《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 隐私信息安全管控难

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—信息安全管控案例及要求

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

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