Open Journal of Legal Science 法学, 2026, 14(3), 1-7
Published Online March 2026 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2026.143061

Hans汉斯

大数据时代个人信息安全问题及对策研究

伍超凡

宁波大学马克思主义学院，浙江 宁波

收稿日期：2026年1月26日；录用日期：2026年2月10日；发布日期：2026年3月3日

摘　要

大数据技术的飞速发展在推动社会治理效能提升、促进数字经济繁荣的同时，也对个人信息安全构成严峻挑战。个人信息泄露、滥用、非法交易等问题频发，既侵害公民合法权益，也扰乱社会治理秩序。本文结合大数据时代个人信息处理的法律界定差异与体量庞大、流转快速、采集隐蔽等特征，系统分析当前我国个人信息安全保护面临法律规则细化不足、新型侵权规制滞后、数据全生命周期安全隐患、企业与个人主体责任缺位、监管协同与技术手段滞后等问题，为破解困境，提出相关建议：需从提升公民防护与维权能力、强化技术防护、细化法律规范、优化行政监管等方面构建多元协同保护体系，在保障公民合法权益的同时，促进数据合理利用，助力数字经济与社会治理高质量发展。

关键词

大数据，个人信息安全，个人隐私，监管治理

Research on Personal Information Security Issues and Counter Measures in the Era of Big Data

Chaofan Wu

School of Marxism, Ningbo University, Ningbo Zhejiang

Received: January 26, 2026; accepted: February 10, 2026; published: March 3, 2026

Abstract

The rapid advancement of big data technology, while enhancing the efficacy of social governance and fostering the prosperity of the digital economy, poses severe challenges to personal information security. Frequent incidents involving personal information leakage, misuse, and illegal transactions not only infringe upon the legitimate rights and interests of citizens but also disrupt social

文章引用: 伍超凡. 大数据时代个人信息安全问题及对策研究[J]. 法学, 2026, 14(3): 1-7.
DOI: 10.12677/ojls.2026.143061

order. Considering the legal definitional discrepancies in personal information processing and characteristics such as massive volume, high-speed circulation, and covert collection in the big data era, this paper systematically analyzes the current challenges in personal information security protection in China. These include insufficient refinement of legal regulations, lagging oversight of emerging infringements, security risks throughout the data lifecycle, deficiencies in the accountability of enterprises and individuals, and inadequate regulatory coordination and technical measures. To address these challenges, relevant recommendations are proposed: it is necessary to establish a multi-stakeholder, collaborative protection framework by enhancing citizens' protective and remedial capabilities, strengthening technical safeguards, refining legal norms, and optimizing administrative oversight. This approach aims to safeguard the legitimate rights and interests of individuals while promoting the reasonable utilization of data, thereby contributing to the high-quality development of the digital economy and social governance.

Keywords

Big Data, Personal Information Security, Personal Privacy, Regulatory Governance

1. 引言

大数据时代的技术革新为政务服务、公共管理、经济运行等领域赋能增效，让个人信息成为关键生产要素，极大便利了人们生活，但大数据“杀熟”、个人信息泄露等问题也逐渐暴露。其收集广泛、处理隐蔽、共享跨域的特征，加之“海量信息的收集及信息技术的发展使信息对特定个人的辨识能力日益增强，传统个人信息的边界越发模糊，大幅扩张了个人信息保护法的潜在适用范围，也使得个人信息的有效匿名化日益困难”[1]。尽管《个人信息保护法》《数据安全法》等上位法已出台，但地方制度落地与行政监管仍存适配难题。梳理现有研究发现，学界多聚焦国家层面法律框架构建，对地方制度适配、全生命周期风险防控等实操性问题关注不足，针对新型侵权场景的规制研究亦有待深化。基于此，本文以“问题导向”为核心，明确研究目的为系统剖析个人信息安全保护的现存困境，探寻兼具针对性与可操作性的破解路径。后续将围绕个人信息核心范畴、现存问题、对策建议等章节展开，为提升公众保护意识、破解监管困境、保障公民权益、推动数字经济与社会治理良性发展提供理论与实践支撑。

2. 大数据时代个人信息安全的核心范畴

2.1. 大数据时代个人信息的法律界定

依据《中华人民共和国网络安全法》，个人信息是指以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，包括姓名、身份证件号码、通信联系方式等；《中华人民共和国个人信息保护法》第四条规定，个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。再到《信息安全技术公共及商用服务信息系统个人信息保护指南》中规定个人信息可为信息系统所处理、与特定自然人相关、能够单独或通过与其他信息结合识别该特定自然人的计算机数据。个人信息可以分为个人敏感信息和个人一般信息。从以上可知，随着大数据时代的发展，个人信息还涵盖了计算数据等衍生信息。在我国现行的法律和相关规范中，关于个人信息的概念内容并不一致，这就也会导致处理方式和保护措施的实施中出现偏差的可能性。

2.2. 大数据时代个人信息的核心特征

随着大数据时代的到来以及互联网技术的日益普及，个人信息也呈现出新的特征。一是数据体量庞大、流转速度快。这是随着大数据时代的发展，个人信息所呈现的突出特征。大数据时代的信息呈现爆炸式增长，个人信息中包括个人的体貌，家庭、社会关系等逐渐数据化，互联网的传导性使得相关信息的传播超越了时空的限制，也正是如此，监管和保护的难度进一步提升；二是价值密度高，“个人信息具有社会价值、商业价值、个人利益价值”[2]，大数据的发展使得海量数据的处理效率大量提升，同时也增加了信息泄露的风险，个人信息成为了新的原材料和生产力，与个人信息相关的买卖屡见不鲜；同时，不同信息之间的可识别性与关联性，使得个人信息安全风险的传导性更强，极大提高了监管者的人力和技术投入；三是采集的隐蔽性与“无意识性”。大数据时代的个人信息采集往往具有隐蔽性，用户常处于“无意识授权”的状态。企业通过埋点技术、Cookie 追踪、传感器采集等方式，在用户使用 APP、浏览网页的过程中，自动收集各类行为信息，而用户往往未明确感知或未获得充分告知。这种“被动式采集”区别于传统的“主动提交”模式，也成为个人信息保护的难点之一。

3. 大数据时代个人信息安全存在的问题

大数据时代，个人信息成为关键生产要素，在便利生活与赋能发展的同时，安全风险愈发凸显。当前，我国个人信息保护面临法律法规不完善、数据全生命周期安全隐患、主体防护意识薄弱、监管协同能力不足等多重困境，既侵害公民合法权益，也阻碍数字经济健康发展。

3.1. 相关法律法规不完善

近年来，随着依法治国基本国策的逐步推进，相关法律法规也在逐步完善与发展。《个人信息保护法》虽已确立“最小必要”“告知同意”等核心规制原则，但在规则落地层面仍存在显著漏洞。一方面，敏感个人信息的界定边界模糊，消费习惯、位置轨迹等衍生信息是否纳入敏感范畴缺乏明确标准，导致企业常以“服务优化”为借口，突破“最小必要”原则超范围收集个人信息；另一方面，“默示同意”的适用场景未予以清晰界定，“一揽子授权”“默认勾选”等变相强制授权行为屡禁不止，司法实践中对企业违法收集行为的举证、认定难度较大。与此同时，面对大数据杀熟、算法个性化信息推送、跨境数据流动等新业态衍生的新型个人信息侵权问题，现有法律规范尚未形成针对性规制条款。以跨境数据流动为例，跨境电商平台的用户数据跨境传输，既缺乏清晰的审批流程与分级分类管理规则，也未建立全链条的责任追溯机制，极易出现监管真空。

“长期以来个人信息安全保护以维护基本社会秩序为出发点，重刑事打击和行政处罚，忽视个人信息保护的预防机制和遭受侵害后民事侵权责任的追究，导致即使侵权行为人最终被科处刑罚或行政制裁，但对于受害者而言，其个人财产或非财产的名誉等损失却无法得到相应补偿。”[3]然而，法律责任体系的惩戒力度与维权渠道也存在不足。对企业违法收集、泄露个人信息的处罚金额，与其通过滥用数据获取的商业收益严重不匹配，难以形成有效震慑；受害者的个人维权则面临“举证难、成本高、赔偿低”的现实困境，集体诉讼与公益诉讼的适用范围较窄，难以充分保障受害群体的合法权益。

3.2. 技术应用层面：数据全生命周期存在安全隐患

随着科技的飞速发展，大数据时代个人信息安全的问题也随着“技术化”，数据的全生命周期都存在着未曾可知的安全隐患。在数据收集环节：部分 APP、小程序通过“一揽子授权”“默认勾选”等方式强制用户授权非必要权限(如计算器 APP 要求获取通讯录的查看权限)；还有的通过埋点技术、Cookie 追踪等隐蔽手段，在用户不知情的情况下收集浏览记录、设备信息等，违背“知情同意”原则；同时，

现如今越来越多的中老年人接触到智能手机，他们在似懂非懂的状态下点击了“确认”键，在“不知”的情况下主动授权。在数据存储与流转环节：中小企业普遍缺乏专业的数据加密、脱敏技术，大量个人信息以明文形式存储；数据流转过程中，第三方服务商、合作平台的权限管理混乱，容易因信息倒卖、黑客攻击导致大规模数据泄露。浙江台州 6 名技术人员暗网倒卖个人信息案便是典型，涉案人员利用原公司未注销的管理员账号，编写爬虫脚本非法爬取 9 万余条公民 ETC 敏感信息，暴露出企业在数据存储环节缺乏严格的权限分级与动态管理机制，无加密、脱敏等基础防护措施，权限管理漏洞成为信息泄露的重要诱因[4]。此外，数据交易黑市猖獗，个人信息被打包售卖的产业链难以根除。前述台州案件中，嫌疑人将非法爬取的信息通过暗网以 0.8~3 元/条的价格售卖，暗网的匿名性、跨境性让数据交易难以被察觉和监管，即便本案倒卖获利极低，仍有不法分子铤而走险，反映出数据流转环节的监管空白与产业链根除难度。数据利用环节的乱象丛生：大数据算法在精准画像的同时，容易引发“算法歧视”(如基于消费数据的信贷歧视)、“信息茧房”等问题；部分企业利用用户数据进行定向诱导消费，甚至将个人信息用于非法营销，侵犯用户的自主选择权，而此类算法层面的信息滥用行为，因技术隐蔽性强，更难被及时发现和规制。

3.3. 个人信息安全防护意识薄弱

在主体责任履行层面，企业与个人均存在明显缺位，具体表现为：

一方面，企业合规意识薄弱，数据安全投入不足。多数企业将数据安全视为“成本项”而非保障业务合规的“必要投入”，未建立专门的数据安全管理机构或完善的合规体系，难以形成全流程风险管控；部分企业虽形式上公示了隐私政策，但内容晦涩冗长、权责表述模糊，实质是通过技术性表述规避自身责任，并未真正履行信息披露义务，导致用户无法清晰知晓信息收集、使用的具体范围与风险。

另一方面，个人信息保护意识与维权能力不足。普通用户对个人信息的商业价值和泄露风险认知不足，日常存在“随手授权”APP 权限，不仔细阅读隐私政策、在社交平台随意公开身份证号、手机号等敏感信息的行为，“隐私政策作为强化个人信息保护和实现个人控制的工具似乎只是一厢情愿，隐私政策更可能异化为互联网平台的‘避风港’”[5]；同时，用户普遍缺乏应对数据泄露的维权知识与有效途径，即便发现个人信息被泄露，也因维权流程复杂、成本较高而往往秉持“自认倒霉”，“维权终将无果”的态度，难以有效主张自身权益。台州倒卖案中，9 万余条被泄露的公民信息主体，多数直至案件曝光才知晓自身信息被倒卖，即便发现，也因缺乏证据留存、维权渠道等相关知识，最终选择放弃维权，而中老年群体因对智能手机、网络授权规则不熟悉，更易成为个人信息侵权的受害群体，进一步凸显了个人信息保护意识的普遍缺失与维权能力的不足。

3.4. 行政监管能力不足

面对个人信息大量滥用、网络黑灰产业盛行的现实背景下，政府执法部门应当承担起对个人信息安全保护的切实义务。但就目前来看，我国尚未建立明确的个人信息保护专门机构。在监管协同层面，当前个人信息保护工作面临职责划分不清与监管能力滞后的双重困境，难以适配大数据时代的监管需求。

一方面，跨部门与跨区域协同监管机制不畅。个人信息保护涉及网信、公安、市场监管、工信等多个职能部门，但各部门间的监管职责边界尚未完全厘清，导致实践中既存在多个部门重复监管的乱象，也存在部分领域权责空白的“无人监管”真空；同时，针对大数据跨地域、跨行业自由流动的核心特征，跨区域、跨行业的监管联动机制建设滞后，缺乏统一的协同执法流程与信息共享平台，难以形成监管合力，无法对跨区域流转的个人信息实施全链条有效监管。

另一方面，监管技术手段与监管模式滞后于技术发展。当前监管仍较多依赖传统的人工检查、定期

抽检等方式，而大数据技术下的个人信息采集、流转往往具有隐蔽性、碎片化、规模化的特点，传统监管模式难以精准识别“埋点追踪”“静默采集”等隐性违法行为；此外，监管部门普遍缺乏先进的技术监测工具与智能化分析平台，无法实现对企业数据操作行为的实时监测、动态预警与精准溯源，导致监管始终处于“事后查处”的被动局面，难以提前防范和及时遏制违法行为，监管时效性与有效性大打折扣。

4. 大数据时代个人信息安全保护的对策

多中心治理理论的核心要义是打破单一主体垄断治理的模式，构建“政府－企业－社会－个人”多元参与、权责明晰、协同高效的治理网络。结合大数据时代个人信息安全保护的现实困境，本文基于该理论，从法律制度完善、技术防护升级、公民意识提升、行政监管优化四个维度，构建全链条、多主体的协同保护对策体系。

4.1. 政府主导：完善相关法律法规

在多中心治理框架中，政府承担着制度供给、规则制定与监管保障的核心职责，是治理体系有效运转的“掌舵者”。大数据时代的背景下，个人信息泄露的风险进一步提升，建立起一套完善、操作性较强的个人信息保护体系是当务之急。政府应在整合现有法律的基础上，牵头完善个人信息保护法律体系的空缺。首先，要明确敏感个人信息的界定，《中华人民共和国个人信息保护法》第二十八条对敏感信息的定义为“敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满 14 周岁未成年人的个人信息”。在大数据时代，敏感个人信息正在逐步扩展，相关法律也应不断更新；其二，对新型个人信息侵权问题，现有法律规范尚未形成针对性规制，在新的时代背景下，完善相关法律，对大数据时代产生的新型信息侵权问题做出相应规制；最后，“对个人信息安全立法不仅要考虑到预防信息泄露的问题，而且要考虑到个人信息一旦泄露应该如何处罚，以及由谁来承担举证责任的问题。由于被侵权者收集证据和举证都比较困难，建议个人信息安全立法采取过错推定原则，由大型的互联网企业和高科技公司等涉嫌侵权者承担举证责任”[6]。完善企业违法收集行为的举证方式，优化认定方式，加大法律责任体系的惩戒力度。

4.2. 企业主责：加强大数据环境下个人信息保护技术的研究

企业作为个人信息的直接收集者、处理者与使用者，是多中心治理体系中责任落实的“核心执行者”，需以技术防护与合规管理筑牢安全防线。“大数据时代对个人信息安全的保护，制度保障是基础，强化技术研发，提高物理层面的技术防护手段是关键。”[3]“应将个人隐私信息保护纳入国家战略资源的保护和规划范畴。”[2]众观当今社会的犯罪案例，我们不难发现呈现“方案跟着问题跑”的现象，问题出现时再提出相应的对策，难免有一定的滞后性，相关部门被“牵着鼻子走”。因而，各企业相关技术人员应该加大人力、物力的投入，加强技术研究，未雨绸缪，扩大研究范围，深入研究可能出现的问题，从不同的角度对个人隐私和信息加强保护，从技术层面防护个人信息的安全。

4.3. 个人参与：提升公民个人信息安全意识与权利救济能力

个人是个人信息的权利主体，也是多中心治理体系的“末端参与者”与“直接受益者”，其主动防护与依法维权是治理效能落地的关键。保护个人信息安全，从根源上是要提升公民个人的信息安全意识，从源头降低信息泄露的威胁。“个人信息保护意识薄弱，反个人信息侵害能力低下，以及企业的干扰使得我国公民个人信息控制能力总体较低，制约了法律在维护公民个人信息安全方面发挥重要效用。”[7]因而，加强个人信息保护意识至关重要。日常生活中，个人要养成良好的上网习惯，不点击陌生网址、

链接、二维码等，不轻易在社交网站泄露个人信息，明确网络与现实之间的安全线。除此之外，当个人信息受到侵害时，能够找到除了法律之外的途径解决问题，要“制定完善信息主体申诉的权利和渠道，以保障个人信息权益被不当侵害后及时获得私力救济的同时获得公力救济”[3]。还要优化个人信息的救济方式：例如简化个人信息权利救济程序，鼓励公民通过行政投诉、民事诉讼等途径，维护自身在信息泄露后的合法权益。

4.4. 社会协同：凝聚治理合力

社会力量(包括社区、学校、行业协会、媒体等)是多中心治理的“桥梁纽带”，能够衔接政府、企业与个人，扩大治理覆盖面与影响力。地方政府要联合社区、学校、媒体等开展反诈宣传，通过典型电信诈骗案例讲解，普及个人信息保护法律知识与防范技巧，锚定青少年和中老年群体等目标群体，开展针对性的知识普及，提升公众对个人信息商业价值与泄露风险的认知，提升公民个人信息保护的安全意识；畅通社会监督渠道，鼓励媒体曝光违法收集、滥用个人信息的行为，支持公益组织参与个人信息侵权公益诉讼，形成“社会监督 + 司法保障”的外部约束机制，弥补政府监管的盲区。

4.5. 多元协同：提升个人信息安全行政监管效能

在行政监管方面，首先要明确监管职责分工，政府及有关部门之间应当在合作与效率的双重原则下有序推进个人信息安全的保护，充分运用部门联动机制，定期通报监管情况，协调重大监管事项。与此同时还要确立网信部门为牵头监管部门，厘清网信、公安、市场监管等部门的监管权限，明确权限范围，避免监管重叠与真空。依据大数据时代的特征，各部门要针对性地站好自己的一班岗。其二要强化执法能力建设。执法人员是解决信息安全问题的实际践行者，其能力建设永远在路上。随着大数据时代，信息技术的日新月异，行政执法人员的大数据技术与法律知识培训也要随着更新加强，以备组建专业监管队伍；同时要配备必要的技术监管设备，运用大数据、人工智能等技术手段开展智能化监管，提升风险识别与取证效率，提升公民的满意度和办事信心。其三要完善执法程序与处罚机制：规范个人信息安全行政检查、调查、处罚等程序，保障行政相对人的合法权益，“建立个人信息侵权的民事赔偿制度，在侵权人实施侵权行为后，不仅要追究侵权人的行政责任和刑事责任，还要依据实际情况追究侵权人对受害人的民事赔偿责任”[8]，以便能最大限度弥补受害人的损失。同时，要适当加大对严重侵权行为的处罚力度，实行“处罚与教育相结合”，“同时应从泄露信息类型、行为次数、损害后果等明确规定具体违法情节的判断标准，根据不同犯罪情节科处不同刑罚，以实现罚当其责”[3]督促违法主体整改到位。

5. 结语

大数据时代的个人信息安全保护是关乎公民权益、数字经济发展与国家数据安全的系统性工程。我国已构建个人信息保护基本法律框架，但从立法到落地仍需破解诸多难题。未来，随着新技术新业态兴起，个人信息安全风险将呈现新特征，保护体系需动态优化。需进一步细化法律规范，完善责任与维权机制；强化技术主动防护研发；开展全民信息安全教育，培育社会共治氛围；构建智能化、协同化监管体系，实现从“事后查处”向全流程防控转型。唯有多方合力，才能平衡个人信息安全与数据合理利用，守住权益底线、释放数据价值，为数字中国建设筑牢安全屏障。

参考文献

[1] 范为. 大数据时代个人信息保护的路径重构[J]. 环球法律评论, 2016, 38(5): 92-115.

[2] 宋阳, 张崙, 张志勇, 张志刚. 物联网+大数据环境下个人信息安全防范与保护措施研究[J]. 情报科学, 2020, 38(7): 93-99.

[3] 党振兴. 大数据时代个人信息安全现状与保护[J]. 重庆交通大学学报(社会科学版), 2022, 22(4): 14-22.

[4] 6 名高学历技术人员从“暗网”坠入法网[N]. 浙江法治报(浙江), 2023-02-10(00002).

[5] 贺小石. 大数据背景下公民信息安全保障体系构建——兼论隐私政策的规制原理及其本土化议题[J]. 中国特色社会主义研究, 2021(6): 100-109.

[6] 郭雪慧. 人工智能时代的个人信息安全挑战与应对[J]. 浙江大学学报(人文社会科学版), 2021, 51(5): 157-169.

[7] 鲁佑文, 马亚鑫. 信息源与风险源: 大数据时代个人信息安全困境及应对[J]. 现代传播(中国传媒大学学报), 2019, 41(11): 81-85.

[8] 郑毅. 信息消费时代个人信息安全的法律保护[J]. 郑州大学学报(哲学社会科学版), 2014, 47(4): 54-57.