CHINA LEGAL
Executive Council

信息技术与电子商务系列（一）数据跨境传输风险分析及企业应对

主讲人：陈际红

中伦律师事务所
ZHONG LUN LAW FIRM

演讲人简介

陈际红 ，中伦律师事务所合伙人

- 全国律师协会信息网络与高新技术委员会，副主任；
- 北京市律师协会电信法律委员会，主任;
- 国家知识产权局国家知识产权专家库，专家；
- 国家知识产权战略办公室，入库知识产权战略专家；
- 北京重点产业知识产权联盟，知识产权专家；
- 中国互联网协会法治工作委员会，顾问，

陈际红律师于2005年被法制日报及中国电子商务协会联合评为“2005IT法务人年度十佳”；2006年入选国家知识产权战略办公室评选的国家知识产权战略专家；2011年入选英国Corporate INTL Magazines 评选的“中国最佳50名律师”；2011年入选国家知识产权局评审的国家知识产权专家库；2013年陈律师被北京市律师协会授予“北京市十佳知识产权律师”的称号；2015年被Asia Law and Business评为中国15佳知识产权律师；2016年被Corporate INT评选为中国年度最佳电信法律师。

目录

01 数据跨境传输的立法概述

（一）数据跨境传输的立法概述

网络安全法

第三十条：关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

何谓重要数据？

- 是否会区分业务数据和商业信息数据

如何进行安全评估？

- 具体内容
- 评估程序

个人信息和重要数据出境安全评估办法（草案修改稿）

第二稿与第一稿的主要区别

- **境内存储：** 第二稿中，对于在境内收集和产生的个人信息和重要数据不再一般性地要求首先在境内存储；
- **宽限期**：第二稿评估办法给出了18个月的“宽限期”：2018年12月31日起，网络运营者数据出境应当符合本办法的要求；
- **数据处境的定义：** 第二稿中，数据接收方由“位于境外的机构、组织、 个人”修改为“境外机构、组织、个人 “。
- **推定同意：** 针对跨境的信息主体自主的通信、交易行为，由于此类通信、交易的相对人由于无法事先取得该行为人的授权，第二稿评估办法明确了信息主体默示同意的效力。

个人信息和重要数据出境安全评估办法（草案修改稿）

何谓“数据出境“：规定了一个物理边界，将数据提供给境外主体，即构成数据的出境。

评估方式：自行评估和监管机构评估。数据出境监管的基本原则为，对于一般性数据，企业自行评估，并自行负责；对于特定数据，监管机构负责组织评估，并决定是否允许出境。

监管机构：网信部门起到统筹协调作用，各个行业主管或监管部门具体组织开展本行业内的数据出境安全评估。

个人信息和重要数据出境安全评估办法（草案修改稿）

重新评估：对于评估情形发生了变化，比如当数据接收方出现变更，数据出境目的、范围、数量、类型等发生较大变化，数据接收方变更或发生重大安全事件时，应及时进行安全评估。是阶段性评估而非逐笔评估。

评估内容：首先要证明数据出境的合法性、正当性和必要性。在评估过程中，数据的性质和内容、数据的数量、接收方的安全措施、所在国家的法律环境、数据被滥用的风险等都会被纳入到评估的范围。

不得向境外提供的情形：凡有个人信息出境的，均需要获得信息主体的同意， 而且，为了满足评估的程序性要求，获得的授权应当是书面和可证明的。对于可能不符合国家法律、行政法规、部门规章约定的，以及可能损害公众和国家利益的、危害国家政治、国土、军事、经济、文化、社会、科技、信息、生态、资源、核设施等安全等信息，不能出境。

数据出境安全评估指南（征求意见稿）

何谓“重要数据”？

是指我国政府、企业、个人在境内收集、产生的不涉及国家秘密，但与国家安全、经济发展以及公共利益密切相关的数据(包括原始数据和衍生数据)，一旦未经授权披露、丢失、滥用、篡改或销毁，或汇聚、整合、分析后，可能造成以下后果：

a.危害国家安全、国防利益，破坏国际关系；
b.损害国家财产、社会公共利益和个人合法利益；
c.影响国家预防和打击经济与军事间谍、政治渗透、有组织犯罪等；
d.影响行政机关依法调查处理违法、渎职或涉嫌违法、渎职行为；
e.干扰政府部门依法开展监督、管理、检查、审计等行政活动，妨碍政府部门履行职责；
f.危害国家关键基础设施、关键信息基础设施、政府系统信息系统安全；
g.影响或危害国家经济秩序和金融安全；
h.可分析出国家秘密或敏感信息；
i.影响或危害国家政治、国土、军事、经济、文化、社会、科技、信息、生态、资源、核设施等其它国家安全事项。

数据出境安全评估指南（征求意见稿）

安全评估流程

包括：

（1）评估启动

（2）制定数据出境计划

（3）评估数据出境计划的合法正当和风险可控

（4）完成评估报告

（5）检查修正

如经评估出境安全风险为极高或高的，个人信息和重要数据不得出境。评估报告应至少保存5年。

如数据出境计划不满足合法正当要求，或经评估后不满足风险可控的要求，网络运营者可修正数据出境计划，或采用相关措施降低数据出境风险（如数据脱敏），并重新开展自评估。

数据出境安全评估指南（征求意见稿）

评估要点

1、合法正当：

个人信息主体是否已经授权同意个人信息出境；数据出境是否符合我国政府与其他国家、地区签署相关条约的约定；是否是法律法规命令禁止的；数据出境是否为网络运营者在合法的经营范围内从事正常业务活动或履行合同义务所必需的；数据出境是否为司法协助需要等。

2、风险可控：

应综合考虑出境数据的属性和数据出境发生安全事件的可能性。出境数据的属性包括个人信息或重要数据的数量、范围、类型、敏感程度和技术处理情况等。对数据出境发生安全事件的可能性的评估要点包括（1）发送方数据出境的技术和管理能力；（2）数据接收方的安全保护能力、采取的措施；（3）数据接收方所在国家或区域的政治法律环境。

02 何谓数据跨境？

（二）何为数据跨境？

数据处境的方式

何谓法律规制数据的跨境传输？

- 网络直接连接传输数据；
- 境外用户可以读取数据；
- 境内数据传给第三方，再通过其它方式境外传输或携带；
- 为数据处理的目的向境外传输数据。

（二）何为数据跨境？

特定数据的本地化

其他相关规定：

- 征信数据（《征信业管理条例》第24条）
- 个人金融信息（《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》第6条）
- 地图数据（《地图管理条例》第34条）
- 网络出版服务所需的必要的技术设备（《网络出版服务管理规定》第8条）
- 网约车业务相关数据和信息（《网络预约出租汽车经营服务管理暂行办法》27
- 人口健康信息（《人口健康信息管理办法（试行）》）
- 保险业务数据、财务数据等重要数据《保险公司开业验收指引》

03 信息主体的合法授权

（三）信息主体的合法授权

个人信息的范围

- **个人信息** 是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。
- **判断关键：是否具有身份可识别性**
- **核心概念的对比**

个人信息	非个人信息
个人信息	隐私
个人一般信息	个人敏感信息
个人信息保护	数据保护

授权的法定要求

知情同意	网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。
必要原则（最少够用）	网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。
跨境的额外要求	个人信息出境，应向个人信息主体说明数据出境的目的、范围、内容、接收方及接收方所在的国家或地区，并经其同意。未成年人个人信息出境须经其监护人同意。

（三）信息主体的合法授权

敏感信息与一般信息

- **个人信息**
  - **个人一般信息** → **默许同意**
  - **个人敏感信息** → **明示同意**

《信息安全技术公共及商用服务信息系统个人信息保护指南》（GB/Z 28828-2012）	信息安全技术个人信息安全规范（征求意见稿）
个人敏感信息指的是一旦遭到泄露或修改，会对标识的个人信息主体造成不良影响的个人信息。各行业个人敏感信息的具体内容根据接受服务的个人信息主体意愿和各自业务特点确定。**个人敏感信息可以包括身份证号码、手机号码、种族、政治观点、宗教信仰、基因、指纹等。**	**个人敏感信息**指的是一旦泄露、非法提供或滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或歧视性待遇等的个人信息。 注1：个人敏感信息包括身份证件号码、个人生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪轨迹、住宿信息、健康生理信息、交易信息、14岁以下（含）儿童的个人信息等。

* **个人一般信息** 指除个人敏感信息以外的个人信息。

授权方式

◆ **明示授权**

含义：完整公示条款、有合理机会阅读条款、没有诱导性或替代性选择、有主动的行为、表达肯定或同意。

适用：个人敏感信息的收集、个人信息出境、

个人信息主体通过书面声明或主动做出肯定性动作，对其个人信息进行特定处理做出明确授权的行为。

注：肯定性动作包括个人信息主体主动作出声明（电子或纸质形式）、主动勾选、 主动点击“同意”、 “注册”、 “发送”、 “拨打”等。

◆ **默示授权**

含义：根据信息主体的一定行为，基于某些公认的准则而推定其为授权的意思表示。
比如，网站公示了Privacy Policy，用户有机会阅读，适用或继续使用网站的行为。

适用： 非敏感信息的收集，普遍性、一般性的网络服务（网络新闻、搜索引擎）。

（三）信息主体的合法授权

授权方式

◆ 单独授权

- 与一般性授权（general consent）区分开来，就某项特定的信息收集，
- 需要获得信息主体的明示和单独的授权，以彰显其重要和敏感性。

◆ 逐次授权

- 在每次获取该信息时，均要求信息收集方获得信息主体的同意。
- 比如精确的位置信息或运动轨迹。

信息主体的授权

北京百度网讯科技有限公司与朱烨隐私权纠纷　　案号：（2014）宁民终字第5028号

问题	一审	二审
cookie信息的性质	属于个人信息。 展示了个人上网的偏好，在一定程度上标识个人基本情况和个人私有生活情况。	不属于。 一旦与网络用户身份相分离，便无法确定具体的信息归属主体，不再属于个人信息范畴
侵权方式	隐私权侵权不仅有公开、宣扬他人隐私的方式，也包括不当收集、利用他人隐私信息的方式	百度的个性化推荐是通过技术手段完成，并没有向第三方或公众展示、及公开用户的cookie信息，因此不构成侵权
明示/漠视同意	百度采取的是“默示同意”原则，不足以保障用户的知情权和选择权。	百度提供的隐私权保护声明及退出机制，已足以保障用户权利。非敏感的个人信息的收集、使用仅需要适用默示原则

（三）信息主体的合法授权

北京百度网讯科技有限公司与朱烨隐私权纠纷　　案号：（2014）宁民终字第5028号

“百度网讯公司已经明确说明cookie技术、使用cookie技术的可能性后果以及通过提供禁用按钮向用户提供选择退出机制”，因此认 为“朱烨在百度网讯公司已经明确告知上述事项后，仍然使用百度 搜索引擎服务，**应视为对百度网讯公司采用默认“选择同意”方式的认可**”，并进而认定“...将个人信息区分为个人敏感信息和非个人敏感信息的一般个人信息而允许采用不同的知情同意模式，旨在保护个人人格尊严与促进技术创新之间寻求最大公约数”。

——二审判决书摘要

04 数据跨境的合规

（四）数据跨境的合规

合规实施

（四）数据跨境的合规

数据合规基本考虑

合规要求

第一点

知情同意

- 数据分类
- 授权协议
- 授权流程

第二点

内部数据管理制度

- 数据安全管理制度
- 人员和组织
- 全方位和全生命周期的管理流程

第三点

数据流转的控制

- 分类管理
- 数据脱敏
- 出境安全评估

05 问题讨论

（五）问题讨论

热点问题

1、在我国现有互联网管制体系下，跨境是否包括港澳台地区？

2、数据出境，除了物理转移外，是否包括境外直接访问、镜像境内服务器的逻辑转移？

3、意见稿无法规制苹果应用商店等在中国没有落地实体的情形，是不是反倒对在中国有落地实体的企业不公平？

4、作为大型零售企业，我们有非常多的消费者信息，若欧洲总部要求将数据传回总部，有哪些潜在风险，应该如何操作？

CHINA LEGAL
Executive Council

THANK YOU !