互联网治理与法律研究

丛书主编　李欲晓

个人信息保护法研究

GEREN XINXI BAOHUFA YANJIU

崔聪聪　巩姗姗　李仪　杨晓波　王融　何培育　著

北京邮电大学出版社
www.buptpress.com

互联网治理与法律研究

丛书主编　李欲晓

个人信息保护法研究

崔聪聪　巩姗姗　李　仪
杨晓波　王　融　何培育　著

北京邮电大学出版社
www.buptpress.com

内 容 简 介

本书从个人信息在大数据时代所面临的威胁着手，通过梳理国外个人信息保护立法的最新趋势，提出以个人信息控制权为核心，使个人信息保护理念由重归属向重应用转变，设置科学的个人信息损害赔偿机制和技术保护机制，以实现个人信息安全和网络产业发展之间的平衡。

本书可供立法机关工作人员、互联网监管机构工作人员和网络信息安全从业者参考使用，并可作为法学、信息安全、计算机网络、信息系统工程等专业的本科高年级或研究生的参考用书。

图书在版编目(CIP)数据

个人信息保护法研究 / 崔聪聪等著. -- 北京：北京邮电大学出版社，2015.10
ISBN 978-7-5635-4223-9

Ⅰ. ①个… Ⅱ. ①崔… Ⅲ. ①隐私权—法律保护—研究—中国 Ⅳ. ①D923.04

中国版本图书馆 CIP 数据核字(2014)第 277877 号

书　　名：个人信息保护法研究
著作责任者：崔聪聪　巩姗姗　李仪　杨晓波　王融　何培育　著
责 任 编 辑：王琴秋
出 版 发 行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号(邮编：100876)
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京鑫丰华彩印有限公司
开　　本：720 mm×1 000 mm　1/16
印　　张：11.25
字　　数：226 千字
版　　次：2015 年 10 月第 1 版　2015 年 10 月第 1 次印刷

ISBN 978-7-5635-4223-9　　定　价：29.80 元

前　言

大数据时代，个人信息已成为国家的战略资源，个人信息控制权也因此成为网民在网络时代的基本权利。大数据虽然赋予了我们洞察未来的能力，但分散和分布式网络环境给个人信息保护带来了新的挑战，大量的个人信息不仅可能在今天被滥用，在几年甚至几十年后仍然可能被滥用。因此，迫切需要现行个人信息保护立法做出调整，以应对日益严峻的数据安全问题。

中国目前尚无形式意义的个人信息保护法，有关个人信息保护的法律规范散见于《刑法》《消费者权益保护法》和《居民身份证法》等法律中。本书通过梳理个人信息在大数据时代所面临的安全威胁，总结国外个人信息立法的最新趋势，分析我国现行个人信息保护立法的不足，提出完善我国信息保护立法的建议，期冀能够为中国出台形式意义上的个人信息保护法提供支撑。

本书分为7章。第一章向读者介绍云计算、物联网、移动互联网等网络新技术和新应用对个人信息保护提出的挑战。第二章和第三章介绍域外个人信息保护立法及其最新立法趋势。第四章厘清了个人信息控制权的法律属性为人格权，并阐述了个人信息控制权的内容。第五章分析了个人信息再利用的风险及其安全保障机制。第六章介绍了经规划的隐私保护机制(Privacy by Design)及其对中国的启示。第七章提出应从实体和程序两个层面完善我国个人信息损害赔偿机制。

本书是中国博士后科学基金“大数据时代个人网上行为信息安全的法律保障”(编号：2013M541499)的阶段成果，同时受国家出版基金资助，在此表示感谢。

本书各章撰写分工如下：

第一章、第六章由北京邮电大学互联网治理与法律研究中心研究人员杨

晓波编写；第二章由重庆理工大学知识产权学院副教授、法学博士何培育编写；第三章由中国信息通信研究院政策与经济研究所法律研究部副主任王融编写；第四章及第五章第一、三节由重庆三峡学院副教授、法学博士李仪编写；第五章第二节、第七章由华东政法大学博士后研究人员、北京邮电大学互联网治理与法律研究中心副教授崔聪聪与石家庄经济学院法政学院讲师、法学博士巩姗姗编写。

目　录

第一章　相关技术场景下的个人信息安全风险

云计算、物联网、移动互联网以及大数据技术是时下信息技术产业最前沿和最具发展潜力的几个方向。互联网作为20世纪最伟大的发明之一，改变了人类社会生活的各个方面。云计算、物联网和移动互联网等的发展，是对传统互联网的一次变革。云计算将改变互联网的技术基础，甚至会影响整个产业格局；物联网让传统的人与人之间的互联拓展到人与物、物与物之间的互联，世界信息产业发展的第三次浪潮正在进行；移动互联网将移动通信与互联网相结合，正在逐步渗透到人们生活、工作的各个领域。中国国民经济和社会发展第十二个五年规划中也将云计算、物联网和移动互联网等新一代信息技术作为重要的领域和方向进行发展。但是，上述技术的发展也可能对个人用户的信息安全带来威胁，这些威胁有许多是在传统互联网环境中所不存在的。因此，我们在此对这几个信息技术场景中的个人信息安全风险进行分析，并借此挖掘中国信息技术环境下个人信息保护方面存在的问题。

第一节　云计算场景

云计算（Cloud Computing），是对基于网络的、可配置的共享资源计算池能够方便地、随需访问的一种模式。这些可配置的共享资源计算池包括网络、服务器、存储、应用和服务。[①] 其最终目标是将计算、信息服务和应用作为一种公共设施提供给公众，使人们能够像使用水、电、煤气和电话那样使用网络信息资源。[②] 作为一种新型的应用模式，云计算自诞生以来就备受国际关注，近年来更是被视为新一代信息技术变革和商业模式变革的核心。咨询机构Gartner发布的报告显示，2013年全球最终用户的公共云服务开支达到1310亿美元；而到2015年，公共云

① 雷万云，朱近之，薛峰等．云计算：技术、平台及应用案例［M］．北京：清华大学出版社，2012：7.

② 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），2011，23（4）：39-47.

服务市场规模将超过 1800 亿美元。[①]

一、中国云计算发展现状

在国家产业政策扶持方面，2010 年 10 月国家发改委联合工业和信息化部印发了《关于做好云计算服务创新发展试点示范工作的通知》，确定在北京、上海、深圳、杭州、无锡五个城市先行开展云计算服务创新发展试点示范工作。短短几年间，中国云计算产业发展迅猛，北京和上海先后推出了“祥云工程”和“云海计划”，各地也纷纷建立起云计算基地和云计算产业中心。同时，中国的“十二五”规划中也将云计算列为新一代信息技术产业的重点领域和战略性新兴产业，并将重点推进云计算技术研发的产业化。国家发改委、工信部、财政部等部委带头扶持云计算产业发展。

在发展规模方面，从 2009 年到 2012 年，云计算的市场规模从 92.23 亿元增长到了 606.78 亿元。而根据赛迪智库提供的数据，到 2013 年，云计算市场规模达到 1 174 亿元。[②] 但是中国云计算市场在世界范围内所占的比例只有 3%。[③]

在发展特点方面，中国云计算主要呈现出以下六个特点：（1）处于应用的初级阶段，云计算技术与设备已经具备一定的发展基础。（2）大型互联网企业是目前中国主要的云计算服务提供商，业务形式以 IaaS（Infrastructure as a Service，云基础设施即服务）加 PaaS（Platform as a Service，平台即服务）形式的开放平台服务为主，其中 PaaS 服务相对较为成熟，其服务初具雏形。（3）信息通信技术制造商在云计算专用服务器、存储设备以及企业私有云解决方案的技术研发上具备了相当的实力。（4）软件厂商逐渐转向云计算领域，开始提供 SaaS（Software as a Service，软件即服务）服务，并向 PaaS 领域扩展。（5）电信运营商依托网络和数据中心的优势，主要通过 IaaS 服务进入云计算市场。（6）互联网数据公司依托自己的机房和数据中心，将 IaaS 作为云服务切入点，目前已能提供弹性计算、存储与网络资源等 IaaS 服务。[④]

在具体应用方面，中国目前云计算服务有：电子商务云、中小企业云、医疗

---

① Gartner. 预计 2015 年公共云市场规模将超 1800 亿[EB/OL].(2013-12-14)[2013-12-18]http://www.cniteyes.com/saas/2013/1214/104571.html.

② 赛迪顾问.2013 年云计算市场规模将达 1174 亿元 [EB/OL]. (2012-02-16)[2013-04-20] http://www.eeo.com.cn/2012/0216/220889.shtml.

③ 周文，井明洋，等. 中国云计算产业结构和商业模式 [J]. 上海大学学报（自然科学版），2013，19 (1)：26-30.

④ 工业和信息化部电信研究院. 云计算白皮书 2012 [R/OL]. (2013-04：9-11) [2013-06-27] http://www.catr.cn/kxyj/qwfb/bps/201212/P020121204616814780528.pdf.

云、教育云等 SaaS，应用引擎等 PaaS，存储云、虚拟机租用服务等 IaaS。[①]

二、云计算与个人信息安全风险

虽然云计算的应用和推广在如火如荼进行，但从诞生开始，云计算的安全就一直是各方担心的问题。当所有的计算行为和数据存储都散布在虚无缥缈的“云”中时，人们会产生云是否会泄露自己的个人信息、损害自己权益的质疑。云计算中的数据安全、平台稳定性以及传统网络安全问题在云计算场景中的蔓延等，都成为阻碍云计算快速发展的重要因素。

自云计算服务出现以来，发生的大量安全事件已经引起了各界的广泛关注。2011 年 3 月，谷歌邮箱发生大规模用户信息泄露事件，约 15 万 Gmail 用户受到影响。2011 年 4 月，由于 EC2 业务的漏洞和缺陷，亚马逊公司爆出了史前最大的云计算数据中心宕机事件。同月，黑客利用亚马逊 EC2 云计算服务，对索尼 PlayStation 网站进行了攻击，造成了用户信息大规模泄露。[②] 2012 年 8 月，盛大云服务器因磁盘损坏而导致部分用户的个人信息丢失。[③]

目前已有许多研究组织或机构对云计算场景中的个人信息安全风险进行了体系性的研究。如美国国家标准技术研究所（National Institute of Standards and Technology，NIST）就对公有云面临的安全与隐私问题进行了分析，其发现的威胁涉及应急响应、架构、身份管理与访问控制、软件隔离、数据保护、管治、合规、信任、可用性 9 个方面（如图 1.1 所示）。云安全联盟（Cloud Security Aliance，CSA）从对云的不良使用、不安全接口与 API、恶意的内部人员、共享技术问题、信息泄露与丢失、账户或服务劫持、未知的风险 7 个方面分别对 IaaS、PaaS 和 IaaS 进行了分析（如表 1.1 所示）。咨询机构 Gartner 则认为，云计算中的安全风险包括 7 类：特权用户接入、可审查性、数据位置、数据隔离、数据恢复、调查支持、长期生存性。[④]

---

① 中国电子技术标准化研究院．云计算标准化白皮书 2012[R/OL].(2012-08-27:30-31)[2013-06-27] http://cesi.gov.cn/cesi/guanwanglanmu/biaozhunhuayanjiu/2012/0827/10153.html.

② 工业和信息化部电信研究院．云计算白皮书 2012[R/OL].(2013-04:9-11)[2013-06-27] http://www.catr.cn/kxyj/qwfb/bps/201212/P020121204616814780528.pdf.

③ 仲浩．盛大云致数据丢失用户：谁让你在云主机之外不做备份的？[EB/OL].CSDN 资讯,(2012-08-07)[2013-04-03] http://www.csdn.net/article/2012-08-07/2808269.

④ Gartner. 云计算技术存在的七大风险分析[EB/OL]. 凤凰网,(2010-12-03)[2013-04-22]http://tech.ifeng.com/it/special/cloud-computing/content-4/detail_2010_12/03/3342519_0.shtml.

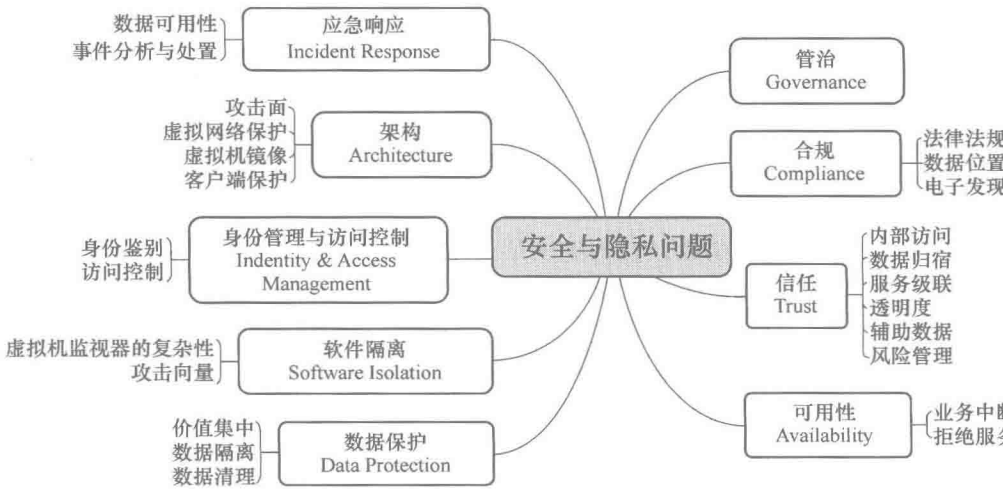

图 1.1 美国 NIST 列出的公有云面临的隐私和安全问题

表 1.1 CSA 对云计算安全的分析

安全威胁	云计算服务模型		
	IaaS	PaaS	SaaS
对云的不良使用	√	√	×
不安全的接口与 API	√	√	√
恶意的内部人员	√	√	√
共享技术问题	√	×	×
信息泄露与丢失	√	√	√
账户或服务劫持	√	√	√
未知的风险	√	√	√

云安全包含多个方面的内容，个人信息安全只是其中一个比较重要的部分。我们认为，虽然上述各种类型的威胁也会涉及个人信息安全，但云计算场景中个人信息问题的关键在于用户数据的安全。在用户将数据托管给云服务商后，实际的数据控制权转移，对数据享有优先访问权的不是用户，而是云服务商。这种控制权旁落的状况无疑会对个人信息安全构成极大风险。[①] 云中数据可以分为静态数据和动态数据，而个人信息正包含于这些数据类型中。对云计算场景中的个人信

① 云计算安全政策与法律工作组．中国云计算安全政策与法律蓝皮书［R］．西安：西安交通大学信息安全法律研究中心，2012-10-12：28.

息安全风险的分析可以参考数据安全的思路，从网络结构分层、管理制度等角度去分别论述（如图 1.2 所示）。国际标准化组织提出了 OSI 模型，将网络分为七层：物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。其中，物理层面会涉及数据是如何存储和保护的；网络和传输层面事关数据在网络中的传输安全；应用层面与数据的处理密切相关。因此，这里主要对这几个层面中的个人信息安全风险进行分析。此外，对数据管理不当也可能导致用户个人信息泄露，所以也将数据管理作为一项独立的内容进行分析。

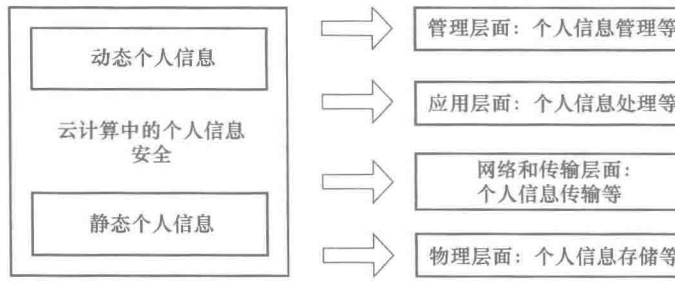

图 1.2 云计算场景中的个人信息安全分析思路

三、物理层面的个人信息安全风险

云计算物理层面的个人信息安全风险主要来自云服务器的物理环境、个人信息存储、个人信息销毁、个人信息恢复等几个方面。物理层面的个人信息安全主要是指静态个人信息的安全。

（一）云服务器的物理环境安全隐患

用户的各类个人信息都被存放于云端，云端并非虚无缥缈之概念，而是实际之物——云服务器。云服务器放置环境的安全（免于自然灾害、人为破坏等）是云计算安全最基本的保障，只有建立在环境安全的基础之上，才有可能对其他的安全风险进行分析。

（二）个人信息存储位置具有不确定性[①]

与传统的信息服务相比，云计算中数据的流动更具有灵活性且更难以控制，用户无法得知其个人信息确定的存放位置，甚至在多个数据中心的情况下，云服务提供商也无法获知某一特定时刻个人信息存储的具体位置，这显然对用户是十分不利的。同时，云内数据存储的这种特点将可能带来法律适用上的冲突，从而给利益相关者带来不利的法律后果。如由于文化、制度等的不同，当事人的一则

① 云计算安全政策与法律工作组．中国云计算安全政策与法律蓝皮书［R］．西安：西安交通大学信息安全法律研究中心，2012-10-12：28-31.

信息在本国属于个人信息法律保护的内容；而它存放在外国的云服务器上，根据该外国法律，这一信息不属于法律保护范畴，于是，法律冲突问题随之产生。

此外，在多用户共享资源的情况下，云内个人信息安全风险往往与 API、IP 动态分配、资源共享等技术特征相关，云服务商通常将用户数据集中存储，缺乏数据隔离措施和安全的 API 控制，很可能产生个人信息混同和个人信息丢失情况。技术云服务商承诺数据是安全可靠的，但对于用户而言，目前缺乏有效的声明或审计证实这种可靠性的存在。这些都将不利于用户的个人信息保护。

因此，对个人信息的加密存储是非常重要的，CSDN 泄密事件就充分反映了这一点。如果对云内数据采用明文存储的形式，那么用户个人信息泄露的风险将成倍增加。

（三）个人信息销毁存在不彻底性[①]

对于不用的或使用目的达成的个人信息，应当尽早删除并销毁。这种销毁应当是彻底的、有效的。但是，个人信息销毁的具体方法，目前并不一致。简单的删除操作仅仅是将个人信息占用的空间标记为可用，即便是空间被其他数据覆写多次后，删除的个人信息依旧是可以恢复的。为实现个人信息销毁的目的，应当考虑物理销毁或其他措施，但这些措施通常是用户无法核实的。

云服务商为了提高服务的可靠性，需要对云内数据做多个备份，并且可能将这些备份数据分布在不同的服务器上。当用户要求云服务商删除其个人信息时，如果云服务商没有完全删除所有的数据及备份（如覆写失败、备份以往），个人信息的安全性便会受到威胁。

为满足协助执法的要求，各国法律通常会规定服务商的数据存留期限，并强制要求服务商提供明文的可用数据。但在实践中很少受到收集限制原则的约束，公权力与个人信息保护的冲突也是用户选择云服务需要考虑的风险点。

（四）物理性云故障将导致个人信息无法恢复

该点与前面提到的云内个人信息“难以销毁”并不矛盾。“难以销毁”是从用户主动希望删除之目的的实现出发，而“难以恢复”是站在用户主动希望恢复的角度。用户将数据存于云端，一般情况下不会将数据备份在本地，如果云端服务器发生物理性损毁，那么数据（包括其中的个人信息）将无法恢复。

四、网络和传输层面的个人信息安全风险

云计算网络和传输层面的个人信息安全风险主要来自中间人攻击、个人信息保密性、个人信息完整性、非授权接入、个人信息可用性等方面。网络层面的个

① 云计算安全政策与法律工作组．中国云计算安全政策与法律蓝皮书［R］．西安：西安交通大学信息安全法律研究中心，2012-10-12：31-32.

人信息安全主要指动态个人信息的安全。

（一）中间人攻击

在用户与云服务器进行数据交换的过程中，各个服务器节点和各层软件都可能存在中间人攻击的情形。攻击者同时在用户与服务器之间建立连接，并伪装成服务器与用户进行交互，伪装成用户与服务器交互，并且获得两端交互的私密信息，如密钥等。[①] 如此，就极有可能使个人信息落入中间攻击者手中，从而导致个人信息泄露的风险。

（二）个人信息传输过程中的保密性和完整性

传输过程中的个人信息安全风险首先体现为是否保证了传输个人信息的保密性和完整性。传输的个人信息有可能没有采取加密措施或采用的是极为简单的加密措施；同时，在传输过程中有可能受到病毒影响或黑客攻击，从而对个人信息的完整性造成影响。

（三）非授权接入和非法访问

在传统的网络安全模型中，针对网络终端用户的安全接入和访问控制有成熟的解决方案，但云计算环境下数据传输将更为开放和多元化，传统物理区域隔离的方法无法有效保证远距离传输的安全性，电磁泄漏和窃听成为更加突出的安全威胁。特别是在 IaaS 中，服务商为每个用户提供服务管理界面，需要针对不同类型的租户提供差异化的用户身份认证管理授权策略，确保“合法”用户访问正确的服务器，同时也需要在用户访问行为的日志记录和安全事件的报告分析方面提供差异化的解决方案，用户认证、网关、授权、审计方面因为差异性的存在而更加难以管理。薄弱的用户验证机制，或者是简单的用户密码验证很可能产生个人信息安全隐患，而按需服务所具有的潜在安全漏洞又将导致各种未经授权的非法访问，从而产生新的安全风险。[②]

（四）拒绝服务攻击

云计算场景中的拒绝服务攻击（DoS），是指在某一时刻，利用多台主机耗尽目标云服务器的网络带宽和处理能力，使云无法正常提供服务，用户无法进行数据交互。拒绝服务攻击是传统网络安全中最严重的威胁之一。[③] 在云计算环境下，它让个人信息的可用性受到严重的影响，一定程度上阻碍了用户对其个人信息的支配和控制。

---

① 张逢喆，陈进，陈海波等．云计算中的数据隐私性保护与自我毁灭［J］．计算机研究与发展，2011，48（7）：1155-1167.

② 云计算安全政策与法律工作组．中国云计算安全政策与法律蓝皮书［R］．西安：西安交通大学信息安全法律研究中心，2012-10-12：29.

③ 徐国爱，张淼，彭俊好．网络安全（第二版）［M］．北京：北京邮电大学出版社，2010：77.