法学新前沿 New Law Frontiers

Guided Reading on
Law and Technical Standard
of Network
Lawful Interception

网络通信监控
法律与技术标准导读

马民虎　果园　方婷　著

法律出版社
LAW PRESS · CHINA

Guided Reading on
Law and Technical Standard
of Network
Lawful Interception

网络通信监控
法律与技术标准导读

马民虎　果园　方婷　著

法律出版社

图书在版编目(CIP)数据

网络通信监控法律与技术标准导读 / 马民虎等著. —北京:法律出版社,2013.11
ISBN 978-7-5118-5623-4

Ⅰ. ①网… Ⅱ. ①马… Ⅲ. ①电信—法规—研究—世界②电信—技术标准—研究—世界 Ⅳ. ①D912.290.4②TN91

中国版本图书馆 CIP 数据核字(2013)第 266753 号

网络通信监控法律与技术标准导读

马民虎
果 园 著
方 婷

责任编辑 王 扬
装帧设计 汪奇峰

开本 720 毫米×960 毫米 1/16
印张 23.5 **字数** 389 千
版本 2013 年 12 月第 1 版
印次 2013 年 12 月第 1 次印刷
出版 法律出版社
编辑统筹 独立项目策划部
总发行 中国法律图书有限公司
经销 新华书店
印刷 三河市龙大印装有限公司
责任印制 张建伟

法律出版社/北京市丰台区莲花池西里 7 号(100073)
电子邮件/info@lawpress.com.cn
销售热线/010-63939792/9779
网址/www.lawpress.com.cn
咨询电话/010-63939659

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、子公司电话:
第一法律书店/010-63939781/9782
西安分公司/029-85388843
重庆公司/023-65382816/2908
上海公司/021-62071010/1636
北京分公司/010-62534456
深圳公司/0755-83072995

书号:ISBN 978-7-5118-5623-4
定价:58.00 元

导　读

网络通信监控作为各国普遍认可的一种技术侦查手段，有着非常悠久的历史，被认为是警察部门预防犯罪，侦查犯罪活动的重要措施和技术方法。随着通信技术的迅速发展和广泛应用，通信监控经历了传统电信监控到互联网通信监控，甚至物联网通信监控的嬗变，技术实施环境更加复杂，配合义务主体不断扩大，执法要求越来越严格。

为了更好地发挥通信监控的作用，保护国家安全、社会治安秩序，维护公民通信秘密及通信自由权益，许多国家纷纷建立了网络通信监控法律框架，严格规范执法机关实施网络通信监控技术手段的程序，明确通信服务提供者的协助执法义务，制定有关网络通信监控的技术标准，逐步建立覆盖全面、功能完善、作用强大、执法规范的网络通信监控技术体系。在通信监控法律规范方面，比较典型的是欧洲通信监控立法框架和美国通信监控立法框架，这些法律法规伴随着通信技术的发展，不断积淀不断完善，有力地支撑了各个国家通信监控技术手段体系的建立，不断契合警察部门打击犯罪，尤其是恐怖犯罪活动的需要，在执法实践中发挥了不可替代的作用。可以说，网络通信监控法律框架反映了一国通信监控技术体系的架构，反映了一国利用这一技术手段开展犯罪调查的技术能力，甚至也代表着一国法治文明的程度。

在各国网络通信监控法律框架中，欧盟通信监控法律框架最为清晰，指导意义更强。近年来，欧盟连续颁布了一系列通信监控法律法规，调整范围覆盖各个通信网络业态，包含了实时通信数据获取以及数据留存等各个方面，对其成员国甚至全球的通信监控立法具有很强的指导作用。例如，欧盟《通信监控决议》的内容十分全面，对欧洲电信标准化协会（ETSI）制定有关通信监控标准具有一定的导向性，也对其成员国制定相关的技术法规、标准

产生了一定的影响。尽管欧盟法经历了从1995年《通信监控决议》到《网络犯罪公约》以及2006年新通过的《数据存留指令》的发展，但其精神实质没有发生根本的改变，要求通信服务提供者履行协助执法的立法原则更没有发生根本的动摇。欧盟推出的ETSI通信监控技术标准被世界上各个国家借鉴和采纳。

美国通信监控的历史悠久，在1934年《电信法》中就规定了电子监听的使用。“9·11”以后，美国为打击恐怖组织的犯罪活动，迅速扩大侦查机关的权力，于1994年制定《通信协助执法法》，规定通信行业要为政府机构提供必要的设备工具与技术条件，以增强政府机构实施通信监控的能力。2004年以后，该法案经联邦通信委员会（FCC）进一步扩大解释，将宽带服务、网络通话纳入其调整范围。通过2005年和2006年FCC发布的两份报告与命令可以看出，随着技术的进步，《通信协助执法法》的实施面临着巨大的挑战。两份报告与命令是FCC基于美国执法机关、国会及有关适用主体的要求，经过征求各方意见并进行合理分析后出台的。同时，美国《通信协助执法法》的监控技术标准也成为世界上著名的通信监控标准之一。

为了使读者对国外网络通信监控的法律制度和技术标准有一个清晰的认识，本书梳理了各国有关网络通信监控的法律框架，分析了欧美通信监控技术标准的发展趋势，提供了各国网络通信监控法律法规的文本导读。

目　录

1 网络通信协助监控法律框架

1.1 欧盟及其成员国

1.1.1 欧盟

1)对执法机关及其他部门的要求

2001年11月23日通过的*Convention on Cybercrime*[1],对计算机通信监控进行了原则性的规定:

*Convention on Cybercrime*第20条涉及通信流量数据(traffic data)实时收集,其中规定各缔约国应当采取必要的立法或其他措施,授权执法机关在其管辖范围内采用技术手段实时收集和记录通信流量数据,或者授权执法机关强制服务提供者依其技术可行性在其管辖范围内采用技术手段或与执法机关配合与协作实时收集和记录通过计算机系统传输的与特定通信相关的通信流量数据。所谓"通信流量数据",是指任何与借助计算机系统进行的与通信有关的计算机数据,该数据由构成通信链的一部分计算机系统生成,指明了通信的来源、目的地、路径、时间、日期、大小、持续时间或基本服务类型。

*Convention on Cybercrime*第21条涉及通信内容数据(content data)[2]监控,其中规定各缔约国应当采取必要的立法或其他措施,在国内法规定的严重犯罪的范围内,授权执法机关在其管辖范围内采用技术手段实时收集和记录通信内容数据,或者授权执法机关强制通信服务提供者依其技术可行性在其管辖范围内采用技术手段或与执法机关配合与协作实时收集和记录通

---

〔1〕 通常译为《网络犯罪公约》。

〔2〕《网络犯罪公约》规定,收集和记录的通信内容数据指在成员国管辖范围内通过计算机系统传输的相关的特定通信。

过计算机系统传输的相关的特定通信内容数据。

Convention on Cybercrime 第 20 条和第 21 条均包含用于收集和记录通信数据的两种不同方法。

第一种方法是各缔约国通过采取必要的立法或其他措施，授权执法机关直接收集和记录所需的通信数据。

第二种方法是各缔约国通过采取必要的立法或其他措施，授权执法机关强制服务提供者收集和记录执法机关要求的通信数据。这种方法通常要求国际互联网服务提供者安装一个监控接口，向执法机关传输所需的通信数据，这使得执法机关能够利用服务提供者一般已具备的现有技术能力和知识实现侦查犯罪的目的。

将上述两种方法相结合，其意图是确保在各缔约国执法机关不具备收集和记录所需通信数据的相关技术时，能够在通信服务提供者的技术协助和配合下完成调查。

Convention on Cybercrime 要求各缔约国通过采取必要的立法或其他措施使得通信服务提供者对监控的执行本身以及相关信息保密。

虽然 *Convention on Cybercrime* 旨在改进和协调各国与网络犯罪有关的法律方面的问题，但是根据其规定，以上所述条款不仅适用于与网络犯罪有关的违法行为，还适用于涉及通信网络的其他违法犯罪行为。第 14 条第 3 小段使各缔约国能够做出保留，并将条款的应用限于某些违法行为。

2）对通信服务提供者的协助执法要求

（1）欧盟理事会《关于通信监控的决议》[1]

1995 年 1 月 17 日，经各成员国达成协议，欧盟理事会发布 *Council Resolution of* 17 *January* 1995 *on the lawful interception of telecommunications*，涉及执法机关与通信服务提供者的通信监控要求。决议中的有关要求符合成员国国内法，并遵循其现行的国家政策。在该决议中，欧盟赋予各国执法机关对网络运营/服务提供者提出通信协助监控法律要求的权力。概括而言，这些法律要求包括法律义务、技术性能、安全保密等等。具体而言，执法机关有权要求网络运营/服务提供者具备以下能力：

1. 实时、全时的通信监控能力。呼叫关联数据应当确保能够实时监控。

---

[1] Council Resolution of 17 January 1995 on the lawful interception of telecommunications.

如果呼叫关联数据不能实时获取，要求在呼叫终止后尽可能迅速地获取。

2. 要求网络运营/服务提供者提供一个或多个接口，以确保监控的通信信息能够传输至执法机关的监控设备。接口必须经监控执法机关和网络运营/服务提供者的同意。其他相关事宜应当按照各国通行的方式处理。

3. 要求网络运营/服务提供者以精确对应的方式提供呼叫相关数据和目标服务的呼叫内容。

4. 要求向监控设备传输监控信息的格式为通用格式。该格式的使用应得到各国同意。

5. 如果网络运营/服务提供者对通信信息进行编码、压缩或加密，执法机关要求网络运营/服务提供者提供明文的监控通信。

6. 要求网络运营/服务提供者能够通过固定或交换连接装置将监控通信信息传输至执法机关的监控设备。

7. 要求上述监控通信的传输符合现行的安全要求。

8. 要求确保监控的实施，为实现监控指令，监控目标和其他未经授权个人不应当获知（通信状态）的变化。尤其是目标服务的运营必须对监控实体显示为无变化。

9. 要求网络运营/服务提供者保护执行监控的信息，不得泄露如何实施监控的任何信息。

10. 要求网络运营/服务提供者在监控过程中提供信息或协助，以确保所要求的监控接口的通信与目标服务相关。该类型的信息或协助可能按照各国通行的方式而有所不同。

11. 要求网络运营/服务提供者为执行同步监控进行安排。并可能要求对单个目标服务部署多路监控，以允许多个执法机关实施监控。为此，网络运营/服务提供者应当保护监控机构的身份，并确保调查的秘密性。给定用户的最大同步监控数量应符合各国要求。

12. 要求网络运营/服务提供者尽可能迅速地实施监控（紧急情况下应在数小时或数分钟内实现）。执法机关的响应要求会因各国和监控的目标服务不同而不同。

13. 实施监控过程中，执法机关要求监控支持服务的可靠性至少应当和向监控实体提供的目标服务的可靠性一致。执法机关要求向监控设备传输的监控服务数量应当符合网络运营/服务提供者的执行标准。

(2)欧洲议会和欧盟理事会《关于存留因提供公用电子通信服务或者公用通信网络而产生或处理的数据及修正第2002/58/EC号指令的第2006/24/EC号指令(数据存留指令)》[1]

欧盟对于数据存留的规定,其实早在 *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*[2]中即有体现。由于该指令只针对数据存留进行规定,但对于数据应存留的内容、期限与利用范围,未多着墨。

2006年3月15日发布的 *Directive 2006/24/EC*,规定了六个方面的内容,即目的和适用范围、数据存留的类别、数据存留的义务、数据的保护与销毁、存留数据的提供与罚则以及评估。

存留的数据仅包含所有自然人或法人的流量数据与位置数据,以及其他用来识别订购者或已登记用户所必需的资料,不得存留内容数据。*Directive 2006/24/EC* 中还专门规定了存留数据的类别,依其存留项目的不同,主要分为六大类。而且各成员国需确保这些数据自流通之日起,得存留6个月以上,但最多不得超过2年。

由于存留的数据涉及公民的隐私,若不慎外泄或被不当利用,将对公民隐私造成重大侵害,其影响程度不亚于实时通信监控所造成的侵害,故 *Directive 2006/24/EC* 专门在第7条规定,对于被存留数据的质量、安全和保护等级,应等同于数据传输时的保护。

各国更应积极采取适当的技术或政策措施,避免意外或非法损毁、灭失、更改存留的数据,或未经许可、非法存留、处理、获取或披露数据;而对于届满存留期限的数据,除非有特殊情况,应立即销毁。

存留数据的机构须确保其存留的数据可配合执法机关的调查而随时提供,用以协助执法机关进行严重犯罪与恐怖嫌犯之调查时的参考利用。

---

〔1〕 Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC.

〔2〕 通常译为《欧洲议会和欧盟理事会2002年7月12日关于电子通信行业个人数据处理与个人隐私保护的第2002/58/EC号指令(隐私与电子通信指令)》。

1.1.2　法国

法国制定和颁布了很多与通信监控有关的法律，其中最具影响力的立法是 *Loi Sur Le Secret Des Correspondances*（*Law No.* 91－646）[1]，该法就通信监控的一般条件、权限以及程序作了明确的规定。法国的 *The Code of Criminal Procedure*[2] 对通信监控的适用范围、期限、地点等也做出了相关规定。其他与通信监控有关的法律还包括：*The Code of Criminal Procedure*，*The Fiscal Procedure Code*[3]，*The Monetary and Financial Code*[4]，*Loi Informatique Et LibertÉS*（*Law No.* 78－17）[5]，*Loi Rela-Tive À La LibertÉ De Communication*（*Law No.* 86－1067）[6]，*The Posts and Telecommunications Code*[7]，*Loi De SÉCuritÉ IntÉRieure*（*Law No.* 2003－239）[8]，*Loi Sur La SÉCuritÉ Quotidienne Or LSQ*（*Law No.* 2001－1062）[9]。

1）对执法机关以及其他部门的要求

从整体上讲，法国的通信监控制度在遏制犯罪和保障人权的价值取向上，更注重查明事实而忽略对公民隐私权和通信自由权的保障。在监控案件的适用范围、组织实施、证据运用上，法国持比较宽松的态度，并且缺乏有效的救济措施。

（1）监控的适用条件。在案件适用范围上，法国与德国的通行做法不同。依据 *The Code of Criminal Procedure* 的规定，可能判处 2 年或者 2 年以上监禁的重罪或者轻罪案件即可适用监控，低于大多数国家最少 3 年监禁的要求。适用监控的实质性条件即为“侦查必须”，而何谓“侦查必须”并无法律明文规定。

（2）监控令状的签发和内容。监控由预审法官授权并监督，检察官和警察无权做出监控决定。监控令状以书面形式发布并且必须包括监控用户的

---

〔1〕 1991 年 7 月 10 日通过的第 91－646 号法律《电信通信保密法》，也被简称为 1991 法案。

〔2〕 通常译为《刑事诉讼法》。

〔3〕 通常译为《财政程序法》。

〔4〕 通常译为《货币及金融法》。

〔5〕 1978 年 1 月 6 日的《数据保护法》。

〔6〕 1986 年 9 月 30 日的《通信自由法》，于 2000 年 8 月 1 日得到修正。

〔7〕 通常译为《邮政和电信法》。

〔8〕 2003 年 3 月 18 日的《内部安全法》。

〔9〕 2001 年 11 月 15 日的《日常安全法》。

数量和监控持续的时间。

(3)监控期限、地点和对象。对于监控的期限、地点和对象,*The Code of Criminal Procedure* 规定比较宽泛。首先,监控期限最长可达4个月,但是也可以根据 *Law No.* 91-646 的第6条进行延期,并且没有次数限制,长于英国规定的3个月的授权期限;其次,可以实施监控的地点不限于公共场所,还包括私人住宅,即只要为了"侦查必须",预审法官可以决定对任何地点实施监控;最后,监控的对象包括犯罪嫌疑人、第三人和民事当事人,并不保护在其他国家一般规定的享有拒证特权[1]的人。直到1993年,法国才做了补充规定,要求对律师的监控需要通知律师公会会长。到了1995年,规定对议员的监控应通知议会主席,否则监控获取的信息无效。

(4)监控的救济措施。*The Code of Criminal Procedure* 没有规定监控的救济措施,对秘密监控的决定法国规定不允许当事人申请救济,"监控决定书以书面的形式作出,此项决定不具有司法性质,不得上诉"。

(5)监控所得证据的运用。如果当事人被起诉,监控时录制的谈话可以作为证据来证明案件事实及采取监控措施的正确性。

2)对通信服务提供者的协助执法要求

Law No. 91-646 的第1章对通信协助监控进行了授权,并规定在根据 *The Code of Criminal Procedure* 第100至100-7条,获得调查法官、巡回法院或者最高上诉法院的授权时,通信服务提供者有义务协助监控通信。总理批准授权的情况下,服务提供者也应协助监控通信。允许实施前述监控是基于阻止例如恐怖主义、间谍活动或者威胁国家安全等严重犯罪的目的。

根据 *Law No.* 91-646 的第11-1章,通信服务提供者有义务提供加密信息的解密版本或者向当局提供解密密钥。

Law No. 91-646 第9条命令执法机关应当在总理的监督之下,于监控结束后10日之内销毁监控的信息。

根据 *The Posts and Telecommunications Code* 第L35-5条的规定,通信服务提供者必须提供所有当局所需通信信息的访问。这些信息可能包括最新的用户名单、地址和呼叫应答号码。

---

〔1〕 拒证特权(privilege of witness),又称免证特权或保密特权,是指在诉讼过程中,具有作证义务的公民在法定的情形下享有的拒绝充当证人或拒绝提供证言的权利。

The Posts and Telecommunications Code 第 D98 - 1 章要求通信服务提供者与执法机关协作实施通信监控，安装监控需要的技术设备并保证其可用。第 D99 章声明，在涉及公共安全或防御的情况下，任何独立的通信服务提供者都应服从于执法机关。

根据 *The Posts and Telecommunications Code* 第 35 - 6 条的规定，法国政府承担部署监控技术及随后而来的维护费用。实施监控而产生的运营成本和为了传输监控信息的连接成本也都应由政府进行补偿。

法国第 2002 - 997 法令规定了运营加密通信服务的通信服务提供者的义务；*The Monetary and Financial Code* 授予侦查人员要求通信服务提供者为其提供相关信息的权力。

1.1.3　德国

在德国，网络监控通信的涵义很广，包括有线电话交谈、电子邮件、网络电话监听等。规制通信监控的主要法律是 *Strafprozeβordnung*（*StPO*）[1]、*Telecommunications Act*（*TKG*）[2]、*The Act on the Restriction of the Privacy of Correspondence, Posts and Telecommunications*（*G - 10*）[3]、*Telecommunications Interception Ordinance*（*TKÜV*）[4]。其他有关法律还包括：*Foreign Trade and Payments Act*[5] 和 *Customs Investigation Service Act*[6]。

1）对执法机关以及其他部门的要求

（1）监控的适用条件。德国 *StPO* 规定，监控适用的案件范围仅限于政治性或军事性犯罪、烟毒麻醉药品犯罪、有组织犯罪、特定的依外国人及难民程序法规定的犯罪，或者威胁德国国家安全的犯罪这五类最重大的犯罪。适用监控的实质条件为：在有一定的事实认为某人具有上述之一犯罪行为的嫌疑，并且以其他方式不能或者难以查明案件事实或者犯罪嫌疑人居所的情况下，可以对其电话通信进行监控和录音。而对于“在以其他方式不能或者难以查明案件事实或者犯罪嫌疑人居所的情况下”这一实质条件的要求，在实践中，只要可以选择的侦查手段将浪费更多的时间或者花费更多的努力，有

---

〔1〕 1987 年的《刑事诉讼法》。

〔2〕 1996 年 7 月 25 日的《电信法》，于 2004 年 6 月得到修正。

〔3〕 2001 年 6 月 26 日的《限制信件、邮政和电信隐私法案》，简称 G - 10 法案。

〔4〕 2002 年 1 月 22 日的《电信监控法令》，于 2005 年得到修正。

〔5〕 通常译为《对外贸易和支付法》。

〔6〕 通常译为《海关调查机构法》。

关部门就认为满足了这一实质条件。

(2)监控令状的签发和内容。根据 *StPO* 第 100a 条的规定,这些监控都必须获得法官授权。第 100b(2)条规定,授权必须是书面的,并且保持 3 ~ 6 个月的有效期。德国内政部部长也可以命令实施通信监控。在极端紧急的情况下,公诉人可以授权监控。监控令状只须写明监控针对的当事人的姓名,地址,采取措施的种类、范围及持续时间。

(3)监控的地点、对象和期限。对于监控的实施,并无最小程度原则的要求。监控的范围既可以指向嫌疑人住所和营业地的通信线路,也可以包括所有可能为嫌疑人接收和传递消息的个人通信,或者嫌疑人在通信所有人可能不知晓的情况下使用的通信。由于监控命令具有广泛的使用范围,因此,嫌疑人的配偶、亲属或律师的通信都可以被监控。监控的期限不得超过 3 个月,但只要法定理由继续存在,则监控可以延期且没有次数限制,每次延期期限不得超过 3 个月。

(4)监控所得证据的运用。根据监控令,有关的通信服务提供者必须提供用来监控和录制特定通信线路上的通话技术设备。由警察安装录制接收设备,并由其检测录音带以获得侦查线索和可能的证据。监控所得资料可以作为证据使用,但嫌疑人与律师之间的谈话内容除外。

(5)实施监控的主体。*G* - 10 授予联邦和州执法机关监控和记录通信。*Customs Investigation Service Act* 授予海关犯罪办公室监控和记录电信信息的权力。

(6)监控适用的范围。根据 1996 年 *TKG* 第 3(16)条和 3(17)条对电信和电信系统的定义,电信涵盖 IP 通信的所有方面,包括 VoIP、虚拟主机(Web Hosting)、电子邮件等互联网服务。德国的相关法律规定所有的通信服务提供者都负有监控义务,没有地址信息与内容信息的区别。

2)对通信服务提供者的协助执法要求

1996 年 *TKG* 第 88 条声明通信服务提供者需要配置用以实施监控的技术设施并保证其可用。根据第 88(2)条的规定,只有当监控设施被联邦网络局(形式上被称为电信和邮政监管管理局)批准后,电信运营系统才被允许运营。

G - 10 的第 2 节和 1996 年 *TKG* 的第 88(4)条清楚地规定通信服务提供者将使用这些功能来监控呼叫信号和内容。通信服务提供者也将被迫交出

任何通过其网络传输的电子邮件，并向执法机关提供对正在传输的监控通信信息的网络访问。

2004 年 6 月 22 日，德国议会批准了电信法的修正，根据 2004 年 *TKG* 第 110 条的规定，通信服务提供者应当自费部署实施监控所必需的技术设施。

为了进一步明确哪些主体将负有通信协助监控的义务，德国于 2002 年 1 月通过了 *TKUV*，规定了监控电信的技术和实施要求。该法令明确规定只有公共通信服务提供者才负有通信协助监控的义务，并且对于公共电信服务和其他电信服务的提供者，此种义务仅限于提供公共电信服务的部分。依此定义，宽带和拨号接入服务提供者以及互联网服务提供者都应当承担监控义务。其中第 21 条规定，对用户量少于 10,000 人的通信服务提供者减轻监控义务，第 3(2)(5)条进一步规定，用户量少于 10,000 人的通信服务提供者的义务仅限定于协助当局监控和录音电话。*TKUV* 规定小型运营商只要在其接到监控的司法通知后 24 小时之内实施监控即可(第 21(3)条)，并且将此种要求限制在“能使执法机关监控和记录”的范围以内。此外，所有的电信公司需要自己结成联盟，规定技术标准以遵从 *TKUV* 规定的法定义务。

1.1.4　荷兰

根据 2003 年德国马克斯普郎研究所关于外国和国际刑法的报告，荷兰是世界上第二大实施通信监控的国家。荷兰每十万居民中平均有 62 人的通信被监控，仅次于意大利的 76 人。在荷兰，有许多法律共同规制通信监控，包括 *Wetboek Van Strafvordering*[1]、*Telecommunicatiewet* (*TW*)[2]、*Wet Bijzondere Opsporingsbevoegdheden* (*Wet BOB*)[3] 以及 *Wet Inlichtingen En Veiligheidsdiensten*[4]。除了窃听之外，荷兰的通信监控已延伸到公开提供的互联网服务，比如电子邮件、聊天和网页浏览。

1)对执法机关以及其他部门的要求

与很多国家的规定相似，在荷兰，窃听或者监控程序开始之前需要获得

---

〔1〕 1921 年 1 月 14 日的《刑事诉讼法》。

〔2〕 1998 年 10 月 19 日的《电信法》。

〔3〕 2000 年 1 月 1 日《特别调查权法案》。

〔4〕 2002 年 1 月 7 日的《情报和安全机构法》。

法庭签发的授权令状。根据 *Wetboek Van Strafvordering* 第 125m 节规定，为了调查刑事案件而监控通信可以由法庭批准并授予令状。其中，第 126m 节和第 126t 节授权通信内容监控，而第 126n 节和第 126u 节授权通信流量数据监控。此外，情报机构从事的监控活动由内政部部长授权。

2）对通信服务提供者的协助执法要求

TW 列举了通信服务提供者的特殊义务。根据第 13－1 章第 1 段的规定，通信服务提供者只有启用了相关网络的窃听功能才能提供商业服务。第 13－2 章规定通信服务提供者有义务在通信监控上协助执法机关。

TW 第 13－4 章第 1 段要求通信服务提供者向执法机关提供监控指令需要的所有的技术信息，例如用户的号码、地址、城市、服务类型等。此外，通信服务提供者应当将通信流量数据存储至少 3 个月用于数据分析。

第 13－8 章规定了在特殊情况下可以允许豁免窃听义务。这种豁免只能由经济事务部部长在与内政部部长和司法部部长协商之后批准。然而，针对这些特殊情况的规定十分含糊，因为法规中并没有定义属于豁免范围的情况。

根据 *TW* 第 13－6 章的规定，通信服务提供者应当承担为了使网络窃听设备可用而支付的安装、维护和间接费用，而政府只报销向执法机关传输监控流量而花费的行政和人工费用。

于 2004 年 9 月生效的 *Vorderen gegevens telecommunicatie*[1] 也授权公诉人从通信服务提供者处获得通信流量数据。只有当犯罪的刑罚至少需要 4 年时，此项授权才有可能获得批准。

此外，荷兰有两部针对互联网通信的监控规范：荷兰通信监控互联网流量的功能规范，即 WAI 功能规范；以及 IP 流量传输（TIIT）规范。WAI 功能规范特别应用于 IP 和电子邮件的监控，而 TIIT 规定了适用于执法机关的切换接口的细节。这些规范都是用来在遵从协助义务方面指导通信服务提供者的行动，能够在法律规范的框架下为通信服务提供者提供更加具体、明确的、具有可操作性的技术标准指导。

1.1.5　英国

在英国，通过国家权力对通信进行监控的历史非常悠久，早在二百年前

〔1〕 通常译为《恢复数据通信法》。