大数据时代侦查权的扩张与规制

胡 铭 张传玺

【摘 要】大数据时代下侦查活动正在经历着深刻的变革。基于对犯罪活动的有效治理目标,大数据基础设施建设、侦查权外溢等方面显示出侦查权的显性扩张;同时,侦查节点前移、数据收集泛化、分散式立法等层面上也逐渐显现出侦查权的隐性扩张脉络。大数据时代的侦查权扩张存在现实合理性,但也带来了法律制度上的规制困境和公民权利保护的难题。应理性看待大数据时代侦查权的扩张,纳入刑事诉讼法的现有体系,按照强制性程度分类进行规制,从长远来看,应通过专门立法集中规制大数据时代侦查权的扩张,还需要调和国家治理逻辑与司法自洽逻辑的内生冲突。

【关 键 词】大数据时代;侦查权;刑事司法;国家治理

【作者简介】胡铭(1978-),男,浙江乐清人,法学博士,浙江大学光华法学院常务副院长,教授,博士生导师,浙江大学国家制度研究院研究员,教育部“青年长江学者”,研究方向:刑事诉讼法学、司法制度;张传玺(1992-),男,江苏徐州人,浙江大学光华法学院博士研究生,研究方向:刑事诉讼法学(杭州 310008)。

【原文出处】《法学论坛》(济南),2021.3.5~14

【基金项目】本文系国家社科基金重大项目《深化司法体制改革和现代科技应用相结合的难点与路径研究》(18ZDA137)的阶段性成果。

大数据时代的到来令网络信息生活成为民众基本的生活方式,传统的治理手段已经无法有效应对复杂性、风险性和时代的挑战。[①]据中央政法委统计:“中国网络犯罪已经占到犯罪总数的1/3,并以每年30%以上的速度增长”,[②]且近年来已成为第一大犯罪类型。绝大多数刑事案件的涉网背景将侦查工作推到了科技战场的最前线,而犯罪在科技时代层出不穷的变化,使得侦查机关不断产生扩权的冲动以应对新的犯罪形势。

从社会变迁和刑事司法的发展轨迹来看,现代侦查权的扩张总是和公民权利保障的强化及法律制度的完善相伴相生。其中,我们需要认真思考的是侦查权扩张对正当程序的冲击以及法律规范如何更好的回应这种挑战。大数据时代的社会是一个信息社会,也是一个风险社会,大数据及大数据技术在刑事侦查活动中的运用是信息技术革命给刑事司法带来的红利,也必然带来新的风险与挑战。我们应当更加理性地看待这种时代背景下侦查权的扩张问题,如大数据技术发展带来的可能性与依法治国原则下侦查权的应然边界,社会公众的现实需求及外部评价与公安司法机关办案的内在需求等。既要看到大数据时代侦查权扩张的内在合理性,又要面对侦查权扩张的实践带来的法治困境,这便需要我们在理性认知的基础上,对大数据时代侦查权扩张的实践样态及其背后的机理,侦查制度的变革及其边界等问题进行深入思考。

一、实践样态:侦查权扩张的两类新趋势

大数据时代侦查权的扩张并不能等同于所谓的大数据侦查。从广义上理解,大数据时代的侦查并不意味着以数据库为必要条件,数据库建设只是大数据时代侦查模式变更中的一种重要实现方式,公安机关以实现犯罪预防和社会秩序稳定为主要目

标，进行各类数据库建设，法律法规也基于上述目标，通过制度性设计，在立法上保障公安机关基于公共利益的前提下获取外部政务数据和民用数据。学界目前对于何谓大数据侦查，仍有争鸣，[③]但整体上均认可大数据在侦查实务中扩张了侦查权限，对公民的基本权益亦带来了相当程度的侵害风险，并应当予以规制。显然，大数据确实给侦查权的运行带来了众多变化，实践中大数据背景下侦查权也正在呈现出显性扩张和隐性扩张两类新趋势。

(一)侦查权的显性扩张

1.扩张基础：大数据基础设施建设。金盾工程、天网工程和雪亮工程是我国当前涉及公民个人信息的社会治理基础设施建设典型，但在数据采集类型、程度上各有其侧重。金盾工程，又称公安通信网络与计算机信息系统建设工程，主要目的在于实现公安机关整体的信息化架构建设。其一期工程主要集中在公安基础通信设施和网络平台建设，二期工程的建设重点开始转向信息资源的管理与共享，即在信息化平台的基础上，进行数据资源库的建设与使用。金盾工程建设的全国类数据库包括八大主要信息库和上千类子信息库，[④]促进了信息化系统的深度应用，以为基层实战服务为核心目标。天网工程是公安机关为了有效打击犯罪，在城市的交通要道、繁华地区、治安卡口、公众聚集场所、宾馆、医院等地方安装的实时监控系统。通过监控可以得到实时的影像资料，并可以实现图像的传输监控、显示等用途，以实现对城市的治安监控和管理，可以有效地预防犯罪、打击犯罪。[⑤]总结来看，天网工程主要是针对城市地区的视频全覆盖监控，视频是一种非结构化的数据，虽然不如数据库中结构化数据的查询效率，但是安防技术已经可以实现对视频中人像的识别，因此天眼工程在实际效果上已经成为一种城市整体信息监视大数据库。雪亮工程则是农村地区的视频覆盖工程，是天网工程在地理位置上向乡村地区的延伸。

金盾工程、天网工程和雪亮工程，充分体现出我国当下的风险社会治理逻辑——充分运用现代科技手段构建数据基础设施，提高治安管理水平和打击刑事犯罪的效能。此类数据基础设施建设确实取得了一定程度的成功，近年来我国重大犯罪案件的下降有相当一部分原因可归功于此类数据资源平台的建设。[⑥]但此类数据基础设施对民众的基本信息收集已经呈现出一种大规模的监控趋势，其在建设、运行和使用上由于缺乏民众参与和透明性，合法性也受到了批评。还有研究发现，域外不少城市大规模视频监控系统在刑事案件侦查上的作用被验证多为“寒蝉效应”，是一种犯罪的事前恫吓，事后侦查利用作用则甚微。[⑦]

2.侦查主体的扩张：积极主体与消极主体。侦查权的行使中，可以从三个层面确定侦查主体。一是法定性，只有国家或地区的法定侦查机关才有权进行侦查活动，[⑧]我国《刑事诉讼法》第108条也明确规定了我国侦查主体主要为公安机关和检察机关，除法定侦查主体外，其他机关团体个人均无权行使侦查权。二是实际控制性，基于司法协助或者辅助，非法定主体提供犯罪预防与治理相关信息给侦查机关，难以一概而论其活动是侦查行为，应当视侦查机关对此类主体的控制强弱程度而有所区别，如果侦查机关处于完全支配的地位，此时可以说协助主体是“国家机关侦查手臂的延伸”，那么协助主体的行为属于国家追诉行为的一环，应当受到取证规范的约束。[⑨]三是实质业务内容判定，该行为是否是基于犯罪预防和犯罪治理而进行的取证、保全行为。

大数据时代，技术的专业性让第三方主体顺势进入侦查主体建设中，这是技术红利转化成司法红利过程中不可避免的侦查权力外溢现象，主要有两种形式：积极参与主体和消极参与主体。积极主体指平台建设的第三方参与建设主体，消极主体指立法上的协助义务主体。前者如与深圳市公安局合作共建“网络远程勘验与取证实验室”的某网络技术公司，这类是以主动参与公权大数据侦查平台建设的企业为主体；后者如我们熟悉的各大互联网公司，基于《刑事诉讼法》第52、54条规定，作为被动履行协助义务的主体，以自身的数据平台为侦查部门提供协助或便利。同时，某些掌握了海量民众基本生活信息的商业公司兼具积极和消极属性，以腾讯为例，其已经与全国诸多省市公安机关建立了战略框架协议，双方将“强强联合，整合资源，充分运用腾讯的大

数据基础，成熟的云计算能力和微信、QQ等社交平台产品……推动互联网、大数据与公安机关打防管控、便民服务等警务工作的深入融合发展。”[10]从国际范围来看，当前世界各国一般认为服务商基于隐私权保护所产生的保密义务，不足以阻却侦查机关获取相关信息的要求。当然，在我国，也有很多商业数据公司愿意配合侦查机关进行资源的合作共享，而域外更多的是大型互联网通讯商和侦查部门的互相博弈，立法和技术上同时进行。

(二)隐性扩展脉络

1.侦查启动节点的前移：初查措施的强制性与立案的虚化。刑事立案是侦查的开始，也是侦查权启动的前提，采取强制性侦查措施只有在立案之后才可以进行。实践中，侦查部门接到的报案、控告、举报材料仅通过书面审查难以确定是否达到立案标准，因此对案情进行初查是具备现实合理性的。但伴随着立法对初查阶段相关手段获得的证据的容忍态度，以及大数据时代侦查技术带来的不断升级的强制性侦查措施内涵，初查阶段的法律风险将会越来越多，犯罪嫌疑人的权益保护也将面临极大隐患。《公安机关办理刑事案件程序规定》第171条和《人民检察院刑事诉讼规则》第169条对初查可采取措施做出了规定，公安机关可以“依照有关法律和规定采取询问、查询、勘验、鉴定和调取证据材料等不限制被调查对象人身、财产权利的措施”，检察机关除上述措施外，列举了一些禁止性规定，包括“不得查封、扣押、冻结初查对象的财产，不得采取技术侦查措施”。但是，传统的初查措施在大数据技术的帮助下带有诸多强制性侦查的色彩，大有突破现有法律规定的趋势。例如，电子取证是大数据技术融合传统侦查措施的主要场域，在电子证据收集过程中，因大数据技术手段的运用，执法部门往往出现“以侦查技术之名行技术侦查之实”，如网络行政执法中的打击盗版和色情直播的泛洪攻击[11]和大数据技术中的DNS欺骗以及会话劫持[12]。再如，2016年最高人民法院、最高人民检察院、公安部《关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》和2019年《公安机关办理刑事案件电子数据取证规则》中的网络在线提取、网络远程勘验等侦查措施，本质上就是进入特定的计算机信息系统中寻找犯罪线索，进行查询勘验以保留犯罪证据，虽然初查阶段可以进行查询勘验，但这种远程的大数据收集、搜索行为在形式和实质上往往和技术侦查难以区分，这便深刻改变了传统的勘验检查、搜查等措施的规范内涵。[13]实践中，初查阶段对这些大数据技术辅助下的侦查措施的使用，已经出现了在审批程序上的“补位审批”现象，将实质上审批层级高的侦查措施变相适用低审批标准，将强制性措施在立案前就赋权给侦查人员，导致立案制度的虚化。

2.数据收集目的错位：风险社会治理与大规模监控。大数据时代，公民个人信息的收集应当符合比例原则。以风险社会治理的目标进行数据收集存在目的合理性，但是在打击犯罪为目的的情况下，收集数据信息的执行主体以及后续对数据信息的使用主体均为公安机关，将会带来对数据收集行为的法律性质判断难题。当公安机关基于社会治理进行数据收集时，这种行为在法律定性上属于普通的社会治安管理下的行政执法行为，但如果是基于打击犯罪目的进行的信息收集行为，则属于犯罪侦查行为，而这两者很难严格界分。一般认为，类似于城市大规模公共空间监控、网络公开执法巡查等不属于对公民隐私权的侵害，即便是存在侦查行为，也属于任意性侦查的范畴。但实践中，公安机关具有二元职能属性，行政执法职能与刑事侦查的职能混同现象在大数据时代的犯罪治理中较为常见，往往出现公安机关行政执法过程中采取强制性措施的现象，大数据技术的运行加剧了职能混同现象，而两种不同属性的行为，在启动程序、审批程序、执行方式与主体上均面临着不同的法律规制。

公民敏感信息的常态化收集，并不符合风险社会治理目标下数据收集的必要性原则，会带来数据收集目的的客观错位。在数据的收集使用上，因疫情而产生的健康码是大数据时代数据收集而产生良好社会治理效果的一个典型，但是随着疫情防控常态化进行，数据的收集渐渐呈现出一种敏感信息收集常态化的特点。2017年最高人民法院、最高人民检察院《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第5条将侵犯公民个人信息按

情节严重程度大致划分三类：一是绝对敏感信息，包括行踪轨迹信息、通信内容、征信信息、财产信息；二是相对敏感信息，包括住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息；三是上述以外的其他普通信息。健康码是通过输入自然人姓名、身份证号、联系电话、健康情况、地理位置及行踪等大量个人真实数据为基础，依托大数据、人工智能技术而生成的申请人单独享有的个人二维码，[14]这些信息涉及上述公民的三类敏感信息。当健康码收集成为一种常态，健康码背后所涉及的各类公民敏感信息，在低层级的法律授权、高敏感性的适用场景下，大数据技术可能会让其成为另一种形式的高危人群犯罪地图，成为一种建立在公民个人信息监控之上的犯罪治理工具。

不同于我国基于治安管理的大规模信息收集实践，多数西方国家把监控类信息收集行为纳入技术侦查的规制范畴，虽然各国此类数据信息的收集在实体范围、执行场域、执行具体方式有所不同，但整体而言，均对信息收集行为认定为强制性行为，予以严格规制。例如，根据德国联邦宪法法院对《德国基本法》第13条的解释，对私人和住宅、公共商场等商务场所的监控，收集私人信息和公共场所的大规模监控，必须是基于“已然犯罪”才可以进行，且需要采取技术侦查的规制程度，否则即便是法官司法审查后予以同意进行收集证据的搜查行为也属违宪。[15]那么举重以明轻，如果仅基于治安管理的目的，应不可以大规模收集私人信息和进行公共场所的大规模监控。但是我国采取“公开”方式，对不特定对象的监控与个人数据信息全面收集，这便容易受到以公共利益为由侵犯公民个人权益的批评。

3. 立法模式解绑权力：分散式立法与模糊性授权。我国大数据收集的立法分散化，且往往是由公安机关主导，通过不断赋权以建立更全面的大数据收集体系。目前的公共数据收集，主要基于治安管理下的行政权限收集，上文所谈到的金盾工程即是基于公共服务的角度、以公安业务范围为限进行收集。公安机关往往通过自我授权，使得大数据收集的广度和深度不断扩展，比如网安警务室建设中规定，互联网通信服务企业凡月活量在10万以上的单位，均需要设立网安警务室，由公安机关入驻直接管理，这种赋权以及设置派出机构的正当性需要仔细考量。在《网络安全法》《刑事诉讼法》《公安机关互联网安全监督检查规定》等上位法或相关规定已经明确了互联网企业在数据留存、数据报送以及基于国安、犯罪侦查目的的数据协助义务后，再设计这样制度的必要性是存疑的。上述做法的主要目的就是更加便利公安机关对数据的直接获取，以便利于后续不管是行政执法还是刑事侦查中对数据的使用，这便留下了数据收集滥用的隐患。

这种分散式立法延续了技术类侦查措施中“模糊授权”以拓展侦查权空间的做法。[16]我国技术侦查在立法规定上，存在实体条件上适用对象较为模糊、审批手续上的“严格性”并不明确、具体执行程序较为宽松的特点。立法体例上，技术侦查以刑事诉讼法的规定为主要法律依据，但涉及“技术”“监控”的场景下，不少相关措施并未纳入刑事诉讼规范当中。从域外立法来看，针对侵权风险较大的监控类措施，多采用专门的明确立法以规范相关的侦查行为。如美国对于执法机关的电子取证和通信信息获取，主要法律大致经历了1986年《存储通信法案》(Stored Communication Act，SCA)、2001年《爱国者法案》(US Patriots Act)、2018年《澄清境外数据合法使用法案(Clarifying Lawful Overseas Use of Data Act，CLOUD Act)》(又称“云法案”)这样的专门立法发展脉络。[17]日本和我国台湾地区也对通讯数据信息的获取设置了专门的立法，以保护民众的隐私权在侦查活动中能够得到合理的保护。类似我国的天眼工程、天网工程这类的大规模公共监控，域外也已有通过专门立法以削弱对公众隐私权侵害的范例。[18]

二、侦查权扩张的现实合理性与法治困境

大数据时代侦查权呈现出显性层面和隐性层面的扩张，但扩张并非都是不合理的，背后有着现实合理性。

(一)现实合理性：推动侦查权扩张的多重因素

1. 国家治理体系和治理能力现代化的新要求。推进国家治理体系和治理能力现代化是中央制定的国家整体发展战略，在这样的顶层设计之下，刑事司法治理体系和治理能力现代化是必然要求，而以大

数据、人工智能等现代技术在司法中运用为代表的改革新举措正是在此背景下快速推进，并呈现出实践先行、制度再予以供给的现象。中共十八届三中、四中全会以来，我国公检法三机关都在加速探索各自领域的“智慧警务”“智慧检务”“智慧司法”建设，出台了诸多独立或者联合的司法信息建设文件，也落地了“206系统”等科技司法新探索。

具备强力应对犯罪的能力是我国政治体制的传统和优势。我国公安体制是一种一元集中下的综合组织架构，这为系统引入大数据侦查等新举措带来了可能性。这种组织架构既是权力结构传统的惯性体现，也是“高效打击犯罪”理念下的民众惯性心理预期互相影响的结果。这导致了公安体制下权力合法性要满足民众打击犯罪的期待，在面对犯罪这种严重破坏社会秩序的行为时，有效快速的处理犯罪活动被认为是“司法为民”的基本功能。当下，新型网络犯罪和传统犯罪的新变化直接带来犯罪治理难度的上升，因此，就不难理解大数据时代在服务社会、治理犯罪的需求下，相对比较宽松的侦查机关大数据收集权优先于严格的公民个人信息保护的制度选择了。

2.对社会变迁的积极回应。大数据时代侦查权的扩张是基于社会治理效率考量而进行的技术性变革。一方面，面对风险社会，警力不足是新常态。作为主要侦查力量的基层派出所的工作内容繁杂，除刑事案件外，众多的社会治安管理事务占据了基层派出所的主要精力，而专业侦查力量薄弱。不但刑侦、经侦专业人才队伍方面缺口大，且在办理疑难复杂案件，特别是大型团伙、涉众型犯罪案件时，办案经验和专业知识不足、警力匮乏问题突出。另一方面，“条块结合”的体制以及地区之间的发展差异，令侦查环节的数据共享、侦查协作开展困难重重。大数据警务基础设施建设则是“向科技要警力”，将基层警力从繁重的传统侦查工作中抽离出来的必然选择。大数据技术给人感观上的“高大上”，容易得到政府层面经费的支持，又能缓解侦查实践中警力资源匮乏的现实。原有的技术侦查手段虽然易操作、成本低，但在实际操作中还不足以应对网络诈骗犯罪等新型犯罪。

侦查权扩张是对大数据时代作为犯罪线索的数据特点以及犯罪全球化特点的回应。一方面，数据的地域属性逐渐模糊，数据的“无地域性”带来犯罪侦查中“跨境取证”的难题。如美国的云法案就是基于这样的背景出现的，在微软诉合众国案中，控辩双方争议的焦点之一就是数据存储地的标准问题，公诉机关希望获取微软存储于爱尔兰的数据，认为数据的地域认定标准应当是“获取地标准”，而微软公司认为数据的地域认定标准应当是“数据的真实存储地标准”，而随着云法案的出台，美国政府相当于认可了公诉机关的标准，赋予了美国司法机关在数据获取上的跨境长臂管辖权限。另一方面，网络犯罪的线上虚拟特点，导致传统侦查措施的针对性不足，只能在传统侦查措施的基础上探索新型的侦查手段。这一点域外早有先例，20世纪末欧盟就已经开始探索网络犯罪的新治理模式，并于2011年通过了《网络犯罪公约》。但这一公约出台时，尚不具备当下大数据技术的发展水平，犯罪场景更多的是狭义上的计算机系统，比如计算机中存在的电子数据，而非当下的“分布式云存储数据”，亦即“云端存储”。因此，缔约国之间只是在国内刑事侦查措施上进行搜查、查封、扣押、冻结或者“相似方式”刑事程序设计，这些立法设计具有相当的前瞻性，虽然没有解决跨境取证的问题，但为现代电子取证中的“网络远程在线提取”“网络远程勘验检查”“网络技术侦查”等基于大数据挖掘技术的电子取证侦查措施确立了合法性来源。

3.绩效考核的内在需要。大数据时代侦查权的扩张契合侦查机关内在需求，特别是绩效考核的需求。侦查机关自身需要通过有效的犯罪控制来实现自身的价值，特别是在法律规定和正当程序日益严格的情况下，大数据监控等新措施的引入为侦查机关办案打开了另一扇窗。通过有效打击犯罪，特别是对于恶性案件和新型案件的破案率提升，能够使得侦查机关在严格的绩效考核体系中获得充分肯定，并且能够得到公众的认可，进而侦查机关自身的地位得以巩固。我们可以称之为侦查权力的绩效合法性。

破案率长期以来都是侦查机关绩效考核的桎

梏，特别是所谓“命案必破”虽然并没有明确的法律或中央文件层面的依据，却始终是侦查机关追求的直接目标。大数据等新技术的引入，使得侦查机关获得了提升办案绩效的新办法，替代刑讯逼供等被严格禁止的旧办法，也因此获得了各级侦查机关的普遍推崇。

(二)侦查权扩张带来的法治困境

1.侦查措施与行政执法措施的混同及侦查措施的技术化。首先，基于社会治理而进行的很多行政执法管理行为有侦查强制性措施的属性。作为网络安全监督检查与执法的主体，我国网络警察负有网上公开巡查的职能，[19]同时接受网民的在线举报，发现并处理相关问题。这种职能之下的网络执法常涉及对网站、论坛、社交媒体、生活类APP的常规巡查。一般而言，学界对于此类互联网公开平台或者通信信息平台的公开巡查，虽有侵害言论自由等权利的批评，但此种形式的公开巡查本质上只是把传统的警察巡逻线上化，并不需要特别规制。[20]只是越来越多的实践表明，网络警察监控网络不良信息在执法方式上存在超职权行使的现象，如网民下载色情影片被网警巡查发现后进行罚款的新闻屡见报端，背后就是网警执法行为的强制化程度严重超过传统的公开巡逻。

其次，侦查场域的电子化带来侦查措施的虚拟化，出现了侦查权行使中刻意规避审批程序的行为，典型的场景即为电子取证。上文扩张样态中初查措施的强制化和立案制度的虚化，背后的真实原因在于传统侦查活动痼疾难消之际，传统侦查行为本身和行使场域的大数据化，在实践与规范上的连锁反应让侦查行为法律控制和立案制度进一步被虚置。大数据时代数据的特点，让网络在线提取和网络远程勘验检查，在实质上超出了传统的勘验这一侦查措施的内容，以勘验之名行搜查、查封、扣押之实。有研究者发现，实务中侦查人员自己也区分不清或者说有意不去区分远程勘验与在线提取，并在更多地使用最狭义的普通在线提取(即通过网络直接秘密复制或下载)进行实际上的远程勘验或者网络技术侦查。[21]而侦查人员进行网络勘验、检查均不需要侦查机关负责人的批准，实施搜查、查封、扣押则需要经过侦查机关负责人批准，这是大数据技术下传统强制性侦查措施的法律性质被刻意模糊带来的审批程序上的回避与漏洞问题。

再次，大数据时代的侦查措施呈现出技术化的特点，与技术侦查的界限日益模糊。技术侦查具有对象特定性、手段秘密性、执行主体特定性、内容涉及高度隐私性等特点[22]，而大数据侦查往往也具有上述特点。虽然我们不能将大数据侦查简单等同于技术侦查，但两者的相似性使得相关法律制度在设计完善时有诸多共通之处。同时，大数据监控等新措施的适用范围显然要超出技术侦查的范围，并且在组织架构上不断扩充、职权管控范围日益扩大、技术样态造成权利干预程度显著上升，这种权力扩张的态势使得即便采取严格的技术侦查程序控制标准，可能也无法有效规制不断扩权的新侦查举措。

2.证据属性定位的模糊性与证明标准的概率化。大数据能够为侦查活动提供重要线索，但如何从证据法上定位侦查中获得大数据，还是一个难题。虽然实务上大数据侦查活动获取线索并最终破案的例子很多，但在司法审判环节有效运用大数据类证据认定犯罪的案例尚不多见，这主要是源自大数据侦查所获得的数据在现有法律体系及证据规则中尚未有明确规定，也就是说大数据并不能纳入传统的证据种类，也就很难在法庭上成为认定犯罪的证据。笔者曾调研某地级市的智慧检务系统，其运用大数据侦查思维对套路贷、虚假诉讼等行为进行大数据分析，以获得犯罪相关线索，再把大数据分析结果移交公安机关进行其他证据收集，取得了良好的效果。但大数据本质上还只是一个概率问题，大数据分析的高概率并不一定就与案件事实相一致，还需要通过收集其他物证书证等传统证据才能对犯罪行为进行认定，最终在审判环节进行定罪量刑所依据的也往往并非大数据分析报告。[23]

大数据的预测性冲击了传统的证明标准。大数据的预测性带来了无罪推定原则的实质性改变，其主要影响在于通过科学技术对基于概率的真实性加以背书，从而进一步加强了侦查人员的有罪推定心理，其关键又在于对“排除合理怀疑”的主观证据标准的冲击。大数据在数据挖掘上带来的无限趋真的

相关性，在主观上重塑了侦查阶段的排除合理怀疑标准。以审判为中心的诉讼制度改革要求“在刑事诉讼的全过程实行以司法审判标准为中心，核心是统一刑事诉讼证明标准”。[24]但侦查实务活动是一个不断提升证据标准并接近客观事实的过程，不可能一蹴而就地达到审判阶段的证明标准。大数据是一种概率，对于侦查人员的心理极易形成某种导向，使得侦查阶段的证据标准概率化，如果将大数据作为审判阶段的证据则更加使得有罪判决的证明标准成为一种概率，这与我国传统的客观标准是有显著差异的。

3.个人信息权的过分让渡与辩护权受限。大数据侦查措施的采用，将对公民权利保障带来直接影响，特别是对个人信息权的冲击最为明显。为了社会责任和控制犯罪，公民个人信息权做出适当让渡，如上文所述是具有现实合理性的，但这种让渡显然不是没有边界的。2020年6月28日提交全国人大常委会审议的《中华人民共和国数据安全法(草案)》，提出国家将对数据实行分级分类保护、开展数据活动必须履行数据安全保护义务并承担社会责任等，是我国在大数据立法上迈出的重要一步。[25]但该法对于公民个人信息保护和侦查机关的权力边界等尚未作出充分规定，还有待《个人信息保护法》的进一步规制。[26]我国立法层面对待数据与个人信息保护的处理导向，一直坚持的是在保障数据安全和充分发挥经济效益下对数据隐私进行保护原则，这是城市大规模监控系统能够落地实施的原因所在，亦是我国立法和西方国家相关立法的主要差异之所在，我国更侧重数据安全，西方国家则更注重个人权利。当然，毋庸置疑的是刑事司法活动中应对公民的个人信息权利加以保障，我国在实体法和侦查程序设置上也进行了相关设计。如《刑法修正案(九)》增设了“侵犯公民个人信息罪”，规定任何单位和个人违反国家有关规定，获取、出售或者提供公民个人信息，情节严重的构成犯罪。但在如何限制侦查机关的权力以有效保障公民个人信息权利方面，尚存在法律规定较为原则、内部规范较为粗糙、规则与实践有较大落差等问题。

辩护权是公民权利重要组成部分，也是公民权利保障的重要倚仗。侦查权在大数据时代的扩张，使得诉讼构造中控方力量进一步强化，而对应的是辩护方实力的相对减弱。不管是数据获取能力还是数据分析能力，辩护方均无法与侦查机关相抗衡，特别是基于数据黑箱，辩护方很难在侦查阶段对大数据侦查措施做出积极应对。[27]目前研究者强调的刑事司法活动中公民个人信息的保护路径，如制度上保障知情权、监控后的告知义务等，最终还是要回归到对辩护权的保障上，尤其是保障辩护律师在侦查阶段的有效介入及其职权行使。

三、侦查权扩张的合理规制：理性认知与制度完善

(一)理性对待侦查权扩张及权力控制

涉及公民基本权利的强制处分采行令状主义，且令状决定权属于法官，是西方国家普遍的做法，这也被称为侦查权控制的“法官保留原则”。但近年来，令状主义正受到批评，如强制处分权尽归法官带来对犯罪追诉“效率不彰”问题；又如大数据时代对电子数据搜查扣押的“无限定搜刮式搜索扣押”，使得令状内容下明确性不足，导致架空令状规制[28]。从域外刑事诉讼发展趋势来看，普遍呈现出一个值得关注的现象，即各国在审判程序设计、证据规则等方面的理论与实践日益发达，而对侦查权的控制却未有显著发展，原有的令状审查也主要局限于启动要件、行使内容与范围，隐约呈现出“公正”对“效率”的让步。

究其原因，首先，在于侦查活动具有形成性。面向未知的活动探索不可能进行过分细致的行为规定，框定在法律条文内的侦查行为细节可能成为犯罪分子进行反侦查的“逆向犯罪指引”。因此，各国刑事诉讼法中对于侦查活动多在“任务指示”和“概括授权”的双重基础上进行“模糊性规定”。其次，侦查活动与司法审查的价值追求有所差异。监督职责下的检察官和司法审查下的法官，在法律事实和程序合法性的司法审查活动的能力上有优势，但法院、检察院并不具有侦查机关那样发掘案件事实的职责和能力。检警关系中，检察官不直接执行侦查行为，也无法对侦查活动进行细节上的把控，检察官只是“刑事进展程序中的过滤器”[29]；法院对侦查行为的令

状审查也只是侦查行为在法律规范上的界限审查。总体来看,法院、检察院在侦查权的控制上以法律规范文本的适用合法性审查为主,这决定了对侦查行为的控制能力不足,其价值追求是为了“公正”而非“效率”。检察院、法院的审查并不促进侦查活动发现真相的能力,而是为了“抑制滥权”。再次,控权有效性不能脱离侦查活动的功能性作用的实现。域外对侦查权的司法审查机制往往是希望在事前或者事中对侦查措施进行法律规制,但即便是对监听等技术侦查措施,实际上也未达到预期的良好结果。[30]反而是事后的司法审查控权模式表现出更积极的作用,通过事后的法庭审判和证据规则适用对侦查权的行使进行合法性审查,这种事后审查并不直接影响侦查机关充分行使侦查权以查明案件事实。

(二)侦查权有效规制的具体路径

1.数据基础设施的建设主体与使用主体分离,数据资源收集主体与使用主体分离。主体上的分离可以发挥以下作用:首先,改变公安机关主导下的数据库建设自建、自用、自批、自执的局面,借助第三方公权力机关如大数据资源局构建城市大数据基础设施,抑制侦查权的过度扩张和侦查启动节点的过度前移。现有法律规范中,基于公共利益(国家安全、犯罪侦查为目的)的数据协助义务打通了政务数据、商用数据和公民个人数据向公安机关的单向流动途径,但是由于侦查机关具有自批自执的支配性力量,无法保障数据的这种单向流动的合法性和必要性。杭州等地已经尝试设立大数据资源局,为数据基础设施的建设主体与使用主体分离提供了可行的思路。[31]其次,这种主体分离的设计,对于如天网工程、雪亮工程等社会大规模监控工程而言,既可以满足犯罪预防的数据收集功能,同时又有利于对数据资源滥用的有效救济。例如,公安自身使用大规模技术监控,往往因职权性质模糊,介于行政执法和刑事侦查之间,而侦查行为的不可诉性令公民权益被侵害时难以进行有效司法救济。相比之下,大数据资源局是行政主体,公民可以通过行政复议、行政诉讼进行救济。再次,对数据的收集主体与使用主体进行“基于犯罪侦查目的使用数据”的主体分离,可以防止侦查机关因为自身的侦查利益而滥用侦查权。如我国台湾地区《通讯保障及监察法》中,对于侦查机关的通讯监听这一类技术侦查就设计了申请、审查、执行的主体分离制度,负责执行通讯监察的建置机关分别为“法务部”调查局通讯监察中心和“内政部”警务署通讯监察中心。[32]

2.纳入刑事诉讼法的现有体系,按照强制性程度分类进行规制。有学者指出,比较好操作的一种方式是在刑事诉讼法“侦查”章第八节“技术侦查措施”中将大数据侦查增列为一种全新的侦查行为加以规范。[33]在此基础上,可按照强制性程度对大数据侦查措施进行分类,区分任意性侦查措施和强制性侦查措施。对于无强制力且对公民个人信息权干预轻微的侦查行为,即仅涉及一般人格权或信息自决权的非强制性干预措施,可纳入侦查机关的一般侦查权限,且可以在初查中使用。对于《国家安全法》《反恐怖主义法》《网络安全法》《数据安全法》等相关法律已经有特别规定,或者是涉及干预宪法所明确的公民基本权利的,不应纳入这里的一般调查权限。侦查机关可以援引一般调查权限收集相关数据,但要受到比例原则的限制。对侦查机关干预公民隐私权、个人信息权和财产权的强侵权性措施,应当纳入强制性侦查措施范畴,比照技术侦查措施在实体范围、程序控制要件和非法证据排除三个主要方面进行控制。这里的程序控制要件又包括审批主体与执行主体、适用期限、告知程序、数据信息保存与销毁规定等。[34]此外,还需要考虑大数据侦查措施所获得材料的证据法上的定位,可参照“品格证据”与“习惯证据”规则赋予大数据证明资格,以“衍生证据”对大数据侦查获得的证据进行定性。[35]以基本权侵害程度为标准认定大数据侦查的程序性规制,通过非法证据排除,对大数据侦查的执行监督由行政逻辑转向司法控制逻辑。[36]

3.强化个人信息和数据保护。我国正在审议《数据安全法》并正准备出台《个人信息保护法》,这些法律和《刑事诉讼法》是并行保护公民的个人信息权利的。对于个人信息保护,应当考虑收集数据主体在数据采集时的告知义务以保障数据主体的知情权,但不同于民事活动中数据主体以“授权”与否为标准进行风险分配与平衡责任,在犯罪治理目标下,

私权的让渡在刑事场域的界限可以“知情”为标准作为权利保护原则，最大限度平衡数据信息所有者自主选择、数据控制的权限和犯罪治理的公共利益。同时，应从外部监督侦查机关数据的收集，这便需要在刑事司法的程序中赋权辩护方有效参与，证据开示制度或可成为现有的可资利用的制度基础，还可以完善数据鉴定和数据专家辅助人制度以提高辩护方抗衡侦查机关的技术能力。

4.通过专门立法集中规制大数据时代侦查权的扩张。从长远来看，集中立法是解决该问题之优选。大数据时代的侦查行为，越来越难以厘清技术侦查与侦查技术的界限，实践中亟须具体明确的法律规范指引，明确侦查行为属性及内容才可更好限制权力弥散扩张。从域外立法来看，如美国、日本和我国台湾地区，都对通讯监听等进行了专门的立法以便将技术侦查及大数据侦查纳入法律规制，典型的立法例是美国的《通信电子存储法案》及后续的《爱国者法案》《云法案》、日本的《通信监听法》、我国台湾地区的《通讯保障及监察法》等。大数据时代的侦查行为，虽然表现形式繁多，但典型的场域就是对电子通讯信息进行收集提取以实现犯罪线索及证据的获取，从域外的立法例来看是可能通过统一立法来规制相关实体、程序、证据问题的。集中立法的另一作用在于，有了明确的上位法来规制公安机关基于自身管理便利而出台的规范性文件，以限制公安机关的借授权立法自我扩权。

此外，需要调和国家治理逻辑与司法自洽逻辑的内生冲突。国家治理强调“积极主动”并追求“绩效”，而司法具有“消极被动”和“独立性”特点，如没有犯罪自然不能主动采取侦查措施。“当国家治理把合法性来源建立在绩效之上时，它就必须努力兑现一些现实的承诺。这是任何以绩效为基础的政权必然要背负的沉重负担。”[⑱]国家治理的主动性会模糊司法自洽逻辑对权力约束的界限，这表现为，大数据时代侦查机关的权力扩张显然不是侦查机关自身就可以实现的，大数据侦查的基础设施建设、新侦查措施的模糊化授权等都不是侦查机关自身可以任意而为的，而是国家将侦查权本身作为治理工具的一种体现。因此，必须在国家治理层面尊重刑事司法本身的规律和逻辑，如审判中心主义、令状主义、辩护权保障等，在此基础上维护司法活动正常的效益产出的绩效合法性更符合法治发展的长远进路。

结语

张文显教授提出了“构建智能社会的法律秩序”这一重要命题，并指出“我们要以法治的理性、德性和力量引领和规制智能科技革命，让智能化系统更加安全可控、科技运用更合乎伦理法理，使之成为促进社会有序发展、共享发展、公平发展、开放发展、和谐发展的生产力基础。”[⑲]大数据时代的侦查权研究，便可遵循上述理路，大数据侦查措施既可以成为维护智能社会法律秩序的重要力量，又需要我们用法治的理性、德性和力量来有效规制。当前，深化司法体制改革与现代科技应用相结合是我国司法改革的重要路径，侦查权的扩张问题便是这一改革过程中应当关注的一个重要方面。改革强调应当更加积极主动拥抱大数据、人工智能时代，把理念思路提升、体制机制创新、现代科技应用和法律制度完善结合起来，但如何实现上述改革目标，达成多方共赢局面，实现科技红利的司法转化，最大限度的实现打击犯罪与保障人权的平衡，还需要理论研究、立法供给与实务工作的多方努力。

注释：

①参见胡铭主编：《聚焦智慧社会：大数据方法、范式与应用》，浙江大学出版社2018年版，第17页。

②参见汤瑜：《中国网络犯罪占犯罪总数1/3》，载《民主与法制时报》2017年1月17日。

③有学者认为大数据侦查是伪命题，大数据只是侦查信息化的一个面向，参见彭知辉：《“大数据侦查”质疑：关于大数据与侦查关系的思考》，载《中国人民公安大学学报(社会科学版)》2018年第4期；有学者认为大数据侦查给侦查活动带来了整体性变革，从认识论和方法论两个方面给侦查工作产生了直接影响，参见裴炜：《个人信息大数据与刑事正当程序的冲突及其调和》，载《法学研究》2018年第2期。

④八大主要数据库为：全国重大案件、在逃人员、派出所人员、违法人员、盗抢汽车、未名尸体、失踪人员、杀人案件数

据库。参见艾明:《新型监控侦查措施法律规制研究》,法律出版社2013年,第169-170页。

⑤参见尚云杰:《论现代科技手段在警务工作中的应用——以DNA技术、金盾工程与天网工程的应用为例》,载《科技情报开发与经济》2012年第10期。

⑥参见江涌:《数据库扫描侦查及其制度建构》,载《中国人民公安大学学报(社会科学版)》2013年第2期。

⑦参见涂子沛:《数文明》,中信出版社2018年版,第235页。

⑧参见陈永生:《侦查程序原理论》,中国人民公安大学出版社2003年版,第23页。

⑨参见傅美惠:《侦查法学》,中国检察出版社2016年版,第74页。

⑩参见福建日报:《福建公安携于腾讯打造"互联网+警务"》,载新华网,http://www.xinhuanet.com/local/2017-05/24/c-129616866.htm,2020年12月8日访问。

⑪简单来说,泛洪攻击是指攻击者在短时间内向目标设备发送大量的虚假报文,导致目标设备忙于应付无用报文,而无法为用户提供正常服务。

⑫两者均是一种中间人劫持技术,具体使用过程是:通信主机A和B在通信时,A发送的信息数据被第三方C所劫持,并转发给B。对于A和B来说,C的存在可能造成巨大威胁,C不仅可以获取A与B之间的通信内容,而且可以轻易篡改A发送的数据包中的敏感信息给B。而A与B通话时,并不会发现C的存在,这种通讯过程中的秘密性监控手段,如运用于侦查过程中,是一种标准的技术侦查手段。

⑬参见胡铭:《电子数据在刑事证据体系中的定位与审查判断规则》,载《法学研究》2019年第2期。

⑭参见王勇旗:《个人行踪信息的法律保护》,载《检察日报》2020年6月30日。

⑮参见赵宏:《实质理性下的形式理性:〈德国基本法〉中基本权的规范模式》,载《比较法研究》2007年第2期。

⑯参见胡铭:《技术侦查:模糊授权抑或严格规制》,载《清华法学》2013年第6期。

⑰关于隐私权保护,美国在1974年通过了《隐私法案》,1986年颁布了《电子通讯隐私法案》,1988年又出台了《电脑匹配与隐私权法》及《网上儿童隐私权保护法》。

⑱如2019年5月14日,美国旧金山通过《停止秘密监视条例》(Stop Secret Surveillance ordinance)的修订,成为美国第一个禁止使用人脸识别技术的城市。该条例全面禁止旧金山当地政府部门如警察局、治安官办公室、交管部门等使用人脸识别技术。同时,购买任何类似的新监控设备如自动识别车牌号系统、带有摄像机的无人机等,都需要得到市政府的许可。该条例还要求明确政策,以确定市政府如何使用监控技术。该条例指出,"人脸识别技术危害公民权利和公民自由的倾向大大超过了其声称的好处,这项技术将加剧种族不平等,并威胁到我们不受政府长期监控的生活能力"。目前,除了旧金山外,奥克兰和马萨诸塞州的萨默维尔也在考虑通过类似的法令。马萨诸塞州的州立法机构计划通过一项法案,暂停人脸识别和其他远程生物监控系统。参见CAICT互联网法律研究中心:《2019年美国隐私保护立法最新动态》,载安全内参网https://www.secrss.com/articles/10728,2020年6月20日访问。

⑲网上公开巡查执法是指网警通过搜索引擎等技术手段对网络进行全天候巡查,及时发现网络违法犯罪信息和其他有害信息,并分情况对其进行处理。

⑳参见王士帆:《网路之刑事追诉——科技与法律的较劲》,载《政大法学评论》(2015年)总第145期。

㉑参见朱桐辉、王玉晴:《电子数据取证的正当程序规制——〈公安电子数据取证规则〉评析》,载《苏州大学学报(法学版)》2020年第1期。

㉒参见胡铭、龚中航:《大数据侦查的基本定位与法律规制》,载《浙江社会科学》2019年第12期。

㉓参见曾于生、黄昶盛:《以信息化为引领合力打造虚假诉讼监督新模式》,载《人民检察》2019年第14期。

㉔参见沈德咏:《论以审判为中心的诉讼制度改革》,载《中国法学》2015年第3期。

㉕参见刘华东:《数据安全法草案提交全国人大常委会审议》,载《光明日报》2020年6月29日。

㉖我国此次《数据安全法》立法将数据和个人信息相区分,而《个人信息保护法》也正在立法进程中,与《民法典》对"个人信息保护"立法思路一脉相承,与已有的《网络安全法》也有立场和体系的不同安排。这一立法思路清楚地划分了不同法律的规范对象:相比较而言,《数据安全法》更加强调总体国家安全观,对国家利益、公共利益和个人、组织合法权益给予全面保护;而《个人信息保护法》侧重于对个人信息、隐私等

涉及公民自身安全的保护。

㉗参见卫跃宁、袁博:《守定与融合:大数据时代的刑事诉讼方法论省思》,载《浙江工商大学学报》2019年第1期。

㉘参见朱朝亮等编:《日本刑事判例研究(一)侦查篇》,元照出版公司2012年版,第245-253页。

㉙参见林钰雄:《刑事诉讼法(上册)》,新学林出版股份有限公司2017年版,第132页。

㉚参见陈卫东等:《德国刑事司法制度的现在与未来》,载《人民检察》2004年第11期;胡铭:《英法德荷意技术侦查的程序性控制》,载《环球法律评论》2013年第4期。

㉛杭州自2018年开始建设城市大数据资源局,该局设立旨在加强"统筹全市数据资源管理工作、组织实施国家和地方数据技术标准、负责全市政务数据和公共数据平台建设和管理、组织协调全市政务数据和公共数据资源整合、归集、应用、开放、共享,推进落实各级各部门信息系统互联互通,打破信息孤岛,实现数据共享……"。参见杭州市政府门户网站,http://www.hangzhou.gov.cn/col/col1390103/index.html,2020年6月12日访问。

㉜参见李荣耕:《数位时代中的搜索扣押》,元照出版有限公司2020年版,第1-38页。

㉝参见程雷:《大数据侦查的法律控制》,载《中国社会科学》2018年第11期。

㉞参见王东:《技术侦查的法律规制》,载《中国法学》2014年第5期。

㉟参见王燃:《大数据时代侦查模式的变革及其法律问题研究》,载《法制与社会发展》2018年第5期。

㊱参见张可:《大数据侦查之程序控制:从行政逻辑迈向司法逻辑》,载《中国刑事法杂志》2019年第2期。

㊲参见赵鼎新:《社会与政治运动讲义(第二版)》,社会科学文献出版社2014年版,第130页。

㊳参见张文显:《构建智能社会的法律秩序》,载《东方法学》2020年第4期。

Expansion and Regulation of Criminal Investigation Power in the Era of Big Data

Hu Ming　Zhang Chuanxi

Abstract: In the era of big data, investigative activities are undergoing profound changes. Based on the effective governance target of criminal activities, the construction of big data infrastructure and the spillover of investigation power show the explicit expansion of criminal investigation power. At the same time, the investigation node moving forward, data collection generalization, decentralized legislation and other aspects also gradually show the implicit expansion of the investigation power. The expansion of criminal investigation power in the era of big data is reasonable in reality, but it also brings about the legal system of regulation dilemma and the difficult problem of civil rights protection. The expansion of investigation power in the era of big data should be viewed rationally, incorporated into the existing system of criminal procedure law, and regulated according to the degree of coercion. In the long run, the expansion of criminal investigation power in the era of big data should be regulated centrally through special legislation, and the endogenous conflict between the logic of national governance and the self-consistent logic of judicature should be reconciled.

Key words: big data era; criminal investigation power; criminal justice; national governance