随着新一轮科技革命和产业变革的不断推进，以大数据为代表的数据资源正向生产要素的形态演进，对生产力发展、生产关系变化都产生了深远影响。2020年4月9日，中共中央、国务院印发《关于构建更加完善的要素市场化配置体制机制的意见》，把数据从重要资源提升为关键生产要素，将促进大数据发展作为国家战略。同时，我国数据安全和保护的法律法规也日益完善，网络信息治理和数据保护基础法律的“三驾马车”——《中华人民共和国网络安全法》(以下简称《网络安全法》)《中华人民共和国数据安全法》(以下简称《数据安全法》)和《中华人民共和国个人信息保护法》(以下简称《个人信息保护法》)均已施行，为数据要素的有效保护和合法利用提供了制度保障。

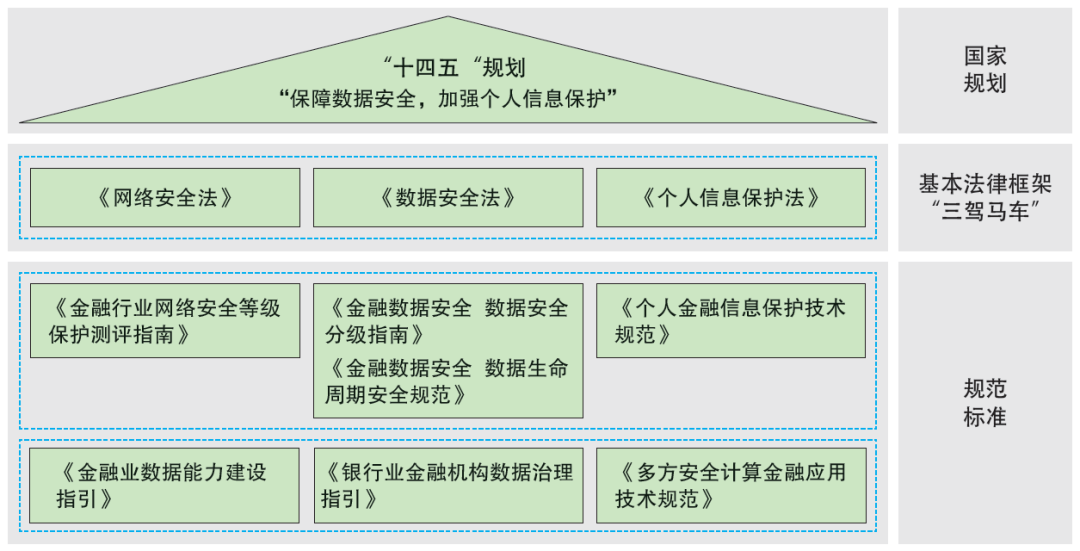
在银行的经营发展中，数据要素具有基础性、全局性和引领性作用。如何完善数据治理方法和制度，促进数据要素合法、安全、有效流通，充分发挥数据要素价值，是新时代银行面临的重要课题，也对金融数据安全技术提出了新的挑战。

**一、金融行业数据能力与合规建设指导体系**

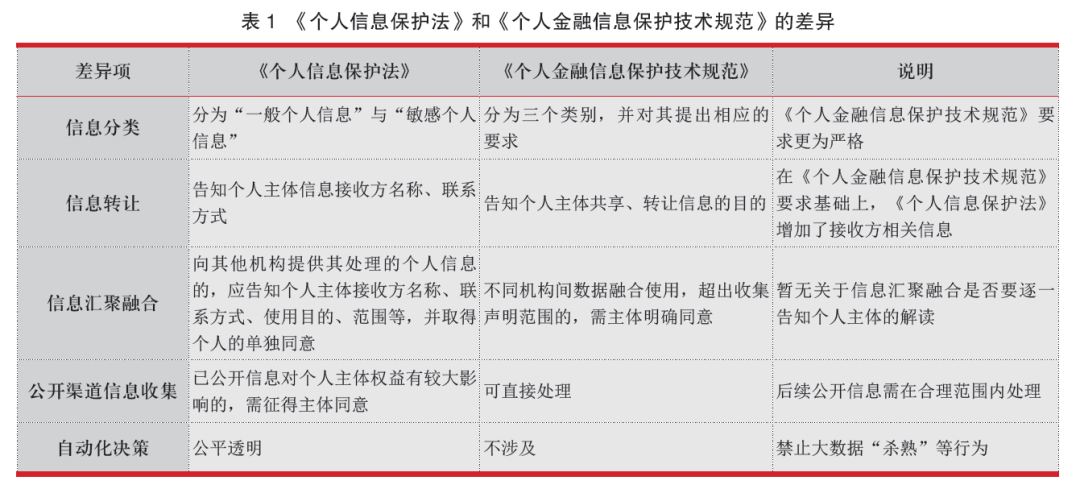
**1.上位法的行业对标分析**

《网络安全法》明确提出了有关国家网络空间安全战略和重要领域安全规划等问题的法律要求，宣示了我国的网络空间主权;《数据安全法》为数字经济合规发展保驾护航;《个人信息保护法》从国家层面建立健全个人信息保护制度。上述法律共同构成了我国网络安全与数据保护领域的基本法律框架。

我国金融业当前实施的行业标准、规范，也是根据相关法律或征求意见稿，立足金融行业制定的推荐性标准(如图1所示)。《数据安全法》强调数据分级分类和数据生命周期管理，而《金融数据安全数据安全分级指南》提出了金融数据安全分级的目标、原则和范围，明确了数据安全定级的要素、规则和定级过程。在数据的生命周期管理方面，《金融数据安全数据生命周期安全规范》在数据分级的基础上，明确了金融数据生命周期的安全框架，构建涵盖数据采集、传输、存储、使用、销毁全生命周期的数据安全治理体系。《网络安全法》明确了我国实施网络安全等级保护制度，且金融领域在实施等级保护的基础上实行重点保护;《金融行业网络安全等级保护测评指南》对此进行了细化，并给出了相关指导意见。此外，《个人金融信息保护技术规范》在《个人信息保护法》的基础上为个人的金融数据保护打上了补丁，作为行业标准，其在部分口径上与《个人信息保护法》有少许差异(见表1)。



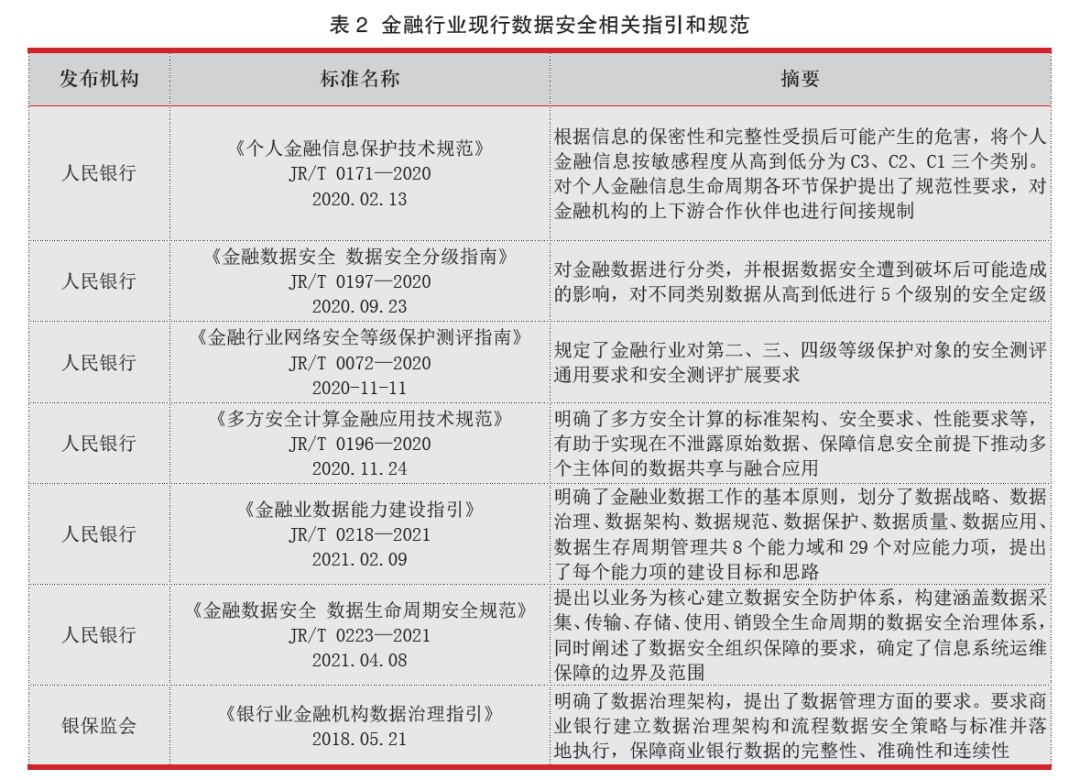
*图1 我国数据安全建设体系*



对于金融机构来说，法律条款中明确提及的数据分级分类保护、数据治理、风险评估、监测预警、应急处置等体系要求，必须遵守并强制执行。而目前的行业规范，后续也可能作为强制执行的标准。金融机构需跟踪相关法律动向和权威解读，重新审视、梳理本机构相关的管理制度和技术方法，在规范的指导下制定符合自身特色的内部管理制度。

**2.行业规范和标准实施现状**

近年来，人民银行及相关机构颁布的一系列金融行业数据安全规范支撑起了金融数据安全的体系框架，为金融数据能力和安全建设提供了依据和指引(见表2)。



《金融数据安全数据安全分级指南》给出了金融数据安全分级的目标、原则和范围，明确了数据安全定级的要素、规则和定级过程。《金融业数据能力建设指引》为金融机构内部进行金融数据能力建设提供了全面指导。在目前已经实施的规范中，《金融数据安全数据生命周期安全规范》定义了数据全生命周期的安全框架，以数据安全原则为指导，将数据分类分级的基本精神贯彻于数据生命周期各个环节。底层通过贯穿数据生命周期的组织保障和运维保障来实现安全防护，为金融业机构开展内部数据安全保护工作提供了实施上的指导。

为保护自然人的隐私和权益，《个人金融信息保护技术规范》从安全技术和安全管理两个方面，对个人金融信息全生命周期的保护提出了规范性要求。《多方安全计算金融应用技术规范》保障多个数据方在数据相互保密的前提下进行高效数据融合计算，为数据开放共享、交易流通和数据要素化奠定技术基础。另外，银保监会发布的《银行业金融机构数据治理指引》旨在要求银行业金融机构加强数据治理，提高数据管理和数据质量质效，进一步通过组织架构来保障金融机构的数据安全。

可以看出，鉴于金融行业在国民经济中的枢纽地位，在整个顶层的建设指导体系中，一方面，要求企业从组织、制度、技术等各方面保障金融安全，明确安全和保护是重中之重；另一方面，大力促进数据使用环节新技术的应用推广，为盘活数据要素市场发挥示范先行效应。

**二、金融行业数据安全技术现状**

金融行业作为一个数据密集型、高安全标准和强监管的行业，在传统的以机密性、完整性、可用性为核心的数据安全领域已经建立了比较完善的技术体系。以工商银行的数据安全技术能力框架为例(如图2所示)，在底层的基础安全方面，全生命周期的身份认证、访问控制、数据授权、密钥管理等环节已经过长时间验证，拥有成熟的技术解决方案。



*图2 工商银行数据安全技术能力框架*

在数据生命周期安全方面，每个环节均有各自侧重的关键技术。在数据采集环节，不论涉及的是个人主体还是企业组织，数据源的可信度都至关重要，需通过数字签名等技术对数据源进行鉴别和认证。在数据传输环节，可信物理信道、数据安全传输和通信协议约定等构成底层基础支撑技术。在数据存储环节，应用加密和备份恢复是保障大数据安全的重要能力。在数据处理阶段，由于不同岗位人员对不同等级安全域的数据进行访问和导出，目前已经普遍应用数据控权和数据脱敏等技术保障数据安全。在数据交换环节，多方安全计算和联邦学习技术在数据不出域的情况下发挥数据融合联动效能，实现数据可用不可见。在数据出域共享或交易的情形下，可通过数据水印溯源来保障数据质量和维护数据要素利益方。在数据生命周期的末端，通过数据清理和存储介质的销毁来形成闭环。

在以上环节中，数据采集、传输、存储和销毁阶段的技术相对成熟和稳定。在数据处理和交换领域，近年来数据使用需求和水平的快速提升，推动了一系列新兴技术的发展。除了多方安全计算、联邦学习、数据水印等，传统技术如数据脱敏、基于角色的数据授权方式等也在效率、适用性等方面面临着升级压力，催生出敏感信息自动识别、动态鉴权等新技术。

**三、金融行业面临的数据安全挑战**

目前，金融行业在数据安全方面面临以下挑战。

首先，强监管下的数据安全治理迫在眉睫。《数据安全法》和《个人信息保护法》的实施，以及金融业相关规范、指南的不断深化和落实完善，表明法律规范和监管层面对金融行业数据安全保护及合规审查的要求日趋严格。为保障数据在机构内外部安全合规流通，体系化的数据安全治理迫在眉睫。

其次，新技术及新业态暗藏风险。人工智能赋能金融行业，在营销、风控、产品创新等业务领域都有上佳的表现，但同时人工智能模型也存在强数据依赖、黑箱、鲁棒性不足等问题，受到数据投毒、模型逆向攻击等攻击方式的威胁。云计算在有效提升计算资源使用效率的同时，打破了传统的物理隔离，但也显著提高了管理的难度，加剧了安全风险；智能终端在数据采集、处理、存储和传输环节均有可能遭到恶意攻击；联邦学习、多方安全计算为金融机构的数据要素流通打下良好基础，但是外部数据来源复杂，其确权、安全责任划分、访问等机制尚需探索，也存在信息安全的隐患。

**四、金融行业数据安全技术展望**

为了应对上述金融行业面临的数据安全挑战，金融行业在数据安全技术方面应注意以下几点。

**1.数据保护建设应以用户为中心**

《个人信息保护法》将“告知同意”作为信息处理的原则，对用户授权、回撤等操作提出了更高要求。以用户为中心的数据保护是指数据的所有者能够充分了解和控制其数据的被使用状况，可借鉴头部互联网产品和服务中已经逐步普及的隐私仪表盘或隐私门户等功能。通过隐私仪表盘，用户能够就其本人信息被采集和使用的情况设置和更改个人偏好。目前，该类功能主要提供相对粗粒度的静态个人信息类别和偏好的选项，未来可能会朝着更细粒度以及动态化数据展示和控制功能的方向发展。

**2.持续升级隐私和数据保护技术**

当数据在内外部之间流转时，如何兼顾数据保护和数据使用，发挥数据生产要素的作用，是新时代数据保护工作的重要课题。数据可使用差分隐私、同态加密、多方安全计算、联邦学习等技术实现隐私增强。在用户的设备端或者浏览器层面，可增加基于隐私增强技术的隐私引擎(Privacy Engine)等应用，用于边缘端集中管理和控制用户的个人信息采集和使用。

**3.建设全生命周期的安全保障平台**

在《金融数据安全数据生命周期安全规范》的安全框架基础上建设安全保障平台，提供统一的服务能力，保障数据流转和使用的安全合规。在机构内部建设统一的数据安全平台，整合零散的安全管控服务，以松耦合方式嵌入全部业务流程中，实现数据在内部链路的集中安全保护和审计追溯。

**4.智能化、自动化数据安全保护运营**

企业在数据保护治理方面的加强和深化，会相应带来运营和管理成本的上升。人工智能技术和流程自动化技术在这方面有广阔的应用空间，包括但不限于以下场景：通过AI技术自动识别敏感信息，对信息进行分类分级；通过客服机器人解决用户在个人数据管理方面提出的诉求；自动检测异常事件，如违规传输敏感信息、试图以伪造的身份非法访问或窃取个人信息等；运用自动化合规检查工具对企业的隐私政策、数据采集声明和数据保护制度等进行合规完备性审查。

**5.提升AI模型安全用数能力**

金融机构应着眼于AI模型数据准备、模型训练、模型服务等模型生命周期各阶段，提升数据防投毒相关技术水平。在数据准备阶段强化异常数据监测过滤技术，优化现有数据标注机制；在模型训练阶段，逐步试点推广自动化机器学习技术，减少人工建模参与步骤，降低人为数据投毒风险；在模型服务阶段，引入数据方投毒算法，同时做好投毒指标测评工作。

**6.灵活高效控制数据访问权限**

对数据保护和数据使用要求的同步提高，可推动数据访问控制向多维度和动态化管控方向发展。基于属性的数据访问控制，通过动态计算数据访问请求的一组属性是否满足某种条件来进行授权判断。典型的属性包括用户属性(如用户类别)、环境属性(如当前时间和地点)、操作属性(如数据访问要求、使用目的等)和资源属性(如数据表、字段等)，理论上可以灵活实现权限控制，几乎能满足所有控制类型的需求。授权决策依据元数据、访问政策、法规制度实时完成，减少了传统基于角色的访问控制中依赖管理员为不同系统、存储方式、使用目的维护静态角色的繁复工作内容，从而更灵活高效地满足企业用数需求。

**7.积极建设隐私计算平台**

金融机构可将隐私计算平台作为与外部交互的可信安全计算平台，整合不同技术路线接口，提升服务能力，从数据边界上守护好数据安全端口。由于计算结果的真实性、准确性、可靠性依赖于可信数据和可信节点，因此在数据共享过程中，参与节点建模时应当防范数据污染和数据投毒。此外，探查和防范恶意节点作为隐私计算的参与方也至关重要。