云计算环境下的商业秘密保护

周铭川

(上海交通大学　法学院,上海　200240)

[摘　要]　在云计算环境下,商业秘密保护面临着一些与云计算模式及网络技术有关的特殊问题,例如商业秘密的存在形式、侵权表现、侵权特点、安全隐患等均与传统环境下有所不同,为此,有必要有针对性地采取一些安全保密技术和制度措施,而目前学界对云计算的商业秘密保护问题存在诸多误解。

[关键词]　云计算;商业秘密;安全;保密

[中图分类号]　D923.4　　[文献标识码]　A　　[文章编号]　1000-5072(2014)01-0043-11

互联网时代的知识产权保护问题尚未圆满解决,云计算时代的到来,又使知识产权保护问题雪上加霜。国内外此起彼伏、乱象丛生的大小纠纷,以及网络与纸面媒体的跟踪报道,无不让人们感受到商业秘密保护的难度与热度。不过,与云计算专利、商标、版权的保护问题相比,云计算商业秘密保护问题远未得到应有的重视,目前相关研究成果非常少见,以"云计算商业秘密"为题在中国期刊网上尚检索不到一篇论文。为此,笔者不惴学识浅陋,拟就云计算环境下的商业秘密保护问题作一探讨,目的不在于解决太多难题,仅在于引起学术界对此问题的重视,以推动云计算商业秘密保护的发展。

一、云计算既是一种技术也是一种服务

自 Google 首席执行官埃里克·施密特(Eric Schmidt) 2006 年在世界搜索引擎大会(SES San Jose 2006)首次提出"云计算"(Cloud Computing)概念以来[1]13-23,这一概念已获举世公认,云计算也被视为继大型机、PC、互联网之后全球 IT 产业的第四次革命[2]59-60。但是,对于云计算的定义,却远未达成共识[3]39-41。例如,有人认为,"云计算是指通过网络以按需、易扩展的方式获得所需的资源(硬件、平台、软件)。基于云计算这种共享架构,可以将巨大的系统池连接在一起以提供各种 IT 服务,而提供资源的网络被称为'云'"[4]49-53。有人认为,云计算作为一种软件或服务提供行为,是以网页浏览器的方式通过远程服务器中的软件来执行某些应用功能,其应用成果既可以存储于远程服务器上,也可以下载到用户本地计算机上[5]84-95。有人认为,云计算是对基于网络,能够对可配置的共享计算资源池进行方便的、按需访问的一种模式,如纳米手机、在线编辑、在线游戏等[6]55-61。而学术界引用较多的,则是美国国家标准与技术研究院(NIST)的定义,认为云计算是一种无处不在的、便捷的、按需使用的对共享的可配置的计算资源(如网络、服务器、存储、应用和服务)进行网络访问的模式,能够通过最少量的管理或与云服务商的互动实现

[收稿日期]　2013-07-01

[作者简介]　周铭川(1975—),男,江西丰城人,上海交通大学法学院讲师,法学博士,主要从事法学理论研究。

[基金项目]　教育部人文社会科学研究规划基金项目《云计算知识产权问题研究》(批准号:12YJAZH116);
上海市软件和集成电路产业发展专项资金项目《云计算产业法律政策保障研究》(批准号:沪经信信(2012)698 号);
上海交通大学文理交叉专项基金重点项目《云计算知识产权问题研究》(批准号:11JCZ04)。

计算资源的迅速供给和释放[7]。

虽然学术界对云计算的定义众说纷纭,但对于云计算既是一种技术又是一种服务,却基本上没有争议。

从技术角度来讲,云计算是网格计算、分布式计算、并行计算、效用计算、网络存储、虚拟化、负载均衡等传统计算机技术和网络技术融合发展的产物[8]100-101,其关键技术是虚拟化技术。该技术能将应用系统的不同层面——硬件、软件、网络、存储和数据等隔离开来,打破服务器、网络、存储、数据中心、数据和应用中的物理设备之间的划分,实现架构的动态化,达到动态使用和集中管理物理资源和虚拟资源、提高系统结构的弹性和灵活性、降低成本和减少风险等目的[9]22-29。

从商业角度来讲,云计算是一种新的 IT 服务模式,包括基础设施即服务(IaaS)、平台即服务(PaaS)、软件即服务(SaaS)和数据即服务(DaaS)等[10]13-16。其中,基础设施即服务(IaaS)向用户提供计算、存储、网络、中间件等基础资源,用户可以控制操作系统、存储、网络设备[11]9-10;平台即服务(PaaS)向用户提供一个应用的运行环境,用户只能控制应用和该运行环境,但不能控制操作系统、硬件和网络基础设施[12]80-84;软件即服务(SaaS)则把软件使用作为一种服务来提供,是一种将应用软件统一安装在自己的服务器上,并通过浏览器提供给用户使用的模式[13]43-48;数据即服务(DaaS)是通过数据挖掘和分析技术,从看似毫无规律的海量数据中,将隐含的、尚不为人所知的、潜在的有用信息提取出来,转化为有用的数据信息,以提供给感兴趣的客户[14]45-46。

从部署模式来看,云计算可分为私有云、公共云、社区云和混合云[15]24-26。其中,私有云是只服务于组织内部的云计算系统,相当于某主体在"云"中租赁一个空间以获取并存储信息;公共云通常用于公共场所,属于开放的云场所,任何人都可以通过网络获取云服务,社区云和混合云则是私有云与公共云的结合,既有私有空间也有公共部分[16]2-14。

从实际功能来看,由于云计算是将大量的可规模化的 IT 资源作为一种服务通过互联网提供给多个外部用户使用,云服务提供商包揽了软硬件等计算资源的管理和维护,用户只需关心需要何种计算而不必关心这种计算以何种方式实现以及发生在哪里,因此,用户无需进行硬件计算资源的维护、软件的维护、升级、容错、安全保护和优化能耗等工作,从而可节省需要高度专业技术的系统维护成本,而云服务提供商则拥有了比以往大得多的资源整合和优化空间,从而能够在规模化效应中探索节省成本的空间[17]。并且,云计算服务还能给用户带来安全可靠(由于数据储存于云端,用户不用担心因本地电脑损坏、被盗或被病毒入侵等原因而导致数据丢失)、使用方便(对客户端的需求相当低,只需要一台智能手机等能联网的终端设备即可使用)、共享数据迅速便捷等优良体验[18]51-53。此外,在软件即服务(SaaS)中,由于云服务提供商只是为用户提供服务接口,并不将其软件出售给用户,故能有效防止用户或者竞争对手通过对软件实施反向工程来获取软件中包含的商业秘密[19]。

二、云计算环境下商业秘密侵权的特征

根据《刑法》第二百一十九条第三款和《反不正当竞争法》第十条的规定,所谓商业秘密,是指不为公众所知悉,能为权利人带来经济利益,具有实用性,并经权利人采取保密措施的技术信息和经营信息。就保护力度而言,法律对商业秘密的保护,在云计算环境下和在传统环境下是一样的,都要求有关信息具备秘密性、价值性、实用性和保密性等法定特征。但是,由于云计算至少涉及两方主体——用户和云服务提供商,甚至涉及用户、云服务提供商、云提供商三方主体,并且与云计算技术与网络传输技术密不可分,因而导致商业秘密保护在云计算环境下面临着一些特有的问题。

(一)云计算服务的产业结构图

有 IT 从业人士概括了云计算服务的产业结构图(图 1)[20]30-35:

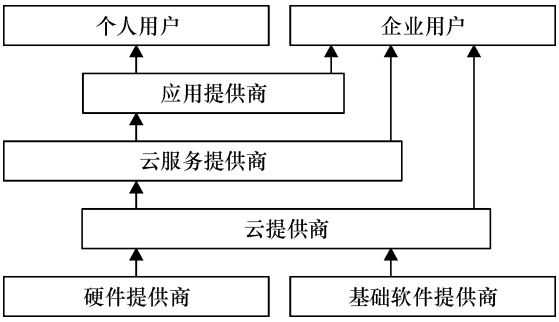

图 1

可见,在云计算的产业结构中,从底层到顶层的结构关系依次是: ①硬件提供商和基础软件提供商分别向云提供商提供硬件和基础软件; ②云提供商再为云服务提供商搭建公有云环境,或者为企业用户搭建私有云环境; ③云服务提供商向应用提供商或者企业用户提供开发和运营各种应用所需的资源; ④应用提供商向个人用户或者企业用户提供各种云计算服务。其中,个人用户仅直接与应用提供商发生关系,企业用户则可能同时与应用提供商、云服务提供商、云提供商发生关系,以向应用提供商实时按需购买软件的使用权,向云服务提供商购买计算和存储资源来运行企业机构内部的自有应用,向云提供商实时按需购买私有云。不过,笔者认为,与该结构图所示不同的是,实践中可能缺少"应用提供商"这个环节,或者说,"应用提供商"与"云服务提供商"有可能是同一个主体,这样,就使云计算主要呈现为两种互动模式,第一种是云服务提供商与用户双方主体互动,第二种是云提供商、云服务提供商与用户三方主体互动。加上其他用户或者网络黑客等可能侵犯商业秘密的人,将使商业秘密的侵权及责任承担关系结构更加复杂。

值得一提的是,为了使美国政府、行业和个人对云计算有一致的认识,NIST 组织制定了《云计算定义》和《云计算参考架构》,提出了"参与者——角色"的云计算参考架构模型,如图 2 所示[21]20 - 24。

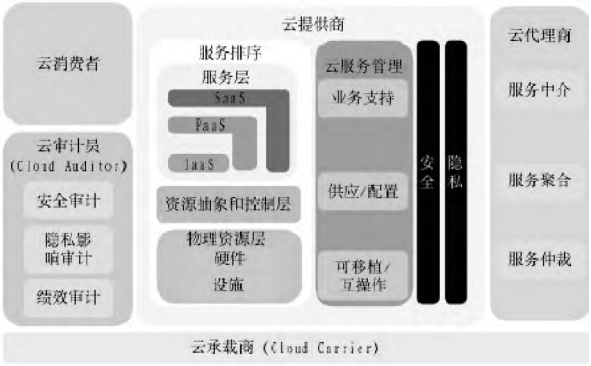

图 2　云计算参考架构

(二) 云计算环境下商业秘密存在的形式

在传统环境下,商业秘密主要用物理介质来保存,并且保存于权利人或者合同相对方的物理场所内,例如,保存于保险柜、抽屉、文件箱中等,具体表现形式如生产工艺、化学配方、图纸、模型、销售方法、配送方法、合同形式、商业计划、价格协议的内容、消费者数据、广告战略、供应商或客户名单、计算机软件及数据库等。在云计算环境下,商业秘密则主要以电子数据的形式存在,借助磁性介质(U 盘、硬盘或光盘) 来记录和保存,并通过计算机进行管理,其表现形式主要有: ①通过软件、硬盘、光盘、U 盘等载体记载的技术信息和经营信息,前者如设计图纸、产品配方、技术工艺等,后者如企业发展规划、经营状况报告、市场调研报告、重要会议通知等。②企业从事电子商务活动时建立的各种数据库,比如客户资料数据库、产品数据库、支付数据库、工艺数据库等。③电子交易过程中传递的信息,如客户的姓名、银行卡卡号、订货信息和付款信息等[22]93 - 96。此外,有学者认为,为了确保电子商务安全而设置的有关用户名、口令、密码、密匙等,虽然严格说来并不属于商业秘密,但由于它对商业秘密的保护具有重要作用,亦有必要作为广义上的商业秘密加以保护[23]39 - 43。笔者认为,由于用户名、口令、密码、密钥等不完全具备商业秘密的法定特征,比如不具备秘密性、实用性、价值性甚至保密性等,能否作为商业秘密进行保护,主要是一个保护政策的问题。

(三) 云计算环境下商业秘密侵权的形式

我国刑法和反不正当竞争法等法律法规列举了侵犯商业秘密的主要形式: 一是以盗窃、利诱、胁迫或者其他不正当手段获取权利人的商业秘密; 二是披露、使用或者允许他人使用以前项手段获取的权利人的商业秘密; 三是违反约定或者违反权利人有关保守商业秘密的要求,披露、使用或者允许他人使用其所掌握的商业

秘密;四是明知或者应知存在前述三种侵权情形,仍获取、使用或者披露他人的商业秘密。在云计算环境下,这些侵权形式仍然存在,只不过结合了网络传输、云计算和侵权主体的特点而已。具体言之,云计算环境下商业秘密的侵权形式主要有:

1. 以不正当手段获取权利人的商业秘密。是指行为人以盗窃、利诱、胁迫或者其他不正当手段获取权利人的商业秘密。既包括从使用云计算服务的用户或用户的雇员那里获取,也包括从云服务提供商、云提供商及其雇员那里获取;既包括权利人公司外部的人员以不正当手段获取,也包括权利人的雇员以不正当手段获取,比如雇员擅自复制载有商业秘密的文件资料或擅自收集不应该知道的商业秘密等;既包括第二人以不正当手段从权利人或义务人处获取,也包括第三人明知或应知第二人的侵犯商业秘密行为,仍从第二人处获取[24]491-492。其中,比较突出的问题是窃取商业秘密。常见有黑客利用木马病毒等技术侵入他人电脑硬盘、电子邮箱或者公司数据库窃取商业秘密,利用网络嗅探技术寻找云计算系统的软硬件缺陷、取得云计算系统的控制权从而冒充合法用户窃取商业秘密,利用科技设备拦截在网络传输过程中从网络设备中泄露出去的电磁波以窃取商业秘密[25]39-47,云服务提供者或其雇员利用管理网站和服务器的优势,秘密窃取用户的商业秘密等。此外,在企业的加密强度不够等场合,黑客可能通过互联网、公共电话网或搭线,在电磁波辐射范围内安装截收装置,或在网关和路由器上设置装置截获通过的数据包,通过分析信息流量、流向、通信频度和长度等参数,来推出有用信息,如消费者的银行账号、密码等商业秘密[26]115-118。需要注意的是,虽然以不正当手段获取权利人的商业秘密是一种侵权行为,但是,这种侵权行为并不必然导致权利人遭受现实损失,如果侵权人并未披露、使用或者允许他人使用,并未使权利人失去对其商业秘密的使用可能,则在通常情况下不会导致权利人遭受损失,不过,在侵权人是权利人的商业竞争对手的情况下,即使没有披露、使用或允许他人使用,仅仅是获取并知悉权利人的商业秘密,也会缩短侵权人与权利人之间技术水平的差异,从而削弱权利人的竞争优势,这在某种意义上也是一种现实损失。

2. 非法披露、使用和允许他人使用权利人的商业秘密。既包括以不正当手段获取商业秘密者披露、使用或允许他人使用,也包括云服务提供商、云提供商违反约定或者不顾用户的保密要求而披露、使用或允许他人使用,还包括恶意第三人披露、使用权利人的商业秘密。其中,与云计算比较密切的问题是非法披露。所谓披露,是指以口头、书面或其他方式将权利人的商业秘密向他人公开。例如,将权利人的商业秘密上传至 BBS、FTP、MSN、QQ、BT、Newsgroup、Telnet[27]33-36、博客、微博或其他网页上,供网友下载或传播。而商业秘密一旦被人上传至网上,就会丧失秘密性。这是因为,所谓秘密性,是指有关信息不为同一行业或者领域内的大多数人所知或可轻易获得,这些人如果要想获得同一信息,必须付出较大程度(值得法律保护程度)的辛劳和努力才行,只有这样的信息才值得国家作为商业秘密来保护。反之,如果某一信息已经为同一行业或者领域内的大多数人所知,则属于众所周知的信息,当然不值得作为商业秘密来保护;或者虽然同一行业或者领域内的大多数人仍然不知,但是如果这些人只要想知悉就能很容易地获取并知悉的话,同样不值得国家作为商业秘密来保护。实际上,保护同一行业或者领域内的大多人所知或者可轻易获取并知悉的信息,对于其他从业者而言也是不公平的,无异于以法律来保障特定人对公知信息的垄断地位。正如美国法院相关判例所言,无论权利人对其商业秘密采取了何种程度的保密措施,一旦有关信息被公布于网上,就属于普遍公知的信息,不能再获得商业秘密法的保护①。不过,也有的法官在判断网络公开是否会导致商业秘密丧失秘密性时,会综合考虑信息

① 908 F. Supp. 1362 (E. D. Va. 1995).

公开时的各种情况、商业秘密权利人的利益、鼓励竞争的相关政策、善意第三人的言论自由等因素①，例如，在 DVD Copy Control Association v. Bunner 一案中，被告 Bunner 将其从网上下载的原告的 DVD 解密程序上传至个人网站上，初审法官认为，商业秘密不能仅仅因为公布在网上而丧失秘密性，因为这样做只会鼓励侵权人尽其可能地快速散布信息，以彻底破坏商业秘密的秘密性，因此，初审法官禁止 Bunner 在任何网站公布原告的商业秘密，但后来该判决被上级法院改判，认为原告的信息早已被公开而不属于商业秘密②。此例中，初审法官对被告下达禁止令是有必要的，因为任何散布行为都可加速信息的公开与传播，但是，其脱离秘密性的通常判断方法来认定秘密性，却与商业秘密保护原理相悖，这里存在一个形式合理性与实质合理性何者优先的问题。尽管在实质上，一项公布于某网站上的信息，有可能由于公布者、传播者及时删除网页而仍然处于同一行业或者领域内的大多数人所不知并且不能轻易获取并知悉的状态，因而仍然符合秘密性的一般定义，但是，这一点在司法实践中是极难证明的，原告也难以举证证明其信息没有丧失秘密性；对于这种纯粹属于原被告双方民事权利均衡保护的问题，也不宜参照适用刑事诉讼中对事实存在疑问时的处理原则，否则，对转播信息的被告不公平；加上信息被出版物或者网络公开会丧失秘密性的一般经验常识，大多数法官还是坚持形式合理性优先原则，认为只要某一信息曾经被公布于网上，即使其实际上有可能仍然符合秘密性的一般定义，也认定其已经丧失了秘密性，转播这种信息并不构成商业秘密侵权。由此可见，在类似案例中，完全可能出现在民事上不构成侵权(因为某一信息一旦被上网就被认为丧失秘密性，转播这种信息不构成侵权)，而刑事上构成犯罪(如果该信息仍然具有秘密性，则转播它仍可构成犯罪)的情况，这是由于民事重形式、刑事重实质的思维差异所造成的。

3. 采用黑客技术，破解用户、云服务提供者、云提供者计算机的安全防护系统，侵入他们的计算机信息系统并故意传播计算机病毒等破坏性程序，对储存在服务器上或正在传输过程中的商业秘密数据进行删除、修改、插入等操作，破坏权利人商业秘密数据信息[28]119－121。实施这种侵权行为的人，既可能是想显示自己黑客技术高超的电脑爱好者，也可能是商业秘密权利人的竞争对手，这种侵权行为会全部或者部分破坏权利人商业秘密信息的完整性和实用性，导致商业秘密丧失其原有的价值。

(四)云计算环境下商业秘密侵权的新特点

与网络传输及云端数据处理与存储等特点相对应，云计算环境下商业秘密的侵权也呈现出一些新特点。

1. 侵权主体的多元化。既包括企业内部的侵权，又包括企业外部的侵权，前者如企业内部员工将企业的商业秘密从企业内部网上下载出售，或者内外勾结为外人获取企业内部网上的商业秘密提供便利，虚拟企业或者虚拟企业联盟非法披露、使用或允许他人使用成员企业合作投入的商业秘密或者合作后产生的商业秘密[29]121－123；后者如黑客入侵用户或云服务提供商、云提供商的计算机信息系统，散布计算机病毒程序，破译企业计算机系统密匙，冒充合法用户登录以窃取用户的商业秘密。既包括云服务提供商、云提供商或其员工非法披露、使用或允许他人使用用户的商业秘密，也包括黑客、无意中获取权利人商业秘密者获取、披露、使用或者允许他人使用用户或云服务提供商、云提供商的商业秘密。一个侵权行为往往涉及二方、三方甚至四方、五方主体，法律关系非常复杂。

2. 侵权手段的高科技性。在云计算环境下，权利人特别是用户的商业秘密通常存储在云端，在用户、云服务提供商、云提供商以及各企业内部，有关商业秘密均依靠网络来传输，面

① Daniel W. Park, Trade secrets, The First Amendment, and Patent Law: A Collision on the Information Superhighway, 10 Stan. J. L. Bus. & Fin. 46, Autumn, 2004.

② DVD Copy Control Association inc. v. Bunner, 116 Cal. App. 4th 241, 10 Cal. Rp tr. 3d 185 (2004); http://caselaw.lp.findlaw.com/data2/californiastatecases/h021153a.pdf.

临着身份假冒、虚拟层软件漏洞、数据泄露、篡改和丢失、非法用户访问、分布式拒绝服务(DDoS)等安全风险[30]87-89,黑客攻击、网络钓鱼、域欺骗、木马病毒、蠕虫病毒、恶意软件、间谍软件等手段也比较常见。利用技术手段非法解密、破坏防火墙等安全保护措施,从而非法侵入他人计算机信息系统或者远程登录他人计算机终端,通过无线网窃听、窃取、破坏他人商业秘密的行为屡见不鲜,体现出很高的科技性[31]80-83。由此导致防范侵权的难度极大。

3. 侵权行为的隐蔽性和侵权后果的难以控制性。由于权利人的商业秘密储存于云端的服务器中,一个商业秘密的电子数据可能拆开并分散存储于多个服务器上,"这些服务器可能位于街边的某个位置,可能分散于全国各地,也可能在世界的另一头"[32]64-69,通过网络来传播,并以无形无体、稍纵即逝的电子数据形式来体现,加之侵权主体非常广泛、侵权技术含量高超,导致侵权行为很难被发现,侵权的后果非常不容易控制,权利人甚至根本找不出侵权者位于何处。

4. 原告举证难度加大。在我国,商业秘密侵权属于一般侵权,仍适用"谁主张谁举证"原则,权利人向人民法院提起商业秘密侵权诉讼时,至少应提出证据证明自己拥有商业秘密,被告能够接触到自己的商业秘密,被告获取、使用或披露的商业秘密与自己的商业秘密相似等事实。但是在云计算环境中,相对而言,商业秘密权利人的技术水平往往比不上黑客或云服务提供商等侵权人,即便明知对方侵权,也很难收集到相关证据,特别是证明被告能够接触到自己的商业秘密和被告侵权的证据。目前的云计算服务也不利于调查取证,因为多个用户的数据和日志记录既可能同地协同工作,也可能通过一组随时变化的主机和数据中心进行传播,而大规模分布式异构虚拟计算基础设施也使非授权的调查取证工作雪上加霜。有些侵权方式即使是刑侦手段也无能为力,例如,目前至少有三分之一的云实例是通过虚拟专用网络(VPN)访问,而网络刑侦对这种方式几乎完全检测不到,如果在网吧、图书馆或公众开放环境通过 VPN 进行访问,那就更加没有办法侦测到,大量的新兴多媒体终端设备通过无线方式接入到开放网络中,都使问题更加复杂和恶化[33]38-40。因此,对于权利人而言,尽可能事先防范是非常必要的。

三、云计算环境下商业秘密的技术保护和制度保护

如前所述,云计算环境下商业秘密的保护与传统环境下没有本质区别,只是由于商业秘密数据化电子化、侵权主体多样化、侵权手段科技化、侵权行为隐蔽化等特征,导致有必要采取一些不同的手段,特别是针对商业秘密所面临的主要安全隐患而采取相应的手段,以防止商业秘密被泄露或窃取。

(一)云计算环境下商业秘密面临的主要风险

在云计算环境中,商业秘密等电子数据主要面临如下风险:①用户数据的安全性可能会受到来自于云服务提供商、其他云用户或网络黑客的损害;由于云计算环境中数据和计算的高度集中,攻击者能够低成本地使用云服务来实施各种攻击,比如,密码破解、DDoS、恶意软件、垃圾邮件和僵尸网络控制器等[34]36-38。②虚拟化技术以及虚拟机动态迁移是云计算中的核心技术,用于计算资源的动态调度,但这些技术本身均可能给用户数据带来安全隐患,从 2007 年开始,经常发现主流的虚拟层软件存在着漏洞。③作为云计算软件层的核心,虚拟机监控器本身的安全隐患日益突出,一旦虚拟机监控器被攻破,建立于其上层的所有虚拟机及其中的用户数据将被攻击者控制。④云计算服务器存在被直接接触与对硬件的攻击,例如总线与内存探测,甚至存在攻击者用被篡改的硬件替换正常硬件的风险[35]。⑤云服务提供商的信用风险。由于云服务提供商拥有超级用户角色,一旦其滥用这种角色,就会增加用户数据泄露风险;云服务提供商的员工也可能滥用权力访问客户的数据及应用。据 Verizon Business 一项数据泄漏调查报告显示,48% 的数据泄漏

是由于内部员工滥用权限所致[36]。⑥用户控制权丧失的风险。在云计算中,用户数据的控制权会转移到云服务提供商手中,用户可能丧失对数据的创建、传播与销毁等控制权,可能无法知道自己的数据存放在哪里,也不知道云服务提供商是否对数据进行了正确的保护,难以监管其程序和数据的处所或使用情况,比如,云平台是否隔离了多个用户的数据、云服务提供商是否按照用户的要求删除了相关数据、是否对存储位置进行了清洗、是否周期性地对存储的数据进行完整性检查等。⑦数据传输过程中的风险。用户在上传数据时,可能面临种种风险,比如,云服务提供商可能不按用户要求加密数据、数据在传输过程中可能被偷窥、加密过的数据在传输过程中可能发生加密密钥丢失导致数据泄露或数据不能解码而报废。⑧云计算服务意外中断的风险,例如,云平台故障导致云服务终止、云平台不能为用户提供独立的运行环境、云服务提供商不能完全保证其服务的质量等[37]。

此外,美国 Gartner 咨询公司在 2008 年发布了一份云计算安全风险分析报告,认为云计算主要面临以下七类安全问题:①特权用户访问风险。管理数据的特权用户可能绕过监管对内部程序进行控制,从而对来自企业外部的敏感数据造成安全风险。②法规遵从风险。如果云服务提供商拒绝监督和审计,最终只能由用户对其数据的安全性和完整性负责。③数据保存位置不确定风险。由于云计算采用虚拟化技术以及分布式存储,用户无法得知数据托管于何处。④数据分离风险。由于多个用户的数据一起保存在一个共享的云环境中,因此需要对数据进行加密以保证用户数据之间的隔离,但这可能影响数据的可用性。⑤数据恢复风险。在发生灾难的情况下,云服务提供商能否对数据和服务进行完整的恢复,也会影响数据的安全性。⑥调查支持风险。因为多用户的日志文件和数据可能存放在一起,也可能散落于不断变化的主机和数据中心内,所以不太可能对云计算环境中的侵权行为或违法行为进行调查。⑦长期可用性风险。当云服务提供商破产或者被收购时,如何确保数据仍然可用也是一个突出的安全问题[38]。

(二)云计算环境下商业秘密的技术保护

云计算的安全保护技术对于权利人商业秘密的保护的重要性是显而易见的,既有利于防止用户数据泄露或者被其他用户、黑客等人窃取或破坏,也有利于侵权发生后的调查取证。对于云计算的安全保护技术,计算机界、信息产业界人士已经有较多的探讨,这里仅作简单介绍。对此问题,有学者对云计算安全关键技术从身份管理和访问控制、安全审计、虚拟化安全、数据保护、可信云计算几个方面进行介绍,着重介绍了哪些人员提出了哪些安全保护技术[39]86-89。有学者从用户认证与授权、数据安全、网络隔离、灾备管理、虚拟化安全等方面对云计算的安全技术进行了探讨,具体介绍了身份管理、访问授权、多因素认证、数据隔离、加密、保护和残留、软件和服务器虚拟化等安防技术[40]31-42。有学者详细介绍了云计算的安全模型,重点是云安全联盟 CSA(Cloud Security Alliance)提出的模型(图 3)和我国国内 IT 企业提出的模型(图 4)[41]44-49。

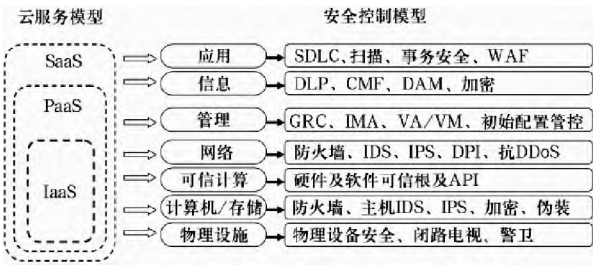

图 3　云安全联盟 CSA 提出的云安全模型

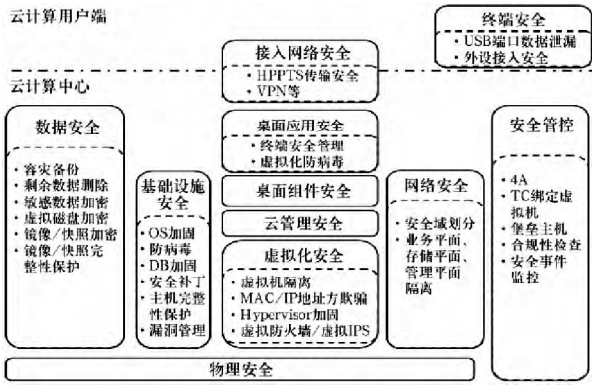

图 4　我国 IT 企业提出的云安全模型

(三)云计算环境下商业秘密的保护制度

就保护制度而言,云计算环境下商业秘密

侵权主要是侵犯用户的商业秘密,侵权行为主要来自于云服务提供商或者网络黑客等人,前者与用户之间存在合同关系,存在违约与侵权竞合的问题,后者则是单纯的侵权。当然,无论何者侵权,如果给权利人造成了重大损失,均涉嫌构成侵犯商业秘密罪;如果实施非法侵入他人计算信息系统、破坏他人数据信息等行为,还可能涉嫌构成非法获取计算机信息系统数据罪、非法控制计算机信息系统罪、提供侵入或非法控制计算机信息系统的程序或工具罪、破坏计算机信息系统罪、非法侵入计算机信息系统罪等犯罪。为此,有必要针对不同的安全隐患采取不同的保护措施。

首先,加强合同保护。由于云计算服务涉及用户、云服务提供商、云提供商甚至云应用提供商等多方主体,为了事前尽量避免纠纷,事后及时解决争议,有必要强化合同意识,订立内容详尽、科学合理、利益均衡的合同,明确各方的权利义务、违反合同的违约责任等,例如,有必要在合同中约定双方均有义务对用户或云服务提供商的商业秘密采取保密措施、保密措施的形式和种类、商业秘密的存储方式、擅自披露、使用或者允许他人使用对方商业秘密的违约责任、由于疏忽大意导致对方商业秘密遭受第三人侵权时的违约责任等。尤其需要注意的是,除了与企业法人本身订立合同之外,还有必要与企业法人的主要员工订立合同,因为许多违约/侵权行为都是由这些员工擅自实施的,有必要让这些员工增强不侵犯他人商业秘密的法律意识,若违约/侵权则要对其违约/侵权行为承担责任,而不仅仅是公司主体承担责任。至于合同的具体内容,国家有必要制定一些法律、法规、规章和技术标准,行业协会有必要制定一些指导性规范,企业内部也有必要听取有关技术专家和专业律师的意见,事先拟定一些内容翔实、科学合理的合同条款。

其次,加强法律保护。充分利用好现有法律法规中有关商业秘密保护的规定,例如劳动合同法、民法、合同法、侵权行为法、反不正当竞争法和刑法等中的相关规定,防范与打击侵犯商业秘密的行为。在企业内部定期或不定期地举行商业秘密保护知识培训,强化企业员工的商业秘密保护意识,提高员工保护企业商业秘密的使命感和责任感,促使员工树立商业秘密权是绝对权、财产权的意识,帮助员工掌握商业秘密的构成要件及认定标准,帮助员工熟悉商业秘密侵权的常见手段和途径,促使员工自觉遵守法律法规,尊重他人商业秘密,不以不正当手段获取、披露、使用或者允许他人使用权利人的商业秘密等。

最后,重视保密措施。在云计算环境中,商业秘密保护所面临的最大问题是被非法披露和窃取的问题,几乎所有探讨云计算安全的论文都在探讨电子数据的保护问题。因此,虽然"合理的"保密措施即能满足商业秘密的"保密性"要求,但是,为了防止黑客入侵或者其他人侵权,仍有必要采取较为高端的安全防护措施。此外,明确商业秘密的范围和密级,对与其商业活动有关的网站实施监控以防保密信息泄露,定期使用搜索引擎检查网络上是否存在未经授权的公开信息,利用网页爬虫程序(Web Crawling Program)随时搜索可能披露公司保密信息的网站[42]52-63,禁止员工通过电子邮件传输商业秘密,禁止员工在 QQ、MSN、FACEBOOK 等社交网站上谈论公司的商业秘密等[43],对商业秘密的保护都有一定作用。

四、云计算商业秘密保护的其他问题

由于商业秘密的构成要件和保护水平取决于现有的法律规定和国家政策,而非取决于技术的发展,故商业秘密保护在云计算环境下与在传统环境下没有本质差异,都必须认定存在商业秘密和侵权人侵犯了商业秘密,都采用"接触+相似-合法来源"原则来认定被告是否侵权,都统一适用商业秘密法和相关理论。只不过,由于在云计算环境下,商业秘密以电子数据的形式存储于云端服务器中,并且必须通过互联网来传播,其保护必须结合云计算服务和网络技术的特点来进行,故确实存在一些依赖于云计算和网络技术的特有问题,主要是如何防止他人利用技术手段窃取、披露或破坏商业秘

密的问题。

而目前散见于“云计算知识产权保护”主题下的论文中有关商业秘密保护的问题,很多都不是真正的商业秘密保护问题。例如,有学者提出,‘商业秘密保护的前提是权利人对特定具有商业价值的信息采取保密措施,在‘云计算’的情形下,企业技术信息与经营信息存储于‘云端’,‘云端’的安全措施是否可以视为用户的安全措施?什么样的安全措施可以被法院认定为采取了保密措施?如果‘云服务商’按照政府的要求向政府有关部门提交,是否构成丧失秘密性?如此等等的问题都处于不确定状态之中”[44] 7 - 11。其实,这些问题都是理论上早已解决了的问题。由于用户与云服务提供商之间存在服务合同,即便知悉对方的商业秘密,只要不恶意地披露、使用或者允许他人使用,就不构成违约或者侵权,故无论是用户自己还是云服务提供商对用户的商业秘密采取保密措施,都是对商业秘密采取了保密措施,云端的安全措施当然可以视为用户的安全措施,只有在双方都故意或者由于疏忽大意而未能采取保密措施时,才会导致该商业秘密丧失保密性,当然,最好在合同中约定双方均有义务采取保密措施及其违约责任。由于保密措施只要求是“合理的”即可,只要对商业秘密所采取的保密措施能够让第三人知道这里存在商业秘密,知道权利人具有保密的意愿,即可认为采取了“合理的”保密措施,即使是最简单的登录网站的用户名和密码,都符合“保密性”要求[45] 16 - 22; 要求较高端保密措施的目的,在于防范黑客等技术高超者的入侵和防止数据破坏,并不意味着提高了法律对“保密性”的要求; 至于为什么对保密措施只要求“合理的”即可,是因为法律保护商业秘密的目的,在于保护诚实劳动者的劳动成果,鼓励和促进科技发明创造,维护合理的商业道德,如果要求采取较高端的保密措施才予以保护,无疑是对权利人提出过高的要求,科以不应当科以的义务,不符合商业秘密保护的宗旨。至于云服务提供商按照要求向政府有关部门披露用户的商业秘密,也是商业秘密保护理论中老生常谈的问题,只要商业秘密仍然处于同一行业或领域内大多数人所不知并且通过正当手段不能轻易获知的状态,就不会因此丧失秘密性,而政府有关部门对所获知的商业秘密亦有保密义务,如违反保密义务也会构成侵权[46] 45 - 50。

又如,有学者提出,‘在云模式中,所有的数据处理都在云端服务器完成,数据通常也是储存在云端服务器内,一旦云端服务器自身出现问题或遭受攻击,就很可能导致涉及商业秘密的数据无法访问、丢失或遭受破坏或篡改; 在此情况下,用户的商业秘密专属权是否受到侵害,云服务商又应承担何种法律责任?对此,现行法律无法做出明确的回答”[47] 102 - 104。其实,这个问题也不是一个太难解决的问题。在此情形下,用户的商业秘密权当然受到了侵犯,因为其商业秘密信息已经被破坏、丢失或者无法访问,信息本身的完整性和秘密性都存在问题,权利人也无法使用该信息从而无法取得收益; 至于应当由谁来承担责任以及如何承担责任,则由双方事前在云服务合同中明确约定即可; 如果云服务提供商违反约定故意披露、使用或者允许他人使用权利人的商业秘密,给权利人造成重大损失的,则不仅涉及商业秘密侵权问题,还涉嫌构成侵犯商业秘密罪。因此,类似问题依民法、合同法和刑法等现有法律法规完全可以合理解决,并非现行法律难以规制。

再如,有学者提出,‘在云计算模式中,用户端往往只存在一个与云端沟通的界面,而所有操作结果和数据都在云端,分布存储在网络设备中,这些数据涉及商业秘密,如何来保护是个令各国头疼的问题。如何避免相关商业秘密被云计算系统的运营商用作分析和评价,甚至打包销售,一旦发生侵权如何规制?如果这些数据被云计算系统存储在国外的网络设备中,那么侵权和泄密又应当依据哪个国家的商业秘密法案来进行判断?都是亟待解决的问题”[48] 38 - 42。其实,这些也不是什么新问题。前者,无非是个合法知悉权利人商业秘密者违反约定或者违反权利人有关保守商业秘密的要求,披露、使用或者允许他人使用权利人商业秘密的侵权/违约行为,当然,如何发现对方违约/

侵权、如何收集对方违约/侵权的证据,无疑是一个与云计算有关的问题,但是,这并非商业秘密保护所特有的问题,如果将商业秘密替换为其他电子数据信息,同样存在这些问题;后者,无非是个网络环境下地域管辖或国际私法中准际法的适用问题,而这既是个程序上的问题,又不是商业秘密保护本身所特有的问题。

此外,诸如在云服务合同终止以后,云服务提供商是否及时删除储存于其服务器上的用户的商业秘密数据,是否允许用户将其商业秘密数据迁移于其他云服务提供商的"云"中之类的问题[49]60-64,虽然是一个涉及商业秘密的问题,但严格说来并不是一个商业秘密侵权问题,与商业秘密保护没有太大关系,因为即使将此中的"商业秘密"替换为并不构成商业秘密的其他电子数据,对于问题的存在和解决同样不会有丝毫影响。只有那些涉及信息的秘密性、价值性、实用性和保密性等商业秘密的构成要件,以及那些涉及以不正当手段获取、披露、使用或者允许他人使用权利人商业秘密等传统问题,才是真正的商业秘密保护问题。

参考文献

[1] 刁胜先. 我国的版权法治建设的问题与建议—以云计算为主要视角[J]. 中国软科学,2013,(1).

[2] 宋凯. 中国移动云计算的发展探索[J]. 电信技术,2011,(10).

[3] 吴绍忠,李靖. 基于云计算架构的公安情报信息平台建设研究[J]. 中国人民公安大学学报(自然科学版),2010,(3).

[4] 李秀娟. 从专利保护规则看多方参与云计算专利[J]. 电子知识产权,2011,(12).

[5] 梁志文. 云计算,技术中立与版权责任[J]. 法学,2011,(3).

[6] 张耕,黄细江. 略论云计算环境下的著作权保护[J]. 法学杂志,2013,(1).

[7] Evelyn Brown. Final Version of NIST Cloud Computing Definition Published — From NIST Tech Beat[EB/OL]. http://www.nist.gov/itl/csd/cloud-102511.cfm[2011-10-25].

[8] 陆建伟. 云计算网络资源调度难点分析及解决方案[J]. 科技信息,2011,(15).

[9] 周奇. 云计算技术专利保护初探[J]. 电子知识产权,2012,(12).

[10] 罗迪. 云计算环境下的数字图书馆信息安全研究[J]. 科技文献信息管理,2011,(1).

[11] 许四平. SaaS 软件即服务模型研究[J]. 硅谷,2009,(2).

[12] 周剑,张明新. 云计算平台即服务 PaaS 架构研究与设计[J]. 常熟理工学院学报,2012,(8).

[13] 彭强,魏森. 对云计算知识产权保护的思考[J]. 电子知识产权,2011,(12).

[14] 吕卫锋. 云时代的数据即服务[J]. 中国制造业信息化,2012,(18).

[15] 李爱国,原建伟. 云计算部署模式及应用类型研究[J]. 电子设计工程,2013,(1).

[16] 贾一苇,赵迪等. 美国联邦政府云计算战略[J]. 电子政务,2011,(7).

[17] 张逢喆. 公共云计算环境下用户数据的隐私性与安全性保护[D]. 复旦大学博士学位论文,2010.

[18] 夏荣. 云计算技术在电子数据取证领域的应用研究[J]. 信息网络安全,2011,(8).

[19] Christopher Soghoian. Caught in the Cloud—Privacy[J]. Encryption and Government Back Doors in the Web 2.0 Era. 8 J. on Telecomm. & High Tech. L. 359,(2010).

[20] 杨松城. 云计算环境下的专利保护问题[J]. 电子知识产权,2012,(12).

[21] 周平,王志鹏等. 美国政府云计算相关工作综述[J]. 信息技术与标准化,2011,(11).

[22] 冯晓青. 网络环境与企业商业秘密保护策略[J]. 重庆大学学报(社会科学版),2006,(5).

[23] 李莹. 试论我国网络环境下商业秘密的法律保护及立法完善[J]. 福建商业高等专科学校学报,2009,(3).

[24] 张玉瑞. 商业秘密法学[M]. 北京:中国法制出版社,1999.

[25] 周昕. 云计算时代的法律意义及网络信息安全法律对策研究[J]. 重庆邮电大学学报(社会科学版),2011,(4).

[26] 陈志. 论网络环境下的商业秘密法律保护[J]. 重庆工商大学学报(社会科学版),2004,(3).

[27] 刘替. 网络环境下侵犯商业秘密的法律保护[J]. 电子知识产权,2010,(2).

[28] 杜华玲. 网络环境下商业秘密的认定及侵权责任[J]. 潍坊学院学报,2006,(3).

[29] 王伟军,汪琳. 网络环境下企业的商业秘密保护[J]. 科技进步与对策,2002,(7).

[30] 胡春辉. 云计算安全风险与保护技术框架分析[J].

信息网络安全,2012,(7).
[31] 韦文广. 对网络条件下企业商业秘密的形式特点及保护途径的理性审视[J]. 广西教育学院学报,2004,(4).
[32] 古天安. 云计算与知识产权[J]. 电子知识产权,2012,(3).
[33] 周刚,麦永浩,等. 云计算应用对计算机取证技术的挑战和对策[J]. 警察技术,2011,(3).
[34] 丁秋峰,孙国梓. 云计算环境下取证技术研究[J]. 信息网络安全,2011,(11).
[35] Konstantinos K. Stylianou. An Evolutionary Study of Cloud Computing Services Privacy Terms[J]. 27 J. on Marshall J. Computer & Info. L. 593,(2010).
[36] 赵粮. 云计算七大安全威胁[EB/OL]. http://www.cnii.com.cn/internet/content/2011-06/16/content_885746.htm.
[37] 郭晶晶,张秀山等. 云计算及其安全性分析[J]. 信息与电脑,2012,(7).
[38] Jon Brodkin. Gartner: Seven Cloud—Computing Security Risks[EB/OL]. http://www.infoworld.com/d/security-central/gartner-seven-cloud-computing-security-risks-853[2008-07-02].
[39] 段翼真,王晓程,等. 云计算安全:概念、现状与关键技术[J]. 信息网络安全,2012,(8).
[40] 房晶,吴昊等. 云计算安全研究综述[J]. 电信科学,2010,(4).
[41] 李玮. 云计算安全问题研究与探讨[J]. 电信工程技术与标准化,2012,(4).
[42] 罗立. 网络背景下的商业秘密保护[J]. 华东政法学院学报,2006,(6).
[43] Joshua Gold. Protection in the Cloud: Risk Management and Insurance for Cloud Computing[J]. 12 J. on Internet Law. L. 15,(2012).
[44] 高富平. "云计算"的法律问题及其对策[J]. 法学杂志,2012,(6).
[45] 周铭川. 云服务用户商业秘密的法律保护[J]. 暨南学报(哲学社会科学版),2013,(4).
[46] 周铭川. 论刑法上商业秘密的构成特征[J]. 山西警官高等专科学校学报,2008,(1).
[47] 伍艳. 云计算环境下的知识产权问题初探[J]. 法制与经济,2013,(1).
[48] 唐春. 基于云计算模式特点的知识产权保护新问题探讨[J]. 电子知识产权,2011,(12).
[49] 罗先觉,尹锋林. 云计算对知识产权保护的若干影响[J]. 知识产权,2012,(4).

[责任编辑　李晶晶　责任校对　王治国]