新形势下征信数据安全问题研究

撰文 _ 周　娇　李宇翔

征信数据作为金融体系乃至整个社会信用体系的基石，其安全问题不仅直接关系到信息主体合法权益，还可能影响国家金融和社会经济秩序的稳定。本文通过梳理新形势下征信数据安全风险的主要表现形式和现实案例，介绍美、英两国防范征信数据安全风险的有关做法，思考并提出相关建议。

新形势下征信数据安全风险的主要表现形式

数据泄露风险

数据泄露是征信领域最常见的数据安全风险问题，包括被动泄露和主动泄露两种。前者指征信机构或信息提供者、信息使用者因内控制度不健全、信息系统软硬件安防措施不齐全、人员管理不到位、业务档案保存不妥当等问题，导致外界通过非正当途径获取征信数据。例如，2017 年艾可飞核心业务系统出现严重安全漏洞，超过 1.45 亿美国公民的个人信息遭泄露，引发了全球公众对征信机构数据安全问题的担忧，艾可飞为此支付了 7 亿美元的赔偿金和罚款。而后者，主要为征信从业人员利用其职务特殊性和便利性，非法查询征信信息或直接拷贝系统内存储的征信数据，并批量对外提供或出售。

数据污染风险

AI 作为现今最前沿的信息技术，受到国际征信机构的大力追捧，征信机构纷纷将其运用到信用评分、风险评估、数据画像等业务模型中。但新技术的背后，也潜藏着其特有的数据污染风险：AI 计算的原始数据来源于多

个渠道，每个渠道的数据都存在独特的属性和偏差[①]，且各渠道数据规模和权重不一致。随着数据量的不断积累，数据库整体的某项属性与偏差可能被放大至与事实相悖的情况，导致评价结果出现歧视性内容，对征信数据库造成污染。例如，2022 年，艾可飞在客户数据迁移过程中发生技术编码问题，某些渠道的数据出现较大的偏差和失衡，致使 30 多万特定身份的消费者信用评分被 AI 模型无故扣除 25 分，大量用户的借贷申请被驳回，引发了针对该公司的集体诉讼和经济索赔。

数据篡改风险

即信息提供者或征信机构为达成特定目的，人为改写信息主体身份、信贷交易等信息的情况。例如，因业务纠纷接入机构非法篡改征信数据。近年来征信维权黑灰产唆使信息主体滥用诉权，逼迫接入机构删改征信信息的情况也屡见不鲜。若涉事接入机构为“息事宁人”或掩盖其他违规问题，可能私下妥协而篡改征信数据。

数据窃取风险

出于谋利、炫技等目的，黑客组织或个人会利用软硬件安全漏洞，通过木马植入、钓鱼攻击、爬虫软件等技术手段，非法入侵存储、对接征信数据的相关系统以盗取数据，且黑客攻击事件一旦发生，往往导致海量数据被窃取并滥用。例如，2022 年，巴西黑客组织攻破环联南非分部服务器，窃取了南非 5400 万人的身份信息、信用评分、电话号码等数据，并对环联实施勒索，对环联造成了严重的经济和声誉损失。

数据非法获取、非法利用风险

常见有 3 类表现形式：一是未经信息主体授权或通过非法途径获取、提供、利用征信数据。二是具有合法资质的主体获取、利用了法律法规禁止采集、使用的数据。例如，即使经过个人信息“授权”，征信机构采集其基因、家族遗传病、指纹、血型等信息的行为，依然属于非法获取数据。三是不具备合法资质的主体，获取、利用了征信数据。

美、英强化征信数据安全保护的主要做法

健全法律体系，夯实制度基础

美国通过渐进式完善《公平信用报告法》等征信业法律法规，逐步建立了“权责清晰 + 多元救济”的征信数据安全保护架构，通过严格限定信用信息的采集范围、使用目的和传播条件，从源头防止个人信用隐私受侵犯；明确信息提供者和征信机构在确保信息来源合法、真实准确、及时更新和纠正等方面的法律责任；赋予消

随着数据量的不断积累，数据库整体的某项属性与偏差可能被放大至与事实相悖的情况，导致评价结果出现歧视性内容，对征信数据库造成污染。

① 不同来源渠道的数据存在整体性偏高或偏低问题，例如来源于税务部门的企业财务数据可能数值整体偏低，但来源于银行机构的企业财务数据数值可能整体高于实际。

费者在信用报告被非法手段获取或使用、因错误信息导致权益受损等情况下的知情权、异议权和救济权等。英国则以《消费信用法》《数据保护法》实现征信数据的全流程防护。全面禁止非持证机构从事信用信息服务，细化了防范征信数据安全风险的要求，详细规定禁止采集的个人敏感数据，强制要求征信机构必须采取有效措施防止征信数据被篡改或恶意销毁等。

严格机构监管，压实行业责任

近年来，美国主要由消费者金融保护局加强对信用评分模型中数据运用的监管，防止 AI 算法偏见导致的歧视问题。同时，通过在执法过程中开具额外的“天价”罚单用于成立“受害者救济基金”，促使征信机构和数据使用者将数据安全保护提升至最高优先级。作为补充，美国征信业自律组织在消费者金融保护局的指导下，具体推动征信市场主体开展数据和算法相关安全审计、建立健全应急预案、举办安全演练活动等工作，进一步夯实数据安全保障。英国由信息专员办公室负责征信数据安全及隐私保护的监管，提出了“授权合法、最小化采数、保障数据准确性和更新及时性、强化技防建设、限制访问权限、保护数据跨境传输安全”6 项征信数据安全保护措施。

美、英两国分别由美国全国信用管理协会、邓白氏、英格兰银行、英国信用管理学院等权威机构面向全球提供信用管理经理短期培训、资格认证、征信职业教育等服务。

强化科技赋能，加固安全防线

益博睿研发了个人信息保护系统、数据对接 API 监测等数据安全模块，支持实时人脸识别登录认证，监控、分析用户操作轨迹，智能识别被病毒感染设备、可疑模拟器和异常外网 VPN 链接，及时阻断非法登录，防止征信数据被窃取；艾可飞在发生 AI“数据污染”问题后，积极推动数据安全保护的新技术与新专利研发，推出了纠正 AI 算法歧视的辅助程序、检测虚假身份登录的识别系统、防篡改数据的自动化防护软件等安全产品。

普及职业教育，提高应对能力

美、英两国分别由美国全国信用管理协会、邓白氏、英格兰银行、英国信用管理学院等权威机构面向全球提供信用管理经理短期培训、资格认证、征信职业教育等服务。以帮助征信从业人员全面掌握征信业和数据安全相关法律法规知识并提高守法意识，增强识别各类征信数据安全风险和应对新型威胁的能力；指导征信机构完善内控制度，优化数据处理流程和操作规范，提升征信数据安全管理水平。

强化国内征信数据安全保护的启示

细化补充专项监管制度，阻断新技术运用的伴生风险

针对现行征信制度体系对新技术运用监管适配的空缺之处，建议围绕 AI 算法治理、隐私计算、跨机构和跨

境数据融合安全等新技术、新领域，研究制定征信业数据安全管理相关专项办法，进一步明确、细化监管规则与技术标准，界定新技术在征信领域的应用场景与合规边界。同时，可参考国际经验，对新技术在信用评价模型中的使用做出规范，要求征信机构对 AI 计算模型定期开展数据清洗、算法审计并提交风险报告，防范和纠正因数据偏差与 AI 算法歧视带来的征信数据污染风险。

注重优化监管队伍结构，强健基层征信监管保障

目前，地市级人行征信监管队伍多以经济、金融、法律学历背景为主，在应对数据安全风险、参与需要处理和分析海量业务数据的征信合规监管工作时，存在专业不足等短板弱项。建议优化征信监管队伍结构，着重培养熟练掌握征信业务、计算机与网络通信技能、法律知识的复合型人才，全面增强基层人行对征信领域新科技应用、征信数据安全及合规等方面的监管保障。

指导加强征信技防建设，筑牢征信数据安全源头防线

监管实践中发现，地方法人、中小银行及村镇银行接入机构的征信技防建设滞后问题相对明显，诸如征信前置系统数据缓存时间过长、用户管理限制性功能不多、防病毒软件未强制更新等问题，使得征信数据泄露风险增加。建议重点指导中小接入机构完善征信前置系统功能，着重加强与本机构人事管理系统对接，从技术上杜绝非授权访问和用户管理违规问题；引导和鼓励有条件的接入机构、征信机构探索基于 AI 的用户身份认证、异常行为实时监测、隐私数据保护等新型应用场景，构建智能化的征信数据安全防护体系。

研发升级跨境传输技术，实施数据出境分类监管策略

跨境数据传输由于线路长、环节多，通信节点、跨国光缆、编程接口、终端设备等均可能成为黑客攻击目标，加之云存储和分布式架构技术的运用，征信数据传输至境外后的存储物理位置分散，数据被窃取、篡改、泄露等风险显著提高。因此，建议结合区块链技术研发跨境联网核查模式，核心数据不在境外落地，引入数字水印技术，确保征信数据跨境传输过程的可追溯并支持事后审计。同时，可针对征信数据出境制定更细化的分类标准，可按用途划分为“核心征信数据”“一般征信数据”“敏感征信数据”等，对不同类别征信数据适用差异化的出境监管强度，平衡数据出境安全保护与征信业务的合法跨境交流共享。

逐步健全职业教育体系，加强征信从业人员素质培育

国内尚未建立征信从业人员系统性教育、能力测验和资格认证体系，征信职业教育机构稀少，高校开设的征信专业选修课也较难满足征信在职从业人员的实际需要。对此，建议持续建好、用好“征信中心远程业务推广系统”，以及发挥征信行业协会的作用，进一步丰富征信数据安全保护相关的培训内容和培训形式，提升从业人员专业素养；建议各地基层人行加强与地方高校合作，推动开设面向征信从业人员的脱产培训课程和专业化的征信业务培训，帮助征信从业人员提高合规履职水平和征信数据安全风险应急处置能力。

责任编辑：刘音露