

数字时代下个人信息保护的宪法基础

李凯

内蒙古工业大学, 内蒙古 呼和浩特 010080

DOI:10.61369/SE.2025120021

摘 要 : 数字技术深刻重塑社会结构, 个人信息作为关键要素, 其法律属性具有独特的时代意义。本文主张个人信息保护权应被确立为独立的宪法基本权利。其核心价值植根于人格尊严的维护、个体自由的保障以及实质平等的追求, 其本质在于个人自治的实现, 并由此要求国家承担积极的制度创设与保障义务。当前, 我国虽初步形成以宪法精神为指引、以《个人信息保护法》为核心的规范框架, 但仍存在宪法规范供给不足、部门法间协调不畅、司法救济效能有限等难题。未来应着力于通过宪法解释将个人信息权明确纳入第33条或第38条的涵摄范围; 细化配套法规, 构建覆盖数据全生命周期的规则体系; 强化网信监管机构的独立性与专业能力; 探索技术赋能的创新监管模式。

关 键 词 : 数字时代; 宪法; 个人信息保护权

The Constitutional Basis for Personal Information Protection in The Digital Age

Li Kai

Inner Mongolia University of Technology, Hohhot, Inner Mongolia 010080

Abstract : Digital technology profoundly reshapes the social structure. Personal information, as a key element, has unique contemporary significance in terms of its legal attributes. This article holds that the right to protect personal information should be established as an independent constitutional fundamental right. Its core values are rooted in the maintenance of personal dignity, the guarantee of individual freedom and the pursuit of substantive equality. Its essence lies in the realization of individual autonomy, and thereby requires the state to undertake the obligation of active institutional creation and guarantee. At present, although China has initially formed a regulatory framework guided by the spirit of the Constitution and centered on the Personal Information Protection Law, there are still problems such as insufficient supply of constitutional norms, poor coordination among departmental laws, and limited judicial relief effectiveness. In the future, efforts should be made to explicitly incorporate the right to personal information into the scope of Article 33 or Article 38 through constitutional interpretation. Refine supporting regulations and build a rule system covering the entire data life cycle; Strengthen the independence and professional capabilities of cyber information regulatory agencies; Explore innovative regulatory models empowered by technology.

Keywords : digital age; constitution; the right to personal information protection

引言

在数据驱动发展的时代洪流中, 个人信息经济价值与社会价值日益凸显, 已成为数字经济不可或缺的生产要素。然而, 其大规模收集、处理与流转也伴随着日益严峻的泄露、滥用与侵权风险。以“侵犯隐私权”、“侵犯人格权利”、“一审”为关键词在聚法数据库检索, 相关案件数量呈现增长态势: 2023年28件, 2024年47件, 2025年截至7月2日已有6件。这一现象直观反映了个人信息权益受侵害问题的普遍性与紧迫性。

面对传统隐私权框架在数字环境中的适用局限, 学界逐渐形成共识: 个人信息保护权应作为一项独立权利获得法律承认^[1]。个人信息是公民个体在信息空间的映射, 兼具人格利益与财产价值的双重面向。对其内涵的界定、保护路径的选择以及边界的厘清, 均非单一或数个部门法所能妥善解决。这必然要求回归作为根本法和最高法的宪法, 寻求其价值统摄与规范支撑。同时, 个人信息的强交互性与公共性特征, 使得个体在对抗强大的数据处理者时往往力不从心。现实中普遍存在大量轻微、分散但频发的个人信息侵害行为, 虽未造成即时显著损失, 却持续侵蚀着个体的信息自主空间^[2]。因此, 将个人信息受保护权提升至宪法基本权利的高度, 是强化其保护力度与效能的必然要求。

一、个人信息保护的宪法正当性根基

（一）个人信息的内涵界定及其宪法价值指向

关于个人信息的定义，学界存在“识别说”、“关联说”与“场景理论”等不同学说。尽管视角各异，其核心共识在于强调信息与特定自然人之间的可识别关联性，即“可识别性”构成个人信息的本质特征。数字技术的发展在带来便利的同时，也潜藏着消解个体主体性的风险。

我国现行宪法文本虽未直接规定“个人信息保护”，但其蕴含的基本价值理念为个人信息保护提供了深厚的宪法土壤。《宪法》第33条确立的“国家尊重和保障人权”原则以及第38条对“人格尊严”的宣示，构成个人信息保护最根本的宪法渊源。个人信息的核心宪法价值可归纳为：其一，人格尊严，保障自然人在信息处理活动中的主体地位不被客体化；其二，个人自由，维护其自主决策空间；其三，平等保护确保个体在数字环境中获得公平对待。

（二）个人信息保护权作为宪法基本权利的证立

判断个人信息保护权能否上升为宪法基本权利，关键在于其是否满足宪法权利的内在标准。

凯·莫勒在《全球模式的宪法权利》中的研究表明，当代宪法权利实践的核心范式已转向对“个人自治”的保障。这不仅要求防御国家权力的不当干预，更强调国家需积极创造和维护个体实现自主生活的社会条件与制度环境^[9]。而区分宪法权利与法律权利的关键在于权利实现的依赖路径。个人自治的实现既仰赖国家构建有利的客观制度环境，也要求国家行为非经宪法正当化事由不得侵害公民的自治领域。据此，一项权利具备宪法基本权利地位需满足双重条件：第一，该权利承载着“个人自治”这一核心价值；第二，该价值的实现内在要求国家承担特定的保障与尊重义务。

将此标准适用于个人信息保护权。首先，其蕴含深刻的个人自治价值。在数字时代，个人信息具有公私交融的双重属性。其公共属性体现为，国家基于公共管理、社会服务等目的收集利用个人信息，如司法执行信息公开影响个人信用与社会评价。其私人属性则表现为，基于个体身份特征形成的信息深刻影响着个人的社会生活与经济机会。其次，个人信息保护权自治价值的实现强烈依赖国家义务的履行。在平等主体间的信息处理活动中，民法规则固然重要。然而，当信息处理涉及公民与国家的关系时，仅凭私法规则无法有效约束公权力、平衡力量悬殊。从权利义务平衡的角度看，唯有将个人信息保护提升至宪法位阶，明确国家对公民信息自决权的尊重、保护与实现义务，才能有效应对公私领域交织的复杂风险。

综上，个人信息保护权完全符合宪法基本权利的标准：一方面，其紧密关联自然人的社会存在与发展，是实现个人自治的关键要素；另一方面，数字技术极大扩展了信息收集与处理的深度广度，使得国家积极介入以保障个体信息自主变得尤为迫切和必要。

二、数字技术对传统宪法保障模式的颠覆性挑战

（一）权力格局的重构与公私领域界限的模糊

数字技术的广泛应用深刻改变了国家与社会、公域与私域之间的力量对比。一方面，国家借助网络监控、生物识别、大数据分析等技术手段，将其触角深入以往难以企及的私人生活领域。虽然此类技术应用在提升公共安全方面成效显著，但其侵入性亦不容忽视。另一方面，大型科技公司依托其掌控的海量用户数据与先进算法，在商业和社会领域形成了强大的“私权力”。这些平台利用其市场优势和技术壁垒，可能实施诸如“大数据杀熟”、“算法操控”等行为，对用户权益构成系统性、隐蔽性的侵害。

（二）传统宪法保障机制的功能性失灵

数字环境导致多项传统的个人信息保护机制效能衰减甚至失灵：

第一，“知情—同意”框架的实践坍塌。信息的高度不对称性、冗长晦涩的隐私政策文本、以及“默认勾选”、“捆绑同意”等设计，使得用户“同意”往往流于形式。信息主体难以在充分理解后果的前提下做出真实、自由的意思表示，导致“同意”作为个人信息处理合法性基础的正当性受到严重质疑。

第二，匿名化技术防护效能的削弱与“合理隐私期待”的消解。大数据强大的关联分析能力使得“匿名化”处理后的信息面临极高的“再识别”风险。零散、看似无害的非敏感信息经过聚合分析，足以精准刻画个人画像。同时，公共空间监控的普及与社交媒体的分享文化，极大地压缩了传统意义上的“隐私空间”，导致个人在公共场所的“合理隐私期待”变得日益模糊和脆弱。

第三，新型系统性风险的激增。大规模个人信息的汇聚与分析催生了“用户画像”和“信息茧房”效应。精准推送在提升服务效率的同时，也可能被用于针对特定群体进行诱导性行为操纵甚至政治宣传，对个体的思想自由和独立判断构成潜在威胁。更深远的影响在于，算法决策若存在偏见或歧视，可能固化甚至加剧社会不平等，侵蚀民主协商的平等基础，对民主进程产生系统性风险。

三、现行个人信息保护宪法规范体系的审视

宪法作为国家根本法，是个人信息保护法律体系的最高渊源与价值基础。虽然我国宪法未直接明文规定“个人信息权”，但其多项条款蕴含了保护个人信息的精神内核。第33条人权保障原则、第38条人格尊严、第39条住宅不受侵犯、第40条通信自由和通信秘密共同构成了个人信息保护的宪法依据。特别是第33条国家尊重和保障人权和第38条公民的人格尊严不受侵犯的规定，为国家设定了保护公民个人信息权益的概括性义务，是下位法具体化个人信息保护的根基。

部门法层面，《民法典》第1034条首次在民事基本法中宣示“自然人的个人信息受法律保护”，并采用“概括+列举”方式定

义了个人信息，同时规定私密信息优先适用隐私权规则，体现了对个人信息中核心隐私利益的特殊保护。《刑法》第253条之一设立了“侵犯公民个人信息罪”，该罪属于法定犯，以“违反国家有关规定”为前提要件，其核心指向即为《个人信息保护法》的相关规定。

《个人信息保护法》（以下简称《个保法》）作为我国个人信息保护的专门性、综合性立法，具有里程碑意义。其开宗明义“根据宪法，制定本法”，明确了宪法依据。该法系统规定了个人信息处理规则、个人信息主体的各项权利、处理者的义务与责任，并对个人信息进行了最新、最全面的定义，是落实宪法个人信息保护精神的关键载体，具有显著的“宪法实施法”属性。其核心原则——如第5条的“合法、正当、必要、诚信原则”与“最小必要原则”直接体现了宪法比例原则的精髓；第6条的“目的限制原则”是对处理者权力/权利滥用的有效制约；第9条的“权责一致原则”强化了处理者的责任担当。

综上所述，我国已初步构建起“宪法为基、《个保法》为干、部门法为补充”的个人信息保护法律体系框架。然而，宪法规范的原则性如何有效转化为具体的国家行动义务，以及如何确保该体系内部协调一致并高效运行，仍是亟待解决的难题。

四、宪法实施视角下的主要困境

首先，从宏观视角来看，宪法约束公权力与监管效能的不足。第一，公权力约束机制缺位。对于国家机关大规模收集、处理个人信息的行为，缺乏清晰的立法授权边界、严格的必要性审查程序以及有效的常态化监督机制。宪法比例原则在公共监控、政务数据共享等领域的适用标准模糊，导致权力行使的恣意性风险。第二，监管机构独立性与能力挑战。作为主要监管者的国家网信部门，其独立性、权威性、专业技术能力以及跨部门协调能力均面临严峻考验。面对海量数据处理主体和日新月异的技术模式，如何确保监管行为的合法性、合理性和科学性，缺乏成熟的制度方案。

其次，从具体的法律法规来看，部门法衔接与协调的冲突。《个保法》与《民法典》的层级冲突。《民法典》将隐私权置于人格权编核心位置，个人信息保护规则在某种程度上被视为隐私权保护的延伸或补充。虽然《个保法》对个人信息保护进行了更详尽规定，但二者在保护理念、规则侧重上存在差异。实践中，当个人信息侵权案件同时涉及隐私权和个人信息保护规则时，如何确定法律适用位阶、处理规则交叉问题，尚存争议。《个保法》与《刑法》的衔接不畅。在侵犯公民个人信息罪的认定中，如何准确界定“个人信息”范围、区分“合法处理”与“非法获取、提供、出售”的行为模式、确立刑事违法性的具体审查标准以及协调行政责任与刑事责任的界限，均需《个保法》与《刑法》理论

及实践层面进行更深入的衔接与细化^[4]。

最后，从救济途径来看，司法救济途径的效能困境。第一，个体诉讼维权难。个人信息侵权通常具有受害者众多、单个体损害轻微、侵权行为隐蔽且技术性强等特点。这导致个体受害者面临举证困难、维权成本高、获赔金额低的现实困境，诉讼积极性严重受挫。第二，公益诉讼的功能局限。《个保法》引入的公益诉讼是重要制度创新，但其在运行中暴露问题：线索来源过度依赖刑事案件的移送，意味着公益诉讼往往在损害后果已较严重时才介入，侧重事后惩戒，预防功能发挥不足。在损害认定上，因个人信息侵害的“无形性”和“累积性”，“侵害众多个人权益”的标准在司法实践中存在理解分歧^[1]。在责任承担方式上，尤其是赔偿金的计算、归属、管理以及能否与行政处罚/刑事罚金并处等问题，缺乏统一、明确的规则，导致适用混乱^[6]。

五、完善数字时代个人信息保护的宪法路径

第一，强化宪法解释与规范具体化。推动全国人大常委会通过宪法解释或发布具有指导意义的典型案例，明确阐释《宪法》第33条“人权”或第38条“人格尊严”条款包含对个人信息权的保障，赋予其明确的宪法基本权利地位，为国家设定清晰的保障义务。

第二，构建精细化、全流程的规则体系。在《个保法》基础上，亟需制定配套行政法规、部门规章及国家标准，重点针对自动化决策、数据跨境流动、敏感信息处理、死者个人信息保护等关键环节，设计从信息收集、存储、使用、共享到删除的全生命周期管理规则。同时，必须确保下位法严格遵循宪法原则和精神。

第三，重塑监管架构与提升监管能力。强化国家网信部门作为核心监管机构的独立性、权威性和技术能力，赋予其必要的强制性调查权、有效处罚权及专业的技术支撑。鉴于数据治理的复杂性与跨领域性，应建立网信部门牵头，市场监管、公安、金融、卫健等相关职能部门深度参与的常态化跨部门协同监管机制，形成监管合力，覆盖不同场景。

第四，推动技术赋能与创新监管模式。探索利用技术手段提升监管效能，在收集阶段，在操作系统、应用软件交互界面强制嵌入用户友好型隐私设置工具，保障用户实时知情与便捷控制。在存储与传输阶段，建立数据库安全防护强制标准与审计制度，推广使用加密、访问控制等安全技术。在使用与加工阶段，建立隐私增强技术的合规认证体系，严格要求处理者实施有效的去标识化、匿名化措施。在提供、公开与删除阶段，保障信息主体的访问权、更正权；明确赋予并保障用户对个人信息公开范围与时限的控制权；确立并有效落实“被遗忘权”，确保用户能要求彻底删除其不再需要或被非法处理的个人信息。

六、结语

本文立足于数字时代背景，系统论证了个人信息保护的宪法正当性基础，揭示了数字技术对传统宪法保障机制构成的根本性挑战，并深入剖析了我国现行规范体系在宪法实施层面面临的主要困境。当务之急是通过权威宪法解释明确个人信息权的宪法基本权利属性；修订完善《个保法》及相关配套规范，构建覆盖数

据全生命周期的精细化规则；实质性增强监管机构（特别是网信部门）的独立性、权威性与技术能力，强化跨部门协同；积极探索并应用技术手段赋能监管实践。唯有通过多维度、系统性的宪法工程努力，方能筑牢数字时代个人信息保护的坚实根基，实现技术进步与人格尊严保障的平衡发展。

参考文献

- [1] 王正鑫. 个人信息保护还需要隐私权吗? ——比较宪法层面的考量 [J]. 数字法治, 2024, (05): 91-106.
- [2] 丁晓东. 从个体救济到公共治理: 论侵害个人信息的司法应对 [J]. 国家检察官学院学报, 2022, 30(05): 103-120.
- [3] 李艺. 个人信用信息何以应由宪法保护? ——一个权利论证的进路 [J]. 人权, 2023, (02): 78-95. DOI: 10.16696/j.cnki.11-4090/d.2023.02.002.
- [4] 曹险峰, 陈明辉, 苏蓓, 等. 用人单位之受损型用人者责任的归责原则适用; 建筑规划许可中利害关系人的认定; 保险人代位求偿权的行使范围研究 ——聚焦保险人对第三者的利息主张应否支持; 侵犯公民个人信息罪与《个人信息保护法》的关系与衔接; 刑事案件准予撤回上诉后的再审抗诉对象认定 [J]. 中国应用法学, 2025, (03): 195-212.
- [5] 潘鑫鑫. 大数据时代下个人信息保护公益诉讼制度研究 ——基于330份裁判文书的分析 [J]. 湖北工业职业技术学院学报, 2025, 38(02): 72-77.
- [6] 何沁霖. 个人信息保护民事公益诉讼损害赔偿适用问题研究 [J]. 中国价格监管与反垄断, 2025, (04): 66-69.