Open Journal of Legal Science 法学, 2026, 14(7), 69-75
Published Online July 2026 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2026.147196

Hans汉斯

数智时代隐私权保护的挑战与应对

梁词霞

广西师范大学法学院，广西 桂林

收稿日期：2026年5月25日；录用日期：2026年6月8日；发布日期：2026年7月9日

摘　要

数智时代隐私权正在从消极的不受侵扰的权利，演变为一种积极的个人信息自我决定与对抗自动化决策的复合型基本权利。传统隐私权具有时代局限，数智时代隐私权权利主体仍为个人，但侵权主体扩展至政府、网络平台等多元主体。客体范围从传统领域延伸到个人数据足迹、虚拟空间隐私以及算法干预下的私人事务等新领域。隐私权范围扩张带来的权力博弈、制度缺位、技术失控等挑战，需要通过完善宪法解释与救济途径、构建隐私增强型技术与合规标准、建立多元协同监管机制等手段，以平衡技术发展与权利保障的关系。

关键词

数智时代，隐私权范围，个人信息，隐私权保护

Challenges and Responses to Privacy Protection in the Digital Intelligence Era

Cixia Liang

School of Law, Guangxi Normal University, Guilin Guangxi

Received: May 25, 2026; accepted: June 8, 2026; published: July 9, 2026

Abstract

In the era of digital intelligence, the right to privacy is evolving from a negative right to be free from intrusion into a positive, composite fundamental right that integrates personal information self-determination with the right to challenge automated decision-making. The traditional right to privacy bears the limitations of its own time. In the digital-intelligence era, while the subject of the right remains the individual, the infringing actors have expanded to diverse entities such as governments and online platforms. The object of the right extends from traditional domains to new spheres, including personal data footprints, privacy in virtual spaces, and private affairs subject to algorithmic intervention. The expansion of the scope of the right to privacy gives rise to challenges

文章引用: 梁词霞. 数智时代隐私权保护的挑战与应对[J]. 法学, 2026, 14(7): 69-75.
DOI: 10.12677/ojls.2026.147196

such as power struggles, institutional gaps, and loss of technological control. These challenges must be addressed by improving constitutional interpretation and remedies, establishing privacy-enhancing technologies and compliance standards, and building a multi-stakeholder, coordinated regulatory mechanism, so as to balance technological development with the protection of rights.

Keywords

Digital Intelligence Era, Scope of Privacy Rights, Personal Information, Privacy Protection

1. 引言

数智时代是数字化与人工智能深度融合的社会发展阶段。隐私权是指自然人维护其私人生活安宁以及对属于自己私人生活范畴的事项依法自由支配并排斥他人非法干涉的权利。传统隐私权以私生活安宁为价值指向，以私密信息、私密空间、私人事务自决的“三元结构”为保护范围[1]。在数智时代，传统隐私权理论面临深刻的解释力危机。私人领域从物理住宅延伸至云端与平台账号，算法决策以隐蔽的方式侵蚀自主决定权，权力作用方式从物理侵入转变为隐蔽的信息性控制与预测。传统消极防御范式的隐私权面临解释力危机。我们必须厘清数智时代隐私权的保护范围，这是健全数智时代隐私权利保障体系的前提。

2. 数智技术冲击传统隐私权

传统隐私权理论能够成立，得益于公私领域的边界相对清晰且稳定。当前大数据技术深度嵌入社会生活、信息网络深刻重塑社会交往方式，上述前提性条件不可避免地遭到撼动。在数智时代，无关紧要的信息经由大数据的聚合分析，也展现出惊人的揭示能力。隐私信息与非隐私信息的边界变得模糊，隐私权对个人信息保护的重点从信息的私密性转向信息的可关联性和推断能力。个人的私生活不再局限于物理性住宅，人们在社交平台、云端储存完成具有私密性质的交流与活动，墙与门不再是保护隐私空间的有效屏障。

此外，在传统社会治理的过程中，政府在面对隐私权纷争时多以中立的政策制定者和矛盾调和者的身份出现，较少直接成为隐私权纷争的主体[2]。公民隐私权纠纷以往更多发生在私主体之间，这导致公民隐私权保护问题在以往更多在私法领域呈现，公法领域很少涉及。进入数智时代，政府基于社会治理需要，成为了公民信息的最大收集者和利用者。政府收集、处理公民信息的过程，存在侵犯公民隐私权的可能性[3]。传统隐私权范式中，政府和私人对隐私权的威胁具有明确的时间、地点、行为和可感知性。但在数智时代，政府、信息业者对信息的收集从单点采集转变为全时采集，信息处理从简单归类转为深度挖掘，权力作用效果也由干扰安宁转变为塑造行为。算法决策系统通过数据对个人行为进行预测和引导，将干预的方式从事后窥视转变为事前塑造，私人事务自决面临更深刻的威胁。以空间防御和消极安宁为核心的独处权理论范式，无法应对数智时代的冲击[4]，数智时代的隐私权理论需要向以信息自决和对抗自动化决策为核心的积极控制权转变[5]。

3. 数智时代隐私权主体范围的扩张

在数智时代，隐私权的权利主体仍然是个人，并没有拓展到法人、人工智能机器人等主体。与隐私

权权利主体的相对稳定不同，隐私权的侵权主体发生了较大程度的扩张，具体扩张到了政府、网络服务平台提供者、公司、医疗机构等。

3.1. 权利主体：从个体到集体的延伸

集体能否成为宪法隐私权主体这一问题，可以分“共同隐私”、“同类隐私”两种情况讨论。共同隐私存在于家庭、同学、同事等特定团体之间。但从根本上讲，共同隐私权仍是一种个人权利，这种群体隐私中的群体并不足以构成一个隐私权独立的主体，其隐私也完全可以借由个人隐私权给予保护。“共同隐私产生以后，对共同隐私上的各个权利人来说，该共同隐私是其每个人的与公共利益无关的私生活秘密与信息，从而分别成为他们各自隐私权的客体”[6]。因此，集体隐私可以作为个人隐私的一种特别情况，无需赋予集体隐私权主体法律资格，完全可以依靠个人的隐私权主体地位救济。同类隐私是指与同一权利相对人产生同类隐私利益的多个人的多个权利集合。这种多个人的多个人权利，其各个权利与个人隐私权别无二差，更没有单独为其设置独立的主体之必要。但基于相对人的统一性和权利的无差性，可以形成一种集体救济的方式进行统一保护。

此外，法人的隐私权和死者的隐私利益也是讨论隐私权权利主体所不能忽视的。尽管宪法和民法典中没有直接规定法人或其他组织的隐私权，但在某些特定情境下，法人或其他组织的商业秘密、内部决策过程等可能受到法律的保护。这些可以被视为一种隐私权益，但它们通常不被称为“隐私权”[7]。死者作为无生命的个体，不能承担义务，因此也不能享有权利。尽管死者没有隐私权，但我们必须承认死者具有隐私利益，且死者的隐私利益值得保护，对事关人的尊严的利益的延伸保护，这符合法律人本主义价值取向。死者的隐私利益在一定程度上也可以视为死者近亲属的名誉利益，因此可以赋予死者近亲属一定的救济权利，以维护死者的隐私利益。

3.2. 侵权主体：公权力与网络平台的双重渗透

公共权力的信息化使得公权力主体在借助大数据技术的支持下，其权力得到了一定程度的强化，这在一定程度上增加了对公民隐私权的威胁。政府或其授权的机构可能通过监控系统、数据挖掘等手段，对公民的隐私权造成威胁[8]。此时，如何确保政府能够获得足够的公民信息以完成高效而科学的社会治理，同时又保证公民隐私权不因政府的信息处理行为而受侵害，就成为理论必须予以回应的重要问题。其次，大数据杀熟、信息茧房等私人领域的隐私权侵犯也普遍存在。网络平台提供者通过数据检测，深入分析消费者的个人偏好和行为模式，这在一定程度上也可能侵犯到网络用户的隐私权，甚至可能在不良言论的信息茧房的影响下危害社会稳定。商业公司通过算法和数据分析，能够预测并影响个人决策，这种能力如果不加以规范和限制，同样会对隐私权构成威胁。随着数据的跨境流动，隐私权的侵权主体也可能跨越国界，涉及到跨国公司和国际组织。这意味着，隐私权的保护需要国际合作和全球性的法律框架来应对[9]。

不同主体的侵权的原因或有差别，但无论何种原因，我们都难以否认侵犯他人隐私权不再是小概率事件，更不是单一主体导致的。侵犯他人隐私权主体的多样化、复杂化正给隐私权保护带来了不小的压力，当传统单一个体转变为个人信息的发布者、传播者、挖掘者，每一个环节都可能会发生侵权行为，每一个环节的参与者都可能会成为侵权人。

4. 数智时代隐私权客体范围扩张

数智时代的数据采集、分析与利用技术，彻底颠覆了传统隐私权赖以存在的信息生态。当零散的、表面的数据碎片可以经由算法聚合成为穿透力极强的数字人格画像时，隐私权“保护什么”的问题亟待重新审视。

4.1. 个人数据：从隐私信息到“数字画像”

传统上，隐私信息主要指直接识别个人身份的信息，这些信息因其直接关联性，被明确认为是个人隐私的一部分，受到法律的保护。在数字技术条件下，大量原本被认为不具有可识别性或私密性的零散信息，经由聚合分析可以产生惊人的揭示能力，人们由此产生对个人信息的隐私期待[10]。隐私的范围从不愿公开的个人信息扩展到了包括推断性信息在内的更广泛内容。从更深层次来看，数智时代隐私信息保护的焦点，正在从个体性的私密信息转向整体性的个人数字画像。通过电脑、网络乃至逐渐开发出来的各种感应器，物理世界的活动直接变成数字世界的信息，只要联网，人的活动痕迹就变成能够永久记录和保存的数据，且在大数据处理下建构个人的数字画像[11]。个人消费偏好、健康状况、政治态度、社交网络、情感倾向等多个维度的行为数据，被平台不断采集、汇聚和交叉分析，最终形成个人数字画像。个人数字画像的形成往往未经个人的充分知情和同意[12]。基于深度学习算法的不可解释性、用户对平台处理数据的预先“同意”，公民在信贷领域、就业领域的知情权、反对权等隐私子权利实际上遭到架空。数智时代隐私权的信息维度，不应再局限于保护不愿为他人知晓的私密信息，而应当延伸至保护个人对其数字人格画像的控制权，即个人有权知悉、质疑并自主决定是否允许他人通过各种数据聚合分析来构建和利用自己的数字人格。

4.2. 空间隐私：从实体空间到虚拟空间

传统隐私权保障实体性私生活安宁，并且倾向于保护物理上的实体空间，如私人住宅不受侵犯。随着网络技术的不断兴起，让个人空间从现实拓展到了网络上的虚拟空间。网络用户在网络中也如在现实空间中一般拥有自己的个人领域，王秀哲教授将其称为个人网络领域。个人网络领域即存放个人信息的网络载体，是个人信息得以在网络上传播的前提，并为个人信息提供网络活动的私人空间。个人信息网络空间载体类似于传统隐私权保护的住宅等空间载体[13]。

个人信息网络空间载体包括三类：第一类是入网工具，即帮助个人加入网络空间的设备。这些电子设备储存了大量的个人信息，人们可以借助这些电子设备完成网络空间的社交和个人信息传播。第二类是网络服务器。个人在网络上的所有数据资料都存放在网络服务器中。尽管网络用户对服务器不享有所有权，服务器中的数据资料存在权属争议，但存放这些数据的空间仍属于个人领域，没有精尖计算机知识的人无法在没有账户信息的情况下处理服务器中的数据，网络服务器的代理商也不可随意侵犯个人信息。第三类是个人自主管理的平台空间，如微信、微博等。人们通过注册账号，在相应平台上进行通信、娱乐，抒发个人情感、记录生活点滴。网络服务平台存储着大量的个人信息，其中或多或少的存在隐私信息，亦或者是网络用户不愿为特定人外的其他用户所知晓的信息，这些信息也值得宪法隐私权保护。

4.3. 私人事务：自主决策与算法干预

私人事务的自决权是个人行为领域的隐私。这种隐私的范围通常包括生活方式、恋爱方式、交往方式、生活习惯、子女教育等，与人的个性发展和自治密切相关的，比较私人化的内容。随着高科技的发展，私人载体性事务越来越广泛。例如，身体载体，传统上仅指可见的身体的隐秘部位不能侵犯，如今已发展到保护个人身体完整性，具体包括个人对于自身呼吸、血液检验、DNA 等体内物质的控制权。引起广泛关注的个人基因隐私涉及的也是个人对于自己身体隐私的控制权问题。

在数智时代，算法通过数据收集与分析，深度介入个人的消费选择、职业规划、社交行为等私人事务，模糊了自主决策与外部干预的边界。一方面，算法推荐系统通过用户的浏览历史、购买记录等信息，完成精准营销，看似便利，实则通过信息茧房效应削弱消费者自主权。另一方面，信息业者有能力获得隐私权利主体不能凭借自己的能力获得的隐私，私自利用这种隐私信息进行利益变现，实际上也侵犯了

用户的隐私权。私人事务的范围已从传统的家庭生活、健康管理等领域拓展至数字化生存的方方面面。如何在技术赋能与权利保护之间寻求平衡，成为隐私权理论亟需回应的问题。

5. 数智时代隐私权保护的挑战

科技是一把双刃剑，数智化的广泛应用在便利了人们日常生活的同时，也在无形之中增强了公民隐私权遭受侵犯风险，并且侵犯公民隐私的途径和方式也逐渐呈现出愈加的复杂多样化趋势。

5.1. 公权监控与私权资本的双重压迫

传统监控受人力与物理空间限制，仅能针对特定对象与场所开展。而数智时代，公共区域摄像头、人脸识别、交通实名数据、基站定位等已构成全域数字感知网，通过无差别、全时段被动采集，使个人在公权力监控下近乎“透明”。数智时代的公权力基于公共利益的需要，通过信息采集的泛在化、数据处理的技术化以及干预逻辑的预防化，形成对公民隐私权的压制[14]。这种监控的无形性与处理过程的不可见性，使得传统的“知情－同意”机制与事后救济途径面临失灵的风险。

私权资本对公民隐私权的威胁也不容小觑。在现代社会中，淘宝、百度、小红书等 APP 软件利用大数据偷偷地收集并整合公民的个人隐私，甚至对其个人隐私进行整合和披露，在此过程中忽视了公民的隐私权、知情权和同意权。此外，苹果 IOS 系统通过封闭生态强制数据本地化处理，将用户锁定在自身服务体系内。这使用户在设备更新换代之时，为了方便个人信息的移转储存，不得不优先考虑特定产品。这种以保护之名行控制之实的行为，割裂了数据主权与个人权利的有机联系。平台既是个人信息的处理者，又是自身行为合规性的审查者，这种自我监督模式存在着先天性的利益冲突。当平台商业利益与用户个人信息权益发生冲突时，内部机构很难保持真正的独立性和中立性。

5.2. 保护规范的滞后与精细度不足

在数智时代，隐私权的保护问题变得尤为复杂，尤其是对于公众人物、劳动者、传染病人员以及违法行政相对人这些特殊群体。保护个人信息的本质目的其实在于保护公民的个人隐私，对个人信息的保护也需要以潜在的隐私利益为基础[15]。公众人物虽然在一定程度上放弃了部分隐私以换取公众关注，但这并不意味着他们的所有私人信息都可以被无限制地曝光。公众人物的隐私权同样受到法律保护，尤其是在与公共利益无关的私人生活领域。媒体和公众应当尊重公众人物的合理隐私需求，避免侵犯其个人生活。在职场中，劳动者的个人信息、健康数据等可能被雇主收集和使用。在传染病防控的工作过程中，有关部门需要在公共卫生安全与个人隐私权之间找到平衡点。执法机关在处理违法案件时，应当在法律框架内保护涉案人员的隐私信息，避免不必要的公开和传播。这些特殊人群的隐私权保护需要法律的明确规定、社会的广泛认识以及技术的有效支持，共同构建一个既保护个人隐私又维护公共利益的平衡体系。

5.3. 算法黑箱与系统性不公

算法歧视的本质在于数据驱动的自动化决策系统因设计缺陷或数据偏见，对特定群体产生系统性不公。亚马逊平台通过分析历史招聘数据发现，部分行业中男性求职者录用率显著高于女性，算法因此自动降低女性求职者的简历推荐优先级。类似地，35 岁以上求职者常被算法标记为低匹配度，导致其简历无法进入企业筛选池。这种数据偏见并非人为，而是亚马逊的算法自己学习的结果。算法歧视引发的隐私权保护问题还存在于信用评分系统。部分互联网金融平台通过分析用户地理位置和消费记录，自动降低三四线城市用户、频繁购买低价商品用户的信用评分，导致他们的贷款额度受限。基于深度学习算法的不可解释性、用户对平台处理数据的预先“同意”，公民在信贷领域、就业领域的知情权、反对权等隐私子权利的实际上遭到架空。在数智时代，算法歧视与数据集中削弱了个体对自身数据的控制权，形

成结构性权力失衡，对隐私权的平等保护造成极大的威胁。

6. 数智时代隐私权保护的路径

6.1. 立法完善与加强宪法保护

定性为私权的隐私权研究已经无法满足当前社会对公民隐私保护的需要。将隐私权上升为宪法性权利，既是对隐私背后精神利益的重视，又是在重塑日益模糊的公共领域与私人领域界限[16]。有关部门应畅通宪法救济渠道。一方面激活合宪性审查机制，各级法院审理隐私权案件时，遇法律合宪性疑问可逐级上报至最高人民法院，由其提请全国人民代表大会常务委员会审查[17]。另一方面探索建立数字权利公益诉讼制度，允许社会组织就平台算法歧视等行为代表不特定多数人提起诉讼，克服个体维权成本高、举证难的困境。除了加强宪法保护外，特定领域的精细化立法同样是应对制度缺位的重要路径。金融领域禁止将社交数据纳入信用评分模型；就业领域建立算法决策的透明度与反歧视规则；公共卫生领域完善传染病人员隐私保护规范，明确公共安全与个人隐私权的平衡标准。

6.2. 构建隐私增强型技术与合规标准

隐私增强型技术是指一系列旨在保护个人隐私的技术手段，包括数据加密、匿名化、去标识化、安全多方计算、同态加密等。这些技术可以有效保护个人数据的安全性和隐私性，防止数据泄露和滥用。隐私保护的合规标准是指对数据处理行为进行规范和指导的标准，包括数据收集、存储、处理和利用的合规标准，数据主体权利的合规标准，数据控制者和处理者责任的合规标准等。在数智时代，传统隐私保护技术难以应对数据聚合与算法推理带来的风险，亟需通过隐私增强型技术与合规标准的系统化建设，实现数据利用与权利保障的平衡。该路径需融合前沿技术成果与法律规范要求，形成以技术落实法律、以标准约束技术的闭环机制。

6.3. 建立多元协同的监管机制

隐私权保护需突破政府单一监管模式，建立多元协同的监管机制，形成政府主导、平台问责、公众参与、国际协同的治理生态。在政府主导层面，可在各级人大下设独立数据监察专员机构，对政务数据滥用行为行使调查权与质询权；同时建立算法审计制度，要求日活超百万的平台定期提交算法审计报告，由网信部门联合高校专家库进行独立审查。在平台问责层面，强制平台设立由外部专家和用户代表组成的算法伦理委员会，对重大算法变更行使否决权；推行隐私托管模式，由第三方非营利机构受托管理用户数据，形成平台内部自治与外部制衡的双重约束。在公众参与层面，除前述数字权利公益诉讼制度外，应将社会听证确立为影响公民隐私权的重大行政决策的前置程序，充分吸纳公众意见，发挥社会监督的规模效应。在国际协同层面，建立隐私保护的国际政策协调、技术标准互认和跨境监管执法合作机制，共同应对数据跨境流动带来的全球化治理挑战。

隐私权范围扩张带来了公权与私权越界风险、特殊群体隐私保护难题以及算法歧视和数据垄断等问题，严重威胁着公民的隐私权。我国需要构建更加完善的隐私权保护体系，以适应数智化时代的新需求，在保障公民个人隐私、维护人格尊严的同时，促进大数据技术的健康发展，推动社会的和谐稳定。

参考文献

[1] 魏振瀛, 主编. 民法[M]. 第八版. 北京: 北京大学出版社, 2021: 611.

[2] 张新宝. 从隐私到个人信息: 利益再衡量的理论与制度安排[J]. 中国法学, 2015(3): 38-59.

[3] 陈锦波. 从私法到公法: 数字时代隐私权保护的模式延展[J]. 政治与法律, 2023(11): 24-38.

[4] 王秀哲. 公共安全视频监控地方立法中的个人信息保护研究[J]. 东北师大学报(哲学社会科学版), 2019(5): 57-68.
[5] 余成峰. 信息隐私权的宪法时刻规范基础与体系重构[J]. 中外法学, 2021, 33(1): 32-56.
[6] 何志文. 共同隐私的法律保护[J]. 前沿, 2004(7): 142-144.
[7] 彭錞. 再论中国法上的隐私权及其与个人信息权益之关系[J]. 中国法律评论, 2023(1): 161-178.
[8] 谢馥. 大数据时代公民隐私权的宪法保护[J]. 法学, 2023, 11(4): 1993-1999.
[9] 李沛儒. 大数据时代隐私权保护研究[J]. 法学, 2024, 12(7): 4400-4406.
[10] 戴昕. “看破不说破”: 一种基础隐私规范[J]. 学术月刊, 2021, 53(4): 104-117.
[11] 王秀哲. “隐”与“私”流变中的信息隐私权[J]. 河北法学, 2022, 40(11): 46-71.
[12] 王秀哲. 大数据时代个人信息法律保护制度之重构[J]. 法学论坛, 2018, 33(6): 115-125.
[13] 王秀哲. 信息社会个人隐私权保护的公法研究[M]. 北京: 中国民主法制出版社, 2017: 35.
[14] 姚建宗, 龚志旺. 数字时代权力技术化及其法律风险应对[J]. 河南大学学报(社会科学版), 2024, 64(5): 17-24+152.
[15] 李忠夏. 数字时代隐私权的宪法建构[J]. 华东政法大学学报, 2021, 24(3): 42-54.
[16] 李延舜. 论宪法隐私权的类型及功能[J]. 烟台大学学报(哲学社会科学版), 2017, 30(6): 29-42.
[17] 李世豪. 大数据时代隐私权的宪法保护进路[J]. 西南交通大学学报(社会科学版), 2021, 22(2): 60-68.