法学以外的伦理学、心理学、社会学等领域专家。二是普通民众的参与。在风险评估阶段，政府通过公众参与，可知晓社会对个人信息侵权、差别对待、资料独裁风险的认知程度，引导规制资源的有效分配[37]。在风险管理与沟通阶段，通过公众参与确保利害关系人的意见与需求被决策程序吸纳，双方在相互交换信息与意见反馈的过程中逐步确立结果，避免政策立场过度激进或者僵化。三是最坏情况分析，即将发生概率未知或者较小但是可能酿成重大损失的风险纳入事先考虑的应对范围[38]。比如，用户画像治理不宜忽略大数据杀熟、大数据黑名单效应等最坏情况的发生，法律应当预设不同主体的责任分担与应对机制。四是信息反馈机制，将最新研究进展反馈并融合于规制结构，尽量消除不确定性条件对决策的影响，确保规制措施的适时调整与优化。

2. 国家担保责任原则

国家担保责任原则，即政府委托私人参与公共任务履行时，为了避免由于履行责任的转移导

致该公共任务不能充分实现或者公私利益受到侵害，国家承担确保任务履行公平、有效、稳定的担保责任。行政法意义的担保不仅包括民法意义的排除或确保无瑕疵，还扩展到预防瑕疵的出现[39]。依据该原则，政府与私人组成公益责任共同体，彼此之间承担履行公共任务的连带责任，政府以担保者身份保证、监督、引导与调控私人实现公共目标。根据德国学者的归纳，其内涵包括三项内容[40]：一是准备责任，即政府应当预设法律框架控制公私协力可能出现的争议，如准入门槛、遴选程序等。二是监督责任，即为了维护公共管理与服务质量，政府依据公共任务的公益性强度，通过外部监督、信息披露等方式限制私人机构的自主性，抑制其自利偏差行为。三是承接责任，即为了避免私人机构对公共任务的履行出现严重负面影响，要求政府承担“补破网”的潜在履行责任。如果政府的监督管理效果不佳，则有必要终止企业运营或者强制接管。

用户画像自始就呈现“商业机构自我规制为主、政府外部规制为辅”的特征。很多商业机构采取平台自身内设治理机制的“元规制”方式，依托大数据技术运行规则、自律检核机制等加强风险防范。《国务院办公厅关于促进平台经济规范健康发展的指导意见》强调商业机构依法承担与其技术能力、掌控能力相匹配的自我规制义务，包括对平台内商户的审查登记、信息报送和采取必要措施义务。究其原因，是由于用户画像及其技术应用趋于复杂，专业性强且发展变化迅速，外部规制的贸然干预不但容易冲击大数据分析、智能算法等技术原理与发展规律，而且有悖于开放竞争的法律要求。但是，用户画像治理作为公共任务的目的在于，通过风险预防方式避免个人或者群体遭到用户画像使用者的侵权损害，尤其是智能算法带来的差别对待和资料独裁风险具有隐蔽性、扩散性，产生类似于公害的侵权效果。因此，政府仍要对商业机构履行自我规制义务的结果进行担保，促使作为被委托主体的私人展现预期的规制效能。对照国家担保责任原则，现有制度应作出以下完善：一是健全商业机构自我规制的组织与程序法律框架。在组织规范层面，政府基于公共任务需求仍应引导商业机构的人员配置与组织安排，如按照《数据安全法》设立负责数据合规的首席数据官。在程序规范层面，政府应一方面强化利益回避机制，防范商业机构由于追求私利而影响用户画像治理的结果公平性；另一方面，也要通过技术性规制标准的清晰化且合理化，提高商业机构的自我规制效能。自我规制范围应限于违法标准十分清晰且能以技术逻辑实现的内容。二是建立商业机构自我规制的接管机制。商业机构未能切实履行用户画像治理的公共任务时，政府不宜仅限于单纯的事后处罚，应当预设适当的接管条件，亲自承担该任务或者挑选其他的适格主体。

五、结语

用户画像正在重塑经济产业形态与社会治理规则，不可避免地带来了个人信息侵权、差别对待等风险，需要通过行政规制的力量来化解这些技术风险。我国初步建立了支撑用户画像政府治理的法律制度，构成政府部门的责任界限。用户画像的治理责任分配应当充分考虑发展促进与风险预防两种价值的平衡，对治理模式进行延伸迭代，协同适用“以信息主体信任为中心的个人信息治理模式”和“以算法主体责任为中心的智能算法治理模式”，并且基于预警原则和国家担保责任原则配置具体的治理责任。

注释：

① 参见《信息安全技术——个人信息安全规范》(GB/T 35273—2017)第 3.7 条规定。

参考文献：

[1] HEIDEGGER M. The question concerning technology and other essays[M]. New York: Garland Publishing, 1977: 120−123.

[2] COOPER A. The inmates are running the asylum[M]. Indianapolis:Sams Technical Publishing, 1999: 22−25.

[3] 亓丛，吴俊. 用户画像概念溯源与应用场景研究[J].

重庆交通大学学报(社会科学版), 2017,17(5): 82−87.

[4] RICH M. Machine learning, automated suspicion algorithms, and the fourth amendment[J]. University of Pennsylvania Law Review, 2015, 164: 871.

[5] MACCARTHY M. Standards of fairness for disparate impact assessment of big data algorithms[J]. Cumberland Law Review , 2017,48(4): 67−148.

[6] CHRISTIN A. Algorithms in practice: Comparing web journalism and criminal justice[J]. Big Data & Society, 2017, 4(2): 1−13.

[7] 宋美琦, 陈烨, 张瑞. 用户画像研究述评[J]. 情报科学, 2019, 37(4): 171−177.

[8] 黄文彬, 徐山川, 吴家辉, 等. 移动用户画像构建研究[J]. 现代情报, 2016, 36(10): 54−61.

[9] 张文显. 构建智能社会的法律秩序[J]. 东方法学, 2020,79(5): 4−19.

[10] 刘艳红. 公共空间运用大规模监控的法理逻辑及限度——基于个人信息有序共享之视角[J]. 法学论坛, 2020, 35(2): 5−16.

[11] 吴旭阳. 法律与人工智能的法哲学思考——以大数据深度学习为考察重点[J]. 东方法学, 2018,63(3): 18−26.

[12] 王利明. 论数据权益：以“权利束”为视角[J]. 政治与法律, 2022(7): 99−113.

[13] 吴亮. 网络中立管制的法律困境及其出路——以美国实践为视角[J]. 环球法律评论, 2015, 37(3): 127−139.

[14] NISSENBAUM H. Privacy in context: Technology, policy, and the integrity of social life[M]. California: Stanford Law Books, 2009:220−226.

[15] 汪庆华. 人工智能的法律规制路径: 一个框架性讨论[J]. 现代法学, 2019, 41(2): 54−63.

[16] 赵惟. 加快完善数据要素市场化配置[N]. 人民日报, 2021−8−2(4).

[17] 凌锋. 以数字治理助推国家治理能力现代化[N]. 法治日报, 2021−06−23(5).

[18] 韩鑫. “用户画像”, 用好更要管好[N]. 人民日报, 2020−7−17(4).

[19] 鲁鹏宇. 法政策学初探——以行政法为参照系[J]. 法商研究, 2012, 29(4): 111−118.

[20] 陈潭, 王颖. 人工智能时代政府监管的实践转向[J]. 中南大学学报(社会科学版), 2023, 29(2): 136−144.

[21] BALKIN J M. The fiduciary model of privacy[J]. Harvard Law Review, 2020,133(1): 11−33.

[22] MITTELSTADT B. From individual to group privacy in big data analytics[J]. Philosophy & Technology, 2017, 30(4): 475−494.

[23] CUSTERS B, U VRABEC H, FRIEDEWALD M. Assessing the legal and ethical impact of data reuse[J]. European Data Protection Law Review, 2019, 5(3): 317−337.

[24] 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.

[25] SIMMONS R. Big data, machine judges, and the legitimacy of the criminal justice system[J]. U.C. Davis Law Review, 2018,52(2): 1067−1068.

[26] 梅立润. 人工智能时代国家治理的算法依赖及其衍生难题[J]. 中南大学学报(社会科学版), 2022, 28(6): 123−131.

[27] DOSHI−VELEZ F, KORTZ M, BUDISH R, et al. Accountability of AI under the law: The role of explanation[J]. Electronic Journal, 2017: 1−21.

[28] BAMBAUER JANE, TAL ZARSKY. The algorithm game[J]. Notre Dame Law Review, 2018,94(1): 1−25.

[29] 崔靖梓. 算法歧视挑战下平等权保护的危机与应对[J]. 法律科学(西北政法大学学报), 2019, 37(3): 29−42.

[30] 徐琳. 人工智能推算技术中的平等权问题之探讨[J]. 法学评论, 2019, 37(3): 152−161.

[31] 吴亮. 政府数据授权运营治理的法律完善[J]. 法学论坛, 2023, 38(1): 111−121.

[32] 王旭. 论国家在宪法上的风险预防义务[J]. 法商研究, 2019, 36(5): 112−125.

[33] ZINN J. Recent developments in sociology of risk and uncertainty[J]. Historical Social Research, 2006, 31(1): 275−286.

[34] CASS R SUNSTEIN. Worst−case scenarios[M]. Massachusetts :Harvard University Press, 2009: 17−70.

[35] 黄锫. 元宇宙的行政规制路径: 一个框架性分析[J]. 中国法学, 2022(6): 175−196.

[36] BODANSKY D. Law: Scientific uncertainty and the precautionary principle[J]. Environment, 1991, 33(2): 4−44.

[37] 陈潭. 国家治理的大数据赋能：向度与限度[J]. 中南大学学报(社会科学版), 2021, 27(5): 133−143.

[38] STEPHEN TROMANS. High talk and low cunning: Putting environmental principles into legal practice[J]. Journal of Planning and Environmental law, 1995, 39(2): 779, 782.

[39] 施密特·阿斯曼. 秩序理念下的行政法体系建构[M]. 林明锵, 等译. 北京: 北京大学出版社, 2012: 163−174.

[40] CITRON D K, PASQUALE F. The scored society: Due process for automated predictions[J]. Washington Law Review, 2014, 89(1): 1−33.

[41] 陈爱娥. 国家角色变迁下之行政任务[J]. 月旦法学教室, 2003,3(1): 104−111.

[42] 杨登峰. 国家任务社会化背景下的行政法主题[J]. 法学研究, 2012, 34(4): 26−29.

On the government governance responsibility of the application of user portrait in commercial organizations

WU Liang

(School of Law, East China University of Science and Technology, Shanghai 200237, China)

Abstract: User portraits of commercial organizations are now widely used in artificial intelligence systems, intelligent forecasting, scene recognition and other aspects. The risk of personal information infringement brought by the "monitoring based" information aggregation method, the filtering bubble effect and differential treatment risk brought by algorithm decision-making, pose new challenges to the government's user profile governance. China has initially formed a policy system for the development and governance of user profiles, and the corresponding legal framework has gradually taken shape. User profile governance responsibilities include two different modes: personal information governance and intelligent algorithm governance. The government's responsibility for user profile governance should be coordinated with the value of promoting development and preventing risks within the framework of the constitutional national protection obligation. China should extend and iterate the governance model through top-level design, promote the synergy between personal information governance and intelligent algorithm governance, and use the principles of early warning and national guarantee responsibility as the allocation principles of governance responsibilities.

Key Words: user profile management; government responsibility; personal information governance; intelligent algorithm governance

[编辑：苏慧]