重大事件驱动下的美国情报监控政策立法演变及中国路径

何治乐[1] 孔华锋[2]

[1](公安部第三研究所 上海 201204)

[2](华中科技大学 湖北 武汉 430074)

摘 要 新近披露的美国 CIA 窃听全球多国最高机密的监控事件,再度引发了各界对情报监控活动合法性边界的思考。美国是情报监控政策立法极为发达的国家,其改革具有突出的事件导向性特点。全面回顾美国情报监控典型政策立法脉络,有利于观察情报监控中“授权”与“限权”的博弈过程,对完善我国相关制度构建具有重要意义。建议我国完善情报监控流程、透明度、隐私保护等制度,构建科学、有效、可操作性强,具有中国特色的情报监控政策立法体系。

关键词 国家安全 情报监控 透明度 隐私保护 区别对待

中图分类号 TP301.6 **文献标志码** A DOI:10.3969/j.issn.1000-386x.2020.11.051

EVOLUTION OF US INTELLIGENCE SURVEILLANCE POLICY AND LEGISLATION DRIVEN BY MAJOR EVENTS AND CHINA'S PATH

He Zhile[1] Kong Huafeng[2]

[1](*The Third Research Institute of the Ministry of Public Security, Shanghai 201204, China*)

[2](*Huazhong University of Science and Technology, Wuhan 430074, Hubei, China*)

Abstract The recently disclosed US CIA eavesdropping most confidential surveillance events of many countries has caused community's thinking about the legal boundaries of intelligence surveillance activities again. The US is a country with highly developed intelligence surveillance policy and legislation, and its policy and legislative reforms have prominent event-oriented characteristics. A comprehensive review of the development of US intelligence surveillance policy and legislation is conducive to observing the process of 'authorization' and 'restriction of power', and it is of great significance to improve China's related system. It is suggested that China should improve the intelligence surveillance process, transparency and privacy protection, and build intelligence surveillance policy and legislative system which is scientific, effective, operable and has Chinese characteristics.

Keywords National security Intelligence surveillance Transparency Privacy protection Differential treatment

0 引 言

尼克松水门丑闻、911 恐怖袭击、棱镜门大规模监控等重大安全或灾难性事件对美国情报监控活动产生了深远影响。以上述事件为节点,美国情报监控立法进行了三次重大调整,整体表现为从“授权”到“扩张”再到“限制”的变革脉络,其间也充斥着安全与隐私的利益平衡。新近披露的美国中央情报局通过控制瑞士 Crypto 公司窃听全球 120 国最高机密长达数十年的安全事件,再度引发了各界人士对于情报监控活动合法性边界的思考。不论是出于维护国家安全与主权目的,亦或是保护个人隐私权利角度,都有必要全面审视美国情报监控政策立法体系的发展脉络。鉴于美国情报监控政策立法体系非常庞大且复杂,本文以国家层面的《国家情报战略》、授权扩展数据收集活动的基本文件第 12333 号行政令,以及具有里程碑意义的《涉外情报监控法》、《爱国者法》、《情报改革和预防恐怖主

收稿日期:2020-03-17。公安理论及软科学研究计划项目(2019LLYJGASS048);公安部第三研究所 2020 年基本科研业务费专项资金项目(C20251)。**何治乐**,助理研究员,主研领域:信息安全法律。**孔华锋**,教授。

义法》、《美国自由法》等为主线研究我国情报监控的法制化路径。

1　水门事件:构建情报监控立法的“金三角”体系

1973 年,水门事件爆发,引发了美国各界对总统容易滥用 1968 年《综合犯罪控制与街道安全法》赋予其特殊权利的反思。美国以“限制政府权力滥用”为核心进行了史上第一次大规模立法改革,构建了 20 世纪末期情报监控立法的“金三角”体系,为 911 恐怖袭击及棱镜门之后的立法改革奠定了坚实基础。

1.1　《涉外情报监控法》确立涉外情报监控合法性

美国国会于 1975 年成立特别委员会,调查 1936 年至 1975 年近 40 年间美国政府滥用监控的情况。随后,特别委员会发表十四卷报告和文件,证明政府实施了大量滥用监控行为收集海量信息。这些监控经常仅以公民的政治信仰、政治反对者信息为目标,即使这些信仰不会构成暴力威胁或不代表敌对外国势力的非法行为[1]。

1978 年,美国国会发布《涉外情报监控法》(FISA),旨在抑制政府滥用监控权力。但本质上,这部立法主要确立涉外情报监控的合法性,允许政府对外国势力及其代理人的情报信息进行合法收集。该法明确:1)在美国境内仅允许出于收集外国情报和外国反情报的目的使用非犯罪性电子监控;2)外国势力及其代理人可以作为电子监控目标的实体和个人;3)允许电子监控前须满足的条件;4)设立涉外情报监控法院(FISC),审查在美国进行的与外国势力及其代理人有关的国家安全窃听申请。

制定之初,FISA 仅适用于电子监控,后来进行了重大修改,以解决对某些有形实体、笔记录仪和通信追踪装置使用的搜索。1995 年,国会将 FISA 的监控范围扩大至物理搜查,允许在出现某些可能因素时对房屋进行实地搜查,可能因素包括:搜查对象可能是外国势力或其代理人;待搜查处所有外国情报信息;待搜查处所是某外国势力或其代理人所有、使用、占有,或正在外国势力或其代理人之间发生转移。

1998 年,国会进一步修改 FISA,准许在国际恐怖主义和秘密情报活动的调查中安装和使用笔记录仪、通信追踪装置。此类设备的安装和使用申请必须由总检察长或政府指定的检察官提出,并且应当包括申请人的认证,认证信息可能是通过与正在进行的防止国际恐怖主义或秘密情报活动相关的调查而产生。新权限不仅扩大到电话跟踪,还扩展到任何形式的电子通信跟踪。但是,修正案明确禁止调查受到宪法第一修正案保护的美国人的活动。

在 1990 年的美国诉 Verdugo-Urquidez 案中,美国政府在法庭文件中指出,“宪法第四修正案通常不会保护非美国人(位于美国境外的外国人)”,“第 702 条规定的外国目标缺乏第四修正案的权利”。尽管美国公民自由联盟坚持认为政府的分析是错误的,但不得不承认,在评估非美国人可获得的补救措施时,美国政府经常辩称,试图挑战无监控程序保障的非美国人无权获得宪法保护或救济[2]。

根据 FISA 规定的监控条件和程序,实践中,FISC 对于申请的批准极为宽松,自 1978 年成立至 2013 年,仅拒绝 12 个申请,批准 34 000 多个。

1.2　《电子通信隐私法》保障通信存储和传输安全

1986 年,美国国会通过《电子通信隐私法》(ECPA),防止政府未经授权获取私人电子通信,保障通信的存储和传输安全。该法是对 1968 年《综合犯罪控制与街道安全法》第三编的一项修订,包括《窃听法》《存储通信法》《笔记录仪法》三章。

《窃听法》保护传输过程中的有线、口头和电子通信。明确非法监听信息的证据排除规则,禁止将违反监听授权、程序等条件获得的信息内容的任何部分及延伸信息作为证据使用。通信监听只适用于能够提供证据的严重犯罪行为,授权和批准监听的命令期限不得超过 30 天。该法对执法机构实施的监控行为设置严格的程序要求,规定国会进行监督。

《存储通信法》保护存储的电子通信。禁止电子通信服务提供商自愿披露客户通信或记录。根据存储信息的时间不同(180 天内和超过 180 天),政府部门获得信息的程序也不同。

《笔记录仪法》禁止在没有法院命令的情况下,使用追踪设备记录有线或电子通信传输过程中使用的拨号、路由、地址、信号信息。在 Smith v. Maryland 一案中,法院认为,“由于电话公司可以访问通信信息,因此人们对此类信息没有合理的隐私期待”,裁定笔记录仪不受宪法第四修正案的保护。虽然该法将笔记录仪纳入规范,但对个人信息的保护程度明显弱于前两章,政府机构只需要很低的条件就能获得安装或使用的授权命令。

1.3　《通信协助执法法》明确电信运营商通信协助执法义务

数字通信技术的迅速普及给传统侦查手段带来巨

大挑战,联邦调查局和其他安全机构开始担心执法方式的有效性。1994 年,美国国会通过《通信协助执法法》(CALEA),确保电信运营商和设备生产商协助安全机构拦截数字交换设备上的通信,为政府机构实施监控提供便利。该法明确了电信运营商、设备生产商、电信后勤服务提供商等主体的协助义务和能力,要求电信运营商向用户提供的设备设施和服务能够根据合法授权,迅速对某类通信进行隔离并使政府实施监听。

2004 年以来,联邦通信委员会(FCC)一直在考虑如何将 CALEA 应用于新技术(如 VoIP)。2005 年 8 月,FCC 发布《拟议规则制定和声明性裁决的通知》,要求基础设施的宽带互联网访问服务商、提供使用公共交换电话网络服务的 VoIP 提供商必须接受执法部门监听。

水门事件后,美国构建了以保护国家安全和利益为核心的 FISA、以公民隐私为核心的 ECPA、以企业协助执法义务为核心的 CALEA。三部立法各有侧重,为美国情报监控制度提供了比较成熟的基础性支撑法律框架,主要内容和特点体现为:(1) 监控对象方面,严格区分美国人和外国势力及其代理人,二者的情报收集和监督程序不同,后者的情报收集条件更加宽松;(2) 监控客体方面,既包括对有线、口头、电子通信的动态和静态保护,笔记录仪、通信追踪装置的安装使用,对电话、电子通信的跟踪,也包括以获取涉外情报为目的经过授权和批准的物理性搜查;(3) 监控流程方面,一般通过法院签发的授权命令进行,总统可以根据规定通过司法部长授权在没有法庭命令的情况下实施不超过 1 年期限的物理性搜查。

2 911 恐怖袭击:促使政府情报监控权力不断扩张

911 恐怖袭击使得国家安全被提到前所未有的高度,为提高灾难性事件的防范和应对能力,美国进行了以“权力扩张”为核心的第二次大规模情报监控立法改革,通过《爱国者法》在内的多部立法扩张政府情报监控权限,公民自由权利受到极大限制。

2.1 《爱国者法》全面扩张政府监控权力

美国国会在对 911 事件进行调查后认为,政府机构的情报工作不力,特别是多个政府机构之间缺乏信息方面的沟通与合作,这是导致未能防范 911 事件的重要原因[3]。为了回应公众对政府未能阻止恐怖袭击的强烈抗议,事件发生仅六周后,美国便迅速通过《爱国者法》,削弱 FISA 及《窃听法》建立的有限隐私保护措施,扩大政府机构的情报监控权力。

该法在监控目的、客体、对象等各方面都有所扩张:目的方面,从“收集外国情报或调查国际恐怖主义”,扩大到“收集外国情报或防止国际恐怖主义”,“调查”意味着取得相关证据以证明事实,而“防止”则意味着不需要取得明确证据,只要怀疑与恐怖活动有关即可。客体方面,扣押物品从“业务记录”扩大到“任何有形物品”,将电子邮件等相关信息包括在笔记录仪、通信追踪装置监控之内。对象方面,从主要监控“外国人或外国势力”扩大到“任何人”。

《爱国者法》突破了情报监控立法的诸多限制,为政府情报监控行为提供了有力支持,也为政府以反恐名义更多涉入公民私人生活提供了法律依据,美国民众受宪法保护的部分公民权利也因此受到侵蚀[4]。《爱国者法》引起了国家公权力与公民私权利之间长达 14 年的争议,也为《美国自由法》的颁布奠定了基础。

2.2 《情报改革和预防恐怖主义法》完善情报机构职责

911 事件后,美国决策层决定打破之前“以机构为中心”的情报监控体系,将分散的情报力量聚合起来,形成一体化的国家情报工作[5]。2004 年 12 月 17 日,美国布什总统签署长达 235 页的《情报改革和恐怖主义预防法》(IRTPA),主要对国家情报界的结构和流程进行改革,明确各机构的监控职责,并适当维护隐私安全。该法是美国国家情报监控立法的重大举措,以推动和引领美国自二战后最彻底的改革而闻名[6]。

机构设置方面,明确总统在参议院的建议和同意下任命国家情报总监(DNI)。要求主任根据 1978 年 FISA 确定收集外国情报信息的要求和优先事项,并协助司法部长传播根据 FISA 收集的关于搜查和监控的信息。至此,国家情报总监接替并扩大了 1947 年《国家安全法》确立的中央情报总监(DCI)的职责,成为美国情报界的统一领导人,美国情报机构监管的分散化趋于集中化和统筹化,形成了“统一领导、协同合作”的监控模式。

隐私保护方面,规定在总统行政办公室设立隐私和公民自由监督委员会,负责分析和审查行政部门为保护国家免遭恐怖主义而采取的行动,确保其与隐私和公民自由保护的平衡;确保在制定和执行与保护国家免遭恐怖主义有关的法律、条例和政策时适当关注自由,要求提交主要机构活动的年度报告。在 DNI 办公室设立公民自由保护官,负责确保将公民自由和隐私适当纳入国家情报局的政策和程序,以及国家情报界的情报计划内容;监督 DNI 遵守宪法和所有与公民

自由及隐私有关的法律、法规、行政命令的实施准则。

2.3　12333 号令修正案扩大情报机构监控职责

根据 1974 年《国家安全法》的规定,美国总统对情报监控活动具有一定控制权和监督权,可以通过发布行政令的方式行使职权,这也是美国实现情报监控的重要手段。1981 年,美国总统发布 12333 号行政令《美国情报活动》,扩大美国情报机构的权力和责任,规定了包括国防部、能源部、财政部等在内的国家情报机构的作用,指示美国联邦机构领导人支持中央情报机构的信息请求。该令被美国情报界视为授权扩展数据收集活动的基本文件,成为美国国家安全局收集谷歌和雅虎数据中心传输的未加密信息的合法授权来源。该令在 2003 及 2004 年进行修订,对个别机构职责进行调整。

2008 年 7 月,DNI 发表声明称:“12333 号令已经成为美国情报界的基石,并在超过四分之一世纪的时间里为情报界提供了良好服务,2003 年、2004 年的修订都在 IRTPA 之前,未能符合 IRTPA 的规定,随着新的国家安全机构兴起和我们应对当前、未来国家安全威胁能力的提高,是时候更新这一基础文件以反映现实问题,更好地支持情报活动。”同年 8 月,布什总统发布 13470 号行政令《12333 号行政令美国情报活动的进一步修正案》,加强情报机构权力。DNI 将为国家情报活动设定目标,发布管理收集、分析和情报共享的指导方针,制定政策指导美国与外国的情报关系;在必要时建立国家情报中心,决定情报界的使命和职能;更多地参与选举,并在必要时参与高级情报人员的免职。此外,行政令维护并加强了对美国人自由和隐私权的保护,所有关于美国人的信息收集、保留和传播都必须按照司法部长批准的程序进行。

2.4　FISA 相关修正案进一步强化政府监控权力

随着无线通信技术的发展,FISA 已经不能覆盖所有的情报范围,且政府很多情况下都需要获得法院命令才能开展情报监控工作,这为情报的迅速转移提供了时机,可能无法使美国政府获得实时信息。为促使 FISA 紧跟时代发展,美国政府对相关条款进行修正,严格限制 FISC 的授权,加强对包括美国人在内的监控。

2007 年 8 月 5 日,布什总统签署《保护美国法》,主要修正 FISA 第 105 条,强化对非美国人的监控。该法明确,FISA 中电子监控的定义不得被解释为包含针对有理由相信是非美国人的监控,这就允许情报人员无须获得 FISA 规定的法院命令,就可以收集非美国人的情报信息。此外,该法为 FISC 审查情报机构监控非美国人提供了额外程序:基于“获取不构成电子监控、目的是外国情报信息、获取活动使用最小化程序”等条件,DNI 和总检察长可以在不超过 1 年的时间内授权获取被合理地认为是非美国人的情报信息。该法颁布后 180 天即失效,但根据该法获得的涉外情报监控授权及根据授权发布的命令,一直到授权或命令自身期限到期为止。

2008 年 7 月 10 日,布什总统签署《2008 年 FISA 修正案》。2012 年 9 月和 12 月,众议院、参议院分别投票通过将该修正案延长 5 年。该修正案的重要内容是增加 702 条,授权美国政府无条件从美国境内电信和互联网服务提供商等企业处获得美国人的国际通信。虽然 702 条进行的监控依然在美国境内进行,但与 FISA 历来进行的监控相比,702 条的范围更广,且仅受有限的司法监督形式约束。

首先,702 条允许政府毫无依据地监视美国人和非美国人之间的通信,授权政府在“电话或互联网通信中至少有一方是非美国人”、“监控的重要目的是收集外国情报”的情况下截获通信。允许政府将任何非美国人作为目标以获取外国情报,例如允许政府在未授权情况下获得可能正在策划袭击事件的非美国人的电子邮件或通话记录。702 条允许进行的监控远超过维护国家安全所需要的范围,为美国进行大规模情报活动奠定了合法基础。

其次,对 FISC 在授权 702 条进行监控中的作用进行“严格限制”。FISC 并非单独审查行政部门的目标或被监控主体,而是每年审查一次能够明确外国情报监控类别的美国政府的“证明”。这些类别实际上十分宽泛,往往涵盖“外国政府及类似实体”、“反恐”和“大规模杀伤性武器”。根据外国政府证书的泄露版,FISC 已允许美国情报机构行使其酌处权对 190 多个不同国家进行监控[7]。

《2008 年 FISA 修正案》增强了《爱国者法》赋予美国国家安全局的权力[8]。政府的官方披露显示,政府使用 702 条至少进行了“上游”监控和“PRISM”监控,对数据进行了大规模不加处理的收集。上游监控涉及到大量复制和搜索流入、流出美国的互联网通信,在 Verizon 和 AT&T 等公司的帮助下,国家安全局通过直接进入美国内部互联网骨干网——承载全球数亿人口通信的物理基础设施进行监控。通过上游监控,NSA 可以无限制地复制并搜索通过其监控设备传递的大量个人元数据和内容,因此可以广泛访问通信内容。PRISM 监控是直接从美国互联网和社交媒体平台公司获取通信内容和元数据,政府先确定要监控的用户账户,然后命令提供商向其披露这些用户所有的通信和数据。通过 PRISM 监视,美国政府可以获取实时通信

和存储通信。

鉴于911恐怖袭击带给美国国家安全的担忧,这一时期政府情报监控立法改革以“权力扩张”为核心,主要内容和特点包括:1)监控对象方面,《爱国者法》扩大到所有人,但仍然区别对待美国人和非美国人,对于二者进行监控的目的、流程等设置不同条件。所有关于美国人的信息收集、保留和传播都必须按照司法部长批准的程序进行,而对于非美国人的信息收集要求则相对宽松。2)监控客体方面,物理搜查扩大到“任何有形物品”。电子监控将电子邮件、通话记录包括在内。3)监控流程方面,增加新的情报收集机构,明确美国增加情报授权的合法渠道,DNI、总检察长等情报人员无需获取法院命令收集信息的情况。设立公民自由保护官负责监督DNI有关隐私制度的执行。

3 棱镜门事件:推动隐私保护成为立法改革的重要元素

2013年,美国情报机构长期进行大规模情报监控行动的棱镜门计划被披露。从传统盟国到敌对国家,从国家呼吁民用互联网接入记录,世界各国网络已被美国列入监控和监视类别[9]。为了提高美国在国际社会中的信誉并继续保持监控的合法地位,美国进行了以“维护隐私权”为核心的第三次大规模情报监控立法改革,通过发布总统令、修订FISA等制定有效机制限制政府监控权力。

3.1 《信号情报活动的总统令》确定非美国人隐私保护

2014年1月17日,美国白宫新闻秘书办公室发布第28号总统令《信号情报活动》(PPD-28),要求从政策和程序上保障信号情报活动中收集的个人信息。该令提出四大原则:合法收集,尊重隐私和公民自由,收集外国私人商业信息或商业秘密的目的限制,尽可能有针对性地进行信号情报活动。将批量收集非公开信号情报限制在侦查和反击使用数据。

虽然该令承认非美国人的隐私,但后续几乎没有进行有意义的修订或改革,美国总统可以很容易地修改或撤销该令。2017年6月,美国政府发布2014年FISC意见的部分修订版本,裁定PPD-28“按其条款而言不具有司法强制性。”[10]因此,即使法院裁定美国政府对PPD-28拥有司法管辖权,实际上也无法执行该裁决。PPD-28几乎可以说是未对政府机构的监控行为作出有意义的限制措施,美国政府的监控行为仍在大规模持续进行。

3.2 《美国自由法》严格限制大量收集电话元数据

无论是出于维护国家安全和利益的政府行为,还是促进创新发展的企业行为,棱镜门引起的大规模监控都令人无法容忍,越来越多的大型科技公司对其向美国政府提交用户数据的方式质疑[11],美国开始重新思考情报监控的适用范围。在通信技术不断进步的环境下,考虑到未经授权披露的风险以及维护公众信任的需要,2013年8月,白宫新闻秘书办公室发布《审查我们全球信息情报收集和通信技术的总统备忘录》,指示建立情报和通信技术审查小组,审查美国是否利用技术收集能力最好地保护国家安全并有效推进外交政策。

2013年8月,奥巴马总统宣布该审查小组正式成立。12月,审查小组发布长达300页的《变化世界中的自由与安全》报告,提出旨在保护美国国家安全和推进外交政策的46项建议。明确美国政府必须保护两种不同形式的安全,即国家安全和个人隐私安全,呼吁将1974年《隐私法》适用于全世界人民[12]。报告分析了《爱国者法》和FISA的相关条款,针对二者即将到期的现实情况及批量收集数据的行为,建议制定立法限制批量收集数据、提高透明度、加强非美国人的隐私保护并改革机构。

在此背景下,美国情报监控立法进行了历史性的重大改革。2015年6月2日,美国颁布《美国自由法》,对情报机构大量收集公民电话元数据的行为施加严格限制,电话服务提供商将持有和查询电话详细记录而不是政府。该法是1978年FISA通过以来,国会首次采取措施限制而不是扩大政府的监控权力,在第114届国会(2015—2016)上曾被称为寻求“国家安全和隐私保护的一种平衡方法”。该法延伸了《爱国者法》中很多到期的条款,主要内容包括:

1)禁止根据《爱国者法》第215条批量收集美国人的私人记录。对批量收集美国人电话记录和互联网元数据的国家安全机构进行重大改革;禁止根据215条和FISA笔记录仪的相关规定批量收集数据,要求政府在合理可行的最大程度内限制收集范围,禁止政府收集所有与特定服务提供者或广泛地理区域相关的信息,例如城市或地区代码;禁止根据国家安全信函批量收集数据。2)授权情报机构以更有针对性的方式收集电话记录。授权政府一天获得两项“电话详细记录”,当能够向FISA法院证明具有合理理由怀疑搜索词与外国恐怖组织有关时。3)增加监控活动透明度。要求FISA中的情报机构进行政府报告;私人企业向公众报告其收到FISA命令和国家安全信函数量;要求

FISC 对含有重要法律解释的意见进行解密,如果无法解密则需要公开意见的摘要。

根据该法要求,美国法院行政办公室主任必须在互联网上公布 FISC 活动的统计数据。2015 年至 2019 年,办公室已发布五份报告,公布世界各国或地区政府机构向 FISC 提出的电子监视、物理搜索等申请、批准及被拒绝数量。美国法院行政办公室主任每年向参议院情报委员会、司法委员会,众议院情报委员会、司法委员会分别提交年度报告,接受 DNI 和总检察长的解密后在互联网上公开发布。解密后的内容至少包括:情报机构提交的监控申请订单和数量,涉外情报监控法庭审议后直接批准、修改后批准、全部驳回,以及部分驳回的申请数量,任命的法庭之友名单等。

3.3　12333 号令最新程序限制信息收集及处理

情报是预防恐怖主义、维护国土安全最为有效的手段,但这不能成为践踏人权、损害国际关系的借口,一切情报活动都必须纳入法治轨道在法律框架内进行,相应的监督机制亦是确保情报活动合法性与正当性的必要手段[13],美国政府显然对此有更加深刻的理解。2017 年,中央情报局(CIA)发布根据 12333 号令收集、保留和传播美国人信息的最新程序,平衡 CIA 情报责任与美国人隐私保护的关系。新程序共包含三个文件《CIA 情报活动:司法部长根据 12333 号行政令批准的程序》《关于发布 CIA 更新 12333 号行政令程序的声明》《CIA 更新 12333 号行政令的司法部长指南》。

新程序对收集、查询、处理信息都进行限制:1)收集限制。对于无法及时评估其价值的信息,应该采取“合理步骤”将信息收集限制在实现 CIA 被授权的情报目标所需的最小数据子集中。收集针对美国人的信息只能在正式授权的情报活动中进行。2)查询限制。查询 CIA 持有数据情况时,仅能针对 CIA 授权的情报活动进行。对特别敏感的数据进行查询应附有查询声明,例如查询美国人的通信内容。3)处理限制。限制访问未评估的电子通信及类似敏感数据,对这些数据的处理需要经过培训后进行;除非符合例外条件,否则 CIA 专业人士提供后的五年内必须销毁这些数据。4)合规与监督。对可能导致获取美国人个人信息的活动规定了授权、文件和定期审计要求。

3.4　《FISA 修正案再授权法 2017》加强涉外情报监督制度

2018 年,美国总统特朗普签署《FISA 修正案再授权法 2017》,加强涉外情报收集的保障、问责和监督制度,同时将 702 条的有效期(2018 年 1 月 19 日到期)延长至 2023 年 12 月 31 日。修正案签署当天,特朗普发布声明称:“702 条已经被证明是最有效的外国情报收集工具之一,签署修正案对维护国际安全至关重要。该条为美国人提供了强有力的隐私保护,禁止政府使用该条监控美国人,只有非美国人可能成为监控目标。”此次修正,意味着美国情报机构将能继续在无授权情况下,监控美国境外目标的电子邮件和短信等通信。

修正案对 702 条进行了重大改革,增加了一些前所未有的保障措施,主要内容包括:1)查询程序要求。要求司法部长和 DNI 采用“符合第四修正案要求”的程序查询根据第 702 条授权收集的信息,这些程序将控制搜索受到外国情报监视法院审查的有关美国人的通信。2)使用和披露规定。限制根据 702 条获取的美国人信息作为刑事诉讼的证据使用,除非 FBI 获得该修正案要求的法院命令,或该刑事诉讼涉及死亡、绑架、严重身体伤害、对未成年人犯罪、关键基础设施失能、网络安全和跨国犯罪。要求分类披露有关美国人和非美国人的电子监控目标。3)公开发布。司法部长和 DNI 必须每年公开发布适用于处理根据 702 条收集的美国人信息最小化程序的解密版本。

2020 年 4 月,FISC 发布的 2019 年度报告显示,2019 年 FISC 完全拒绝 20 份申请,部分拒绝 38 份申请,修改 264 份申请中所请求的命令,批准 688 份申请。仅 2019 年,FISC 所拒绝的申请就超过了 1978 年至 2013 年间的申请数量总和,可见情报监控立法改革取得了显著成效,对隐私保护产生了积极效应。

3.5　《国家情报战略 2019》强调隐私和透明度

美国情报监控战略涵盖内容广泛且体系复杂。从横向领域来看,美国情报战略体系可划分为若干相互联系又相互独立的平行部分,如反情报、信息共享、网络空间以及情报人力资本等[14];从纵向看,有国家层面的、情报界层面的、情报机构层面的,上一层面的情报战略指导下一层面情报战略的目标确立和基本原则。这里以美国情报的最高指导文件《国家情报战略》为对象,考察其与情报监控法律的相互推动和促进作用。

早在美国情报局成立十周年之际的 2005 年,美国便发布了国家层面统一的《国家情报战略》(NIS)。该文件提出了一个更加统一、协调和有效的情报监控框架,用于指导美国情报界的政策、规划、收集、分析、运作、获取、预算和执行等。NIS 最早源于 2002 年的《国家安全战略》,法律依据是 2004 年的 IRTPA,主要目的是在美国情报界创建一个信息共享的新系统,使得美国情报监控工作更加有效率。NIS 于 2009 年、2014 年

分别进行更新。21 世纪,美国面临着国内和全球环境的重大变化,为应对新威胁并抓住新机遇。2019 年,美国国家情报局发布第四版 NIS,明确了情报机构的职责和分工,在未来四年指导美国十七个情报机构的工作方向。面对充满对手和威胁的整体战略环境,改版战略提出了四大优先事项:整合、创新、伙伴关系、透明。

NIS 自从 2005 年发布之后就被不断调整,迄今为止一共发布四版,但本质目标都是通过构建集中化、一体化的情报界和创新实现美国情报活动的转型,以便在执行任务中取得最佳效果和价值。而隐私保护、透明度是 NIS 的重要组成部分,第四版 NIS 明确要求“将隐私和公民自由纳入情报界的政策和计划”,“在不损害国家安全的前提下,促进情报界有适当的透明度来公开信息。”

棱镜门逼迫美国在立法上限制政府监控行为,采取调整监控权力的迂回路线,以迎合国内外对于隐私和知情权被侵犯的担忧。此次情报监控立法改革侧重规范监控流程、增加透明度及保护隐私:1)监控对象方面,仍然区分美国人和非美国人,但进一步加强了两者的隐私保护措施;2)监控客体方面,加大限制政府收集信息的范围,例如禁止政府大规模收集电话元数据,禁止收集城市或地区代码等与特定服务提供者或广泛地理区域相关的信息;3)监控流程方面,在收集、查询、处理、披露、公布信息等阶段都增加了严格的程序限制,尤其强调增加透明度。

4 我国情报监控政策构建及法制化路径

我国更多通过部门规章或内部文件进行情报监控活动,情报监控立法层级低,情报活动缺乏透明度。通信技术的广泛应用使传统调查和侦查方法变得越来越困难,强化和扩张情报监控活动成为各国的普遍选择。2017 年,我国发布情报领域第一部综合性立法《国家情报法》,提升立法层级,推动我国情报活动的法制化道路。然而,我国目前存在的立法内容较为原则、监控活动具有秘密性问题,使情报监控活动仍然面临着巨大的不确定性,且容易产生公权力滥用的风险。美国情报监控政策立法的发展历程及内容,对改进我国的国家安全情报工作、建成情报强国,具有重大借鉴意义[15]。

4.1 完善情报监控的顶层设计

美国在 2005 年就发布了国家层面的情报战略,并且随着情报活动的实际需求、国内外环境变化、新技术的挑战不断更新完善。迄今为止四版的 NIS 都提出了情报界的任务目标和企业目标,为美国情报未来发展指明方向。此外,美国还通过发布总统令、行政令的形式确定情报监控的原则、行动方向等,以此指引立法改革。我国情报监控并未有政策层面的规定,即使网络空间领域的首部文件《国家网络空间安全战略》也并未对情报监控活动作出指示。情报监控在维护国家安全、便利重大刑事调查、预防和打击恐怖主义方面具有不可替代的重要意义,国家和政府的情报收集及分析能力在一定程度上决定了突发和应急事件处置的完备性和有效性。战略、政策文件等顶层设计能够划定当前和未来规划,洞察国内外网络安全发展形势。我国应该借鉴美国对于情报监控的战略及指令体系,加快顶层设计,以指引法律、行政法规层面的情报监控制度完善,提升国家情报收集和分析能力。

4.2 完善情报监控的程序规定

以我国公开的法律层面的情报立法《国家情报法》而言,在情报监控流程方面,主要强调“任何组织和公民依法支持、协助和配合国家情报工作”,“国家情报工作机构根据工作需要,按照国家有关规定,经过严格的批准手续”。这里的“依法”、“按照国家有关规定”表述模糊,对于“严格的批准手续”并未明确具体的审批流程和有权批准的机构。要求组织和个人配合国家情报监控是国际通行做法,美国和我国的情报立法都不例外。但《国家情报法》关于“依法”等类似规定,导致情报监控流程难以合规,不仅会降低法律的可操作性,还可能使得外国政府及企业以“中国企业将配合政府开展窃密行为”为由(主要针对第七条),对我国进行无端指责。建议我国情报监控按照信息生命周期制作详细流程,明确信息收集的条件、原则、存储措施、存储时限及违反的处罚制度。建议成立专门的情报申请审批机构(类似美国 FSIC 的独立审查员),并严格机构成员的选拔条件,由机构对申请进行独立审查并授权。

4.3 增加情报监控的透明度

出于维护国家安全和利益需要,情报监控一般具有秘密性。然而,透明度对于公众监督政府机构监控行为及分析立法影响至关重要,公众的知情权必须被保证。最近几年,美国情报监控立法对政府和企业增加了公开义务,政府机构要进行报告并接受监督,私人企业要向公众公开其收到的监控命令和国家信函数量。此外,美国在最新的 NIS 中再次强调透明度的重要性。出于保护国家秘密或者商业秘密的考量,监控过程的细节可以不公开,但至少应该公开政府情报活

动的结果。我国《国家情报法》未要求政府机构公开披露监控结果,不利于保护公众知情权,更有可能引起境外政府机构和企业的不信任。为保证公众知情权,建议国家安全、公安机关情报机构在解密之后公开企业或个人的协助结果,披露申请数量、情报监控主体等基本情况。

4.4　构建内外平等的隐私保护原则

日益增长的网络攻击、恐怖主义、网络犯罪迫切需要情报活动开展重要工作以保护安全。但应对这些威胁的大规模情报监控工作会干扰民众的基本权利,尤其是隐私和数据保护[16]。情报监控立法应始终以"寻求一种能够获得必要调查数据,同时增加隐私保护的解决方案"为目标。对于个人信息,建议严格按照《信息安全技术 个人信息安全规范》(GB/T35273 - 2020)标准所规定的范围进行分类,对敏感和隐私信息应该具有更严格的收集条件、审批流程和保护措施。出于执法需求等收集敏感信息的应该以邮件、短信等方式通知信息主体,保证其知情权和申诉权。机构设置方面,可以借鉴美国 2004 年 IRTPA,在情报机构内部设立公民自由保护官,监督隐私信息收集过程的规范性。目前,我国加快了《个人信息保护法》的制定进程,应该在这部专门性立法中增加公权力侵犯私权利的民事补偿或救济措施。需要特别注意的是,区别对待原则容易使得政府机构滥用监控权力,引发执法不规范情况,我国应避免美国的内外有别原则。

5　结　语

美国是运用情报监控最为灵活和多元的国家,这也使其国内的情报监控立法极为发达。为了适应不断变化的国际形势,美国情报监控立法对透明度、隐私保护等进行了多角度改革,在保障个人基本权利与维护国家安全利益之间寻找"最大公约数"[17]。网络恐怖主义、网络攻击等安全事件频繁发生,愈发凸显出情报监控活动的重要性,而公民隐私意识的觉醒增加了情报监控流程制定和立法内容的复杂性。2020 年 2 月,"华盛顿邮报"披露,美国中央情报局通过控制瑞士 Crypto 公司,窃听全球 120 国最高机密长达数十年,此事件使得情报监控活动的合法性边界再度被思考,各国的情报监控立法行动和态度更为审慎。我国应该尽快推动情报监控活动的顶层设计,发布相关政策、战略文件予以重视。在法律层面,应该致力于推动情报监控的程序合法化、增加监控行为的透明度,并完善监控过程中的隐私保护措施。

参　考　文　献

[1] Solove D J. Reconstructing electronic surveillance law[J]. George Washington Law Review,2004,72(6):1701 - 1747.

[2] Ashley gorski american civil liberties union foundation. Summary of U. S. foreign intelligence surveillance law, practice, remedies, and oversight[R/OL]. ACLU, 2018: 1 - 44. https://www. aclu. org/sites/default/files/field_document/cjeu_schrems_report_final_august_30_2018. pdf.

[3] 周学峰. 解读美国电子监控制度的演变[J]. 北京理工大学学报(社会科学版),2014,16(6):110 - 118.

[4] 刘卫东.《爱国者法》及其对美国公民权利的影响[J]. 美国研究,2006,20(1):75 - 88.

[5] 谢海星. 聚焦"一体化"的美国国家情报体系改革[J]. 情报杂志,2019,38(10):27 - 31.

[6] 邓娥荣. 论 21 世纪美国国家情报立法的利益竞争困境——以美国《情报改革与恐怖主义预防法》的颁布和落实为主要依据[J]. 情报杂志,2017,36(1):18 - 22.

[7] Affidavit of general Keith B. Alexander, united states army, director, national security agency. In the matter of foreign governments, foreign factions, foreign entities, and foreign-based political organizations[R/OL]. 2010: 1 - 4. https://www. clearinghouse. net/chDocs/public/NS-DC-0074-0002. pdf.

[8] Kulesza J. USA cyber surveillance and eu personal data reform: PRISM's silver lining? [J]. Groningen Journal of International Law,2014,2(2):72 - 89.

[9] 刘天慧. 中美俄欧网络安全立法比较研究[D]. 哈尔滨:哈尔滨工业大学,2018.

[10] United States foreign intelligence surveillance court Washington, D. C. [R/OL]. ACLU, 2014:1 - 39. https://www. intelligence. gov/assets/documents/702% 20Documents/declassified/Bates%20510 - 548_OCR. pdf.

[11] 惠志斌, 覃庆玲. 中国网络空间安全发展报告(2016)[M]. 社会科学文献出版社,2016.

[12] Diersch V. The president's the review group on intelligence and communications technology[J]. Zeitschrift für Sicherheits-und Auβenpolitik 2014,7(3):417 - 419.

[13] 王君清, 屈健. 美国涉外情报监控活动监督机制评析[J]. 武警学院学报,2017,33(5):83 - 88.

[14] 聂宏. 美国情报战略体系解析[J]. 情报杂志,2018,37(10):42 - 49.

[15] 高金虎. 一个情报强国的崛起路径——以美国为例[J]. 情报杂志,2020,39(1):1 - 9.

[16] European union agency for fundamental rights. Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU[R/OL]. 2017:1 - 166. https://fra. europa. eu/sites/default/files/fra _ uploads/fra-2017-surveillance-intelligence-services-vol-2_en. pdf.

[17] 王新清, 李响. 美国电子监控与情报搜集制度研究——兼论我国反恐情报与技术侦查制度的完善[J]. 中国刑事法杂志,2017,1(1):94 - 112.