

# 人脸识别技术对数字个体的增权与抑制

郭森, 檀晓涓

(西北政法大学新闻传播学院, 陕西西安 710062)

**摘要:** 人脸识别技术作为生物识别技术, 是数字时代对个体信息收集使用的最新探索。在数字化社会和技术理性主导治理思维的背景下, 人脸识别被广泛应用于社会治理各个领域。人脸识别技术对生物信息的使用流程包括采集、存储、流通、应用, 在使用个体信息的过程中, 人脸识别塑造新的信息传播和应用生态, 并对数字个体的权利产生增权和抑制的双重效果。技术本身的工具性决定技术对个体的延伸, 技术对个体权利的抑制是人对技术应用和规制的不完全, 最终对技术使用进行规制和透明化处理是“技术为人”未来转变的必然。

**关键词:** 人脸识别; 数字个体; 社会权利

**中图分类号:** G206

**文献标识码:** A

**文章编号:** 2096-8418 (2021) 02-0052-07

## 一、人脸识别技术的发展溯源与应用场景

### (一) 技术沿革与研究回顾

从人脸识别技术的应用范围和层次来看, 人脸识别的信息抓取根植于图像摄影等图像抓取存储技术的成熟, 图像处理、人脸区分、深度学习等算法技术的成熟使人脸识别真正成为人与人交往能力的延伸, 人脸识别对人脸信息的云端存储使社会网络的陌生节点间实现信任基础上的交往。就技术发展层次而言, 人脸识别技术是在指纹等生物识别技术上结合图像处理技术和大数据技术对个体生物信息应用领域的拓展, 探索对个体身体数据使用的边界。

学界普遍认同人脸识别属于身份核验的生物识别技术, 通过“自动定位、跟踪采集、比对提取、分离存储”等人脸特征信息处理环节完成录入数据与人脸数据库的关联比对, 最终指向特定自然人。<sup>[1]</sup>

机器自动人脸识别研究开始于1966年PRI的Bledsoe的工作。1990年, 日本研制的人像识别机可从千人中识别特定对象。1993年, 美国国防部高级研究项目署和美国陆军研究实验室成立了Feret项目组, 建立了Feret人脸数据库, 用于评价人脸识别算法的性能。2008年, 人脸识别应用于奥运会的安防。2014年3月, 香港中文大学信息工程系系主任汤晓鸥团队发布研究成果, 基于原创的人脸识别算法准确率达到98.52%, 首次超越人眼识别能力(准确率为97.53%)。

人脸识别的学术图谱从学科侧重可以分为对人脸识别技术的改进策略、人脸识别技术的应用策略, 以及人脸识别技术的规制策略。对人脸识别技术的改进策略的探讨集中在研发技术层面, 主要包括对面部信息的抓取和分析。对人脸信息的分析过程经历了从单一个体的表情分析到多元数据关联下身份识别的转变, 而对人脸信息处理也经历了从2D时代的图像处理到3D时代的深度学习和场景优化。在人脸识别的应用策略层面, 主要是各行业从业者对人脸识别应用可能性、有效性和使用优势进行论证。人脸识别的规制策略则立足于人脸识别在社会各领域的广泛应用以及与此相关的社会侵权现象, 探讨

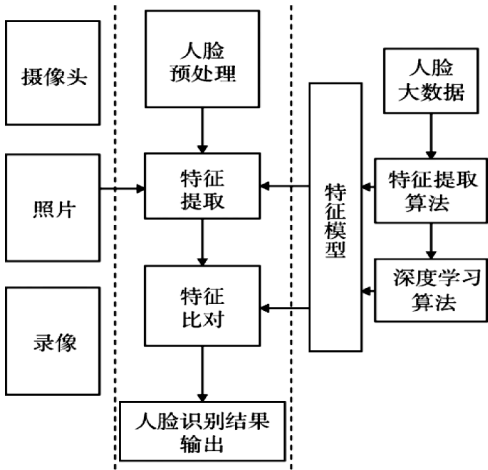
**基金项目:** 国家社科基金重大项目“国家关键信息基础设施系统安全协同防护体系研究”(19ZDA127); 陕西省社科界重大理论与现实问题研究项目“预警视角下移动社交平台生态环境焦虑与知情权研究”(20FX—51)。

**作者简介:** 郭森, 女, 副教授, 硕士生导师, 博士后; 檀晓涓, 女, 硕士研究生。

相关法律和社会规制措施。

(二) 技术逻辑和应用场景

人脸识别系统的运作模式主要通过既有人像信息的采集，集合对人脸信息的图像分析和相关算法技术，对人脸进行自然人相关的身份核验。人脸识别的具体技术使用包括使用端和管理端两个层次。客户端主要是建立起人脸检测调用和抓取的数据平台，管理端则是通过建立起一系列与人脸数据相关的存储、识别极端、通信、管理模块，通过调用人脸识别计算单元进行人脸特征提取比对，提供人脸识别能力。<sup>[2]</sup>从根本上来讲，人脸识别就是技术对人眼识别的模仿、替代和超越。



人脸识别系统结构<sup>[3]</sup>

当前人脸识别主要包括“1 对 1”“1 对 N”两种识别模式。前者是为了验证“A 是否是真的 A”，即人脸数据简单比对的身份核验，与其他身份信息关联小，如手机的人脸识别开锁。后者则是为了验证“A 到底是谁”，通过大量人脸数据录入，通过深度学习完成自然人的定位和身份信息的关联对比，“排他性”地解释“A 究竟是谁”。<sup>[3]</sup>

现代理性主义视角下，技术理性成为人类社会中根植于日常的潜在逻辑，人脸识别成为基于各方利益驱动的综合性的日常行为。基于现有生物识别应用基础上的技术逻辑，包括教育（智慧教室）、职场（数字后勤）、社会管理（平安社会、疫情防控、社区管理）、社会服务（养老）等领域都对人脸识别的应用场景有所探索。人脸识别现实应用范围不断拓展，南都人工智能伦理课题组发布的《人脸识别应用公众调研报告（2020）》显示，在两万名线上受访者中，94.07%的受访者使用过人脸识别技术，报告指出该技术在支付转账、开户销户、实名登记、解锁解密、换脸娱乐、政府办事、交通安检、门禁考勤、校园/在线教育、公共安全监管等领域带来高效便捷的体验。

(三) 技术的适用动因

生物识别技术从指纹向人脸的演进是人通过技术对自身感官的适应。亚里士多德认为视觉最能让我们认识事物，也最能解释事物之间的许多差异。人对视觉的依赖使人脸信息成为社会交往中的重要媒介和直观认知，也使人脸识别技术得到迅速广泛应用。

就使用人脸识别技术的最微粒个体而言，人脸识别是最为直观并且可接受的信息采集方式，人脸信息和身体的紧密依附也使人脸使用更为便捷。而人对自身的探索和自我传播中外界认知的影响使个体趋向于在互联网进行与人脸相面相关的一系列互联网娱乐活动。

就平台选择而言，人脸识别在摄像头普及的社会环境中接近性高，基于既有基础设施进行的人脸识别投入和更新成本低。同时，与单一生物识别技术相比，人脸信息普适性、可采集性与被采集者的

可接受性较高,具有方便友好、易于接受、不易伪造等一系列优点。

就社会治理而言,人脸识别的场景化使用具有长距离、无接触、轻干扰、高精准的特征,“人脸毋庸置疑地成为陌生人社会框架下信赖重构的重要工具”。<sup>[1]</sup>人脸识别的无接触和隐蔽性符合社会治理过程中治理主体和客体保持一定距离的实际需要,同时也在特殊情况,如新冠疫情中,满足无接触的管理需求。

## 二、人脸识别技术赋能数字个体

技术对个体的数字化延伸本质是对个体能力的延伸,人脸识别技术在数字城邦社会中构建起一套以面部信息为语言的交流系统,将陌生的社会成员以技术联结,人脸识别终端成为数字个体与社会连接的外在器官。同时,人脸识别技术的验证能力作为社会神经系统的一部分,促使整个社会的生产效率提升,对数字弱势群体使用能力的延伸补足,为数字社会发展的短板提供必要的技术网络支撑。这种赋能前景的基础在于技术的普及和系统被整体社会成员的全面接入,以及社会对信息的收集、流通、存储、应用环节的透明可控。

### (一) 信息获取的数据联动

缺少视觉体系的数据具身是不成熟的后人类主体,个体的生物识别信息是数字世界中后人类主体虚拟具身的拼图。人脸识别技术实质上是对现有图像采集技术和图像数据库的资源再利用,在信息采集的数据联动中,放大人脸信息的价值,使以人脸为代表的个人生物信息成为延展个体能力和社会联系的重要接口。在人脸识别技术广泛应用之前,人脸信息数据库已有一定的基础。人脸信息作为日常和档案认证记录被广泛采集,而摄像头等图像采集抓取设备的普及使人脸信息的抓取更为便捷。人脸识别技术完善了既有人脸信息与其他信息相关联的信息链,构建起数据联动网络,使数字个体在虚拟世界里的数字具身基本完善,赛博格化的“物质—信息混合物的后人类主体”<sup>[4]</sup>基本成型。

### (二) 信息存储的数字记忆

人脸信息在互联网云端的存储使个人起居注式的互联网记忆有具体视觉呈现。人脸采集真正完成数字个体的构建,而数字存储使这种数据具身成为真正的数字记忆并得以在互联网社会中存留痕迹。人脸信息数字存储和智能识别使个体记忆被网络刻录,在个体记忆之外成为数字生成的回忆,如百度网盘基于人脸识别生成数字故事相册,个体的历史被记录和梳理,个体的存在于数字化存储中真正彰显,个体价值在数字记忆的可靠存储中不断放大,数字记忆超越时间的束缚,在历史发展中记忆个体的发展和立体的“自我”。

### (三) 信息流通的社会神经

在信息关联基础上,人脸数据流通的社会神经系统构建起视觉感官下的信任系统。个体生命数字化并将数据身体上载的生命治理过程中,传统社会中阶层的区隔标准变化,每个个体都成为数据化的个体而消解了现实社会中由于阶层、经济、学历、民族等方面的差异,深度数据化的数据身体作为网络社会有机体的“细胞”,与其他数据生命和社会大系统相连接,通过算法构建社会“神经网络”。

### (四) 信息应用的个体扶助

在个体的具体使用层面,传统数字技术的使用往往需要一套复杂的使用机制,如数字支付过程的绑卡、扫码,各种社会保障 APP 的验证码、登录码,智慧门禁中的密码输入,火车出行的实名认证等等。人脸识别简化传统数字技术使用的复杂程序,在已经接入人脸识别技术的前提下,成为拓展人类能力范围的辅助性工具。人脸识别只靠“刷脸”就能完成以往需要多层级完成的数字技术使用,方便高效的使用体验在一定程度上降低了数字弱势群体的使用倦怠,通过面部信息云数据系统构建的信任体系,人脸识别使人际交往重归以关系联结的信任社会,整个社会变为人人“相识”的“桃花源”。对

使用能力欠缺的数字弱势群体而言,通过弥合使用沟的差距,理念中的资格平等在技术扶持下有转向能力平等的可能,人脸识别技术辅助数字弱势群体更便捷地接入数字社会。

### 三、技术赋能后的权利抑制

人脸识别技术的抓取边界、应用边界、流通边界、存储边界目前还没有明晰的界定,与之相适应的法律法规尚不完善。边界的混乱导致人脸数据信息和人脸识别技术被滥用,使得算法黑箱之下数字主体的部分权利被动让渡,成为新型的数字弱势群体。

#### (一) 采集层面的隐私侵犯

当前人脸信息采集和抓取行为尚未被重视,人脸信息的接近性和易得性使人脸识别的隐私信息被侵犯。首先,当前涉及人脸识别的产业采集规范尚未形成。人脸识别第一案中,郭兵的人脸信息在未经同意的情况下就被强制采用,房地产销售中也会采用“戴口罩也能识别的人脸识别系统”。其次,人脸信息的重要性和敏感性还未被足够重视,人脸信息抓下的算法黑箱使人脸识别技术被泛滥应用在对主体身份识别、需求分析等商业统筹乃至日常出行等领域。再次,技术主体与责任主体分散多元、无法准确界定。“个人私密信息和公共信息之间的界限实际上模糊不清,没有办法事先划定好边界或者计算‘比例’。个人信息实际上是社会整体信息的一部分,有时可能流向公共机关,成为公共数据进行披露使用,也可能流向私人领域,以隐私名义进行保护,其并不完全隶属于信息主体。”<sup>[5]</sup>从此,人脸识别摄像头无处不在,“1对1”人脸识别场景下的采集信息可能被应用于“1对N”。同时,人脸信息收集应用的强制性同意和隐蔽性收集处于主体无意识进而拒绝无力的尴尬境地。最后,由于人脸信息采集的早期习惯,人们对人脸采集的警惕性不足。在《人脸识别应用公众调研报告(2020)》中,30.86%受访者已经因为自己的人脸信息泄露、滥用等遭受损失或隐私被侵犯。随着人脸信息的隐私化,数字社会的主体在深度数据化过程中将会进一步进入算法黑箱的计算范畴,被技术控制甚至操纵。

#### (二) 存储层面的资本霸权

在信息存储层面,数据垄断造就资本主导的数字利维坦,技术背后的资本逻辑形成群体性的权利侵害。资本追求利益最大化使其在操纵技术过程中有意识进行带有明显算法偏见的筛选,数据造假和故意进行算法程序过滤都是资本驱动下的技术行为,没有消费能力以及对技术没有使用能力的“数字新穷人”将在算法的过滤中逐渐被边缘化,人被资本物化最终失去存在的价值和主体性。人脸数据这一核心资源的统筹和使用被互联网独角兽公司所掌控,将带来更大限度上资本对弱者的价值剥削,当可以影响政治生态的算法完全且不受监管地由网络科技公司掌控,追求最大利益的目标刺激超越了政治利益与企业社会责任,将对公民权利、政治生态造成极大伤害,最终弱者愈弱,数字个体的权利消弭于无。

同时,社会存储的数字记忆会侵害个体的被遗忘权。资本霸权下,社会存储能力的扩张与不完善的存储规范不相匹配,技术接近性和易得性与使用的规范性不匹配,最终使数字个体的权利受到侵害。

#### (三) 流通层面的技术理性

数字具身拼图的完善使社会观念中个体被物化成为数据存在,对个体信息的重视不够使个体成为物化的数字个体,数字具身不是个体代表,而是冰冷数据。

技术型治理的生命政治将对个体生命的认知异化为数字和人口。在生命政治的视角下,技术在生命治理中的权力“把整个国家所有单独的个体整合成一个抽象的庞大的人口来对待。”<sup>[6]</sup>个体作为社会有机体的部分成为政治必然干预的组成部分,个体的主体性被人类意义的宏观价值所掩盖,生命不仅是“让人生活更好”的政治口号对象,更是物化个体生命情况下要使人类更好地繁衍下去的政治行为。波斯曼认为,“人类技术的发展可分为工具运用、技术统治和技术垄断三个阶段。科学带来的不是幸福



而是灾难，不是自由而是控制，不是开放而是封闭”。被监控的个体生命成为“监控式国家”的表征，“监控式国家较以往任何时候都能更强也更易于掌控各类信息，千万别低估其风险。当然，更值得警惕的是权力将资本与技术一并收入‘帐下’而实现的全能主义统治”<sup>[6]</sup>。

#### （四）应用层面的匹配困境

在具体应用层面，已经出现瘫痪老人被抱着在柜台进行人脸识别的极端个案，也存在低收入人群没有相关终端而产生人脸识别应用障碍。个体能力的差别、技术的广泛使用和使用界面不匹配情形下会出现技术排斥和偏见、使用倦怠、技术遮蔽等。

技术与现有社会认知的不匹配造成规制的缺失与技术错漏。如果忽视数字弱势群体的技术使用能力，片面强调秩序唯美主义下的技术治理，结果将是使个人更加透明，工具理性下个体的意愿与选择被忽视，数字弱势群体在社会治理过程中被无意识边缘化，会加剧社会资源分配的不均衡，难以共享技术发展的红利。同时，社会信任系统的背面是技术主导的社会偏见和对边缘群体的遮蔽，人脸识别在算法验证过程中对原始数据库的偏见复制导致边缘化群体选择性失明和结构性偏见复制，作为技术掌控者的资本方和算法程序编写者在程序设计中的偏见循环，会进一步影响权重调节和刻意偏见，算法本身在人机互动中的偏见习得。<sup>[7]</sup>

人脸识别技术认识和编码的不完善使人脸识别的错误率依旧存在错误可能，对个体的财产名誉相关权利造成损害，深度伪造的生成对抗机制更与人脸识别形成“矛盾相击”的复杂局面。小学生使用打印的人脸图片可以打开快递柜，手机刷脸开机也能在睡梦中被窃取隐私信息……人脸信息具有整体性和敏感性，一旦泄露和误用损失难以估量。目前，这类问题主要集中在人脸信息与财产相关的应用领域，如公共交通、物流和支付领域，而随着人脸识别技术的广泛应用，人脸信息与数字身体的所有信息全面关联后，在技术理性和量化计算对现实的“理想化建构”下，人脸识别的技术错误会带来更为严重的后果。如在司法层面，法庭审判如果采用了人脸识别的错误报告，或者基于人脸识别的数据信息产生偏见，那么有可能造成“事实认定错误及司法不公，尤其是‘假阳性’错误可能将无罪之人认定为有罪”<sup>[8]</sup>。

## 四、人脸识别技术增权的优化可能

人脸识别技术通过技术手段将人脸数据化，在人脸信息的抓取和上传中建立人脸大数据库。由于人脸信息在应用过程中与财产、隐私等其他个人权益产生强关联，其重要性越发凸显。人脸识别普及过程中的信息采集、存储、流通和应用的保护和认知不足，对识别后数据使用的规制不力，都带来人脸识别技术缺陷对数字个体的权利侵害。

个人信息和隐私保护是宪法规定下个体天赋权利，在“数据即人”向“数据为人”的算法逻辑转型中，个体的数字具身是数字虚拟世界的权利主体，身体与技术的同源、同构关系下，对数字具身的保护是数字社会的基本共识和运行底线。数据收集的采集、存储和流通边界模糊，个人私密信息和公共信息之间的界限实际上模糊不清，没有办法事先划定好边界或者计算“比例”。资本主导下数据信息的采集不会带来个体的延伸和增权，导致更大程度上资本对弱者的价值剥削，可以影响政治生态的算法完全且不受监管地由网络科技公司掌控，追求最大利益的冲动超越政治利益与企业社会责任，数字个体自身的媒介素养不足加剧技术霸权的可能，技术背后资本的控制加剧数字个体在数字异化中逐步丧失主体地位，最终弱者愈弱。人脸识别成为数据科学家凯茜·奥尼尔所称的“数学破坏的武器”。技术霸权可能会覆盖每一个数字公民，即每一个数字社会公民都可能成为“数字弱势群体”。

纵观人类技术发展史，新技术的出现和发展总是会带来恐慌和悲观情绪，但是，技术是被人所创造所掌控的人的器官的外延，这种器官还在不断地自我完善和更新以适应人类的发展需求。要利用人脸

识别,最大限度地为人类服务并实现技术对个体的增权可能,就要最大程度上发挥技术的工具性,并增强技术的可控性。在产品设计、技术规制、个体素养、政策关怀和制度规制几个层次下,从技术和人的关系出发对技术本身和操纵技术的人进行规制和约束。

### (一) 人性化趋势的产品设计

技术本身的设计初衷和定位是从人本身出发进行规制,人在技术发展过程中有意识地使技术趋向“人性化”。有学者认为,“未来的社交产品开发,需要考虑更开放、更适合公共交流的机制设计”<sup>[9]</sup>。人工智能主导的人脸识别技术可以大幅度提升人类的认知能力和实践能力,社会数据网络中数字化的个体成为未来人类发展的新景观。同时,后人类主体确为人类社会向更高水平发展提供了契机,尤其是对于人脸识别对社会交流系统的更新可能对人类社群中的弱势群体加以扶助。

同时,技术也在被受众隐性形塑。“媒介受众是主动且批判的;以不同方式对传播作出反应;并且受众主动性源于由其所属的社会网络支持的先验信念与态度。”<sup>[10]</sup>大数据时代的数据收集带来“受众涵化媒介”的转变,受众参与到网络虚拟环境的构建,媒介内容根据受众需求的反馈而进行调整。网络媒介极大地满足了不同时空受众的个性与需求,特别是数字弱者作为技术使用的蓝海和政策发展的方向,对技术进行积极的反向塑造。

通过人在技术发展过程中有意识的调适,使技术趋向“人性化”。在以人为本、注重公共适用性的前提下,人脸识别技术需兼顾公共性与商业性才有更广的发展前景。

### (二) 技术设计的产品规制

就人脸识别侵犯个人信息隐私权和财产权的担忧而言,在采集、存储、流通、应用全过程以技术升级和技术嵌入抵消可能的权利抑制。用算法完善算法是最基本的技术规制方法,通过在编码过程中对人脸识别技术应用场景等进行规范条件的设置,算法本身实现自我限制和自我监控的功能,尽可能减少对个人隐私信息的无理窥探。此外,通过区块链等技术的应用,利用区块链对数字对象的唯一性、无法复制、不可篡改等特性,在数据链实现可行的数字化,实现透明、多方信任且有路径可查的信息流通存储协议,优化人脸识别数据库构建,通过使用技术对人脸识别技术加以规制,可以进一步挖掘人脸识别的潜在应用和适用领域。

### (三) 社会个体使用素养升级

人脸识别技术的广泛使用对技术的开发者、使用者以及影响人群的素养都提出了新的要求。为了避免数字弱势群体的知识性不足,应当对数字时代个体进行媒介素养的培养,在技术理性之外培养对技术的批判精神和怀疑精神,始终保持对自身权利的高度重视。此外,对技术提供者 and 使用者而言,树立起对个体隐私信息的尊重和敏感性,充分尊重隐私信息提供者的个人意愿。在实践中遵循最低限度原则,能不收集的信息就不收集,能少收集的信息就少收集;高门槛准入原则,即对于涉及个人信息收集的业务开展必须有严格的准入制度,对于个人信息的储存、数据安全和业务必要性进行严格审核;相关利益者知情原则;社会许可原则;事后补救原则;目的和结果一致性原则;明确的责任承担原则以及信息严格设定使用和保存时限原则。<sup>[11]</sup>通过完善行业规范和行业伦理,在相关行业中树立起相应的道德遵循,提升从业者技术开发和使用的道德标准。

### (四) 政策法规的社会规制

威廉斯认为,每一个社会发明都是提升生产力这一初始意向,而社会各要素会影响技术的使用情况。真正的决定是社会过程,要通过社会各要素对技术不断地修正使之不断向人性化趋势发展。

在顶层设计角度,人脸识别技术的规制一方面有赖于技术提供方的资本提供与策略设计,对技术使用方的具体使用方向进行规制,更重要的是通过对技术的立法进行边界限定。关键在于对技术背后的操纵者进行规制,面对当前人脸识别技术法律规制缺失的情况,应延展宪法规定的基本人格权的概

念，从实体法和程序法的双重层面全面构建权利保障机制。如在郭兵诉杭州动物园的“人脸识别第一案”尝试中，通过诉讼将个人人脸信息保护带入立法规制讨论中。需要通过立法确立起数字人权的理念，完善人脸识别的应用领域和信息使用范围，强制对算法黑箱过程保持公开是对作为隐私信息提供者的数字弱势群体的负责，还要明确技术使用和侵权行为的责任主体，使技术提供者有方向、有克制、有界限，规避“赢者通吃”的庞大商业生态圈，让技术、资本、社会权力真正在牢笼中办事，完成法律遏制强者剥削弱者的使命，为数字弱势群体的权利保护提供制度支持和方向引导。

#### 参考文献：

- [1] 赵精武.《民法典》视野下人脸识别信息的权益归属与保护路径 [J]. 北京航空航天大学学报 (社会科学版), 2020 (5): 21-29.
- [2] 刘婧雯, 郭漫雪. 生物识别技术在金融行业的应用研究 [A]. 中国通信学会无线及移动通信委员会. 2017 全国无线及移动通信学术大会论文集 [C]. 中国通信学会无线及移动通信委员会: 中国通信学会, 2017: 4.
- [3] 工宇. 生物识别与隐私权保护之法律冲突及其协调 [J]. 科技与法律, 2009 (6): 25-28.
- [4] 彭兰. 人一机文明: 充满“不确定小生”的新文明 [J]. 探索与争鸣, 2020 (6): 18-20.
- [5] 胡凌. 个人私密信息如何转化为公共信息 [J]. 探索与争鸣, 2020 (11): 27-29.
- [6] 肖唐镖. 中国技术型治理的形成及其风险 [J]. 学海, 2020 (2): 76-82.
- [7] 郭小平, 秦艺轩. 解构智能传播的数据神话: 算法偏见的成因与风险治理路径 [J]. 现代传播 (中国传媒大学学报), 2019 (9): 19-24.
- [8] 汝绪华. 算法政治: 风险、发生逻辑与治理 [J]. 厦门大学学报 (哲学社会科学版), 2018 (6): 27-38.
- [9] 彭兰. “液态”“半液态”“气态”: 网络共同体的“三态” [J]. 国际新闻界, 2020 (10): 31-47.
- [10] 展宁. 伊莱休·卡茨与大众传播研究: 半个多世纪的学术演变 [J]. 新闻与传播研究, 2020 (10): 5-22, 126.
- [11] 王俊秀. 数字社会中的隐私重塑——以“人脸识别”为例 [J]. 探索与争鸣, 2020 (2): 86-90, 159.

[责任编辑: 华晓红]