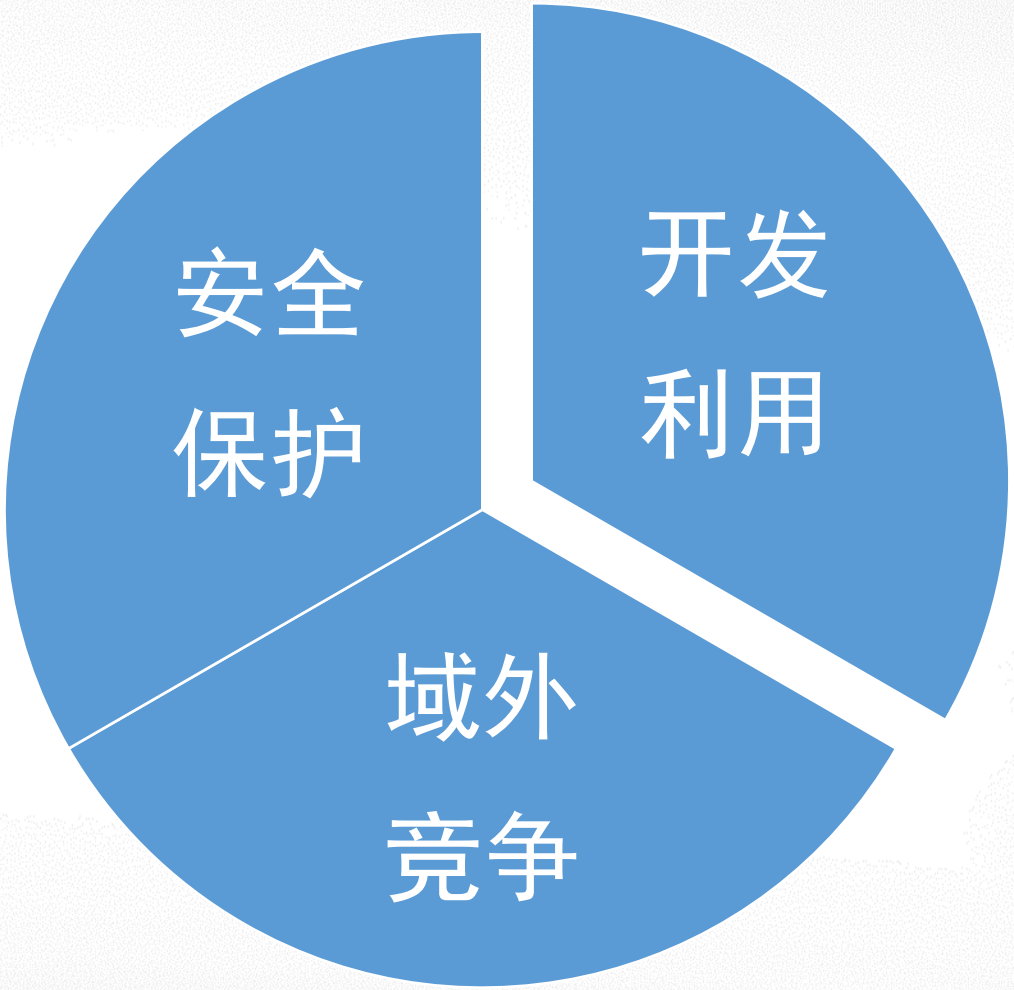
内地数据安全和个人信息保护新发展

北京理工大学 洪延青

2023年5月

中国数据政策的三组核心价值

2014年至今



2022年起始

《网络安全法》

- 网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

信息安全等级保护制度

网络安全等级保护制度

关键信息基础设施安全保护

《个人信息保护法》

- 第一条　为了保护个人信息权益，规范个人信息处理活动，促进个人信息合理利用，根据宪法，制定本法。
- 第二条　自然人的个人信息受法律保护，任何组织、个人不得侵害自然人的个人信息权益。

《数据安全法》

- 维护数据安全，应当坚持总体国家安全观，建立健全数据安全治理体系，提高数据安全保障能力。
- 数据安全，是指通过采取必要措施，确保数据处于有效保护和合法利用的状态，以及具备保障持续安全状态的能力。

《网络安全法》

- 网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

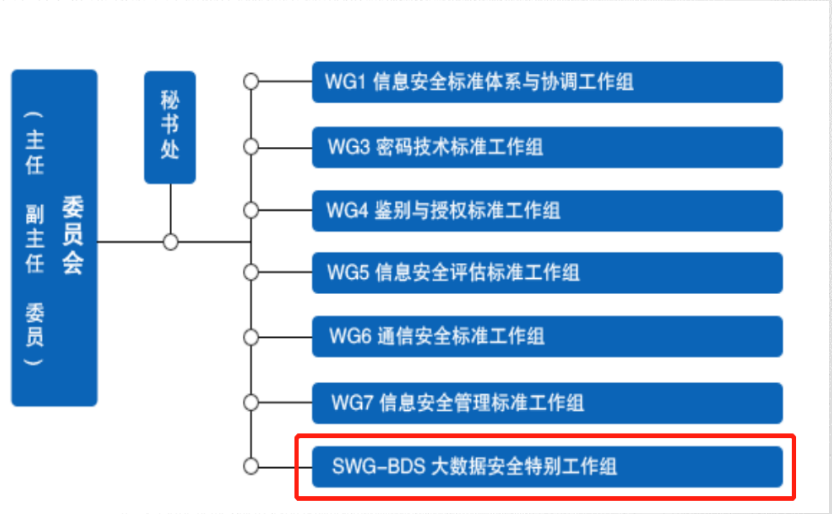
网络安全标准体系

信安标委秘书处

2002年4月，国家标准化管理委员会批复成立“全国信息安全标准化技术委员会”（简称信安标委，编号SAC/TC260），**业务上接受中央网信办指导；**
国际对口组织：**ISO/IEC JTC1 SC27、WG13**

工作范围：包括信息安全技术、机制、服务、管理、评估等领域标准化工作
工作职责：**TC260对网络安全国家标准进行统一技术归口**，统一组织申报、送审和报批 （中网办发文[2016]5号）

2016年，TC260成立**大数据安全标准特别工作组（SWG-BDS）**，负责数据安全、云计算安全等新技术新应用的安全标准研制。



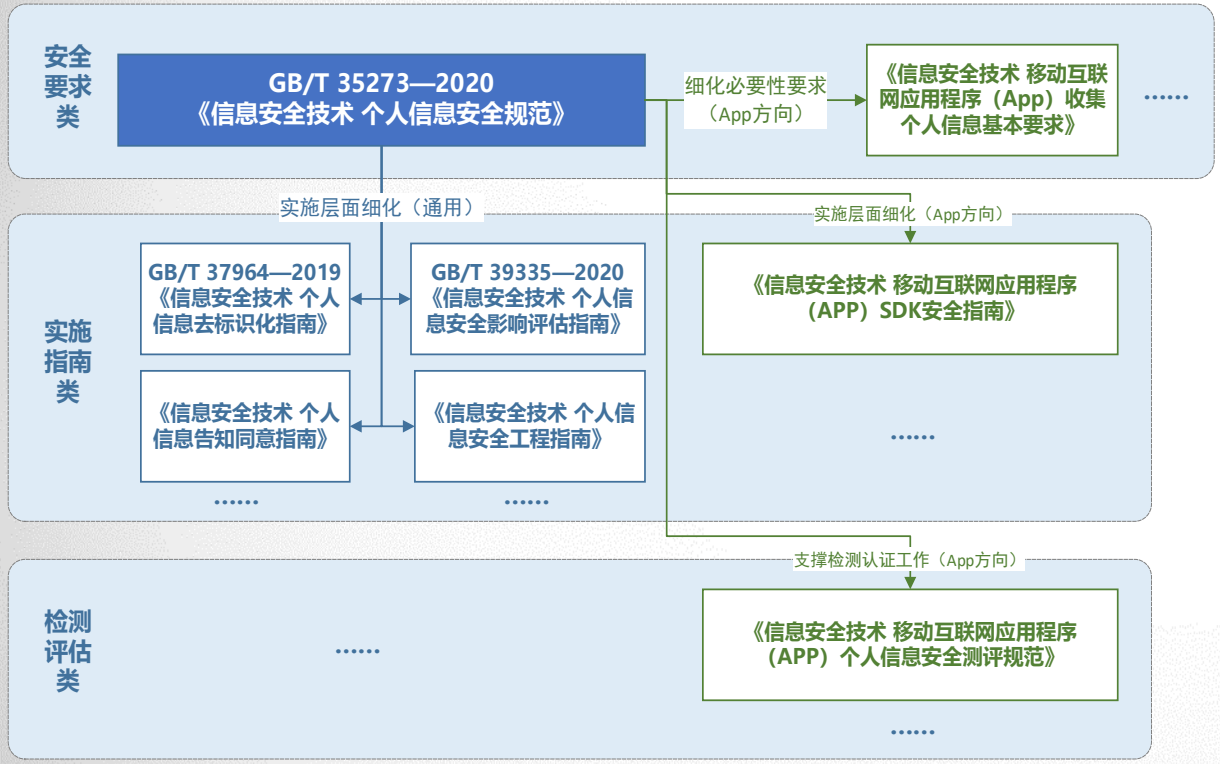
主任委员：
赵泽良 中央网络安全和信息化委员会办公室

副主任委员：
高　林　国家互联网信息办公室网络安全协调局
杜广达　工业和信息化部网络安全管理局
郭启全　公安部十一局
江常青　中国信息安全测评中心
何良生　国家密码管理局

秘书长：杨建军　中国电子技术标准化研究院
秘书处：中国电子技术标准化研究院 网络安全研究中心
委　员：100名
成员单位：截止目前已有650多家单位。

- **AI**（智慧城市安全、人工智能安全）
- **Blockchain**（区块链安全）
- **Cloud**（云计算安全）
- **Data**（数据安全）

标准研制：现有个人信息保护国家标准



在制定标准（10项）

序号	标准名称	标准状态	标准内容
1	移动互联网应用程序（App）收集个人信息基本要求	报批稿	App收集个人信息必要性等
2	个人信息安全工程指南	报批稿	产品和服务隐私设计
3	个人信息告知同意指南	送审稿	告知同意
4	个人可识别信息（PII）处理者在公有云中保护PII的实践指南	送审稿	公有云个人信息保护
5	个人信息去标识化效果分级评估规范	征求意见稿	去标识化效果评估
6	移动互联网应用程序（APP）个人信息安全测评规范	征求意见稿	App个人信息安全测评方法
7	移动互联网应用程序（APP）SDK安全指南	征求意见稿	SDK安全
8	应用商店的App个人信息处理规范性审核与管理指南	草案	应用商店审核App个人信息安全
9	移动智能终端的App个人信息处理活动管理指南	草案	移动智能终端管理App个人信息安全
10	互联网平台及产品服务隐私协议要求	草案	隐私协议

标准研制：国家标准支撑个保法落地

通用要求	GB/T 35273 个人信息安全规范等
个人信息保护影响评估	GB/T 39335 个人信息安全影响评估指南 等
最小必要	移动互联网应用程序收集个人信息基本要求 等
告知同意	个人信息告知同意指南 等
隐私政策	互联网平台及产品服务隐私协议要求 等
App个人信息安全	移动互联网应用程序收集个人信息基本要求、App个人信息安全测评规范、应用商店、移动智能终端 等
生物识别信息安全	人脸识别、声纹识别、步态识别、基因识别等4个生物特征识别数据安全要求
个人信息保护技术	GB/T 37964 个人信息去标识化指南、个人信息安全工程指南 等
互联网平台	网络预约汽车、网上购物、即时通信、快递物流、网络支付、网络音视频等6个数据安全要求标准

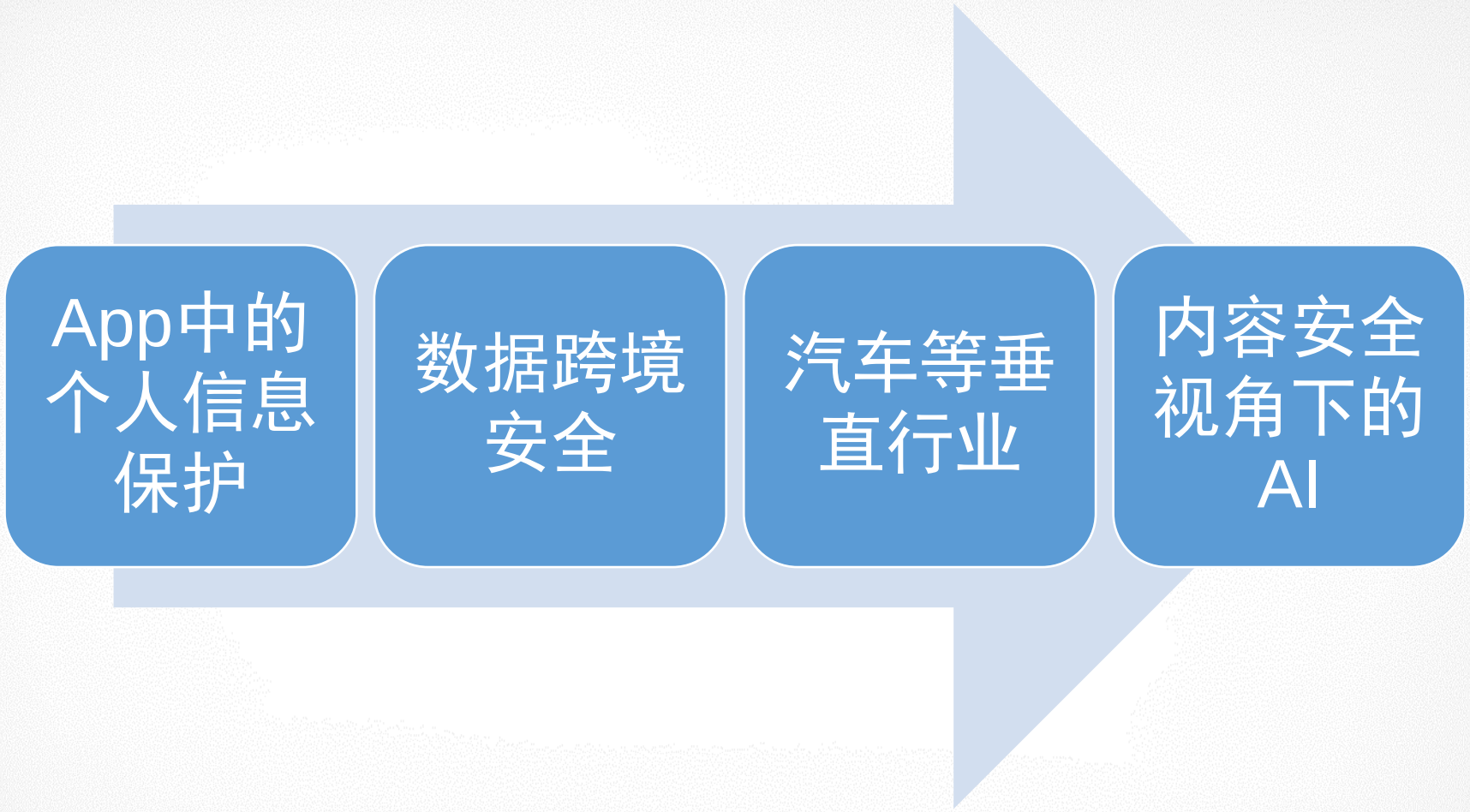
……

标准研制：国家标准支撑个保法落地

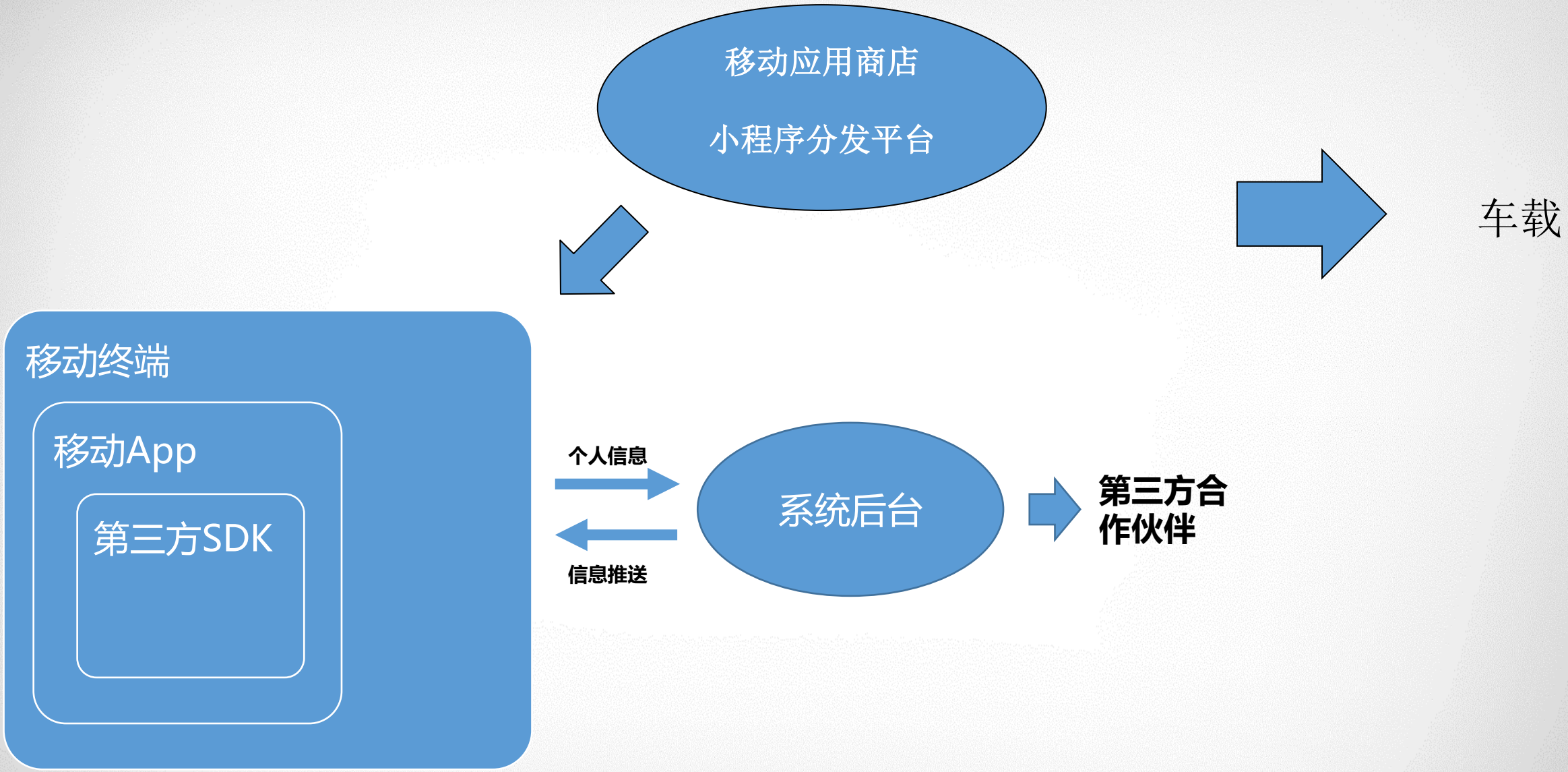
小型个人信息处理者个人信息保护要求	支撑《个人信息保护法》第六十二条
敏感个人信息处理安全要求	支撑《个人信息保护法》第二十八条、第二十九条、第三十条、第六十二条
自动化决策及应用安全指南	支撑《个人信息保护法》第二十四条
人工智能应用个人信息保护指南	支撑《个人信息保护法》第六十二条
个人信息出境标准合同要求	支撑《个人信息保护法》第三十八条
未成年人个人信息处理安全要求	支撑《个人信息保护法》第三十一条
个人信息出境认证	支撑《个人信息保护法》**第三十八条、第六十二条**

……

监管实践

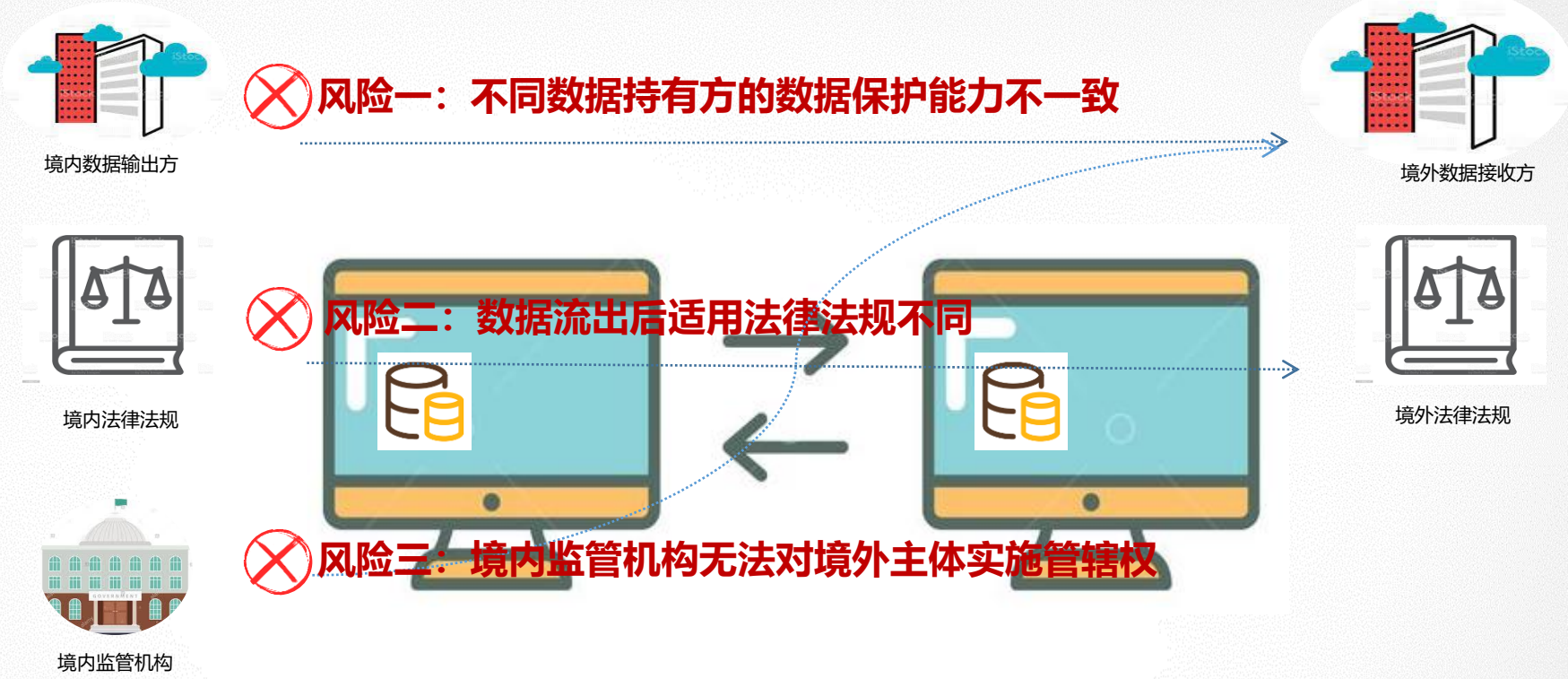

App中的个人信息保护
数据跨境安全
汽车等垂直行业
内容安全视角下的AI

App个人信息保护


移动应用商店
小程序分发平台
车载
移动终端
移动App
第三方SDK
个人信息
信息推送
系统后台
第三方合作伙伴

数据跨境安全

数据跨境流动的风险



风险四：个人数据主体维护自身合法权益困难

国家安全风险


标准
合同
保护
认证
安全评估

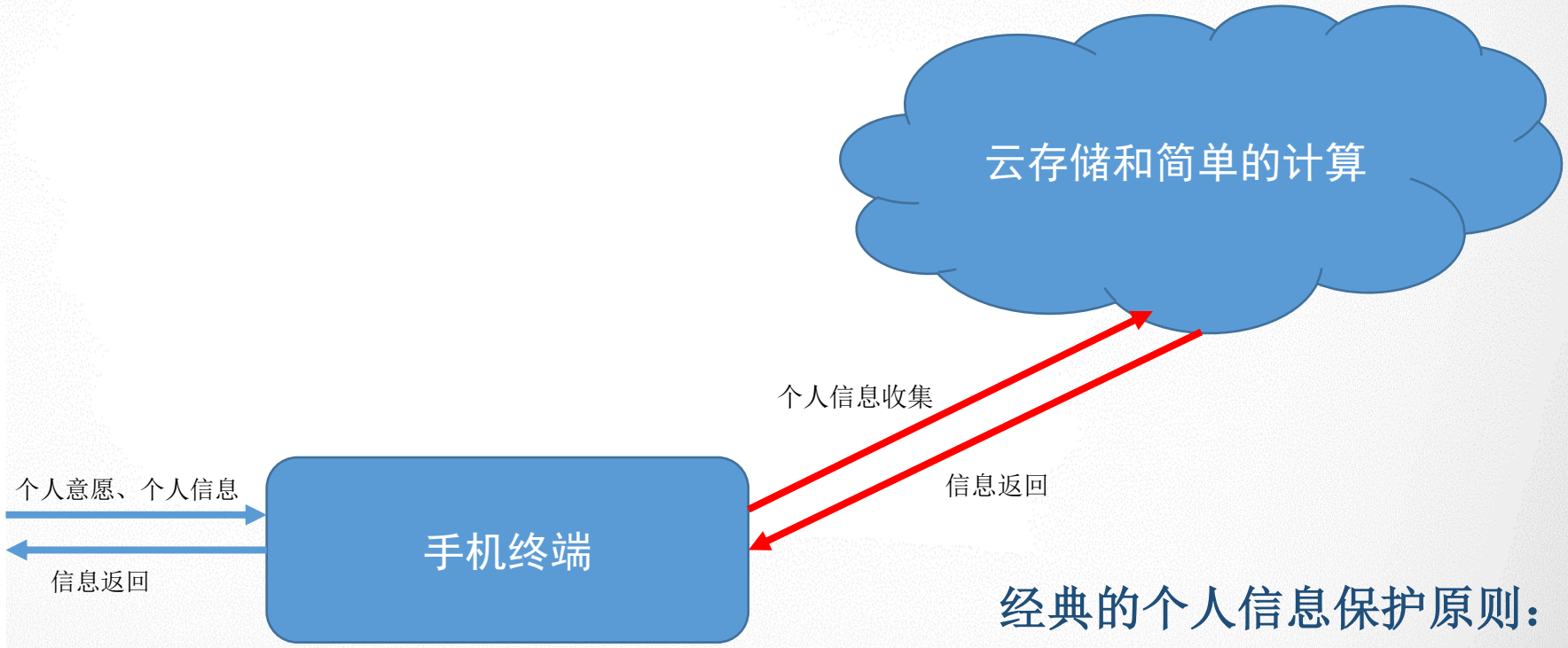
自评估与国家网信评估内容高度一致

风险自评估事项	安全评估事项	说明
数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性	数据出境的目的、范围、方式等的合法性、正当性、必要性	前者较后者增加“境外接收方”处理目的等合法、正当、必要性
出境数据的规模、范围、种类、敏感程度	出境数据的规模、范围、种类、敏感程度	一致
数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；	数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险	虽然前者与后者一致，但后者在表述上与其他所有安全评估事项构成“总分”关系
境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；	N/A	前者需要重点评估接收方履约能力
数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险；	出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险；	一致
个人信息权益维护的渠道是否通畅等；	数据安全和个人信息权益是否能够得到充分有效保障	后者涵盖的范围比前者更广
与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等（以下统称法律文件）是否充分约定了数据安全保护责任义务。	数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务。	一致
N/A	境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响；境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求。	仅在后者列出，评估部门的特有审核事项
N/A	遵守中国法律、行政法规、部门规章情况	仅在后者列出，评估部门的特有审核事项

内容视角下的AI

传统的业务模式下的个人信息保护问题

1. 终端操作系统设计（设计理念、权限分组、权限分级、权限申请机制等）
2. APP的设计（申请的系统权限、告知和授权机制、第三方插件行为等）
3. 个人信息存储于后端时对外提供的情况和个人控制的程度



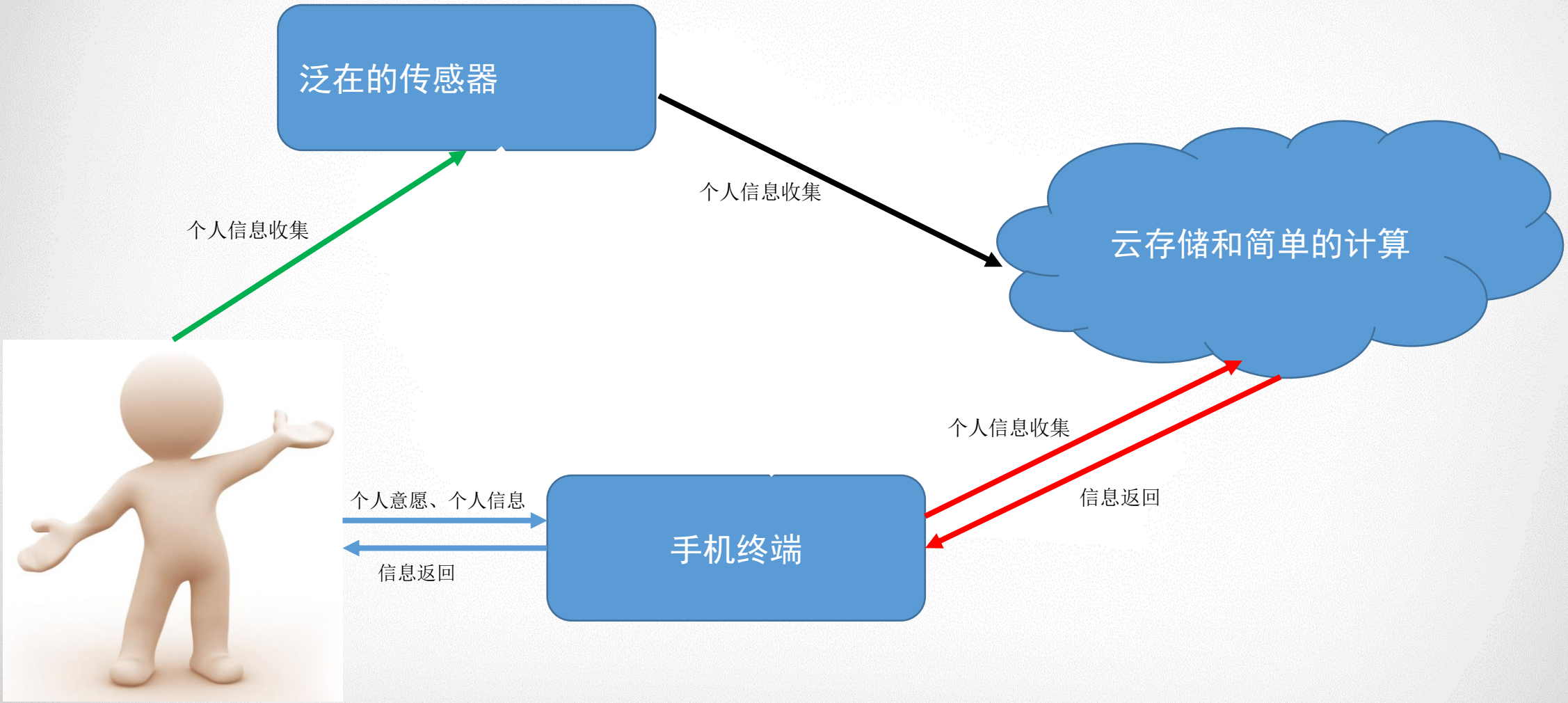
经典的个人信息保护原则：

目的明确、选择同意、最少够用、公开透明、确保安全、主体参与

传统业务模式+泛在的传感器

新的问题：

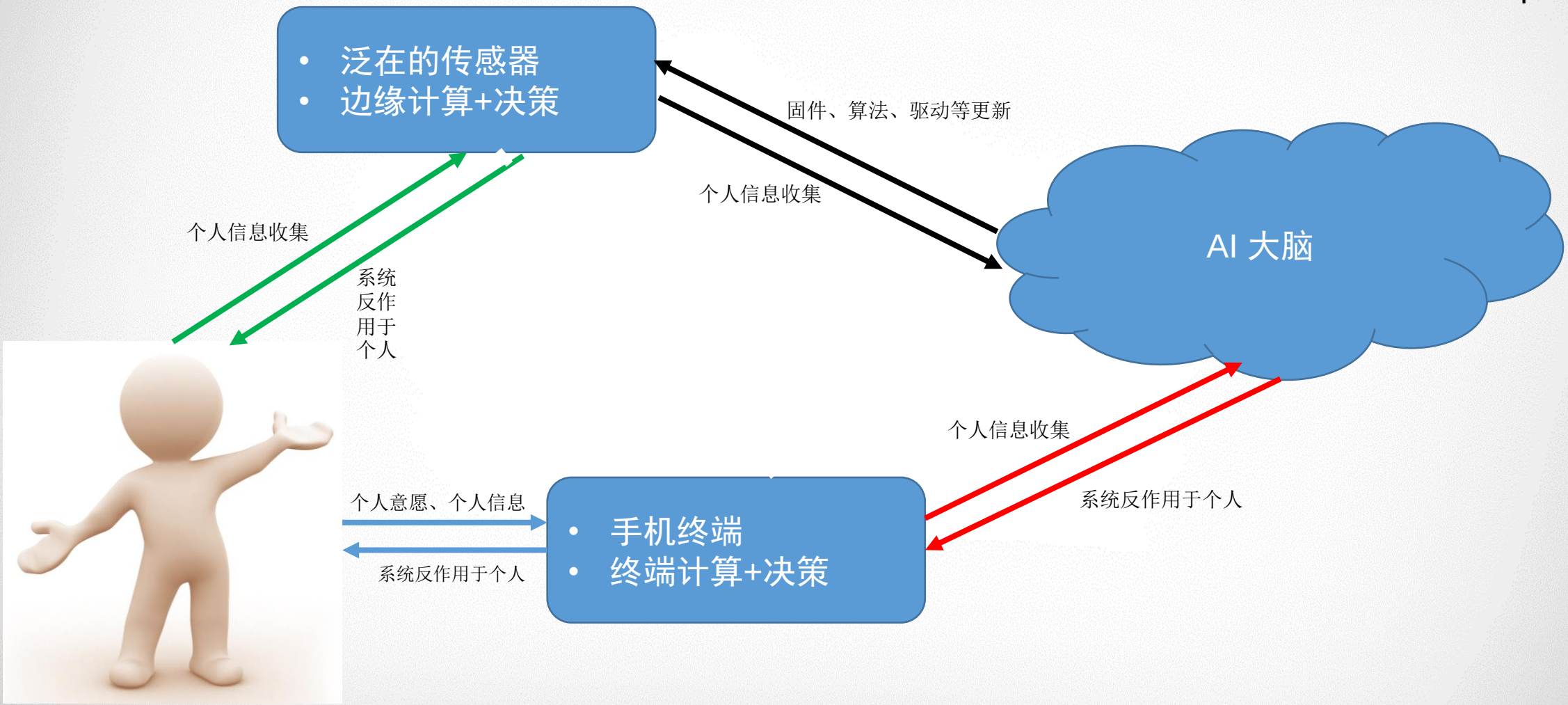
1.泛在的传感器
2.数据融合的问题



传统业务模式+IOT+AI

更新的问题：

1.边缘计算+决策
2.系统反作用：公平性（fairness）+操控（manipulations）



传统的业务模式

1. 终端操作系统设计（设计理念、权限分组、权限分级、权限申请机制等）
2. APP的设计（申请的系统权限、告知和授权机制、第三方插件行为等）
3. 个人信息存储于后台，对外提供的情况和个人控制的程度

传统业务模式+泛在的传感器

1. 泛在的传感器
2. 数据融合的问题

传统业务模式+泛在的传感器+AI

1. 边缘计算+决策：
2. 系统反作用：公平（fairness）+操控（manipulations）

生成式AI

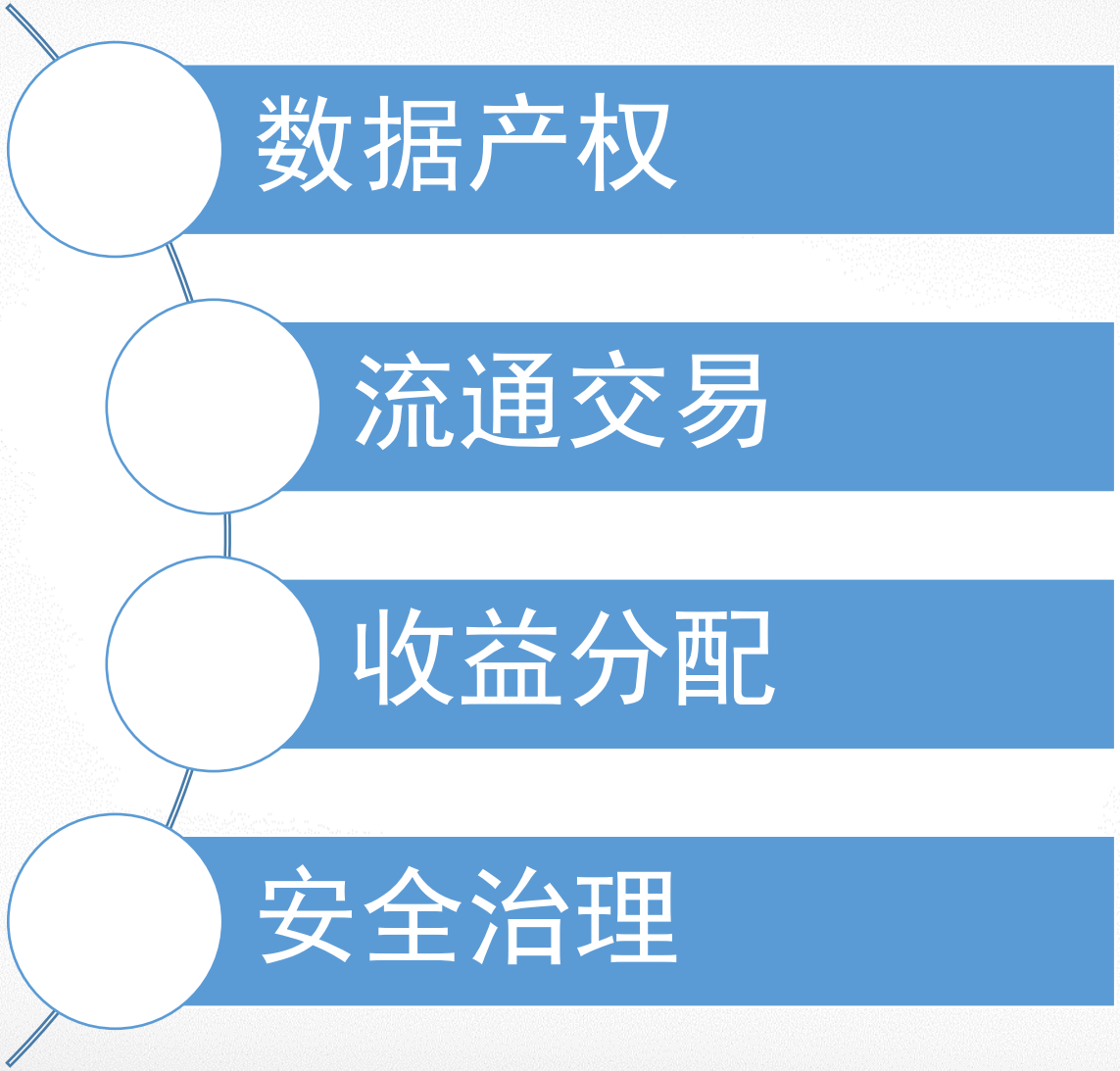
- 有害内容：事前/事后
- 技术黑盒：测评方法？
- 训练数据：数据质量

数据要素化、资产化

“数据二十条“

主线：

促进数据合规高效流通使用、赋能实体经济



数据基础制度的特点：

- 适应数据特征
- 符合数字经济发展规律
- 保障国家数据安全
- 彰显创新引领

“数据二十条“

1. 促进数据使用价值复用与充分利用，促进数据使用权交换和市场化流通。审慎对待原始数据的流转交易行为
2. 建立健全基于法律规定或合同约定流转数据相关财产性权益的机制。

需求侧

数据交易场所

数据需求方


中央网络安全和信息化委员会办公室
和改革委员会
部（重新组建）
息化部
事务委员会
全部
国务院部委管理的国家局
企业债券发
推进数字中国、数字经济、数字社会建设划入
数据资源整合共享和开发利用
国家数据局（组建）
国家粮食和物资储备局
国家能源局

敬请指正

公众号：网安寻路人