



数据安全“暗战”升级 多举措夯实数字金融“防火墙”

中经记者 张漫游 北京报道

数据,作为数字经济时代的国家基础性战略资源和关键生产要素,在金融领域的战略价值尤

为突出。它不仅直接关系用户的隐私保护与财产权益,更深度关联国家金融稳定与经济安全。

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》,明确要求金融机构应建立全面数据安全治理体系,构建覆盖数据全生命周期的安全保护机制。2025年9月15日至21日,国家网络安全

宣传周如期举办,再次凸显了数据安全在社会治理和金融活动中的核心地位。

当前,数据驱动金融业务创新、服务升级的同时,也逐渐成为

风险集中地带。业内人士对《中国经营报》记者表示,数据战略价值与国家经济安全紧密相连,跨境数据流动风险、大规模泄露事件频发正倒逼系统性防护体系加

速建成。在此背景下,银行业作为数据密集行业,正从管理制度、技术防护与合规实践等多维度构筑安全防线,但仍需应对技术迭代、跨境合规等多重挑战。

数据安全战略价值凸显 防护形势严峻复杂

目前,数据已成为与土地、劳动力、资本、技术并列的第五大生产要素,其战略价值日益凸显,也让我国对数据安全的重视程度持续提升。盘古智库高级研究员江瀚对记者表示,随着数字经济规模占GDP比重持续提升,数据资源的掌控力直接关系到国家经济安全与科技主权;加之全球地缘政治博弈加剧,跨境数据流动中的敏感信息泄露风险上升,部分国家对中国科技企业实施数据审查,更倒逼我国加快构建自主可控的数据治理体系。

从实际风险来看,个人与机构层面的威胁交织叠加,形势复杂严峻。在个人端,中信银行(601998.SH)方面提示,不法分子窃取数据手段不断翻新:以账户认证、领福利等名义非法索权,诱导过度授权;伪装公检法、银行等机构制造恐慌,骗取密码或诱导屏幕共享;虚构高回报投资、刷单返利等交易,诱骗转账或套取支付信息。记者了解到,此类案例也多次在国家网络安全宣传周警示展中提及,成为侵害用户财产权益的高频风险点。

机构端的问题同样突出。中金金融认证中心(CFCA)行业专家高英博向记者分析道,金融机构在征信授权环节存在多重隐患:身份验证仅靠“姓名+身份



证+短信验证码”等弱方式,易被破解冒用;部分机构自建CA证书缺乏公信力,密钥管理不符合国密标准;授权存证缺失、内部合规意识不足也加剧风险。

大成律师事务所上海办公室方面则指出,银行保险机构数据安全概念范畴广泛,既有私密性又有公共性。例如个人金融信息带有私密属性,相较而言,银行保险机构监管过程中收集的

数据又具有公共属性。因此,银行保险数据特有的多重概念属性增大了银行保险数据安全管理的复杂度。

新技术应用更带来全新挑战。江瀚表示,人工智能和大数据技术的深度应用,使得数据聚合分析可推导出敏感信息、匿名化处理难度加大;物联网设备与工业互联网普及,攻击面显著扩展,关键基础设施面临高级别持续性威胁;

随着数据跨境流动需求激增,国际规则缺口导致合规风险上升,企业面临多国监管冲突。

大成律师事务所上海办公室方面表示,从业务的形态、逻辑和内涵审视,当下银行保险业务具有交错关联、复杂深厚的特性,数据流转的管控难度增大。因此,银行保险业务的融合创新客观上可能提升银行保险数据安全风险的危害程度。

从管理到技术 金融机构多路径构建防护体系

面对严峻的数据安全形势,监管层为行业划定了清晰的防护底线。2024年12月27日,国家金融监督管理总局印发的《银行保险机构数据安全管理办法》明确提出:“银行保险机构应当建立与本机构业务发展目标相适应的数据安全治理体系,建立健全数据安全管理制度。银行保险机构利用互联网等信息网络开展数据处理活动,应当在网络安全等级保护制度基础上,履行数据安全保护义务。”在此指引下,金融机构正从管理优化、技术革新等多个维度系统推进数据安全体系建设,形成“制度+技术+合规”的立体防线。

在数据风险管理方面,工商银行(601398.SH)在其2025年中期业绩报中指出,该行持续推进数据安全分类分级贯标,深化数据安全技术管理系统和数据安全运维监测平台建设,常态化开展数据安全评估和风险监控。与此同时,深入梳理收敛风险暴露点,提升个人客户信息安全管控能力;持续开展培训提升全行数据安全保护意识。

技术革新成为防护体系的“硬核支撑”。建设银行(601939.SH)建立了隐私保护计算平台。该平台可在保障数据隐私的前提下实现联合计算,且该平台采用分布式计算,实际运算功能仅在各参与方本地计算子系统完成。同时,平台可利用区块链对关键中间结果及

时进行上链存证,支持离线任务重跑,可完整复现原流程,从而对参与方的作恶行为进行审计。

不仅大型银行,小型金融机构亦对数据安全投入很大。民营银行苏商银行为破解传统数据交换“要么不给、要么全给”的痛点,联合南京大学研发的《动态数据分片与端到端加密的隐私保护方法》,近日获国家知识产权局专利授权。该专利核心是实现数据“可用不可见”,从根源提升敏感数据流转安全性,为金融、医疗等合规高要求行业提供技术支撑。

在行业层面,高英博指出,金融机构在数据安全与隐私保护中,核心问题集中于“流程无标准、技术应用不规范、事后难举证”,既让机构面临法律与运营风险,也威胁用户信息权益。

为此,CFCA积极配合中国人民银行征信管理局,参与制定了《个人征信电子授权安全技术指南》,并通过“安心验、安心证、安心诉”产品针对性破局:以“身份证+两种以上强验证”或数字证书解决“身份核验”问题,防止身份被冒用;由权威第三方留存授权全流程操作细节与结果,形成不可篡改存证,解决“证据留存”问题;提供标准化报告,助力机构在纠纷中快速证明合规性,高效解决“事后举证”问题。

信息安全加码:司法保护筑牢数字经济“安全线”

中经记者 郑瑜 北京报道

当罗某在英语学习网站注册时被强制填写“职业”“英语水平”等非必要信息,当黄某欢开通公交“先享后付”功能却意外发现名下多了个信用账户,这些发生在普通人生活中的小事,实则是数字经济时代个人数据权益保护困境的微观缩影。

个人信息是数字经济时代的重要生产要素,既承载着人民群众的切身利益,也关系到数字经济健康发展与社会公共利益。在《中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见》(以下简称“数据二十条”)明确加强个人信息保护的背景下,最高人民法院(以下简称“最高法”)近期首次发布数据权益司法保护专题指导性案例,以多个典型案例为切口,回应数据权属认定、数据产品利用、个人信息保护、网络平台账号交付等社会高度关注的问题,为这场关乎每个人数字权利的博弈,划出了司法层面的清晰刻度。

司法引领:为数据保护划出“硬边界”

最高法此次发布的六个指导性案例,共同构建起数据权益司法保护的裁判规则体系。其中,《罗某诉某科技有限公司隐私权、个人信息保护纠纷案》(指导性案例265号)直指企业过度收集个人信息的行业痛点。

2021年,罗某在某科技公司线下体验店被收集两个手机号码并创建英语学习网站账号,5天后登录时却遭遇“强制填写”困境——要求填写“职业”“学习目的”“学龄阶段”“英语水平”及中英文名等信息,全程无“跳过”“拒绝”选项,亦无授权同意收集个人信息的提示。最终,北京互联网法院认定涉App经营者(科技公司)侵害个人信息权益,判令其提供信息副本、停止处理并删除相关数据,同时赔礼道歉并赔偿律师费与取证费合计人民币2900元。

该案的核心裁判逻辑在于,最高法明确“用户画像信息并非App提供网络服务的必要个人信息”。

多方协同发力:织密权益保护“安全网”

在数字经济时代,数据作为数字化、网络化、智能化的基础,正在快速融入生产、分配、流通、消费和社会服务管理等各环节,深刻改变着生产方式、生活方式和社会治理方式。作为数字经济时代的重要“燃料”,数据的价值毋庸置疑。

据最高法披露,近年来,全国法院审理的涉数据类案件数量增长明显,2024年一审审结的案件数是2021年的两倍;而且,由于数据

这一认定正与“数据二十条”中“不得采取‘一揽子授权’、强制同意等方式过度收集个人信息”的要求高度契合。上海靖霖(北京)律师事务所合伙人刘笛对《中国经营报》记者表示,当前企业应该摒弃通过“搭便车”方式获利的互联网野蛮发展时代的旧思维,根据法律法规和行业标准的要求,让用户在明知、自愿的情况下,体会到其个人信息的提供是值得的、安全的。

另一案例《黄某欢诉某信用管理有限公司个人信息保护纠纷案》(指导性案例266号),则从正面回答了“何为必要信息”的问题。黄某欢在开通重庆公交乘车码“先享后付”功能时,授权交通乘车码收集姓名、手机号、身份证信息用于实名与评估风险,后认为信用公司存在误导、强迫、非必要开通某信用服务的行为。法院在判决过程中认为,该功能涉及第三方平台先行垫资,收集信息用于信用



9月16日,在江苏南通如皋市丁堰镇三河、三桥社区,民警向老街老人宣讲网络安全和个人信息保护知识。

视觉中国/图

评估是“确保债权的实现”的必需;且平台仅向公交公司提供“准入与否”的结论性信息,符合“最小必要原则”。

北京市中伦(上海)律师事务所合伙人刘新宇表示,这一案例

为我们在判断是否“为履行合同所必需”时提供了三步走的思路:第一步界定服务性质,判断相关服务是否属于基本功能服务;第二步分场景初步筛选,基本功能服务直接进入“必要性判断”,非

基本功能服务需先判断用户是否“自主主动选择”;第三步判定非基本功能服务必要性,未自主选择则不属于“为履行合同所必需”,已自主选择则进一步判断个人信息处理的必要性。

法律权利、自我保护的体现。可以从“为了使用这个App的功能,这个信息(例如阅读通讯录的权限)我是否愿意提供”的角度出发,来决定自己是否要授权信息收集和使用的。若发现企业超范围、超约定收集、使用个人信息,可通过工业和信息化部网站投诉、向律师咨询处理方案或向公安机关报案。

个人数据权益保护是数字经济高质量发展的重要基石,此次最

高法发布专题指导性案例,既是对“数据二十条”要求的具体落实,也为数据治理提供了清晰的司法指引。未来,随着司法规则持续完善、企业合规意识不断增强、公众保护能力逐步提升,各方将形成更强合力,共同构建“安全、规范、有序”的数据治理体系,让数据在保护中充分流通、在流通中创造价值,为数字中国建设注入更坚实的法治力量。