doi:10.11835/j.issn.1008-5831.2017.01.012

欢迎按以下格式引用:齐爱民,祝高峰. 论云存储中数据安全的法律保护[J]. 重庆大学学报(社会科学版),2017(1):101-108.

Citation Format: QI Aimin, ZHU Gaofeng. Legal protection of data security in cloud storage[J]. Journal of Chongqing University(Social Science Edition),2017(1):101-108.

论云存储中数据安全的法律保护

齐爱民,祝高峰

(重庆大学 法学院,重庆 400044)

摘要:云存储是云计算的演变形式,云存储与云计算既有联系又有区别。云存储是指借助网络(尤其是Internet),运用应用软件,为用户提供数据存储及访问功能的一个软硬件结合的数据集合系统。云存储本身并不是一种服务,它是为了实现数据存储服务功能而提供的一个系统支撑。云服务器位置的不确定性导致云存储中数据位置多变。云存储中的数据安全及隐私安全问题给数据用户提出了严峻的挑战。云存储中数据安全主要是指数据的采集、存储、访问、处理及数据交易安全。云存储中的数据安全与网络安全息息相关,数据安全的法律保护亟需制定。

关键词:云存储;数据安全;网络安全;法律保护

中图分类号:D922.8 **文献标志码**:A **文章编号**:1008-5831(2017)01-0101-08

数据安全将成为云存储发展前进道路上的"拦路虎"。互联网已经融入社会生活的各个领域,随着网络科技的迅猛发展,"云端"更是让人们难以认知,随之而来的网络安全问题、数据存储安全问题、数据访问安全问题、数据处理安全问题及数据交易安全问题亟需有效的法律规制。数据资源的跨地域存储与数据的本地化监管之间的矛盾不可避免。云存储中数据安全问题的有效规制,不仅影响到网络安全及数据安全的稳定运行,甚至会影响到国家数据安全及国家数据主权安全。

一、云存储的概念、特征及其架构模式

(一)云存储的概念

云存储与云计算的概念既有联系又有区别。一般认为,云计算(Cloud Computing)是一种新兴的共享基础架构的方法,是此前 IT 领域几项重要理念与技术——分布式处理(Distributed Computing)、并行处理(Parallel Computing)和网格计算(Grid Computing)的发展,或者说是一种商业化的实现[1]。国外学者克里斯托弗·米勒德(Christopher Millard)在其著作《云计算法》(*Cloud computing law*)中将云计算定义为:"云计算就是一种通过网络尤其是通过因特网,提供公共服务计算资源的一种方式,而这种公共服务方式可以根据用户的需求向上下扩展。"[2]虽然研究者各自对云计算的定义有不同的看法,但对于其是一种高速的计算处理方式,可以为云服务提供支撑是肯定的,云计算可以理解为云的初始发展阶段状态,而云存储则是在云计算基础上的延伸,理应对其概念有新的认识及解释。

国内有研究者认为:"云存储即云计算的资源存储,它是一个由网络设备、存储设备、服务器、应用软件

修回日期:2016-11-24

基金项目:国家社会科学基金重大项目"国家网络空间安全法律保障机制研究"(13&ZD181)

作者简介:齐爱民(1970-),男,河北冀州人,重庆大学法学院教授,博士,博士研究生导师,主要从事网络信息法与知识产权法研究,1309978103@qq.com;祝高峰(1978-),男,山东潍坊人,重庆大学法学院博士研究生,主要从事网络信息法与知识产权法研究。

等多个部分组成的通过应用软件来对外提供数据存储和业务访问的服务。”[3]维基百科给云存储的定义是:“云存储是一种将数据资源存储于逻辑池中的数据存储模式,而物理环境中的数据存储跨越多个服务器(通常是多处位置),并且通常由托管公司拥有和管理,云存储服务可以通过共同位置的云计算机服务来访问。”[4]可见学者和各研究部门对云存储的定义界定也不尽相同。

从对云存储的界定不难看出,有学者试图用所有与云储存有关的内容来进行定义,我们应当看到,云存储的定义与云存储的内容及组成结构有着本质的区别,笔者在界定云存储的定义时,分析了云存储的自身性质、云存储的特征及云存储的组成结构,将云存储定义为:云存储是借助网络(尤其是Internet),运用应用软件,为用户提供数据存储及访问功能的一个软硬件结合的数据集合系统。云存储本身并不是一种服务,它是为了实现数据存储服务功能的一个系统支撑,云存储中真正提供服务的是基础管理层的数据管控者和应用接口层的云存储服务提供商。云存储的运行起决定作用的仍是应用软件,软件必将定义未来。

(二)云存储的特征

为了有效规制云存储中的数据安全,有必要对云存储的特征作进一步分析,在掌握其特征的同时从其特征着手进行有效的规制,势必起到事半功倍的效果。

虚拟性。虚拟性是云存储的显著特征之一,云存储体现为虚拟存储,有别于通过传统物理设备的存储。借助于互联网,云存储中的数据资源是虚拟化的资源,也可以说是代码“0”和“1”的集合,在云存储中都是无形的。因此云存储的典型特征就是其有虚拟性的一面。云存储展现了其既在实现了数据存储的同时又实现了数据资源的共享特性,实现存储完全虚拟化。对于终端用户来讲,只要在可以连入互联网的任何地方,有权访问的终端用户,都能够借助云存储提供的支撑系统,实现其对网络空间数据资源的访问。

灵活性。云存储的灵活性不仅体现在存储协议方面的灵活上,更多地体现在云存储的网络空间扩展能力以及云存储性能扩展的能力和容量上,云存储的实现主要通过应用软件来发挥作用。区别于传统的固定设备存储,云存储不仅仅是存储,更多的是应用。云存储对于终端用户来说,通过网络,终端用户可以在任意云端提取及存储数据。

高效易用性。云存储通过其特有的架构系统,在云存储的环境中,可以拓展数据存储的空间和能力,提高数据资源的传输效率,以达到减低成本,实现整个数据资源的高效利用率。因此,数据能够在移动或者是迁移应用中,仍具有高效的易用性,不受影响。

国际商用机器公司IBM(International Business Machines Corporation)认为云存储可以提供四种类型的存储:(1)个人存储(Personal Storage),能够存储个人数据并在多个设备上同步使用;(2)公共存储(Public Storage),云存储服务提供者完全可以异地管理企业的数据;(3)专用存储(Private Storage),云存储服务提供者在一个有组织的数据中心为客户端服务;(4)混合存储(Hybrid Storage),公共存储和专用存储的混合[5]。笔者简单言之,个人存储就是个人数据存储的服务,公共存储主要是为了实现数据存储的共享,提高效率、降低成本,专用存储则是一种专属服务,混合存储就是公共存储服务与专属存储服务的混合。在笔者看来,云存储中的数据可以被划分为不同种类,但是从其保护的实质看,都是数据自身安全,只是有些数据涉及个人数据信息,有些涉及商业数据信息,有些涉及国家安全数据信息罢了,终归都是存储于网络空间的数据,对不同性质的数据采取不同程度的保护也是对数据更加有效保护的需要。

通过互联网,用户在应用数据时,不需要了解到底使用什么硬件、有多少交换机及路由器,只要接入互联网端口,有用户名和密码上网就可以,云存储之所以具有商业价值且日益受到青睐,也是源自其自有的特征。

(三)云存储的架构模式

对云存储的架构模式进行分析,有助于清晰明确地认知云存储的运行,只有掌握了云存储的运行模式,才能实现保护云存储中的数据安全。

通说认为云存储系统的架构模式包括四个部分:存储层、基础管理层、应用接口层、访问层。存储层是

云存储的基础部分。基础管理层是云存储最核心的部分。应用接口层即不同的云存储服务提供商可提供不同的应用服务。访问层也就是云存储系统的用户[6]。笔者将云存储的架构模式做一个初步解析,云存储的访问层即用户,即,云存储的应用接口层即云存储服务的提供商,云存储的基础管理层即云存储数据的实际管理者,云存储层即数据存储的所在地。笔者认为,无论在云存储架构模式的哪个层面,都离不开应用软件。因此,对应用软件的规制对于云存储的数据安全至关重要,同时在云存储的运行安全中,云存储服务提供商的责任及义务和云存储的管理者对数据的管控行为也都直接影响着云存储中的数据安全,所以有必要对其两者的责任及权利义务进行明确的规制。

笔者认为云存储本身并不是一种服务,真正提供服务的是基础管理层的数据管控者和应用接口层的云存储服务提供商,但是两者面向的对象却大相径庭,管理层的管控者主要是面向存储层的数据安全和应用接口层的云存储服务商,而云存储服务商虽然也面向管理层的管控者,但是更多的是面向访问层的终端用户。离开了应用软件,讨论云存储不切实际。云存储是一个包含了综合数据库的软件应用系统。

二、云存储中的数据安全危机

在大数据时代,对云存储中的数据安全进行有效的法律规制具有重要的现实紧迫意义,云存储中的数据应用、存储、访问、处理及交易已逐步渗透到各行各业,云存储在给人们的生活带来便利的同时,也使数据安全问题面临着现实的冲击及威胁,云存储中的数据安全问题不仅影响到用户对云存储中数据安全的应用,也会对网络安全运行等各方面带来冲击。因此,分析云存储中影响数据安全存在的主要因素,维护云存储中数据安全,对其进行行之有效的法律规制刻不容缓。

(一)云端数据自身特征危及数据安全

云端的数据存储是一个虚拟存储,数据经过采集、处理之后上传到云端存储,然而数据一旦传输到了云端,基本上对用户来说就丧失了对数据的绝对控制权,云存储中的数据将面临着易丢失和泄露的风险。

数据易丢失。云存储是网络技术应用与软件应用的一个综合体系,人们在享受云存储便利的同时,也要承受其带来的风险。在云存储中,数据的存储、传输、访问、处理以及复制和迁移等方面都变得更加便捷和频繁,同时也容易导致云存储中的数据丢失。云存储的服务提供者一直在努力寻求对策以保证终端用户和云存储中的数据安全,但现实中,终端用户遭受数据泄露和丢失风险的情况仍时有发生。如果云存储中数据应用安全不能得到有效规制,那么数据用户对使用云存储系统存储数据将会更加担忧。

数据易泄露。由于互联网的开放性、即时性及跨界流动性等自身特征,加之许多存储在云中的网络数据信息比较敏感,涉及公民个人身份信息、隐私、商业数据信息甚至是国家安全数据信息等,这些数据一旦被用心不良的人所掌控,就会造成严重后果。现今仅仅从数据加密技术上来保护云存储中的数据安全,显然对于当下日新月异的技术来讲,防止数据泄露的风险已显得捉襟见肘。2011 年 3 月,Google 的 Gmail 电子邮箱爆发大规模用户数据泄露事件,近 15 万 Gmail 用户在周日早上发现自己的所有邮箱和聊天记录被删除,部分用户的账户被重置而无法登陆[7]。可见数据信息泄露时有发生,云存储中的数据遗失和泄露既有技术上的原因,也有具体保护制度不完善的原因。因此,对于云存储中数据安全的保护立法已是箭在弦上。

(二)缺乏对云存储服务提供商的责任及义务规制

处于云存储应用接口层的云服务提供商,对云存储中的数据保护责任及应尽义务程度将直接影响云存储中的数据安全。云存储服务提供商扮演的是超级用户角色,一定程度上掌控着攫取大量数据资源必经之门的“金钥匙”。某些数据其本身可能包含恐怖主义和煽动国家分裂以及颠覆国家政权等不法有害信息,如果云存储服务提供商不能尽到应有的数据保护义务和责任,而放任或默认该不法有害信息任意传播,那么此时数据安全不仅会影响国家数据安全、网络运行安全,还有可能影响到社会稳定和国家安全。比如 2009 年爆发在中东伊朗的“Twitter 革命”(也称茉莉花革命)就使伊朗的政治格局发生了改变,其主要原因之一就是对数据信息的传播缺乏管控。因此,现阶段明确规制云存储服务提供商的责任及义务,对保障云存储中的数据安全乃至国家安全责无旁贷。

(三)数据终端用户引致的数据安全风险

终端用户处在云存储系统中的访问层,也可以说是云存储中的顶端,云存储中访问层的数据安全与终端用户有着直接的联系。互联网时代,终端用户既是网络数据的制造者,又是网络数据的参与者,云存储的益处就是可以将终端用户的数据信息资源同步存储和共享。因此,对于终端用户在对数据进行存储、应用、传播、删除等行为时,应当明确终端用户应尽的权利及义务。网络数据无论怎样虚拟无形,怎样无具体物理位置,其要发挥作用必然离不开人的行为,否则网络数据即使能够存储在网络空间,也不过仅仅是"僵尸数据"。目前中国终端用户普遍都缺乏必要的网络安全意识,用户要进行数据存储始终要通过终端服务,而终端用户在获取云存储中的数据时也依然需要依靠终端设备,在终端设备上输入数据用户名和密码,登录某一个云存储去下载或上传存储于云端的数据。一旦终端用户账号和密码被泄露或者是被木马等病毒侵入,那么在云存储中的数据会在终端用户毫不知情的情况下,被恶意人随意存储、删除、传输。因此,对于数据终端用户的数据使用行为进行有效规制,从"源头"上解决对云存储数据安全的法律保护问题非常必要。

(四)应用软件缺乏统一的安全认证标准

云存储的应用其核心之一就是应用软件。云存储不只是存储,更多的是应用。应用软件将直接影响云存储的运行,对云存储中的数据采集、处理、挖掘等方面起着不可替代的作用。然而目前因对应用软件缺乏有效的法律规制,已导致数据在通过应用软件存储时,很容易造成用户数据的泄露及丢失,因此应当对应用软件安全认证实行统一认证标准,禁止在设计应用软件时使其存在某些自动收集用户数据信息、自动收集与用户数据信息相近及相关的数据信息行为,禁止其带有某些不法入侵程序设置。从目前的发展趋势看,软件应用已普遍渗透到各个领域,日后必将出现"软件定义一切"的局面,因此对应用软件进行必要的法律规制,是治理云存储中数据安全有效保障的根本。

三、欧美云存储数据安全保护的法律制度

各国都不同程度地面临着云存储中数据安全的挑战。各国对数据安全的立法保护主要从两个方面着手:一是数据信息资源的利用,包括商业信息、公共信息及政务信息;二是注重个人数据安全的保护。当下,各国都面临着云存储中数据安全问题的严峻挑战,从事云安全问题研究的组织不少,但只有个别组织机构和有代表性的国际大公司(微软、亚马逊等)取得了一些初步研究成果,具体到云存储安全方面问题的研究则主要是 CSA①(Cloud Security Alliance,云安全联盟)和 ENISA②(European Network and Information Security Agency,欧洲网络和信息安全研究所)两个机构,其研究最具代表性,对云存储的数据安全关注较多,取得了一定成绩。

虽然各国都通过了部分数据保护法,保护本国的国家数据安全,但是我们应当看到,美国仍是信息技术最发达的国家,根服务器包括主根服务器大多数仍在美国,美国汉姆林大学法学院教授莎朗 . K. 桑迪恩(Sharon K. Sandeen)在论及云计算时认为"在过去的十几年里,云计算已经从一个优雅而被误解的术语进入到一个蓬勃发展的行业,在其进入的计算机行业、互联网行业和电信行业中都是非常著名的大公司,包括 IBM、微软、谷歌、Amazon、戴尔和 Verizon"[8]。伴随着云计算产业的不断演进,将会出现更多的新产品和新服务。我们清晰地看到,云计算的应用基本上都被国外大公司所控制和垄断,目前要想真正实现云存储中的数据安全,中国在数据保护方面仍有很长的路要走。

①CSA 成立于 2009 年,作为一个非盈利性组织,其宗旨是"促进云计算安全技术的最佳实践应用,并提供云计算的使用培训,帮助保护其他形式的计算"。自成立始,CSA 迅速获得了业界的广泛认可,其企业成员涵盖了国际领先的电信运营商、IT 和网络设备厂商、网络安全厂商、云计算提供商等。云安全联盟确定了云安全的 15 个焦点领域,对每个领域给出了具体建议,并从中选取较为重要的若干领域着手标准的制定,在制定过程中,广泛咨询 IT 人员的意见,获取关于需求方案说明书的建议。参见冯登国《云计算安全研究》(《软件学报》,2011 年第 1 期第 76 页)。

②ENISA 是负责欧盟内部各个国家网络与信息安全的研究机构,负责为欧盟内各个国家的网络与信息安全问题提出建议,指导安全方面的实践活动。该机构主要是从企业数据安全角度出发进行研究。参见张健《全球云计算安全研究综述》(《电信网技术》,2010 年第 9 期第 15 - 17 页)。

(一)英美国家保护数据存储安全的网络安全基本法

美国为了在国家层面加强其对网络数据信息的控制,同时又为其对网络安全信息共享的监管提供法律依据,2014 年通过了《国家网络安全保护法》。在此之前美国为了维护其国家数据安全,通过的《爱国者法案》(2001 年)赋予了执法机关过于宽泛的信息调查与获取权利。对窃取以及非法利用政府部门数据信息行为的处罚规定则主要体现在英国《计算机滥用法》(1990 年)和美国《计算机欺诈和滥用法》(1986 年)。美国《反窃听法》和《电信法》(1996 年)加强了对在个人数据安全方面的保护,重点对在数据信息传输过程中,窃取个人数据的行为和非法拦截的行为进行了限制[9]。

(二)欧盟加强对云存储数据的同等保护原则

欧盟成员国为了加强对个人数据安全的保护,明确了个人数据保护的基本原则,制定了各自的个人数据保护法,并在对个人数据的留存、处理、使用等方面都作了相应规定。欧盟的数据保护法规定,欧盟公民的个人数据在非欧盟国家传输必须贯彻同等保护原则,即接受国必须提供和欧盟保护水准相一致的保护才能传输欧盟公民个人数据,能够提供同等保护之前不能传输至非欧盟国家。由于"斯诺登"事件的影响,欧盟认为存储于美国服务器上的数据信息并非真正意义上的"安全港"。因此,2015 年欧洲法院废除了欧美于 2000 年签署的允许网络运营商忽略欧盟各国法规差异而自动合法传输网络数据的《安全港协议》。美国 Google、Facebook 等众多科技公司应立即停止将收集到的欧洲用户数据传输至美国[10]。

为了加强欧盟民众的网络安全意识,保护和繁荣欧洲数字经济,2013 年由欧洲网络与信息安全局(ENISA)和欧洲委员会共同举办的欧洲"网络安全月"③活动正式启动。这一点非常值得中国借鉴和学习。因为中国网民很大一部分将网络信息视为"游戏",缺乏基本的网络安全意识。建议中国积极策划在各个相关主要领域开展类似的全民网络安全宣传教育活动。

(三)俄罗斯对云存储数据保护的本地化要求

俄罗斯可谓是对云存储的数据保护作出了大胆创新及尝试。俄罗斯《个人数据保护法》于 2015 年 9 月 1 日生效,该项法律明确规定俄罗斯公民的个人数据只能存储于俄罗斯境内的服务器中,以实现数据存储本地化。"斯诺登"事件以来,各国都非常关注本国公民个人数据安全及国家数据安全。该项法律并未禁止公民数据的跨境传输,只要求让数据存储于俄罗斯本地。该法律通过后,全球购物网站巨头易趣公司和苹果公司也积极响应数据存储本地化。但是有些公司,比如社交网络公司 Facebook 以及全球音乐流媒体服务巨头 Spotify 在内的少数公司,则提出反对意见[11]。俄罗斯新立法的目的非常明确,该项立法旨在维护其本国公民的数据存储安全和国家数据存储安全。

四、构建云存储数据安全的法律保护制度

云存储中的数据安全问题日益凸显,然而对云存储的数据安全问题进行有效的规制仍未得到解决,中国对云存储的数据安全保护缺乏相对明确的法律法规,现有对云存储数据安全的法律保护制度也较模糊。笔者认为,应当在分析中国目前相关网络法律法规基础上,结合云存储的实际架构运行系统,构建中国对云存储数据安全的法律保护制度。

(一)中国对云存储数据安全的法律保护现状

从中国先前有关保护网络数据信息的法律法规看,对于网络数据的存储安全基本都未有明确规定,包括对于一些基本概念也未有明确界定,大都是针对计算机系统的保护,而对于急切需要规制的云存储中的数据安全基本都未涉及。令人欣慰的是,近几年对网络信息安全立法的工作一直在稳步快速地推进,且已

③该活动以"在线安全需要你的参与(Online security requires your participation)"为主题,吸纳私营部门和企业界的参与。其中,欧盟 27 个成员国都参与其中。欧洲网络安全月采取的宣传活动形式多样,包括举办会议、论坛和演讲,通过电台和电视节目、在线游戏和在线交易等渠道进行宣传。自 2014 年以来更是开展了对专业技术人员进行网络安全演练、针对在校学生举行代码编程等主题活动以及针对公共和私营组织进行员工培训、针对所有网络用户开展计算机和移动保护以及隐私保护的宣传。欧洲网络安全月旨在提升公众网络安全意识,改变公众对网络威胁的理解,同时通过教育和共享最佳实践等方式为公众提供最新的安全信息。参见《欧洲网络安全月:推动所有用户更安全使用互联网》(http://world.huanqiu.com/article/2014-11/5212674.html,2016-09-26 访问)。

取得部分成效,在《关于加强网络信息保护的决定》④中明确强调了“网络服务提供者和其他企业事业单位在业务活动中收集、使用公民个人电子信息时的基本义务”。在《中华人民共和国刑法修正案(九)》⑤(以下简称《刑法修正案(九)》)中明确了:“在违反国家有关规定时,向他人出售或者提供公民个人信息,情节严重的可以入刑,同时也明确了网络服务提供者的法律责任”。至此,我们看到法律对保护网络数据和个人信息的工作向前迈进了一大步。明确维护网络空间主权、保护网络数据安全,阐明网络、网络安全、网络数据、公民个人信息、网络运营者等基本概念是中国《网络安全法》的基本要求及内容。

(二)云存储数据安全法律保护制度之构建

规制云存储中的数据安全,应当采用“源”与“流”并进的策略,既从源头找出问题所在,又在后期的新环境应用中进行补充规制,实行“双轨”规制。故此,笔者建议从主要制度方面规制云存储中的数据安全。

1. 确立网络服务提供者的责任制度

云存储的运行离不开网络服务提供者的运作。不论从技术上还是网络数据的管控上看,必须明确网络服务提供者对云存储数据安全的保护责任及义务。网络服务提供者应当积极制定内部数据安全保护管理制度,落实安全责任制,对数据采取分类和对重要数据进行备份等措施来保护云存储中的数据安全。

对于云存储中用户和云服务提供商传输数据的规制方面,国外研究者约瑟夫 . A. 斯霍尔(Joseph A. Schoorl)认为云计算技术的使用仍在美国的出口管理制度内,但不构成与其他物理和非物理出口环境下相同的国家安全问题。因此他提出了在通过云存储传输技术数据时,应当设置云计算许可证例外(License Exception Cloud Computing,简称“License Exception CLC”)的规定,他认为云计算许可证例外比现有的规制原则更加清晰和灵活,将减少云用户由于云传输的时间和目的地的不确定性而无法满足的大多数许可要求。同时许可证例外也要求云用户在上传管控技术数据之前采取某些措施,并限制不符合该资格例外的数据类型和云服务提供商[12]。许可证例外设立的主要目的就是在云环境下维护美国的国家数据安全,实现美国企业经济利益的最大化,推动高新技术企业发展。中国在《刑法修正案(九)》中对刑法第 286 条进行了修订,明确了网络服务提供者违法后的法律责任,具体情形有四种:(1)致使违法信息大量传播的;(2)致使用户信息泄露,造成严重后果的;(3)致使刑事案件证据灭失,情节严重的;(4)有其他严重情节的。这一修正案的通过,强化了网络服务提供者对网络数据保护的责任。笔者认为不论是经营性网络服务提供者还是非经营性网络服务提供者,都应当适用该法条,虽然该法条对“信息大量传播”当“情节、后果严重”以及最后的兜底条款“有其他严重情节的”未作出明确界定,但是,就目前看至少在处罚网络服务提供者的违法行为时可以做到有法可依。

2. 制定用户滥用数据信息的处罚机制

终端用户是最开始将数据采集、处理通过互联网上传至云端的数据服务提供者,因此对于终端用户也应当明确其维护数据安全的义务及法律责任。《刑法修正案(九)》对刑法第 253 条进行了修改,明确了违反国家有关规定,向他人出售或者提供公民个人信息,情节严重的刑事责任。该条为公民个人信息受到侵害时提供了有法可依的根据。但是对于公民个人信息之外的采集、处理、传输和交易的数据未有提及,对于在云端中存储的数据安全问题则更是没有涉及。应当在对公民个人信息保护的同时,对其他由用户通过采集、处理、传输等方式获得的数据进行进一步的补充规制,数据用户是治理云存储数据安全法律保护的“源头”之一。

同时,在一定程度上,应当控制用户的访问权限,访问限制控制是指应用技术控制策略对用户访问、特定操作、IP 地址等不同类型的属性进行选择性权限设置,在允许用户访问前对其个人信息、IP 地址等信息进行严格检查,同时建立日志机制将用户的登录信息以及登录时的各项操作以日志的形式记录下来,同时还可以将恶意篡改、盗取数据的行为应用日志记录下来,便于管理人员进行安全管理[13]。只有从利用数据“源

④《关于加强网络信息保护的决定》,在 2012 年 12 月 28 日第十一届全国人民代表大会常务委员会第三十次会议通过。

⑤《中华人民共和国刑法修正案(九)》,在 2015 年 8 月 29 日第十二届全国人民代表大会常务委员会第十六次会议通过。

头”上提前进行数据应用的保护,才能真正维护网络云端存储数据的安全并为之提供有效的保护。

3. 构建应用软件行业的标准体系及软件安全认证制度

制定应用软件的行业标准及认定软件安全的统一标准,云端存储数据的应用主要靠应用软件来实现。对于软件开发者来说,对其适用相对统一的安全标准及认证制度,对于维护云存储中的数据安全起着至关重要的作用。不安全的 API(Application Programming Interface,应用程序编程接口),势必会给云存储中的数据带来安全隐患,云存储的数据安全、存储能力以及用户对数据的管控能力与 API 的安全性有直接关联。因此,应用软件行业开发软件时,应明确其 API 应用的禁止性标准,对于 API 接口的设计实行统一的安全认证标准模式,以确保用户在云端中应用其软件时,能保护云端中的数据安全。对于没有达到安全标准的软件开发者,或者是不能达到软件安全认定标准的软件服务提供者,应将其排除在外,严格应用软件的准入标准。

4. 建立数据安全保护的双重强制认证机制

建立双重强制认证机制,是保护云存储中数据安全的有效方式之一。笔者认为双重强制认证机制应当从以下两个层面来实施:一个层面是终端用户,在用户访问云存储中的数据时对其严格认证,以确保用户具有合法有效的身份去获取云存储中的网络数据资源。另一个层面应从云端的网络数据服务提供者着手,一定程度上说,云端网络服务数据提供者既是提供云端存储数据服务的运营者,也是最大数据库资源的拥有者。对于网络数据服务提供者的强制有效认证非常必要,因为可达到让其在合规的范围内处理云存储中的数据。在保护用户个人隐私的同时,建立双重的强制认证机制才能真正有效预防不法身份用户访问云存储的数据,合理控制网络数据服务提供者的权利使用,保障云存储中的数据安全,维护网络空间安全稳定运行。

5. 构建网络数据监测及预警制度

网络数据具有即时流动性、无形性、易传播性等自身特征,其自身特征要求对其进行监测以及预警处置,云存储中的数据物理位置难以确定,这就使得云存储中的数据安全难以保证,为了维护云存储中的数据安全,维护网络数据安全,甚至国家数据安全,应当积极主动监测、记录网络信息运行动态,留存网络日志,从国家和地方两个层面积极构建网络数据监测及预警制度。

对于云存储中的数据安全保护,目前中国的相关法律及制度仍处于探索阶段,各项制度尚不完善。而数据信息已然突破了传统的法律保护范围,因此在不断完善现有法律保护制度的同时,应当充分解释数据或信息的法律含义、法律特征及法律属性,按照中国现有网络数据安全保护的实际情况,结合国际及其他国家数据安全的立法经验,不断完善中国网络安全立法,维护网络空间安全,维护网络空间数据信息的存储、处理及交易,确保国家数据安全,维护国家数据主权。

五、结语

数据驱动未来,软件定义一切。大数据时代,新兴技术要求日新月异快速更新,而法律保护上又表现出滞后性,立法者及决策者总是在不断调和两者之间的矛盾,试图从制度上更好地规制新兴技术所带来的数据安全问题及挑战,云存储的数据安全问题是各国都面临的一个现实问题,一定程度上,云存储中数据安全能否得到有效的保护,将直接决定云存储在未来的发展走势。虽然很多国家及相关的组织和研究机构都在积极地对云存储中数据安全问题进行分析和研究,但收效甚微。云存储中的数据安全问题涉及的层面比较复杂,云存储中数据安全问题的解决既需要技术上的规制也需要法律制度上的保障,要实现云存储中的数据安全保护需从技术、标准、监管、法律等多维度着手,综合考量。

参考文献:

[1]黄维真,何荷. 疑云逼近——“云计算”时代的国家安全(上)[J]. 国防,2010(4):77 - 79.

[2]MILLARD C. Cloud computing law [M]. New York: Oxford University Press,2013:50.

[3]申丽君. 云存储及其安全性研究[J]. 电脑知识与技术,2011(16):3829 - 3832.

[4]WIKIPEDIA. Cloud computing[EB/OL]. [2016 - 09 - 06]. https://en. wikipedia. org/wiki/Cloud_computing.

[5]IBM. Maintaining and accessing data kept remotely[EB/OL]. [2016 - 10 - 06]. https://www. ibm. com/cloud - computing/what - is - cloud - storage.

[6]看图识云 全面解析云存储的网格架构[EB/OL]. (2010 - 03 - 17)[2016 - 10 - 06]. http://server. cnw. com. cn/server - cloud/htm2010/20100317_192514_3. shtml.

[7]徐慧丽. 云计算环境中的法律风险——以数据安全为视角[J]. 科技与法律,2013(6):1 - 9.

[8]SANDEEN S K. Lost in the cloud: Information flows and the implications of cloud computing for trade secret protection[J]. Virginia Journal of Law and Technology,2014,19(1):1 - 103.

[9]尹立波. 多国力推网络安全立法 美颁 4 部法保护关键基础设施[EB/OL]. (2015 - 07 - 22)[2016 - 09 - 26]. http://news. xinhuanet. com/politics/2015 - 07/22/c_1116007385. htm.

[10]欧洲废除欧美数据安全港协议[EB/OL]. (2015 - 10 - 07)[2016 - 09 - 26]. http://world. huanqiu. com/article/2015 - 10/7699653. html.

[11]卧龙传说. 俄罗斯"个人数据保护法"任性实施 从"存储本地化"到数据安全之路还有多长?[J]. 信息安全与通信保密,2015(10):76 - 77.

[12]SCHOORL J A. Clicking the "Export" button: Cloud data storage and U. S. Dual - Use export controls[J]. George Washington Law Review,2012,80(2):632 - 667.

[13]徐欢. 云计算时代监测数据安全保护分析[J]. 无线互联科技,2016(12):124 - 125.

Legal protection of data security in cloud storage

QI Aimin[1], ZHU Gaofeng[2]

(*School of Law, Chongqing University, Chongqing 400044, P. R. China*)

Abstract: Cloud storage is the evolution of cloud computing, cloud storage and cloud computing both connections and differences. Cloud storage refers to the use of the network (especially Internet), the use of application software, to provide users with data storage and access functions of a software and hardware combination of data collection system. Cloud storage itself is not a service, it is in order to achieve data storage services provided by a system support. Uncertainty about the location of the cloud servers has led to variable data locations in cloud storage. Data security and privacy security in cloud storage pose a serious challenge to data users. Data security in cloud storage mainly refers to the security of data collection, storage, access, processing and data transaction. Data security in cloud storage is closely related to network security, the legal protection of data security urgently needs to be developed.

Key words: cloud storage; data security; internet security; legal protection

(责任编辑 胡志平)