工程与管理科学
Engineering and Management Science
第 8 卷◆第 2 期◆版本 1.0◆2026 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

个人信息保护法背景下 APP 安全治理路径探索

彭盛晟
广西诺远科技有限公司　530022

DOI：10.32629/ems.v8i2.18473

［摘　要］《个人信息保护法》的施行构建了 APP 个人信息保护的法治框架，为数字时代 APP 安全治理提供根本遵循。面对 APP 领域存在的个人信息过度收集、数据流转不规范、安全防护薄弱等突出问题，APP 安全治理需立足法律要求，聚焦全生命周期风险防控。治理路径以权益保护为核心，涵盖企业内生合规体系构建、技术防护能力升级、协同监管机制完善、社会共治生态培育四大维度，通过多元主体协同发力，将法律刚性约束转化为可落地的治理实践。

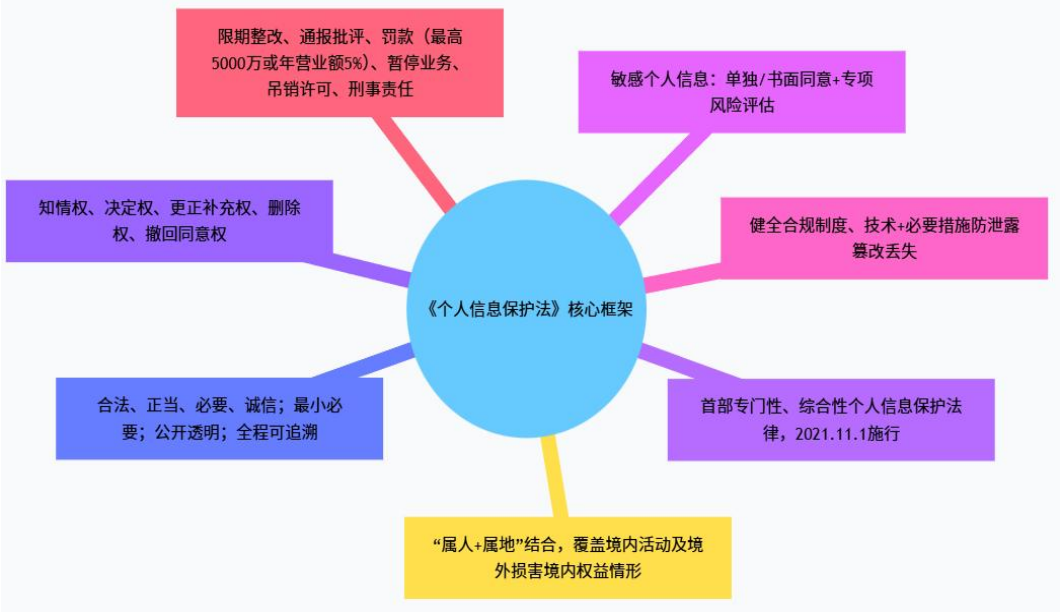
［关键词］个人信息保护法；APP；安全治理路径

引言

数字经济的快速发展使 APP 成为公众生产生活的核心载体，其在便利社会的同时，也带来个人信息泄露、滥用等安全风险，严重威胁用户合法权益。《个人信息保护法》的正式实施，从法律层面明确了个人信息处理的基本原则、权利义务与法律责任，为 APP 安全治理划定红线底线。当前，APP 安全治理仍面临企业合规意识参差不齐、技术防护水平不足、监管协同效能待提升、社会监督机制不健全等挑战，亟需构建系统完备的治理路径。

一、个人信息保护法

《中华人民共和国个人信息保护法》于 2021 年 11 月 1 日正式施行，是我国首部专门规范个人信息保护的基础性、综合性法律，标志着我国个人信息保护进入法治化、系统化新阶段。该法立足数字时代发展需求，以保护个人信息权益、规范个人信息处理活动、促进个人信息合理利用为立法宗旨，构建了兼顾权益保护与产业发展的制度框架。其适用范围覆盖境内个人信息处理活动，同时针对境外处理境内自然人个人信息、对境内自然人合法权益造成损害的情形设置了域外效力，形成“属人+属地”相结合的管辖原则。在核心原则上，明确个人信息处理应当遵循合法、正当、必要、诚信原则，不得超出目的范围处理个人信息，坚持“最小必要”和“公开透明”要求，确保处理活动全程可追溯。法律赋予自然人多项核心权利，包括个人信息知情权、决定权、更正补充权、删除权、撤回同意权等，同时明确个人信息处理者的安全保障义务，要求建立健全个人信息保护合规制度，采取相应技术措施和其他必要措施防范信息泄露、篡改、丢失。针对敏感个人信息，法律设置了更为严格的保护规则，要求取得个人的单独同意或书面同意，并进行专项风险评估。



图一　个人信息保护法核心框架

二、个人信息保护法在APP安全治理中的作用

（一）明确源头治理标准，遏制过度收集乱象

《个人信息保护法》以“合法、正当、必要、诚信”为核心原则，为 APP 个人信息收集划定刚性边界，从源头遏制长期存在的过度收集、强制授权等乱象。法律明确要求 APP 收集个人信息必须限于实现服务目的的最小范围，不得收集与服务无关的信息，同时需以显著方式、清晰易懂的语言告知用户处理规则，采用非默认勾选方式获取用户明确同意。针对生物识别、医疗健康、金融账户等敏感个人信息，法律进一步设置单独同意、专项评估等更严格的保护规则，尤其强化未成年人个人信息的特殊保护，禁止以拒绝提供基本服务为由强制要求用户同意非必要信息处理。这一规定重构了 APP 与用户的权利关系，让个人信息不再是换取服务的“默认成本”，而是用户可自主掌控的合法权益，推动 APP 从“野蛮收集”向“合规采集”转型。

（二）规范全流程处理，筑牢数据安全防线

APP 个人信息处理涉及收集、存储、使用、共享、传输等多个环节，《个人信息保护法》构建了全生命周期安全治理体系，明确 APP 运营者的安全保障义务。法律要求 APP 运营者将个人信息保护融入产品设计、开发及运营全流程，采取加密存储、访问控制、安全审计等技术措施，防范信息泄露、篡改、丢失。对于委托第三方处理、向第三方提供个人信息的常见场景，法律规定必须签订书面协议，明确双方权利义务，APP 运营者需对第三方处理活动进行全程监督，未尽到监督义务的需承担连带责任。针对数据跨境传输，法律设置了安全评估、标准合同等合规条件，确保境外接收方达到同等保护水平。同时，法律要求个人信息保存期限不得超过实现目的所需的最短时间，到期后必须依法删除或匿名化处理，从流程上堵塞数据流转中的安全漏洞。

（三）保障用户权利落地，强化主动维权支撑

《个人信息保护法》赋予用户知情权、决定权、更正补充权、删除权、撤回同意权等一系列核心权利，为 APP 用户主动维权提供坚实法律支撑。法律明确要求 APP 必须提供便捷的权利行使渠道，包括一键撤回同意、账号注销、信息查询与更正功能，不得因用户撤回同意或拒绝提供非必要信息而拒绝提供基本服务。针对 APP 普遍存在的自动化决策、个性化推荐等功能，法律规定必须保证决策公平公正，不得实行不合理差别待遇，同时提供不针对个人特征的替代选项或便捷拒绝方式。当用户发现 APP 存在违法处理行为时，可依法向监管部门投诉举报，或直接提起民事诉讼主张赔偿，构成犯罪的还将依法追究刑事责任。这些规定让用户从信息处理的被动接受者转变为主动监督者，倒逼 APP 运营者重视用户权益，提升隐私保护体验[1]。

（四）健全监管惩戒机制，推动行业合规升级

《个人信息保护法》明确了多部门协同监管机制，为 APP 安全治理提供强有力的执法保障，推动行业从“被动整改”向“主动合规”转型。法律赋予监管部门限期整改、通报批评、罚款、责令暂停相关业务、吊销许可等多种处罚权限，对情节严重的违法行为可处五千万元以下或者上一年度营业额百分之五以下的罚款，形成强大震慑力。监管部门基于法律授权开展常态化整治，对未按规定提供删除或更正功能、违反最小必要原则等常见违法违规行为依法查处，逾期未整改的坚决予以下架，构建起“发现-查处-整改-复核”的闭环监管体系。同时，法律鼓励行业组织制定自律规范，开展合规评估认证，推动 APP 运营者建立健全内部合规制度。这种“法律约束+监管执法+行业自律”的多元治理模式，既划定了 APP 安全运营的红线底线，也为合规企业创新发展营造了公平环境，推动整个行业在法治轨道上实现高质量发展。

三、个人信息保护法背景下APP安全治理路径

（一）筑牢企业内生合规体系，夯实全生命周期治理基础

APP 安全治理的核心起点是运营者的主动合规，需以《个人信息保护法》为根本遵循，构建“组织-制度-流程-培训”四维联动的内生合规体系，贯穿产品全生命周期。在组织架构层面，应建立层次分明的合规管理组织，设立个人信息保护负责人及专职部门，明确决策层、管理层、执行层的权责边界，将合规要求纳入企业战略决策。

制度建设上，需制定数据分类分级、个人信息保护管理规范等专项制度，细化一般信息与敏感信息的处理标准，尤其对生物识别、医疗健康等敏感信息明确“特定目的+单独同意”的刚性规则。流程优化方面，将“最小必要”原则嵌入产品设计，采用非默认勾选授权模式，建立敏感信息采集二次审批机制，同时完善用户权利保障流程，提供便捷的信息查询、更正、删除及账号注销通道，确保撤回同意后数据及时删除或匿名化处理。针对第三方 SDK 合作场景，搭建前置合规审查流程，签订数据保护协议，在隐私政策中如实披露第三方处理情况，并定期开展隐私合规审计[2]。此外，需建立常态化合规培训机制，覆盖产品、技术、运营等全岗位，通过案例教学、考核奖惩等方式强化全员合规意识，将合规要求内化为日常工作准则。

（二）强化技术赋能治理效能，构建全流程安全防护屏障

技术创新是落实《个人信息保护法》要求的关键支撑，需通过“防护-监测-溯源-优化”的技术闭环，将合规要求转

化为可落地的安全防护能力。在数据采集环节，部署权限调用监测工具，实时拦截非必要权限申请，对敏感信息采用动态脱敏技术，在展示时隐藏关键字段，同时通过二次验证机制确保“单独同意”的真实性。

数据存储与传输阶段，采用 SM2、SM3 国密算法对敏感信息加密存储，传输过程全程启用 HTTPS 协议，结合可信执行环境（TEE）构建安全存储区域，防范未授权访问。针对数据流转风险，部署数据防泄漏（DLP）系统，监控文件操作、网络传输等行为，对敏感数据外发自动拦截或加密，同时嵌入数据水印技术，为每条数据添加唯一标识，实现泄露溯源。算法合规方面，搭建算法监测平台，杜绝“大数据杀熟”等不合理差别待遇，强制提供便捷的个性化推荐关闭选项，并公示算法基本原理与运行机制。建立动态风险防控体系，通过 AI 技术开展常态化安全扫描，记录全流程操作日志，对异常数据访问行为实时预警，同时引入隐私计算、联邦学习等新技术，在不泄露原始信息的前提下实现数据价值挖掘，平衡安全保护与产业创新需求[3]。

（三）构建协同监管执法体系，强化合规约束与震慑力度

有效的监管执法是《个人信息保护法》落地见效的重要保障，需建立“数字化监管+精准执法+分级管控+司法衔接”的协同体系。在监管模式上，搭建政企一体化数字化监管平台，运用非现场监管手段实现远程监测、无感监管，实时掌握 APP 权限调用、数据流转等情况，通过动态预警减少重复检查，提升监管穿透力。执法机制方面，健全网信、工信、公安、市场监管等部门的线索互移、标准统一机制，推行“双随机、一公开”与信用监管衔接，对超范围收集、强制授权等违法行为，依法采取限期整改、罚款、下架等处罚，对情节严重的适用高额罚款，形成强大震慑。

分级管控上，建立“一企一档”数据特征库，依据用户规模、数据敏感度、风险等级赋码管理，对高风险 APP 加大检查频次，对低风险 APP 实行“无事不扰”，实现监管资源精准投放。针对用户数量巨大的“守门人”平台，严格落实单独监督机构、规则公开、社会责任报告等特殊义务，强化对平台内服务商的合规管控。司法衔接层面，畅通执法与司法的线索移送通道，支持检察机关、消费者组织提起个人信息保护公益诉讼，通过典型案例发布、违法主体曝光等方式，强化法律实施的社会影响力，构建“违法成本高于收益”的制度环境[4]。

（四）完善社会共治生态格局，凝聚多元主体治理合力

《个人信息保护法》的全面实施需要多元主体协同参与，构建“企业自律+行业监督+公众参与+跨境协作”的社会共治生态。行业组织应发挥桥梁作用，制定 APP 个人信息保护自律规范与合规评估标准，开展合规认证与培训，推广最佳实践案例，建立行业黑名单制度，对严重违规企业实施联合惩戒。

公众参与方面，通过公益宣传、短视频、线上讲座等多元化形式提升用户数字素养，明确投诉举报路径，搭建统一便捷的投诉小程序与“隐患随手拍”平台，建立“上报-核查-整改-奖励”的闭环机制，让用户成为合规监督的重要力量。第三方机构应强化专业支撑，开展独立合规审计与安全检测，为 APP 运营者提供合规咨询服务，为监管部门提供技术支持，推动合规评估结果公开公示，形成社会监督压力。跨境治理层面，针对数据跨境传输场景，加强与相关国家和地区的监管协作，推动保护标准互认，建立跨境数据安全风险预警机制，防范境外非法处理境内用户信息的风险。同时，鼓励企业公开个人信息保护白皮书，主动接受社会监督，推动行业从“被动合规”向“主动合规”转型，实现个人信息权益保护与数字经济健康发展的良性互动[5]。

结语

综上所述，APP 安全治理是《个人信息保护法》落地实施的重要场景，其核心在于构建“合规为基、技术为翼、监管为要、共治为本”的多元协同体系。通过强化企业主体责任、升级技术防护能力、健全协同监管机制、凝聚社会共治合力，能够有效防范化解 APP 个人信息处理全流程风险，保障用户合法权益。这一治理路径既彰显了法律对个人信息权益的刚性保护，又为 APP 行业合规创新预留了空间，实现了权益保护与产业发展的动态平衡。未来，随着治理实践的不断深化，需持续优化治理机制、创新治理手段，推动 APP 行业从被动合规向主动合规转型，为数字经济高质量发展筑牢安全屏障。

[参考文献]

[1]田宇申.互联网保险中个人信息保护的法律规制——以个人信息保护政策为切入[J].兰州学刊，2021（9）：19-19.

[2]陈涛，曾一洋，黄俊逸.大数据背景下公民个人信息的保护的困境与出路[J].中文科技期刊数据库（全文版）社会科学，2022（1）：4-4.

[3]张力，黄鑫.大数据背景下个人信息保护的公私法衔接[J].重庆邮电大学学报：社会科学版，2021，33（1）：9-9.

[4]王倩.网络平台过度收集个人信息法律规制研究[D].大连海事大学，2024.

[5]马博.手机 APP 收集个人信息的行政法规制[D].内蒙古财经大学，2024.