武漢大學學報(哲学社会科学版)
WUHAN UNIVERSITY JOURNAL (Philosophy & Social Science)
第72卷第3期 2019年5月
Vol. 72 No. 3 May 2019 156~164
DOI:10.14086/j.cnki.wujss.2019.03.015

大数据时代个人信息权在侦查程序中的导入

蒋 勇

摘 要 个人信息权已经成为大数据时代人权的新面相。我国大数据侦查模式发展忽视了对个人信息的保护,出现了信息收集行为权能性质不明、信息收集门槛过低、信息过度收集等问题,其根本原因在于个人信息权在侦查程序中的缺位。在侦查程序中导入个人信息权,既需要宪法对个人信息保护的确权化,也需要刑事诉讼的立法精细化,同时亦需要司法审查发挥作用。国家在必要时可以设立专门的信息监察机构,以强化对个人信息权的保障。

关键词 大数据;个人信息权;宪法权利;侦查程序;侦查机关;非法证据排除;新兴权利
中图分类号 D915.3 **文献标识码** A **文章编号** 1672-7320(2019)03-0156-09
基金项目 西南政法大学校级青年科研项目(2017XZQN-19);中国博士后第64批面上资助项目(2018M640896)

大数据应用的兴起使得个人信息保护问题逐渐在部门法中显现,2016年美国苹果公司与美国联邦调查局的密钥解锁争议揭示出侦查机关信息收集需求与个人信息保护之间的平衡难点。在大数据时代到来前,侦查机关对犯罪信息的收集与调查通常分布在传统侦查措施中,以对人的询问、讯问与有形物的搜查、鉴定分析为代表,侦查机关的信息收集行为能够被"有形力"的侦查强制措施所吸收,尚未发展出个人信息权的干预形态。而在我国大数据侦查的战略之下,侦查机关对个人信息大数据的倚重衍生出了许多新型的侦查手段与方法,势必对现行侦查程序带来挑战。因此,对于个人信息的保护不仅是私法的任务,同样也是刑事司法领域不可回避的问题。

一、个人信息保护的确权化

借助于大数据的技术条件,个人信息的体量不断增加,功用日趋丰富,并在现代国家治理中形成了基于个人信息的"权力—权利"互动格局。个人信息也逐渐为人权所吸纳,进而转换成一种宪法权利。

(一)个人信息权:大数据时代人权的新面相

人权保障已经成为现代法治国家的共同选择,并在联合国的相关文件中达成共识。在人权达成共识的初期,信息化尚未兴起,人权仍然受制于人类在历史发展中所积累的生存与发展经验,然而当大数据时代来临时,个人信息已经成为一种重要的数据资源,个人信息所包含的身份识别、关系纽带、活动轨迹等功能不仅具备了商业价值,同样也成为政府管制的重要依据。在大数据技术环境下,个人的自治逐渐受到挑战,当公权力与信息技术相结合时,极易产生福柯所描述的"一种无限普遍化的'全景敞视主义'的国家监控形态"[1](P242)。同时,对于个人信息的收集和利用也是各种公权力行为的前置性依据,个人信息的使用效应与公民其他权利可能会产生连锁反应。因而个人信息的保护就不能仅仅局限于安全管理思维,而需要与宪法进行对接,成为新的宪法权利组成部分。欧盟在2007年通过的《欧盟基本权利》宪章第8条确立了个人资料受保护的权利,在2016年通过的《通用数据保护条例》引入了新型的基本权利——个人信息被遗忘权,意图赋予人们删除那些不充分、不相关或过时不再相关的数字信息的

权利[2]（P50）。此外，2017 年欧盟则提交了新的《隐私与电子通信条例》，不仅将脸书（Facebook）等即时通信软件纳入隐私监管框架，还将保护对象从原有的通信内容扩展到时间、地点、来源等标记通信内容的元数据[3]（P85-87）。

美国宪法虽然没有明示个人信息权，但在各种分散立法中均涉及了个人信息的保护问题，比如 1974 年《隐私法》、1968 年《综合犯罪控制和街道安全法》、1970 年《美国公平信用报告法》、1978 年《财务隐私权利法》均涉及公权力收集信息的限制。其中 1974 年《隐私权法》是规范联邦政府收集与处理个人信息的立法，是美国保护信息隐私的根本大法[4]（P113）。而在“Roe v. Wade 案”以及“Whalen v. Roe 案”的司法判例中已经从美国宪法第 1 条、第 4 条、第 5 条以及第 14 条修正条款中形成了信息隐私权的论证路径[5]（P20-30）。可以说，域外国家均将个人信息权视为是一种宪法权利，通过解释判例或者制定法来动态解释个人信息权。

（二）刑事诉讼中的个人信息权构造

正是意识到个人信息已经成为人权的新面相，域外国家一直坚持个人信息入宪的基本立场，并通过判例发展出了若干与个人信息相关的宪法权利从而影响侦查行为的规制，主要有以下四种。

1. 通信秘密与自由。在大数据时代，包括手机、电脑在内的电子通信已经相当发达，而电子通信在传递过程中会出现因脱离通信双方可支配的范围而使通信内容被截获的危险。德国法律也认为，无论通信以何种载体进行，只要具备空间上远距离之通信的性质，均落入通信秘密与自由的保障范围。我国台湾地区学者则认为，“不仅通讯内容有保持秘密的自由，通讯之对象、时间、方式等皆属于保障范围之内”[6]（P6），我国台湾地区司法院大法官解释亦将通信记录和通信者身份纳入通信秘密与自由的范畴[7]（P15）。

2. 隐私权。美国法上以“卡兹案”为起点，在隐私的合理期待上发展出了一系列的识别标准，从而将隐私权与原有的财产权进行了分离，将界定刑事搜查行为的重心放在对公民的隐私利益的保护上[8]（P109）。而在互联网时代，亦存在网络空间中的隐私合理期待。判断个人是否在网络空间中有合理隐私期待，可将储存资料的电脑视为一密闭容器，美国宪法第四修正案一般是禁止执法者无搜索票进入电脑资料库查阅资料，就如同没有搜索票就不能打开密闭容器检查一样[9]（P300）。还有学者从例外的角度来探讨网上隐私合理期待的范畴：“除非在公共论坛，聊天室或者将控制权给第三方，或者属于网上信息的一览无遗，否则网上通信仍具有合理的隐私期待。”[10]（P13-14）2014 年美国最高法院在“Riley 案”中推翻了之前关于附带搜查中适用“密封容器理论”的司法认定标准，转而认为个人手机尤其是智能手机储存有传统设备所不能比拟的海量的数据信息，这些数据信息既不会影响警察执法安全，也不会产生证据保全风险，却具有强烈的隐私合理期待，因此，在逮捕时不适用手机等电子设备的附带搜查[11]（P284-288）。

3. 资讯自决权。不同于美国法上对隐私概念的看重，德国联邦宪法法院在 1983 年人口普查案中依据一般人格权发展出了资讯自决理论，用以保障个人享有自主决定个人资料之揭露与利用的权限[12]（P24）。德国联邦宪法法院曾经在 2008 年判决石勒苏益格—荷尔斯泰因州 2007 年授权警方对车辆的车牌进行自动识别的法案违宪，理由是该法案无差别地辨识车牌，没有标明具体的目的与原因，不符合比例原则，因而不当干预了公民的资讯自决权[13]（P203）。

4.“IT 系统”基本权。德国联邦宪法法院曾经在 2008 年“秘密线上搜查案”的判决中发展出了 IT 系统私密性和完整性之基本权[14]（P41-42）。该基本权利之创设用于区别之前既有的资讯自决权。这是因为网络时代资讯科技系统本身成为一种公民个人信息的重要集合体。虽然资讯自决权可以涵盖公民对个人信息之控制，但其着眼点在于结果，即国家公权力对信息之占有与使用。但如果侦查机关仅仅是篡改、监控了资讯科技系统本身，尚未开展有效的信息收集活动，则未进入资讯自决权或者隐私权的

射程范围。对于此部分的公权力行使,公民缺少积极的防御权。同时,资讯自决权的保障范围仅仅在于防御个别警察的信息收集行为,发生在 IT 系统内的大规模资料收集已经超出了资讯自主决定权的保障范围[15](P24)。IT 系统基本权作为新型的基本权利,适用于所有可以储存电子数据的 IT 系统和设备,但其最终指向仍在于人,因而 IT 系统本身也会成为人格尊严的衍生品,同住宅等隐私空间具有同等的保护价值。

二、大数据侦查模式对个人信息保护的挑战

大数据时代到来前,侦查办案并不倚重个人信息,技术条件上也无法深度收集和分析个人信息。而随着信息技术的发展,侦查机关在网络监控、"天网工程"以及"金盾"大数据平台建设方面取得了长足的进步,从而为深度收集公民个人信息奠定了基础,侦查机关也开始重视个人信息在线索指引、早期干预方面的作用。然而,当前刑事诉讼法所预设的取证情景并非是大数据时代,侦查机关对个人信息的倚重无法为当前侦查程序所规制,并遮蔽了对个人信息的保护。

(一)个人信息收集行为的性质界定难

在我国现行的侦查强制措施体系中,人身和财产是最主要的划分标准,呈现出明显的有形力特征。而大数据侦查模式的发展,使得刑事诉讼法无法涵盖愈来愈丰富的大数据侦查权能,出现了权能性质难以识别的问题。

利用个人信息来定位追踪犯罪嫌疑人是大数据侦查的常用手段,大数据时代信息留痕能力的强化使得公民的轨迹可以外化为信息的流动轨迹,进而丰富了侦查机关的追踪措施。虽然 2012 年《刑事诉讼法》确立了技术侦查的合法地位,但对技术侦查的范畴并没有界定,而学理上对技术侦查措施的范畴亦存在着争议。《公安机关办理刑事案件程序规定》中将技术侦查定义为:由设区的市一级以上公安机关负责技术侦查的部门实施的记录监控、行踪监控、通信监控、场所监控等措施。该规定将技术侦查的识别限定在技术侦查部门。在实践中,网络地址定位、利用 GPS 定位、利用通联记录进行轨迹分析亦是一种有效的定位措施,而网络地址定位通常由公安机关的网警部门执行,调取通联记录任何一个执法警种均有权为之,GPS 定位的实施部门则尚无定论。如果严格按照上述规定,将其排除出技术侦查的范畴,势必会造成侦查机关援引法律依据上的分歧。在司法实践中,已经出现了"调取通联记录"措施适用不同侦查规范的矛盾情形①。此外,随着人脸识别技术的发展,在视频监控系统中融合个人身份信息以达到实时轨迹监控的效果已经成为可能[16](P128-129)。此种由视频警种所实施的行踪监控行为,是否属于技术侦查措施亦存在界分上的困难。若类似信息收集措施长期得不到明确的法律界分,会产生两种极端的情形:一是侦查机关"降格处理",以不属于技术侦查措施为由,规避技术侦查实施的严格程序,从而更便捷地收集公民隐私信息;二是在庭上质证时,侦查机关"升格处理",以属于技术侦查措施为由,要求庭外核实,从而削弱辩护律师的质证权。

(二)个人信息收集的不当放权

对于个人信息大数据的收集,除了侦查机关依职权直接收集外,侦查机关还会依托公安机关的政策网络,共享第三方社会信息。由于公安机关是社会治安综合治理体系的主导者与发起者,借助此优势地位,公安机关近年不断强化与其他行政机关及其所属行业的信息共享。例如北京市公安局、市商务委、市工商局、北京海关、北京出入境检验检疫局五部门在 2011 年共同签署《北京市五部门行政资源整合机制框架协议书》中就决定建立联席会议机制、"绿色通道"机制、信息共享机制。这种共享路径大多通过地方性政策框架协议来实现,很少接受合法性审查[17](P2)。而在某些政策的窗口期,公安机关能获得更多的政策收益空间,这些政策大多以警企合作的形式呈现,其规范性更弱。而侦查机关借助公安机

① 例如在福建省龙海市法院审理的"林某某诈骗罪"(2014 龙刑初字第 580 号)一案中,公诉机关提供的通信记录是通过技术侦查手段而来,而安徽省合肥市中级法院审理的高某某贩毒案中,公诉机关提供的通信记录是由侦查机关向移动公司调取而来(2014 皖刑终字第 185 号)。

关的整体政策推进，也同步获得了信息共享的红利。这些被共享的信息在公安大数据平台的支撑下，被高度集成与标准化储存，为信息查询创造了技术条件。信息查询只需要通过人机交互即可完成，无需再持证调取。随着移动警务客户端的普及，信息查询也无需在办案场所进行，时空限制进一步放宽。同时，属于其他警种监管的基本信息（如旅馆业、机动车登记信息、视频监控信息），侦查机关也可查询。虽然在金盾平台的管理上，公安机关也规定了信息查询的权限，但这些条令仅仅是一种纪律约束，缺乏事前控制。

同传统侦查相比，大数据侦查更多地依赖情报分析来推动侦查进程，因而侦查权能中包含了情报信息的检索与分析。长期以来，情报信息的检索、分析一直被视为公安机关的内部管理事项，并不产生外部法律效果。基于公安大数据平台的信息查询虽然在形式上只是信息的检索，但在本质上却是一种证据调取。我国刑事诉讼法第 52 条规定了人民法院、人民检察院和公安机关有权向有关单位和个人收集、调取证据。有关单位和个人应当如实提供证据。在前信息化时代，一些涉及公民隐私的数据需要侦查人员实地调取方能查阅，在调取时，需要填写《呈请调取证据报告书》并经县级以上公安机关负责人批准，因而发动要件是相对明确的。而在公安大数据平台下，由于事先实现了信息数据的共享，公民隐私数据已经直接储存在公安大数据平台或者搭建了查询通道，侦查人员的检索、查询行为成为一种变相的调取证据行为。在如今的技术条件下，检索、查询行为只需要数字验证，并无发动要件之规制，调取证据的任意性有增无减，而在实践中已经出现民警不当泄露个人隐私的案件，这表明侦查机关调取和查询公民个人信息的权限过于宽松。

（三）个人信息的过度收集

大数据侦查不仅强调个人信息在侦查破案上的功能，即犯罪线索上的指引作用，在犯罪预防上的功能也很突出，即在犯罪早期干预和阻断上的效果。这容易激发侦查机关收集公民个人信息的热情，易造成个人信息的过度收集，而现行刑事诉讼法缺乏有效的节制手段。

在个人信息中，由于生物样本（如 DNA、指纹）可以关联个人身份，亦可做同一认定，因而成为侦查机关进行身份识别的重要依据。但在我国的侦查程序中，人身检查的对象、手段、范围并没有进行严格的限制，相反，在公安部 2014 年颁布的《规范使用执法场所办案区“四个一律”》中规定，违法犯罪嫌疑人在被带入办案区后一律先行采集信息，而不论违法犯罪嫌疑人的最终处理结果如何。从实践来看，嫌疑人只要处于到案状态，公安机关均可进行强制采样，甚至不需区分是侦查措施还是行政措施。而强制采样结论的数据化共享对办案效率提升的作用则更加促进了公安机关进行无差别强制采样的动机。在大数据平台的支撑下，所有的嫌疑样本均可以通过数据化加以保存，任何案件无论是初查还是正式侦查阶段，侦查人员均可以按照级别权限自由查询嫌疑样本的信息，因此，已经被公安机关收集了的公民隐私信息难以得到有效保护。例如在 2013 年“武汉女大学生遇害案”中，侦查机关对案发地周围高校的数千名男性师生采取了撒网式的 DNA 采验，而对这些 DNA 信息究竟如何处置，侦查机关没有给出明确答复，从而引起舆论争议[18]。

除此之外，在大数据时代通过对海量电子数据（如手机通话记录、网购信息）的分析，可以得到关于公民个人兴趣、生活模式、行踪轨迹相关的情报，能够直观地展现特定人员与案件的联系，因而备受侦查机关青睐。虽然《刑事诉讼法》并未对电子数据的搜查与扣押作出专门规范，但 2016 年颁布的《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》（以下简称《电子数据规定》）规定了电子数据调取、网上在线提取、网上远程勘验、电子数据冻结、电子数据检查五种措施，然而这些条款中均无对发动要件的限制，也没有对收集范围的限制。值得注意的是《电子数据规定》第 16 条规定：对扣押的原始存储介质或者提取的电子数据，可以通过恢复、破解、统计、关联、比对等方式进行检查①。该条款

① 公安部 2019 年《公安机关办理刑事案件电子数据取证规则》第 43 条亦重复了该项内容，并没有进一步严格适用。

对电子数据的搜查没有任何限制,这意味着只要公安机关扣押了原始存储介质——尽管扣押该存储介质可能基于其他授权(如盘查、人身检查)或者属于办理其他刑事案件的需要,那么对其中电子数据内容的查看(包含了搜查、扣押)均是合法的。而许多电子数据中的个人隐私(如手机、IPAD 等移动客户端)较为敏感,如此便利的搜查与扣押为侦查机关无差别的信息收集提供了制度空间。

三、个人信息权在侦查程序中的缺位

大数据侦查带来的挑战,从表面上看是刑事诉讼法的滞后与粗疏所致,然而实际上是由于缺乏个人信息保护的观念,导致个人信息权在侦查程序的运行中一直处于缺位状态。

(一)宪法上个人信息权碎片化

虽然在私法上,多有关于个人信息保护的规范与判解,但在我国宪法上,并没有明示个人信息权,与此直接相关的只有宪法第 40 条关于公民的通信自由与秘密的条款。虽然通信秘密与自由确属于个人信息敏感隐私范畴,但个人信息的范畴却要大于通信自由与秘密,例如网络注册资料、位置资料、网络浏览记录等。因此通信自由与秘密条款的射程是有限的。此外,宪法第 38 条虽然规定了人格尊严,但却又附加上"禁止用任何方法对公民进行侮辱、诽谤和诬告陷害"的条款,由此我国宪法上的人格尊严仅具私法上人格权的指示功能,缺乏解释和发展个人信息权的空间。同样的局限性也表现在宪法第 39 条上,该条规定的非法搜查仅仅是针对住宅自由而言的,而不包括处于虚拟空间的个人信息与资料,这种狭义的对象限定,也使得该条款无法被用来对抗侦查机关对个人信息的非法搜查。由此可见,我国个人信息权并没有如域外国家那样成为宪法权利,而仅有的宪法权利也难以解释和发展公法维度上的个人信息权。个人信息权在宪法上的碎片化,影响了侦查程序对个人信息权的接纳与保护。如《电子数据规定》的大部分规范是立足于电子数据的审查判断,特别是电子数据的证明力规则,对电子数据取证行为属于刑事诉讼中的何种侦查措施仍然言之不详[①],而电子数据的来源、取证手段恰恰与公民个人信息保护紧密相关,《电子数据规定》在取证手段与程序上的规范粗疏不利于个人信息的保护,并在一定程度上造成了执法与司法上的适用困难。

(二)司法审查有心无力

在对权利的保障上,除了立法预设外,法院的司法审查亦是一种有力的武器。例如美国宪法上并没有隐私权的条款,但美国联邦最高法院在"卡兹案"中通过解释什么是搜查,从侧面展示了隐私的合理期待标准,进而保障了公民在住宅外的通信隐私权益。德国基本法上也没有关于 IT 系统基本权的规定,但德国宪法法院针对警方黑客技术的发展,在资讯自决权之外填补了新的权利空缺。相比之下,我国法院并不具有解释和发展宪法权利的能力,虽然在 2001 年"齐玉苓案"中最高人民法院曾经以宪法规定的受教育权作为批复依据,但最高人民法院 2008 年又废止了这一批复[②],2009 年,最高人民法院在《关于裁判文书引用法律、法规等规范性法律文件的规定》中明确了引用规范性法律文件的范围限于法律、法规等范围,不包括宪法,于是法院对侦查程序中个人信息的保护途径就只剩下非法证据排除规则了。

2012 年《刑事诉讼法》颁布后,我国虽然有了非法证据排除规则,但与域外国家主要立足于证据能力的审查判断不同,在我国的规则体系下,只有刑讯逼供等非法言词证据被严格排除,而实物证据只有在严重影响司法公正且不能补正的情形下才予以排除。这说明立法者更关注证据的真实性,而非取证行为背后的权利干预。如 2016 年《电子数据规定》在合法性审查判断上也只规定"取证是否符合技术标准"及"是否手续齐备",而取证的发动要件、取证行为的性质则并未作为审查重点。这仍然是侧重于电子数据的证明力,而非证据能力。"作为证据审查人员,首先应当审查取证方法是否符合《刑事诉讼法》的

① 《电子数据规定》设立的"网络在线提取"和"网络远程勘验"与刑事诉讼法上的"搜查""技术侦查"是何种关系,并未明确。公安部 2019 年《公安机关办理刑事案件电子数据取证规则》亦没有提及。

② 详见《最高人民法院关于废止 2007 年底以前发布的有关司法解释(第七批)的决定》

程序规范包括解释性规范。而要求遵循相关技术标准以及审查是否符合相关技术标准，对于一般执法、司法人员，在一定程度上也许是勉为其难。”[19]（P13）不仅是电子数据，其他非法实物证据的排除也存在上述逻辑，法院只需审查取证的要式是否合规，而不论取证的裁量权是否合理。在这一过程中，法院只是以侦查机关的立场，对侦查人员的取证手续进行了重新审核，对个人信息的保护并无多大助益。

（三）内部控制的局限性

虽然公安部一向重视内部控制体系的建设，并在 2008 年开启了执法规范化建设周期，还陆续颁布了各种规范性文件，这些举措在一定程度上确实有利于弥补立法粗疏与司法审查缺位所带来的规制漏洞。但是作为内部控制体系的执法规范化建设，也存在局限性。一是将执法步骤、策略等同于执法操作规范。对于承接立法授权的部门规章、规范性文件而言，应当按照“假定条件 + 行为模式 + 法律后果”的规则模式进行细化，然而大量的执法细则却将重心放在执法的方法、步骤上，导致执法标准与执法操作规范甚至是执法策略相混同，未能起到应有的补缺功能。在信息收集方面也并没有设定门槛要件，没有进行类型区分。二是结果导向型的控制。在内部控制体系下，执法规范化建设强调科层式的执法考核，并形成了项目化的运作方式。为了迎合政策目标，部分地方公安机关更加看重执法结果——特别是把考评材料是否齐全完备、是否引起了执法争议（如信访、行政诉讼、行政复议）作为评判标准，这种结果导向型政策工具并不重视对警察执法行为的过程监督，而只是以业务部门反馈的各种静态数据作为事后奖励或者惩罚的依据，因而很难控制侦查行为的发展过程。其主要表现是：在侦查情报信息的收集、存储与共享中缺少事前控制，只能在出现违法犯罪现象之后，才能进行回应①。三是对大数据侦查的特质认识不足。公安系统内部的执法规范化建设并没有意识到大数据侦查的特质，仅仅将其当作是一种警务模式的变革，将其归类于公安管理事项，在内部控制上放任侦查权隐形扩张；同时，由于大数据侦查带来了破案效益的增长，近年来的执法规范化建设并没有去专门约束大数据侦查行为，其重心仍然在于对涉案财物、人身自由的规范执法，而在个人信息保护上着墨不多。

四、个人信息权在侦查程序中的导入

在侦查程序中导入个人信息权，既需要在宪法层面接纳个人信息权，也需要在刑事诉讼立法中革新方法论，亦需要在司法审查中加强释法和指导性案例建设，在必要时国家可以设立专门的信息监察机构，以强化公法层面对个人信息的保障。

（一）以入宪为基础的个人信息权利体系

个人信息是否入宪，并不是简单的宪法观念问题，它将直接关系到部门法对宪法权利的具体化从而形成基于部门法的“客观法秩序”。在刑事诉讼中，对宪法权利的尊重和保护就体现在区分任意侦查与强制侦查的标准上。正如罗科信教授指出的，刑事诉讼法上的强制措施均为对基本权利之侵犯[20]（P273）。正是在这个层面上，任意侦查与强制侦查的区分标准才逐渐转向“权利干预说”与“综合判断说”[21]（P15-19）。

无论大数据时代侦查方法与手段如何发展，只要构成了对基本权利的干预，就应当视为是一种强制侦查。这些新型侦查手法，已不是技术上能不能执行，而是法律上是否容许及法律要件如何设计的问题[22]（P343），这意味着对基本权利类型、保障范围与审查标准的认定就成为立法的前提条件，对基本权利的认识、接纳程度不同，相应的取证程序设计也就不同。例如，在对待通信记录调取的问题上，由于德国立法坚持对资讯自决权的保障，认为通信记录属于资讯自决权的保障范围，因此，德国刑事诉讼法坚持任何形式的通信记录调取均需遵循法官保留原则，也即法官核准[23]（P50）。而在美国，由于坚持隐私权的审查标准——隐私的合理期待，而这一标准又以第三方披露为例外，“宪法第四修正案并不保

① 在出现多起民警违规查询、泄露个人信息案后，公安部在 2015 年制定了《公安机关信息查询共享应用“七不准”》。

护那些自愿暴露给第三方的信息”[24](P563),而在“United States V. Miller 案”中,美国最高法院重申了这一立场,并强调,即使公民认为第三方应当谨慎地适用这些信息并防止外泄,只要公民自愿暴露给第三方,仍然丧失了合理期待[25]。这导致对服务商所占有的通联记录数据并没有被强制纳入隐私权的保护范围,因此,美国《联邦通信存储法案》规定侦查机关调取通信信息并不是一种搜查行为,最低只需要持有“行政传票”(18 U.S. Code § 2703[d]),而不需持有法官的司法令状。

因此,将个人信息权纳入宪法保护范畴是域外国家的通行模式,只是个人信息保护的路径与侧重点不同。虽然我国宪法中并未明确规定个人信息权的基本权利类型,但在一些部门法中,已经将个人信息当作一种独立的法益加以保护。如 2016 年《网络安全法》也将公民个人信息的保护视为网络安全的组成部分。而在民法与刑法的规范体系中,则不断出现对个人信息的法益描述,如 2009 年《刑法》修正案(七)增加了出售、非法提供公民个人信息罪、非法获取公民个人信息罪;并在 2015 年拓宽了该罪的适用范围。2014 年《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》则首次将基因信息、病历资料、健康检查资料、犯罪记录、家庭住址、私人活动等明确为需要保护的个人隐私。因此,个人信息权入宪不仅影响着侦查程序的设计,也是其他部门法的共同需求。

(二)以个人信息权为核心的立法精细化

在个人信息权入宪的基础上,侦查程序可以围绕个人信息权干预的正当程序进行细化,其问题与路径相对清晰。一方面,在宪法权利的视角下,所有的侦查强制措施均是一种宪法权利的干预,侦查机关的信息收集行为需要转化成为刑事诉讼中的法定侦查措施,可以按照是否具有权利干预特性将侦查机关的信息收集行为区分为任意侦查与强制侦查。在强制侦查行为中又可以按照证据调取、搜查与扣押、技术侦查①等脉络进行细化,从而使立法能够适应动态发展的大数据侦查方法与手段。另一方面,侦查机关的信息收集行为,尤其是干预性职权需要接受比例原则的约束。比例原则的要义在于目的和手段的对称性,在目的层面,要考虑到“罪有轻重、人有差别、事有缓急”[26](P158-161)。在手段层面,则要考虑侦查强制措施的强弱、控制程序的宽严。干预性越强的职权,就越需要在比例原则构造上精细化。例如,2014 年欧盟法院之所以判定 2006 年《数据留存指令》违反了《欧盟基本权利宪章》第 8 条②,就是因为该指令并未对隐私权之干预设立足够的限制,却又使几乎全欧洲的人口都受到基本权利干预。其中与比例原则相关的批评包括:未界定严重犯罪或者恐怖犯罪侦查与通信监控的关系;没有确立中立机关的事前审查制度;个人信息也没有区分类型而一律保留 6 个月[27](P88)。而我国侦查程序中存在过多的概括条款,尤其在规制侦查机关的信息收集行为上,缺乏应有的程序刚性,因此,比例原则应当着重作用于信息收集行为的发动要件上,至少应当包括犯罪类型、证明标准(证据要求)、干预对象、审批主体、当事人救济权、特殊情形等,从而建立一种权能强弱有别、程序宽严相当的侦查强制措施体系,以修正概括条款过多、欠缺可预测性等立法弊端。其整体思路如图 1 所示。

(三)司法审查的适度作用

我国虽然没有强制侦查的司法令状制度,但法院在事后的司法审查中仍具有一定的能动性,这体现在对侦查措施的类型识别上。例如,2015 年黑龙江省建三江农垦法院在《建刑初字第 42 号刑事判决书》中认为,侦查机关调取的被告人的通话记录属于证据调取行为。法院之所以能够在侦查措施的识别上发挥司法审查的作用,是因为在庭审质证中,对证据来源及证据方法的质证是必不可少的环节,而侦查措施的性质必然与证据来源、证据方法紧密相关,在庭审实质化的司法政策下,法院对侦查措施的性质识别成为质证在庭上的必经阶段。这种附属于质证程序的司法审查,虽然不能援用宪法解释和发展基本权利,且个案中的审查结论也不具有普遍的拘束力,但在当前刑事诉讼立法还不够精细,而立法任务

① 在我国立法技术下,技术侦查包含了秘密侦查措施,因此秘密侦查措施不再单列。

② 第 8 条内容包括:人人均有权享有个人数据的保护;仅基于特定明确目的,且与数据所有人同意或者其他法律授权下,数据才可以被公正的处置;人人有权了解其数据使用情况,并有权销毁其个人数据;应由专门的独立机关来监督上述规则的执行。

又极繁重的现实条件下，通过司法审查来推进侦查机关信息收集权能的显性化与类型化无疑是可行且快捷的路径。而最高法院颁布的指导性案例，又为这种司法审查提供了制度化的平台，可以将个案的司法审查结论以指导性案例的形式作为全国法院审判的参考。“虽然基于现实的政治性考虑，‘两高’都否定了指导性案例的法源地位，但为保证指导性案例的有效性，‘两高’都试图通过司法或行政程序要求办案人员切实注意并遵守指导性案例，使指导性案例具有事实上的约束力。”[28]（P45）如此，不仅可以拓宽个人信息的司法保护渠道，也可以进一步加强司法权对侦查权的制约。

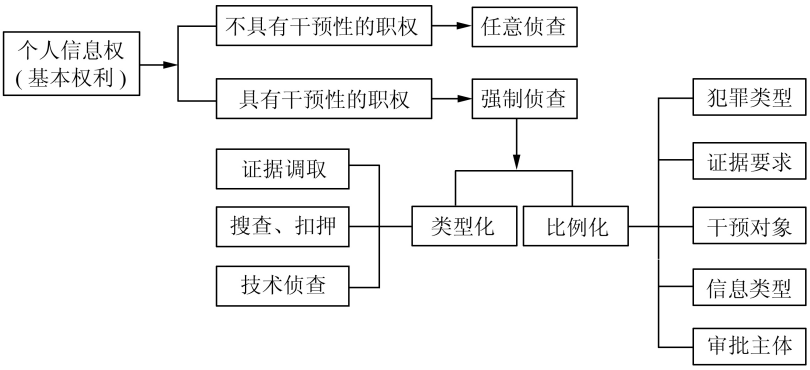

图 1　侦查程序中的个人信息权保护规范体系

（四）专门信息监察机构的设置

鉴于公安机关在犯罪控制中的积极角色，在司法令状阙如的条件下，为了监督公安机关妥善地利用和处理个人信息，有必要引入个人信息保护监察人制度。比如，德国通过《联邦个人资料保护法》专门成立了个人资料保护监察人，由联邦政府提名，经过议会选举而出，非具有终身法官免职之理由，不得罢免。监察人可监督联邦内所有公务单位对个人资料保护规定之遵守，拥有相关的查阅、调查权，并能就个人资料保护制度之缺失提出相关建议，同时亦受理任何人关于联邦机关搜集、处理和利用其个人资料侵害其权利之申诉。而欧盟 2018 年开始实施的《通用数据保护条例》，设立了欧盟个人数据保护委员会作为最高监督机关，由各成员国个人数据保护监督机构领导和欧盟个人数据保护专员共同组成。此外，所有成员国须设立独立的数据保护监督机关[29]（P93）。此类制度在我国拥有一定的现实基础。在中央层面，我国已经成立了中央网络和信息化领导小组，国务院亦在 2011 年成立了国家互联网信息办公室，两者均具有信息安全管理的职责。借鉴欧盟信息监察制度的经验教训，我国可在网信办体系下设立独立的信息监察机构，并赋予其个人信息保护的专项职责与监察权能，从而提供个人信息保护的专门申诉渠道，加强对公权力机关信息收集的监督。

参考文献

[1] 米歇尔·福柯. 规训与惩罚. 刘北成，杨远婴译. 北京：生活·读书·新知三联书店，1999.
[2] 郑志峰. 网络社会的被遗忘权研究. 法商研究，2015，(6).
[3] 曹金峰，李金磊. 欧盟《隐私与电子通信条例》草案评述. 信息安全与通信保密，2017，(1).
[4] 齐爱民. 美国信息隐私立法透析. 时代法学，2005，(2).
[5] 阿丽塔·L. 艾伦. 美国隐私法：学说、判例与立法. 冯建妹，石宏，郝倩等译. 北京：中国民主法制出版社，2004.
[6] 黄清德. 位置资料搜集与基本人权保障. 警专学报，2009，(5).
[7] 詹镇荣. 秘密通信自由. 法学讲座，2003，(21).
[8] 向燕. 美国最高法院“隐私的合理期待”标准之评介. 环球法律评论，2011，(1).
[9] Rolando V.del Carmen. 美国刑事侦查法制与实务. 李政峰，林灿璋，邱俊诚等译. 台北：五南图书出版公司，2006.

[10] İlker PEKGÖZLÜ, Mustafa Kemal ÖKTEM. Expectation of Privacy in Cyberspace: The Fourth Amendment of the US Constitution and an Evaluation of the Turkish Case. *Sosyoekonomi*, 2012, 18(2).
[11] 李荣耕. 数位资料及其附带搜索——以行动电话内的资讯为例. 台北大学法学论丛,2016,(1).
[12] 蔡宗珍. 电信相关资料之存取与利用的基本权关联性. 月旦法学杂志,2018,(2).
[13] 黄清德. 科技定位追踪监视与基本人权保障. 台北: 元照出版公司,2011.
[14] 伯阳,刘志军. 一般人格权之具体体现: 新创设的保障 IT 系统私密性和完整性的基本权利. 中德法学论坛,2008,(6).
[15] 谢硕骏. 警察机关的骇客任务——论线上搜索在警察法领域内的实施问题. 台北大学法学论丛,2012,(6).
[16] 肖军. 人脸识别技术在公安领域内的应用研究. 计算机科学,2016,(11).
[17] 侯莎莎. 公安工商等五部门共享执法信息. 北京日报,2011-05-11.
[18] 武汉一女大学生返校时遇害 附近四校数千男师生采血验 DNA. 网易新闻,2013-11-21.[2018-04-27]*http://news.163.com/13/1121/02/9E60MQ6500014Q4P.html.*
[19] 龙宗智. 寻求有效取证与保证权利的平衡——评 "两高一部" 电子数据证据规定. 法学,2016,(11).
[20] 克劳思·罗科信. 刑事诉讼法. 吴丽琪译. 北京: 法律出版社,2003.
[21] 马方. 任意侦查研究. 北京: 群众出版社,2009.
[22] 王士帆. 网络之刑事追诉——科技与法律的较劲. 政大法学评论,2015,(3).
[23] 林钰雄. 通联记录之调取——从几则基地台相关判决谈起. 台湾法学杂志,2014,(1).
[24] Orin S. Kerr. The Case for the Third-party Doctrine. *Michigan Law Review*, 2009, 107(4).
[25] United States v. Miller (1976). Supreme Court of the United States, 425.
[26] 秦策. 刑事程序比例构造方法论探析. 法学研究,2016,(5).
[27] 刘静怡. 通信监察与民主监督: 欧美争议发展趋势之反思. 欧美研究,2017,(1).
[28] 秦宗文,严正华. 刑事案例指导运行实证研究. 法制与社会发展,2015,(4).
[29] 阮爽.《欧盟个人数据保护通用条例》及其在德国的调适评析. 德国研究,2018,(3).

The Implantation of Personal Information Right in Investigation Procedure in the Era of Big Data

Jiang Yong (Southwest University of Politics and Law)

Abstract Personal information right has become a new aspect of human rights in the era of big data. The development of big data investigation mode in China has ignored the protection of personal information, which has caused problems such as the unclear nature of the power to collect information, the improper delegation of power to collect information, and the excessive collection of information. The fundamental cause is the absence of personal information right in the investigation procedure. Implanting personal information right into the investigation procedure requires not only the constitution right to protect personal information, but also the refinement of the legislation of criminal procedure and the participation of judicial review. When necessary, special information supervision organizations should be established to strengthen the protection of personal information right.

Key words big data; personal information right; constitutional right; criminal investigation procedure; criminal investigation department; exclusion rules of illegal evidence; emerging right

■ **收稿日期** 2018-04-28
■ **作者简介** 蒋 勇,法学博士,西南政法大学法学院讲师;重庆 401120。
■ **责任编辑** 李 媛