

# 《数据隐私保护的技术手段》

-段方

某电信企业大数据总设计师

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 大数据安全的法规**

### **1.3.1 《中华人民共和国数据安全法》简述**

### **1.3.2 国家的数据主权**

## **1.4 大数据隐私保护的难点**

### **1.4.1 用户身份匿名保护难**

### **1.4.2 敏感信息保护难**

### **1.4.3 隐私信息安全监管难**

## **1.5 大数据风险管控技术**

### **1.5.1 隐私保护的基本原理**

### **1.5.2 隐私保护相关算法概览**

## **1.6 大数据如何变现？**

### **1.6.1 从原始数据开始的“变现”**

### **1.6.2 如何提升数据加工能力？**

### **1.6.3 如何打造数据“产品”？**

## **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 《数据二十条》的急迫**

### **1.8.1 数据要素需要流通**

### **1.8.2 哪些权利可以明确**

### **1.8.3 场内交易与场外交易**

### **1.8.4 《数据二十条》的意义**

**1.9 【思考】防不胜防的隐私泄露——透明倒逼的“善良”**

**1.10 【示例】附件 - 《数据二十条》简介**

## **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】附件一信息安全管理案例及要求

## **3 现行法律下的大数据“服务”**

**3.1** 哪些数据能够服务？

**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“服务”？

**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 “服务”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 服务过程的安全管控**

### **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 大数据隐私保护现状及热点**

## **4.1 身份匿名保护与去匿名化技术**

### **4.1.1 综合多个数据源攻击**

### **4.1.2 DNN 轨迹重识别**

### **4.1.3 集中式差分隐私保护**

### **4.1.4 本地差分隐私保护**

## **4.2 敏感信息隐私挖掘与防护技术**

### **4.2.1 隐私分类**

社交关系隐私

属性隐私

位置隐私

**4.2.2** 攻击者社交距离推算敏感信息

**4.2.3** 模型逆向攻击

**4.2.4** 面向机器学习的隐私保护方法

**4.3** 密文检索与密文计算技术

**4.3.1** 密文检索

关键字检索

区间检索

**4.3.2** 密文计算

同态加密

函数加密

**4.4** 基于风险分析的访问控制技术

**4.4.1** “自顶向下”访问控制模式

**4.4.2** “自底向上”访问控制

**4.4.3** 基于风险的访问控制

基于角色

非负矩阵分解方法

**4.5 【示例】附件——密码学技术基础**

## **5 大数据隐私保护的新技术**

**5.1 区块链技术**

**5.1.1 区块链技术基础**

**5.1.2 区块链如何应用于数据传输鉴权**

**5.1.3 区块链在数据传输的安全局限性**

**5.2 水印技术**

**5.2.1 什么是水印？**

**5.2.2 基于文本内容的水印技术**

**5.2.3 水印的反向识别**

**5.3 联邦学习技术**

**5.3.1 联邦学习技术基础**

**5.3.2 联邦学习的数据保护**

### **5.3.3 联邦学习中技术难点**

## **5.4 安全多方计算**

### **5.4.1 安全多方计算的引出**

### **5.4.2 SMC 技术原理**

### **5.4.3 SMC 的主要特点**

### **5.4.4 SMC 的关键技术**

### **5.4.5 安全多方计算的使用场景**

### **5.4.6 安全多方计算的应用范围**

### **5.4.7 安全多方计算的优势**

### **5.4.8 安全多方计算与区块链技术的结合**

## **5.5 同态加密技术**

### **5.5.1 同态加密基础**

### **5.5.2 同态加密算法原理**

### **5.5.3 技术局限性**

### **5.5.4 相关加密技术的对比**

## **5.6 差分隐私计算**

**5.6.1 差分隐私计算基础**

**5.6.2 差分隐私保护的特点**

**5.6.3 差分隐私计算算法原理**

**5.6.4 差分隐私的应用场景**

**5.7 【示例】附件-联邦学习案例**

## **6 大数据安全管理架构**

**6.1 层层防御的技术理念**

**6.1.1 从敏感数据角度的层层防御**

**6.1.2 从数据出来环节的层层防御**

**6.1.3 从数据生命周期的层层防御**

**6.2 数据访问策略**

**6.2.1 隐私数据策略管理**

**6.2.2 告警策略管理**

**6.3 “三分技术、七分管理”**

**6.3.1 安全管理的重要性**

### **6.3.2 安全管理的内容和范围**

### **6.3.3 技术围绕管理需求**

## **6.4 与网络安全的关系**

### **6.4.1 层次不同**

### **6.4.2 解决网络突破后的数据安全问题**

## **6.5 数据导出管理与监控**

### **6.5.1 数据水印技术**

### **6.5.2 访问轨迹追踪**

## **6.6 安全管理的关键点**

### **6.6.1 明确的规章制度**

### **6.6.2 严格地执行规章制度**

## **6.7 访问终端的安全管控**

### **6.7.1 终端的安全管控原则**

### **6.7.2 应用的管控流程**

## **6.8 机房的安全管控要求**

### **6.8.1 设备隔离要求**

## **6.8.2 访问监控要求等**

## **6.9 安全的“态势感知”技术**

### **6.9.1 什么是“态势感知”？**

### **6.9.2 态势感知如何实现？**

## **6.10 【案例】附件-某企业安全管理架构案例**

# **7 （可选） 数据金库等管理应用**

## **7.1 4A 认证模式**

### **7.1.1 4A 概念**

### **7.1.2 与大数据权限管理的关系**

## **7.2 金库管理模式**

### **7.2.1 何为金库模式？**

### **7.2.2 金库模式的要点**

### **7.2.3 金库模式的意义**

## **7.3 管理规章制度设计**

### **7.3.1 设计哪些规章制度**

### **7.3.2 规章制度的设计原则**

### **7.3.3 规章制度的设计分类**

## **7.4 访问日志管理**

### **7.4.1 大数据的日志如何管理**

### **7.4.2 日志的价值分析**

### **7.4.3 日志的分析应用**

## **7.5 安全实时告警**

### **7.5.1 如何进行实时监控**

### **7.5.2 监控规则的实时计算**

### **7.5.3 告警信息的实时传送**

## **7.6 【案例】附件——某企业数据金库实现案例**

# **8 总结**