2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE

数据安全法规及标准建设

中国电子技术标准化研究院 副院长
程多福

一、数据安全政策监管进展

数字经济时代数据安全事件频发

2019年3月
网友曝光墨迹天气 App 上传用户所有 Wi-Fi 账号（包含当前IP和连接WIFI名称等），均属于**网络信息**。多位专家表示，Wi-Fi名称信息可用于用户画像。

2019年2月
网友曝光安卓版京东金融APP**未经用户授权**获取用户敏感截图并上传

京东金融 JD Finance

2020年2月16日
体育连锁巨头迪卡侬（Decathlon）发生大范围数据泄露，起因是1.23亿条记录被保存在一个并不安全的数据库中

DECATHLON 迪卡侬

社

SAMOYED 萨摩耶金服

2019年3·15晚会曝光
1、曝光萨摩耶公司生产的**探针盒子**能探测用户手机的MAC地址，并可转换成电话号码。
2、“社保掌上宝”APP通过不合理条款获得用户授权，在用户注册、使用社保查询服务，将用户的社会保障号、社保查询密码等个人敏感信息**传送至第三方服务器**。

2020年3月10日
Facebook被澳大利亚政府起诉，涉嫌泄露30万澳大利亚用户个人信息。

2019年6月
今日头条被用户起诉，未明确告知和同意，擅自读取用户通讯录推荐好友。

头条 今日头条

2020年3月
Google因泄露用户隐私，违反了瑞典的数据保护法被罚款800多万美元。

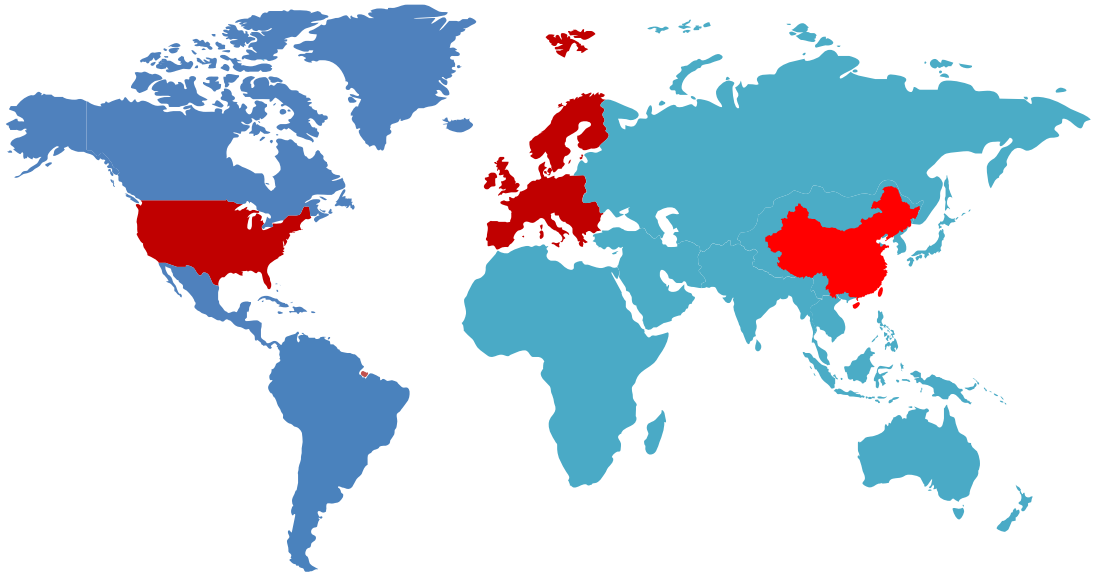
Google 谷歌

2020年3月
针对媒体报道的新浪微博因用户查询接口被恶意调用导致App数据泄露问题，**工业和信息化部网络安全管理局**对新浪微博相关负责人进行了问询**约谈**。

2020年6月
新华社文章，曝光手机App强制跳转启动、自启动、关联启动的现象。

2020年7月
工业和信息化部发布了《关于侵害用户权益行为的App通报（2020年第二批）》，通报智慧树等15款App涉及过度索取权限、私自收集个人信息、私自共享给第三方、超范围收集个人信息等问题。

全球数据安全监管环境趋严



全球107个国家和地区已制定数据安全和隐私保护法律
亚洲、非洲只有不到40%的国家有相关法律

欧盟《通用数据保护条例(GDPR)》

- 跨境数据流动限制
- 个人数据权利加强
- 高额罚款：营业额4%

美国《加州消费者隐私法案（CCPA）》

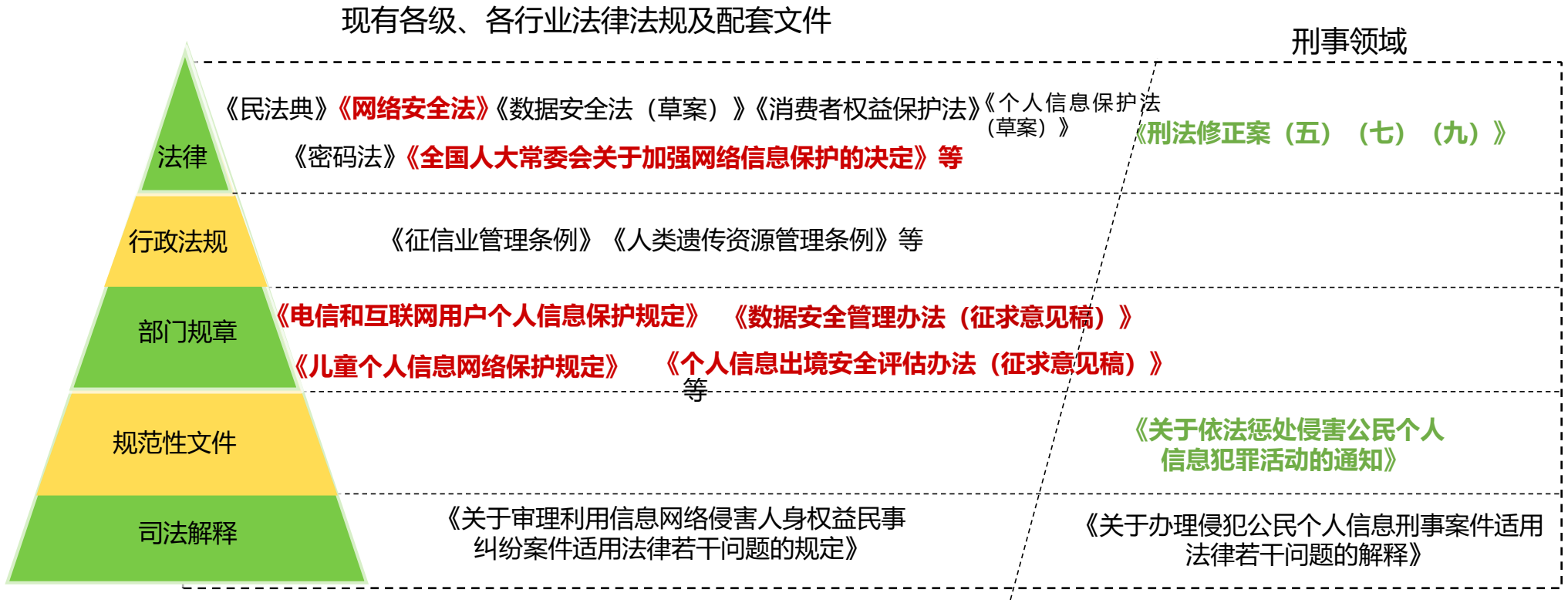
- 参考GDPR，同时相较GDPR对于个人信息类别扩展
- 高额罚款：7500$/人
- 2020年1月1日生效

中国《网络安全法》、《数据安全法（草案）》

- 网安法提及数据16处：数据安全、个人信息保护、数据跨境流动、国家重要数据安全等。

我国数据安全相关法律法规

现状：分散立法，正在制定数据安全和个人信息保护专门的法律

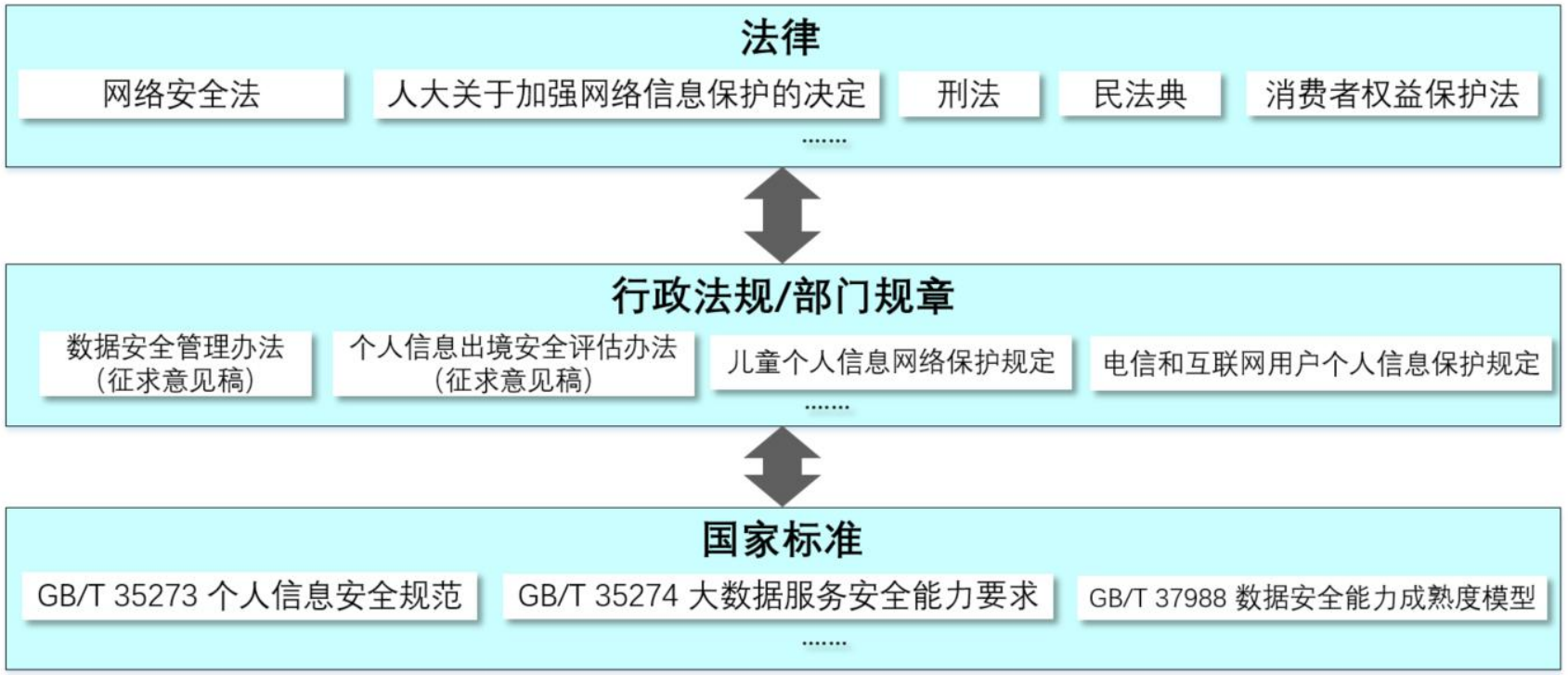


2018年9月，我国《数据安全法》《个人信息保护法》已被列入人大常委会立法规划，并列入条件比较成熟、任期内拟提请审议的第一类项目。

二、数据安全国家标准进展

数据安全国家标准定位

- 《网络安全法》：**国家建立和完善网络安全标准体系**。
- 《数据安全法（草案）》：国家推进数据开发利用技术和**数据安全标准体系建设**。
- **支撑法规政策。**数据安全国家标准是对国家法律法规和政策规章的细化支撑，也是大数据安全保障体系的重要组成部分。
- **规范引导行业。**基于问题导向原则，及时发现数据安全典型问题和安全风险；推广优秀的数据业界安全实践，为组织数据安全实践提供参考。



全国信息安全标准化技术委员会(TC260)

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）TC260是国家标准化管理委员会的直属标委会；业务上接受中央网信办指导；国际对口组织：ISO/IEC JTC1 SC27

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）

主任委员：
赵泽良 中央网信办副主任

副主任委员：
胡　啸　中央网信办网安局副局长
韩　俊　工业和信息化部科技司原巡视员
赵　林　公安部科信局巡视员兼副局长
李守鹏　中国信息安全测评中心副主任
何良生　国家密码管理局副局长
王京涛　国家保密局总工
刘卫军　国家认监委副主任

秘书长：赵波　中国电子技术标准化研究院院长

秘书处：设在中国电子技术标准化研究院，负责委员会的日常工作。

委员：81名，国内企业代表近50%，4名外企代表

成员单位：截止目前已有647家单位。

TC260数据安全相关标准

技术支撑类标准

- 这一类标准规范了通用的**安全支撑技术**，而且这些技术可以**直接支撑数据安全的保护技术**，典型地如密码技术类标准。

通用安全类标准

- 此类标准提出了**体系化的安全要求**、实施指南或相关产品和系统的测试规范，而其中**覆盖到数据安全领域**，并提出了一些具体的要求或措施，典型地如网络安全等级保护、云计算、信息安全管理、智慧城市以及测试评估等相关标准。

以系统为中心的数据安全类标准

- 此类标准是传统数据安全保护类标准，其主要内容是围绕网络系统（数据信息系统）为中心，**从网络系统的视角来规范各种数据安全技术手段和实施措施**，典型地如数据库管理管理系统、灾难恢复和数据交换相关的标准。

以数据为中心的数据安全类标准

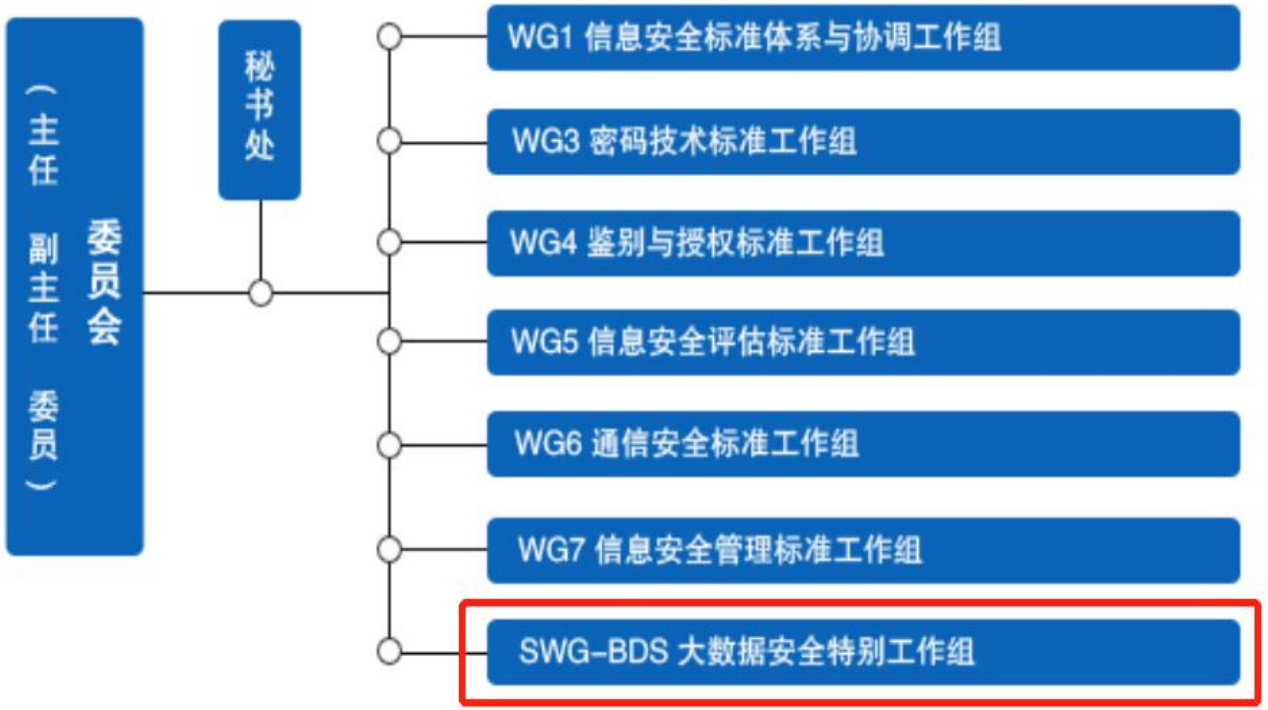
- 以数据为中心的数据安全类标准的主要内容也是规范各种数据安全技术手段和实施措施，但和“以网络系统为中心的数据安全类标准”不同的是，它是以数据为中心、**从数据安全的视角来提出各类技术要求和实施措施规范**。通常地，此类标准**从数据的全生命周期来考虑各种数据安全保护需求**，并以此提出相关技术要求和措施规范。

个人信息安全类标准

- 近年来，**个人信息非法采集、使用和泄露事件**越来越多，针对此类安全保护要求，全国信息安全标准化技术委员会（TC260）制订了多项**个人信息安全标准**，并开展了相关的研究工作，提出了相关的保护要求和实施措施指南。

大数据安全标准特别工作组（SWG-BDS）

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。

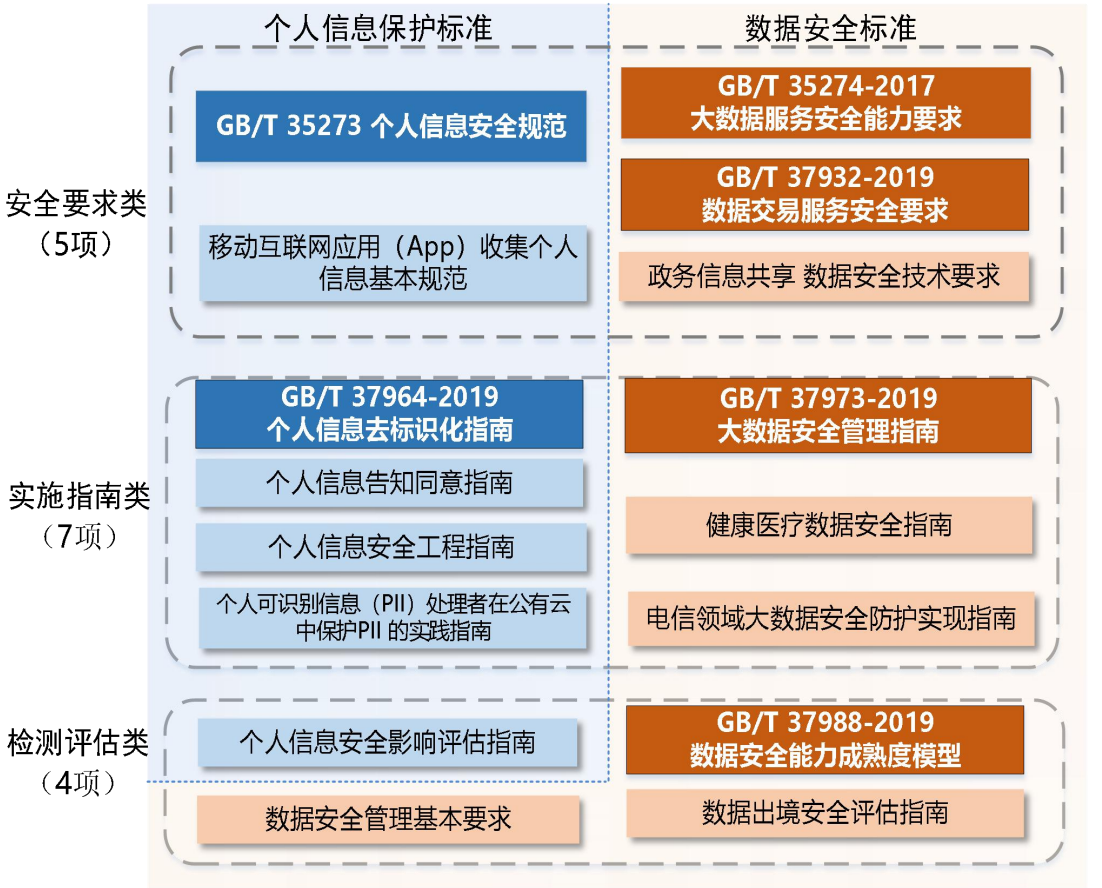


- **AI**（智慧城市安全、人工智能安全）
- **Blockchain**（区块链安全）
- **Cloud**（云计算安全）
- **Data**（数据安全）

- 组　长：清华大学　王建民
- 副组长：四川大学　陈兴蜀
- 秘　书：清华大学 金涛
- 成员单位：301家

数据安全国家标准体系初见规模

- TC260围绕数据安全和个人信息保护两个方向，**已发布6项国家标准，在研国家标准10项。**
- 数据安全方向，主要围绕数据安全能力、数据交易服务、出境评估、政务数据共享、健康医疗数据安全、电信数据安全等内容。
- 个人信息保护方向，主要聚焦于个人信息保护要求、去标识技术、App收集个人信息、隐私工程、影响评估、告知同意等内容。



GB/T 35273-2020《个人信息安全规范》

- 本标准规定了开展收集、存储、使用、共享、转让、公开披露、删除等个人信息处理活动应遵循的原则和安全要求。
- 本标准适用于规范各类组织的个人信息处理活动，也适用于主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估。
- 针对服务或功能强制捆绑的问题，修订个人信息收集；拆分使用环节；第三方接入管理；个人信息安全工程；个人信息记录管理等。

采集 → 保存 → 使用 → 对外提供　　安全

Collection of PI
- 合法性要求和最小化要求
- 授权同意和例外
- 敏感信息明示同意
- 隐私政策的内容和发布

External providing of PI
- 委托处理要求
- 共享、转让要求
- 收购、兼并、重组要求
- 公开披露要求
- 共同的个人信息控制者要求
- 跨境传输要求

Retention of PI
- 保存时间最小化
- 去标识化处理
- 敏感信息存储
- 个人信息控制者停止运营

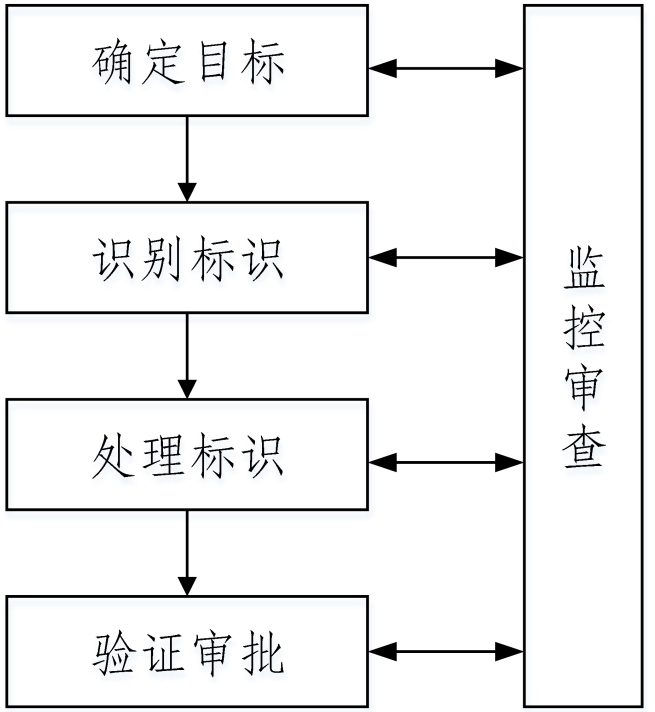
Use of PI
- 访问控制措施
- 使用和展示限制
- 访问、更正、删除、撤回同意、注销账户、获取副本等机制
- 响应个人信息主体的请求和申诉管理

- 本标准描述了个人信息去标识化的目标和原则，提出了去标识化过程和管理措施。

- 本标准针对微数据提供具体的个人信息去标识化指导，适用于组织开展个人信息去标识化工作，也适用于网络安全相关主管部门、第三方评估机构等组织开展个人信息安全监督管理、评估等工作。

去标识化原则

- 合规
- 个人信息安全保护优先
- 技术和管理相结合
- 充分应用软件工具
- 持续改进



去标识化过程

GB/T 35274-2017《大数据服务安全能力要求》

- 本标准规定了：
  - 大数据服务提供者应具有的组织相关的基础安全要求；
  - 数据生命周期相关的数据服务安全要求；
  - 大数据平台与应用安全运行相关的系统服务安全要求。
- 本标准可为政府部门、企事业单位等组织机构的大数据服务安全能力建设提供参考，也适用于第三方机构对大数据服务提供者的大数据服务安全能力进行审查和评估。

本标准将大数据服务安全能力分为一般要求和增强要求两个级别。

一般要求

- 能够抵御或应对常见的威胁
- 能够控制损失在有限的范围和程度内
- 具备基本的事件追溯能力

增强要求

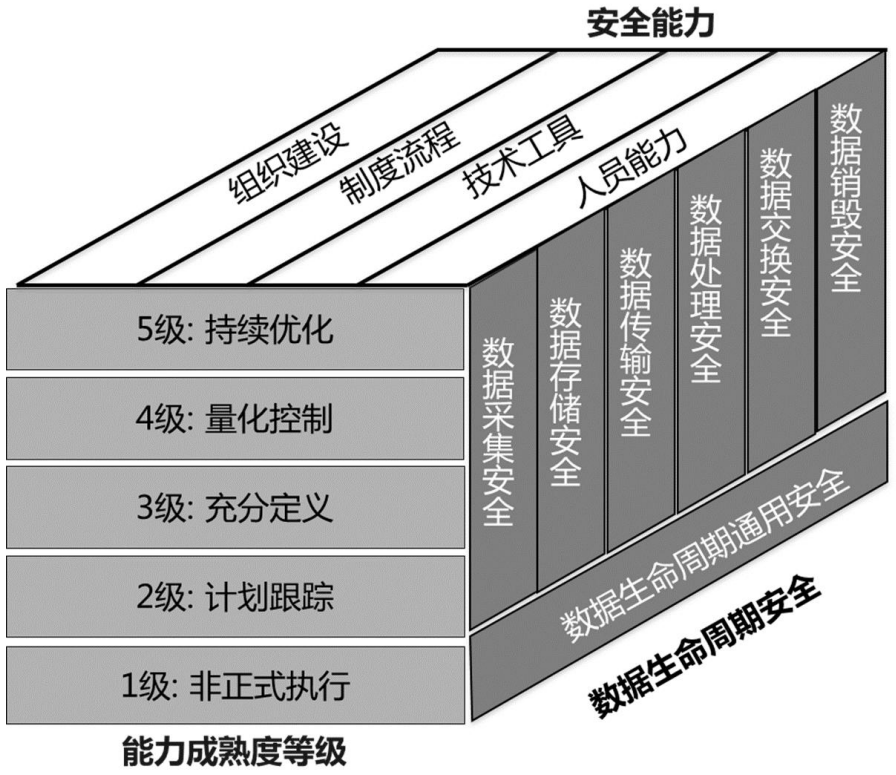
- 涉及国家安全，或对经济发展和社会公共利益有较大影响
- 主动识别并防范潜在攻击的能力
- 高效应对安全事件并将其损失控制在较小范围内
- 保证安全事件追溯的有效性
- 保证大数据服务的可靠性、可扩展性和可伸缩性

GB/T 37973-2019《大数据安全管理指南》

- 本标准提出了大数据安全管理基本原则，指导组织开展大数据安全需求分析、数据分类分级、大数据活动和风险评估 等安全管理工作。
- 本标准适用于各类组织进行数据安全管理，也可供第三方评估机构参考。

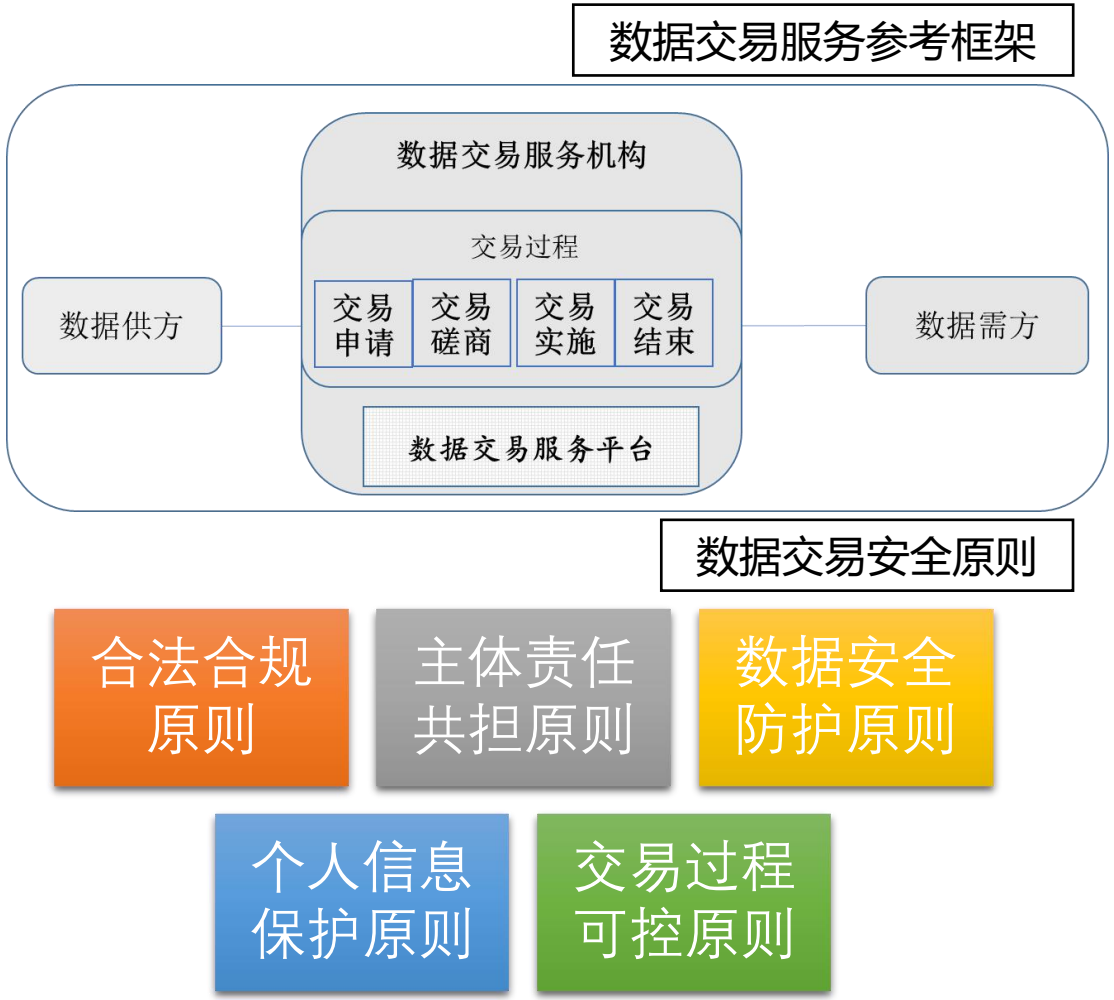
- 本标准规定了组织机构数据安全保障的能力成熟度模型：
  - 以数据为中心
  - 重点围绕数据生命周期
  - 从组织建设、制度流程、技术工具和人员能力四个方面进行安全保障。
- 本标准适用于对组织机构数据安全能力进行评估，也可供组织机构开展数据安全能力建设时参考。

数据安全能力成熟度模型



GB/T 37932-2019《数据交易服务安全要求》

- 本标准将对数据交易服务进行安全规范，增强对数据交易服务的安全管控能力，在确保数据安全的前提下，促进数据资源自由流通，从而带动整个数据产业的安全、健康、快速发展。
  - 数据交易参与方
  - 交易对象
  - 交易过程
- 本标准适用于数据交易服务机构进行安全自评估，也可供第三方测评机构对数据交易服务机构进行安全评估时参考。



三、标准应用实践

数据安全标准宣贯

1 标准宣贯研讨交流

标准宣贯研讨交流

- 网安安全产业联盟专题研讨
- 全国政务外网安全培训宣贯
- 互联网金融协会交流培训
- 冬奥组委、文化部、汽车行业、医疗行业等培训交流
- 发布系列解读文章20余篇

宣贯活动超过二十余次，受众超过万人

2017年隐私条款专项工作

工作内容

2017年，在网信办、工信部、公安部、市场监管总局等四部门指导下，选取用户数量大、与民众生活密切相关、社会关注度高的10款互联网应用产品和服务进行评审，分别为：微信、淘宝网、京东商城、支付宝、高德地图、百度地图、滴滴出行、航旅纵横、携程旅行网、新浪微博。

评审活动受到全社会广泛关注，参评产品和服务上线新版隐私政策，调整相应功能，更新和上线新版本。参评的十家互联网企业，在评审结束后，主动加入了**个人信息保护倡议**。

后续跟踪8类**100款常用App**，发现**60%App**参照首批产品的隐私条款和实现机制进行了更新。

个人信息保护标准应用

2018年隐私条款专项工作

工作内容

2018年，选取与民众日常生活紧密相关、具有较大用户数量的**出行旅游类、生活服务类、影视娱乐类、工具资讯类和网络支付类5类30款网络产品**，采用自研的个人信息保护专项评审工具，对其隐私政策及实现机制进行评审，帮助机构提升个人信息保护水平。专家组对专项工作给予了充分肯定和高度评价。

个人信息保护标准应用

2019年支撑“App违法违规收集使用个人信息专项治理行动”

- 牵头制定《大众化应用基本业务功能必要信息规范》，参与制定《App违法违规收集使用个人信息治理评估要点》。
- 《大众化应用基本业务功能必要信息规范》，主要针对地图导航、网络约车、即时通讯、社区社交、网络支付、新闻资讯、网上购物、短视频、快递配送、餐饮外卖、交通票务、婚恋相亲、求职招聘、金融借贷等典型类别大众化应用基本业务功能，给出了各类基本业务功能正常运行所需收集的必要个人信息。
- 国家标准《移动互联网应用（App）收集个人信息基本规范》

二、全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会，依据法律法规和国家相关标准，编制大众化应用基本业务功能及必要信息规范、App违法违规收集使用个人信息治理评估要点，组织相关专业机构，对用户数量大、与民众生活密切相关的App隐私政策和个人信息收集使用情况进行评估。

数据安全标准推广应用

《信息安全技术 数据安全能力成熟度模型》

现已正式发布（GB/T 37988-2019），国际标准同步推进

1 政府支撑下的标准试点

已在贵阳大数据局、成都网信办、武汉硚口区三地政府支持下在当地开展近20个应用试点。

2 生态企业推广

在包括国泰产险、邦道科技、中和农信、中交兴路、小码科技、公交云、米雅科技、钧正网络、信美人寿、易诚互动等蚂蚁金服的TOP300生态企业中推广，识别生态企业整体数据安全能力水位，并通过评估，有针对地提出建议，推动头部生态企业的数据安全能力提升。

3 2018年TC260标准试点

2018年TC260通过自研评估工具，选择10家数据量大、数据应用典型、具有行业特点的企业开展标准试点：

阿里健康（互联网医疗）	旷视科技（人工智能）
美团金融（金融）	成都人社（社保）
货车帮（互联网物流）	软通动力（互联网）
银川大数据局（政务）	携程（旅游）
天弘基金（金融）	上海如家（酒店）

数据安全标准推广应用

《信息安全技术 数据安全能力成熟度模型》

4 2019年TC260标准应用推广

2019年开展国家标准GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型》国家标准应用推广试点工作，20余家机构参与试点工作。

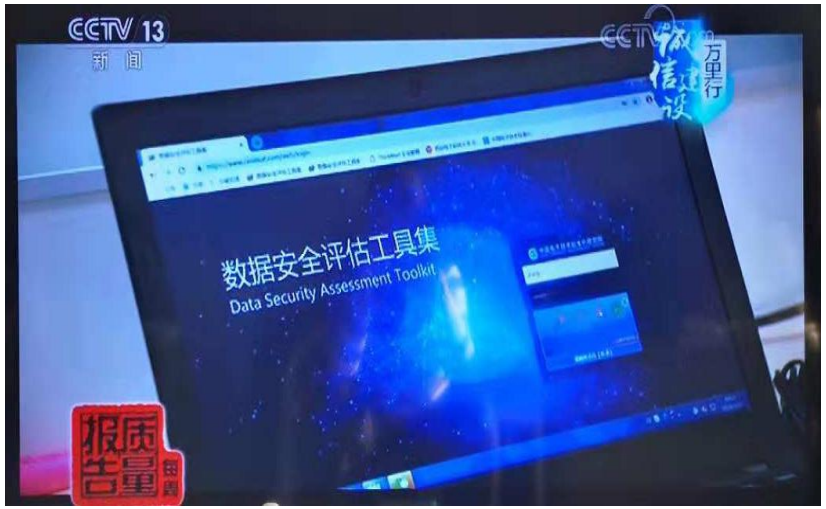
- 北京腾云天下科技有限公司
- 京东数字科技控股有限公司
- 联通大数据有限公司
- 奇安信科技集团股份有限公司
- 中国第一汽车集团有限公司
- 博彦科技承德有限公司
- 顺丰速运有限公司
- 医渡云（北京）技术有限公司
- 国家电网有限公司大数据中心
- ……

5 标准覆盖

标准应用实践已覆盖二十余个重点行业，上百家典型企业

- 制造业：乳制品制造、电器制造
- 软件行业：税务软件、地图软件
- 金融行业：互联网金融、证券
- 文娱行业：体育、音乐、视频领域
- 零售行业：电器销售、百货零售
- 物流行业：物流公司
- 电力行业：电力公司
- 服务行业：酒店
- 互联网+新型企业

伊利 · 中国南方电网 广州供电局有限公司 · YOUKU · 首旅如家 · 广发证券 GF SECURITIES · SAKURA 樱花 · 拾羽 · 百世 · 微贷网 · 高德 AutoNavi · 小站教育 zhan.com · 龙图信息 DRAGON DREAM · 极课大数据 · iSoftStone · 更多…



敬请指正

秉承“科学 公正 创新 服务”的精神，履行“支撑政府 服务产业 奉献标准化最大价值”的使命，加快把电子标准院建成国内一流、国际知名的创新型现代化科研机构。

信息安全研究中心数据安全部，主要负责数据安全、个人信息保护、人工智能安全方向的标准研制、技术科研、政府支撑和安全服务。

联系方式：(010)64102745
联系邮箱：pipcat@cesi.cn
联系地址：北京市东城区安定门东大街1号


2020北京网络安全大会
2020 BEIJING CYBER SECURITY CONFERENCE
THANKS
全球网络安全 倾听北京声音