云计算隐私保护法律的管辖权研究

弓永钦　钮贵芳

摘　要：云计算带来了个人数据经常性的跨境传输，给传统隐私保护法律的管辖权提出了空前的挑战。传统隐私法律管辖权主要遵循“属人”、“属地”以及“设备所在地”原则，而云计算给“属人”、“属地”、“设备所在地”原则的使用都带来了困惑，也不能很好地解决“二次传输”的问题。应根据云计算的特点设计新的隐私保护法律管辖权理论，以“属人”原则为主，改限制存储地点为限制向第三方披露，采取加密方式保护云计算中的个人数据。

关键词：云计算；隐私保护法律；管辖权

中图分类号：DF415　　**文献标识码：**A　　**文章编号：**1006-1894（2017）04-0071-09

一、云计算对传统法律管辖权的冲击

云计算服务是近几年兴起的一种以先进网络技术为基础的商业服务模式。“云”是对这种计算方式的隐喻，体现其飘忽不定的特性。云计算可以有效地利用位于世界各地的数据中心、同时调动数十万台电脑的运算能力、让客户可以随时随地上传并访问相关数据，省却了公司建立自有硬件设备的麻烦，极大地降低了客户享受网络服务的成本，因此受到了公司和个人的欢迎。

美国国家标准化及技术研究所（NIST）给云计算下的定义是“一种应客户需求、只需花费最低的管理成本、只需进行服务提供商之间最低程度的沟通就能够方便迅速地向客户提供可配置、可共享的计算资源（比如网络、服务器、存储空间、应用软件以及服务）的模式。”[①]该定义在国际上得到了广泛认可，比以往的定义更加清晰一些。

然而，云计算的特点却给网络隐私管辖权提出了空前的挑战。传统法律管辖权理论主要以地域和国籍为基础，对个人数据的跨境流动做出严格的限制，与这种新型的商务模式显得格格不入。如果隐私保护法律对云计算进行地域限制，会束缚它的服务功能和效果，有违云计算的内在特性；如果对其毫无限制，又会使频繁进行跨境传输的个人数据处于失控状态，不能有效保护数据主体的权益。云计算对传统的隐私管辖权理论提出了最严重的挑战。

作者简介：弓永钦，对外经济贸易大学国际商务研究中心，北京劳动保障职业学院副教授，博士，研究方向：全球数据隐私规则；钮贵芳，常州工程职业技术学院讲师，研究方向：国际商务。

① Badger, Lee, et al. Cloud Computing Synopsis and Recommendations [EB/OL].2012, http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf. (2016-03-22).

二、传统网络隐私保护法律的管辖权理论

（一）属地管辖理论

许多国家的网络隐私保护法律采取属地管辖原则，并且分为两种趋向：一种让经营者所在地法律具有管辖权，另一种让消费者所在地法律具有管辖权（王娟，2005）。前者对于经营者更有利一些，因为经营者了解本国法律，接受本国法律的管辖对其具有确定性；但是对于消费者可能产生不利影响，因为消费者不熟悉他国法律，不方便起诉，如果经营者所在国法律的隐私保护水平低于消费者所在国，则消费者不能很好地维护自己的权益。后者有利于消费者进行维权，但是给经营者带来了极大的风险，因为网络经营者的商品销往世界各国，就有可能受到任何国家法律的管辖，从而给经营者带来极大的不确定性和败诉的风险。

为了避免法律风险，网络经营者经常使用服务合同中的法院地选择条款来确定法律管辖范围，即消费者在购物前需选择争议管辖法院，通常是经营者所在地的法院。这样经营者就避免了遭受他国法律制裁的风险，而消费者通常为了享受网络服务不得不接受该约定。目前，各国法律大都承认法院地选择条款的合法性，美国法院已有相关判例存在，法院的判决并没有强调该条款必须显示双方当事人的共同自愿。2001年欧盟修订了于1968年订立的《布鲁塞尔关于民商事案件管辖权及判决执行的公约》（简称“《布鲁塞尔公约》”），规定消费者既可以在本国进行投诉，又承认了法院地选择条款的有效性，这样就平衡了网站和消费者的利益（朱萍，2002）。

（二）国籍管辖理论

除了属地管辖理论之外，传统法律还有另外一个重要的管辖原则，即属人管辖。早在中世纪时期，欧洲法律主要采用属人管辖原则，如果一个人犯了罪，不管他身在何处，只有其国籍所在国法律才对他具有管辖权。到了数字时代，个人数据是个人在网络中的存在形式，法律管辖权不再需要基于数据主体的国籍，而是基于个人数据本身。在属人管辖原则下，如果个人数据从一国输出到另一国，需继续受到输出国法律的管辖。比如，欧盟的企业把个人数据业务外包到美国企业，则欧盟个人数据保护法将其管辖范围拓展至该美国企业，如果该美国企业对个人数据保护不力，将接受欧盟法律的制裁。通过“属人”原则拓展法律的境外管辖权，经常会导致国家法律之间的冲突，这种冲突已经比较频繁，因为每个国家通常不愿意接受别国法律的境外管辖（Kuner，2013）。

1. 欧盟法律的规定

欧盟法律在对个人数据的保护方面确实体现了“属人”原则，但在事实上并不是直接对境外数据接收方实施管辖权，而是采取了迂回的方式。欧盟个人数据保护法指令（Directive95/46/EC）第25~26条对个人数据跨境流动的规定就是欧盟向境外拓展管辖权的方式。第25条规定欧盟的个人数据只能向欧盟认可为具有“充分保

护地位”的国家和地区传输，而这个地位的授予要经过对该国法律的严格评估，以保证符合欧盟法律的标准，这样变相地把欧盟隐私保护法律拓展到了数据接收国。第 26 条除外责任规定，欧盟的个人数据也可以向不具有“充分保护地位”但是却具有一定保障措施的国家和地区传输。欧盟认可的保障措施包括两种：一是双方需签订欧盟委员会颁布的《标准合同条款》（SCC，Standard Contractual Clauses），二是欧盟推出的针对跨国公司制定的《约束性公司规则》（BCR，Binding Corporate Rules）。两个保障措施都体现了欧盟的个人数据保护标准，而符合标准的境外接收方也就间接地接受了欧盟法律的管辖（弓永钦和王健，2015）。

2. 美国的长臂管辖原则

美国在法律管辖权方面推行长臂管辖原则（long arm jurisdiction），通过某种“最低限度接触（minimum contact）”即可对境外企业具有管辖权。“长臂原则”其实也是“属人”原则的一种体现，对侵害了本国居民权利但是从未在本国出现过的境外企业进行管辖。在电子商务领域，如果美国法律认为外国网站侵害了美国居民的个人数据权利，并达到了“最低限度接触”，则美国法律将对该外国网站具有管辖权。关于“最低限度接触”的判断标准，美国发明了“滑动标尺（slide scale）”理论，根据“接触”的程度来确定是否对境外企业具有管辖权。美国把境外网站分为 3 类：（1）被动型网站（passive sites），只在网站上公布商品信息，并没有指向某国的消费者；（2）互动型网站（interactive sites），用户可以与网站交换信息；（3）积极主动型网站（active sites），利用网络从事商业活动，并主动吸引消费者购物。美国法律一般不对被动型网站具有管辖权，对互动型网站是否管辖取决于互动的程度和目的，而对积极主动型网站则可以根据“长臂原则”对其行使管辖权（陈亚飞，2007）。

（三）设备所在地管辖理论

如果说“属人”和“属地”原则是传统法律管辖理论在网络经济时代的延伸，那么设备所在地管辖原则就是针对互联网时代而设立的。欧盟 1995 年颁布的《个人数据保护指令》第 4 条“适用法律”规定，如果数据控制者没有在欧盟区域成立公司，但是出于数据加工目的使用了欧盟区域内的设备，则欧盟法律对该控制者具有管辖权，仅出于传输目的而使用设备的情况除外。①

根据我国《民事诉讼法》的规定，对个人数据侵权案件既可以采取设备所在地管辖，也可以采取被侵权人所在地管辖。2015 年 2 月 4 日起施行的《最高人民法院关于适用〈中华人民共和国民事诉讼法〉的解释》第 24 条规定：民事诉讼法第 28 条规定的侵权行为地，包括侵权行为实施地、侵权结果发生地。在该解释中，针对

① EU Data Protection Directive (1995), Article 4.

日益活跃的信息网络，还专门就侵权行为实施地以及侵权结果发生地进行了更为具体明确的界定。该解释第 25 条规定：信息网络侵权行为实施地包括实施被诉侵权行为的计算机等信息设备所在地，侵权结果发生地包括被侵权人住所地。也就是说，被侵权人住所地（原告所在地）法律可以管辖。

三、云计算隐私保护法律管辖权的困惑

（一）涉案地点判断的困惑

云计算天生不受地域的限制，服务提供商、用户、数据主体和服务器都可能分属不同的国家，而各国隐私保护法律的管辖权又通常以国界为限，因此给法律管辖权的适用造成了不少困惑。以一个情境为例，一个澳大利亚公民把其个人数据上传到一个美国云服务提供商的云端。那么哪国法律应该对存储在云端的个人数据具有管辖权？可能有几种选择：（1）澳大利亚法律，因为数据主体是澳大利亚公民；（2）美国法律，因为云服务提供商是美国企业；（3）上传或访问个人数据的地点，也许该澳大利亚公民正在欧洲旅游时访问了自己的邮箱；（4）存储该数据的数据中心所在地；（5）根据数据主体投诉的性质来定，如果属于侵权案件，则适用侵权行为所在地法律（Gray，2013）。一个简单的云服务案例可以涉及 5~6 个地点，包含至少 3 个国家，而且有的地点很难确定，比如侵权行为发生地和数据中心所在地。相比较，数据主体和云服务商的国籍非常明确，如果用“属人”原则来确定云计算的法律管辖权要比“属地”原则更加明确和简单。

（二）合同管辖权的困惑

数据主体在使用云服务之前一般都会与服务提供商签订服务合同（由服务提供商写好的统一合同），其实就是通过点击同意而达成协议。合同是由服务提供商所写，通常要求消费者同意争议管辖法院为服务商所在国法律。很多云服务用户在使用云服务前并不仔细阅读合同条款就选择了同意，原因有二：其一，合同条款冗长，一般用户没有耐心和专业知识把它完全研究清楚；其二，如果不选择同意合同条款，用户就不能使用云服务，因此很多用户只能被迫接受服务提供商的服务合同。《布鲁塞尔公约》、《罗马条例 I》[①]以及美国判例都承认了法院地选择条款的合法性。如果合同中没有写明争议管辖法院，《罗马条例 I》第 6 条规定，合同受用户常规居住地法律管辖，服务提供商应遵守用户居住地的强制性法律。根据《罗马条例 I》的规定，云计算隐私保护案件既有可能受服务提供商所在地法律管辖，又有可能受用户所在地法律管辖，可见法律界对于到底让网络服务提供商所在地还是消费者所在

① European Parliament and the Council Regulation (EC) No598/2008 on the Law Applicable to Contractual Obligations (17/6/2009) (Rome I).

地法院管辖还没有一个清楚的指向。

（三）属人管辖原则的困惑

2013 年 12 月，美国政府依据《1986 年电子通讯隐私法案》（ECPA）向微软公司发出搜查令，要求微软公司提供某美国公民在爱尔兰都柏林云服务器上存储的邮件信息。微软公司拒绝了这一要求，认为该邮箱服务是爱尔兰地区专属的，该美国公民邮件来往对象主要是爱尔兰居民，美国政府无权获得爱尔兰居民的个人数据，而应向爱尔兰政府请求协助。美国政府则认为微软公司的注册地在美国，有义务协助美国政府进行某美国公民的调查。而欧盟认为微软公司在欧盟提供服务需遵守欧盟个人数据保护法律，不能把欧盟居民的个人数据传输给美国政府。微软公司在两国法律夹击下无所适从，该案件轰动一时，把云计算的隐私法律管辖权问题推到了风口浪尖（Svantesson，2015）。

微软公司向美国法庭提出辩护后，至少有 12 个非当事人意见陈述支持微软公司，其中包括苹果、亚马逊和 AT&T 等跨国公司，国际法和计算机科学领域的学者，爱尔兰的公共利益组织，爱尔兰政府以及欧盟议会成员。可见，对此案的主流意见是美国政府没有权利向跨国公司索取别国公民的个人数据。

微软公司的首席法律官 Brad Smith 于 2015 年 10 月在博客上发表了关于美国政府向云服务商索取个人数据行为的意见[①]：美国和欧盟都应该对本国居民的数据具有管辖权。如果美国想从美国的云服务商那里获取欧盟居民的个人信息，则应遵守欧盟法律；反之，如果欧盟想从美国的云服务商获取美国公民的个人信息，也应遵守美国法律。Brad Smith 建议美欧双方签订新的“跨大西洋协议”，就个人数据的跨境管辖权达成一致，以保护双方公民的数据权益以及跨国公司的经营权利。Brad Smith 批驳了美国政府向云服务商索取他国居民信息的行为，认为它侵犯了服务地用户的权益，影响了美国云服务商的声誉。现在很多企业客户由于害怕美国政府向云服务商索取个人数据，都不愿意选择美国企业的云计算服务。他建议美国政府应该直接向当地相关企业索要信息，而不要向云服务商索要；两国政府间可以建立双边法律协助机制（legal mechanism of mutual assistance），以减少法律冲突。Brad Smith 的建议其实对解决云计算的法律管辖权问题具有很大的启示意义。

（四）设备所在地管辖原则的困惑

欧盟《个人数据保护指令》第 4 条“适用法律”规定，如果境外企业出于数据加工目的使用了欧盟区域内的设备，则欧盟法律对该控制者具有管辖权，仅出于传输目的而使用设备的情况除外。在云计算的法律管辖权问题中，该规定也受到了质疑。

① Armasu, Lucian. Microsoft Deems Privacy A Fundamental Right, Asks E.U. and U.S. Governments to Obey It[EB/OL]. 2015, http://www.tomshardware.com/news/microsoft-privacy-rights-safe-harbor,30379.html.[2015-10-02](2017-03-22).

比如一个美国企业雇佣了一个美国云服务提供商为其加工美国的消费者或者员工数据，该美国云服务商在加工数据时使用了法国境内的云服务器，当该云服务商要把加工后的数据从法国转移到美国时还需要取得法国的同意吗？显然不合情理。因此，指令第 4 条应该加上一个限定条件“使用欧盟设备并且与欧盟个人数据相关”。云计算的优势就是整合世界各地的计算资源，出于方便与节省成本考虑会重复跨越国境，法律不应该对这种特殊的服务模式构成不必要的限制。

为了适应云计算这种新型的商务模式，法国数据保护当局（CNIL）已签署决定，把在提供云服务过程中使用法国设备加工境外个人数据的情况作为法律管辖的例外，加工后的数据向境外传输可不受法国个人数据保护法律约束。事实上，法国法律也不愿意为保护美国公民的个人数据而消耗自己有限的法律资源，只是因为云计算这种新的商务模式通过指令第 4 条使得法国“被动”地获得了管辖权。但是为了享受这个特权，云服务商需要指定一家法国企业作为它的代表，对该云服务商遵守法国的数据安全要求负责（King and Raja, 2012）。其他欧盟国家也做出了类似的规定，减少了云计算的法律壁垒。

（五）二次传输管辖权的困惑

这里的二次传输（onward transfer）指的是 A 国把个人数据合法地传输给 B 国，B 国又把同样的个人数据传输给 C 国；A 国对数据接收国的要求严格，要求 B 国必须具备与之对等的个人数据保护法律，而 B 国对数据接收国的要求没有那么严格，那么如何保证 A 国居民的数据在 C 国仍然是安全的？欧盟个人数据保护指令对于保护本国居民的个人数据设置了严密的防护措施，第 25 条和第 26 条对数据接收国或接收企业的条件进行了严格的限制，但是却没有解决二次传输的个人数据保护问题。比如欧盟认为处于“安全港”之外的美国企业都不具有“充分的个人数据保护水平”，如果欧盟企业想使用“安全港”之外 D 公司（美国）的云计算服务就违反了欧盟指令。但是，如果欧盟企业把个人数据传输给 D 公司在加拿大的子公司（加拿大具有欧盟认可的“充分数据隐私保护地位”），再由子公司传给 D 公司（欧盟不认可具有“充分保护水平”）就可以成功地绕过欧盟的法律壁垒。这是欧盟指令的一个漏洞，在实际操作中也存在不少这样迂回的方式（Esayas，2012）。欧盟还能对二次传输的个人数据具有管辖权吗？如果有，可是欧盟只能选择一次传输的数据接收方，而无法干涉二次传输的流向；如果没有，可是二次传输的个人数据还是欧盟的数据。因此，探讨云计算隐私保护法律的管辖权问题还应该考虑到二次传输的问题。

四、云计算隐私保护法律管辖权的思考

云计算服务是网络经济时代由于新技术的应用而产生的一种新型的商务模式，它的出现给各国隐私保护法律提出了空前的挑战，因为以前从来没有出现过这样随

时随地、反复跨越国界的商务模式。然而，法律不适应并不是云计算的错误，作为上层建筑的法律应该随着经济和技术的发展而变化。因此，隐私保护法律的改良也好，重建也罢，都不应当成为云计算发展的障碍，必须平衡商务模式的发展与个人数据保护之间的利益。本文建议云计算隐私保护法律管辖权应遵循以下几个原则。

（一）以属人管辖原则为主

从前面的分析可以看出，属地管辖原则不适应云计算的特点。如果法律限制个人数据的跨境流动，会大大降低云计算的活力和效率，与传统的物理设备加工存储没什么区别了。而且属地管辖原则对于解决前面提到的“二次传输”、“设备所在地”、“境外管辖”等新问题都显得力不从心。

相反，经过进化的属人管辖原则——根据数据主体的国籍来确定法律管辖权，还能抓住云计算的脉搏。就像微软首席法律官提出的建议一样，各国法律管辖本国公民和居民的数据，如果涉及到别国居民数据，需与该国政府进行协商，建立双边法律协助机制。在属人管辖原则下，欧盟对欧盟居民的个人数据具有管辖权，如果境外云服务商或者在本地注册经营的云服务商侵害了欧盟居民的个人数据（数据泄露、不经数据主体同意向第三方披露等等），则数据主体可以行使属地管辖权，向本国数据保护当局（DPA）起诉该云服务商。DPA 对该云服务商行使管辖权，对其采取调查、罚款、责令赔偿及禁令等法律措施；如果该云服务商拒绝伏法，则 DPA 有权将其逐出欧盟区域。

属人管辖原则可以很好地解决“二次传输”和“设备所在地”的难题。根据该原则，欧盟法律对进行“二次传输”的欧盟个人数据始终拥有管辖权；对使用欧盟设备但不涉及欧盟居民数据的云服务不具有管辖权。另外，在处理类似美国政府向微软索要美国公民在欧盟区域的邮箱信息案件时，也可以遵循该原则，如果单纯索要美国公民信息的话，云服务商可以提供；如果涉及欧盟居民信息，就需要与欧盟政府协商，取得法律协助。该案中，美国向微软索要存储在欧盟区域电子邮箱中某个美国居民的信息本来是合法的，但是由于与该美国公民邮件往来的对象大多是欧盟居民，如果把往来邮件交给美国政府就会泄漏欧盟居民的个人数据。因此，美国对此案只具有部分管辖权，需要取得欧盟的协助。

（二）改限制存储地点为限制向第三方披露

不少国家出于对云计算不易掌控的担忧，要求云服务商把本国居民数据留在本国的云服务器上，禁止输出境外。这个举措虽然加强了对本国居民数据的保护，但是却降低了云计算的活力，限制了它的功能。如果个人数据只能留在国内，那么该国居民在国外工作、旅游时就无法访问自己的邮箱，无法登陆自己的微信、脸书，云计算的优势就会荡然无存。同时，云服务商也不愿意把数据固定在一国的数据中心，为了方便提供服务、分散数据中心的压力、降低成本以及减少数据丢失的风险，

云服务商通常会在几个数据中心对同一份个人数据进行复制、镜像。即使云服务商同意用户选择将其个人数据留在国内，谁又有能力对云服务商的行为进行监管而保证它真的不会将个人数据输出到国外呢（Svantesson and Clarke，2010）？其实个人数据无论存储在哪个国家的数据中心都没有关系，只要还在这个云服务提供商的服务器中就是安全的。根据属人管辖原则，数据主体所在国法律对持有个人数据的云服务商具有管辖权，而监管一个云服务商比监管同一个国家的多个数据控制者要容易一些。既然限制国界不适合云计算，不如改为限制云服务商的行为，令其对存储的个人数据的安全全权负责，不得未经数据主体同意向第三方披露。当然，如何确保云服务商不私自向第三方披露个人数据也是个难题，除了通过数据主体的投诉和数据主体所在国 DPA 的隐私保护合规审计以外，还可以在云服务商的准入方面加强审核。审核标准可以包括该云服务商是否通过了权威的隐私保护标准认证，是否加入了某种具有约束力的规则体系，比如安全港、BCR 及 CBPR 等；较高的入门标准可以减少云服务商违规操作的风险。

（三）要求云服务商对个人数据做加密处理

数据主体所在国应允许云服务提供商跨境传输个人数据，因为这样符合云计算的特点，但是又担心公民数据难以得到应有的保护。在这种情况下，数据主体所在国可以要求云服务商对个人数据进行加密后再向境外传输，而各国隐私保护法律通常不会对加密后的个人数据实施限制。这就意味着，云服务商可以把加密后的个人数据传输到不具有“充分保护水平”的国家和地区的服务器或数据中心，真正实现云计算的优势和功能（King and Raja, 2012）。这是一种技术与法律结合的理想状态，前提是加密技术在确保个人数据安全的同时又不会阻碍云计算的功能实现。近年来，属性加密、同态加密、同态签名及消息验证码、非交互可验证计算等功能加密技术被应用于云计算的外包业务中。随着加密技术的不断改进，有望实现技术对隐私保护法律的辅助功能（陈克非和翁健，2004）。

五、我国隐私保护法律管辖权的现状与对策

我国在隐私保护立法方面处于比较落后的水平，至今仍未颁布一部全国性的个人数据保护法律，而世界上已经有 90 多个主权国家进行了相关立法。其中，欧盟地区的隐私保护法律建设最为成熟，近年来已经开始利用法律武器对外国网络公司（尤其是美国的网络企业）进行制裁，首当其冲的是谷歌和脸书。而我国还没有一部全面的、具有较好执行效力的隐私保护法律，不能像欧盟国家那样保护本国居民的数据隐私，对于处理外国数字企业个人数据跨境流动问题以及中国企业如何应对外国隐私保护法律监管问题，还没有一个统一的规范。显然，我国法律还没有深入地探讨有关个人数据保护法律的涉外管辖权问题。

在没有得力的法律武器之前，我国对外国云计算服务商采取的是监管政策，要求它们在我国建立数据中心，向我国主管部门备案业务数据，限制居民数据的境外传输。有的云服务商如雅虎、谷歌、微软等公司拒绝在中国大陆建立数据中心或者不愿意向中国政府提供业务数据，只好被迫放弃中国市场（弓永钦和王健，2016），我国居民和企业也因此而得不到优质的云服务。

我国目前还没有针对数据隐私保护法律的管辖权理论，但是从《民事诉讼法》来看，我国倾向于使用的网络管辖权原则是设备所在地管辖和属地管辖。如前所述，这两个原则对于云计算来说都不太适合，很多时候会显得力不从心。属人管辖原则最有利于保护居民数据隐私，又能够保护云计算的活力，但是前提是我国需拥有一部比较完善的隐私保护法律，并且就管辖权问题与其他国家达成协议，建立法律互助机制。

参考文献：

[1] 陈克非, 翁健. 云计算环境下数据安全与隐私保护[J]. 杭州师范大学学报(自然科学版), 2014, (11).

[2] 陈亚飞. 美国网络侵权管辖权的实践及启示[J]. 浙江学刊, 2007,(6).

[3] 弓永钦, 王健. APEC与欧盟个人数据跨境流动规则的研究[J]. 亚太经济, 2015,(5).

[4] 弓永钦, 王健. TPP电子商务条款解读以及中国的差距[J]. 亚太经济, 2016,(3).

[5] 王娟. 对确认网络管辖权的探讨[J]. 河北法学, 2005,(5).

[6] 朱萍. 虚拟空间管辖权的确定——美国和欧盟实践的启示[J]. 法商研究, 2002,(4).

[7] Esayas, Samson. A Walk into the Cloud and Cloudy It Remains: The Challenges and Prospects of Processing and Transferring Personal Data[J]. Computer Law & Security Review, 2012, 28.

[8] Gray, Anthony. Conflict of Laws and the Cloud[J]. Computer Law & Security Review, 2013, 29.

[9] King, Nancy, Raja, V. Protecting the Privacy and Security of Sensitive Customer Data in the Cloud[J]. Computer Law & Security Review Law, 2012, 28.

[10] Kuner, Christopher. Transborder Data Flows and Data Privacy Law[M]. Croydon: Oxford University Press, 2013.

[11] Svantesson, Dan, et al. Access to Extraterritorial Evidence: The Microsoft Cloud Case and Beyond[J]. Computer Law & Security Review, 2015, 29.

[12] Svantesson, Dan, Clarke, Roger. Privacy and Consumer Risks in Cloud Computing[J]. Computer Law & Review, 2010, 26.

Study on Jurisdiction of Privacy Laws Concerning Cloud Computing

GONG Yong-qin　NIU Gui-fang

Abstract: Cloud computing brings frequent cross-border transfer of personal data, which challenges jurisdiction of traditional privacy laws. Traditional jurisdiction is based on nationality, territory and location of equipment, but cloud computing causes puzzlement to adoption of those principles and cannot well solve the problems like "onward transfer". A new jurisdiction theory should be established according to characteristics of cloud computing, preferring nationality to territory, changing restriction on place of storage to that of illegal disclosure to the third party, and adopt encryption of the personal data in cloud computing.

Key words: cloud computing; privacy laws; jurisdiction

（责任编辑：金孝柏）