公共场所监控视频的刑事证据能力问题

纵　博

内容提要:公共场所监控视频的刑事证据能力问题主要集中于取证手段合法性和证据的可靠性两个方面。即便公民身处公共场所,也依然享有隐私权,因此公共场所的视频监控在特定情形下仍会因侵害公民隐私权而构成技术侦查行为,对于通过非法实施技术侦查型视频监控行为而获得的公共场所监控视频,应按照非法证据排除规则判定是否予以排除。公共场所监控视频的可靠性主要从视频的生成、收集及流转过程中是否存在影响其客观真实性的因素进行判断,可以采取推定、书面笔录及取证录像、证人证言、专家鉴定意见等方式对监控视频的可靠性进行证明。

关键词:监控视频　技术侦查　可靠性　证据能力

纵博,安徽财经大学法学院讲师。

若将人类活动场所按照性质划分,可分为公共场所、半公共场所、私人场所。公共场所即所有人都可以不受禁止地自由出入的场所,如公园、广场、公路、机场等;半公共场所包括经营性的公共场所(如俱乐部、服装店、饭店、游戏厅等)、单位内部的公共场所、居民小区的公共部分等;而私人场所则仅限于特定的人进入,其他人未经许可不得进入的场所,如个人住宅、办公室、卧室等。[1] 本文的探讨对象——公共场所监控视频,即安装在公共场所、半公共场所的视频监控系统所产生的视频。随着影像技术、电子技术及计算机技术的发展,公共场所视频监控系统在我国已经非常普及,成为一种普遍的社会监控和控制手段。[2] 目前,我国公共场所视频监控系统主要由以公安机关为主的国家机关安装使

〔1〕 参见胡建淼、岑剑梅:《公共摄像监视与公民隐私权保护》,《法学》2008 年第 6 期。

〔2〕 我国公共视频监控系统的建设始于公安机关 2003 年以来开始探索和实施的城市报警与监控系统建设。2005 年,公安部在全国确立了 22 个城市作为试点城市,各省、市确立了 477 个二级、三级试点。经过近几年的建设,全国各地视频监控系统发展极其迅速。截至 2007 年,北京市就已经拥有监控摄像头 26.5 万个,上海的监控摄像头也已经超过 20 万,广州市的监控摄像头已达 25 万个。而西部的重庆市在 2011 年就已经拥有 31 万个监控摄像头。参见:《监视时代,我们的生活还有没有隐私可言》,http://www.21csp.com.cn/html/View_2007/07/26/83549BE7C1.shtml,访问日期:2016 年 6 月 10 日。

用。通过在全国范围进行的监控系统建设,公安机关开始发展出一种全新的警务——监控式警务。作为一种直观、有效的监控方式,视频监控系统可以在降低犯罪率、保障社会秩序方面发挥一定的作用。而在刑事诉讼方面,视频监控系统也具有提供侦查线索、锁定嫌疑人、还原案发现场、保存诉讼证据等功能。

在刑事司法实践中,公共场所监控视频在很多案件中都作为诉讼证据使用。要作为证据使用,首要问题是证据能力问题,即符合何种条件的监控视频才能作为证据使用。根据我国现有规范,能够解读出刑事证据能力的要件为关联性、未因取证手段违法而被排除(即取证手段要具备合法性)、未因无法保障真实性而被排除(即证据要具备可靠性)。[3] 对于公共场所监控视频的证据能力来说,关联性与其它类型证据相比并无多少特殊之处,但其它两个方面则存在可供研究的重要问题:一是由于视频监控系统功能日益复杂、智能化程度越来越高,虽然这类视频是在公共场所视频监控系统中产生,但仍然可能会因侵害公民隐私权而面临着是否构成技术侦查以及是否违法实施并需要排除证据的问题;二是由于目前基本上都是数字化视频监控系统,[4] 其产生的监控视频在证据能力上还面临着可靠性判断的难题。但《刑事诉讼法》和司法解释中却没有能够直接规范公共场所监控视频证据能力的规则。通过调研发现,司法人员在使用监控视频时存在很多疑惑和误解,不知如何判断监控视频的证据能力。[5] 对于监控视频是否会因侵害公民隐私权而构成非法技术侦查所获证据,很少有司法人员考虑到这一问题;对于监控视频可靠性的判断也无统一规则,如有的检察部门要求公安机关在提供监控视频的同时必须移送制作说明、提取笔录等手续,以证明来源、取证程序,而有的检察部门则并无任何要求。

为解决公共场所视频监控在实践运用中出现的问题,应当从学理上构建该类证据的证据能力规则,以保障其实践运用的合理性。因此,本文以法律解释、比较研究、学理分析方法,对公共场所监控视频证据能力中的取证手段合法性、可靠性两个问题进行探讨,为实践中监控视频的使用提供学理支持。

一 公共场所监控视频取证手段合法性问题

公共场所监控视频的取证手段合法性问题,主要集中在是否会侵害公民隐私权方面。概括性、普遍性、不针对特定对象的视频监控,由于并未侵害公民隐私权,所以不存在取证

〔3〕 参见纵博:《我国证据能力之理论归纳及思考》,《法学家》2015 年第 3 期。

〔4〕 视频监控系统的发展经历了三代。第一代是模拟闭路视频监控系统(CCTV),第二代是模拟数字监控系统(DVR),第三代是网络视频监控系统。据统计,2004 年到 2012 年,数字监控在我国总体视频监控市场规模中所占的比例从 35.7% 增长到了 56.7%。与此同时,网络视频监控市场正在稳步增长,所占比例由 2004 年的 7.4% 增长到 2012 年的 28.2%。参见《2012 年中国视频监控行业研究报告》,http://wenku.baidu.com/link?url=ULr-pgqIPr2ToeotJ9htkgh4hBZKLT_QXXb_rUvAL_JZxUpZUucXMKMKbH14V3QXb45_jQ7xe9zxNGhTR1walnFiaCjiOR5KKQXaj6dSiPa,访问日期:2016 年 6 月 10 日。

〔5〕 为了进一步了解因证据规则不足而导致公共场所监控视频在实践运用中存在的问题,笔者在 2012—2013 年曾跟随“视频证据在刑事诉讼中的运用机制研究”课题组在四川省部分基层司法机关对刑事诉讼中公共场所监控视频的实际运用情况进行调研。通过调研发现司法人员对公共场所监控视频如何在司法实践中运用存在很多迷惑和误解,尤其集中于如何判断这类证据的证据能力、证明力方面。

手段合法性问题,但公共场所视频监控如果是针对特定对象的,就可能因侵害公民隐私而存在取证合法性问题。对于公共场所视频监控对公民隐私权侵害的探讨,无论中外都有不少学者论及,[6]但基本都集中于宪法、行政法领域,在我国,刑事诉讼领域中对此问题的关注较少。对于何种监控视频才具有刑事证据能力所要求的取证手段合法性,也基本没有研究涉及。我国 2012 年《刑事诉讼法》已经增设技术侦查一节,在立法理由中明确说明:"技术侦查措施在执行过程中可能涉及公民个人隐私和公共利益,必须在法律中予以明确的规范,加以必要的限制。"[7]由此可见,是否侵害公民隐私权是判断侦查行为是否合法的重要标准,而立法说明也体现出《刑事诉讼法》规范技术侦查行为以保障公民隐私权的立法目的。公安部《公安机关办理刑事案件程序规定》第 255 条界定了技术侦查措施的范围:"技术侦查措施是指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。"在特定情形下,公共场所视频监控是有可能属于上述技术侦查措施的。对于我国公共场所监控视频的取证手段合法性问题,也应从上述技术侦查规范角度,探讨公共场所的视频监控是否侵害公民隐私权并构成技术侦查,如果属于技术侦查行为并且是违法实施的话,所获的公共场所监控视频就属非法证据并可能会被排除。

(一)公共场所视频监控是否会构成技术侦查行为

若侦查机关为获取证据而将视频监控系统安装在私人场所,因对当事人隐私造成直接侵害,当然构成技术侦查意义上的监控行为,未履行批准程序则属违法技术侦查,所获视频也应予以排除。但问题在于,侦查机关利用安装在公共场所、半公共场所的视频监控系统获取证据,是否会侵害当事人隐私权并构成技术侦查?对这一问题的解答,需要先解决另一个问题,即公民在公共场所是否享有不受司法机关干涉、侵害的隐私权。对于这个问题,可以先考察一下域外的理论和实践,然后再从我国隐私权理论及相关法律规范出发进行分析。

1. 美国的公共场所隐私权理论与实践

在西方国家,对于公民在公共场所是否拥有隐私权目前并无统一理论。随着公共场所视频监控系统的普及,各国都存在视频监控与公民隐私权的冲突问题,对此问题研究最为集中的是美国,因此在此主要介绍一下美国的理论及实践。

在美国,将隐私权与刑事诉讼联系起来的是宪法第四修正案,虽然第四修正案字面上并无隐私权的规定,但联邦最高法院通过卡兹案(Katz v. United States),将隐私权作为警

---

〔6〕 国外的研究主要集中在英美,相关文献如 Thomas J. Hickey, Christopher Capsambelis and Anthony LaRose, Constitutional Issues in the Use of Video Surveillance in Public Places, 39 No. 5 *Crim. Law Bulletin ART* 1, (2003); Marc Jonathan Blitz, Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World That Tracks Image and Identity, 82 *Tex. L. Rev.* 1349, (2004); Robert D. Bickel, Susan Brinkley & Wendy White, Video Security Technology Compromise an Essential Constitutional Right in a Democracy, Or Will the Courts Strike a Proper Balance? 33 *Stetson L. Rev.* 299 (2003);国内主要是行政法学者的研究,如胡建森、岑剑梅:《公共摄像监视与公民隐私权保护》,《法学》2008 年第 6 期;李晓明:《公共视频监控系统与隐私保护的法律规制——以上海世博会为视角》,《华东政法大学学报》2009 年第 1 期。

〔7〕 全国人大常委会法制工作委员会刑法室著:《关于修改中华人民共和国刑事诉讼法的决定:条文说明、立法理由及相关规定》,北京大学出版社 2012 年版,第 185 页。

方行为构成搜查的标准,改变了之前的财产权标准,而公民是否具有隐私权则根据他是否具有合理隐私期待进行判断。对于“合理隐私期待”,马歇尔法官设置了“双叉标准”:(1)个人必须表现出真实的主观隐私期待;(2)必须证明他所表现出来的是一种能够被社会公众认可的合理隐私期待。[8] 在卡兹案确定的原则之下,当人们离开住所而身处公共场所时,就只能享有极为有限的隐私权期待。联邦法院通过一系列判例表达出这一观点:在住宅外的垃圾袋中搜索并不构成搜查;在开放场域,人们不能以合理的隐私权期待对抗州的特工人员;在高速公路上行驶的汽车中,人们不能具有合理的隐私权期待;警方通过私人飞机在 1000 英尺的高度观察当事人后院中栽培的大麻,当事人也不享有合理的隐私权期待。[9] 在两件关于警方利用无线电发射器追踪被告人在公共道路上行迹的案件中,联邦最高法院同样认为被告人不具有合理隐私期待。[10] 而卡兹案确定的双叉标准也成为公民在公共场所视频监控下是否具有合理隐私期待的判断框架,因此有美国学者曾指出,虽然目前联邦法院尚无直接针对公共场所视频监控是否侵害公民隐私权的判例,但从以上判例反映的倾向来看,联邦法院似乎不会认为公共场所视频监控会对公民隐私权构成侵扰,因为公共场所中公民并无合理的隐私权期待。[11]

但更多的美国学者则认为,即便在卡兹案所确定的原则之下,也不意味着公共场所视频监控就不会侵害公民隐私权,是否侵害隐私不能以场所来判断,而应以人们是否享有实质隐私权来判断。美国昆汀·布鲁斯(Quentin Burrows)博士认为,公共场所视频监控能够在人们不知情的情况下持续对个人进行监控,能监控到人们所读的信、所说的话,从目力不及的地方就能监控到一个打算堕胎的女性进入诊所的画面,这些都是对人们隐私权的侵害,而如果这些监控视频事后再作为证据使用,就使侵害更加严重。[12] 美国马克·J. 布利茨教授(Marc Jonathan Blitz)认为,人们在公共场所同样具有隐私,如在书店、音像店等地方寻找一些争议性的书籍、音像制品,在公共场所与别人交流,或者获取别人的咨询建议等,在这些活动中人们有不被注意的私密行事权利,因此,法院应该放弃卡兹案中难以判断的隐私权期待标准,而应致力于保护特定环境下的公民隐私权。[13] 因此,根据这些美国学者的观点,即便人们身处公共场所,当公共场所视频监控侵入了人们不想为人所知的活动领域时,依然构成对隐私的侵害。

随着对这一话题的热烈探讨,司法实践也有所进展。在 2011 年的 United states v.

---

〔8〕 参见[美]约书亚·德雷勒斯、艾伦·C·迈克尔斯著:《美国刑事诉讼法精解(第一卷)》,吴宏耀译,北京大学出版社 2009 年版,第 73 页。

〔9〕 Robert D. Bickel, Susan Brinkley & Wendy White, Video Security Technology Compromise an Essential Constitutional Right in a Democracy, Or Will the Courts Strike a Proper Balance? 33 *Stetson L. Rev.* 299 (2003).

〔10〕 Thomas J. Hickey, Christopher Capsambelis and Anthony LaRose, Constitutional Issues in the Use of Video Surveillance in Public Places, 39 No. 5 *Crim. Law Bulletin ART* 1, (2003).

〔11〕 Quentin Burrows, Scowl Because You're on Candid Camera: Privacy and Video Surveillance, 31 *Val. U. L. Rev.* 1079, (1997).

〔12〕 Quentin Burrows, Scowl Because You're on Candid Camera: Privacy and Video Surveillance, 31 *Val. U. L. Rev.* 1079, (1997).

〔13〕 Marc Jonathan Blitz, Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World That Tracks Image and Identity, 82 *Tex. L. Rev.* 1349, (2004).

Jones 一案中,联邦最高法院作出一个突破性判决。该案中,琼斯(Jones)涉嫌贩卖毒品,警方于 2005 年向联邦哥伦比亚特区地方法院申请在琼斯所使用的登记于其妻名下的汽车上安装 GPS 追踪器,法院授权在令状核发后 10 日内安装追踪器,但警方在第 11 日才安装,在之后的 28 日内,警方由 GPS 追踪器获知琼斯动向,相关材料都成为控诉琼斯贩毒的证据。该案上诉至联邦最高法院后,所有法官都认为警察行为构成非法搜查、扣押,但理由却不相同。执笔的斯卡利亚(Scalia)法官认为该案主要是因为警方行为侵害了公民财产权(在车辆上物理性侵入地安装追踪器),所以按宪法第四修正案构成搜查,卡兹案所提出的隐私权标准并未推翻财产权标准。但阿利托(Alito)法官在协同意见书中认为,多数意见所采取的财产权标准并不正确,卡兹案中联邦最高法院已经放弃了财产权标准,明确指出搜查不以物理性侵入为要件,而且财产权标准会产生不合理的结果,因此本案应采取隐私权标准。科技的发展会改变人们对隐私权期待以及关于公共场合活动的看法。虽然每个人都可以知悉特定人在公共场所的个别活动或行为,但仅是特定人的部分或片段信息而已,持续 28 日对个人活动的监控与部分或片段信息不仅是量的差异,更是质的差别,如同个别、细小的瓷砖结合在一起就可以形成马赛克镶嵌画,窥见个人生活的全貌,因此就构成搜查。这就是所谓的"镶嵌论"。[14] 索托马约尔(Sotomayor)法官在协同意见书中虽然认同斯卡利亚大法官的观点,但对于阿利托法官对隐私权的分析也持肯定态度,并且强调,通过全面记录个人于公共场所的活动,就可以由此了解特定人的家庭、政治、专业、信仰甚至性生活的各方面细节,因此对于 GPS 之类科技手段是否侵犯隐私权,审查标准应是:人们是否能够合理预期在公共场所的行动会被政府无遗漏地记录分析。对此她认为人们是无法合理预期到的,所以这种长时间监控构成搜查。[15] 虽然琼斯案并不是直接针对公共场所视频监控的判例,但若将琼斯案中对公共场所个人隐私权问题的分析结果及其规则运用于公共场所视频监控是否侵害隐私权的案件,可以得出同样的结论,即在特定情形中(长时间监控或捕捉人们在公共场所活动的细节),会侵害公民隐私权,构成搜查。

联邦上诉法院曾经作出过直接规范视频监控的判例,如在联邦第十五巡回法院审理的 United States v. Cuevas-sanchez 案中,法官认为,被告人已经在庭园筑起了高 10 英尺的院墙,显示出对隐私权的期待,受第四修正案保护,而警察在其庭园后的电线杆安装视频监控设备记录被告人 30 天的活动,是对公民隐私权的侵害。联邦第十巡回法院也审理过类似案件,即 United States v. Apperson 案,该案中,美国缉毒局怀疑被告人在一个废弃的导弹发射基地生产迷幻剂,在取得法院核发的监视录影令状后,缉毒局特工装设了监视系统对该处进行监视,最终被告人被判有罪。[16] 虽然法官在该案中认为无论控方是否取得令状,视频监控都是合法的,因为被告人是在废弃导弹发射基地从事非法活动,所以没有

〔14〕 David E. Pozen, The Mosaic Theory, National Security, and the Freedom of Information Act, 115 *Yale L. J.* 628 (2005).

〔15〕 参见李荣耕:《科技定位监控与犯罪侦查:兼论美国近年 GPS 追踪法制及实务之发展》,《台大法学论丛》2015 年第 3 期。

〔16〕 参见艾明:《论美国对新型监控侦查措施的法律规制——以 GPS 和视频监控为例》,《山东警察学院学报》2015 年第 6 期。

隐私权期待,视频监控并未侵害被告人的隐私利益,但从反面也可推论出,如果根据案情法官认为本案中被告人具有隐私权期待,那么视频监控就会因侵害隐私而构成搜查。

综上可见,在美国的理论和司法实践中,对于公共场所视频监控是否构成宪法第四修正案意义上的"搜查",是根据视频监控是否针对特定公民在公共场所具有隐私权期待来判定的,如果只是普遍性的、不针对特定对象的监控,并不构成搜查行为,其实施也无需令状;但针对特定对象的隐私事项的监控,尤其是持续性监控,属于搜查行为,应根据令状原则来实施。

2. 我国法律规范中构成技术侦查的公共场所视频监控

从美国的理论及实践发展来看,对于人们在公共场所是否拥有隐私权,经历了从否认到部分肯定的过程,而对于政府对公共场所的公民进行监控是否因侵害隐私权而构成搜查,是根据公民在公共场所从事的行为是否属于私密事项、政府的监控行为是否属于持续性监控等方面具体判断的,这是判断警方的监控行为是否合法以及证据是否可采的前提。基于隐私权在本质上属于人的基本权利,我国也应在法理上扩展隐私权保护范围,科学界定公民的隐私权界限,对公共场所视频监控与公民隐私权的关系进行厘清,才能将公共场所视频监控与技术侦查规范进行对接。

对于隐私权,目前我国主要是由民法规范和保护,[17] 而未像国外那样将隐私权作为宪法层面的基本权利进行保护。在民事法律及司法解释中,并未明确隐私权的内容,但根据我国学者的解释,隐私权主要包括以下几项权利:(1)私生活秘密权。即公民所享有的个人信息不受任何人非法侵扰、截取、搜集、利用和公开的权利;(2)空间隐私权。即个人对特定的空间具有不受他人窥看、侵扰、侵入、破坏的权利;(3)私人生活安宁权。即"个人有独立生活、不被他人打扰的权利",西方也有学者将其称为"被社会遗忘的权利",这是一项较为概括的权利,可以视为隐私权内容的兜底性权利。[18] 若按照这种解读,公民即使在公共场所,也不意味着就是将个人所有信息都公之于众,对于那些个人希望保持隐秘性的信息,国家机关或其他个人都不得任意侵犯,因此在公共场所公民也享有隐私权,如在公共场所接收、发出、处理的各种信息不被侵扰、截取的权利;在公共场所的特定空间做出某种行为时不被人直窥的权利;以及个人在公共场所不被他人关注、打扰的权利。因此,若公共场所视频监控对特定人进行持续的、高强度的、近距离的拍摄,对该人而言就构成高度侵犯性的行为,使其丧失安宁感、私密感,其隐私利益即被侵害。[19] 我国也有学者提出与美国"镶嵌论"类似的观点,认为如果根据遍布各地的摄像头所记录的讯息,就可

〔17〕 2009 年颁布的《中华人民共和国侵权责任法》中,已经在第 2 条将隐私权作为一种民事基本权利。另外,在最高人民法院之前颁布的相关司法解释中也对隐私权保护问题作出一些规定,如最高人民法院《关于执行〈中华人民共和国民法通则〉若干问题的意见》第 140 条第 1 款:"以书面、口头等形式宣扬他人的隐私,或者捏造事实公然丑化他人人格,以及用侮辱、诽谤等方式损害他人名誉,造成一定影响的,应当认定为侵害公民名誉权的行为。"再如 2001 年 3 月 10 日颁布施行的《最高人民法院关于确定民事侵权精神损害赔偿责任若干问题的解释》第 1 条规定:"违反社会公共利益、社会公德侵害他人隐私或者其他人格利益,受害人以侵权为由向人民法院起诉请求赔偿精神损害的,人民法院应当依法予以受理。"

〔18〕 参见王利明:《隐私权内容探讨》,《浙江社会科学》2007 年第 3 期。

〔19〕 参见李晓明:《论公共视频监控系统对公民隐私权的影响》,《法学杂志》2010 年第 11 期。

以发现某人生活关系和交往行为的隐秘信息,那么隐私权侵害可能会发生在私宅,也可能发生在公共空间。[20] 更何况,公共场所的视频监控还有可能会监控到私人场所,对公民隐私权构成直接侵害。因此,公共场所视频监控进行的概括的、不针对特定对象的监控,不构成对隐私权的侵害,但针对特定对象行踪的持续监控、针对特定对象的私密信息的监控或直接对私人场所的监控则会侵害隐私权。

具体到刑事诉讼领域,由于《刑事诉讼法》已经明确规定了技术侦查行为,且立法说明也明确了对技术侦查的规制就是为了保障个人隐私和公共利益,这也就意味着,如果侦查机关利用会侵害公民隐私权或其它公共利益的技术手段收集证据、查获犯罪嫌疑人,就构成技术侦查。[21] 而公安部的《公安机关办理刑事案件程序规定》则采取不完全列举的方式,将记录监控、行踪监控、通信监控、场所监控等措施明定为技术侦查措施,这里的"等"就代表着与上述监控措施类似的对公民隐私具有侵入性、干涉性的侦查措施。按照这种理解,如果侦查机关利用公共场所视频监控系统进行下列行为,就构成对公民隐私权的侵害,根据技术侦查的法律规范及学理解释,应属于技术侦查措施。

其一,利用安装在公共场所、半公共场所的视频监控系统,以数个视频监控对特定人进行组合接力式的追踪监控。如前分析,仅对个人在公共场所的行踪片段进行常规的监控,通常不会构成对隐私权的侵害,但利用数个视频监控进行持续的行踪监控则会获取个人生活的"马赛克"全景图,揭露个人不欲为人知的连续行动过程,因此与利用电子设备进行行踪监控产生同样的效果,属于行踪监控类技术侦查行为。

其二,利用安装在公共场所、半公共场所的视频监控系统,通过其放大、录音、遥感等高级功能对公共场所中特定人的隐秘信息进行监控。若仅是通过视频监控系统对不特定人进行概括性的监控,不会构成对个人隐私的侵害,因为这种监控与在公共场所用肉眼观察的性质相同。但利用视频监控系统的高级功能收集特定人的隐秘信息,如利用放大功能窥看个人正在读取或发送的手机短信、利用录音功能监听对话、利用遥感成像对人进行深层窥视,都是直接侵害个人在公共场所的隐私权,属于通信监控、记录监控类技术侦查行为。

其三,通过安装在公共场所、半公共场所的视频监控系统对私人场所进行监控。目前视频监控系统的安装并没有统一的规范,各地政府机关管理的视频监控系统都是依地方需要进行部署安装,即便这些视频监控系统是安装在公共场所和半公共场所,也不可避免地会将私人场所纳入监控范围,更何况多数治安管理功能的视频监控系统都采用球形可旋转摄像头,所以就可能会透过院墙、窗户而监控到私人的卧室、办公室、卫生间、浴室等。如果侦查机关故意通过公共场所、半公共场所的视频监控系统对私人场所进行监控,就与在私人场所安装隐蔽性监控设备毫无二致,构成场所监控类技术侦查行为。

(二)对公共场所监控视频的取证合法性判断

根据美国的理论和实践,既然公民在公共场所也享有一定隐私权,那么政府对公民私

〔20〕 参见胡建淼、岑剑梅:《公共摄像监视与公民隐私权保护》,《法学》2008 年第 6 期。

〔21〕 参见胡铭:《技术侦查:模糊授权抑或严格规制——以〈人民检察院刑事诉讼规则〉第 263 条为中心》,《清华法学》2013 年第 6 期。

密事项进行的视频监控自然也会构成宪法第四修正案意义上的搜查,也必然会有合法搜查与非法搜查之分。因此,对公民在公共场所活动进行的视频监控是否属于合法监控,是由法官在宪法第四修正案的合法搜查要件的框架下判断的,也即法官在颁发令状时或事后审查时,根据此类监控是否构成宪法第四修正案意义上的"搜查",以及这种监控是否必要、是否是最后手段、监控的实施是否超出令状许可范围等方面综合判断,如果认为属于违法搜查就可能会不签发令状或排除监控视频。在 United States v. Cuevas-sanchez 案和 United States v. Apperson 案中,法官都曾经提出具体的合法性判断标准。前一案件法官认为,在进行这类电子监控时,应遵循如下要求:(1)法官签发令状时应审查侦查机关是否已经穷尽其它调查手段;(2)该令状必须针对法律规定的特定犯罪;(3)授权期限不得超过 30 日或调查所需的必要时间;(4)令状应当符合最小侵害原则。后一案件法官提出的标准与之类似。[22] 可见在美国的司法实践中,对于公共场所监控视频的合法性问题被纳入了对强制侦查行为的司法审查制度中,通过法官对视频监控是否构成强制侦查行为、是否符合法定条件而进行判断。

对于我国来说,既然公共场所视频监控也可能构成技术侦查行为,那么自然也就会面临着取证是否合法的问题,而对于是否合法要根据《刑事诉讼法》及司法解释规定的技术侦查批准、实施程序进行判断。在批准与实施程序方面,公共场所视频监控与其它技术侦查手段在很多方面都是相同的,因此如果侦查机关明知上述行为属技术侦查应当在批准后进行,还故意未经批准而实施,或者故意超越批准范围、期限而实施,就属于非法技术侦查行为,所获得的监控视频就属于非法证据。但在这种非法证据的排除方面,由于《刑事诉讼法》第 54 条仅规定了非法物证、书证的排除,明显有立法的漏洞,因此可采取类推适用方式,将其归类于广义"物证"的电子数据、视听资料。[23] 如果侦查机关非法实施技术侦查型视频监控且情节恶劣、对当事人造成严重侵害或在社会上造成恶劣影响,就不应允许其补正或合理解释,而应直接排除;如果未达到上述严重程度,仅是在批准程序或具体执行方面有轻微瑕疵,可以允许补正或合理解释,经过补正或合理解释的监控视频可以恢复证据能力而在诉讼中作为证据使用。[24]

但公共场所视频监控的取证合法性判断中有两个问题需要在实践中予以注意。

一个问题是根据监控行为的侵害性程度把握必要性原则。相对于其它普通侦查措施,技术侦查容易对公民权利造成较大损害,因此应遵循必要性原则,即只有在其它侦查措施难以取得证据的情况下才允许使用技术侦查措施。[25] 对于公共场所视频监控来说同样如此,如果采取其它措施能够实现侦查目的,就无需采取追踪监控、隐私信息监控等

〔22〕 参见艾明:《论美国对新型监控侦查措施的法律规制——以 GPS 和视频监控为例》,《山东警察学院学报》2015 年第 6 期。

〔23〕 参见万毅:《关键词解读:非法实物证据排除规则的解释与适用》,《四川大学学报(哲学社会科学版)》2014 年第 3 期。

〔24〕 对于证据的补正和合理解释问题,只有取证手段轻微违法的证据才属于瑕疵证据,也才可以补正或合理解释;严重违法的属于非法证据而非瑕疵证据,不应允许补正或合理解释,而应直接排除。参见陈盛、纵博:《瑕疵证据规定的法律解释分析——以〈刑事诉讼法〉第 54 条为对象》,《法律方法》2014 年第 1 期。

〔25〕 参见詹建红:《理论共识与规则细化:技术侦查措施的司法适用》,《法商研究》2013 年第 3 期。

手段。若不符合必要性原则,即便监控措施经过批准,也可认定属于违法取证。但对于公共场所视频监控可能构成技术侦查的几种情形来说,其对公民隐私权的侵害性是有差别的。理论上来说,对公共场所特定人进行接力追踪监控的隐私权侵害程度最小,因为传统的跟踪、盯梢、监视也能达到同样效果,只不过是以视频监控取代了人力,使追踪监控更具有技术性、持续性,虽然也属于技术侦查行为,但毕竟监控的是个人在公共场所的行迹、动向,所以相比监听、通讯截取等技术侦查措施来说,隐私权侵害程度较低;而隐秘信息监控则相对来说侵权程度要高,因为个人难以预见其在公共场所时个人的隐秘信息会被他人监控;对私人场所的监控侵害程度最高,因为这是直接对个人隐私的全面侵入,尽管利用的是公共视频监控系统。三种监控方式中,接力追踪监控隐私权侵害程度小于隐秘信息监控,这两种监控方式都小于私人场所监控。在审查各种监控形式的必要性时,除考虑常规侦查手段获取证据的难度外,也要考虑监控的隐私权侵害程度,对于程度较轻的监控方式,其必要性判断可适当放宽,对于程度较重的则应严格控制,综合这些因素判断监控的批准、实施是否合法以及是否应当排除监控视频。

(三)监控中收集的它案信息是否合法

在经批准的技术侦查型公共场所视频监控的实施过程中,可能会意外获得其它案件、其它个人的信息,那么这些信息是否可以作为合法证据呢。《公安机关办理刑事案件程序规定》第 255 条对技术侦查的适用对象作出规定:“技术侦查措施的适用对象是犯罪嫌疑人、被告人以及与犯罪活动直接关联的人员。”根据这一规定,技术侦查的适用对象范围限制主要是对人的范围的限制,关键点在于何谓“与犯罪活动直接关联的人员”,因为对其范围的解释决定了技术侦查能延伸到多大的实施范围,所谓“与犯罪活动直接关联”,包括与犯罪行为、犯罪场所、犯罪收益、犯罪结果等方面具有直接的联系,对其进行监控能够对证明、指控犯罪发挥直接的作用。因此,在申请进行技术侦查型视频监控时,侦查人员应当证明被监控的对象与犯罪行为之间的关联性,如被监控者与特定犯罪行为、地点、财物之间的联系,若无法证明这种联系,则不得对该人进行视频监控。但由于公共场所视频监控系统的监控范围较广,在实施中不可避免地会发现与本案并无联系的其它案件信息,因此就面临着它案信息是否可作为证据的问题。之所以要解决这一问题,主要是为了防止侦查机关以监控属于技术侦查适用案件范围的本案为借口而故意对不属于适用案件范围的它案进行监控。

从比较法角度来看,对于这种情形,美国的判例认为一般应重新提出申请,获得法官许可后证据方可具备可采性,否则只能作为侦查它案线索使用,但如果属于类似犯罪、不可分、默许授权几种情形,则作为例外可以具备可采性。德国的学说和实务也采与此类似的见解,认为若 A 与 B 罪名具有关联性,则对 B 的监控具有证据能力,若不具有关联性,则可作为侦查线索使用。[26] 可见,对于监控中偶然发现它案线索的情形,美、德均不直接承认其证据能力,而仅承认例外情形下的证据能力,且需经过补办手续之后方可作为证据使用。在我国,由于《公安机关办理刑事案件程序规定》已经将技术侦查的对象界定为

〔26〕 参见吴巡龙著:《刑事诉讼与证据法全集》,新学林出版股份有限公司 2008 年版,第 147 - 153 页。

“与犯罪活动直接关联的人员”,因此,在监控过程中如果发现在犯罪行为、地点、结果等方面与本案均无直接联系的它案线索,为防止侦查人员故意声东击西、随意扩大监控范围,应根据它案性质而作出不同处理。若它案属于技术侦查适用案件范围,必须补办批准手续后方可作为证据使用;若不属于技术侦查适用案件范围,则只能作为侦查线索使用。

以上对于我国公共场所视频监控是否会构成技术侦查行为、对监控视频的取证合法性的判断,都是从理论上对现有规范进行的理想化解释。但问题在于,由于我国在侦查控制理念方面与美国尚有一定差距,也未建立普遍有效的侦查行为司法审查制度,所以针对公共场所视频监控行为及其结果,监控视频的合法性判断会面临更多的困难。因为相对而言,美国对于公共场所视频监控合法性判断就是直接采用搜查的判断标准,只要法官认为公共场所视频监控侵害公民隐私而构成搜查,且警方未申请令状而采取,或突破令状许可范围而实施,就可直接宣告监控视频为非法证据,其判断过程较为直接,对于警方的指引作用也更具体。而在我国,由于技术侦查规范较为粗疏、非法证据排除规则并不完善、隐私权保护程度较低,所以在实务中对于公共场所视频监控是否侵害隐私权、是否属于技术侦查、是否违法实施、是否要排除证据,基本上只能由司法人员自由裁量,而裁量结果将具有极大的不确定性。如果更悲观一些来看,目前刑讯逼供、变相刑讯等严重违法取证行为尚且未能完全消除,更遑论对于公共场所视频监控这种“外观无害”的侦查行为!再加上对于技术侦查并无司法审查制度,仅需要侦查机关自行审批即可,因此也无法根据是否遵循司法审查这种程序性标准判定其合法性,而对于侦查机关是否依法履行了内部“严格的批准手续”,法官是难以进行有效审查的,因此司法审查制度的缺失同样增加了公共场所监控视频合法性判断的难度。尽管如此,在《刑事诉讼法》明确将“尊重和保障人权”纳入法律目的之后,对刑事诉讼中公民隐私权的重视程度必将日益提升,对公共场所视频监控这类具有潜在侵害性的侦查行为的控制也将逐渐严格。

二 公共场所监控视频的可靠性

证据能力要件应当包含证据的可靠性,即证据未因不具备保障真实性的条件而被排除。之所以要用“可靠性”这一概念,是为了与证明力意义上的“真实性”、“客观性”进行区别,可靠性是指证据必须有一系列条件能够保障其客观真实性,如果不具备这些条件,证据就很有可能(但未必一定)是虚假的,在这种情况下,为了不造成错误认定案件事实,只能将这些证据排除,否定其证据能力。因此,与证明力意义上的“真实性”、“客观性”不同的是,可靠性并不是指证据的实质真伪,而是指是否有条件保障其真实性。即便具备可靠性的证据也未必是客观真实的,相反,不具备可靠性的证据也未必就一定是虚假的,但由于它具有虚假的风险,才否定其证据能力。所以可靠性实际上是将证明力问题转化为证据能力问题,〔27〕主要用于排除那些在自身性质方面或取证程序方面导致可能虚假,且

〔27〕 所谓证明力问题转化为证据能力问题,正如我国台湾地区学者李学灯所言:“证据容许性之各种法则,除因其他外部之政策而发生者外,迹其渊源,更多由于防止不可信之危险。换言之,即由于证据力之问题而转为证据能力之限制。”参见李学灯著:《证据法比较研究》,台湾五南图书出版公司 1992 年版,第 467 页。

本身真伪不明的证据。也就是说,如果能够确定证据确属真实,即便证据不符合可靠性要求,也可以不排除证据。英美法系很多证据规则都属于可靠性规则,如传闻证据规则、意见证据规则、鉴真规则、最佳证据规则等。但这些规则都有一些例外,创设例外的原因就在于当证据的真实性能够得以保障时,就可以免除可靠性规则的适用,如针对传闻证据的当场印象、激奋言词、当时存在的精神、感情或身体状况等例外。

我国2010年《办理死刑案件审查判断证据若干问题的规定》中也增设了若干证据的可靠性规则,2012年《最高人民法院关于适用〈中华人民共和国刑事诉讼法〉的解释》(以下称《解释》)则基本全部吸收了这些规则,如《解释》第73条第1款规定,在勘验、检查、搜查过程中提取、扣押的物证、书证,未附笔录或者清单,不能证明物证、书证来源的,不得作为定案的根据。就是因为无法证明来源的物证、书证是不可靠的,所以才将其排除。[28] 对于其它种类的证据,《解释》也对何种情况下因不具有可靠性而应排除作出了规定。

因目前的公共场所视频监控系统基本上都是数字或网络系统,所以监控视频属于数字化的视听资料,对其可靠性的判断要同时根据电子数据、视听资料两种证据的特征而进行,在这一点上,监控视频与其它数字化音像资料(如智能手机、数码相机等录制的视频)的性质是类似的,其可靠性判断方式也类似。但问题在于,我国在法律规范上对如何判断电子数据、视听资料的可靠性缺乏可操作性的规范,《解释》对于这两类证据的可靠性是与其证明力判断放在一起规定的,而且规定过于简单,仅规定经审查无法确定真伪的,或制作、取得的时间、地点、方式等有疑问,不能提供必要证明或者作出合理解释的应当排除。这种简单的规定无法满足实践中对科技含量日趋增加的数字化监控视频的可靠性判断需要。[29] 同时,理论上对此也缺乏研究,大多是集中在电子证据的证据能力方面,并且基本上是泛泛而谈,无法满足实践操作的需要。因此有必要根据数字化监控视频的生成过程,对从哪些方面判断其可靠性进行解析,以便实践中司法人员可以通过判断而排除那些不具有可靠性且无法确定其真实性的监控视频。美国针对监控视频等实物证据的鉴真规则与我国上述证据可靠性规则功能类似,我们依然可以从美国这方面的理论与实践获得启示。

(一)美国的监控视频鉴真规则及理论

在美国的证据规则中,对于实物证据是否具有可采性,要通过鉴真规则的检验,也即要证明该展示证据就是案件所涉及的证据物,且没有发生改变,[30] 如果无法证明就要将证据排除,所以鉴真实质上就是对证据的可靠性判断。对于监控视频来说,必须通过鉴真程序证明监控视频没有发生歪曲、变形等情况。为满足鉴真的需求,证据提出方必须以其它证据证明监控视频的可靠性,即证明监控视频如实记录了案件的相关情况且没有发生

〔28〕 最高人民法院研究室著:《〈最高人民法院关于适用中华人民共和国刑事诉讼法的解释〉理解与适用》,中国法制出版社2013年版,第56-68页。

〔29〕 值得注意的是,最高人民法院、最高人民检察院、公安部于2016年9月9日联合颁布了《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》,对刑事诉讼中电子数据证据的收集程序、移送和展示要求、审查要点作出了若干规定,但该司法解释依然未对如何判断电子数据的证据能力作出完善、全面的规定,尤其是对于电子数据的可靠性方面规定不足,而且整个解释文本逻辑体系混乱,对司法实践的指导作用有限。

〔30〕 参见[美]罗纳德·J.艾伦等著:《证据法:文本、问题和案例》,张保生等译,高等教育出版社2006年版,第214页。

改变或替换。鉴真集中于地点、日期、时间、画面的局部或整体变化。对于地点比较容易证明,而日期与时间往往是显示在监控视频上的,如果没有显示的话,就需要证人进行证明。最为关键的就是第四方面的证明,即证明视频中所录制的画面就是实际发生的事实。对于数字化的视频证据来说,要证明的是视频中的画面就是准确的、完整的对事实真相的最初录像。对于这一点,通常需要证人宣誓作证进行证明,但当不存在这类证人时,就需要从技术上进行鉴真。另外,无论对于模拟的视频证据,还是数字化的视频证据,都需要进行保管链条的证明,因为对于这类证据来说,接触到证据的人都有可能会修改、伪造证据。为了实现对保管链条的证明,美国的科学家们发明了数种技术手段,如水印、数字签名、加密等。最后,为了对视频证据进行鉴真,有时不得不依靠专家证人对监控视频的完整性、可靠性进行证明。[31] 需要注意的是,对监控视频进行必要的编辑并不意味着就不符合上述鉴真要求,只要进行编辑的人对编辑过程进行妥善的说明,使法庭对监控视频可靠性没有怀疑即可。但是,如果对监控视频的编辑影响到可靠性,就会导致其不具有可采性,如压缩过度而产生了重影或假象,就会导致该证据不具有可采性。[32]

美国还有其他学者对录像证据的鉴真内容进行了更为细致的归纳,根据该学者的观点,录像证据在生成及保存的过程中,可能会受到多种因素影响而发生失真、歪曲、伪造,因此,对录像证据的鉴真必须对所有容易被注意到的、不容易被注意到的、因录像系统本身造成的、由人为原因而造成的可能虚假之处进行审查,主要包括以下一些方面:(1)在进行拍摄和录制时,因设备成像的原因而导致的图像与真实情况不一致,也即俗谚所称的"地图并非领土";(2)因录像制作者的主观原因而导致的图像失真或歪曲(或任何其他安装自动录像设备的人);(3)因录像录制的环境而导致的图像失真或歪曲,如背景光线、声音等;(4)因录像设备或播放设备的性质而导致的失真或歪曲,如在法庭上使用电视机播放录像证据而导致的失真;(5)因录像设备或播放设备的自身缺陷而导致的失真或歪曲;[33](6)有经验的录像制作者在制作录像或者进行编辑时故意造成的篡改或歪曲;(7)有经验的录像制作者在制作录像时采用高级电影制作技术(如好莱坞技术)而导致的篡改或歪曲,使本来未曾作出某种行为的人在录像上显示的却是作出这种行为;(8)在通常的编辑过程中故意造成的篡改或歪曲;(9)在数字化编辑过程中故意造成的篡改或歪曲。[34]

至于鉴真的方式,在美国的成文法中有一些原则性但并非绝对性的规定。如美国《联邦证据规则》第 901(b)对鉴真的方式作了列举,但在开头就明确说明:"以下仅是能

〔31〕 "IACP Study onIn-Car Cameras: The Impact of Video Evidence on Modern Policing", http://www.cops.usdoj.gov/Publications/video_evidence.pdf. 访问日期:2016 年 6 月 10 月。

〔32〕 James A. Griffin, A Prosecutor's Guide to Obtaining and Presenting Audio and Video Evidence, 29-*DEC Prosecutor* 30, (1995).

〔33〕 原文献注释:"即便将上述情形都予以考虑,各个不同的录像系统,包括录像系统的每个特定部分(如摄像机、录像机、录像带、存储设备、编辑设备等)都有可能导致证据的真实性受到影响,无论这些部分可能导致的影响是多么轻微。"

〔34〕 Jordan S. Gruber, Christopher M. Nicholson and Joshua A. S. Reichek, Video Technology, 58 *Am. Jur. Trials* 481 (Originally published in 1996).

够满足该要求(鉴真与辨认)的证据的示例,这些示例并非全部清单……”然后在 901(b)的(1)至(9)列举了知情证人的证言、关于笔迹的非专家意见、专家证人或者事实审判者所进行的比对、关于过程或者系统的证明等九种鉴真方式,并且在(10)规定了一个兜底性的规定:“联邦制定法或最高法院制定的规则所允许的任何鉴真或辨认方法。”可见,在《联邦证据规则》中,虽然进行了鉴真方法的列举,但并不意味着鉴真仅限于这些方法,更不意味着要求某类证据必须采取哪种鉴真方法,具体采用哪种方法,根据案件具体情况进行选择。[35] 根据成文法及判例,对视频类的电子证据,可采取以下鉴真方式:[36](1)诉讼当事人的自认可以使证据得到鉴真,即如果当事人通过自认的方式对证据的真实性表示认可,证据的鉴真即可完成,这是一种普遍使用的方法;(2)由适格证人通过具结作证方式证明,可以使证据得到鉴真。所谓“适格证人”,一般要对监控系统及计算机有特殊的知识或经验,或者对监控系统及计算机的运行及数据有所掌握;(3)有证据证明监控系统在关键时刻处于正常状态的,推定监控视频具有真实性,可以使其得以鉴真;《联邦证据规则》在第 901 条(b)(9)中也明确规定,描述用于产生某种结果的过程或系统,并表明该过程或系统产生了准确结果的证据,就可以满足第 901(a)条的要求。也就是说,第 901 条(b)(9)中对系统产生准确性结果的证据,足以对 X 光、照片、录像、计算机记录等证据进行鉴真;[37](4)对于监控视频的电子文件来说,如果附有电子签名或附有其它适当的安全程序保障,就可以使该视频得以鉴真;(5)由适格专家鉴定未遭到修改的电子文件,可以使电子文件得到鉴真。需要注意的是,这里的“鉴定”目的是使电子文件完成鉴真的任务,所以只需要证实电子文件未被修改、伪造即可,鉴定之后,电子文件就具备了可采性,但其证明力如何,可能仍需要进一步鉴定。

从以上美国对监控视频鉴真的实践及理论可以看出,鉴真就是对监控视频的生成及流转过程中各个环节都能够保障其真实性进行证明,从而使其具备可采性的基础。但通过鉴真的检验也不表示监控视频就一定是真实的,鉴真只不过是从形式上表明,该监控视频在生成及流转过程中没有出现明显的导致其可能失真的因素。至于其是否真实、是否具有证明力,则并非可采性问题,而是证明力判断阶段的问题。另外,鉴真采取自由证明的方式,并无严格的证明规范,对于用于鉴真的证据也并无可采性要求,并且可以采取较为简便随意的方式进行证明。

(二)我国公共场所监控视频的可靠性判断及方式

1. 监控视频的可靠性判断要点

在我国司法实践中,司法人员之所以不知如何判断监控视频的证据能力,主要就是因为对监控视频的可靠性判断缺乏规范及理论指引,所以部分司法人员对于采纳这种证据感觉没有把握。因此,在规范不足的情况下,就要从证据理论上根据监控视频的生成、收集及流转过程,对如何判断其可靠性进行解析。原则上,对于目前普及的数字化/网络监

〔35〕 参见王进喜著:《美国〈联邦证据规则〉(2011 年重塑版)条解》,中国法制出版社 2012 年版,第 310 - 313 页。

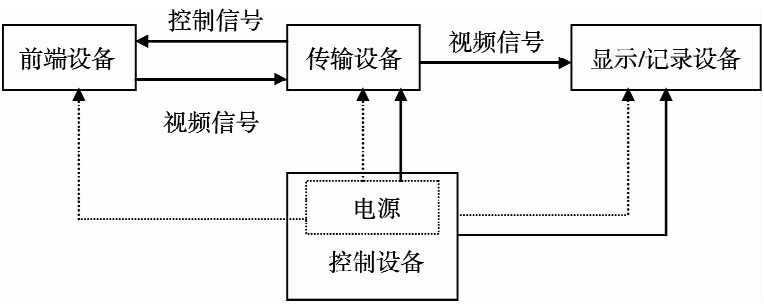
〔36〕 参见何家弘、刘品新著:《电子证据法研究》,法律出版社 2002 年版,第 126 - 130 页。

〔37〕 参见王进喜:《美国〈联邦证据规则〉(2011 年重塑版)条解》,中国法制出版社 2012 年版,第 314 页。

控视频的可靠性,应从以下几个要点进行判断。

第一,必须证明监控视频的生成过程不存在影响其真实性的因素。一般来说,数字化/网络视频监控系统都是由四个最基本的部分构成,即前端设备、传输设备、显示/记录设备、控制设备。前端设备包括摄像机、镜头、防护罩、云台和解码器等,构成整个系统的"眼睛",作用是将监控目标的光信号变为电子信号。传输设备是系统的信号通路,传输的信号包括图像信号、控制中心通过控制台对摄像机等前端设备进行控制的信号等。显示/记录设备主要作用是显示视频监控的图像或声音,并将图像、声音保存在特定的电脑、硬盘录像机中,以备作为证据使用时进行提取。控制设备主要包括主机、主控制台、矩阵切换器及键盘等设备,用于实现视频切换和通讯控制带云台的摄像机动作等功能。[38] 视频监控系统如下图:

图:视频监控系统结构



在监控视频的生成过程中,设备的不合格或故障会导致视频失去可靠性。摄像机、云台设备的光学元件、声音录制元件损坏、云台无法精确控制,会影响图像的可靠性、完整性;如果传输系统出现问题,监控视频的质量也会受到影响,如传输中受到无线电、电磁等干扰,会造成图像失真;而存储载体的物理空间大小、质量好坏同样会影响监控视频的可靠性、完整性。

由上可见,生成过程的可靠性主要是依赖于系统的可靠性,那么如何判断系统的可靠性呢? 对于视频监控系统的技术标准,在我国公安部发布的《视频安防监控系统技术要求》(GA/T 367 - 2001)及其主编的《视频安防监控系统工程设计规范》(GB 50395 - 2007)中已经进行了较为详细的规定,所以有学者主张,对于使用不合格设备录制的视听资料,均不得作为证据使用。[39] 笔者认为这种观点太过偏激,对视听资料的生成要求太高,在目前的中国还不现实。系统设备不合格固然可能会影响视听资料的品质,但只要能够保障基本的真实性,所生成的证据依然是具有证据能力的,若一概排除,不符合证明资源有限性原理。所以对于不符合技术标准的视频监控系统所生成的监控视频,要审查该系统是否能够正常运行,是否能够客观、准确地记录事实,若是能够正常运行、不会严重影响监控视频的客观真实性,就是可靠的系统,所产生的证据就具有证据能力。另外,即便

〔38〕 参见罗世伟、左涛、邹开耀著:《视频监控系统原理及维护》,电子工业出版社 2012 年版,第 2 页。

〔39〕 参见何家弘著:《证据的审查认定规则——示例与释义》,人民法院出版社 2009 年版,第 291 页。

视频监控系统的各个组成部分均符合上述技术标准,也不意味着所生成的监控视频就必然具有真实性,因为监控视频的生成过程中会受到各种复杂因素的影响,如传输过程中受到雷击,就可能使图像丢失或损坏,因此即便对于符合技术标准要求的视频监控系统所生成的证据,也要审查证据生成时系统是否运转正常。

第二,必须证明证据的收集过程中不存在影响其真实性的因素。监控视频生成后,在视频文件的提取、压缩、格式转换、编辑过程中,都有可能导致监控视频失真,因此证据的收集环节影响监控视频可靠性的因素包括证据来源、取证的技术标准、固定证据的程序等。对于证据来源的证明,我国法律及司法解释有明确规定,如《刑事诉讼法》要求搜查、扣押要制作笔录并进行签名、盖章;《解释》要求对于视听资料、电子数据要附带相关的书面制作说明,复制件还要说明复制过程和原件存放地点等;《公安机关办理刑事案件程序规定》也要求搜查、扣押要制作笔录,并且在调取证据时要制作调取证据通知书,并对取证过程进行相应的记录,以证明取证过程及证据来源的合法性,然而对于取证的技术标准及固定证据的程序等,则缺乏相应的规定,尤其是对于电子数据、视听资料的取证技术规范,法律及司法解释都没有进行规范。但按照电子数据、视听资料的特征,对监控视频进行的取证过程应遵循如下几点技术要求。

一是对监控视频的提取,必须取得与视频监控系统中内容完全一致的文件,以保障证据的全面性。一般来说,目前的视频监控系统文件都存储在硬盘录像机或电脑硬盘里,提取、固定的方式主要是文件复制,而不可能提取视频监控系统的硬盘录像机或电脑硬盘。但在复制文件时,为了保障证据信息全部被提取,不能采取日常生活中的简单文件复制,而必须对磁介质中所有的数据按照其存放格式进行全部复制。复制监控视频文件的方法一般有两种,一种是利用系统自带的复制功能进行复制,另一种是根据监控视频的文件命名规律进行复制,〔40〕但无论采用哪种方法,都必须遵循无损固定原则,保证所进行的是无损复制,将监控视频所包含的附属信息、环境信息等附随信息全部复制,如文件生成时间、文件大小、修改时间等信息。〔41〕 对于监控视频,不可采用的复制方式是直接拍摄法和信号转录法。〔42〕

二是在提取证据过程中,应当采取一定的措施保障证据的完整性。目前对于电子证据的技术保护措施有很多种,如数据隐藏技术、数据加密技术、数字签名和数字时间戳技术、数据摘要技术等,〔43〕这些技术的主要功能都是可以证明证据在一定期间内没有被修改、删除,因此可以证明信息的完整性、真实性。因此,在提取监控视频文件时,最好是由具有计算机知识的侦查人员进行证据的收集和固定,以便在提取过程中采取上述保护措施,防止证据被删除、修改,同时也为诉讼中证明证据的真实性和完整性提供保障。

---

〔40〕 参见廖根为著:《监控录像系统中人像鉴定问题研究》,上海人民出版社 2010 年版,第 31 - 33 页。

〔41〕 参见刘品新著:《电子取证的法律规制》,中国法制出版社 2010 年版,第 315 - 317 页。

〔42〕 所谓直接拍摄法,即直接对播放的视频进行拍摄而形成的文件,这将会大大降低视频的质量。所谓信号转录法,是指直接将显示器输出的信号转录为数字文件,这种方法受显示器的影响较大,也会降低数据的质量。参见廖根为著:《监控录像系统中人像鉴定问题研究》,上海人民出版社 2010 年版,第 34 页。

〔43〕 参见蒋平、杨莉莉著:《电子证据》,清华大学出版社 2007 年版,第 142 - 144 页。

三是在提取证据之后,因为视频监控系统生成的文件未必是通用格式,因此,可能需要进行视频格式的转换。目前视频监控系统大多采用的编码技术有图像帧独立压缩技术、活动图像专家组(MPEG)系列标准和视频编码专家组(H.26X)系列标准。因不同地方播放设备的不同,可能需要在上述编码之间进行格式转换,在转换时,需要采用可靠的视频格式转换软件,在转换过程中,不能损坏视频的数据流,要保障视频文件的数据信息、附属信息和环境信息均完整无损。

四是由于提取的视频监控往往比较长,有时需要进行编辑,但编辑只能是必要的编辑,如在长达数天的监控中,具有关联性的仅为其中几分钟的抢劫录像片段,必须进行编辑才能将该监控证据在法庭播放展示。但是编辑不得破坏监控记录待证事实的完整性和连续性,如果不当的编辑导致无法精确的反映待证事实,或者会造成事实裁判者产生混淆、错误认识,就无法保障其可靠性。[44]

若取证过程不符合上述技术性规范,就可能会导致监控视频的真实性、完整性受到损害,不符合可靠性要求,属于应当排除的证据。

第三,必须证明监控视频的保管链条完好,不存在影响其真实性的因素。在取证之后,往往会经过较长的时间案件才能进入审判阶段。在此之间,证据可能会在不同主体之间流转,如由技术人员交给侦查人员,再由侦查人员交给公安机关法制部门,然后再送还给侦查人员,侦查人员移送批准逮捕或起诉时交给检察人员,最后才随案卷移送到法院。为了防止在这些流转过程中发生对证据信息的修改、删除,应当建立完善的保管链条制度,即在每一个流转环节都有相应的书面手续证明经手主体的身份、时间、目的等,如果发生手续的间断或手续不全,就足以对证据的客观真实性产生怀疑。我国的法律及司法解释中,对于各类证据的保管链条问题并不重视,也缺乏相应的规定。但保管链条的完整性对于实物证据的真实性保障来说,无疑是非常重要的。如果保管过程缺乏相应的手续和必要的书面证明,证据在流转过程中极容易被修改、删除、毁灭。在美国,对于录音录像等证据,用保管链条的完善证明其真实性是一个通行的做法,对于录制品而言,无论是有证人的,还是没有证人而自动拍摄的,都需要提供从录制到提交法院的完整保管链条的证明。[45] 因此,在对监控视频可靠性的证明中,我国也应将保管链条作为需要证明的内容之一。监控视频的保管链条包括物理部分的保管链条及数据部分的保管链条两个部分。物理部分的保管链条即对监控视频文件的存储介质、载体的保管链条,数据部分的保管链条即通过数据的技术保护措施而设置的保管链条。只有这两个部分的保管链条都是完整无缺的,才能证明监控视频的可靠性。

2. 监控视频的可靠性证明方式

根据我国现行法律及司法解释规定,结合对美国鉴真方式的参考,对于监控视频的可靠性,主要可采取以下方式进行证明。

---

〔44〕 "IACP Study on In-Car Cameras: The Impact of Video Evidence on Modern Policing", http://www.cops.usdoj.gov/Publications/video_evidence.pdf. 访问日期:2016 年 6 月 10 日。

〔45〕 参见邱爱民著:《实物证据鉴真制度研究》,知识产权出版社 2012 年版,第 359 - 360 页。

其一,推定的方式。推定方式主要适用于监控视频的生成过程,也就是说,只要有证据证明视频监控系统在证据产生时是运转正常的,就直接推定监控视频具备可靠性。这种推定是可辩驳的推定,即如果辩方对此有质疑,应当有必要的证据或提供必要的线索证明系统在录制和存储视频、声音时运行不正常,且可能严重影响证据的真实性,否则,仅提出系统不正常的抗辩,不能推翻监控视频可靠性的推定。

其二,书面笔录及取证录像。书面笔录及录像主要适用于监控视频的取证环节。我国刑事诉讼法及司法解释已经对搜查、扣押、提取过程中要制作书面笔录进行了明确的规定,书面笔录不仅是证明取证过程合法性的方式,也是证明证据可靠性的一种方式。为了补充笔录只可读、不可见的不足,在监控视频的取证过程中,进行录像是最好的选择,因为录像会更全面地记载取证过程,为判断取证过程是否符合技术标准留下更好的证据。

其三,证人证言的方式。证人证言也主要适用于监控视频的取证环节。如前所述,在取证过程中,必须遵循相应的技术规范,才能保障监控视频不因复制、格式转换、光盘刻录等环节中的错误操作而损害其真实性、完整性。因此,除了制作相关笔录、对取证过程进行录像之外,还可以用证人证言的方式,对取证环节是否遵循了相应的技术要求进行证明。这里的证人可以是侦查机关进行取证的侦查人员,也可以是现场的见证人。

其四,数据安全保护技术。对于监控视频的保存、流转环节,可以采取数据安全保护技术对其可靠性进行证明。在提取监控视频后,为了防止在流转环节被恶意篡改、删除,可以使用数据加密、数字签名等技术,这些数据安全保护技术可以给监控视频中的数据信息加上一个“安全阀”,防止没有权限的人访问数据。即便被没有权限的人访问,如果数据信息被篡改或删除,也会在数据中留下痕迹,结合其它证据也可调查出篡改、删除数据的人的身份和行为发生的时间。因此,对于采取了数据安全保护技术的监控视频,可以认定具备可靠性。

其五,专家的鉴定意见。对于有重大争议的监控视频,可以诉诸专家鉴定意见以证明其可靠性。[46] 这里的专家应当是对数字化的监控视频具有一定专业知识的人。鉴定包括对两个方面的鉴定,即对图像内容的鉴定及对数据内容的鉴定,鉴定的目的是为了发现在监控视频生成、收集、保管的环节中是否存在影响客观真实性的各种因素,如是否存在数据的删除、替换、编辑等,而非对监控视频内容真实性进行鉴定。但需要注意的是,即便专家出具了证据未曾被删除、替换、编辑的鉴定意见,也不意味着证据就能直接作为定案根据,因为此时解决的依然是监控视频的证据能力问题,而不是证明力问题。

其六,当事人的自认。如果在诉讼中,当事人对于不利于己方的证据表示认可,那么自然就意味着证据为真实的可能性非常大,因此就无需再以其它方式对证据的可靠性进行证明。

三 余论:新类型证据的证据能力

由以上对公共场所监控视频证据能力问题的探讨可见,随着科技的发展,日趋复杂的

〔46〕 James A. Griffin, A Prosecutor's Guide to Obtaining and Presenting Audio and Video Evidence, 29-*DEC Prosecutor* 30, (1995).

新类型证据在诉讼中将会不断出现,对证据法理论和立法提出新的挑战。对于这类证据的证据能力判断问题,法律规范总会滞后,这种滞后导致司法人员面对新类型证据时要么不加思考地盲目采纳、采信,要么胆小慎微而不敢采用,都会使证据无法充分发挥诉讼证明作用。为了弥补法律规范的不足,学术界应从证据法理论上对各种新类型证据的证据能力要件进行研究,为这些证据的实践运用提供理论参考。由于证据规则是建立在一定的社会价值和科学规律之上的,不仅要体现程序价值的要求,同时也是认识规律的产物,〔47〕因此,对于新类型证据也应当从其与法律价值的关系、证据的证明机理两个方面研究其证据能力问题。前者主要针对取证手段的合法性问题,通过对新类型证据与公民人身权、自由权、隐私权、财产权等基本权利之间关系的探讨,对其取证手段进行证据法的规制,防止侦查机关收集新类型证据的过程中侵害公民基本权利;后者主要针对证据的科技基础及取证技术规范,通过对新类型证据的生成过程、取证过程、保管过程等方面技术原理的探讨,研究如何设置规则以保障证据的可靠性。对于司法人员来说,也不应因为法律规范没有对新类型证据的证据能力问题作出详细规定就拒绝裁判或置之不理,而应以证据法原理作为基础,以法律解释等方法作为辅助,对新问题进行论证、解决,通过对证据能力规则的合理适用和发展,维护当事人的诉讼权利及实体权利,避免冤假错案。总之,诉讼中新类型证据的出现是必然的,对于这类证据的证据能力问题,证据理论及司法实务都应有所作为,才能充分发挥新类型证据的证明作用,最大限度地利用证明资源,在促进准确认定事实的同时也强化对公民基本权利的保障。

[本文为作者参与的四川省学术和技术带头人培养基金项目“视频证据在刑事诉讼中的运用机制研究”(2013DTPY0022)的研究成果。]

[**Abstract**] The research on the evidence competence of public place surveillance video focuses mainly on the legality of the means used to obtain the video and the authenticity of the video. Even in public place, citizens still enjoy certain privacy, and therefore public place surveillance video can still constitute technical investigation because of violation of privacy. The question of whether surveillance video should be excluded should be determined according to technical investigation rules and illegal evidence exclusion rules. The authenticity of video can be judged by whether there are factors affecting the realness in the process of generation, obtainment and circulation of the video, and proved by such means as presumption, paper notes and video records, witness testimony, and expert opinion.

(责任编辑:王雪梅)

〔47〕 参见秦策:《我们研究什么样的证据法学——英美证据法学的转向与启示》,《中国刑事法杂志》2010 年第 4 期。