云环境下政府数据存取的法律困境及应对

马　宁

(西安交通大学　法学院,陕西　西安　710049)

[摘　要]　政府数据存取法律制度是一国政府有效实施调查权的必要保障,为了刑事侦查与反恐之目的,各国立法普遍赋予本国政府进行数据存取的权力。但在云环境下,由于云计算自身的技术特性,政府存取云数据将面临执法方面的障碍,需要云服务商提供必要的执法协助,并对存取途径和方法进行调整。同时,云计算海量用户数据的集中存储为政府利用数据存取进行大规模的数据挖掘提供了可能,加之用户对数据的所有权与控制权相分离,这愈发引起公众对政府公权力滥用的担忧,需要立法对相关利益进行平衡。但我国目前可适用于云计算政府数据存取的法律规定较为笼统且分散,与云用户和云服务商合法权益息息相关的协助执法补偿制度和侵权救济制度仍然存在立法缺位,亟待对相关法律制度进行调整与完善。

[关键词]　云计算; 政府数据存取; 法律困境及应对

[中图分类号]　D923.4　　[文献标识码]　A　　[文章编号]　1000 - 5072(2014)01 - 0054 - 09

一、云计算对政府数据存取的影响

政府数据存取(Government Access to Data)也称政府数据访问或政府数据获取,是指政府机构①在履行其职责的过程中访问及获取相关数据的活动[1]114。为了维护国家安全和社会稳定,各国立法普遍承认和赋予政府为刑事侦查之目的进行数据存取的权力,特别是在"9·11"事件之后,为了更为有效地预防和打击恐怖主义,政府进行数据存取的职权得到强化。例如美国爱国者法案以防止恐怖主义为目的扩张了美国警察机关的权限,规定警察机关有权搜索电话、电子邮件通信、医疗、财务和其他种类的记录。英国调查权管理法案规定,如果政府证明存在合理理由确信存在刑事犯罪(不包括轻微刑事犯罪),而获取数据对于侦破案件有重大价值,政府可以要求法官签发搜查和扣押令,以存取相关数据。随着云计算服务的全球化繁荣和云计算技术的多维度部署,大量的个人和企业数据向云端迁移,数据的集中存储似乎给政府数据存取提供了更为便利的途径,但事实并非如此[2]。

美国国家标准和技术研究院(NIST)②提出的云计算定义目前受到最广泛的认可,其认为云计算是一种能够通过网络以便利的、按需付费的方式获取计算资源(包括网络、服务器、存储、应用和服务等)并提高其可用性的模式。按

[收稿日期]　2013 - 07 - 01

[作者简介]　马　宁(1984—),男,河北保定人,西安交通大学法学院博士生,主要从事信息安全法研究。

[基金项目]　国家社会科学基金西部项目《网络安全监控的法律对策研究——以通信协助执法法律制度的构建为视角》(批准号:10XFX009)。

* 本文在撰稿过程中受到了西安交通大学法学院马民虎教授的指导,得到了方婷博士的大力支持。

① 这里的"政府"包括所有基于执法和维护国家安全的目的的各类执法机关和其他政府机构。

② 美国国家标准与技术研究院(National Institute of Standards and Technology,NIST)直属美国商务部,从事物理、生物和工程方面的基础和应用研究,以及测量技术和测试方法方面的研究,提供标准、标准参考数据及有关服务,在国际上享有很高的声誉。

照 NIST 的定义,云计算模式的技术特性将导致用户数据的收集、使用和处理在整个数据生命周期中凸显出异质性,对政府数据存取产生了多维度的影响。

第一,政府数据存取在云环境下最大的障碍在于可能产生的隐私侵犯。尽管政府公权力与个人隐私权冲突具有相当的普遍性,并非为云环境下政府数据存取特有的关注点,但由于云环境下用户对数据的控制力被削弱[3] 157,这种冲突将变得更为激烈且难于控制。在每一个历史时期,"人们都使各种价值准则适应当时的法学任务,并使它符合一定时间和地点的社会理想"[4]。理论上,云计算和隐私保护是一致的。随着用户数据控制权转移至云服务商一方,用户在选择云服务时往往具有更高的隐私期待。但数据的大规模存储和处理本身就存在极大的安全隐患,技术脆弱性所引发的数据泄露、丢失、混同等安全风险较于传统 IT 环境更为突出,云服务商需要负担更为严格的数据安全义务,云服务商必须采取更为紧缩的数据访问控制策略,例如尽量控制第三方对用户数据的访问、最小化访问特权、严格限制用户数据披露等等。这些内部控制措施在客观上造成政府进行数据存取的过程更为困难,获得数据的周期加长,甚至产生云服务商拒绝政府进行数据存取的情况①。

第二,政府进行数据存取的前提是云服务商提供有效的数据访问途径或提供政府试图存取的数据,这要求云服务商应当知悉数据的实时位置②。但云环境中的数据流动相较于传统 IT 服务而言更为灵活和难于控制,特别是在多数据中心的情况下,云服务商可能无法获知某一特定时刻数据存储的具体位置,而无法满足政府进行数据存取的要求。此外,为了实现成本效益,多租户共享资源是云服务的基本模式,云服务商通常将用户数据集中存储。为了向政府提供可用的数据,云服务商需要把云中所存储的数据重新组合,并将政府所存取的数据分离出来,同时还要保证其他云用户敏感数据的隔离安全。如果不能按照要求提供数据,政府可能会选择对所有存储在服务器上的数据进行存取,这势必增大了数据存取的难度,也将导致政府获得不相干用户的数据,产生隐私侵犯的潜在风险[5] 81。

第三,政府数据存取最根本的目的通常与刑事侦查相关联,因此数据的真实性至关重要。但云环境相对于传统物理隔离的 IT 环境更为开放和具有弹性,用户数据更容易受到未经授权的访问、篡改、变更和删除,任何在技术和管理方面的疏漏都可能对数据的真实性造成减损。最常用的保证数据真实性的方法是在整个数据生命周期中采用加密措施,但这又带来另一个问题,基于刑事侦查的需要,加密的数据通常不符合政府数据存取的要求,各国法律一般要求云服务商提供明文数据。如果数据为云服务商加密,政府可以要求云服务商提供密钥或解密数据,但如果数据为用户加密,在缺乏密钥托管机制的情况下,云服务商需要通知用户解密数据或提供密钥,这造成政府数据存取活动的秘密性降低,也可能由于用户恶意删除或篡改数据的行为而影响数据的真实性。

第四,政府数据存取通常依据特定的管辖权,即只有在立法所确立的司法管辖权范围内,政府才能够进行必要的数据存取。例如美国政府强调本国法律的优先适用原则,当云服务商位于美国,或者在美国有分公司或办事处,或者在美国有连续进行的业务,相关的云服务即被纳入美国的司法管辖权范围。但在云服务中的数据跨境传输成为常态,云用户、云服务提供商、云基础设施提供商、数据中心可能分属不同的国家,因此政府是否有权存取位于管辖区外的数据成为云环境下政府数据存取的重要问题[6] 19-27。出于对用户隐私的考虑,云服务商可能寻求规避政府数据存取强制性法律要求的方法。例如一些云服务商建议用户选择位于安全地区或国家的云数据中心,这些地区或国家通常较少受政府数据存取的影响[7]。尽管从执

① 例如 Google 基于用户隐私保护的考虑开始限制政府存取云端数据。

② 例如欧盟法律要求提供存储服务的经营者在任何时候都应该知道个人数据的所在位置。

法的角度考量,云计算代表了在数据跨境中必然会发生的管辖冲突,但法律互助协议[①]能够显著减少政府获取他国云数据的阻碍。例如,德国政府与美国政府关于刑事调查事项签订的协议[②],允许成员国要求获取和接受位于其他成员国的信息(包括存储在第三方设备上的信息)。因此,政府在云环境下进行数据存取必须开展更为广泛的国际合作,避免管辖权争议。

第五,云计算海量用户数据的集中存储为政府利用数据存取进行大规模的数据挖掘(Data Mining)[③]提供了可能,数据挖掘可以使政府获取隐含的、具有潜在价值的信息,并可以使这些信息更为明确地指向个人,这愈发引起公众对政府公权力滥用的担忧。我们注意到越来越多的国家开始基于反恐目的授权政府进行数据存取,由于以反恐为目的的数据存取很难在立法上划定数据获取的范围,在实践中往往会放宽对数据特定性的要求,受到"最小化收集原则"的限制更小,政府可能会对云端数据不加区分地进行存取,以在最大限度上满足反恐的要求。因此在云环境下,政府数据存取极易被泛化和滥用,对用户隐私产生更为严重的侵犯。需要立法确立更为有效的监督和审查机制,明确对个人隐私的保护态度,强化政府对数据的保密义务。

政府数据存取在云环境下一方面受到外部技术因素的影响,获取数据的难度加大;另一方面云计算海量用户数据的集中存储为政府利用数据存取进行大规模的数据挖掘提供了可能,政府数据存取泛化和滥用的风险加大。这些特殊性需要建立与云环境下政府数据存取更为契合的法律框架,调整和完善现行法律规范,充分应对云环境下政府数据存取的困境,并弱化权力滥用的风险。

二、欧美云环境下政府数据存取的法律实践

(一)美国云环境下政府数据存取的法律实践

通常认为,美国云环境下的政府数据存取以爱国者法案为基础,爱国者法案以防止恐怖主义为目的扩张了美国警察机关的权限,规定警察机关有权搜索电话、电子邮件通信、医疗、财务和其他种类的记录,并减少对于美国本土外情报单位的限制。该法案延伸了恐怖主义的定义,扩大了警察机关可控制的活动范围。尽管爱国者法案普遍被认为赋予政府更多地获取数据的权力,但事实上爱国者法案并没有提供新的更广泛的调查权力,而是扩大了现有的调查方式,并限制了滥用宪法和法律的行为[④],例如根据爱国者法案,政府访问电子文件和通信内容比其他非核心数据信息有着更严格的限制。

但在大多数情况下,政府存取云数据需要受美国电子通信隐私法(ECPA)的规制,根据规定,只有法官发出搜查令,或者政府向云服务商发出有效传票的情况下,政府才能够存取相关的云数据。而法官只有在有理由相信发生刑事犯罪或在云数据中能够找到犯罪证据时,才能对云服务商发出搜查令。在电子通信隐私法的规制下,政府获得搜查令是唯一有权存取云数据的途径。如果政府通过搜查令或传票要求存取用户数据,通常政府在从云服务商手中获取数据之前必须通知用户。此项规定能够保证用户的知情权,允许用户对政府存取云数据提出质疑[⑤]。但如果通知云用户将威胁到其人身安全,这种通知就可能会被延迟。美国电子通信隐私法案禁止云服务商在没有收到正式法律要

① 法律互助协议(Mutual Legal Assistance Treaties,以下简称 MLATS),指影响两个或多个国家的协议,能够允许政府机关基于刑事调查的目的存取存储在其他国家的云数据。

② 2003 年德国政府与美国政府关于刑事调查事项签订了法律互助协议,并在 2006 年关于此项协议签订了补充条约,于 2009 年 10 月 18 日正式生效。

③ 数据挖掘是指从大量数据中揭示出隐含的、先前未知的并有潜在价值的信息的过程。数据挖掘是一种决策支持过程,通过分析数据,做出归纳性的推理,帮助决策者调整策略,减少风险。

④ 如果政府通过搜查令存取用户的非核心数据则不需要事先通知用户,例如联系信息和服务器日志信息,但用户可以在数据披露后质疑法庭搜查令的有效性。

求时自动披露云用户的数据[①],禁止美国政府拦截传输中的电子数据[②]。

此外,美国政府在某些反恐和国外情报收集过程中还可以通过外国情报监视法案命令(FISA Orders)和国家安全信函(NSLs)存取云数据。如果政府表明存在合理理由相信获取云数据与获取外国情报或反对恐怖主义或间谍活动的调查相关,政府可以存取诸如联系方式、服务年限或交易记录等用户非核心数据,但一般不会包括服务器中的电子记录和文件。外国情报监视法案命令和国家安全信函是在美国爱国者法案之前就以立法形式确立的,但爱国者法案扩大了政府存取数据后云服务商协助执法的义务。例如爱国者法案增加了"司法限制言论令"(gag order)[③]的规定,禁止接收到外国情报监视法案命令和国家安全信函的云服务商披露相关事实。但如果云服务商认为政府存取的数据扩大了其实际需要的数据范围,可就该命令提出质疑。

(二)欧盟云环境下政府数据存取的法律实践

欧盟在其相关的条例、公约、指令中明确了政府数据存取的权力,并要求云服务商提供必要的协助。虽然欧盟的网络犯罪公约(以下简称公约)不会被其成员国直接使用,但是会被转化为成员国的国内法发挥效力。该公约规定,执法机关依法有权强制云服务商在成员国领土范围内、在其技术所及范围内采取相关专业技术手段收集和记录有关通信实时数据,以配合或者帮助执法机关的犯罪侦查行为。存取的数据通信包括从云端中下载的文件、由违法者接收或发送的电子邮件以及聊天记录。同时规定收集数据包括两种不同的方法,第一种方法通常要求云服务商安装一个接口,使执法机关能够用来直接访问云服务商的基础设施。第二种方法是使执法机关能够强制要求云服务商收集执法机关要求的数据。该公约同时要求缔约方通过立法以及采取其他措施要求云服务商对存取数据的过程以及相关信息进行保密。

此外,欧盟自成立以来一直积极致力于建立统一的欧洲电子商务市场,并制定了许多与密码相关的政策法规以为其成员国提供指导,促进其内部成员国间政策法规的互融互通。尤其是在政府数据存取过程中云服务商的协助解密义务方面,要求云服务商向执法机关提供其已加密的明文内容。公约设置了关于产品令状的规定,即任何一方应当遵循立法或其他措施,从而实现其主管机关被授权的必要令状,当事人应在主管机关管辖范围内提供其所拥有或控制的存储于计算机系统或计算机数据存储机制中的特定数据信息。同时,其解释性备忘录补充到"缔约国可以对当事人设立必须按照令状指定的形式提供指定计算机数据信息的义务"。因此,公约允许但并不强制其成员国建立解密令状制度。但是,其解释性备忘录也指出,加密技术原则上应被视为对隐私的合法保护措施,因此对于加密技术的应用应被视为是一种合法的权利,从而确立了加密技术在隐私保护中的法定地位。

欧盟还制定了相关法律保障政府数据存取的实施,例如欧盟电子隐私指令和数据存留指令对数据存留的目的、适用范围、数据存留的类别、数据存留的义务、数据存留的期限、存留数据的保护与销毁、存留数据的提供与罚则以及评估等方面做出了详细的规定。从数据存留的主体考虑,欧盟数据存留指令中所明确设定的义务主体是公开提供电子通信服务商或公共通信网络提供商,数据存留的目的是确保执法机关在调查、侦查和起诉各成员国国家立法中所定义的严重犯罪时能够提供相应数据。

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,不得包括内容数据。指令中还专门规定了存留数据的类别,而且各成员国需确保这些数据自流通之日起存留六个月以上,但最多不得超过两年。由于存留的数据涉及公民的隐私,若不慎外泄或被不当

① 但在一些例外情况下,比如在涉及死亡或对身体有严重的伤害危险的紧急情况时,云服务商可以按要求披露用户数据。

② 除非法官认为可能存在包含犯罪证据的数据,而且正常的调查程序已经不能获取证据或者获取证据的成本太大。

③ 即禁言令,该命令由法院下达,禁止涉案各方在公众场合谈论相关案情。

利用,将对公民隐私造成重大侵害,故指令专门规定,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上或政策上的措施,以避免存留的数据被意外或非法损毁,意外灭失或更改,或未经许可或非法存留、处理、获取或披露。而对于存留期限届满的数据,除非有特殊情况,否则应立即销毁。存留数据的机构须确保其存留的数据可随时配合执法机构的调查而提出,用以协助执法机构进行严重犯罪与恐怖嫌犯之调查时的参考利用。

在关于欧洲议会和理事会指令的提案中,欧盟主要关注执法机构为预防、调查、侦查或起诉刑事罪行或执行刑事处罚目的的个人数据保护,以及该数据在成员国之间的自由流动,确立了政府跨境存取数据的一般规定,该提案规定了数据在刑事领域的警察和司法合作中转移到第三国或国际组织的一般原则,澄清了跨境数据存取仅为必要的预防、调查、侦查或起诉刑事罪行或刑事处罚的执行之目的,并且应当为政府跨境数据存取的行为提供适当的保护措施,要求成员国应规定服务商需要按照执法机构的要求履行职责,特别是提供其所必需的数据。

(三)德国云环境下政府数据存取的法律实践

德国法律授权刑事检察官和监管机构通过法院命令存取第三方云服务器中的数据。但要获得法院的相关指令,政府必须证明有充足的理由相信所存取的数据是与刑事犯罪有关的。此外,如果云服务商提供类似通信服务的业务,根据德国电信法规定,为了起诉犯罪,维护公共安全和秩序,或履行政府职能,政府有权在未事先取得法院命令的情况下存取云用户的某些非内容性数据(例如电话号码、地址、出生年月等等),云服务商需要协助政府进行相关的数据存取,并被禁止向包括用户在内的第三方透露政府的数据存取活动。同时,德国数据保护机构可以要求存储在云服务商的服务器中的数据遵从数据保护法的规定,并被授权存取云服务商服务器中的数据,以审计和验证云服务商是否满足德国数据保护法的相关规定。

尽管德国政府机构能够基于刑事侦查或数据安全审计的目的存取云数据,但在一般情况下云服务商不能主动向政府机构披露数据。例如,根据德国电信法的规定,云服务商没有明确法定许可的情况下向政府披露用户数据将违反云服务商对用户数据的保密义务。云服务商在接受政府数据存取的要求后,应当尽快地通知用户,但不能影响刑事调查的目的。德国法律没有明确规定政府数据存取需要基于国家安全或反恐的目的,但考虑到在这些领域刑事犯罪的危害性,德国法院可能授予政府更多的自由裁量权以决定是否进行数据存取。

德国电信法和数据保护法对政府存取数据的规定可以涵盖位于国外的云服务商,但规定并不明确,且德国法院的数据存取命令原则上不适用于位于国外的云服务商,因此,德国政府在希望存取国外云服务商的数据时需要服务器所在国的司法协助。

三、我国云环境下政府数据存取的法律调整与完善

政府数据存取法律的调整与完善不能是盲目的,应当把握两个基本方向:一是在云环境下增强政府数据存取的有效性,满足国家安全与反恐之目的;二是平衡政府公权力与个人隐私之间的冲突,严格规范数据存取的适用条件。结合各国司法实践的经验,我国云环境下政府数据存取应当调整和完善以下事项。

(一)明确云环境下政府数据存取的适用条件

目前,我国尚未建立专门针对政府数据存取的程序性立法,相关规定散见于《宪法》、《国家安全法》、《人民警察法》、《刑事诉讼法》、《电信条例》、《互联网安全保护技术措施规定》、《人民检察院刑事诉讼规则》[224]等法律规范中,原则性规定了政府为犯罪侦查之目的进行数据存取的权力①,但相关数据存取的适用条

① 例如《刑事诉讼法》第一百一十六条规定,侦查机关的工作人员在犯罪侦查活动中如果需要扣押或者检查犯罪嫌疑人的通信内容(如邮件、电报等)时,应按照法定程序经公安机关或者人民检察院批准后才能实施。

件并不明确。

实践中,云环境下政府数据存取涉及存取机关、存取内容、存取程序、协助执法、隐私保护、信息安全义务等内容,权利义务关系十分复杂,政府机构通常对云服务商协助执法具有迫切需求,但缺乏相关法律的明确规定与授权,这使得政府机构要求云服务商提供数据存取协助的权力受到质疑。一般而言,国家安全机关和公安机关在犯罪案件的侦查活动中对公民通信进行秘密侦查的权力依据主要来源于《国家安全法》和《人民警察法》。前者在其第十条中明确规定国家安全机关在基于国家安全保护的需要时,依照有关规定经过严格程序批准后,可采取技术侦查措施,但该"有关规定"具体包括哪些法律规范,以及严格程序如何规定并没有进行说明。后者在第十六条中规定,公安机关因侦查犯罪的需要,在依照有关规定经严格程序审批后,方可进行技术侦查,但是其尚未明确规定审批程序的实质内容,因此在实践中缺乏可操作性与实用性。

从功能上看,明确政府数据存取的适用条件能够抑制行为的随意性,适用条件对恣意的限制就是通过程序中的时空因素来防止和克服行为的人格化[10]338。适用范围的缺位将导致法律缺乏可操作性,监管机关的权限不明,使得政府存取云端数据的实体性工作缺乏有效的规范和监督。在某些情况下,如果诉讼双方的利益博弈失衡,政府机构及其工作人员滥用权力的可能性加大,最终将极大影响政府执法工作的公信力和公平性。

云计算政府数据存取与云服务商的合法权益和用户的个人隐私息息相关,其适用条件应当以法律的形式予以确定。在审查案件是否需要进行政府数据存取时,必须审查其是否符合法律规定的适用条件,避免政府通过数据挖掘不加区分地存取相关数据。政府数据存取的适用条件应当包括: 第一,适用的案件性质具有严重的危害性,比如危害到国家安全和社会稳定等; 第二,除实施政府数据存取以外,没有其他方式能够查明案情、侦破案件,或者即使有其他方式,但须耗费大量的人力、物力和时间,并可能对个人利益及公共利益造成更大的损害。

纵观各国相关的法律规定,通常对可适用政府数据存取的案件类型进行了较为细致的划分。结合我国国情,我国可以采用罪名列举法与罪行轻重限定法相结合的方法划定政府可以进行数据存取的范围。首先,在犯罪类型的适用方面对于具有重大危害性的罪名进行列举,将危害国家安全的犯罪、黑社会性质犯罪、有组织犯罪、恐怖犯罪、跨国犯罪这五类犯罪明确规定在适用政府数据存取的范围内。其次,从罪行轻重来看,除了上述五类特定犯罪以外,对于法定刑在十年以上的有期徒刑、无期徒刑和死刑的犯罪案件,犯罪行为达到一定的严重程度也可以通过申请审批程序适用政府数据存取法律制度。对于何为"一定的严重程度"则应视具体情况而定。2012 年通过的《刑诉法修正案》中明确将危害国家安全犯罪等四类罪行以及严重的职务犯罪纳入技术侦查的范围,这种诉讼法的立法模式对于我国现阶段的国情来说是必要可行的。但是从长远来看,我国应以专门法的形式对政府数据存取的适用条件进行具体规制。此外,《刑诉法修正案》在适用范围上采用的是罪名列举法,这种标准存在一定的缺陷,对于新出现的严重犯罪具有严重的滞后性,因而在专门立法时还应将罪名列举法与罪行轻重限定法相结合。

(二) 明确云服务商的协助执法义务

目前,我国立法初步明确了云服务商的协助执法义务,在相关法律规范中确定了数据存留和保密等义务要求。例如,《互联网安全保护技术措施规定》针对互联网接入服务单位、互联网信息服务单位、互联网数据中心服务单位和互联网上网服务单位规定了落实系统运行和用户上网登录时间和网络地址等数据记录存留的技术措施要求。《计算机信息网络国际联网安全保护管理办法》规定,从事国际联网业务的单位和个人应当接受公安机关的安全监督、检查和指导,如实向公安机关提供有关安全保护的信息、资料及数据文件,协助公安机关查处通过国际联网的计算机信息网络的违法犯罪行为。《互联网信息服务管理办法》、《互联网电子公告服务管理规定》以及《互联网电子邮件服务管理办法》分别对互联网信息服务提供者、互联

网接入服务提供者、电子公告服务提供者和互联网电子邮件服务提供者应当存留的通信信息进行了规定。《保守国家秘密法》规定互联网及其他公共信息网络运营商、服务商应当配合公安机关、国家安全机关、检察机关对涉密案件进行调查,并负有立即停止传输,数据存留,报告及删除涉密信息的义务。

虽然政府机构已充分认识到现代通信技术发展的复杂程度和数据存取的困难程度,纷纷对网络服务商提出了相应的协助存取要求。但是,服务商的协助存取义务究竟包括哪些具体内容,相关法律法规中并未做出明确且细化的规定,无法对云服务商协助政府进行数据存取提供明确的法律指引。云计算本身所具有的特殊性使得政府数据存取变得更加困难,这为立法上进一步明确和细化云服务商的协助执法义务提出了更高的要求。具体而言,我国应当在相关立法中对云服务商的协助执法义务予以明确,具体的义务内容应当包括协助存留数据义务、协助解密数据义务、信息保密义务等。

1. 协助存留数据义务

数据存留的目的是为了维护国家安全,或者为了预防或侦查犯罪或起诉可能与国家安全有直接或间接关系的犯罪。在云服务中,政府进行数据存取可能不是实时的,云服务商仅仅提供访问特权是不够的,需要对特定数据进行存留以满足政府数据存取的要求。我国应当明确云服务商进行数据存留的义务,并且强调云服务商对存留数据负有安全保障的义务,因为只有保证存留数据的真实性和完整性,才能确保该数据具有可用性。为此,云服务商必须确保存留数据的质量、安全和保护等级,应当采取适当的技术措施和组织措施保护数据安全,以避免数据被意外或非法毁损、灭失或更改,未经授权不得非法储存、处理、获取、披露数据。除了合法访问和保存数据外,云服务商必须在存留期限届满后完全销毁存留的数据,使这些数据不能再被访问[11]。

2. 协助解密数据义务

为了便利执法,各国立法一般要求政府存取的数据应当是明文的,因此云服务商需要负有协助解密数据的义务。在司法实践中,存在两种协助解密的原则,其一是“谁运营,谁解密”原则,即云服务商应负责对其运营业务过程中所涉及的所有加密信息和数据进行解密。但是,在涉及跨国的多方加密主体时,云服务商很难具有所有加密文件的解密能力。其二是“谁加密,谁解密”原则,即政府执法部门只要求云服务商对提供加密信息或加密资源的部分进行解密,这种方法看似会使解密过程变得更为烦琐、复杂,但在应对多方高强度加密信息和数据的解密时,反而会以较高的效率实现政府数据存取的目标,因此“谁加密,谁解密”的解密原则更符合云计算的特征,应当为我国立法所采用。

3. 信息保密义务

从云用户角度而言,政府数据存取的本质是第三方访问及获取用户数据的过程,在这一过程中可能存在数据泄露的风险。基于云服务商对用户数据的保密义务,应当在政府提供合法证明和授权的前提下才能协助存取数据,并不得披露不必要的用户信息。从政府角度而言,云服务商在协助政府数据存取执法的过程中可能了解到执法机关对案件的侦破情况,各国法律普遍规定云服务商对通过协助执法获取的案件调查与进展情况不得向包括用户在内的第三方披露。因此,云服务商还须承担对案件内容的保密义务。同时,尽管云服务商为保障用户的知情权可以将协助执法进行数据存取的情况告知用户,但是如果该告知可能影响案件的调查与侦破,该告知是不能进行的,云服务商需要对协助执法的情况保密。

(三) 加大对协助义务主体的补偿

我国目前对于云服务商的协助执法义务属于强制性要求,主要表现在强制性地满足法定协助能力的要求,如果云服务商拒绝协助政府数据存取,很可能因违反强制性规定而承担不利的法律后果。但云服务商在满足协助执法要求的同时,可能在云服务过程中引入安全风险。具体而言,云服务商为满足协助政府数据存取要求所负担的成本较高,包括审计日志、数据备份、数据存留副本在内的证据材料都需要隔离

存储,并保证只有经授权的人员才能接触; 为保证容灾能力,这些数据通常需要在距离足够远的数据中心分别保存; 为满足审计和溯源的要求,云服务商在基础设施方面的投入也非常巨大[12]。但是,在我国,云服务商协助政府数据存取目前还无法获得相应的补偿,这对于云服务商而言,无疑将增加额外的经营负担。更为重要的是,云服务赖以生存和发展的基础是用户信任,因信任危机而导致的业务链断裂可能对云服务产生毁灭性的影响。云服务商履行协助政府数据存取义务在一定程度上将引发与用户个人隐私之间的冲突,这必然会对个人隐私和信息安全保护的现有秩序带来巨大的冲击,对云服务商的商业信誉产生负面影响,导致云服务商的用户大量流失。缺乏有效的协助执法补偿制度将在很大程度上制约云计算产业在我国的发展。

从产业发展的角度考虑,大多数国家都在其政府数据存取法律制度体系内建立了协助义务主体的权利救济制度,以保障云服务商履行协助执法义务享有一定的权利救济途径和法定依据。具体而言,尽管云服务商负有协助实施政府数据存取的法定义务,但是其对于执法机关做出的协助执法要求中的不合理之处仍然享有法定的申诉权利。因此,云服务商作为协助义务主体对于执法机关不合理的协助执法要求,有权向做出协助执法要求的执法机关或其上级机关提出申诉,以保障企业自身的发展权益。此外,云服务商为配合政府对云端数据进行存留而安装或配置相关设备、设施及对其服务进行调整的任何合理费用,应当有权要求政府给予支付或补偿。但是,云服务商要求支付的费用必须是合理的,且与政府进行数据存取的执法活动直接相关。

(四) 完善监督及侵权救济措施

实践证明,云环境下的政府数据存取将对公民隐私、通信自由等宪法性基本权利产生负面影响,如果政府机构滥用公权力,违反法律规定实施数据存取,甚至任意进行披露,用户数据的完整性、保密性和可用性将受到严重损害,缺乏充分的监督及侵权救济将导致相对人的合法权益无法得到保护。特别是在政府通过数据存取进行大规模数据挖掘的情况下,政府获取的数据能够更为容易的指向特定的个人,对于用户隐私的侵犯可能构成政府侵权行为的基本方式。根据权责统一和依法行政的实质性要求,政府存取云数据作为国家执法机关的行为,必须合理厘定对其侵权行为的监督和救济措施,督促执法机关及时纠正违法行为,弥补对执法对象合法权益所造成的损害,这一措施能够更大程度地获得私权利主体的理解和支持,提高政府数据存取的工作效率,这也是依法保障人权和构建法治社会的深层次需求。

我国目前的立法对政府数据存取的规定鲜有涉及,执法实践通常依据一些行政部门的内部文件,加之执法机关的执法行为只受内部监督,因而政府机构实施数据存取很可能无法得到有效限制与约束。尽管《刑诉法修正案》将技术侦查措施的执行机关限定为公安机关,取消了国家安全机关与人民检察院的执行主体资格。但是,其并没有明确规定由哪个机关进行审批与授权,因而并没有改变内部审批制的实质。这种内部审批制缺乏有效的外部监督,使得政府数据存取行为多由政府机构的负责人自行决定,而这种内部自我监督机制形同虚设,无法真正约束其行为,极易导致公权力的滥用[13] 318 - 319。

我国之所以缺乏有效的监督机制,盖因于我国长期存在司法行政化的严重问题。在缺乏相关法律法规的情况下,对于执法机关行为的监督,主要采取的是自我监督方式,属于行政手段而非法律手段,其主要是通过制定行政规章、下发行政文件等方式规范和调整政府数据存取的相关活动。这种调整方式随意性很强,很难实现对政府数据存取行为的真正监督与制约,极易导致侵权行为的发生。为此,政府数据存取的监督应当紧紧围绕比例原则,在国家利益、企业利益以及公民个人利益之间取得最佳平衡。按照比例原则的要求,政府在存取云数据时必须满足基本条件,即数据存取应当在用尽常规措施的情况下才能够予以实施,对云服务商和用户合法权益造成的损害必须与所保护的

利益相适应。结合我国的审判机构体系,人民法院应当作为政府存取云数据的授权机关,是法定的监督机关,负责对云数据存取授权令状的签发、存取数据的事后审查等方面进行监督,在发现政府执法机关的侵权行为时应当及时责令执法机关改正,甚至可以撤销授权存取云数据。

但是,即使能够有效进行监督,权力滥用的问题依然不能得到根除,在用户与云服务商的合法利益因政府数据存取而遭受侵害时,相应的救济措施是必须予以明确的。在具体立法设计中,首先应当设立明确的救济条件以及追究责任的形式。其次是要有明确的救济渠道。再次是确立科学的救济程序,将实体公正与程序公正相结合,同时保证执法效率,保证救济的及时性。最后是建立完善的相关救济规则,明确因政府获取云数据而造成的侵权损害可以获得赔偿,并列明赔偿额度。

四、结 语

政府数据存取法律制度是一国政府有效实施调查权的必要保障,为了刑事侦查与反恐之目的,各国立法普遍赋予本国政府进行数据存取的权力。云计算技术的全球化繁荣为政府基于国家安全和反恐进行数据存取提供了更为便利的机会,但也由于自身的技术特性客观上为政府数据存取设置了障碍。由于用户对云服务有较高的隐私期待,云服务商也负有更为严格的数据安全保护义务,因此用户和云服务商将更为关注政府数据存取所引发的数据安全危机。在云环境下,政府数据存取所面临的最大法律困境在于,如何在促进执法效率的同时防范政府"越界"进行数据挖掘所产生的隐私侵犯,这需要解决诸多基本问题,如政府数据存取可获得的数据范围;在非正式要求之下,云服务商是否可以主动向政府披露数据;用户享有怎样的知情权;政府存取用户数据是否需要法官审查;政府是否有权存取境外的数据等等。我国在相关领域的立法仍然缺乏有效的规定,亟待明确政府数据存取的适用条件,规定可获取的数据"边界",细化云服务商的协助执法义务和相应的补偿机制,建立监督和侵权救济制度。

[参考文献]

[1] Francoise Gilbert. Demystifying the Patriot Act: Cloud Computing Impact [J]. Tech Target, 2012, (5).

[2] Winston Maxwell, Christopher Wolf. A Global Reality: Governmental Access to Data in the Cloud [R/OL]. [2013 - 01 - 29]. http://www.cil.cnrs.fr/CIL/IMG/pdf/Hogan_Lovells_White_Paper_Government_Access_to_Cloud_Data_Paper_1_.pdf.

[3] 蒋洁. 云数据隐私侵权风险与矫正策略 [J]. 情报杂志,2012,(7).

[4] 庞德. 通过法律的社会控制 [M]. 北京: 商务印书馆,1984.

[5] 邓仲华,朱秀芹. 云计算环境下的隐私权保护初探 [J]. 图书与情报,2010,(4).

[6] 史本懿,林举琛. 全球信息保密管理: 在网络环境下的跨境信息流 [J]. 黄义也,译. 科技与法律,2010,(5).

[7] Scott M. Fulton. EU's Reding to Cloud Providers: Stop Sheltering Yourself from US Patriot Act [R/OL]. [2012 - 03 - 02]. http://www.readwriteweb.com/cloud/2011/12/eus-reding-to-cloudproviders.php.

[8] Kromann Reumert. Government Access to Information in "The Cloud" [R/OL]. [2013 - 03 - 06]. http://www.kromannreumert.com/en-UK/Publications/Articles/Documents/Government%20access%20to%20information%20in%20the%20cloud.pdf.

[9] 马民虎. 网络信息安全保障的法律监管研究 [M]. 西安: 陕西科学技术出版社,2007.

[10] 张文显. 法理学 [M]. 北京: 高等教育出版社,2003.

[11] UK Data Retention Requirements Information Data Retention and Disposal [R/OL]. [2009 - 01 - 08]. https://www.watsonhall.com/resources/downloads/paper-uk-data-retention-requirements.pdf.

[12] 中国云计算安全政策与法律蓝皮书 [R]. 西安: 云计算安全政策与法律工作组,2012.

[13] 曹卫. 秘密侦查的实施主体 [J]. 中国商界,2010,(2).

[责任编辑 李晶晶 责任校对 王治国]