DXCon 2021

国际数字化转型最佳实践管理峰会

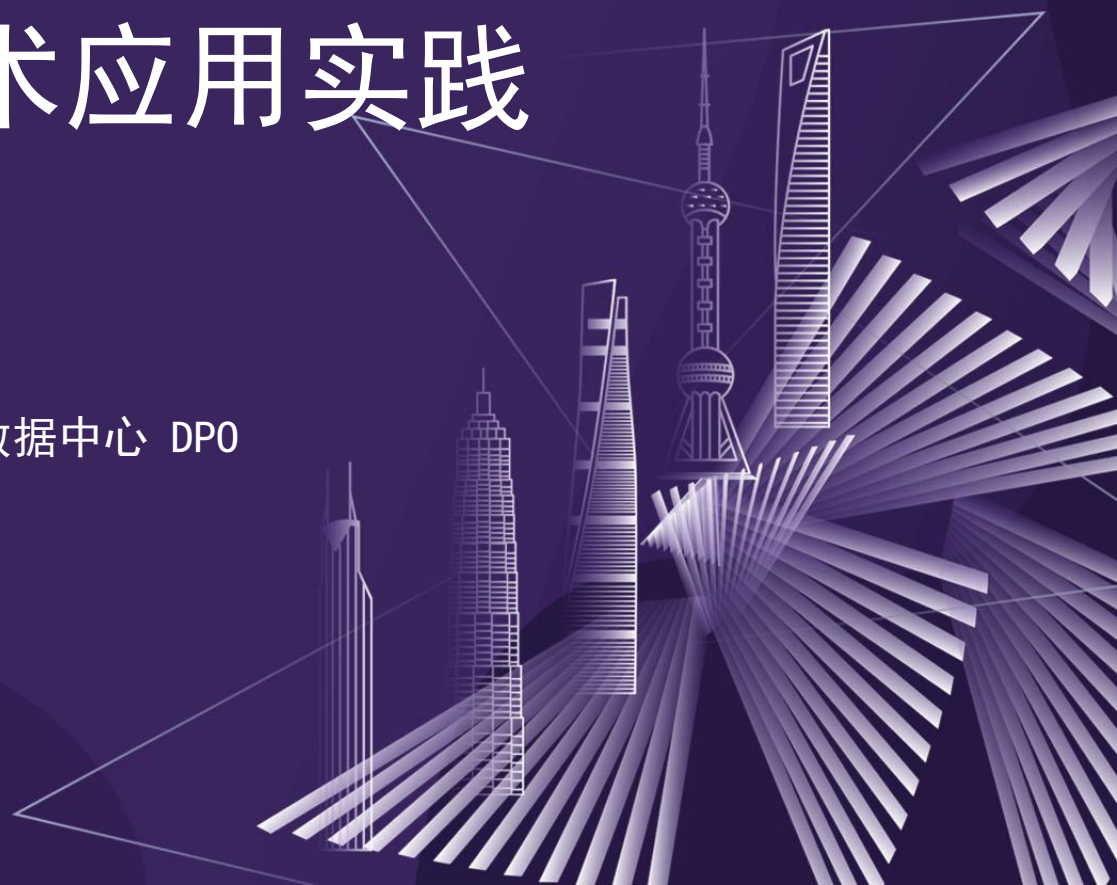
– 4月16日 •上海 –

隐私与数据保护技术应用实践

刘 骊

龙盈智达（北京）科技有限公司 大数据中心 DPO

主办方: EXIN BEST PRACTICE



刘 骊 （Mary）

龙盈智达（北京）科技有限公司 大数据中心 DPO

领域：隐私与数据保护、IT服务管理、业务连续性管理、信息安全管理等；

第一届参加DPO培训成员，第一批为国内企业提供GDPR咨询服务的团队成员，DPO讲师。

主要认证：

- DPO （EXIN 认证讲师）
- CIPP-E （Certified Information Privacy Professional/Europe, IAPP）
- ISO 27701 Management Professional （DNV）
- ITIL 4 Managing Professional （PeopleCert, AXELOS）
- CBCP（DRI 国际灾难恢复协会专业认证）
- PMP （PMI项目管理学会）

骊-Mary

北京 朝阳

思考：从桌面到地面的距离

一、数据与隐私保护的工具与技术

二、数据保护的典型技术实践初探

- 可用不可见：隐私计算及安全多方计算
- 分而治之：自然语言处理（NLP）的数据分类分级

一、数据与隐私保护的工具与技术

类型	主要功能	工具、技术举例
咨询管理类	提供及时更新的国家以及全球隐私保护动态和相关法律法规要求。	咨询服务、DPO职能外包、法规跟踪
	实现并记录个人信息保护工作“计划、执行、监督、反馈”闭环，为银行提供个人信息保护工作的有效证明；隐私政策的维护更新等。	沟通及流程工具、培训与专业拓展、
隐私评估类	开展定期的、持续的隐私影响评估及合规风险评估等。识别、分析个人数据的风险，以制定合理的保护措施及风险应对措施。	合规风险评估工具、数据影响分析工具
数据主体权益类	记录、维护用户对数据使用的同意授权，实现可选择、可撤销、可更新的用户同意。	同意管理、数据主体请求管理
	管理cookies设置、APP授权等。	Cookies管理
事件管理类	及时发现、响应数据泄露风险及事件，快速控制影响范围，及时上报监管，以及妥善进行客户沟通。	事件响应与管理
	对可能已泄露的数据，监控网络中的个人信息售卖、身份冒用、盗用行为，保护客户权益。	网站扫描、网络信用监控
数据管理类	通过手动或自动表单填写来帮企业勾勒出数据流图，实现数据全生命周期的可控处理。	数据地图、数据血缘分析、数据标签
	扫描数据，根据规则进行分级分类，便于企业梳理存量数据，作为隐私风险合规及管控的基础。	数据发现、数据分类、数据资产管理
数据处理及安全类	对个人数据实现脱敏保护，对沉淀数据实现匿名化保护，实现数据可用不可见。	数据销毁、数据匿名化、数据去标识
	监控个人信息被谁访问，做了什么操作，并提供阻断等控制措施。	数据行为监控、SDK检测
	隐私计算及加密，通过密文或混淆明文方式实现多方数据安全共享、汇总、计算、联合建模等处理。	安全多方计算、同态加密、差分隐私、可信执行环境 、零知识证明、联邦学习
其它	数据安全与隐私保护相关的诉讼服务、保险等。	网络安全保险、数据泄露保险

1.1 咨询与管理类工具

- DPO、咨询顾问、法律顾问等在数据与隐私保护领域提供评估、建议、指导和专业知识；
- 跟踪相关国家和地区的数据与隐私相关法律法规、指南、司法解释、案例等的最新信息。

领域动态

保持对法规、监管、技术等动态发展的了解

- 搜索关于数据保护、隐私保护的法律法规、行政决定、事件、技术工具、行业动态等的新闻及信息，抽取相关内容
- 提供相应的合规提示、行动建议、趋势预判等
- 相关领域知识库管理和维护

法规对标

法规基线以及合规的统一性和差异性

- 监测变化的法律和法规，判例法，执法行动，和官方指南
- 了解最新的执法判例、司法解释、执法和处罚跟踪
- 利用GDPR（或其它较完善的法规）作为基准，识别相关隐私法之间的关键相似性及差异性，确定企业合规基线

管理体系

隐私与数据保护管理体系、人员组织、沟通机制、运作空间

- 为隐私与数据保护项目、工作范围和职责功能等提供运行保障
- 组织和维护易于访问和反馈的指导说明和规程文档
- 建立沟通协调机制，确保关键信息被发送到每个相关成员

行动指导

指导企业解决业务和运营过程的具体问题

- 适用性研究，识别适用的立法和监管部门的指导意见
- 结合业务发展规划和业务范围流程等，解决特定的隐私保护的问题
- 形成“基于设计和默认”的隐私与数据保护机制

1.2 评估类工具

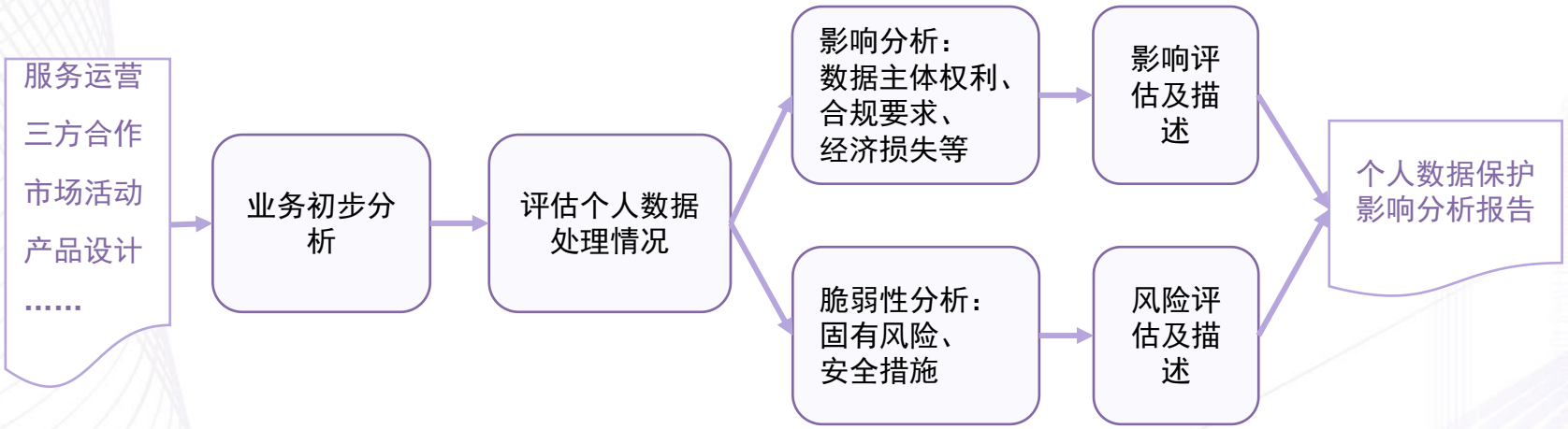
隐私与数据保护中的各种评估作为隐私保护的策略、功能与产品设计、服务过程、技术决策等的依据。
包括：
隐私及数据保护合规评估及差距分析、隐私影响评估、数据保护影响评估、供应商风险评估、数据安全风险评估、数据主体请求评估等等。

流程化的自动评估

创建、分发和分析PIAs和DPIAs，自动化、有效地实现“基于设计的隐私” 。可管理评估模板库，可根据组织工作流程进行工作过程定制。

不同的评估模板以及灵活调整

提供隐私影响评估(PIA)，供应商风险评估，主体权利请求和数据泄露事件评估等评估模板，并通过参数、选项等灵活控制。



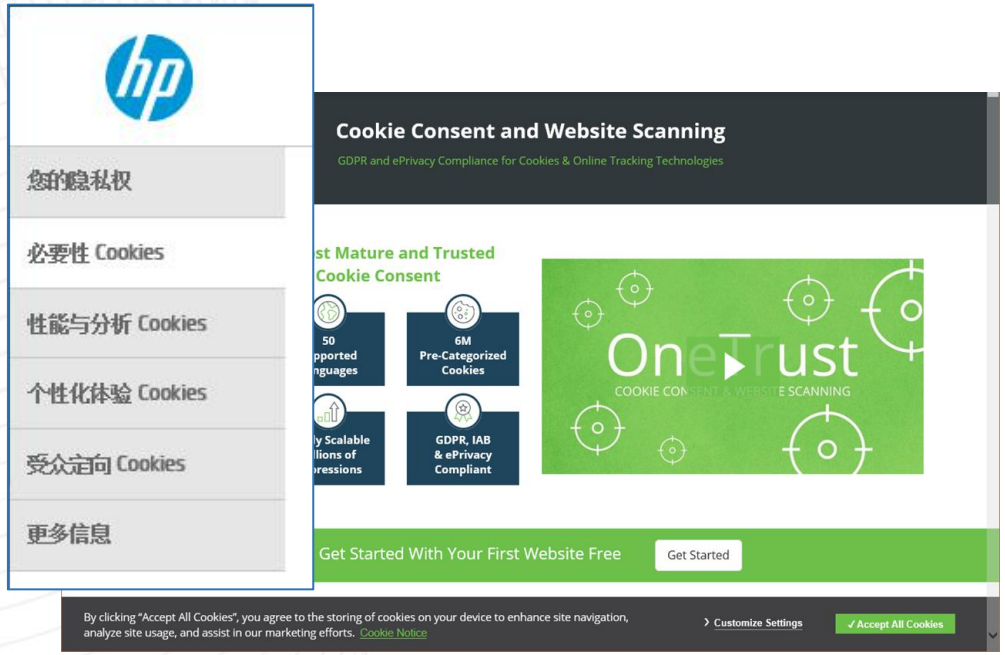
DPIA主要流程

1.3 数据主体权益类工具

“同意”：

指的是数据主体通过一个声明，或者通过某项清晰的确信行动而自由作出的、充分知悉的、不含混的、表明同意对其相关个人数据进行处理的意愿。（GDPR 第4条）

请求获得同意应当完全区别于其他事项，并且应当以一种容易理解的形式，使用清晰和平白的语言。（GDPR 第7条）



跨渠道收集同意书

集成到现有的许可收集工作流程中，包括网页表格、移动应用程序、电子邮件、电话、纸质表格、人工面对面、视频等。使用SDK、API或通过批量数据提要导入，同意被记录并集中存储。

允许细分的偏好选择（opt-in or opt-out）

让数据主体对他们的信息偏好有更大的控制和可见性。通过提供选择下拉选项或调整交流的频率、话题和内容，减少全盘撤回同意的情况。

创建用户同意的审计记录

通过集中存储，生成细粒度的报告，以简化内部和外部审计。保持最新和完整的同意记录，包括详细的记录，如谁同意、同意的信息及功能、同意方式等。

与现有系统的同步

与现有业务应用程序集成，在客户关系管理(CRM)和营销自动化应用程序、标签管理器、内容管理系统(CMS)和其他技术中保持准确的沟通首选项和同意细节。

1.3 数据主体权益类工具

数据主体权益满足：
协助希望行使其数据主体权利的个人进行查询、知情、更正、可携带及删除信息的权利的要求。

- 自动完成数据主体请求，以提高响应时间、降低成本，实现数据主体请求并建立客户信任。
- 通过配置自动化工作流的能力，结合隐私策略解决方案，动态评估数据主体请求，并安全地向其提供准确的响应，并且所有响应都在所需的监管时间限制内。

多部门协调联动
提供权益满足服务

安全的身份识别认证体系
敏感判断、服务提供的判断

端到端的服务与处理流程
保障数据主体满意度

根据业务变化灵活调整
满足变化的法规要求

1.4 事件管理类工具

数据泄露处置难点

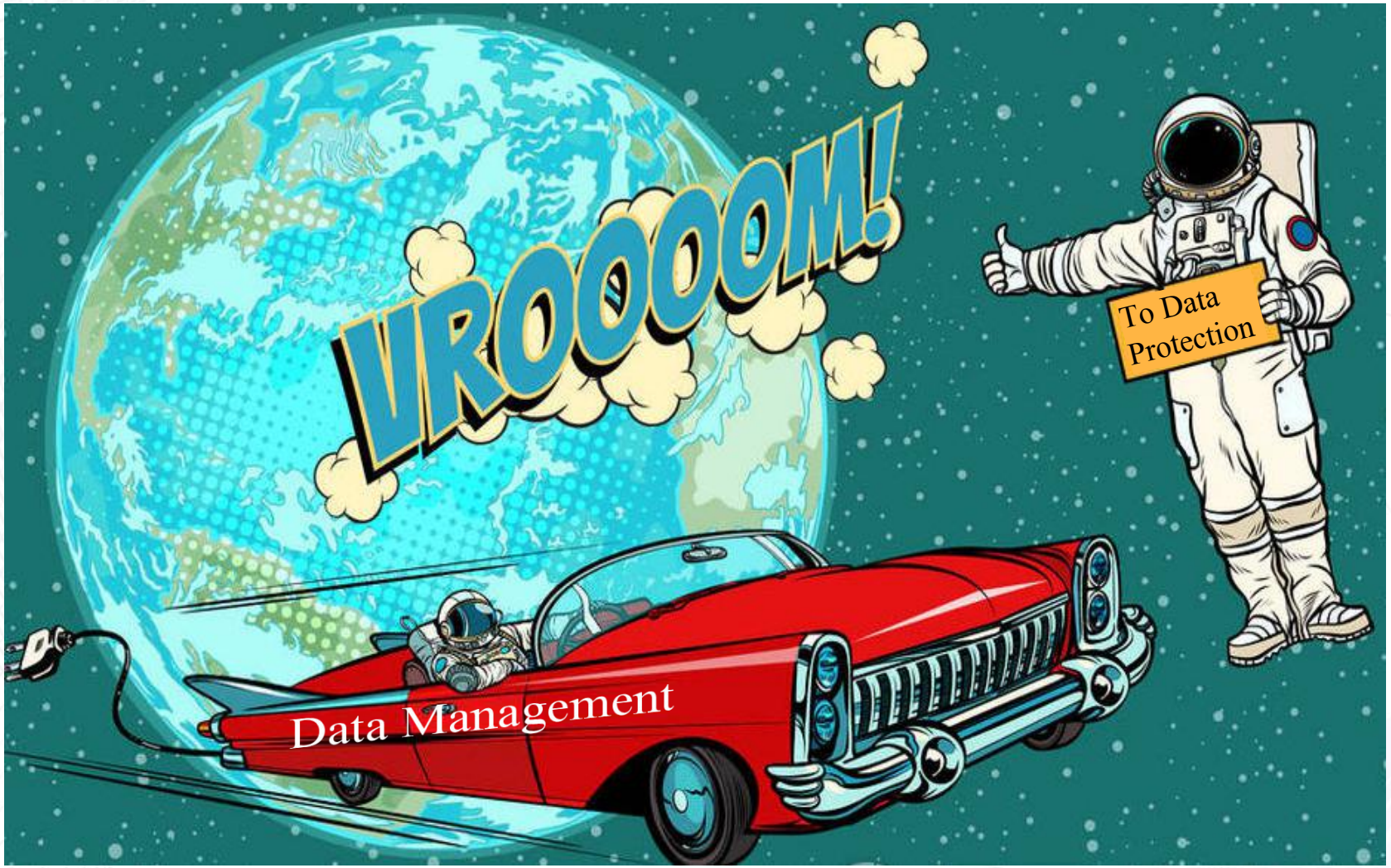
- **事件评估：**

  事件性质、范围、规模、影响……

- **通知流程：**

  - **处理者**：最快的第一时间告知控制者
  - **控制者向监管**：监管要求的上报的标准和时间，确定是否上报，以及上报的内容（事件性质、涉及人 员规模、数据规模、已有措施、可能的影响、后继措施等）……
  - **代理者**：最快的一时间报告给被代理方。
  - **控制者向数据主体**：是否需要通知？通知谁？通知的内容？通知的方式和渠道……
  - **媒体沟通**：对外媒体的沟通时机、内容、方式等……

1.5 数据管理类



1.5 数据管理类

数据资产管理

开发、执行和监督有关数据的计划、政策、方案、项目、流程、方法和程序，从而控制、保护、交付和提高数据资产的价值。

主要功能：
- 数据资产目录
- 主数据管理
- 元数据管理
- 数据资产使用管理
- 数据标签

数据发现和分类

提供用于发现、分类、标记和报告数据库中的敏感数据的基本功能。

主要功能：
- 发现和建议
- 敏感度标记
- 计算数据集的敏感度
- 可视化

数据地图

以手动或自动的形式确定整个企业的数据流。

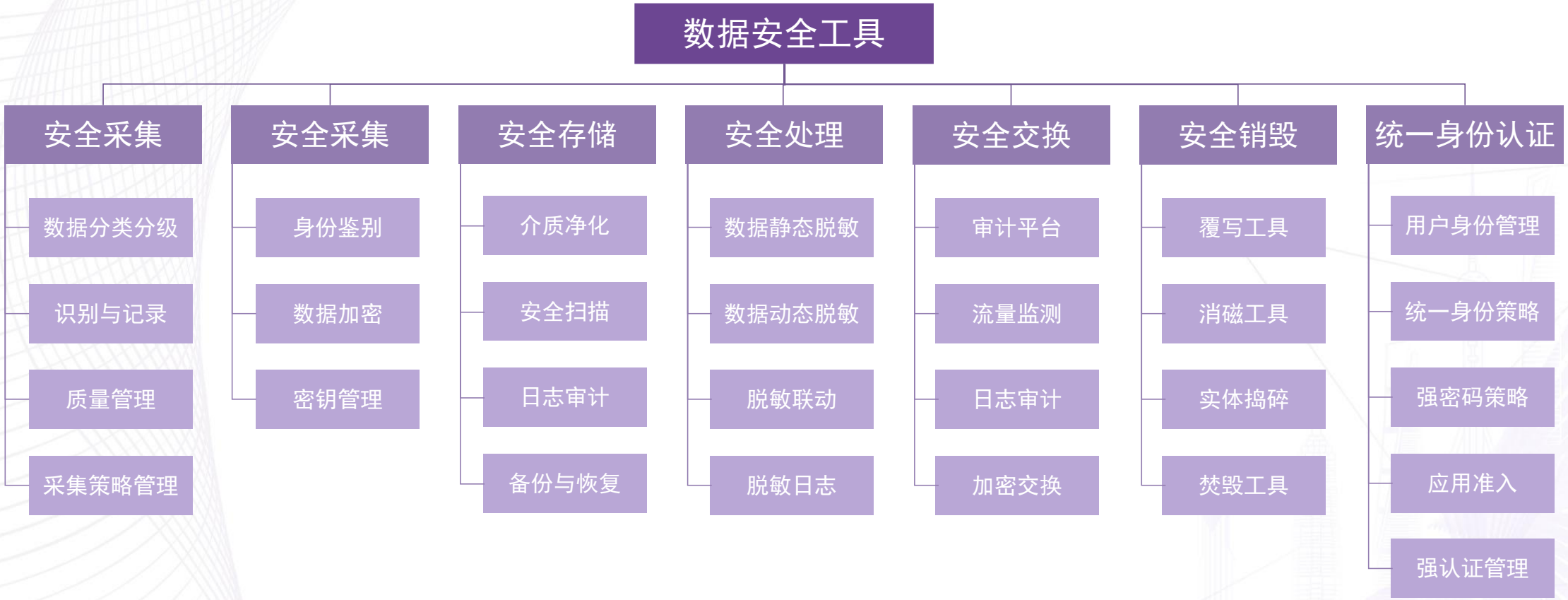
主要功能：
- 数据概览
- 元数据查看
- 数据预览
- 数据目录
- 数据检索
- 数据注释

血缘分析

一般放在数据地图/数据管理，是对数据的上下游进行来龙去脉的分析。

主要功能：
- 数据来源跟踪
- 数据影响分析
- 任务依赖分析
- 影响分析报告

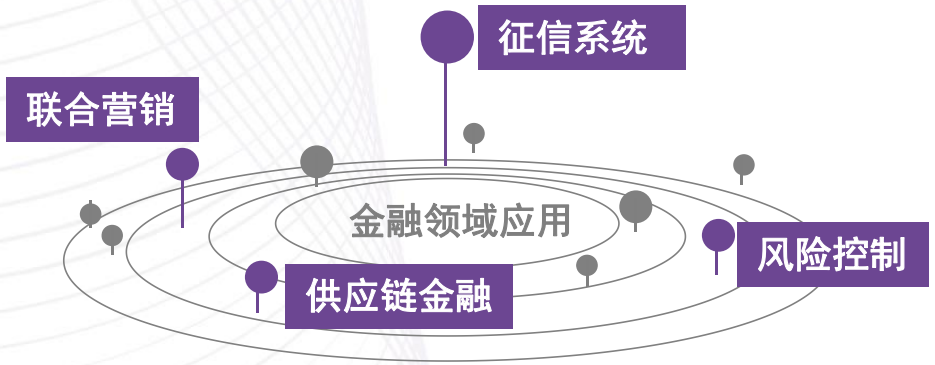
1.6 数据处理及安全类



源自：数据工匠俱乐部

1.6 数据处理及安全类

隐私计算是指借助现代密码学和信息安全技术， 在保证原始数据安全隐私性的同时， 实现对数据的计算和分析。



安全多方计算

能够实现计算参与各方在原始数据保留在各自本地的情况下， 完成数据的协同分析， 并产生正确的结果。

同态加密

同态加密可实现对密文数据进行任意函数的计算，这意味着将原始数据加密后，通过一个计算资源强大的第三方，即能对数据拥有者的数据密文进行所需的处理分析。

零知识证明

零知识证明技术是一种特殊的证明系统。在这一证明系统里，证明者知道关于某个问题的答案，他要向验证者证明“他知道答案”， 但是要求验证者不能获得答案的任何信息。

可信执行环境

可信执行环境（TEE） 通过硬件技术对数据进行隔离保护，将数据分类处理。支持TEE的CPU中，有一个特定的区域，该区域的作用是给数据和代码的执行提供一个更安全的空间。

联邦学习

联邦学习本质上是一种分布式机器学习技术， 或机器学习框架， 其目标是在保证数据隐私安全的基础上，实现共同建模，提升AI模型的效果。

差分隐私

差分隐私指通过对原始数据进行转换或者是对统计结果添加噪音来实现隐私保护。 差分隐私技术的研究主要面向传统数据隐私安全中的数据脱敏、匿名化等问题。

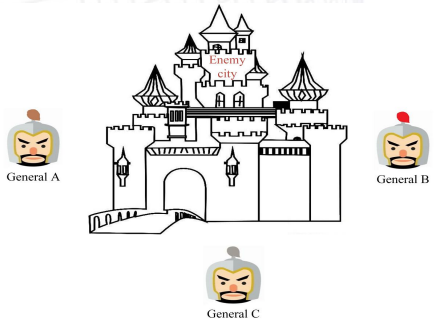
一、数据与隐私保护的工具与技术

二、数据保护的典型技术实践初探

1. 可用不可见：隐私计算及安全多方计算
2. 分而治之：自然语言处理（NLP）的数据分类分级

2.1 可用不可见：隐私计算及安全多方计算

秘密共享(Secret-Sharing) 是多方安全计算和联邦学习等领域的一个基础应用技术，它源于经典密码理论，最早由Sharmir和Blakley在1979年分别独立地提出秘密共享的概念，并给出了(k,n)门限秘密共享方案。(k,n)门限秘密共享表示把秘密信息分成n份无意义的子秘密，只有拥有至少k份子秘密才能恢复秘密信息。



拜占庭位于如今的土耳其的伊斯坦布尔，是东罗马帝国的首都。由于当时拜占庭罗马帝国国土辽阔，为了达到防御目的，每个军队都分隔很远，将军与将军之间只能靠信差传消息。

在战争的时候，拜占庭军队内所有将军和副官必须达成一致的共识，决定是否有赢的机会才去攻打敌人的阵营。但是，在军队内有可能存有叛徒和敌军的间谍，左右将军们的决定又扰乱整体军队的秩序。在进行共识时，结果并不代表大多数人的意见。这时候，在已知有成员谋反的情况下，其余忠诚的将军在不受叛徒的影响下如何达成一致的协议，拜占庭问题就此形成。

安全多方计算（Secure Multi-Party Computation） 主要是针对无可信第三方的情况下，如何安全地计算一个约定函数的问题。

安全多方计算起源于1982年姚期智的百万富翁问题。姚期智（1946年12月24日－），中国计算机科学家，2000年图灵奖得主，是目前唯一一位获得此奖项的华人。

两个百万富翁都想比较到底谁更富有，但是有都不想让别人知道自己有多少钱。在没有可信的第三方的情况下如何进行？

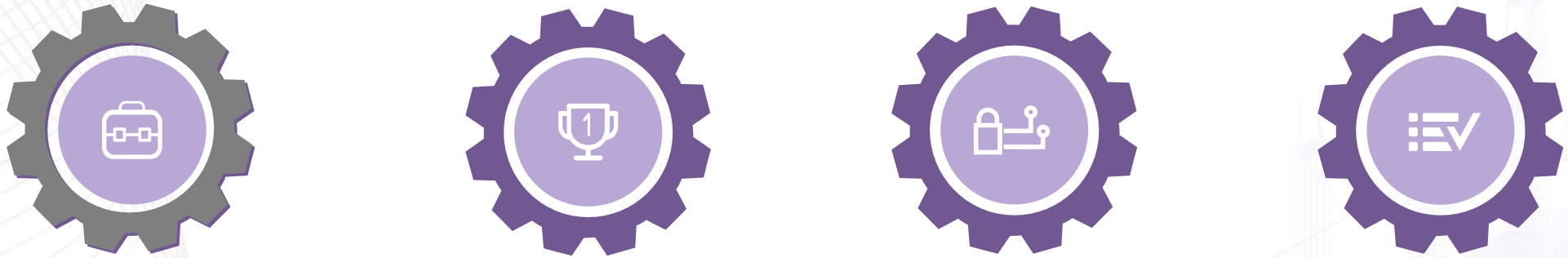
2.1 可用不可见：隐私计算及安全多方计算

保护个人隐私与商业秘密的金融风控与监管

国家普惠金融政策指引下，各家银行及金融机构纷纷放宽贷款政策；
各银行及金融机构缺乏安全可信并保护客户隐私和商业秘密的放贷数据共享手段；
单一放贷机构的风控模型无法检测借款人的多头借贷、过度授信风险；
需要一种多方参与、允许不披露各机构具体贷款金额、同时可以计算出贷款汇总金额的算法。

隐私计算

解决互不信任的参与方在保护客户隐私与商业秘密的前提下协同计算的难题！



金融风控　数据共享　隐私保护　监管合规

2.1 可用不可见：隐私计算及安全多方计算

监管要求

银保监会就《商业银行互联网贷款管理暂行办法》于7月12日发布实施。其中，第二十一条明确要求：

“商业银行应当构建有效的风险评估、授信审批和风险定价模型，加强统一授信管理，运用风险数据，**结合借款人已有债务情况，审慎评估借款人还款能力**，确定借款人信用等级和授信方案”。

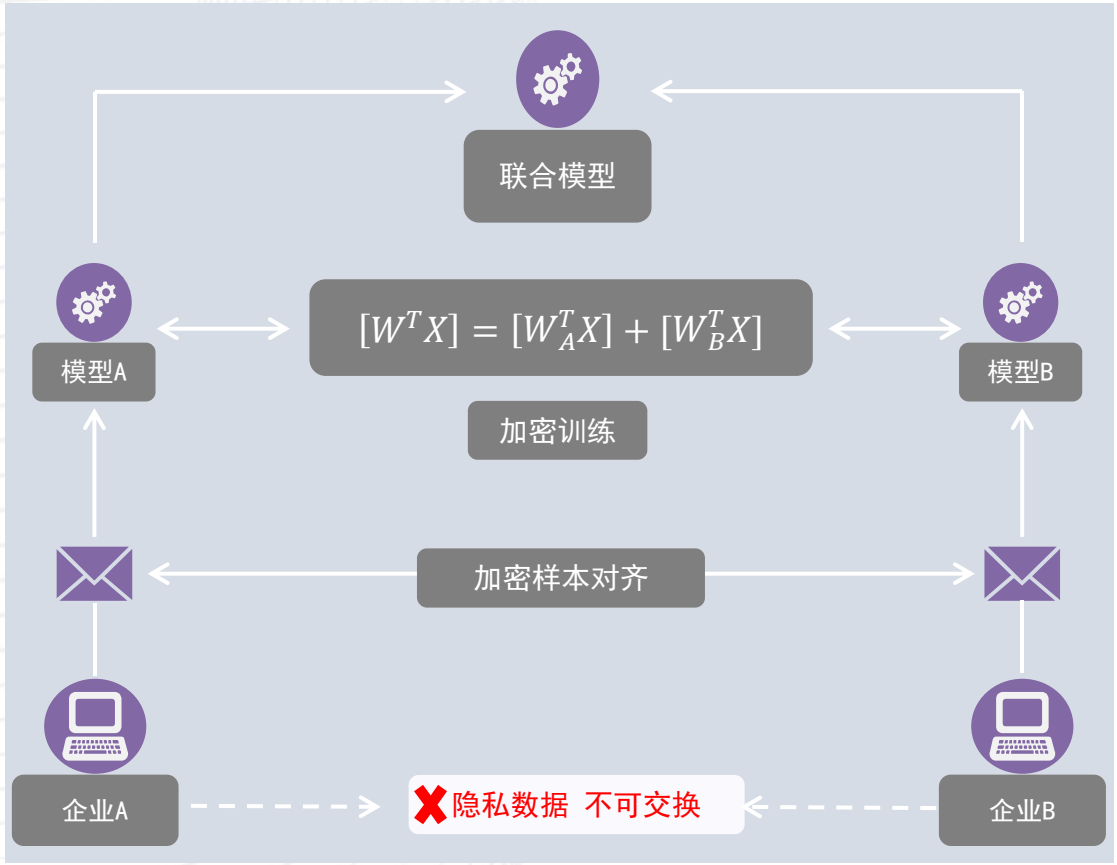
业务背景

对于各银行或小贷公司，客户在该机构的贷款金额是一个商业秘密，普遍不愿意向竞争对手共享该放贷数据。在这种情况下，企业或个人可以恶意地向多家放贷机构同时申请贷款，最终累积到远超过其还款能力的贷款金额。为了保证普惠金融政策的平稳有序执行，需要设计一种依托区块链实现的遵循安全多方计算原则的密码学算法，在各方不披露具体贷款金额（包括某方贷款为0的情况）的前提下，计算出某客户所有放贷机构的贷款总金额。

客户 \ 银行	A	B	C	D
UserA	0	50	7000	0
UserB	0	0	0	60
UserC	0	0	100	50
UserD	200	50	500	?

注：为简化展示，目前以**贷款总金额**为核心目标；后续的金融具体业务实践中，建议根据业务实际需求，可**增加贷款期限、贷款余额、风险敞口**等要素。

2.1 可用不可见：隐私计算及安全多方计算



银行A
企业D：200

$Y_A=a_0+a_1X+a_2X^2$

$Y_A=200+1X+2X^2$

X=0, Y=200
X=1, Y=203
X=2, Y=210
X=3, Y=221

银行B
企业D：50

$Y_B=b_0+b_1X+b_2X^2$

$Y_B=50+3X+4X^2$

X=0, Y=50
X=1, Y=57
X=2, Y=72
X=3, Y=95

银行C
企业D：500

$Y_C=c_0+c_1X+c_2X^2$

$Y_C=500+5X+6X^2$

X=0, Y=500
X=1, Y=511
X=2, Y=534
X=3, Y=569

交 换

X=1, Y_A=203
X=1, Y_B=57
X=1, Y_C=511

X=2, Y_A=210
X=2, Y_B=72
X=2, Y_C=534

X=3, Y_A=221
X=3, Y_B=95
X=3, Y_C=569

Y_1 = 203+57+511=771

Y_2 = 210+72+534=816

Y_3 = 221+95+569=885

智能合约上链

X=1, Y = 771 = $\alpha_0 + 1\alpha_1 + 1\alpha_2$
X=2, Y = 816 = $\alpha_0 + 2\alpha_1 + 4\alpha_2$
X=3, Y = 885 = $\alpha_0 + 3\alpha_1 + 9\alpha_2$

α_2 = 12, α_1 = 9, α_0 = 750 （即： 200+50+500）

2.2 分而治之：自然语言处理（NLP）的数据分类分级

数据分类分级是数据治理工作的基础工作，是数据治理标准化、自动化、智能化的前提保障工作之一。
确立合理合规的分类角度、维度和颗粒度，建立数据分类分级的模型框架，为数据资产的使用和保护提供保障和基础。

资产清点：

要将数据作为资产管理的第一步是需要厘清银行究竟有哪些数据，数据分类是建立资产台账的前提。

资产估值：

在数据分类的前提下，方可梳理不同类型资产的规模、数量、成本、价值。

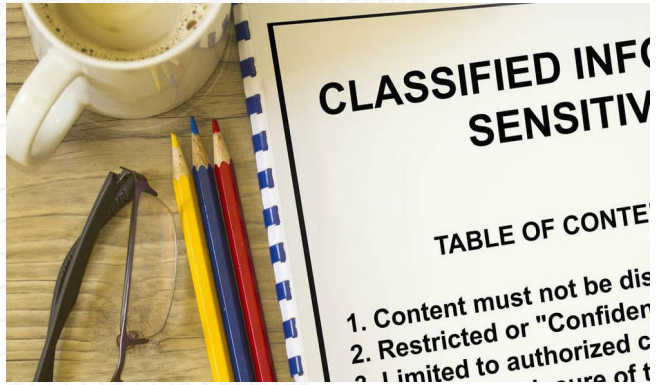
开放共享：

细化的数据分类分级规则，通过配套差异化的安全控制措施，充分释放数据资源价值潜能，又能够有效控制成本投入的最佳路径。

金融领域

2020年人民银行发布《个人金融信息保护技术规范》和《金融数据安全分级指南》两大金融标准，明确出金融数据的分类分级的严格要求。
包括：
客户签订的合约协议类文本、对客户进行尽职调查类文本、客户对银行的好差评文本、客户对银行的咨询建议类文本、银行内部的审计报告类文本、银行内部会议纪要类文本、银行内部员工绩效数值类文本（述职，工作总结报告等）

2.2 分而治之：自然语言处理（NLP）的数据分类分级



非结构化数据中的敏感信息识别

1、在非结构化数据（包括文本、图片识别文字等）中的分类分级
2、结构化数据表中的大段文字描述类的字段

敏感信息不可见的自动解读、处理

1、输入提示：账号、密码信息
2、信息脱敏传输：确定不同安全级别
3、敏感信息辅助处理：如敏感信息字段的内容进行质量检查。
4、个人身份再识别检查、敏感度计算

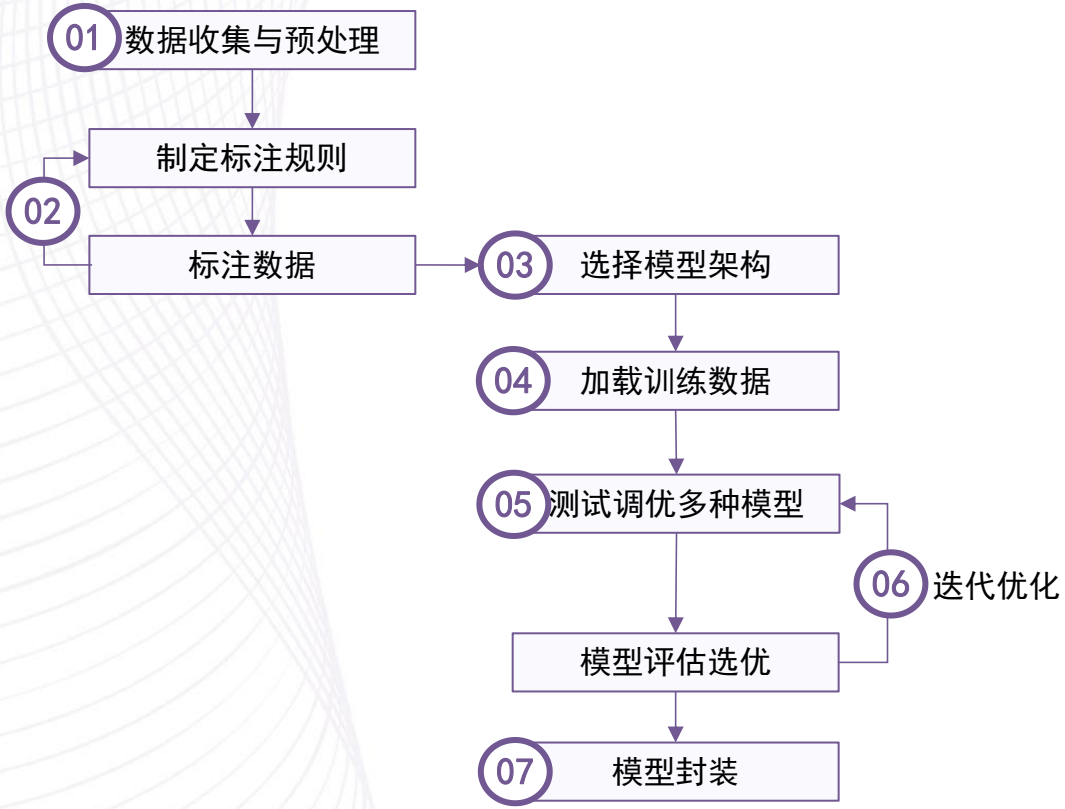
对敏感信息的监控以及审计检查

1、舆情监控、社交媒体监控：识别社交媒体中个人信息泄露（如防疫流调报告泄露），及时进行干预处理，追溯信息源头和路径。
2、数据自动化审计：在低敏感度级别的数据库中，检查是否包括高敏感信息，以验证数据分级的执行情况。

2.2 分而治之：自然语言处理（NLP）的数据分类分级

采用半监督学习，利用大量的无标签样本和少量的有标签样本来训练分类器，解决有标签样本不足这个难题。

例如：针对数十万条客户留言，人工对数千条信息进行标注（一般个人信息、公司信息、隐私信息、公开信息、舆情信息、服务投诉等）后，投入模型训练，经过反复调优、测试等，确定最终模型；用于个人信息发现、服务优化、舆情监控等。



01 准备数据，清洗数据，以及其他准备

02 根据数据指定标注规则，并在实际标注过程中不断反馈修改规则

03 筛选适合的模型架构，包含机器学习和深度学习模型，得到备选模型

04 利用准备好的数据训练备选模型，并对所有备选模型进行调优

05 利用训练测试数据，记录所有备选模型的准确率，性能等指标

06 利用测试数据，综合选取准确率高，性能优秀的模型

07 确定模型，记录结果，并封装模型

Thanks

感 谢 聆 听