

[文章编号] 1672-7320(2010)05-0733-06

# 比较法视野下的技术侦查制度研究及其启示

王 彬

**[摘要]** 随着科学技术的发展,技术侦查在犯罪侦查中的作用越来越重要。为此,不论是大陆法系国家还是英美法系国家大多通过立法对技术侦查的种类、适用范围、适用原则、审批程序以及侦查结果的保存使用进行了明确规定,以规范本国的技术侦查。在我国,一方面是技术侦查在立法上规定过于原则甚至缺失;另一方面是侦查实践中侦查机关大量使用技术侦查手段侦查刑事犯罪。因此,有必要研究并借鉴国外技术侦查立法的成功经验,以刑事诉讼法修改为契机,通过立法对技术侦查的相关问题加以明确规定。

**[关键词]** 比较法;技术侦查;研究与启示

**[中图分类号]** DF6 **[文献标识码]** A

技术侦查,简称“技侦”,是指秘密利用科学技术手段(主要是电子技术手段)发现、跟踪、证明犯罪的特殊形式的侦查活动,其表现形式主要有电子监听、电子监控、电子跟踪、秘密录音录像、秘密拍照、秘密截取电子资料信息等。目前,不论是英美法系国家还是大陆法系国家,大都在立法上对技术侦查加以肯定并进行了较为全面的规范。英美法系国家多以专门立法的形式对技术侦查进行规范,而大陆法系国家多在刑事诉讼法典中对技术侦查作统一规定。

## 一、英美法系国家:以英国、美国为代表

### (一)英国

在英国,通讯数据获取、通讯截获、侵入监控、直接监控等被划归到技术侦查的范畴。“通讯数据获取”是指对已经存在的通讯数据的收集和提取,即对何人、何时、何地、如何进行通讯方面的信息的“获取”,英国法将其细分为往来数据、服务使用数据与用户信息数据三类。通讯截获则包括对各种通讯方式所包含的内容在传递过程中进行的监控或获取。将私人住宅或私人车辆作为监控对象,从而获取上述空间内的个人信息,在英国法上被称为侵入监控,如在私人住宅内安装秘密录像设备、监视器、窃听器。在英国,计算机数据的获取以及相应的与计算机有关的技术监控并不认为是一类单独的监控手段,与计算机有关的各种监控手段都被归入通讯截获与直接监控之中。如对正在进行的电子邮件进行即时监控的行为,就属于通讯截获的范围;对计算机内部的资料进行扣押,无论是通过有形干涉还是通过特殊的软件获取,都属于搜查扣押手段的使用,同时也是一种干预财产的技术监控手段;如果需要通过监视、拍照等手段在计算机使用地点即时监控犯罪嫌疑人使用某一计算机的情况,则属于直接监控手段的使用;当犯罪嫌疑人通过电子邮件与被害人进行犯罪联络时,经被害人同意对电子邮件进行监控或获取的行为,则归入到直接监控手段内;当需要对私人住宅中的计算机使用情况进行监控时,则涉及侵入监控手段的使用。

英国通过一系列法律、法规对技术侦查手段进行了规范,《通讯截获法》规定,截获通讯必须基于维

护国家安全、防止和侦查重大犯罪、维系联合王国经济稳定之目的。令状必须载明截获的对象及其名称、依据、电话号码和有效期限。2000年《侦查权力规范法令》也有类似规定。对于监控记录的保管,以及事后的告知程序,英国法则没有规定。由于英国在技术侦查的控制体系方面实行行政审查而非司法审查,为了弥补司法审查机制的欠缺,立法者在采取技术侦查手段的外来监督方面设置了众多的保护措施,如对议会报告工作的监控委员会办公室,每年对技术侦查手段的使用情况进行检查,提交年度报告;设置了专门负责技术侦查损害赔偿的法庭,对违法的技术侦查进行监督与救济。

## (二)美国

在美国,技术侦查大致分为通讯监控、有形监控与业务记录监控三类。通讯监控是对口头、有线或者使用电子媒介或者其他手段进行的电子通讯的同步监控;有形监控是同步观察或发现被监控者的行动、活动与周围情况;业务记录监控是获取已经存在的通讯记录、信用卡消费记录、其他金融交易数据以及交通旅行订票记录等。电话监听、对口头谈话的窃听,对传真、寻呼机、电子邮件的监控都可以归入到通讯监控的范畴,而获取通讯记录以及银行记录等则可以归入到业务记录监控的范围内;秘密拍照、追踪定位装置、热显像仪以及探测装置等侦查措施的使用则可以归入到有形监控的范畴之中。

最初,通讯监控在美国不受法律保护,1934年美国国会通过的《联邦通讯法》规定,包括执法机关为侦查犯罪而实施的电话监听都是非法行为,禁止在未经通话方同意的情况下实施电话监听。1968年美国《综合犯罪控制与街道安全法》规定,在没有法院授权的情况下,禁止任何人以电子的、机械的或者其他类型的设计装置来达到监听或者企图监听谈话和电话传输的目的。侦查机关需要采取监听手段时,除经通讯一方当事人事先同意的以外,原则上必须事先申请有管辖权的法官授权,在紧急情况下,也可先进行监听,然后申请有管辖权的法官认可。《综合犯罪控制与街道安全法》对通讯截获虽然进行规范,但仅限于电话、对讲机等设备的使用与监控,目的是对声音类信息的获取,对传真、电子邮件、寻呼机等通过文字、电子信号、图像等传递方式进行的信息交流则不能适用。1986年《电子通讯隐私法令》在美国获得通过,该法将非声音类通讯科技的监控,如电子邮件、传真、寻呼机等通讯方式的监控纳入到监听法令之中,统称为“电子监控”。

在美国,各种单纯依靠视力,以及其他人的感觉或者通过科技设备的使用增强监控能力而对相对人的活动、动向以及周围环境进行的监控,都属于有形监控,它比电话监听、窃听等传统通讯监控手段对隐私权的干预程度更强。在缺乏制定法依据的情况下,美国法院借助于宪法修正案中的搜查条款对隐私权的保障,对有形监控的使用进行了有限的规范。之所以称之为“有限”的规范,是因为法院只能通过对各种新兴科技手段的使用是否侵犯了被监控人合理的隐私期待从而构成搜查的推理模式,对各种有形监控手段进行判断与衡量。在这种模式下,问题的关键在于是否构成对隐私合理期待的干预、是否构成搜查,如果构成搜查,则相应的手段必须履行宪法为搜查设置的各种限制程序,有形监控就被视为搜查手段的一种,反之,有形监控不受任何法律的约束。

在美国,业务通讯记录监控主要针对业务活动结束后形成的各种“记录”,具有事后查询的特点。所谓“业务记录”不仅包括商业交往,还包括了个人在社会生活中的许多方面,如医疗记录、个人财务管理状况;个人购物、租赁、房地产交易记录、各种证照、资格记录;电子邮件的登录使用情况、发送的地址及浏览网页的历史记录等。在美国法中,关于业务记录监控的法律依据十分零散,既有判例法也有制定法,但总体上看欠缺系统性且限制条件十分宽松。

## 二、大陆法系国家:以德国、法国、日本为代表

### (一)德国

德国的技术侦查规范体系承袭了大陆法系制定法的传统,技术侦查手段是由刑事诉讼法典加以规定的,在历次修改后的刑事诉讼法典中,监听、电信监控/截获和电子监视(包括秘密拍照与录像)是德国主要的技术侦查手段

德国刑事诉讼法典规定,根据一定的事实有理由怀疑某人作为主犯、共犯实施了法定范围内的犯罪,如叛逆罪、反和平罪、危害公共安全罪等,不论既遂、未遂或者是以犯罪行为预备实施的犯罪,在采用其他方法难以或者不能查明案件情况、侦查犯罪嫌疑人住所的条件下,应当允许对电讯往来实施监视、录制。监视、录制仅适用于通过公用电讯设备进行的电子通讯,监视、录制的范围采取“具体列举式”的方法加以说明。在监视、录制电讯往来时,只允许针对被指控人员,或者针对基于一定的事实可以推认在为被指控人代收或转送所发出的信息的人员,或者针对被指控人在使用其电话线路的人员。

是否监视、录制电讯往来,法官享有决定权;只有在延误就有危险时,才可由检察院决定;但检察院的决定必须在3日内获得法官的确认,否则即自动失去效力。监视、录制必须采用书面形式制作令状,当事人姓名、地址、措施的种类、范围和持续时间必须在令状中明确作出规定;监视、录制的期限为3个月,但法定的前提条件如果继续存在,准许延长期限,但延长期限每次不得超过3个月;依据书面令状,德国联邦邮政局、公用电讯设备经营机构都负有配合义务,在法官、检察院以及它辅助官员对电子通讯进行监视、录制时予以配合。如果不再存在监视、录制的前提条件时,应当及时地停止书面令状中所规定的各种措施,并以书面形式通知法官、德国联邦邮政局,以及其他公用通讯设备经营机构。

除对电子通讯的监视、录制外,1992年德国《刑事诉讼法典》增加了第100条c,该条规定了一种“不经当事人知晓的措施”,即在采取其他措施进行侦查将成果甚微或者难以取得成果的情况下,可以经法官批准(紧急情况下也可以由检察院或它的辅助官员批准),不经当事人知晓而(1)拍照、录像(2)在所侦查事项对于查清案情十分重要的条件下,使用其他特别侦查技术手段侦查案情和行为人的居所;根据一定的事实认为某人具有实施了法定范围内的犯罪行为嫌疑,并且采取其他方式不能或者难以查清案情、侦查被指控人居所的情况下,允许使用技术手段窃听、录制非公开的言论。

为了加强对有组织犯罪的侦查能力,1998年1月16日,德国联邦议会针对住宅监听问题召开了专门会议,会议对德国《基本法》、《刑事诉讼法》、《刑法》及《洗钱法》等相关法律进行了修改。修改后的德国《基本法》将原第13条关于住宅不受侵犯的规定设置了例外,允许在符合特定条件时,对住宅采取监听等方法进行“听觉性监视”,亦即在有足够的理由怀疑某人实施了法定的重大犯罪、且采取其他方法很难或者不可能查明事实时,为了保全刑事程序中使用的证据,可以根据经过由三名法官组成的合议庭签发附期限的命令,对被指控人现在所在的住所使用监听的技术手段。修改后的《刑事诉讼法典》将“重大犯罪”限定为“杀人、抢劫、集团盗窃、恐吓、绑架、涉及武器、毒品犯罪以及洗钱罪等。但是,对于被指控人与所有有拒绝作证权的人之间的通讯,不得进行监听。为了防止监听权力的滥用,联邦议会要求联邦政府每年必须向联邦议会报告采取监听等措施的情况,各州政府采取监听等措施的情况也得向州议会报告,受州议会监督”<sup>[1]</sup>(第24页)。

## (二)法国

在法国,《刑事诉讼法典》第91条第1款规定,预审法官“应当依据法律进行一切他认为有助于发现真实的侦查”。依据该规定,侦查机关经常性地使用技术侦查手段,如电话窃听等。法国最高法院1980年10月9日判决及以后多次判决肯定了这种做法,但法国侦查机关的这种做法,受到欧洲人权法院的强烈指责,国内各界也纷纷要求将技术侦查手段立法化以规范和指导侦查机关的侦查活动。1991年7月10日,法国专门法律(并入《法国刑事诉讼法典》第100条第6款),专门就电话窃听的一般条件、权限和基本程序作出了明确规定,1993年和1995年又对窃听律师的办公室和住宅以及针对议员和参议员的电话窃听补充作了特殊规定。

法国《刑事诉讼法典》第100条规定,监听措施包括截留、录制和抄录邮电通讯,适用范围是可能判处2年或2年以上监禁刑的重罪或轻罪(“罪行轻重”限定法),条件是“为了侦查的必需”,不包括对住宅内的私人谈话的监听,法国权威学者对此的解释是:“当传统的侦查技术不太有效时,即可采取这种侦查手段”<sup>[2]</sup>(第33页)。根据该条规定,法国侦查中的电话窃听内容可以是私人或非私人电话线路以及电传线路上所进行的通讯,窃听的对象可以是犯罪嫌疑人,也可以是第三人,甚至可以针对律师的办公室

和住宅的电话线路以及国民议会的议员和参议员的电话线路进行窃听。但是,对律师事务所或住宅的电话线路进行窃听,必须事先通知律师公会会长;对于国民议会议员或参议员的电话线路进行窃听,必须事先通知当事人所属议会的议长,否则窃听视为无效。

电话窃听的决定权在法国属于预审法官,即电话窃听必须根据预审法官的授权进行,侦查机关无权自行决定直接适用。预审法官的授权决定必须采用书面形式,并应当具体写明窃听对象的姓名、特征、导致窃听的罪行和允许窃听的期限。授权后的每次窃听与录制活动,都必须制作笔录,写明窃听的日期、开始与结束的時刻;录制的全部材料必须封存。在诉讼过程中,窃听内容的录制和抄录件应当交给犯罪嫌疑人的律师审核,当事人对于窃听到的谈话归属有异议时,可以请求进行鉴定,并可要求检查封存件;如果当事人受到起诉,窃听时录制的谈话可以用作证据使用,但“不得作为证明并不包括在法官受理之案件范围内的轻罪的证据”<sup>[2]</sup>(第 39 页)。

### (三)日本

日本的技术侦查手段主要有监听通讯、窃听、电子跟踪、电子监视等类型。

2000 年,日本通过了《关于犯罪侦查中监听通讯的规则》,该《规则》规定,通讯监听在性质上应为强制性侦查行为。通讯监听仅适用于毒品的犯罪、有关枪械的犯罪和有组织的杀人罪及集团非法越境罪。通讯监听令状的申请,必须具备法定要件。检察官、警司以上的警官、毒品监督官,或者海上保安官向地方法院的法官提出申请,法官认为申请确有理由时,可以签发通讯监听令状,并可以就监听实施附加适当的条件。令状必须载明犯罪嫌疑人的姓名、嫌疑事实的主要内容、罪名、罚条、应受监听的通讯、作为监听对象的通讯手段、实施监听的方法和场所、监听的期间、实施监听的条件、有效期间等事项,法官须在监听令状上签名盖章。

在日本,窃听是侦查人员秘密听取犯罪嫌疑人或者重要参与人口头对话的秘密侦查方式。该技术侦查手段在日本侦查实践中已广泛使用,但立法还没有对窃听及相关内容作出规定。对窃听的性质,学界与实务界都认为窃听属于强制侦查范畴,但在窃听令状类型及其合法性问题上,还存在着两种观点,即窃听可以依据搜查扣押令状或勘验令状而实施;窃听不能依据搜查及扣押令状或勘验令状而实施。

电子跟踪,是指在跟踪对象使用的汽车、携带的行李或者穿着的鞋子等物品上安装微型电子跟踪器,以掌握其所在位置的侦查方式。在日本,电子跟踪主要适用于控制下交付,其他领域尚未经常使用。日本诉讼理论认为,电子跟踪作为一种高科技侦查手段,使用时必须谨慎判断它使用的合法性,在具体案件中,安装电子跟踪器进行的跟踪,与人员跟踪、监视一样,应依其目的的正当性、必要性及手段的相当性等进行判断。

电子监视,是指在一定场所设置视频监控系统,对人的行为等进行连续不断的、自动观察的一种侦查方式。日本学界对电子监视的性质及合法性争论非常激烈,但判例一般认为,对于在公开场合所进行的电子监视,只要符合紧急性、必要性及相当性等任意侦查的条件,应当被容许实施。

综上所述,对以电子侦听为代表的技术侦查手段,各国立法大都进行了规制。在技术侦查手段适用范围和对象上,一般限于较严重的犯罪或者有特殊需要的犯罪,且使用时必须考虑其必要性、适度性;在技术侦查手段的司法控制方面,各国立法大多规定由法官进行司法审查并作出批准决定。同时,各国立法还对技术侦查手段的具体实施程序、期限和法律后果、侦查对象的人权保障等方面的内容作出了明确规定。此外,还有一些国家设立了专门机构或由法官对技术侦查手段的实施进行监督,力求协调好惩罚犯罪与保障人权的关系<sup>[3]</sup>(第 52 页)。

## 三、启示:对我国技术侦查立法及司法控制机制的构想

### (一)我国技术侦查手段的立法与实践考察

从我国现有法律规定来看,首次提到技术侦查概念的是 1989 年最高人民检察院、公安部《关于公安机关协助人民检察院对重大经济案件使用技术侦查手段有关问题的答复》该答复规定 对经济案件一

般不要使用技术侦查手段。对于极少数重大经济犯罪案件主要是贪污贿赂案件和重大的经济犯罪嫌疑分子必须使用技术侦查手段的,要十分慎重地经过严格审批手续后,由公安机关协助使用。1993年的《国家安全法》第10条规定,国家安全机关因侦查危害国家安全行为的需要,根据国家有关规定,经过严格的批准手续,可以采取技术侦查措施。1995年《人民警察法》第16条也类似的规定。但上述法律、法规的规定过于笼统、原则,对技术侦查手段概念的内涵及外延、适用条件、适用范围以及审批程序等都没有作出明确规定,缺乏具体的可操作性。这种立法上的缺陷引发了以下诸多问题:(1)立法过于原则,缺乏具体的遵循标准,导致侦查机关对技术侦查的认识和把握不统一,实际运用操作不规范;(2)立法没有规定有效的监督制约机制,导致技术侦查手段及其结果的使用呈现随意性;(3)立法未赋予检察机关采取技术侦查手段的权力,导致检察机关在需要时难以启动技术侦查手段;(4)由于立法过于原则、笼统,实际采用过程中不规范、随意性强,容易侵犯公民合法权益,特别是侦查相对人的合法权益。

一方面是立法规定上存在缺失,另一方面是随着科学技术发展,越来越多的技术侦查手段被广泛用于侦查实践。例如,目前,在侦查杀人、抢劫、诈骗等严重刑事犯罪案件中,侦查机关已经大量使用技术侦查手段,利用高科技装备和网络监控技术查找犯罪嫌疑人及其个人信息,而且这种侦查手段的使用范围正呈现出不断扩大的趋势。因此,加强技术侦查手段及其司法控制机制研究,修改刑事诉讼法及相关法律、法规,规范技术侦查手段,以保障公民宪法权利的呼声越来越高。

## (二)我国技术侦查及其司法控制机制的立法构想

目前,采取技术侦查手段侦破重大犯罪案件,打击刑事犯罪已成为各国刑侦工作的发展趋势。因此,我国应立足国情,借鉴国外成功的立法经验,以刑事诉讼法修改为契机,在刑事诉讼法典中对技术侦查手段进行较为全面的规定。在立法时,应充分考虑我国的司法体制,注意把握程序正当性原则,兼顾打击犯罪与保护人权的双重功能,尽可能做到立法授权与司法控制并举,力求建构一个较为规范的技术侦查手段体系。具体来说,这种技术侦查手段体系应当包括以下内容:

1. 技术侦查主体。从《国家安全法》与《人民警察法》的规定来看,公安机关和国家安全机关都享有技术侦查权,立法的惟一缺失是没有授予检察机关技术侦查权。因此,笔者认为,应当通过修改刑事诉讼法,在刑事诉讼法中统一作出规定,公安机关、国家安全机关、检察机关都是行使技术侦查权的主体,侦查犯罪必要时都可以采取技术侦查手段发现和侦查犯罪,从而在立法上授予检察机关侦查犯罪时的技术侦查权。

2. 技术侦查的适用条件与适用范围。在适用条件上,必须严格把握“必要性条件”和“相关性条件”。所谓“必要性”是指,在常规侦查手段用尽或者无法采用常规侦查手段,或者常规侦查手段侦查作用微小或者无法达到要求的侦查效果时,确有采用技术侦查手段的必要。所谓“相关性”,包括“人的相关性”和“物的相关性”两个方面<sup>[4]</sup>(第38页)。“人的相关性”是指,严禁对不相关的人员采取技术侦查手段,技术侦查手段针对的对象只能是犯罪嫌疑人、被指控人以及有证据证明与被指控人存在密切关系的其他人员。“物的相关性”是指,技术侦查采用的具体手段和实施技术侦查的范围应当严格限制在与侦查目的有关的内容上,收集证据材料的范围应当仅限于与指控相关联的内容。在侦查实践中,只有同时满足必要性与相关性两个条件,才能获准实施技术侦查手段。

在适用范围上,考虑到某些刑事犯罪的特点、固有特性和破案成本,笔者认为,应将重大的有组织犯罪、危害国家安全犯罪、智能型犯罪与技术型犯罪以及侦破难度大、用常见的侦查手段难以达到侦查目的、社会危害严重的犯罪纳入到技术侦查的适用范围。具体来讲上述刑事犯罪主要有以下几类:(1)危害国家安全犯罪;(2)毒品犯罪;(3)走私犯罪;(4)有组织犯罪;(5)计算机犯罪;(6)重大贪污贿赂犯罪;(7)法定刑在十年以上确须采用技术侦查手段的其他重大犯罪。

3. 技术侦查的司法控制机制。技术侦查的司法控制机制,包括两方面内容,即由谁作为技术侦查的审查决定主体与审查批准程序。

在审查决定主体问题上,有学者主张移植西方,尤其是英美法系国家的司法审查制度,将是否采取

技术侦查手段的审查决定权交由预审法官(或治安法官、侦查法官)掌控。笔者认为,在我国应当坚持宪法和刑事诉讼法的有关规定,确立由检察机关对包括技术侦查手段在内的所有侦查行为进行审查决定的司法控制机制模式,当然,还应确立审判阶段的非法证据排除规则,由人民法院对通过技术侦查手段获得的证据的合法性进行审查,以弥补检察机关对技术侦查的司法控制的疏漏与不足。

在审查批准程序方面,检察机关应当着重审查技术侦查手段适用范围的法定性和适用条件的必要性。检察机关在接到侦查机关的技术侦查申请后,必须审查以下内容:是否属于法定的适用范围,是否具备法定的适用条件,技术侦查手段的介入是否确属必要,适用对象是否确定,是否具有关联性等。经审查符合法律规定的,应当作出批准实施技术侦查手段的决定。决定书应当详细载明涉嫌案由、确定的侦查对象、采用的具体侦查手段、使用范围、使用期限、使用目的以及禁止性规定等内容。一般情况下,只有检察机关按照法定审查程序作出批准决定后,侦查机关才可以实施技术侦查手段。当然,立法也应规定紧急情况下的例外,以应对突发的例外情况,但事后侦查机关应在规定时间内及时提请检察机关备案确认。

### [参 考 文 献]

- [1] [日]山口和人:《两院通过允许监听的基本法修正案》,载《实用法律杂志》1998年第1131期。
- [2] [法]卡斯东·斯特法尼等:《法国刑事诉讼法讲义》,罗结珍译,北京:中国政法大学出版社1999。
- [3] 宋英辉:《刑事程序中的技术侦查之研究》,载《法学研究》2000年第3期。
- [4] 万毅:《西方国家刑事侦查中的技术侦查措施研究》,载《上海公安专科学校学报》1999年第4期。

(责任编辑 车 英)

## The Study and Its Enlightenment on the System of Technical Detection under the Visual Field of Comparison

Wang Bin

(Wuhan University Law School, Wuhan 430072, Hubei, China)

**Abstract:** Along with the development of science and technology, the function of technical detection in crime detection is getting more and more important. For this reason, no matter in the country of the mainland legal system or that of the UK-US legal system, the type of technical detection, the applicable scope, the applicable principle, the examination procedure as well as the keeping and use of detection result have been stipulated explicitly by the legislation mostly, so as to standard the technical detection of its own country. In our country, on the one hand, the technical detection has been stipulated too general and there even is flaws in the legislation, on the other hand, the methods of technical detection are used massively to detect the criminal offense by the investigating institution in the practice, therefore, it is necessary to study and profit from the successful experience of the legislation of technical detection overseas, taking the revision of the Law of Criminal Procedure as the turning point, to stipulate explicitly the technical detection's related questions by the legislation.

**Key words:** way of comparison; technical detection; study and enlightenment