AI时代的安全拷问：银行数据保护逻辑生变

中经记者 郭建杭
北京报道

伴随AI时代对于海量数据的收集、使用，数据安全重要性凸显。

AI技术发展迅速，人工智能将比预想更快的速度渗透到银行的业务决策和经营活动中。此前，多家银行公开宣布将持续推进数字化转型建设，推动工作模式向数据驱动转变。同时，市场和监管也在拷问银行的数据安全防护能力能否同步跟进，银行的数据安全保护将直接影响银行的合规经营水平。

《中国经营报》记者注意到，截至3月26日，央行及分支机构已公示的行政处罚中，明确涉及“数据安全管理”或“网络安全管理”违规的案例已超30起。

神州信息数据资产交付部总经理张琨指出：“AI时代的银行数据安全管理需要在传统数据治理的基础上，针对AI应用的特点进行创新和升级。关键是要建立‘从数据生成那一刻起就标记清楚用途、权限和生命周期’的精细化管理体系，通过技术手段和制度约束的有机结合，既确保数据安全和合规，又支持AI技术的健康发展。”

开年处罚案例超30起

监管的核心导向，在于推动银行将数据安全和网络安全嵌入公司治理和日常经营管理之中。

在“十五五”开局之年，银行业面临的安全环境更趋复杂。从被动合规到主动防御，从单点治理到体系化运营，围绕数据安全的博弈，从监管开年处罚可见一斑。

据前述央行公布的因数据安全、网络安全违规的处罚公告，国有大型银行部分省份分行、股份制银行及城农商行都收到罚单。

从部分处罚来看，瑞丰农商行被罚316.8万元，在2026年第一季度的处罚金额中较高。央行发布的行政处罚信息显示，瑞丰银行因涉及违反金融统计管理规定、账户管理规定、数据安全与网络安全管理规定，以及未按规定开展客户尽职调查和报告大额交易等多项违法违规行为。对于该罚单情况，瑞丰银行方面对记者表示：“该处罚为早期（前两年）的处罚，目前已经整改到位。主要涉及数据应用不规范的问题，针对细节性问题，后续将结合技术升级与行业变化制定相关计划，并对安全防护系统有升级投入。”

此外，贵州两家银行因“违反信用信息采集、提供、查询及相关管理规定”遭到处罚，这两家银行表示暂未有可公布的整改举措。贵州省内某农商行人士告诉记者：“目前农商行在执行数据安全、网络安全等操作准则时，普遍依据省联社方面制定的规范行为进行管理，行社因违规被处罚后，未来的具体整改措施也是由省联社制定。”

梳理罚单中涉及的处罚缘由可知，违反网络安全管理规定、数据安全管理规定出现频率最高，其次是违反信用信息采集、提供、查询及相关管理规定，未采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施违规行为也有涉及。

监管连开罚单的背后，是金融数据安全监管体系的快速成型。自2024年以来，国家金融监督管理总局与中国人民银行形成了“双线监管”格局。

公开信息显示，2024年12月，国家金融监督管理总局发布《银行保险机构数据安全管理办法》，针对银行保险机构引入了“数据安全评估”；2025年5月，中国人民银行发布《中国人民银行业务领域数据安全管理办法》，细化明确中国人民银行业务领域数据安全合规底线要求，明确“谁管业务，谁管业务数据，谁管数据安全”的原则。

数据安全保护逻辑已发生根本性转变。　视觉中国/图

进入2026年，政策发布节奏稳步前进。国家金融监督管理总局办公厅印发《关于开展金融机构数据安全管理能力提升专项行动的通知》，明确提出“发现一批、整改一批、通报一批、处罚一批”的总体要求。此外，国家网信办就《金融信息服务数据分类分级指南》公开征求意见，进一步细化核心数据、重要数据、敏感一般数据的分级规则。

业内人士认为，监管的核心导向，在于推动银行将数据安全和网络安全嵌入公司治理和日常经营管理之中，实现从阶段性、被动式合规，向长期、持续性治理的转变。

“筑墙思维”转向“管流思维”

在政策法规出台的背景下，银行数据安全建设正面临从“合规驱动”向“风险管控”转变的关键时期。

在监管政策的倒逼下，银行业数据安全建设的薄弱环节也愈发清晰。当前，银行在数据安全建设中存在哪些明显的薄弱环节？

张琨认为，第一是数据资产的全面盘点能力不足。很多银行对自身的数据家底并不完全清楚，特别是对分散在各个业务系统、测试环境、个人电脑以及历史遗留系统中的“暗数据”缺乏有效统一管理。不知道数据在哪里，自然就谈不上有效保护。第二是数据流转过程中的可见性和控制能力不足。业内经常说的一个痛点是“数据可见却不可控”，即数据在核心系统里是安全的，但一旦通过各种方式导出到Excel、测试库或者第三方系统，就进入了“监管盲区”。传统的数据防泄露（DLP）系统更多关注文件流转，但对于通过API调用、数据库查询等方式的数据访问行为，监控和控制能力相对薄弱。第三是内部人员的数据安全意识和操作规范性问题。技术手段再先进，如果人员的安全意识跟不上，仍然会产生很大的风险敞口，特别是业务部门为了提高工作效率而绕过安全流程或在数据共享协作中出现违规操作的情况时有发生。

张琨认为，在政策法规出台的背景下，银行数据安全建设正面临从“合规驱动”向“风险管控”转变的关键时期。但在当前监管环境下，银行的数据安全建设在具体的落地实践中仍面临多项挑战。例如，银行建立了数据分类分级体系，但在实际执行中面临“落地难”。又如，银行业务国际化提速，数据出境场景日益增多，跨境数据流动合规要求收紧，银行需要构建数据出境安全评估机制。目前，数据流动依赖API接口、数据库直连等“新型数据通道”，这也带来了新的风险敞口等问题。

实际上，在人工智能（AI）之类新技术的深度应用背景下，金融行业数据安全保护逻辑已发生根本性转变。

云计算管理与智算调度运营公司佳杰云星技术负责人告诉记者：“AI时代对银行数据安全建设最大的影响是安全策略必须伴随数据的每一次调用、每一个路径动态部署。在由‘用户—应用系统—数据库’的传统数据访问路径下，安全策略主要围绕网络边界与单一应用构建。AI时代，以AI智能体为核心的访问路径变得高度动态，用户通过AI智能体调用各类工具与API，跨系统访问企业数据资源，路径自主规划、跨域流转，使传统基于边界和应用的访问控制难以奏效。同时，数据泄露风险从单一场景扩展为多路径并发。此外，为保障智能体任务完成授予宽泛权限，极易引发越权访问等风险。以上因素都在影响AI时代的数据保护策略转变。”

AI时代，银行的数据安全管理如何覆盖数据的全生命周期？张琨认为，银行需要构建以数据为中心的AI治理框架，从多个维度提升数据全生命周期管理能力。在采集阶段，需要建立AI应用的数据采集专项评估机制。对于AI项目的数据需求，要逐字段说明用途和必要性，坚持“目的限定+最小必要”原则。同时，要引入自动化合规检测工具，对入库数据进行隐私合规扫描，并建立数据来源的可追溯机制，确保训练数据的“清洁”与合法。在存储和使用阶段，应该广泛应用隐私增强技术。特别是差分隐私技术的应用，通过向数据添加数学噪声，使得攻击者无法从模型输出中反推具体个体的隐私信息。在共享环节，应该建立基于场景的精细化数据共享管理机制。针对AI应用的特点，明确不同场景下的数据共享范围、共享方式和安全要求。可以采用联邦学习之类的技术，在保护数据隐私的前提下实现数据价值的共享。在销毁环节，需要建立智能化的生命周期自动化运营机制。利用自动化工具对数据进行全链路标记和管理，当数据完成AI训练任务或超过合规保留期限后，系统自动触发安全销毁流程，并生成不可篡改的销毁凭证。

一库碧波，十年守护：兴业银行金融活水润泽黄河岸

在毛乌素沙漠南缘，一场持续半个世纪的生态革命正在改写荒漠的命运。曾经的流动沙海已不见踪影，取而代之的是沙丘披绿、林草丰茂——毛乌素沙漠成为全球首个即将“消失”的沙漠。就在这片绿洲与黄土交界处，王圪堵水库如一条蓝丝带，静静守护着榆林这座能源之城的生命脉搏。

这座承载着民生期盼与生态使命的水利工程，从纸上蓝图到巍然矗立，离不开兴业银行（601166.SH）榆林分行跨越十年、历经三届班子的金融接力与绿色金融创新。分行党委书记、行长张伟刚强调：“支持王圪堵水库项目，是兴业银行践行ESG理念、积极应对气候变化的战略选择。”

通过“收益权质押+集团担保”的创新金融服务，兴业银行注入的金融活水，将一座单一工业供水的水库，浇灌成润泽百万居民、支撑工农业发展、守护绿色家园、治理周边沙漠的“生命之源”。

民生之渴：从“守着黄河缺水喝”到活水润泽

“过去，榆林真是‘守着黄河缺水喝’！”榆林市水务集团王圪堵水库有限责任公司相关领导的感叹，道出了这座资源型城市的切肤之痛。

榆林煤炭、油气资源富集，却常年笼罩在严重缺水的阴影下。工业发展受限、农业灌溉艰难、居民饮水安全隐忧重重，每年数千万吨泥沙涌入黄河，更成为流域生态治理的“痛点”。

面对困局，王圪堵水库被赋予重任。这座总库容3.89亿立方米、防洪标准达千年一遇的“超级水缸”，设计年供水能力1.5亿立方米。然而，蓝图如何落地？投资巨大、回款周期漫长，如同横亘在前的两座大山。“与传统能源项目‘短平快’不同，水库是真正的‘慢生意’，考验的是金融的耐心与担当。”张伟刚坦言。

2016年，榆林分行毅然接棒。面对“收益低、风险高”的质疑，分行团队跑遍数十个政府部门，深入库区调研。项目曾因多重原因一度搁浅，但分行并未放弃，转而向项目下游企业提供1亿元流动资金支持，缓解集团整体压力，为最终合作埋下伏笔。

破局关键，在于一次“灵光一闪”的金融创新。2024年，榆林分行成功推动“收益权质押+集团担保”方案落地——以水库未来稳定的供水、发电等收益权作为质押核心，辅以实力雄厚的榆林水务集团提供最终担保。这一模式，巧妙地平衡了民生项目的长期性与银行资金的安全性。榆林市水务集团相关负责人感慨：“期限契合了我们的经营特点，真正解了流动性之渴。”

13.5亿元绿色贷款资金如及时雨注入，项目按下“加速键”。效率，成为打动客户的关键。“从深入洽谈到最终落地，仅用月余时间，效率与额度都超预期。”榆林市水务集团负责人称赞道。这笔贷款将企业融资成本牢牢控制在国家相关部门目标范围内，年节约利息超千万元，释放出的资金被优先投入库区环境治理与设施升级，形成了金融活水滋养生态的良性循环。

绿色之钥：解锁气候价值与生态屏障

在王圪堵水库的碧波之下，流淌的不仅是生活生产用水，更是应对气候变化的坚实行动。“我们看重的，远不止保障用水。”张伟刚表示，“它锁沙固土、恢复生态、增强区域碳汇能力的巨大气候价值，是兴业银行践行ESG理念的战略支点。”

水库本身就是一座“固态碳库”。工程设计之初即将泥沙淤积纳入考量，年均拦沙高达318万吨，直接减少入黄泥沙，缓解下游河道淤积与洪水风险。库区周边草木丰茂，形成一道绿色屏障，与曾经的流动沙丘形成鲜明对比。

雷龙湾镇沙峁村是王圪堵水库整村移民搬迁安置村，村干部见证了这片故土的改变：“沙退了，地绿了，生活用水变得便捷又清澈，兴业银行以金融力量让我们感受到生态好转的温度。”

面对日益严峻的干旱挑战，水库巨大的调节库容（2.28亿立方米）如同“生态调节器”，在枯水期年均向下游抗旱补水超9000万立方米，滋养农田、湿地与生态保护区。这种强大的气候适应能力，使水库成为区域水安全的“压舱石”，其价值尤显珍贵。

这份对生态价值的深刻认知，也贯穿于兴业银行的融资实践。ESG理念已深度融入融资血脉。分行虽未将ESG评估作为放贷硬性条件，但将其列为重要的贷后管理指标。“若企业发生重大ESG负面事件，将触发风险管控。”张伟刚强调。这一安排无形中引导企业在日常经营中更加重视环境与社会责任。

发展之锚：一库碧水激活区域转型引擎

王圪堵水库的效益，早已超越一泓清水。它正成为撬动榆林这座能源重镇高质量发展的金色支点，生动诠释了“绿水青山就是金山银山”。

据榆林市水务集团相关领导介绍，水库相继被确定为7个县区、200万以上人口的核心饮用水源地，彻底扭转了“守着黄河缺水喝”的历史。年均4000多万方的供水量虽仅为设计能力的27%，却已是名副其实的“生命之源”。随着东线、西线引黄工程未来竣工，富余水资源将汇入王圪堵水库统一调度，这座“中转站”将升级为全市水资源调配的“中枢神经”，释放更大潜能。

此外，作为榆林工业、农业用水的“总源头”，水库年均提供工业用水3200万立方米，为能源化工基地注入“源头活水”，支撑其产值增长30%；年农业灌溉补水4000万立方米，惠及14.6万亩灌区，让“稻花香”重现沃野；1200万千瓦时的清洁电力，点亮万家灯火。

更值得一提的是，水库所带来的生态效益生生不息。水库建成后，区域小气候改善，生物多样性提升，“塞上江南”风光初显。其智慧灌溉系统进一步减少入河泥沙，巩固治黄成果。

未来之翼：绿色金融活水长流

站在王圪堵水库坝顶，碧波万顷，绿意盎然。雷龙湾镇沙峁村村干部满怀感激：“无论是种植业、养殖业还是特色产业方面，兴业银行用金融力量实实在在支持我们，乡亲们生活质量提高了，致富信心更足了！”这份来自库区百姓的认可，是金融赋能民生与生态最温暖的注脚。

对于榆林分行而言，王圪堵项目不仅是一个成功案例，更是一个可复制的绿色金融样板。“此类项目值得在全行推广。”张伟刚表示。榆林市水务集团也伸出橄榄枝：靖边供水项目合作意向已达成，并期待在绿债、ESG挂钩贷款等创新领域实现突破，寻求更大利率优惠与深度合作。

随着榆林被确定为首批碳达峰试点城市，榆林分行绿色金融布局提速升级：落地首笔水权质押贷款10亿元（授信13.5亿元），绿色贷款余额突破20亿元，绿色融资余额近50亿元，转型领域资产规模持续扩大。

“这是一场永不落幕的接力赛。”张伟刚坚定地说，“未来我们将继续深耕榆林沃土，心系老区人民，以更高水平绿色金融服务，聚焦黄河流域生态保护与高质量发展，持续擦亮‘绿色银行’金字招牌，为谱写老区振兴新篇章贡献金融力量。”

黄河奔涌，金融护航。榆林分行以十年坚守与创新，将金融活水精准滴灌至毛乌素沙地边缘，让王圪堵水库这枚“塞上明珠”焕发出保障民生、修复生态、应对气候变化的璀璨光芒。碧水点亮的不仅是万家灯火，更是可持续发展的“绿金”未来，这条以ESG理念为引领的金融治水之路，正为黄河流域乃至全国的资源型城市转型，提供着充满希望的中国方案。 广告