Open Journal of Legal Science 法学, 2026, 14(2), 106-112
Published Online February 2026 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2026.142051

Hans汉斯

基于大数据视角下的个人信息保护规范研究

杨建清

南京信息工程大学法学与公共管理学院，江苏 南京

收稿日期：2026年1月18日；录用日期：2026年1月29日；发布日期：2026年2月25日

摘　要

在大数据技术深度嵌入社会运行机制的背景下，个人信息的生成、处理与利用方式发生了结构性变化，传统以隐私保护为核心的规范模式面临显著挑战。本文立足大数据条件下个人信息处理活动的技术特征与风险形态，系统梳理我国个人信息保护规范的制度逻辑，分析现行法律在合法性控制、风险防控及制度适配方面存在的不足。在比较考察域外个人信息保护制度经验的基础上，本文进一步提出以风险导向为核心的规范完善路径，强调通过实体规则、执行机制与技术治理的协同配置，实现个人信息保护由事后救济向事前控制的转型。

关键词

大数据，个人信息保护，数据治理，个人信息保护法

A Normative Study on Personal Information Protection from the Perspective of Big Data

Jianqing Yang

School of Law and Piblic Administration, Nanjing University of Information Science and Technology, Nanjing Jiangsu

Received: January 18, 2026; accepted: January 29, 2026; published: February 25, 2026

Abstract

With the deep integration of big data technologies into social and economic activities, the generation, processing, and utilization of personal information have undergone structural changes, posing significant challenges to traditional privacy-centered regulatory models. Focusing on the technological characteristics and risk patterns of personal information processing in the context of big data, this article systematically examines the institutional logic of China's personal information protection regime and identifies its deficiencies in legality control, risk prevention, and regulatory

文章引用: 杨建清. 基于大数据视角下的个人信息保护规范研究[J]. 法学, 2026, 14(2): 106-112.
DOI: 10.12677/ojls.2026.142051

adaptability. Through a comparative analysis of foreign legal frameworks, the article further proposes a risk-oriented approach to regulatory improvement, emphasizing the coordinated configuration of substantive rules, enforcement mechanisms, and technical governance in order to shift personal information protection from ex post remedies to ex ante control.

Keywords

Big Data, Personal Information Protection, Data Governance, Personal Information Protection Law

1. 引言

随着大数据技术的普及，个人信息被收集、存储、分析和利用的规模不断扩大，个人信息泄露事件频发，给个人隐私带来严重威胁。例如，社交媒体上的个人信息泄露可能导致身份盗用、网络诈骗等犯罪活动；医疗数据的泄露可能侵犯患者的隐私权，甚至威胁到其生命安全。此外，大数据技术的广泛应用还使得个人信息泄露的潜在后果更加严重，一旦数据被不法分子获取，可能引发连锁反应，造成难以估量的损失[1]。因此，个人信息保护已成为当前社会亟待解决的紧迫问题。

本文旨在深入剖析大数据视角下个人信息保护的现状与挑战。通过梳理相关法律法规、分析监管机制、调查公众意识等方面，揭示当前个人信息保护存在的问题和不足。同时，结合大数据技术的特点和发展趋势，探讨个人信息保护面临的挑战和机遇，为制定有效的个人信息保护策略提供科学依据。

2. 大数据环境下个人信息保护的现状分析

2.1. 大数据技术对个人信息保护的影响

在大数据环境下，信息技术的发展对个人信息保护格局产生了结构性影响。互联网与大数据分析往往会突破《个人信息保护法》第 6 条规定的“明确、合理的目的，并应当与处理目的直接相关”的“目的限制”原则，以及“收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息”的“数据最小化”原则。同样，互联网与大数据要保证个人信息处理的公开透明、信息质量与准确性原则也非常困难，因为互联网与大数据追求的是整体数据的概率性的质量与准确性，并非某一条个人信息的质量与准确性[2]。随着数据收集、处理与分析能力的显著提升，个人信息在社会运行中的利用效率大幅提高，数据主体的行为特征得以被持续记录、整合与分析。这一技术变革在推动商业模式创新与公共治理精细化的同时，也使个人信息逐渐脱离其原有的具体、分散状态，转化为可被反复利用和深度加工的数据资源。

在大规模数据分析的支持下，个人的兴趣偏好、消费习惯乃至社会关系均可能通过算法推断被精准描绘。此类信息即便并非单独构成高度敏感数据，但在持续聚合与交叉分析后，仍可能形成对个人生活轨迹和行为选择具有高度指向性的“数据画像”。一旦相关数据脱离合法控制，极易被用于实施诈骗、身份冒用等侵害行为，从而对个人的人身财产安全及人格利益造成实质影响。

与此同时，大数据依赖的分布式存储与网络化传输模式，也在客观上扩大了个人信息暴露于风险之中的范围。信息被拆分存储于不同系统节点并在多主体之间频繁流转，使得数据安全防护链条显著拉长，任何一环的防护失效均可能引发系统性泄露风险。相较于集中式数据管理模式，该种技术架构对个人信

息保护提出了更高的安全治理要求。

更为重要的是，大数据技术的持续迭代正在不断突破既有个人信息保护规则的制度预设。以深度学习和算法建模为代表的新型技术手段，使信息处理活动呈现出高度隐蔽化和自动化特征，传统以可识别侵权行为为前提的法律规制模式难以及时发挥效力。在此背景下，个人信息侵害不再局限于事后的非法披露或不当利用，而更多表现为难以察觉的结构性风险，这对现有个人信息保护制度的适应性构成了严峻挑战。

2.2. 个人信息泄露与滥用的典型类型

在大数据应用场景中，个人信息侵害已不再局限于个别数据的偶发泄露，而是呈现出类型化、结构化的发展趋势。在拥有先进计算机技术的大企业面前，个体消费者早已“赤裸”。我们的电子邮件可能被扫描，我们的一切浏览记录与消费记录都会被收集，企业为我们绘制的用户画像细致入微，企业有可能预测我们在当时当下的任何一个需求。伴随着个性化推荐与个性化服务的，是屡试不爽的大数据杀熟和粉碎大众市场的个性化定价[3]。结合现有实践，可以将相关风险大致归纳为以下几类。

其一，基于社交平台的数据聚合型泄露。社交媒体平台在运行过程中持续收集并整合用户的身份信息、行为偏好与社交关系数据，形成高度集中且可关联的个人信息集合。一旦平台的安全管理措施存在缺陷，相关数据即可能被非法获取并用于身份冒用、精准诈骗等活动。由于社交数据本身具有高度关联性，其泄露往往具有连锁扩散效应，侵害后果难以局限于单一信息主体。

其二，电子商务场景中的交易数据滥用风险。电商平台在提供服务过程中掌握大量涉及个人财产安全的交易信息，包括消费记录、收货地址及支付信息等。相关数据一旦脱离合法控制，不仅可能被直接用于非法交易或恶意消费，还可能通过数据转售、交叉比对等方式被进一步加工利用，放大对个人财产利益与信用安全的侵害风险。

其三，医疗健康数据的非正当利用。相较于一般个人信息，医疗数据直接关联个人的生命健康状况与人格尊严，具有更高的敏感性。然而，在数据驱动的医疗研究与商业开发背景下，部分机构在缺乏充分合法依据的情况下，对患者信息进行收集、共享或二次利用，使得医疗数据面临被滥用甚至被非法交易的风险。一旦相关信息被不当披露，其侵害后果往往具有不可逆性。

上述类型化案例表明，大数据环境下个人信息侵害的主要风险并非源于单一违法行为，而是与平台化运营、数据高度集中及多主体共享密切相关。这一现实状况对以个案责任追究为核心的传统个人信息保护模式提出了新的制度挑战。

2.3. 现有个人信息保护措施的制度局限

尽管我国已逐步形成以《个人信息保护法》为核心、由多部法律法规共同构成的个人信息保护规范体系，但在大数据技术深度嵌入数据处理活动的背景下，现有制度在应对新型风险方面仍显不足，其局限性主要体现在规范供给、技术适配与社会认知等层面。

首先，从规范层面看，现行个人信息保护规则在制度完备性与针对性方面仍存在一定缺口。这尤其体现为三个方面：一是综合性立法虽已建立，但统一的、高级别的专门执法机构仍属缺位，监管职责分散、效率不足；二是个人信息，特别是非敏感信息的法律界定仍显模糊，保护范围与实践操作之间存在张力；三是相关规则散见于多部法律法规，缺乏系统整合，导致法律责任不清、救济机制薄弱[4]。在此基础上，现有规则虽对个人信息处理的一般原则和基本义务作出规定，但对于大数据驱动下的数据聚合利用、算法分析以及跨境流动等高风险场景，却缺乏足够精细化的规范回应。在实践中，部分数据处理活动虽形式上符合合法性要求，但其潜在风险并未被现有规则有效识别和约束，导致法律规范难以对复

杂的信息处理行为形成实质性控制。

其次，从技术治理角度看，现有个人信息保护措施在应对大规模数据处理需求时面临适配性不足的问题。传统以加密为核心的安全保护手段，主要着眼于防止数据在存储和传输过程中的非法获取，却难以回应数据在合法处理链条内部被过度利用或不当关联的风险。尽管去标识化、匿名化等新型技术措施在一定程度上缓解了隐私泄露问题，但其在实际应用中往往以牺牲数据可用性为代价，难以在数据利用与人格保护之间实现有效平衡。

再次，从社会层面看，个人信息保护的整体效果亦受到公众认知与企业合规意识不足的制约。一方面，信息主体在复杂的数据处理环境中普遍处于信息与技术劣势地位，难以对个人信息的收集和利用作出理性判断；另一方面，部分数据处理者在合规成本与商业利益之间进行权衡时，倾向于采取最低限度的合规策略，削弱了法律规范的实际约束力。

总体而言，现有个人信息保护措施在大数据环境下面临的并非单一规则缺失问题，而是制度设计与技术现实之间的系统性张力。这一局限性表明，单纯依赖传统的合法性控制与事后责任追究机制，已难以充分回应大数据条件下个人信息保护的现实需求。

3. 个人信息保护的法规框架构建

3.1. 法规框架的理论基础

个人信息保护的法规框架构建，其理论基础主要源于对人格利益的保护。人格利益是公民人格权的客体，是民事主体自然生存和社会生存所必需的利益。在民法上，人格利益分为一般人格利益和具体人格利益，前者如人格独立、人格平等及人格尊严等，后者如生命、健康、名誉、隐私等。在信息时代，个人信息体现了如公民隐私、人格独立、人格尊严等多种人格利益，应为人格权所保护的客体。因此，个人信息保护的法规框架构建应以保护人格利益为理论基础，确保个人信息的安全和隐私不受侵犯。

3.2. 个人信息保护的法律原则

对于广大人民群众来讲，大数据时代的到来极大程度上改变了人们生产生活方式，生产生活更加便捷化、高效化、智能化，但与此同时大数据时代的到来也在一定程度上加剧了个人信息被泄露的可能性。此种情况下需要强化个人信息法律保护，避免个人隐私泄露[5]。个人信息保护的法律原则是构建个人信息保护具体规则的制度基础。这些原则包括安全保护原则、限制收集原则、限制利用原则、目的明确原则[6]。要求处理个人信息应当具有明确、合理的目的并与处理目的直接相关，采取对个人权益影响最小的方式，限于实现处理目的的最小范围，公开处理规则，保证信息质量，采取安全保护措施等。《个人信息保护法》中特别强调了“告知–同意”原则，作为个人信息保护核心规则，保障个人对其个人信息处理的知情权和决定权。该原则最早源于医疗伦理领域，要求医者在实施诊疗前向患者充分说明风险并获取其明确同意，核心在于尊重患者自主决定权。移植至个人信息保护领域后，其内涵演变为：信息处理者须在处理个人信息前，向信息主体履行充分告知义务，并在获得其有效同意后方可实施处理行为，否则即构成违法，除非法律、行政法规另有例外规定[7]。此外，个人信息保护法还要求个人信息处理者不得过度收集个人信息，不得以个人不同意为由拒绝提供产品或服务，并赋予个人撤回同意的权利。

3.3. 个人信息保护的法规框架设计

在大数据条件下引入风险导向的个人信息保护规范，并不意味着对既有合法性原则的简单补充，而应当通过构建可操作的风险评估指标体系，实现对不同数据处理活动的分层规制。近来，有学者从社会

风险防控角度对《个人信息保护法》的相关规则进行了重新解读。在这种理解下，知情同意权、查询权、删除权等权能除了具备私权属性外，更是个人控制信息风险的工具；而处理目的合法、处理手段合理、数据处理评估、数据分类分级保存等规则也都是为了减少数据风险[8]。传统的风险评估主要由政府进行，但对于数字时代的信息风险而言，由于互联网企业是海量个人信息的日常处理者，更具有信息、技术、效率等优势进行风险评估，所以由其进行个人信息风险评估更具有合理性和可行性[9]。具体而言，风险评估可围绕以下要素展开：其一，数据类型因素，即处理对象是否涉及敏感个人信息或经聚合后具有高度人格指向性的衍生信息；其二，处理目的与方式因素，重点考察算法分析、自动化决策等技术是否可能对个人权益产生实质性不利影响；其三，处理规模与影响范围因素，包括数据主体数量、处理频率及潜在外溢风险；其四，技术可逆性因素，即相关技术措施能否有效防止再识别或滥用。

在此基础上，有必要针对不同风险等级的数据处理活动配置差异化的法律责任规则。例如，在人脸识别、精准画像等高风险场景中，可通过加重事前评估义务、强化明示同意标准及引入举证责任倒置等方式，提高处理者的合规成本；而在风险较低、具有公共利益或技术必要性的场景中，则可在严格安全措施前提下，适度引入合规豁免机制，以避免过度抑制数据合理利用。通过风险评估与责任配置的联动设计，方能使风险导向机制真正转化为具有可执行性的规范工具。

4. 个人信息保护的技术手段与实践

4.1. 数据加密与匿名化技术

在法律规范层面，数据加密、匿名化等技术措施的意义，并不在于其具体实现方式，而在于其是否能够产生相应的法律效果[10]。加密算法信息隐匿技术是保障个人信息安全的核心防线，其通过复杂的数学算法将原始个人信息转化为密文形式，使未经授权者难以解读信息内容[11]。现行《个人信息保护法》虽在规范层面鼓励采取去标识化、匿名化等技术手段，但并未明确其在责任认定中的法律地位，导致实践中技术合规与法律合规之间存在脱节。

以匿名化技术为例，其能否作为个人信息处理者减轻甚至免除部分义务的抗辩理由，关键在于是否实质性消除了识别特定自然人的可能性。若匿名化处理仍存在被重新识别的现实风险，则相关数据处理活动仍应适用个人信息保护法的完整义务体系，处理者不得以技术手段为由免除告知、同意等法定义务。反之，在严格技术标准和可验证安全措施的前提下，真正实现不可逆匿名化的数据处理，方可在一定范围内排除个人信息保护法的适用，从而降低合规负担。

同样地，差分隐私等新型技术措施，亦不应被当然视为合规的“免责护符”，而应纳入风险评估框架进行实质审查。只有当技术措施能够在客观上显著降低人格利益受损风险，并与处理目的具有必要性和比例性关联时，方可在法律适用层面产生相应的减责效果。由此，技术手段的法律评价，应当从“是否采用”转向“是否有效降低风险”。

4.2. 数据访问控制与审计

数据访问控制是保护个人信息不被未授权访问的关键技术手段。它包括基于属性的访问控制(ABAC)、基于策略的访问控制(PBAC)和基于信任的访问控制(TBAC)等方法。这些方法可以根据用户的属性、策略或信任级别来决定用户是否有权限访问特定的数据。在数据仓库和大数据系统中，可以通过行级安全和列级安全策略来限制用户对数据的访问权限。此外，数据脱敏和数据加密也是重要的访问控制手段，它们通过替换或加密敏感数据来保护用户隐私。访问控制清单(Access Control List, ACL)则可以基于用户身份、角色、部门等信息，限制用户对数据的访问权限。

数据审计则是监控和记录数据访问和操作的过程，它有助于检测和预防未授权的数据访问，以及在

数据泄露发生后追踪责任。通过审计日志，组织可以分析和识别潜在的安全威胁和异常行为。

4.3. 个人信息保护的最佳实践案例

在实践案例中，欧盟的《通用数据保护条例》(GDPR)是一个个人信息保护的典范，它规定了数据最小化和脱敏化的技术措施，以及对个人信息主体提供权利保障和便利的职责。在国内，一些互联网企业如腾讯公司也开始加强个人信息保护，在其产品中设置了严格的隐私协议和隐私设置。此外，企业在个人信息保护方面的最佳实践还包括识别敏感个人信息并分类定级、出台管理措施、通过技术手段防止个人信息泄露、监测异常信息传播以及通过安全审计措施追踪非法行为。这些实践案例表明，个人信息保护要以法律保护为基础，以代码为规制手段，使个人信息处理的全过程符合《中华人民共和国个人信息保护法》中提及的基本原则，在保证被采集者知情权的基础上，将对被采集者的影响控制到最小，并以数字协议的方式保证个人信息权益[11]。需要综合运用技术、管理和法律手段，以构建全面的保护体系。

5. 国内外个人信息保护经验借鉴

5.1. 欧美国家的个人信息保护立法

欧美国家在个人信息保护方面的立法经验对全球个人信息保护立法具有重要影响。欧盟和美国作为两个典型的代表，其立法模式和实践为其他国家提供了宝贵的借鉴。

欧盟通过《通用数据保护条例》(GDPR)建立了统一的个人信息保护框架，该条例适用于所有成员国，并以“一个大陆、一部法律”为原则，在欧盟内部建立了统一的个人信息保护和流动规则。欧盟已将个人信息保护视为一项独立于隐私权的基本权利，对其采取了强保护立场[12]。在具体机制设计之中，最能体现绝对权利路径的是第 82 条关于数据损害赔偿责任的规定，其规定了一般只存在于人格权侵权中的非物质损害赔偿[13]。GDPR 的实施对全球个人信息保护立法产生了深远影响，其严格的数据保护要求和高额的违规罚款成为全球个人信息保护立法的标杆。

与欧盟的统一法规不同，美国的个人隐私采取的是州级法律管理模式[14]。其采取立法与行业自律相结合的方式保护个人信息，主张政府有限干预。美国通过联邦立法结合各州分散立法构建基础法律框架，并在特定行业如健康保险、金融服务等领域有具体立法。此外，美国产业界也在积极推动产业联盟和行业认证等工作，如“在线隐私联盟”通过隐私认证机构 TRUSTe 推动行业隐私认证。

在个人信息保护方面，加强跨国和跨区域合作至关重要。欧盟通过跨国公司的数据规范义务将欧盟标准渗透至全球商业领域，产生“布鲁塞尔效应”，迫使其他国家主动推进国内法律制度向欧盟靠拢。此外，美欧个人数据跨境传输经历了多次制度安排，双方在限制情报机构活动、完善个人救济路径、更新审查和监督机制上不断磨合并达成暂时一致。

行业自律是个人信息保护的另一重要途径。美国的策略较为灵活，主要采取行业自律模式，即由公司或行业内部制定行业的行为规章或最佳实践指南，为行业的隐私保护提供示范和标杆。这种模式尊重企业自我选择，但也存在缺乏统一自律标准和有效监督的问题。

5.2. 典型案例分析

欧盟 GDPR 案例：欧盟 GDPR 的实施对个人信息保护产生了深远影响。例如，法国监管机构曾对 Google 处以 5000 万欧元的罚款，因为 Google 在未经用户同意的情况下擅自收集了用户的个人数据。这一案例体现了 GDPR 对违规行为的严厉处罚，也警示了企业在处理个人信息时必须严格遵守法律法规。

美国加州 CCPA 案例：美国加州的 CCPA 同样在个人信息保护方面发挥了重要作用。该法案规定，企业需向消费者披露其个人信息的收集、使用、出售等情况，并赋予消费者删除个人信息的权利。这有

助于提升消费者的信息保护意识，促进企业的合规经营。

近年来，我国在个人信息保护方面也取得了显著进展。例如，我国通过网络安全法、数据安全法和个人信息保护法等法律法规，构建了较为完善的个人信息保护法律体系。同时，我国还加强了数据跨境流动的监管，出台了《数据出境安全评估办法》等规范性文件，确保个人信息在跨境流动中的安全。

6. 结论

本文从大数据的视角出发，深入探讨了个人信息保护的规范体系，分析了现有法规的不足，并提出了改进措施。通过对国内外个人信息保护法规的比较分析，本文发现，尽管各国在个人信息保护方面取得了一定的进展，但仍存在差异和不足。欧盟的 GDPR 为个人信息保护提供了一个全面的法律框架，而美国则更侧重于行业自律和分散立法。本文提出的个人信息保护框架，结合了法律、技术和管理手段，旨在平衡数据利用与个人隐私保护。实证研究结果表明，该框架能够有效提高个人信息保护水平，减少数据泄露和隐私侵犯事件的发生。

参考文献

[1] 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.

[2] 丁晓东. 人工智能背景下个人信息保护制度的挑战与应对[J]. 政治与法律, 2026(1): 101-116.

[3] 江溯. 数据刑法概念的反思与重塑——以个人信息保护与数据获取行为的刑法评价为切入[J]. 南京大学学报(哲学·人文科学·社会科学), 2025, 62(2): 22-36+158.

[4] 陈铭熙. 大数据时代背景下公民个人信息保护的法律规制[J]. 文化学刊, 2024(11): 126-129.

[5] 赵瑜. 论大数据时代个人信息法律保护的基本原则[J]. 中国信息化, 2022(2): 68-69.

[6] 袁杰. 大数据时代个人信息的法律保护策略探讨[J]. 河北法律职业教育, 2023, 1(1): 91-95.

[7] 李翰林. 数字时代个人信息保护中“告知同意”的认定[J]. 山东法官培训学院学报, 2025, 41(6): 153-166.

[8] 梅夏英. 社会风险控制抑或个人权益保护——理解个人信息保护法的两个维度[J]. 环球法律评论, 2022, 44(1): 9-14.

[9] 刘权. 风险治理视角下的个人信息保护路径[J]. 比较法研究, 2024(2): 62-76.

[10] 周馨. 王丽华、王小龙: 探寻个人信息安全保护的关键密钥[J]. 大数据时代, 2025(9): 14-23.

[11] 李雪松. 大数据背景下个人信息保护的技术与方法研究[J]. 中国宽带, 2025, 21(6): 73-75.

[12] 李佳祺. 运用技术加强个人信息保护的路径探究[J]. 今传媒, 2024, 32(8): 19-22.

[13] 贾思晴. 个性化推荐技术下个人信息保护研究[D]: [硕士学位论文]. 上海: 华东交通大学, 2025.

[14] 刘绍宇. 论数字时代个人信息保护的风险规制路径[J]. 西南政法大学学报, 2024, 26(4): 142-158.