

# 《大数据变现过程中的安全传输》

-段方

大数据总设计师

教授 北京大学博士后

## 1 概述

### 1.1 大数据与新基建

#### 1.1.1 新基建、新国运

#### 1.1.2 大数据成为新基建的“必然”

### 1.2 大数据成为新的生产要素（《关于构建更加完善的要素市场化配置体制机制的意见》）

#### 1.2.1 生产要素的含义

#### 1.2.2 如何成为生产要素？

#### 1.2.3 电信大数据如何成为生产要素？

### 1.3 电信运营商大数据的特点

#### 1.3.1 电信大数据包含的信息维度

#### 1.3.2 电信大数据的特点

#### 1.3.3 电信大数据的竞争优势

### 1.4 大数据如何变现？

**1.4.1** 从原始数据开始的“变现”

**1.4.2** 如何提升数据加工能力？

**1.4.3** 如何打造数据“产品”？

**1.5** 数据中台的提出及意义

**1.5.1** 适时提出的“数据中台”

**1.5.2** 如何提升数据运营能力

**1.6** 大数据安全的法规

**1.6.1** 《中华人民共和国数据安全法》简述

**1.6.2** 国家的数据主权

**1.7** 大数据变现过程的安全管控

**1.7.1** 哪些数据可以“变现”？

**1.7.2** 哪些数据是敏感数据？

**1.7.3** 如何进行安全管控？

**1.8** 【思考】防不胜防的隐私泄露——透明倒逼的“善良”

**1.9** 【示例】附件-阿里巴巴的数据变现产品

## **2** 大数据数据安全法律基础

**2.1** 大数据时代隐私的重新定义

### **2.1.1 舶来品——隐私**

### **2.1.2 从剑桥分析说起。。。**

### **2.1.3 隐私的相对性**

## **2.2 涉及数据安全的法律案例举例**

### **2.2.1 南京诸女士状告百度侵犯隐私案**

### **2.2.2 谷歌在欧洲输掉的客户隐私案**

## **2.3 涉及数据安全的法律法规**

### **2.3.1 从《网络安全法》说起**

### **2.3.2 各部门出台的安全法律法规汇编**

## **2.4 《中华人民共和国数据安全法》解读**

## **2.5 《数据安全管理办法》——网信办**

## **2.6 《信息安全技术个人信息安全规范》规定的个人敏感信息范畴**

## **2.7 《中华人民共和国刑法修正案》中个人信息犯罪的刑法处罚**

## **2.8 国外大数据安全法律法规——GDPR 等**

## **2.9 【示例】附件一信息安全管控案例及要求**

# **3 现行法律下的大数据“变现”**

## **3.1 哪些数据能够变现？**

### **3.1.1 个人客户数据**

### **3.1.2 群体客户数据**

### **3.1.3 物联网数据**

### **3.1.4 非结构化数据**

### **3.1.5 2B 数据**

## **3.2 如何进行“变现”？**

### **3.2.1 如何卖个人客户数据？**

### **3.2.2 客户授权书的签订方式**

### **3.2.3 汇总数据的价值**

### **3.2.4 分析报告的意义**

## **3.3 从数据到产品的“跃升”**

### **3.3.1 数据加工的层次**

### **3.3.2 数据变现的产品升级**

### **3.3.3 卖算法、卖能力**

### **3.3.4 数据产品的“互联网思维”**

## **3.4 “变现”过程的共享经济**

### **3.4.1 如何让客户愿意共享自己的数据？**

### **3.4.2 如何打造共赢的生态体系？**

### **3.4.3 如何结算数据变现的利益？**

## **3.5 变现过程的安全管控**

### **3.5.1 哪些过程可以进行安全管控？**

### **3.5.2 每个过程如何“留痕”？**

### **3.5.3 安全管控的技术基础**

### **3.5.4 区块链能够解决什么问题？**

## **3.6 政府客户与非政府客户的区别**

### **3.6.1 从司法部门说起的政府客户需求**

### **3.6.2 非政府客户的特点**

### **3.6.3 非政府客户的解决方案**

### **3.7 【示例】附件——某企业大数据的隐私保护**

## **4 变现过程的新技术参考**

### **4.1 区块链技术**

#### **4.1.1 区块链技术基础**

#### **4.1.2 区块链如何应用于数据传输鉴权**

#### **4.1.3 区块链在数据传输的安全局限性**

### **4.2 水印技术**

#### **4.2.1 什么是水印？**

#### **4.2.2 基于文本内容的水印技术**

#### **4.2.3 水印的反向识别**

### **4.3 联邦学习技术**

#### **4.3.1 联邦学习技术基础**

#### **4.3.2 联邦学习的数据保护**

#### **4.3.3 联邦学习中技术难点**

### **4.4 可信计算技术**

**4.4.1** 可信计算的概念

**4.4.2** 可信计算环境

**4.4.3** 可信计算数据保护

## **5 大数据安全管理架构**

**5.1** 层层防御的技术理念

**5.1.1** 从敏感数据角度的层层防御

**5.1.2** 从数据出来环节的层层防御

**5.1.3** 从数据生命周期的层层防御

**5.2** 数据访问策略

**5.2.1** 隐私数据策略管理

**5.2.2** 告警策略管理

**5.3** “三分技术、七分管理”

**5.3.1** 安全管理的重要性

**5.3.2** 安全管理的内容和范围

**5.3.3** 技术围绕管理需求

## **5.4 与网络安全的关系**

### **5.4.1 层次不同**

### **5.4.2 解决网络突破后的数据安全问题**

## **5.5 数据导出管理与监控**

### **5.5.1 数据水印技术**

### **5.5.2 访问轨迹追踪**

## **5.6 安全管理的关键点**

### **5.6.1 明确的规章制度**

### **5.6.2 严格地执行规章制度**

## **5.7 访问终端的安全管控**

### **5.7.1 终端的安全管控原则**

### **5.7.2 应用的管控流程**

## **5.8 机房的安全管控要求**

### **5.8.1 设备隔离要求**

### **5.8.2 访问监控要求等**

## **5.9 安全的“态势感知”技术**

**5.9.1** 什么是“态势感知”？

**5.9.2** 态势感知如何实现？

**5.10** 【案例】附件-某企业安全管理架构案例

## **6** 数据金库等管理应用

**6.1 4A** 认证模式

**6.1.1 4A** 概念

**6.1.2** 与大数据权限管理的关系

**6.2** 金库管理模式

**6.2.1** 何为金库模式？

**6.2.2** 金库模式的要点

**6.2.3** 金库模式的意义

**6.3** 管理规章制度设计

**6.3.1** 设计哪些规章制度

**6.3.2** 规章制度的设计原则

**6.3.3** 规章制度的设计分类

## **6.4 访问日志管理**

### **6.4.1 大数据的日志如何管理**

### **6.4.2 日志的价值分析**

### **6.4.3 日志的分析应用**

## **6.5 安全实时告警**

### **6.5.1 如何进行实时监控**

### **6.5.2 监控规则的实时计算**

### **6.5.3 告警信息的实时传送**

## **6.6 【案例】附件——某企业数据金库实现案例**

# **7 大数据变现中的“互联网思维”（可选）**

## **7.1 中美的互联网发展对比**

## **7.2 堪比文艺复兴的互联网思维**

## **7.3 大数据变现为什么需要互联网思维？**

## **7.4 大数据的客户思维**

## **7.5 大数据的极致思维**

**7.6** 大数据的简约思维

**7.7** 大数据的平台思维

**7.8** 【示例】附件——大数据的互联网思维

**8** 总结