侦查中的网络监控法制化研究

Research on the Legalization of Network Supervision in Investigation

刘梅湘 著

法律出版社 LAW PRESS · CHINA

本书受国家社科基金资助，

侦查中的网络监控法制化研究

Research on the Legalization of Network Supervision in Investigation

刘梅湘 著

法律出版社 LAW PRESS · CHINA

图书在版编目(CIP)数据

侦查中的网络监控法制化研究 / 刘梅湘著. --北京：法律出版社，2017

ISBN 978-7-5197-0487-2

Ⅰ.①侦… Ⅱ.①刘… Ⅲ.①网络系统－监控系统－应用－刑事侦查－研究 Ⅳ.①D918-39

中国版本图书馆 CIP 数据核字(2017)第 006944 号

侦查中的网络监控法制化研究
ZHENCHAZHONG DE WANGLUO JIANKONG FAZHIHUA YANJIU

刘梅湘 著

策划编辑 夏旭日
责任编辑 夏旭日
装帧设计 贾丹丹

出版 法律出版社
总发行 中国法律图书有限公司
经销 新华书店
印刷 北京京华虎彩印刷有限公司
责任校对 王晓萍
责任印制 吕亚莉

编辑统筹 法律应用·大众读物出版第二分社
开本 A5
印张 7
字数 162 千
版本 2017 年 11 月第 1 版
印次 2017 年 11 月第 1 次印刷

法律出版社/北京市丰台区莲花池西里 7 号(100073)
网址/www.lawpress.com.cn
投稿邮箱/info@lawpress.com.cn
举报维权邮箱/jbwq@lawpress.com.cn
销售热线/010-63939792
咨询电话/010-63939796

中国法律图书有限公司/北京市丰台区莲花池西里 7 号(100073)
全国各地中法图分、子公司销售电话：
统一销售客服/400-660-6393
第一法律书店/010-63939781/9782
西安分公司/029-85330678
重庆分公司/023-67453036
上海分公司/021-62071639/1636
深圳分公司/0755-83072995

书号：ISBN 978-7-5197-0487-2
定价：35.00 元
(如有缺页或倒装，中国法律图书有限公司负责退换)

目录 /Contents

导　论

正如 Kerr(克尔)教授所言,我们不再通过电话监听的方式用磁带为电话录音或为文件柜里存的文件进行录像,今天,我们逐渐发展的生活的一部分被作为媒体的计算机所引导,电子证据的收集和分析正在成为调查犯罪的主要方式之一。[①] 在互联网日益发展壮大,网民人数已经达到6.68亿的背景下,针对网络或者利用网络实施的犯罪也越来越多,有些是直接针对计算机网络实施犯罪,如非法侵入计算机信息系统罪、非法获取计算机信息系统罪、非法控制计算机信息系统等。还有一些则是利用计算机实施犯罪或者是利用计算机网络传递犯罪信息,如利用计算机网络实施金融诈骗、盗窃、窃取国家秘密,利用计算机网络传播色情图片(视频)、存储犯罪证据或者进行沟通联络,等等。政府部门为了有效地打击犯罪,必须拥有与之相适应的打击犯罪的手段和能力,针对上述情况,行之有效的手段便是网络监控。如果立法赋予侦查机关进行网络监控的权力,那么,随之而来的问题就是,网络监控的法律性质为何?网络监控对公民的哪些权利造

---

① Orin S. Kerr, "Digital Evidence and the New Criminal Procedure", 105 *Colum. L. Rev.*, 279, 2005, p. 307.

成干预？这些权利是否属于公民的基本人权？其干预的程度如何？其与搜查及监听是否具有同一性抑或同质性？是否属于技术侦查？立法应当对此设置何种程序？获取某个网络账号信息与获取传输的内容信息是否适用同一个程序？等等。这些问题皆是因技术革命而带来的新问题，无论是立法界和实务界，都必须直面这些问题并作出理性回应。

综观我国立法，2012 年修改的《刑事诉讼法》首次写进了技术侦查，这是我国刑事诉讼法上的重大进步，无论对控制犯罪还是保障公民基本权利，都具有重大意义。但新法对技术侦查的规定却相当粗略，仅规定了适用的案件范围及笼统的“严格的批准手续”。新法也没有对启动技术侦查在证据上要达到的要求作出规定，仅规定为“根据侦查犯罪的需要”。至于何为技术侦查，技术侦查包括哪些种类，网络监控是否属于技术侦查也是不得而知。虽然《公安机关办理刑事案件程序规定》第 255 条规定技术侦查措施是指记录监控、行踪监控、通信监控、场所监控等措施，但列举的几种技术侦查中并未见网络监控，这也从一个侧面反映出了立法与现实的脱节。当然，出现立法不足的原因，既受价值观选择上的限制，也因为对这一问题的理论研究还不够深入细致，理论储备不足，必然会影响立法的水平和内容。

反观域外，美国、英国、日本、德国、欧洲委员会以及我国台湾地区通过立法对网络监控进行了程序规范，一些国家对网络监控的程序规定之细致与周密让人叹为观止。如美国法、英国法和欧洲委员会的《网络犯罪公约》都对网络监控问题做出了明确规定，美国法和《网络犯罪公约》对通过网络监控截取的数据分为内容数据和非内容数据，并以这种划分为基础，对两者设置了宽严不同的监控程序。英国、日本、德国、我国台湾地区则未作此区分，无论是内容数据的监控还是非内容数据的监控，都适用相同的程序规范。从上述国家及我国台湾地

区的规定来看,监控实时传输的内容数据适用更严格的程序,包括只能适用于重罪案件、嫌疑事实应达到“相当理由”或者“足以怀疑”的程度、只能作为最后侦查手段、法官核准、令状应满足特定性要求等;监控实时传输的非内容数据之程序相对宽松,如不限于重罪案件、嫌疑事实无须达到“相当理由”的程度。

网络监控不仅是对实时传输的数据进行监控,而且包括通过技术手段获取远程计算机中存储的数据或信息,如通过木马技术获取犯罪嫌疑人计算机中存储的资料,显然,这亦属于严重干预公民隐私权的行为,其严重程度并不亚于对实时传输数据的截取。对此,立法也应当进行程序规制。由于计算机存储海量数据,以2015年普通电脑的硬盘容量来看,差不多能存储一座普通图书馆的文档资料。侦查机关在采取网络技术获取时,不能漫无边际地在嫌疑人计算机中搜取,应遵循搜查的特定性规则,否则便与物理空间的概括式搜查无异。当然,这种规制路径与我国现有的制度并不契合,因这种规制需以搜查制度中确立特定性原则为前提,而我国的搜查制度并未确立此原则,因而,解决这一问题还有较长的路要走。此外,通过远程技术获取嫌疑人电脑中的资料与公开对计算机的扣押与搜查并不可同日而语,后者属于公开搜查,而前者则属于秘密搜查,因而应适用比公开搜查更严格的程序,如只能针对重罪案件适用,必须符合最后手段性或必要性原则,必须具备“相当理由”等。

网络监控涉及多种计算机网络技术,如木马技术、跳板技术、网络陷阱、电磁泄漏探测、网络监听、密码破译、IP查找定位及路由追踪、数据复原等。这些技术是否都可以在侦查中使用,应当遵循何种法律程序和规则,无论是侦查人员还是计算机取证技术人员,一直都感到无所适从。早在2007年9月,在兰州召开的刑事诉讼法学年会上,公

第一章　网络监控之含义

一、网络监控的概念

网络监控是计算机网络安全领域经常使用的一个概念，一般是指利用网络嗅探（Sniffering）技术，获取网络数据封包，并进行相关协议分析（Protocol Analysis），提取监控人感兴趣的信息，从而对网络连接实施控制或者对其网络管理策略进行修正。[①] 其重要功能就是实施网络管理，绝大多数网络监控软件也是以此为目的而开发，如 LaneCat 网猫、同易电脑监控软件、Active Wall、网络警察、网上特工等。无论何种网络监控软件，功能上都大同小异，如记录 HTTP、SMTP、FTP、POP3、ICMP、MSN、ICQ、YAHOO、UC、PP 等所有通信；记录 SKYPE、QQ、微信、MSN 等的聊天内容；记录 FTP 外发文件内容以及 FTP 下载文件内容；记录 WEB、SMTP 外发邮件、POP3 收邮件，对发送者、收件者、抄送者、秘送者、主题、邮件内容和邮件附件等进行完整记录；记录

① 于海涛、蒋凡：《网络监控的应用》，载《网络安全技术与应用》2004 年第 11 期，第 28 页。

WEB、TELNET、POP3、FTP、SMTP、ICMP、NETBIOS 等的上网日志；分时段对在线聊天、网络游戏及文件收发和文件上传下载进行阻挡；记载玩网络游戏的时间，提供聊天或游戏的日报表，等等。

上述网络监控的对象主要为局域网内部联网的主机及使用者，其目的在于保障局域网网络安全和工作秘密不被外泄以及防止员工上班时间不务正业。为了避免侵权诉讼，监控者一般都会事先宣布监控政策，有的则是在开机时在屏幕上显示上网行为及内容将被监控。此外，此类监控所采用的监控技术及监控软件不属于国家管制范围，而是属于市场流通产品，因而可从市场上购得。

随着网络犯罪以及利用计算机网络实施的犯罪逐渐增多，网络监控技术也开始运用在侦查过程之中，侦查部门通过网络监控手段的使用，可以截取犯罪分子在微信、QQ、雅虎通、搜 Q 等即时通讯软件传输的视频音频资料、聊天内容以及传送的文件等，还可以截取通过 E - mail（电子邮件）传输的文本及附件。除此以外，还可以通过木马程序获取犯罪嫌疑人储存在计算机硬盘中的资料，这些资料有可能是现时存在的，也有可能是曾经被删除或格式化的资料。例如，我国公安机关广为采用的“苏 - 27”网络远程取证系统和“美亚网警”网络取证系统，则能监控流经网络的所有信息流，包括监控目标对象浏览 HTTPS 网页的内容，既对即时通讯和网络聊天内容进行监控、甚至可以远程技术获取储存在计算机硬盘中的资料。从技术层面来看，网络监控通常是通过特殊的软硬件实现的，针对的是犯罪嫌疑人。在操作执行上，网络监控可以由侦查部门直接实施，也可以由网络服务提供者实施。因为网络服务提供者了解并熟悉计算机网络的系统结构及技术特点，在一般情况下，网络监控是通过后者实施的，如美国联邦调查局开发的“食肉者”（Carnivore），就是通过网络服务提供者实施的。基

于此，笔者认为网络监控就是指采用特殊软硬件设备获取他人网络传输数据及其电脑中存储的资料的行为。此处的获取又称为截取，包括数据的复制、存储和检索。因此，网络监控既指对互联网上即时传输数据的截取，也指对目标计算机中存储数据的获取。

需要指出的是，本书所指网络监控不仅包括侦查机关对犯罪嫌疑人在互联网上所传输的内容数据与非内容数据的监视与截获，还包括通过木马技术获取犯罪嫌疑人储存在计算机硬盘中的数据。换言之，网络监控是指侦查人员使用包括木马技术在内的多种计算机网络技术秘密获取犯罪嫌疑人电脑中的存储资料和网络传输数据的行为。对于没有接入互联网的监控如酒店、银行、超市等通过装置摄像头进行的监控，网络服务提供者在日常网络管理过程中进行的监控以及网警的网上巡逻均不在本书探讨之列。

二、网络监控的性质

随着计算机网络的出现与普及，网络监控也应运而生。相对而言，网络监控是一项新的侦查方法，由于其在截取即时通讯上与监听有类似之处，因此，在一些国家的立法中，网络监控被当做监听对待，对监听性质的界定也就是对网络监控性质的界定，因而下面的阐析基本上围绕监听展开，然后将其推及网络监控。

（一）搜查说

1. 传统意义上的搜查概念

在科技欠发达时期，犯罪行为皆在物理空间实施，与之相应的犯罪证据也遗留在物理空间，从证据的种类和表现形式来看，除了言词

证据以外，就是实物证据。这些有形的实物证据通常存在于人的住所、身体、物品或其他有关的地方，所谓的搜查就是指对人的“住所、身体、物品或其他有关的地方”进行搜索和检查以发现证据或查获犯罪嫌疑人。“住处”和“身体”属于物质世界中的有形物，对于“地方”的理解，按照一般常识，应当是指实在的地方或物理意义上的场所，“身体”、“住所”或“地方”都是指向有形物或实在物。至于物品，该词本身就昭示着“有形物”之属性，所以，在传统意义上，搜查是指对有形物或实在物的搜索和检查。对于计算机网络中的数字信息之获取①，则不是属于搜查的范畴，因为计算机中的数字信息都是以0和1的形式存储于电磁介质之中，不具有物品的特征。

2. 从物理性侵入到合理隐私期待——英美搜查概念之变迁

(1)英国法的渊源

一直以来，英美都是以有形财产和物理侵入的视角来认识和判断搜查。这种认识方法和途径主要源于自古以来对财产的重要价值的判断。西方先贤们早就认识到财产权利对于自由保障的重要性，正如培根的经典名言所云“控制了一个人的生活，就能控制一个人的意志”，先贤们把私人财产视为个体自由的前提，认为没有私人财产权，个人就会受制于他人，不得不处于服从和被强制状态，并站在社会进步和安宁的高度强调承认和保护私人财产的意义。如亚里士多德曾指出：“财产在一定意义上是共有的，但私有化应作为普遍规则，因

① 我国《刑事诉讼法》第42条规定，证据包括物证、书证，证人证言，被害人陈述，犯罪嫌疑人、被告人供述和辩解，鉴定结论，勘验、检查笔录以及视听资料，除了视听资料外，其余几种证据都可以通过相对应的侦查手段获取，如通过勘验、检查制作勘验、检查笔录，通过搜查、扣押或勘验、检查获取物证、书证，通过讯问获取犯罪嫌疑人、被告人供述和辩解，通过询问获得证人证言、被害人陈述，通过鉴定获得鉴定结论。那么视听资料通过何种侦查措施获得？从现行《刑事诉讼法》的规定来看，视听资料似乎是来历不明。

为，当每个人都有边界确定的利益时，人们就不会互相指责，每个人都要照看他自己的财产，因此人们将会取得更大的进步。”①洛克在《政府论》中曾经提出：“任何人都不得侵害他人的生命、健康、自由和财产。”②当代西方著名学者哈耶克在《自由秩序原理》中说：“对私有财产权或分别财产权的承认，是阻止或防止强制的基本条件，尽管这绝非是唯一的条件。”③“财产神圣不可侵犯”不仅是学者和普罗大众的共同理念，更是被当作一项宪法性权利，如 1789 年法国《人权宣言》第 17 条宣称：“财产是不可剥夺的神圣权利；除非以合法形式建立的公共需要明确要求，并且在公共补偿被事先支付的前提之下，任何财产皆不得受到剥夺。”正是对财产及财产权利的高度重视，对财产权设置了厚重的保护屏障，即使是国王，也不得随意侵入墙损门破之民宅。

从历史来看，英国 1765 年的 Entick v. Carrington 案最先将搜查界定为一种“物理性侵入”。该案原告 Entick 撰写了一些反政府的文章，英国大臣 Halifax 发出无特定性要求的概括搜查证④，Halifax 的执法机关在 Entick 家翻箱倒柜，打开各种箱子、盒子、抽屉以及所有他的个人文件，进行了持续 4 小时的地毯式搜查，后来 Entick 控告英国政府非法侵入，并对该侵入行为提出诉讼，终获胜诉，并获得了 300 英镑

---

① ［古希腊］亚里士多德：《政治学》，吴寿澎译，商务印书馆 1981 年版，第 53 页。

② ［英］洛克：《政府论》（下篇），叶启芳等译，商务印书馆 1964 年版，第 32 页。

③ ［英］哈耶克：《自由秩序原理》，邓正来译，生活 · 读书 · 新知三联书店 1997 年版，第 173 页。

④ 英国政府当时可以持三种搜查令状进行搜查，一是指明搜查范围的搜查令状，二是不记载任何搜查范围的空白搜查令状，三是针对违反进口债务法的人实施的协助搜查令状。在一般情况下，都是采用空白搜查令状执行搜查。

的赔偿。[①] 该案的审判法官 Camden(卡姆登)认为本案搜查令状是无效的,理由在于,虽然私人权利在其有可能侵害民众时,必须受到政府公权力的干预,但概括式搜查令状逾越了在合乎比例的范围内因基于公益而予以侵害的界限,概括搜查令可以说违反了普通法的规范;其次,Camden 法官强调,人之所以能够立足于社会,是因为他拥有财产,并进一步叙述侵入行为的法律规制在于保护财产的见解:"依英国法,任何对私人财产的危害,就是一种侵入行为"。在 Camden 法官看来,对侵入行为进行法律规制之目的在于保护"财产",而文件是一种"财产",而且是一个人最珍贵的"财产",因此原则上不得对其进行检查或扣押。在此案发生一年后,英国学者 William Pitt(威廉·皮特)针对该案发表著述,指出:"最穷的人在他家中,都应该可以抵御国王的强制力。纵然他的家破损,他的屋顶摇晃,纵然风暴雨雪可以进,但国王仍然不得任意进入——他的权力仍然不得任意侵入他家的门槛。"[②]

从 Camden 法官和学者 William Pitt 的论述可以看出:第一,政府不得以概括搜查令状侵入个人的"家的门槛",因为此举在公共利益和私人权利之间不合乎比例;第二,提出了法律对侵入行为的规制在于保护"财产"的观点,这意味着两点,其一是法律所保护的乃"财产利益"或"财产权利",而非指其他利益。换句话说,对搜查的认识是以财产利益的角度切入。饶有趣味的是,Camden 法官认为文件是最珍贵的"财产",可见,按照他的逻辑,文件之所以要得到保护是因为

---

① Stunz, "The Substantive Origins of Criminal Procedure", 105 *Yale L. J.* 393, 1995, p. 397.

② Willianm C. Heffeman, "Fourth Amendment Privacy Interests", 92 *J. Crim, L. & Criminology* v1, 2001, p. 15.