机器学习的法律审视

陶　盈

(首都经济贸易大学法学院　北京　100070)

内容提要: 机器学习是计算机程序通过学习数据,生成能够进行判断和推论的算法,从而模拟人类智能活动,改善系统自身性能。机器学习的应用为社会发展带来了机遇,也为法制改革注入了活力。但是,技术先行对法律规范的挑战也不容忽视,尤其表现在安全、伦理和隐私方面。对于算法的决策失误导致的安全危险和损害责任,构成设计缺陷的,适用产品责任相关规定。对于算法设计上的伦理困境、道德失范应当加强法律防范,尊重被侵权人的知情权、选择权、自我决定权等。对于机器学习过程中收集利用个人信息带来的隐私权忧虑,应当明确合理利用与侵害个人信息权、隐私权的法律边界。

关键词: 人工智能　机器学习　算法黑箱　隐私权　个人信息权

DOI:10.16092/j.cnki.1001-618x.2018.09.006

随着人工智能技术席卷全球,机器学习成为炙手可热的话题,并被视为人工智能领域发展最快、最能够体现智能的一个分支。机器学习(Machine Learning)是人工智能技术的核心,其主要研究计算机怎样模拟或实现人类的学习行为,以获取新的知识或技能,重新组织已有的知识结构使之不断改善自身的性能。[①]简单来说,机器学习就是基于数据构建模型,以计算的手段模拟人类智能活动,从而不断利用经验改善系统自身性能。由于经验通常以数据形式存在,把经验数据提供给计算机并从中产生"模型"(model)的算法就是"学习算法",而机器学习研究的就是"学习算法"(Learning algorithm)。[②]以经典的西瓜问题为例,当机器面对一个新情况时——看到一个没有打开的西瓜,模型就会基于设计者收集并输入的经验数据——色泽青绿、根蒂蜷缩、敲声闷浊提供相应的判断——是个好瓜。

大数据时代的出现为机器学习提供了更大的空间,海量的数据被用以收集、分析和预测。现实生活中人们在搜索引擎中输入关键词搜寻相应内容的过程就应用了机器学习的技术,搜索到的结果正是计算机对无数人搜索的关键词进行统计后筛选出的最可能被需要的目标信

作者简介: 陶　盈(1985—),女,汉族,山东济南人,首都经济贸易大学法学院讲师。

本文为国家社会科学基金青年项目"新形势下个人生活信息的法律保护研究"(项目编号: 16CFX043)的阶段性研究成果。

① 中国电子技术标准化研究院《人工智能标准化白皮书(2018 年版)》

② 参考周志华《机器学习》,清华大学出版社 2016 年版,第 1~2 页。

息，而这一过程本身也被机器学习，被充实到拥有海量信息的数据库中。近年来，机器学习算法在机器视觉和语音识别等领域有了飞跃性发展，识别准确性大幅提升。相对于人类有限的认知能力，机器学习的能力是无限的，程序在不断地自我设定目标，实现成长进化，于是机器通过学习具备了超越设计者本人的智能，也具备了在各个领域战胜人类的实力。其不但可以识别人脸、文字、语音、场景，还可以理解语义、自主创作，甚至战胜围棋大师、预测用户喜好、猜中中奖彩票、选择优质股票等，引发了学术界、产业界的热切追捧。

一、机器学习的兴起带来的法制机遇与挑战

机器学习技术也被广泛应用于建设“智慧法院”“智慧检院”等领域，成为实现智能裁判的重要手段。机器学习会通过各种大数据、身份虚拟账户、评分系统、智能算法的技术装置帮助，形成对法律主体持续追踪认知、认证、评价、识别和反馈的学习性网络。[③] 目前，各地法院争相引入大数据审判辅助体系、裁判文书智能辅助系统等，借助大数据分析技术，由人工智能进行相关演练和操作，为法官裁判案件提供智力支撑。虽然目前距离机器替代法官断案还有很长的路，但由机器助力法官审判已经成为现实。

科技的发展正在为法治进步带来前所未有的机遇，也为司法改革注入强大的活力。不过，技术先行给现有法律规范带来的挑战也已经显现，围绕机器学习的法律课题较为集中地表现在以下方面：

第一，机器学习对人类的最大威胁表现在安全、伦理和隐私三个方面，也带来了机器歧视人类、赶超人类甚至控制人类的恐慌。伴随而来的法律课题主要是因机器学习算法的决策失误致损时的侵权责任问题、对算法本身存在的伦理困境和道德失范的法律防范问题，以及机器学习过程中对个人信息的收集和利用引发的侵害个人信息权、隐私权问题。对于这三个问题，后文将做详细探讨。

第二，机器学习算法的不透明性挑战了法律的可预测性和确定性。从输入数据到产生模型，计算机基于对经验数据的自动学习生成了高级的认知结果，这种机器学习的过程是不透明的，也被称为“算法黑箱”。在司法大数据推进过程中，机器的深度学习与法律的“深度不学习”形成了鲜明对比。[④] 其原因在于法律的核心功能是维护社会规范性期望的稳定，这种规范影响社会成员的行为预期，因此法律规范要保持确定性、持续性、稳定性和可预期性。而机器的深度学习要求机器时刻保持对外界信息的应对，灵活迅速地调整其行为规范。因此，对于机器学习算法及其结果运用的公开性、透明性和公正性问题，需要通过法律制度予以及时关注和回应，避免运用智能算法侵害他人权利。[⑤]

第三，机器学习算法的法律性质和学习成果的权利归属带来了围绕新型民事权利客体的争议。机器学习的不透明性既源于一般公众缺乏专业知识无法理解算法的推演过程，也源于科技企业为保护商业秘密不愿意公布算法的推演过程。算法的性质是物还是发明？亦或是著作物？对此存在认识上的模糊。总的来看，机器学习的过程中会将数据或数据集合体加工成适合学习的训练数据，会对数据进行选择和体系化建构形成特定的学习算法。机器学习所运用的技术如果存在创造性，应当通过知识产权予以保护，如果构成商业秘密，应当受到专利权保护。无论是机器学习的过程还是成果，都应

③ 余成峰《法律的“死亡”：人工智能时代的法律功能危机》，载《华东政法大学学报》2018年第2期，第8页。
④ 余成峰《法律的“死亡”：人工智能时代的法律功能危机》，载《华东政法大学学报》2018年第2期，第5页。
⑤ 王利明《人工智能时代提出的法学新课题》，载《中国法律评论》2018年第2期卷首语。

当作为新型民事权利客体在未来民法典立法过程中得到充分重视。

第四,技术创新领域集中暴露了立法的滞后性,机器学习的相关立法工作任重道远。目前该领域较为先进的立法当属 2018 年 5 月 25 日生效的欧盟《数据保护通用条例》(GDPR),该法将个人敏感数据排除在人工智能的自动化决定之外,增加了数据使用者在个人数据收集时的透明度要求,并要求所有算法解释其输出原理。对此,有学者指出该法规定了自动决策的可解释权:数据主体有权要求算法自动决策给出解释,有权在对算法决策不满意时选择退出。[⑥] 还有学者担心这意味着深度学习将成为非法的方式。[⑦] 针对此类担心,2017 年 10 月欧盟立法工作组做出了澄清:关于自动决策,数据控制者并不必然要解释复杂的算法,对于用户,只需要用尽可能简单的方法告知其背后的基本逻辑或者标准即可。[⑧]

我国关于人工智能和机器学习的立法起步较晚,但近两年追赶速度明显加快。2017 年出台了《新一代人工智能发展规划》《促进新一代人工智能产业发展三年行动计划(2018-2020 年)》等政策文件,鼓励人工智能产业的发展。2018 年 1 月,国家不但出台了首个国家标准《信息安全技术个人信息安全规范》,中国电子技术标准化研究院还出台了《人工智能标准化白皮书(2018 年版)》。在《信息安全技术个人信息安全规范》第 7.10 条"约束信息系统自动决策"中规定了"当仅依据信息系统的自动决策而做出显著影响个人信息主体权益的决定时,个人信息控制者应向个人信息主体提供申诉方法",虽然这一规定保障了信息主体事后申诉的程序性权利,但目前整体上仍然缺乏对基于机器学习做出自动化决策的实质性约束。较之日新月异的科技变革,配套法律制度亟待完善,虽然人类本着便利优先的原则正在大规模地研究和应用机器学习,但也有必要以法律的视角认真审视机器学习带来的法律规则挑战和法律制度重建。

二、机器学习算法决策失误导致的侵权责任

目前,机器学习多被应用于存在规律却难以通过制定规则加以解决的问题上,比如其在对图像的理解和识别上发挥了重要作用。以人脸识别技术为例,辨识出一张面孔无法通过穷尽规则来完成,但是当把所有训练数据"喂给"机器学习算法后,大量的历史数据中隐藏的规律会通过机器分析进行总结并作出判断和预测。机器学习的现实应用非常广泛,例如,自动驾驶车辆依靠机器学习识别与理解街景,无人机驾驶依靠机器学习判断着陆点,可穿戴式设备(如智能手环、带传感器的跑鞋、老年人佩戴的心率传感器等)依靠机器学习监测并预测使用者的行为活动等。

由于机器学习是让计算机通过数据训练形成用以判断和推论的算法,在此过程中,因计算机系统的错误认识导致的行为偏差和由此造成的侵权责任难以避免。在如何规避防范算法的决策失误带来的风险、明确其法律后果和责任分担规则方面,亟待法律发挥更大的指引作用。仍以应用了机器学习技术的人脸识别系统为例,尽管其大大提升了侦查效率和破案概率,但也不能完全避免失误。据报道,在美国,每周超过 1,000 人被机场使用的算法错误地标记为恐

⑥ 王融《〈欧盟数据保护通用条例〉:十个误解与争议》,http://www.sohu.com/a/230057657_117965,访问日期:2018 年 5 月 2 日。

⑦ 许可《人工智能的算法黑箱与数据正义》,载《社会科学报》2018 年 3 月 29 日第 6 版。

⑧ 王融《〈欧盟数据保护通用条例〉:十个误解与争议》,http://www.sohu.com/a/230057657_117965,访问日期:2018 年 5 月 2 日。

怖分子,也有民众因联邦调查局的反恐识别系统误认而被吊销驾驶执照。[⑨]

机器学习过程中,基于错误认识出现决策失误并造成现实损害的事例日益涌现,尤以自动驾驶车辆交通事故最为引人注目。2016 年 5 月,美国佛罗里达州发生了一起特斯拉电动车在自动驾驶模式下冲撞前车致驾驶人死亡的交通事故。据特斯拉公司称是由于阳光照射拖挂车白色面板造成强烈的反光以及拖挂车的底盘较高,自动驾驶系统没有识别出道路前方存在拖挂车。[⑩] 2018 年 3 月发生的首例自动驾驶车辆冲撞行人致死案的初步调查结果也显示,涉事 Uber 自动驾驶车辆虽然成功地识别到路上的行人,但决策系统判断前方障碍未触及系统下限故决定予以忽略,导致车辆未采取躲避措施。[⑪]

机器学习的认识错误不同于驾驶人未尽安全注意义务的主观过失,本质上应当说是由于产品设计上的过失导致车辆性能存在缺陷。这种缺陷体现在系统未能识别出前方障碍物,或者虽然识别出但并没有及时采取避让措施等。在这一问题上存在两个主要争议:一是关于缺陷的判定标准。结合《产品质量法》第 46 条的定义,缺陷是指产品存在"不合理的危险",因此需要考察车辆是否在投入流通时存在结构缺陷、性能不足和警示说明不充分等问题。二是关于是否适用发展风险抗辩原则。以自动驾驶车辆为例,对于现阶段无法发现的产品设计缺陷应当适用发展风险抗辩原则。此外,随着机器自主学习能力的提升,其擅自修改程序等造成损害的情形是程序设计者在设计之初难以预见的,如果将其定义为设计缺陷将极大地阻碍技术进步,故也可以有条件地适用发展风险抗辩原则,坚持以可责难性评价为前提。

自动驾驶车辆交通事故责任兼有道路交通事故责任和产品责任的属性,因此基本上可以通过现有《道路交通安全法》和《侵权责任法》的相关规则加以解决。在尚未实现完全自动化阶段,对于驾驶人责任实行过错推定,只有驾驶人能证明损害的发生是由于车辆存在缺陷,且该损害无法避免时,才能免除自身责任,适用产品责任。若事故完全是由产品缺陷(包括车辆设计缺陷、制造缺陷和警示说明缺陷等)造成的,则由车辆生产者、设计者、销售者等依照产品责任的相关规定承担责任。

从目前发生的自动驾驶车辆交通事故的处理结果来看,多数情况下是驾驶人因违反路况监视义务、紧急制动义务的过失而负主要责任,汽车制造商并未因自动驾驶系统设计上的瑕疵或者警示说明义务上的瑕疵而承担产品责任。这种损害赔偿责任的分配方式虽然备受质疑,但应当说是与目前自动驾驶级别较低、系统仅承担辅助驾驶功能的现状相符的。随着自动驾驶级别的提高,事故责任主体必将实现从驾驶人一方到人工智能系统一方的过渡,而自动驾驶车辆的生产者、销售者、软件开发者、数据提供者、网络服务平台提供者等都有可能基于过错承担损害赔偿责任。同样的规则也适用于无人机交通事故的责任认定。

此外,因可穿戴设备检测失灵和预测错误导致的侵权责任问题同样应当受到重视。目前市场上的可穿戴式检测设备五花八门,包括运动监测腕带、监测老年人生命体征的智能手环、非侵入式血糖监测设备等。制造商们往往通过

⑨ 许可《人工智能的算法黑箱与数据正义》,载《社会科学报》2018 年 3 月 29 日第 6 版。

⑩ 刘洋《特斯拉官方回应 Model S 自动驾驶致死事故》,http://www.sohu.com/a/100682811_115428,访问日期:2018 年 6 月 6 日。

⑪ 《Uber 自动驾驶致死案调查结果:已识别行人 决策系统予以忽略》,http://auto.qq.com/a/20180509/015800.htm,访问日期:2018 年 6 月 6 日。

各种营销手段大力宣传其设备采用精准的算法,配有先进的传感器,具有较高的准确性,甚至能够起到预测疾病发生的作用。如果因设备检测失灵和预测错误导致用户延误治疗、错误治疗等,设备的生产者、销售者、软件开发者、数据提供者、网络服务平台提供者等是否也应当对因此造成的损害承担侵权责任有待学界深入探讨。笔者认为可以基于设备提供者与用户之间的服务协议,并区分商业性利用和公益性利用目的,认定设备生产者、销售者、提供者等承担与过错程度和原因力大小相应的责任。

三、对算法的伦理困境、道德失范的法律防范

(一)机器学习算法导致的伦理困境

围绕人工智能和机器学习的伦理思考虽然目前并没有形成清晰认识和统一标准,但已经在世界范围内获得了积极响应。机器通过对经验数据的学习能够模拟人类智能,不断进化自身的认知能力、判断能力和预测能力。而当机器的智商水平和理性程度足以超越人类时,其是否可以被赋予一定的权力代替人类进行某些决策,比如诊断疾病并自动进行治疗、审理案件并自行作出判决等,这一答案关系着人与机器之间的伦理界限。由于机器学习的对象并非仅限于人的智能,还包括人的感情,如果机器通过学习萌发自我意识,那么其是否应当被赋予人格主体地位?在民法上为这种高端机器人创建"人工人格"等成为颇具时代性的法学课题。而最令人担心的还是拥有学习能力的机器是否会脱离人类的控制,甚至反过来威胁伤害人类。因此,对机器进行合乎伦理的设计,将法律、道德、伦理等规范和价值嵌入智能系统,关系到全人类的福祉,体现了全社会的共同责任。

随着对机器学习的深度开发和广泛应用,对其进行伦理反思在某些领域显得尤为急迫和重要。例如,对于机器学习能否被应用于军事领域,尤其是自主武器系统的研发,各国存在明显分歧,多数国家支持对致命自主武器系统进行有意义的人类控制。[12] 此外,机器学习被应用于自动驾驶车辆在紧急情况下作出的利益衡量和取舍也引发了激烈辩论。比如,面对车辆失控的紧急情况,程序可否为了躲避较多的人牺牲较少的人,为了保护驾驶人牺牲乘客,为了保护贵重财产牺牲动物等。自动驾驶系统的程序难以摆脱这种"死亡算法"的困扰,当车辆发生紧急避险不可避免地要对不同法益作出取舍时,其会选择性地采取被系统预设判断为较小伤害的避险措施。而程序的设计显示出法律与伦理的较量,对于这种人为干预或者机器自主决策是否可以构成"伦理性免责",需要法律谨慎地予以回应。

2016 年 12 月,电器和电子工程师协会(IEEE)发布《合乎伦理的设计:将人类福祉与人工智能和自主系统优先考虑的愿景》,发起自主与智能系统伦理全球倡议项目并提出具体指南。[13] 2017 年 9 月,联合国犯罪和司法研究所在海牙成立第一家联合国人工智能和机器人中心,探讨如何在符合法律、道德和伦理的前提下对人工智能进行管控。欧盟成立了"欧洲科学和新技术伦理小组"讨论建立人工智能伦理准则框架,呼吁各国共同制定标准,深入研究人工智能的伦理学。2018 年,中国电子技术标准化研究院公布的《人工智能标准化白皮书》也提出了人工智能标准体系中应当建立"安全/伦理标准"。目前人工智能安全与伦理标准主

[12] [美]彼得·阿萨罗:《论禁止自主武器系统:人权、自动化以及致命决策的去人类化》,韩阳译,载《红十字国际评论》2012 年第 2 期。

[13] IEEE 自主与智能系统伦理全球倡议项目《人工智能设计的伦理准则》(第 2 版)概要,https://standards.ieee.org/develop/indconn/ec/ead_v2_executive_summary_chinese.pdf,访问日期:2018 年 5 月 2 日。

要集中在生物特征识别、自动驾驶等部分领域的应用安全标准,以及大数据安全、隐私保护等支撑类安全标准,与人工智能自身安全或基础共性相关的标准还比较少。⑭

(二) 机器学习算法滥用导致的认知歧视

利用机器学习的人工智能应用层出不穷,基于计算机学习算法歧视造成的性别歧视、种族歧视、就业歧视、司法歧视、消费歧视也屡见不鲜。购物平台上的精准定向广告、互联网金融领域的信用等级评估、生活服务软件带有价格歧视的大数据杀熟等都是利用了对个人生活信息的自动化数据分析、评估和预测,进而作出因人而异的行为决定。由于从数据的输入到答案的输出之间需要经历"算法黑箱"的操作,机器学习的模式并不透明,人们对人工智能可能作出歧视性决定的担忧日渐蔓延。

尽管开发者们一直在强调技术无罪和数据中立,但事实上机器学习已经不可避免地从人类创造者那里学会了"傲慢与偏见"。那些看似是人工智能的自动化决定,在有些情况下已经与技术的局限性无关,而更多地体现出了人类的授意或疏于注意。比如,2015 年谷歌公司利用机器学习进行人脸识别的照片应用错误地将黑人标注为大猩猩引发了对人工智能种族歧视的批判。2016 年微软开发的 Tay 聊天机器人,仅仅试用 24 小时就被人类调教成歧视女性支持纳粹的不良少女。而由美国政府主导开发的反恐识别系统和犯罪风险评估软件也因为频繁错认和歧视黑人等问题而广受批判。这一方面说明机器学习技术的完善仍然任重道远,另一方面也引发了对机器学习这种数字化技术中立性的质疑。虽然理论上机器人对人类并不会作出歧视性对待,但事实上程序设计本身很可能为设计者政策意图、价值取向等所左右。

此外,机器学习的训练数据本身可能带有现实世界中的歧视与偏见,基于这些数据分析产生的识别错误进一步内化了这些偏见,也可能无意识地侵害了被歧视群体的权利。机器学习算法的基础是大数据,而大数据源自现实社会,抹不去现实社会中固有的偏见歧视、歪曲事实的痕迹。饱受诟病的"大数据杀熟"就是基于算法歧视进行的价格歧视。机器在获取了消费者消费行为相关的数据(如消费记录、浏览记录等)后,会通过算法生成评分机制,对于消费频次高、决策时间短、交易金额大的消费者,作出购买力较强和对商品价格波动不敏感的判断,预测其愿意付出更多的成本获取商品或服务,于是"看人下菜碟"地进行差别定价。经营者利用机器学习分析消费者的个人生活信息,通过算法模拟出千人千面的用户画像,有针对性地制定精准化的定向广告和差异化的杀熟方案。虽然经营者有自主定价权,但其提供差别化的服务可能侵害了消费者的知情权和选择权,违反《消费者权益保护法》的相关规定,也有可能构成垄断。

(三) 机器学习算法滥用带来的认知妨害

近一两年,以"今日头条""抖音""快手"等为代表的一批新生网红 APP 就是利用机器学习技术,基于精准的算法,分析用户阅读喜好,实现平台精准"投食"的。这些应用迎合了现代人速食主义的娱乐消费观,通过推送短消息、短视频,消磨了一大批年轻用户的碎片化时间,造就了纯粹娱乐、极致消遣的流量怪兽。而这个过程就是手机应用开发商通过整合、分析、挖掘用户行为习惯、阅读历史、购买记录等信息,深入学习和分析用户的意图,推测其娱乐喜好、购买倾向等,并进行的卓有成效的精准营销。

算法通过监视读者行为习惯和兴趣喜好,可以选择性地向读者投放由机器判断其乐于阅读的内容,过滤掉其可能不喜欢的内容,从而强

⑭ 中国电子技术标准化研究院 2018 年 1 月颁布的《人工智能标准化白皮书》第 56 页。

大到可以歪曲事实、歪曲消费者需求的地步。美国社交网站 Facebook 之所以被指责影响了 2016 年美国大选,就是因为其泄露用户信息给英国政治咨询公司“剑桥分析”,而这家公司利用机器学习算法分析 5,000 万名用户资料,有针对性地向选民用户发送“专属”的精准政治广告,从而达到左右选民投票、影响政治风向的目的。这样看来,“得数据者得天下”所言不虚。有鉴于此,近日全球最大的媒体集团之一的新闻集团呼吁成立“算法审查委员会”,以监督科技巨头公司不断增长的权力,督促科技公司提高收集用户数据的透明度,防范算法滥用。[15]

像英国剑桥咨询公司这样通过机器学习从庞大的社交媒体资料中提取预测模型、向选民提供微定向广告以操纵舆论的做法已经超越了道德失范的界限,不能再将责任完全归咎于产生不透明算法的“科技原罪”,这是巨大的商业利益诱惑下的赤裸裸的侵权行为。无论是传统媒体、社交媒体还是自媒体,这种利用机器学习过滤信息、操纵舆论的做法妨碍了有效信息的传播效率,违反了媒体中立性和新闻真实性的报道原则,侵害了公众的知情权,损害了社会公共利益,甚至可能诱发“网络倾泻”和群体极化现象,危害国家和社会公共安全,对此我们应当提高警惕,加强防范,及时制定相关法律法规,将“数字利维坦”关进制度的笼子里。

四、机器学习的隐私权忧虑及民法保护路径

如前所述,随着大数据时代的到来,几乎所有个体的生活场景都被网络数据化,运用机器学习技术能够迅速地对这些海量数据进行分析处理,实现人工智能科学决策、未来预测的功能。尤其是在互联网定向广告、手机生活记录软件、内容或新闻推送软件、GPS 定位系统等领域,计算机通过分析个人消费信息、信用信息、位置信息、医疗信息、社交信息、网络浏览记录等个人生活信息,不但可以知悉信息主体的兴趣爱好、行动轨迹、消费能力、健康状况、行为方式等,还可以模拟人类大脑基于经验数据进行思考和预判,为用户提供有针对性的个性化服务。

尽管机器学习一定程度上便捷了生活,优化了服务,但也带来了公众对于隐私不保的普遍忧虑。以个人诊疗信息的收集利用为例,通过构建机器学习的模型,可以根据人的年龄、性别、身体症状、发病原因等信息推测出其职业、罹患疾病名称等敏感信息。如果掌握了这种模型,就有可能根据某个特定人物的年龄、性别、身体症状等推测出精确度较高的疾病名称。这虽然有益于病情的诊断、防控和医学研究,但如果不经本人同意提供给第三人就可能造成隐私泄露。

此类个人生活信息虽不能够较容易地直接识别和映射特定个体身份,但有可能结合其他信息进行比对从而间接识别出特定个人或群体,其与个人身份信息、个人衍生信息共同构建起内涵丰富的个人信息概念体系。个人生活信息具有财产利益和人格利益的双重属性,其法理基础是人格权中的个人信息权,强调以人的人格性自主为核心内容的控制性和自我决定性权利,可以考虑借助公开权理论进行保护。信息时代赋予个人生活信息巨大的财产价值,对其不当利用有可能侵犯公民的隐私权和个人信息权,其大量聚合之后形成的国民信息关系着国家信息主权和信息安全。

诚然,一些用户隐私观念非常薄弱,导致其在社交网站上自我曝露,通过手机 APP 开门揖

[15] 邢斯嘉《新闻集团呼吁成立“算法审查委员会”以监督各科技巨头》,http://news.eastday.com/eastday/13news/auto/news/china/20180513/u7ai7703605.html,访问日期:2018 年 5 月 14 日。

盗,这些行为乍一看是自愿为之,但事实上多出于不明真相或别无选择。据最新数据调查显示,98.5%的安卓应用会获取用户手机隐私,苹果手机应用也高达 81.9%。[16] 尽管为了保护个人隐私、尊重信息主体的知情权和选择权,各国普遍确立了信息收集中的"告知——许可"规则,但由于空洞授权、概括同意、格式化合同泛滥等问题普遍存在,以协议形式获取用户授权的做法多数流于形式。此外,虽然近年来技术界热衷于研究旨在保护隐私的同时实现数据共享的"匿名化——模糊化"处理方式,通过删除数据中具有可识别性的个人身份信息能够一定程度地保护个人隐私,但是随着匿名化信息再识别技术的开发,数据二次利用的再特定化风险显著增加,这种操作也不足以杜绝隐私的泄露。

虽然有越来越多的用户意识到隐私曝露问题的严重性,希望拥有对自身数据的控制力(例如透明性)和财产权(处分、收益),但事实上其得不到较好的技术性安全保障,即使有保障他们也只能默认平台的优先使用权。[17] 而各大平台为争夺用户纷纷积极表态对于数据安全的重视,并探索在收集必要数据信息时以不牺牲用户隐私安全的方式保障用户合法权益。有经营者开发出"差分隐私技术",由用户自行决定要不要上传数据给手机厂商。[18] 也有经营者公开承诺永远不会将客户数据交给任何国家的任何政府监控计划,客户不仅对其终端数据享有权利,还对任何源自其终端数据的算法"学习成果"享有权利。[19]

不过,对于个人信息的保护不能仅靠科技企业的自律和互联网行业的自净,在这一领域法律大有可为。随着个人信息权写入我国《民法总则》,《个人信息保护法》也呼之欲出。围绕个人信息保护的立法应当着力于保障信息主体对个人生活信息享有知情权、选择权、利用权、修正权、删除权等基本权利,并坚持以下原则:第一,正当性原则。网络交易平台提供者、网络服务提供者等信息业者应以正规的渠道和方式获取信息,确保信息主体知情且同意,防范利用格式合同强加服务,赋予信息主体自主选择权。第二,匿名性原则。对信息作匿名化、符号化处理,尽量避免二次利用的再特定化、再识别化。第三,透明性原则。以合理方式通知或使信息主体较容易获知对其信息利用的隐私风险和用途。第四,安全性原则。信息业者出于营利目的利用个人信息的,在存储、传输、使用和转让给第三人的过程中负有安全保障义务,应遵循知情同意规则、提示删除规则和已知规则,确保完备的安全管理措施,防止信息的泄露、灭失、毁损。第五,最低限度原则。严格控制信息收集主体范围,明确公权力机构对个人信息收集、利用、保护的权限,确立政府主导下信息过滤的基本原则,对出于公益目的的利用做必要的最低限度控制,防止信息滥用。第六,可参与性原则。建立投诉、咨询处理体制和信息可追踪制度,信息主体能及时采取停止获取或利用信息的手段,对于不必要、不相关、已过时的信息有权删除。

当然,隐私权、个人信息权也并非绝对性权利,需要与表达自由、营业自由、社会公益、国家

[16] 参见腾讯社会研究中心与 DCCI 互联网数据中心于 2018 年 1 月 17 日联合发布的《2017 年度网络隐私安全及网络欺诈行为分析报告》。

[17] 胡凌《超越代码:从赛博空间到物理世界的控制/生产机制》,载《华东政法大学学报》2018 年第 1 期,第 15 页。

[18] 《苹果公布新版隐私政策:引入差分隐私和智能反追踪技术》,http://www.sohu.com/a/195235030_260616,访问日期:2018 年 5 月 2 日。

[19] [美] 拉娜·福鲁哈尔《隐私将成为科技公司竞争优势》,载《英国金融时报》,http://www.ftchinese.com/story/001074814 Archive,访问日期:2018 年 5 月 2 日。

安全等其他价值综合比较进行相对性判断。现代社会需要信息的流动和分享，应当允许出于公共利益、科学研究、国家安全等正当性目的收集个人信息，并通过法律明确需要合理授权或者强制授权的情形，平衡好优化服务与隐私保护、信息服务与信息防护、个体权利与公共利益、个人信息自由与国家信息安全的关系，探索合理利用和法律规制的边界，尝试构建平衡各方利益的综合防治法律体系。

人工智能时代已经全面开启，机器学习创造出了巨大的商业利益，但也带来了侵犯个人信息权和隐私权的社会争议。“算法黑箱”并不能成为法外之地，要防范因算法的认识偏差和决策失误导致的侵权行为，避免机器学习带来的伦理困境和道德失范，妥善解决层出不穷的侵权事件，不能仅依靠行业自觉自律，还需要树立法治先行的观念，以法律革新保障技术革新。

View of Law Regarding Machine Learning

Tao Ying

Abstract: Machine learning is that the computer program will generate an algorithm for judgement and inference by learning the data, hence to simulate the human intelligent activities and improve the system performance. Widespread application of the machine learning has not only brought opportunities for rapid development of the modern society, but also injected vitality into reform of the legal system; The challenges to social order and legal regulations from technology advancement cannot be ignored, especially in terms of safety, ethic, and privacy. In case of any safety-related accidents caused by decision-making mistakes of machine learning algorithm, it may be deemed that the product is defective and subject to relevant regulations concerning product liability. It's necessary to strengthen legislation to prevent any ethical dilemma and moral abnormality caused by machine learning algorithm and to respect the right to know, right of choice, and right to self-determination of the infringed. For the concerns regarding right of privacy arising from collecting personal information during the process of machine learning, it's important to correctly and properly make use of the legal boundary regarding violation of right to personal information and right of privacy, quicken the legal reform with positive attitude, and guarantee technologic innovation.

Keywords: AI; machine learning; algorithm black box; rights of privacy; right of personal information

(责任编辑：李　辉)