

司法的科技应用:两个维度的观察与分析

张建伟

(清华大学法学院,北京100084)

摘要:司法智能化,诸如数字技术的司法应用,具有两面性。在我国,相关问题的研究主要着眼于网络犯罪领域如何利用科技手段打击犯罪,对于政府权力的限制及其相关的法律的正当程序问题,研究与讨论尚不够充分。可以从两个方面探讨司法的科技应用,特别是大数据司法应用涉及的两个维度问题,一是犯罪控制维度,二是正当程序维度,它们在各自含义中体现了实体正义和程序正义的观念。通过对司法技术性问题进行分析,发现我国法院和检察院作为司法机关,对于侦查权的司法控制还有很大的拓展空间,大数据应用为司法机关加强对侦查权的控制提供了新的契机。

关键词:大数据;控制犯罪;司法审查;正当程序;数字极权主义

中图分类号:DF73 **文献标志码:**A **文章编号:**1009-1505(2021)05-0043-13

DOI:10.14134/j.cnki.cn33-1337/c.2021.05.005

司法智能化,是我国司法改革中充满技术含量的话题。作为智能化司法和数字技术具有代表性的外在表现,大数据在司法中的应用早已由一种讨论中的概念变成刑事诉讼中逐渐普遍化的现实存在。对于这类在当代司法实践中越来越受到重视的技术应用,有两种观察的维度:一是从发现并惩罚犯罪的维度,着眼于该技术方法在维护秩序、提高效率方面的作用,揭示其在证明犯罪嫌疑人、被告人有罪方面带来的变化以及需要解决的某些技术性问题,如大数据分析的证据归属、大数据与司法证明客体之间的关联性等,目标是在全国范围内推广这一智能化司法手段;二是从法律的正当程序角度,着眼于大数据在刑事司法中涉及的个人自由权利的保护,对于履行刑事追诉权的主体获取大数据的方法,试图找出规制的方法,体现自由主义司法而不是威权主义司法的价值。不仅大数据的司法应用如此,与此类似的新的科技应用,也是如此。

当前,从相关司法实践和学术研究看,十分明显在向控制犯罪的需求倾斜,对于正当程序的学术关注尚嫌不够,相应的立法更是有待进一步加强。笔者认为,与刑事侦查学不同,刑事诉讼领域的智能化司法的研究重点,不在于数字技术手段在控制犯罪中令人惊叹的作用,而在于如何对其进行有效的正当程序控制,这是由刑事诉讼法的限权功能重于授权功能的基本特征决定的。但是,新科技手段的应用,构成控制犯罪与正当程序的两种价值,两个方面都有需要解决的问题,彼此之间也存在一定的

收稿日期:2021-06-19

基金项目:2021年最高人民检察院检察应用理论研究课题“量刑建设实务问题研究”(经费资助课题——编号07)

作者简介:张建伟,男,清华大学法学院教授,博士生导师,法学博士,主要从事刑事诉讼法学研究。

联系,包括应当考虑两种价值的平衡关系。

一、数字技术应用与智能司法:控制犯罪之维

《圣经》开篇,上帝说“要有光”,于是就有了光。人类的早期司法,借助的是上帝之光,诉讼证据史上称之为“神判制度”。在漫长的中世纪,人类借助的是长期积累的司法经验,由经验形成规律性认识,如宋慈的《洗冤录》和欧陆中世纪盛行的法定证据制度,就是借助于经验使司法得以改观的典型表现。在当下以及未来,司法需要借助“科技之光”。现在司法科技化发展速度惊人,折射出了司法机关对于科技化司法的自觉意识,科技应用不但体现在司法领域,而且在普法教育方面、网络舆情预警方面都发挥着高效能的作用。

美国学者理查德·萨斯坎德在《法律人的明天会怎样?——法律职业的未来》一书中提到:“目前互联网研究和实践领域最激动人心的话题之一就是‘大数据’。全世界对信息技术和互联网无处不在的使用产生了无边无际的海量数据。由于过于庞大和浩繁,大多数传统工具都无法处理。确实,一个人机交互的产业正在兴起,帮助我们应对数据带来的挑战,帮助我们更高效地处理和驾驭数据中的价值。这项工作吸引人的成果之一,即在于大数据能揭示出过去我们不能发现的模式和关联。”^[1]

的确,当今社会进入了一个“新时代”,许多令人耳目一新的变化构成了这个时代的“新”。早在20世纪90年代,比尔·恩门就提出了“大数据”(Big Data)的概念。所谓“大数据”具有五大特征,即大体量(数据量大,Volume)、多样性(类型繁杂,Variety)、有价值(Value)、时效性(实时高速,Velocity)、准确性(Veracity)^[2]。也有人认为是四大特征,包含大体量、多样性、有价值、时效性^{[3][4]}。无论如何,大数据之所以大,是因为其数据可谓海量数据。大数据主要来自三个方面:商业数据(人们从事商业记录的直接内容记录)、人为数据(人有意识通过大脑创造的内容)和机器数据(机器产生的数据)。综观“上述三类数据,格式异构、类型繁杂、形式多样”^{[3][4]}。

大数据等新的科技手段,使我们的司法会不会也有一个新时代?答案是,不但有,而且到来得很快。近年来,司法智能化取得很大进展,在很多方面都发挥了作用,包括对于犯罪趋势的预测、发现某些犯罪的线索,以及在刑事执行方面,预测再犯可能性,在司法证明方面,大数据应用和智能手段的推广,正在改变司法形态。事实上,许多法律人已经真切地感受到,司法的新时代可能比我们预料的来得快。

我国大陆地区过去的司法长期存在一个问题,就是科技化程度不高。司法审判中关于科学证据的争议并不多见,鉴定人员出庭作证的比例也不高。可以用来对比的是,在西方一些国家,法庭审判有关科学证据的争议既多又大,例如美国的辛普森案件、凯西案件等,有大量鉴识科学人员到法庭上作证,控方、辩方形成一种竞争态势。凯西案件审理中,还有气味方面的鉴识科学人员出庭作证,这种气味鉴别证据涉及弗莱伊规则的应用,法庭要裁决能不能采用这种气味鉴定专家意见,给人深刻印象。这种审判活动不但具有实质性,而且科技化程度非常高。

这种现象,与司法竞争程度、司法制度的总体设计、诉讼模式和辩方的挑战力都有密切联系。一个清楚的脉络是,司法竞争程度越高、司法制度的总体设计中对抗性越强、辩方的挑战力越大,司法的科技应用就越及时。例如,DNA技术最早应用于英国,有其诉讼模式原因。它引出的一个问题是:为什么在对抗制诉讼模式之下科技应用很快,而在其他诉讼模式之下似乎要慢很多?答案就在其竞争主义的诉讼模式、司法机制等因素之中。

现在我国在司法智能化方面取得大跨度的进步,大数据等新的科学技术在司法当中得到快速应用,并取得可观的成绩,固然有诉讼模式中引入对抗制因素以及律师作用加大的原因,但主要原因是这些技术手段在控制犯罪方面令人惊叹的作用。

对于大数据在司法领域的应用,尤其在控制犯罪方面的作用,人们可以从侦查、检察和审判等不同领域进行考察。每个领域又可区分为办案、办公和管理等多个方面。

从刑事侦查角度看,大数据应用于打击犯罪,涉及两个方面。

一是对于已经存在的犯罪,办案机关运用大数据技术收集证据,确定并抓获犯罪嫌疑人,也使有关单位犯罪问题得以曝光。在侦查过程中,大数据的应用有其独特作用,大数据侦查的原理就是“侦查部门通过采集海量数据建立数据库,建立关联性分析、数据碰撞、数据可视化、数据画像等规则,对犯罪嫌疑人进行画像等,获取破案的线索和情报”^{[4]33}。侦查机关借助情报分析系统或者信息云平台,将所有收集到的数据关联起来,进行一键搜索和关联研判,对大数据作出智能分析,从而发现犯罪线索、证据和犯罪嫌疑人信息。其中,数据画像源自交互设计之父 Alan Cooper 提出的用户画像(persona)的概念。“用户画像”是真实用户的虚拟代表,是建立在一系列真实数据之上的目标用户模型,“通过对客户多方面的信息的了解,将多种信息集合在一起并形成在一定类型上的独特的特征与气质,这就形成了用户独特的‘画像’”^[5]。个体画像的构成要素包括:一是静态属性,属于一个人的人口学特征,诸如年龄性别等,由于不会有变化或者短期内不会有变化,因此称为“静态属性”;二是动态属性,如一个人的行为以及行为反映出来的兴趣爱好等,容易发生变化甚至突变,属于更具有个性的特征;三是环境属性,一个人所在位置、所处环境等,属于与一个人紧密联系的自然、地理和虚拟世界等环境因素^[5]。显然,这些对于查缉犯罪人并获得相关证据都具有实际价值。大数据在某些特殊领域的应用,显得尤为重要,如在金融领域,数据革命正在为银行、执法机构和监管机构创建一个新的工具包,用来打击金融犯罪,有利于打击腐败、洗钱和恐怖主义融资等违法犯罪行为。对于政治人物,他们因身居高位、握有重权而便于通过受贿等手段获得巨额资产,大数据可以帮助银行履行对于这类政治人物的识别和监测义务,从而展现国际反腐败合作中的金融力量^[6]。

二是应用大数据,可以对未来的犯罪进行预测,对可能的犯罪进行提前打击,达到阻止犯罪的功效。大数据的价值,可以帮助人们“通过各种途径、运用各种方式,获得尽可能详尽的事物描述性信息”,从而实现预测。因此,大数据形成“一切皆可测量”的局面——“不仅仅互联网线上的事物可测,线下的行为也可以通过某种方式获得数据;很多过去难以量化的事物,如情绪、偏好,基于科技处理数据能力的提升,都能够很好地用数字化的方式记录和表达了”^{[3]7}。基于大数据的这一特征,侦查机关可以通过数据分析掌握人和单位的各种细节,从中发现异常情况,寻踪做出犯罪风险预测,实现防范犯罪的功能。

我国司法机关近年来着力打造司法新时代,不仅有大数据的司法应用,还有人工智能技术带来的革命性变化^[7]。司法上一些令人瞩目的变化出现了:法院开始走进智能法院阶段,刑事侦查中更是加紧利用大数据,这势必使过去侦查极为困难的案件,得以迅速侦破。在刑事司法中,司法机关最初关注的是同案同判,同类相似案件的量刑要大体均衡,如今又提出“类案检索”,在这方面司法智能化得到持续推动,甚至一度出现“电脑量刑”的尝试。

毫无疑问,科学技术的发展成为司法的助力,已经改变并且正在改变司法的样貌。将最新科学技术应用于司法,已成为司法机关的自觉意识。我国公安司法机关近些年来,在提升司法的科技含量方面作出了很多努力,科技应用方面已取得明显的成绩。

二、科技的司法应用需要解决的法律技术性问题

当然,纵观整体司法上的科技应用状况,可以发现我国司法的科技应用仍然具有一定的局限性和被动性特征。另外,数据司法也暴露出智能化存在的不足,如数据孤岛的问题——数据孤岛算法的选择和透明性问题,都是在司法的科技化发展当中产生的问题,还需要有针对性地加以解决。

在司法智能化过程中,大数据等新科技手段在侦查、起诉和审判活动中的应用,引申出程序或者证据问题乃至更深层次的具体问题,诸如以下几方面。

(一) 大数据应用,是否以刑事立案为条件?

司法的科技应用,让我们思考相应的刑事诉讼程序问题时,既要考虑把新的调查措施和证据形式纳入诉讼轨道,也要规范运用高科技手段的取证行为,研究信息化时代取证手段的正当性问题,这已经成为立法和司法的迫切需求。在诉讼程序方面,大数据技术应用带来诉讼程序设计方面的新思考^[8]。

我国对于侦查机关行使侦查权的程序限制之一,是设定了较高的立案条件。这里的“较高”是与许多国家的登记立案制度比较而言的。一些国家以登记(booking)为侦查端绪,这种制度下的立案条件比我国宽松得多——有人报案、自首、控告、举报,警方做一个登记,随即就可以开始侦查。所以,它的侦查大门开启较为容易。不过,许多国家对于侦查的司法控制比我们严格得多,倘若使用强制性侦查手段,依据令状制度,应由法官加以限制。我国刑事诉讼实行审查立案制,这就为立案设置了较高门槛,将某些调查案件事实的措施规定在立案后才能实施,意味着立案前不能采取这些措施预先实现调查案件的初步意图,为进一步侦查打下基础。的确,那些具有强制性的措施,不能不以严格条件和程序加以限制,如查封、扣押、冻结和拘留、逮捕等,立案之前不能采取这些措施,以避免对人身自由和财产权利造成不适当的剥夺,除非情况紧急,如根据需要对于可能犯罪的人进行人身自由的控制(本质上是暂时剥夺其人身自由)。但是,不能不允许侦查机关在立案之前就采取非强制性的措施(即任意性措施),这些措施,如现场勘查措施、鉴定措施是确定是否立案的手段,需要在立案前就进行现场勘查、鉴定,以确定是否具备立案条件;现场勘查中取得的证据和鉴定意见,也应当允许在立案之后的诉讼中使用。有的措施,并不能将其性质限定为侦查措施,如鉴定固然属于调查手段,但是只有在侦查阶段采取这一措施时才称为侦查措施,立案前和侦查终结后就不属于侦查措施,如在审判阶段进行补充鉴定、重新鉴定或者为核实案件事实、证据而庭外进行鉴定已经属于审判阶段且委托鉴定的是法院,就不能再称之为侦查措施。

大数据采集和分析,作为发现犯罪的一种手段,也是如此。在立案之前进行的大数据采集分析,只是立案的信息来源之一,在立案来源中属于“自行发现”这种情况。易言之,作为立案来源之一的大数据采集分析不必然属于侦查措施;但是,立案后作为服务于具体案件办理的大数据采集分析,就是侦查措施的一种了。我国刑事诉讼法规定的立案条件相当严格,要求具备有犯罪事实发生、需要追究刑事责任、符合管辖规定这三个条件才可以立案。显然,如果将大数据技术在侦查前的应用也看作侦查措施(进一步,看作技术侦查措施),就产生应用上的困难——高科技手段在立案之前就需要得到应用,由此才能发现犯罪,如果限于立案后才能采取这一措施,就陷入了“二十二条军规”式的困境。因此,对于非特定目标人物或者团体采取的大数据采集分析,不以立案作为其合法有效的条件,包括办案机关得到重大犯罪即将发生的情报信息,但是尚未确定目标人物或团体,立案之前应当允许采用一定的高科技手段来收集证据和获得犯罪以及犯罪人信息。

不过,对于特定目标人物和团体采取大数据采集分析,应当以立案为条件。但是,这种限制是否适应智能时代的侦查需求,不能不重新进行审视。我国立案条件较高,成为对于特定目标人物和团体采取大数据采集分析的制度障碍,对此解决办法有两个:一是降低立案条件,由审查立案制改为登记立案制;二是将这种措施应用的司法审查与控制延伸到立案前阶段。在我国,未来高科技手段运用于案件的侦查和预防,可以通过司法机关事后审查,或者事中、事前加以控制。亦即,司法机关对于采取这种侦查手段的授权和控制,可以延伸到立案前,侦查机关要采取技术手段应当向司法机关(理想的制度设计是法院,根据我国目前的制约侦查权的制度设计也可以考虑由检察机关承担这一职能)提出申

请,申请时应提供一定的证据、证据线索以及可疑情况,由司法机关审查批准,无论是否批准均采取书面形式。批准书应当明确技术应用的对象范围、时间范围和注意事项。对于技术应用情况,司法机关有权了解和监督。技术性调查结束以后,对于技术应用取得的结果(例如由此获得的证据),侦查机关应向司法机关作出报告,司法机关可以根据技术应用过程合法与否决定是否予以接受。在整个调查过程中,发现技术应用存在违法问题,司法机关应当及时加以纠正,以保证高科技在犯罪控制方面得以充分、正确地应用。

(二) 大数据应用,如何确定证据归类?

关于大数据在司法中的应用,需要确定的是证据归属问题——海量数据,顾名思义,其包含的信息浩如烟海,但是只有其中一部分数据与正在办理的案件有关,这些数据淹没其中,跟大数据是合流的,与案件有关的这部分数据,需要加以提炼和分析,如果不经过分析,那么在司法实践中大家势必搞不清楚具体数据的意义何在,无法进行法律意义上的解读。所以,大数据应用离不开数据分析,但由此形成的大数据分析报告,其证据属性上如何归类立即成为一个疑问。

我国司法制度和证据制度是学苏联的。苏联证据法的特点之一,是将证据种类一项一项列举出来,这种列举式证据种类规定,优点是哪些证据可以在司法中应用一目了然,证据的法定形式非常清楚;缺点是列举不易周延,需要根据诉讼新情况、新变化随时作出调整,如果调整不及时,司法活动中对于新出现的证据种类,办案人员就会产生困惑——它能否作为证据使用?

笔者认为,未来的证据法,有必要将大数据分析报告单列出来作为独立的证据种类,大数据中那些跟案件相关的数据信息,基于其生成机制中的电子技术,可以纳入“电子数据”这一既有的法定证据种类范畴。

(三) 大数据应用,如何确定与证明对象的关联性?

大数据侦查获得的信息材料及其分析结果跟司法证明对象的关联性怎么确认?这是个新的需要给出答案的问题。笔者认为,传统的关联性判断标准可以用于破解这一疑问,这个标准可以分为两个具体标准:一是指向标准,即这些数据和相关分析是不是指向案件的争点问题;二是功能标准,即这些数据和相关分析得出的结论,对于证明对象,有没有证明作用或者证明价值,亦即这个材料的存在使争议中的问题是不是变得更有可能解决或者更无可能解决。传统的相关性判断方法在对大数据证据材料的审查运用当中,有其生命力和应用价值。

在司法活动中,确定信息材料及其分析结果跟司法证明对象有没有关联性的实际做法是,借助有专门知识的人来揭示信息材料及其分析结果跟司法证明对象的关联性。同时,在司法具有一定竞争性的场合,控方举证时提供数据和相关分析,辩方可以借助科技力量,聘请有专门知识的人作为专家辅助人去挑刺、去质疑,双方围绕证据关联性等争议点进行诉讼攻防,这个过程当中由法官在双方发表意见和辩论的基础上进行判断。所以,法庭上控辩双方的一些演示、说明很有必要,要说服裁判者,让裁判者听得懂、看得懂,以便其作出相应的、妥适的判断。

(四) 运用大数据辅助量刑,是否导致司法机械化?

在我国大陆地区,运用大数据辅助量刑,最初的设想是运用电脑辅助量刑。有的法院大胆设想要将已决案例分别编入电脑,承审法院将自己受理的案件的主要事实、情节、当事人基本情况等输入电脑,电脑就会显示以前类似案件作出的判决,法官无须根据自己的心证决定案件的定性和量刑,一切都在电脑掌握之中。对“电脑量刑”的做法,存在争议。应当质疑的是:“每个案件都是千差万别的,它要求法官针对不同情况,作出具体而有针对性的量刑处理。而且,恰恰就是在运用量刑个别化标准的时候,才是最能考验法官智慧和能力的时候,而电脑量刑则把一个法官所必备的经验抛到了九霄云外。”^[9]实际上,“电脑量刑”的做法限制了法官根据自己的良心、理性和对法律的诚挚的理解,在法律

赋予的权限范围内对个案进行处理,实现“个别的公正”。电脑将纷繁复杂的刑事案件简单化,如果法官机械地按照电脑的指示去处理案件(法官只保留了微小的自由裁量幅度),就违反了根据案件具体情况在法定幅度内选择适于本案的刑期的规定,法律赋予法官根据案件实际情况进行自由裁量的权力因此就会被弃置。

(五) 运用大数据确立证据规格,是否导致法定证据制度复归?

法定证据制度又称“形式证据制度”,其核心内容为证据的证明力由法律预先加以规定,即突出体现为法律对各种证据的证明力所作的预先规定。法定证据制度有多种表现,其中之一是有些国家对于运用证据认定某些特定案件作出了具体规定。法定证据制度的形成,就是考虑到用法律的形式,具体规定各种诉讼制度的证明力和运用的规则,消除各地在诉讼中运用证据的混乱状态,为此把某些证据形式上的特征,作为评价所有这些证据证明力的标准;并把这些内容规定在法律中,要求法官在审理案件中加以机械地遵守,因此遏制了法官在审理案件中的理性,束缚了他们的头脑。我国大陆地区一些司法机关尝试统一某些种类案件的证据规则,就根植于从司法实践中总结的经验和大数据分析的结果,具有一定的指导性,但是由此形成的证据规格、标准如果是对于侦查、起诉和审判的统一、硬性要求,就容易忽略案件与案件之间的个体差异,形成僵化的、机械司法的状态,复归到形成法定证据制度,与证据制度由反理性向理性发展的方向相背离。显然,如果证据审查的形式意义大于实质意义,证据的形式审查对于公安司法人员的实质审查产生窒碍作用,曾经存在的法定证据制度的弊端就随着这种形式审查的回潮而自然产生了。

(六) 人的司法被机器司法取代?

在司法科技化的发展过程中,当下强调较多的是科学机械、科技仪器的应用,包括智能机器人在司法中的应用,这些都属于机器的智能化的范畴,所谓“工欲善其事,必先利其器”。然而需要指出的是,在科技化司法发展当中,机器的科技化、司法的智能化,旨在为人服务,科技手段为人提供便利,却不能取代人的智慧。就司法而言,尚难以想象离开人的能力和智慧而成就的正义。人可以“机器化”,如德国学者赖默尔·格罗尼迈尔所言:“人类这一由骨血和体液构成的湿润配件也听从于设计命令。”^{[10]221}但是,机器可以具有人类的情感吗?即使所谓智能型司法,也不能缺少公安司法人员的能力、智慧、感情的注入,更何况纷繁复杂的社会与人生,怎能少了人的观察与判断,司法要具有温度,必须是人的司法而不是机器的司法。借助机器化智能软件的司法,决不能免除法律人维护法律价值尤其是维护宪法允诺保障的各种自由权利的责任。不仅如此,司法智能化的同时应当警惕:这种智能化可能造成司法人员的惰性,久而久之形成智力退化,造就思维懒汉的司法群体,更糟糕的是,“信息和知识社会通过将人类数据化的方式来进行。很明显:数据一体化笼罩在个体的上方,取代了人与人之间的融合。人类把自己变成了附属物”^[10]。司法科技化,只能成为办案人员的司法能力和智慧应用的助力,对于后者发挥提升作用而不是相反。

除了上述问题以外,大数据的司法应用,还存在其他需要解决的问题,诸如数据沉睡与壁垒的问题:公安司法机关“并非没有数据资源,只是相当一部分数据还处于沉睡状态,没有被激活”,不仅如此,不少司法机关的内部数据仅仅处于“内部公开”状态,“局限于某系统、某部门、某地区范围内”^[11],不同系统、不同地区、不同部门、不同级别的公安司法机关各自为政,形成各自森严的壁垒,使大数据的应用受到阻碍,故亟须解决好这一问题。

此外,公安司法机关中能够对大数据进行分析的技术人员的匮乏已经成为一个突出问题,可以预见,“法律大数据将催生一种新型的法律职业——法律数据分析师。大数据既然是一种技术,意味着需要专业知识来掌握,不可能为普通人所掌握。因此,法律研究、审查应用和立法领域都需要具有丰富经验的法律大数据分析人才提供协助”^[12]。到目前为止,司法机关法律数据分析技术人才不足尚未得到

很好的解决。不仅如此,在已有的司法人员和技术人员中也存在着“隔膜”问题:“司法人员与技术人员的‘隔行’是一个非常严重的问题,不是技术人员不懂司法业务,就是司法人员不懂技术原理,导致许多司法需求难以被理解、被转换成技术方案。”^[11]这影响了司法科技化程度和司法专业主义的强化。

三、数字技术应用与智能司法:正当程序之维

现代国家的任务之一是遏制犯罪、维护秩序,反恐怖的国家安全和遏制犯罪的社会防范的需要,为新科技的司法应用提供了正当性和必要性。这种正当性和必要性很容易掩盖司法科技化的另外一面,这就是正当程序理念下对于新科技应用带来的危害的警觉和防控。

不过,令人欣慰的是,如今越来越多的人将保障人权看作现代国家的任务之一,这对于新科技手段引发的个人自由权利的保护制度提供了民意基础。

新科技应用,无不涉及个人的基本权利。特别值得密切关注的:一是大数据技术的司法应用,侦查、起诉和审判获得助力;二是公权力运用科技定位措施,进行追踪监视;三是面部识别技术在社会多领域的广泛应用。这三个方面的科技应用,正在改变司法状况、社会形态和国家治理能力。它们无一例外涉及人权、人性尊严这一类话题,而这一类话题正是多年来国际社会普遍关心的议题。

以科技手段进行定位以及追踪监视,即通过定位科技掌握特定对象的位置资讯,进而对该对象进行跟踪和监视,以获得其行为信息或者进行人身控制或抓捕。这种技术手段具有比过去人盯人式的旧式跟踪监视方法更为便利的特点,“公权力运用科技定位措施追踪监视可以大量又精密地收集资料,尤其很多以传统方式无法达成的任务,都可以透过科技定位来完成”^{[13]73}。这种手段具有比旧手段更优越的是,“虽然公权力广泛在运用这些措施,但是通常民众对于这种公权力运用的措施并没有任何感觉,尤其有些措施并不具有目的性”^{[13]73},它造成的人权侵犯的状况不易为权利受侵犯者所知,这对于公权力机关来说就太方便了,但是从另一方面看,权利保障问题因权利被隐秘侵犯的事实所淡化。

面部识别依靠摄像机作为识别信息获取装置,获取识别对象的面部图像后,依计算机系统对获取的面部图像完成识别过程。这种识别方法,在准确、高精度等方面特性优于肉眼识别,也是指纹识别等过去的识别方式无法比拟的。人脸识别技术在识别恐怖分子以防范危险和需要抓捕的犯罪人员以将其抓获归案方面有着积极的作用,但是这种技术的优点是以更多与此无关的人付出隐私代价为基础的,这势必引起社会的广泛疑虑,进而引出法律学者和立法机关、司法机关予以解答的必要。

大数据“实质上意味着从不同资源中获取巨大信息的能力”,最新科技手段和科技条件及其应用令人惊叹,有论者将各国在这个领域的竞争称为“二十一世纪军备竞赛”(A Twenty-First Century Arms Race)。人们在乐观看待技术进步改变社会生活多方面的同时,不能不注意到,新的科技手段是一把“双刃剑”,“大数据明显有利于执法人员”,这种技术手段在为刑事侦查、起诉和审判提供令人赞叹的助力——特别是为有些依照以往侦查手段难以解决的案件提供了新的解决之道的同时,也提升了政府对于整个社会的控制能力,但同时危及宪法允诺保障的个人自由权利。

在上述科技手段之下,个人日益成为“透明人”,生活在“隐私不保的社会”,在政府的科技控制下成为毫无抵御能力的人,其中大数据采集造成“大数据、小个人”(Big Data, Little Persons)乃至“数据愈大、个人愈小”等现象,成为许多法治成熟的国家与社会格外警惕的问题。

控制犯罪与正当程序再一次以尖锐冲突的局面出现,并连接着国家与社会在自由与威权之间重新位移的可能性,因此,对于科技手段带来的反面乌托邦的担忧,成为当下一些国家的法学研究以及立法与司法集中的焦点之一。

在国际社会,人们意识到:新的科技手段及其广泛应用,为21世纪新的极权模式创造了条件。人们并不是一开始就意识到这一点,“在互联网的语境下,对我们来说尤其重要的是:大多数人甚至根本没

有意识到,这种网络构建的选择已经能够被规制。大多数人认为它们是理所当然的,因此从不提出质疑。在他们眼中,互联网保护自由,是因为其设计理应如此。现在互联网越来越快地控制人们,多数人同样认为这是一种设计的必然”^{[14]232}。

不同国家,包括隐私权在内的自由权利保障状况不同,甚至对于个人信息安全的观念存在差异^[15],对于电子技术控制人的自由权利的意识也会有所不同,有着健全的自由权利保护机制的社会,人们生活在互联网环境中的安全感较强,对于数字极权主义的可能性反倒并不敏感;在自由权利被严格控制的社会,知识阶层对于数字极权主义会有较早的警觉与感受,但是大多数普通民众因素来缺乏隐私权观念和自由传统而反应较为迟钝。不过,“任何文明都可能落入恐惧、科技和暴政共同编制的罗网”^{[16]235}。随着国际交往越来越频繁,会有越来越多的人担心极权主义的梦魇会借助新的科技条件变为现实,这种担心有着充分的理由:如果对于这种可能性不加警惕并加以规制,人的行为和言论将被新的技术手段严密控制。无论是《1984》描述的那种粗暴的压制型社会也好,还是《美丽新世界》描述的那种精致的功利型社会也好,一旦与电子化时代新的科学技术手段结合在一起,对人的全面控制就会获得比以往更加强而有力的条件。

人们对于极权主义(Totalitarianism)并不感到陌生。它首先是一种意识形态,这种意识形态的实体化,体现为一整套严密的制度,在这一意识形态和制度之下,高度集中的领导权没有制约地行使政治权力,去影响总体(Total)社会的进化,包括人的生存条件,植根于全体人民强迫一致的氛围里由领导者倡导的专制意识形态。极权社会是现代社会的产物,古代社会缺乏对社会进行全面控制的技术手段,因此,除了少数城邦国家,不能形成极权社会。

科学技术的高度发达,为人们带来新的极权主义威胁,这就是“数字极权主义”或者亦可称为“科技极权主义”。在大数据等科技条件下,如何善加利用技术进步带来的便利与效能,同时防止个人自由的流失以及社会走向封闭,让不利于人民而只有利于统治者的局面形成,成为世界上许多民主国家关心的问题。例如,在美国,有人警告说:“我们以为政府暗中监视公民只是为了抓获恐怖分子,但我要告诉大家,对一个进步主义政府来说,还能从其中获取更多利益,如果政府已经变成一个小偷,那么监控不过是窃贼的行为而已。换句话说,监控表示我们的政府正在踩点。政府正在收集相关目标资料,其方式与电影《十二罗汉》中的窃贼如出一辙:在赌场内踩点,然后便动手抢劫。政府通过监视对公民们加以控制,同时还可以打击那些反对政府实施盗窃的人。总之,美国政府正在组织力量,不仅是为了对公民系统性地实施盗窃,也是为了能够使用恐怖手段对付他们——如果他们胆敢反对的话。”^[17]

科技手段为数字极权国家的形成提供条件,科技警察国家也会同时形成。警察具有保障人民安全、促进人民福利、改善社会治安等重要而积极的机能,为国家与社会不可缺少的公共机制。不过,警察权如其他国家权力一样,很容易被滥用。特别是,基于这种权力的性质,与其他国家权力相比,它更容易走向暴虐与专横。人们常将警察国家与纳粹德国联系在一起,德国具备一个警察国家的许多特征,人们对于“警察国家”怀有恐惧,希望通过完善刑事诉讼程序来规范警察行为,以防止暴力、威胁、引诱、欺骗等非法方法取证,通过全程录音录像、律师介入以及司法令状制度、司法审批等方式对警察权加以控制,防止“秘密的暴力”。在现代法治社会,“警察国家”已经成为历史的一个梦魇,尽管如此,人们仍需要时刻警惕,并注重以司法权来抑制警察权,避免过去的“警察国家”借助新的科技手段再度形成,正是当下司法制度与诉讼程序的使命。

我国当下技术应用的重心在控制犯罪,正是前文揭示的新技术手段在控制犯罪方面发挥的令人惊叹的作用,激励侦查机关和社会管控部门加快了技术应用的步伐,并从技术应用的结果中尝到甜头,这种技术应用也迅速成为国家和社会治理现代化的组成部分。

不过,也许不久的将来这种技术应用的犯罪控制思维将会向正当程序思维转移,刑事侦查学、治安学的技术应用倾向必然与刑事诉讼法、刑事证据法的权力规范功能结合起来,刑事诉讼法学中的科

学技术程序规范问题必然成为一种“显学”。这种趋势的必然性原因有五:

一是技术具有两面性,我们不能只看重一面而忽视另一面,“技术在带来福音的同时,也是一种危险——确实,作为一种既是仆人又是主人的存在,技术‘进步’从人类文明的角度来看,或许从根本上来讲是一种退步”^[18]。种种事实表明,“技术的发展对社会福利的影响是不特定的,这就解释了为什么很多人认为技术的发展‘难以控制’,并把我们的未来带向不一定有利于社会福利净增加的方向”^[18]。

二是国际社会对于数字极权主义给予足够警惕的观念必然向中国传递,我国跻身世界法治文明国家之林,对于民主世界的这一关切不能有所隔膜,因此我国对于新科技应用带来的权力性质的变化也会有所警惕。

三是宪法“尊重与保障人权”的庄严承诺使我们在进行技术应用时不能不进行人权考量,也就是对于新技术应用需要进行人权审查,这是落实宪法原则和迈向现代法治国家的必要条件。

四是民众获得科技应用的便利(包括通过查缉犯罪人为受害人和一般民众带来的满足感)的同时,也会对隐私权、信息安全等问题产生高度敏感,由此引发的社会不满会增加,导致社会情绪的发酵,乃至影响社会安定,这势必引起立法者和司法者的关切。

五是刑事诉讼法既是一种授权法,也是一种限权法,现代刑事诉讼法的限权功能更重于授权功能,不仅如此,授权之时在划定权力边界意义上也会具有有限权功能。刑事诉讼法学对于新的科学技术应用于司法,思考的重点不在控制犯罪而在正当程序。当大数据与智能司法为越来越多的刑事诉讼法学者所重视,这方面学术研究的正当程序之维将得以彰显。

从上述五个原因可以得出结论:大数据与智能司法的正当程序问题是绕不过去的重要法治问题。

四、数字技术应用下隐私权和信息安全的保障

防止国家权力失去制衡进而危及个人的自由权利,并不是一个新鲜话题,在启蒙思想家的论著中,已经有了太多的言说。这些言说在科技进步的今天,重新变得清晰和尖锐,这是因为技术进步带来了反面乌托邦的可怕前景。有论者尖锐地指出:“当互联网发生改变,变得越来越像控制的工具时,我们表现出的将是一种人性的基本特征:鲁钝。大型动物总是被非常不结实的围栏控制住,而我们就是大型动物。对我们中的大多数人来说,大多数情况下,在网络空间结构内部的规则就等于我们发现的那些限制。经过大量学习,我们才会发现,其实规则是人定的。我们能够也理应——抵制这些限制。”^{[14]233}

目前,防止国家权力添上科技的翅膀走向失控的基本做法,业已包含在过去已经实行的、体现人类智慧的制度之中了。人民主权原理、权力制衡原理等宪法基本原理为人们应对技术进步带来的负面政治与法律的影响提供了逻辑起点。在立法、司法领域已经证明行之有效的制约立法权、司法权、行政权等的制度,势必在新的技术条件下继续发挥作用,其中包含立法过程的民主性,以及对于行政权的司法审查制。

在大数据应用等智能化司法中已经有若干引人注目的立法例或者判例,立法方面的例子有:2019年5月14日,美国加利福尼亚州旧金山市通过立法禁止当地警方及其他市政机构采用面部识别技术。该日市立法机构监事会(Board of Supervisors)以八票对一票通过了《停止秘密监视条例》,该决议经旧金山监事会形式性的第二次投票通过后,在6月发生效力。该法案广泛禁止包括警察机构在内的53个市政部门使用人脸识别技术,并为限制监控设施及操作设定了严格的审批程序:市政机构如果想要引入监控技术或者服务,需要向监事会提出申请,说明这样做的理由和使用方法,监事会批准后才能实施。旧金山市政府还需要就监视设备和服务以及遵守既定要求的情况(包括数据存储和删除情况)提出年度报告,接受监督^[19]。这一法案显示了人脸识别技术的实际应用在美国存在争议,该法案使旧金

山成为全球首个通过立法禁止人脸识别技术应用的地区。

旧金山禁止政府机构采行人脸识别技术和限制监控技术应用的作法,揭示在美国围绕该技术应用的问题存在忧虑,人们担心这项技术的应用如不加以限制与规范,政府就会获得空前的权力来跟踪、事后调查人们的日常生活,从而使隐私权将成为历史,这与自由、民主的基本价值不相容。

美国学者爱伦·艾德曼、卡罗琳·甘乃迪著有《隐私的权利》一书,在该书的序言中,他们指出:“隐私权涵盖了许多层面:它保护创造性思维所需的独处生活;它让我们得以独立,那就是维系家庭的重要部分;它使我们的居住和财产得到保障,确保政府公权力不会任意干扰我们。隐私的概念亦涵盖了我们的决定如何自我定位。即使我们居住在一个嘈杂的自我告解的世界里,隐私权使我们得以保留一些秘密不为人所知,如果我们这么选择的话。如此一来,隐私权似乎使我们更文明一些。”^[20]科技手段的司法应用危及隐私权的事实毋庸置疑。例如大数据司法中数据信息的收集许可及所有权、控制权归属,是一个值得关注的问题。当今社会,存在一个矛盾现象,一方面是人们的隐私权得到强化,另一方面危及隐私权的技术手段应用越来越普遍:各种社交软件的应用、定位软件或定位功能的使用,使个人位置被暴露,对于隐私保护来说是一种严重的威胁。关键是,对于公民的个人信息,政府在说明情况下才能采集和分析以及使用,不能随心所欲。这是因为,隐私权具有保障个人其他自由权利的作用。

与大数据有关的隐私,称为“资讯隐私”。许多执法机构和商业机构在日常性采集人们的信息,“我们拥有行动电话,它与无线电话不同,也与我们过去想象的电话不同。我们担心电子邮件、有声邮件和垃圾邮件,还有一种称作‘截波晶片’的晶片(特别被制造用来让政府得以窃听编码的电子通讯),显然是民众最大的威胁”。值得警觉的是,“电脑改变了一切。如果每一个微小的电晶体都有惊人的储存能力,更多的资讯将可以保存得更久。这种资料将无穷无尽……如果我们还没有意愿提供这些个人资料,新科技已经为我们提供了很多”^[21]。对于大数据的司法应用涉及的隐私权的保护,首先需要的是意识的增强,“依据隐私的观点,我们正处于这场大变革中最混沌的时期。对许多人而言,科技是陌生而令人恐慌的。更重要的,隐私的问题已与过往大不相同,并没有一套解决这一问题的架构。科技变动快速;而法律,依据个别案例,或烦琐立法过程微量的建构,变动缓慢。因此,现今并没有一套全面性的法律专门处理数位时代中产生的隐私问题。”^[21]

一个国家是不是民主和自由的国家,可以藉由隐私权保障的广度与强度来判断,隐私权以及其他个人自由的保障情况折射出了一个国家或者社会的民主与自由程度。因此,与大数据司法应用密切相关的隐私权保障的根本问题是,如何推进和维护国家与社会的民主性以及对于自由价值的尊崇。民主机制是自由的保障机制,促进民主机制的形成与成熟并防止国家或者社会向威权乃至极权的方向倒退,是保护包括隐私权在内的个人自由权利的根本对策。

新科技手段在监控方面具有比《一九八四》描述的电幕更加有效的特征,这是因为“你无法看见,也无从得知资料的收集过程。监视源源不断,却无法透明。不会有机器让你知道它在看你,也不会有密探对你步步紧逼。监视除了对那些真正了解网络运作原理的人之外,都是无形的。而那些了解实情的人自然只是一个很小的群体。监视在你想要访问的任何网络蔓延,无时不在,无处不在”^{[14]229}。针对这一监视具有的隐秘性,增加资讯采集和使用的透明度,是保护个人隐私权和信息安全的重要步骤。因此,相关思考是,在资讯领域应当加强资讯采集及其使用情况的透明度。这样做的效果是,“公开透明的机制免除了奥威尔的另一担心:科技滥用。如今摄像镜头体积更小,价格更便宜,它们的普及程度是当年的奥威尔想象不到的,但是它们的大批量应用并没有导致奥威尔曾经预言的极权效果,这可能是因为如今我们努力使镜头既朝向公众,又朝向掌权者”^{[16]238}。

不仅如此,掌权者进行资讯采集和使用的情况,要向资讯所有权和使用权以及资讯涉及的其他人公开;不宜公开的资讯,也要向法官等特定人员定向公开或者在法庭调查的专门场合予以公开。资讯采集和使用的透明度,有利于相关人实现知情权并寻找获得司法救济的机会。

隐私权保护,在司法领域,需要依靠传统的权力制约方法加以实现。传统的权力制约方法仍然是行之有效的办法,表现为:一方面,需要立法加以规范,一些国家或地区陆续出台一些保护性措施就是以立法权来实现权利保障;另一方面,需要法官依据司法令状制度加以制约,在隐私权保护方面已经有许多判例,涉及执法、媒体等诸多方面,与智能化司法相关的判例也在司法实践中产生出来。一些国家或者地区的法官在个人的隐私权保护方面继续扮演好“自由的屏障”的角色。

在我国,科技发展为社会生活带来了许多变化,也为政治和司法发展增添了助力,大数据的司法应用以及司法智能化的塑造,就体现了这一变化。与此同时,隐私权观念原本不强的我国社会,随着社会的发展进步,逐渐提升了隐私权观念,这两个方面的变化如何协调,成为立法与司法以及法学研究需要共同面对的问题。

在保障公安司法机关借助这一条件实现查缉犯罪人、遏制犯罪和稳定社会秩序的同时,对政府利用这些大数据加以必要的限制,防止科技能力不适当地侵害公民自由权利,理应成为相关立法与司法的重点之一。

其一,在立法方面,资讯所有权与使用权以及相关保护的立法工作应当积极展开,就此有人提出“数权”的概念,研究并推动《数权法》的立法。在这一方面,相关司法制度的建构显得越发重要,在司法领域的科技应用中实行司法令状制度,是完善司法权制约侦查权制度的重要举措,需要立法机关作出努力。毫无疑问,科学技术的发展应用相关的法律制度应该跟进,涉及电子监察方面的司法控制、数据采集运用等方面的司法控制,以及手机追踪定位方面的司法控制都要一一加以实现。

其中,对于科技定位进行追踪监视措施,目前有些国家或地区在这方面已经取得进展,值得我国认真研究和借鉴。例如,科技定位措施侵犯公民基本权利,受害人可以寻求的救济途径:一是通过国家赔偿制度加以赔偿,二是通过刑法设定的相关罪名加以追责,三是通过行政诉讼途径进行救济^{[13]331}。

借鉴这些做法,在我国,要通过立法防止科技能力不适当地侵害公民自由权利。

1. 需要立法划清合法与非法的界限,从而使“违法”的概念得到厘清,为救济手段提供前提。我国已经制定和颁布《个人信息保护法》,涉及个人信息的收集、存储、使用、加工、传输、提供、公开等多个方面。有论者提出:“一些地方、企业和单位滥用人工智能、大数据特别是人脸识别等新技术,无序、任意采集使用乃至泄露敏感个人信息的问题愈演愈烈,有必要从法律上对敏感个人信息处理的源头加强规制,强化保护,并提出比个人信息保护更严格的要求。”为此建议:“除法律、行政法规规定和维护国家安全、公共利益外,敏感个人信息的采集与使用,应当报履行个人信息保护职责的部门备案审查;极度敏感个人信息的采集与使用,应当取得相关行政许可。”^[22]还有人特别建议针对人脸识别技术被滥用且比较普遍的情况进行相应的立法限制。笔者认为,对于个人信息的侵犯,不能不顾及其侵犯者不仅是一些非公权力机关,还有很多公权力机关,包括公安司法机关,所以对于个人信息保护的公权力来源也应进行法律规制,不能顾此失彼。因此,在已经制定的《个人信息保护法》的基础上,应当专门制定“通讯监察法”之类法律,为个人信息和通信自由提供进一步保护,尤其是在刑事司法领域的保护。

2. 采取科技手段监听、追踪和大数据采集等行为,应立法设立事后告知制度,监听、追踪和大数据采集等的人应有权事后知晓被技术侦查等情况,以保障其寻求救济所需要的知情权。告知义务的设定:一是保障权利被侵害人在知情权基础之上的司法救济机会;二是提升科技手段行使机关的谨慎度,防止其滥用手中的科技手段侵犯个人的合法权利。

3. 完善国家赔偿制度,明确将违法的科技手段进行的司法行为纳入赔偿范围。我国《国家赔偿法》中的行政赔偿和刑事赔偿范围尚不包括采取技术手段非法进行监听、追踪和大数据采集等行为,为此《国家赔偿法》应当从行政赔偿和刑事赔偿两个方面为科技手段违法行政或司法的被害人提供赔偿,并以此促使有关机关以法律的正当程序约束手中的科技手段。

4. 完善《刑法》相关罪名及其司法应用,为保护人民不受非法技术手段的侵犯提供刑罚权保障。此外,对于非司法性质的科技监听、追踪和大数据采集等政府行为,提供给被侵害人以行政诉讼的救济途径。这是因为对于隐私权等权利来说,“‘法律的保护’不仅要求在私法和行政法领域采取相关措施,而且还要求在刑法中规定最低限度的禁止性规范,无论这是为了保护性方面的完整性、通讯或电讯的秘密还是荣誉”^[23]。我国《刑法》第253条之一规定了侵犯个人信息罪,从刑法这些规定看,公权力机关在行政和司法中“窃取或者以其他方法非法获取公民个人信息”是否可以该罪名定罪,显然并不明确。《刑法》应从保护人民不受公权力机关非法技术手段的侵犯方面周密考虑《刑法》罪名的设定及其具体应用,为刑罚手段规范这一领域提供立法条件^[24]。

其二,在司法方面,法院在行使司法权维护个人自由权利方面还有许多潜力可以施展。这需要调整司法体制加以配合,公、检、法三机关的关系如果能够形成切实有效的制约关系,并依靠优良的司法程序,使得具有独立、中立、合格的基本素质的法院发挥好约束政府权力的作用,在国家信息安全受到重视的同时也使个人信息安全得到有力保障,则公民的隐私权在很大程度上可以获得保全。我国法院的司法独立性和权利保障意识都需要进一步增强,才能扮演好维护司法人权的重要角色,缺乏这一前提,许多法律权利的保障就可能成为空谈。

其三,检察机关在大数据应用领域也可以发挥积极作用。由于个人信息安全关联着国际人权法和宪法允诺保障的通信自由、隐私权、言论自由、居住安全、人身自由等多项基本自由权利,对于个人信息安全的保护,成为其他一些基本自由权利保障的必要条件,这些具有普遍意义上的权利当然具有公益性质。代表公共利益的检察机关应当密切关注这类案件,以公益诉讼或者其他司法手段如刑事诉讼法赋予的监督职权维护个人自由权利,以实现隐私权的多元保障制度。

参考文献:

- [1] 理查德·萨斯坎德. 法律人的明天会怎样?——法律职业的未来[M]. 何广越,译. 北京:北京大学出版社,2015:62.
- [2] 邹锦涛,张璇. 基于大数据的网络社交媒体情报预测分析[C]//赵志刚,刘品新,缪存孟,等. 检察大数据. 北京:中国检察出版社,2018:75.
- [3] 赵志刚. 大数据与检察工作[C]//赵志刚,刘品新,缪存孟,等. 检察大数据. 北京:中国检察出版社,2018.
- [4] 刘品新. 大数据司法:创新与实践[C]//赵志刚,刘品新,缪存孟,等. 检察大数据. 北京:中国检察出版社,2018.
- [5] 李振. 浅谈大数据挖掘[C]//赵志刚,刘品新,缪存孟,等. 检察大数据. 北京:中国检察出版社,2018:124.
- [6] WRIGHT M. Big Data and the Fight against Financial Crime[EB/OL](2019-12-9)[2021-4-30]. <https://www.refinitiv.com/perspectives/big-data/is-big-data-being-handcuffed-in-the-fight-against-global-financial-crime/>.
- [7] 龙卫球. 人工智能立法规范对象与规范策略[J]. 政法论丛,2020(3):95-106.
- [8] 卫跃宁,袁博. 守定与融合:大数据时代的刑事诉讼方法论省思[J]. 浙江工商大学学报,2019(1):6-15.
- [9] 佚名. 电脑量刑能主持正义吗?[J]. 时代潮,2004(12):37.
- [10] 赖默尔·格罗尼迈尔. 21世纪的十诫[M]. 梁晶晶,陈群,译. 北京:社会科学文献出版社,2007:221.
- [11] 季美君,王燃,姚石京,等. 大数据时代检察机关遇到的挑战与应对[J]. 人民检察,2017(15):11-17.
- [12] 高扬捷,吴美满,黄彭亮. 大数据技术在金融检察工作中的应用[C]//福建省检察官协会. 海峡两岸检察制度研讨会(2018)交流论文汇编,2018:276.
- [13] 黄清德. 科技定位追踪监视与基本人权保障[M]. 台北:元照出版公司,2011.
- [14] 劳伦斯·莱西格. 论互联网及《一九八四》的良性侵犯[C]//阿博特·格里森,玛莎·努斯鲍姆,杰克·戈德史密斯. 《一九八四》与我们的未来. 董晓洁,董玮萍,译. 北京:法律出版社,2013.
- [15] 刘艳红. 民法编纂背景下侵犯公民个人信息罪的保护法益:信息自决权——以刑民一体化及《民法总则》第111条为视角[J]. 浙江工商大学学报,2019(6):20-32.
- [16] 大卫·布林. 带有“自身阻断性”的预言——为什么噩梦能帮助制伏未来的危险?[C]//阿博特·格里森,玛莎·努斯鲍姆,杰克·戈德史密斯. 《一九八四》与我们的未来. 董晓洁,董玮萍,译. 北京:法律出版社,2013.

- [17] 迪内希·德·索萨. 一个国家的自杀[M]. 小小冰人, 译. 成都: 四川人民出版社, 2015: 243.
- [18] 理查德·A·波斯纳. 奥威尔与赫胥黎: 经济学、技术、隐私与讽刺文学[C]//阿博特·格里森, 玛莎·努斯鲍姆, 杰克·戈德史密斯. 《一九八四》与我们的未来. 董晓洁, 董玮萍, 译. 北京: 法律出版社, 2013: 196.
- [19] 曾佳. 美国旧金山禁止市政部门使用人脸识别技术, 防止权力滥用[EB/OL]. (2019-9-2) [2021-3-29]. <http://www.bfxll.com/archives/view-15000-1.html>.
- [20] 林子仪. 资讯与生物科技时代的隐私权难题[C]//爱伦·艾德曼, 卡罗琳·甘乃迪. 隐私的权利. 吴懿婷, 译. 北京: 商周出版公司, 2006.
- [21] 爱伦·艾德曼, 卡罗琳·甘乃迪. 隐私的权利[M]. 吴懿婷, 译. 北京: 商周出版公司, 2006: 439-440.
- [22] 张伟杰. 全国人大常委会分组审议个人信息保护法草案任意、无序采集人脸等个人信息需严管[N]. 工人日报, 2021-5-6(7).
- [23] 曼弗雷德·诺瓦克. 《公民权利和政治权利国际公约》评注[M]. 孙世彦, 毕小青, 译. 上海: 三联书店, 2008: 397-398.
- [24] 刘仁文. 论非法使用公民个人信息行为的入罪[J]. 法学论坛, 2019(6): 118-126.

Application of Science and Technology in Justice: Observation and Analysis from Two Dimensions

ZHANG Jianwei

(School of Law, Tsinghua University, Beijing 100084, China)

Abstract: The judicial application of big data has two sides. The researches on relevant issues in China mainly focus on how to use scientific and technological means to combat crimes in the field of cyber-crime. There are few researches and discussions on the limitation of government power and the related legal due process. This paper attempts to discuss the two dimensions involved in the judicial application of big data from two aspects: one is the dimension of crime control, the other is the latitude of due process. Both of them reflect the concept of justice in their respective meanings. The author analyzes relevant judicial technical issues, in the meantime, points out that as judicial authorities in China, courts and procuratorates still have a lot of room to expand the judicial control of investigation power, and the application of big data provides a new opportunity for judicial authorities to strengthen the control of investigation power.

Key words: big data; crime control; judicial review; due process; digital totalitarianism



(责任编辑 张伟 郑英龙)