数字时代个人信息法律保护路径研究

吴小雨

南京航空航天大学人文与社会科学学院，中国 ·江苏 南京 211106

摘要：数字经济深度渗透社会生产生活全场景，海量个人信息依托算法、云计算、大数据技术实现常态化收集、流转与商业化利用，个人信息泄露、过度采集、算法歧视等风险持续高发。我国已形成个人信息保护法律体系，以知情同意为核心权利框架、民行刑多部门法协同、风险分层差异化规制为三大核心保护逻辑。但司法与行政执法实践中，知情同意形式化、部门法保护标准割裂、统一规制模式适配性不足等现实难题依然突出。本文以现行法律规范为基础，剖析知情同意制度内在缺陷，阐释民行刑一体化规范整合的制度价值，论证风险导向差异化治理的监管转型趋势，从制度修正、法秩序协调、分层监管三个维度构建适配数字场景的完整保护路径，为完善我国个人信息法治体系提供理论参考。

关键词：个人信息保护；知情同意；民行刑一体化

Research on Legal Protection Pathways for Personal Information in the Digital Era

Wu Xiaoyu

School of Humanities and Social Sciences, Nanjing Tech University, China Jiangsu Nanjing 211106

Abstract: The digital economy deeply penetrates into all aspects of social production and life, and massive amounts of personal information are collected, circulated, and commercially utilized through algorithms, cloud computing, and big data technologies. Risks such as personal information leakage, excessive collection, and algorithmic discrimination continue to be high. China has established a legal system for the protection of personal information, with informed consent as the core right framework, multi departmental legal coordination in civil execution, and differentiated regulation of risk stratification as the three core protection logics. However, in the practice of judicial and administrative law enforcement, practical problems such as the formalization of informed consent, the fragmentation of departmental legal protection standards, and the insufficient adaptability of unified regulatory models are still prominent. This article is based on current legal norms, analyzing the inherent defects of the informed consent system, explaining the institutional value of integrating civil and criminal execution norms, and demonstrating the regulatory transformation trend of risk oriented differentiated governance. It constructs a complete protection path suitable for digital scenarios from three dimensions: institutional revision, legal order coordination, and hierarchical supervision, providing theoretical reference for improving China's personal information legal system.

Keywords: Personal information protection; Informed consent; Integration of civil execution and execution

0 引言

数字时代，线上消费、政务服务、移动应用、智能设备无时无刻不在采集自然人身份、生物、行踪、消费偏好等各类信息，信息跨平台共享、第三方流转、商业化画像成为行业常态。非法倒卖公民信息、APP 强制授权、敏感信息无边界扩散、算法滥用侵害权益等纠纷逐年增长，个人信息自决权的实现面临技术与商业模式双重阻碍。自 2021 年《个人信息保护法》正式实施，我国搭建起专门法统领、民事、行政、刑事法律配套的立体保护框架，完成从传统隐私权保护到独立个人信息权益保护的立法转型。但数字技术迭代速度远超立法更新节奏，既有法律规则在落地中显现结构性矛盾。本文整合基础权利制度、跨部门法协调机制、新型风险规制模式，系统阐释数字时代个人信息多层次法律保护路径，平衡人格权保护与数据要素市场化发展双重价值目标。

1 知情同意框架及其现实修正困境

1.1 知情同意作为信息处理首要合法性基础

《个人信息保护法》第 13 条划定七类个人信息处理合法依据，“取得个人同意”居于首位，是普通场景下信息处理的核心正当性来源，剩余六项为无需同意的法定例外，

覆盖订立履行合同、履行法定职责义务、应对公共卫生突发事件、实施新闻舆论监督、维护公共利益等场景，形成“同意为原则、法定例外为补充”的基础规范结构[1]。

立法在同意机制内部设置分层梯度规则，实现风险与保护强度匹配。对于普通一般个人信息，经营者可采用概括、一揽子同意模式；针对人脸、指纹、健康病历等敏感个人信息，以及将信息提供给第三方共享、跨境传输等高风险行为，法律强制要求单独同意，禁止捆绑授权、默认勾选、概括授权涵盖敏感信息处理事项。同时《个人信息保护法》第 15 条明确赋予自然人随时撤回同意的完整权利，强制处理者提供与授权同等便捷的撤回渠道，从制度层面构建动态控制权，将抽象的个人信息自决权转化为可操作、可持续行使的实体权利，形成“事前告知、事中单独授权、事后随时撤回”全流程权利保障机制。

为平衡个人权益保护与信息正常流通，《民法典》第 1036 条设置合理使用免责边界，构成知情同意制度的内在修正规则。两类行为可豁免侵权责任：一是在本人或监护人授权范围内实施的信息处理行为；二是合理处理自然人自行公开、或其他已合法公开的信息。该条款划定个人信息权利行使边界，避免权利人无限度主张权利阻碍社会信息正常流转，在人格权益保护与数据流通价值之间搭建缓冲地带，弥补单一同意规则过于偏向信息主体、忽视数字产业发展需求的立法短板。

1.2 数字经济场景下知情同意制度的结构性失灵

我国知情同意制度虽在立法层面规则完善，但在互联网商业实践中陷入显著的形式化困境，一方面平台普遍将个人信息授权与基础服务使用强制捆绑，加之隐私政策晦涩冗长，使得用户的知情同意流于表面、缺乏实质自由；另一方面撤回同意权存在明显技术壁垒，平台通过繁琐操作、隐性持续采集、跨平台信息留存等方式形成“撤回孤岛”，严重削弱用户对个人信息的动态控制权，同时已公开个人信息的合理使用标准模糊、司法裁判尺度不一，导致传统单一知情同意框架难以适配复杂的数字应用场景。

2 民行刑一体化的规范协调机制

2.1 立法碎片化引发的保护衔接断层

我国个人信息相关立法呈现“刑事先行、民事行政滞后”的发展格局：刑法较早设立侵犯公民个人信息罪，形成严厉事后惩戒规则；《民法典》人格权编确立民事基础权利，但侵权举证、损害赔偿规则较为笼统；《个人信息保护法》搭建行政监管完整体系，但民事、刑事规范与之衔接条款不足。三类法律规范保护目标、归责标准、责任形式存在差异，出现明显立法碎片化问题，保护链条产生衔接断层[2]。

实践中，大量违规过度采集、强制授权、未履行告知义务行为，尚未达到刑事立案标准，行政监管事前预警、事中整改职能发挥不足；即便行政机关作出处罚，被侵权自然人单独提起民事诉讼仍面临举证难、损失量化难、维权成本高的困境，民事补偿救济功能弱化。三类保护机制各自独立运行，未形成“行政事前合规预防、民事事后损害填补、刑事严重行为终极惩戒”的阶梯式保护体系，整体治理效能受限。

2.2 民行刑一体化整合的功能分工与逻辑价值

行政立法侧重事前预防，网信、公安、市监等部门借助合规核查、专项整治、风险评估等监管举措前置治理关口，通过行政约束规范企业数据处理行为，从源头防范大规模信息侵权风险。民事立法健全私权救济途径，细化过错推定、公益诉讼、惩罚性赔偿相关规则，减轻个人举证压力，为信息泄露、滥用引发的财产与精神损害提供完整赔付方案，填补公权力监管难以覆盖个体轻微权益受损的空白。刑事立法恪守谦抑原则，作为兜底保障机制，仅对批量倒卖海量个人信息、泄露敏感生物信息、引发重大人身财产损失等恶性行为予以刑法规制，防止刑罚过度干预合法的数据研发与商业活动，形成梯度化惩戒体系[3]。

2.3 现行立法一体化协调的规范落地体现

2025 年修订完成的《网络安全法》完成民行刑规范衔接的立法实践探索，修订后第 42 条新增专门条款，明确网络运营者处理个人信息，必须同时遵守《网络安全法》《民法典》《个人信息保护法》及配套行政法规，从高位阶法律层面消除不同部门法适用冲突、模糊地带，为行政执法、司法裁判提供统一法律适用指引[4]。在执法司法实操层面，一体化机制逐步落地：行政机关开展专项行动查处违规 APP 后，将涉嫌犯罪线索移送公安机关；检察机关针对大规模信息泄露案件同步提起行政公益诉讼与刑事公诉；法院审理民事侵权案件时，可援引行政监管处罚决定书作为过错认定证据，三类程序证据互通、结果互认，逐步打通公法监管与私法救济壁垒，证明民行刑一体化是适配数字时代个人信息保护的核心整合路径。

3 基于风险等级的分层规制转型

3.1 统一规制模式的适配性缺陷

《个人信息保护法》出台初期采用一刀切统一合规标准，所有信息处理经营者适用完全相同的告知同意、安全评估、合规审计、个人信息保护负责人制度。该模式对字

节、阿里、腾讯等处理上亿条信息的大型互联网平台具备约束效力，但对个体工商户、小型线下门店、微型小程序经营者形成沉重合规负担。小微企业仅处理数万条用户基础信息，无专业法务、技术团队，难以落实全套复杂合规流程，严苛统一标准客观上抑制中小市场主体数字化经营，不利于数字经济均衡发展。在此背景下，监管思路完成从“统一强监管”向风险导向差异化分层治理的转型，核心逻辑为：依据信息处理规模、信息敏感程度、泄露后危害后果划分风险等级，匹配对应强度的合规义务与监管措施，实现高风险严监管、低风险简合规，平衡权益保护与市场经营成本。

3.2 分层治理两大制度支撑：分类分级与小微企业简化合规

第一，《数据安全法》第 21 条确立数据分类分级保护上位法基础，为个人信息差异化保护提供顶层依据。按照信息泄露后对自然人人身、财产权益损害程度，将个人信息划分为一般个人信息与敏感个人信息两类，敏感信息设置更强告知、单独同意、加密存储、出境评估等特殊义务；后续监管文件进一步细化生物识别、医疗健康、未成年人信息为最高风险层级，配套专项合规要求，构建阶梯式保护规则[5]。

第二，2026 年 4 月国家网信办发布《小型个人信息处理者个人信息保护简化措施规定（征求意见稿）》，同年 9 月正式落地实施，是差异化治理最直接的监管实践创新。文件明确小型处理者界定标准为处理不满 10 万人个人信息的经营者，允许其适用多项简化合规措施：简化隐私告知文本、以线下经营场所公示、客户端公告替代逐一个人单独同意；豁免年度强制性合规审计，通过官方个人信息保护认证即可免于自查；发生信息安全事件时可采用简易公告方式通知用户；设置轻微违法容错机制，初次轻微违法及时整改可不予行政处罚，大幅降低小微企业合规门槛中央网络安 ...。

该文件标志我国个人信息监管思路发生根本性转变：不再单纯追求合规规则统一，而是承认不同经营主体风险、合规能力客观差异，通过分层分类规则设计实现精准监管，兼顾大型平台强约束与中小微企业轻负担，形成覆盖全市场主体的立体化规制体系。

4 数字时代个人信息法律保护路径完善优化方案

4.1 修正知情同意核心制度，消解形式化困境

一是细化单独同意禁止捆绑规则，立法层面明确区分基础功能与增值服务信息采集，严禁以拒绝非必要信息授权为由阻断基础服务使用；推行分层告知模式，隐私政策分为极简核心摘要与完整细则，降低用户知情成本。二是完善撤回同意配套保障，强制平台设置与授权入口同等便捷的一键撤回功能，建立跨第三方数据同步清退机制，阻断撤回后第三方持续使用信息渠道。三是细化《民法典》已公开信息合理使用标准，划定商业营销、算法画像等行为的边界，明确超出合理范围抓取公开信息的侵权认定标准，填补规则模糊地带。

4.2 深化民行刑一体化规范协同，打通全链条保护

一是出台统一法律适用司法解释，厘清民事侵权、行政违法、刑事犯罪的界分标准，明确三者证据转化、线索移送流程，解决类案裁判尺度不一问题。二是强化行政监管前端预防职能，常态化开展 APP 合规巡查、企业数据合规指导，提前化解大规模信息泄露风险；完善民事公益诉讼、代表人诉讼制度，降低个体维权成本，强化私法救济实效。三是坚守刑法谦抑边界，仅对情节特别严重信息侵权行为入刑，同时完善行刑衔接移送标准，避免出现“以罚代刑”或“重刑轻管”失衡状态。

4.3 持续完善风险差异化分层治理体系

一是细化个人信息风险分级目录，针对未成年人、生物识别、医疗行踪等高敏感信息出台专项强制合规规范；二是扩大小型处理者简化合规适用场景，完善线上小程序、社区商户、线下服务业简易合规操作指引；三是建立动态风险评估机制，监管部门定期根据企业信息处理规模、安全事件记录调整其合规等级，实现“风险变动、规制强度同步调整”的动态精准监管。

4.4 构建企业合规、行政监管、司法保障多元共治格局

以法律规范为底线，同步配套行业自律、技术防护辅助路径：督促大型平台设立专职个人信息保护负责人，搭建数据加密、访问权限管控技术防护体系；行业协会出台细分领域合规自律规范；网信、市场监管部门常态化开展普法辅导，提升小微企业合规能力；司法机关发布典型案例统一裁判标准，形成法律规制为主、行业技术治理为辅的多元保护格局。

5 结语

知情同意制度奠定信息主体自决权基础，但需通过规则细化破解商业场景下形式化难题；民行刑一体化整合破解立法碎片化缺陷，搭建事前、事中、事后完整保护链条；基于风险的差异化分层治理突破一刀切监管局限，兼

顾人格权益保护与数字产业创新发展。面对技术持续迭代带来的新型信息安全风险，个人信息法治体系仍需动态优化。未来立法、监管、司法应当持续围绕三条核心路径协同发力，在保障自然人个人信息人格权益不受侵害的前提下，合理释放数据要素流通价值，构建兼顾安全与发展、平衡个体权利与公共利益的现代化个人信息法律保护体系。

参考文献：

[1] 高悦. 大数据时代我国个人信息法律保护研究[M]. 中国政法大学出版社，2025.

[2] 路晨光，孙小夕. 数字时代个人信息权的法律保护边界研究[J]. 法制博览，2025(32):43-45.

[3] 韩旭，唐孝辉. 数字时代个人信息的民法保护路径探析[J]. 法制博览，2025(31):51-53.

[4] 张嘉，杨明明，汪涛等. 数字时代个人信息保护面临的现实困境与破解路径[J]. 安徽警官职业学院学报，2025,24(3):24-28+46.

[5] 陈清. 大数据时代个人信息法律保护路径研究[J]. 社科纵横，2024,39(2):91-96.

作者简介：吴小雨（1993.02-），女，汉族，江苏省宿迁市人，本科学历，工程师（职称），研究方向：法学。