Open Journal of Legal Science 法学, 2025, 13(5), 847-852
Published Online May 2025 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2025.135120

Hans汉斯

数智时代个人信息保护的挑战与法律对策分析

周恩菊

宁波大学马克思主义学院，浙江 宁波

收稿日期：2025年4月1日；录用日期：2025年4月10日；发布日期：2025年5月13日

摘　要

在数字化与智能化飞速发展的数智时代，以大数据挖掘、生成式人工智能和自动化决策为核心的技术革新，不断重塑着个人信息搜集、利用和处理的运作模式。个人信息在数智时代兼具隐私属性与经济价值，如何平衡保护与利用成为全球性难题。自《中华人民共和国个人信息保护法》实施以来，已在规范数据流通、保护公民权益方面发挥了重要作用，但面对人工智能技术迭代与数字经济扩张，其实施仍面临技术适配性不足、法律执行差异化等挑战。通过分析数智时代个人信息的数据处理特征，揭示个人信息安全在技术、法律及监管执行层面的困境，提出完善立法体系、强化监管执行、优化技术赋能及多元共治机制等应对策略，为破解个人信息保护难题提供路径参考。

关键词

数智时代，个人信息保护，法律困境，法律对策

Analysis of Challenges and Legal Countermeasures for Personal Information Protection in the Digital Intelligence Era

Enju Zhou

School of Marxism, Ningbo University, Ningbo Zhejiang

Received: Apr. 1st, 2025; accepted: Apr. 10th, 2025; published: May 13th, 2025

Abstract

In the digitalization and intelligence era of rapid development, technological innovations centered around big data mining, generative artificial intelligence, and automated decision-making are continuously reshaping the operational models for personal information collection, utilization, and processing. In this era, personal information possesses both privacy attributes and economic value,

文章引用: 周恩菊. 数智时代个人信息保护的挑战与法律对策分析[J]. 法学, 2025, 13(5): 847-852.
DOI: 10.12677/ojls.2025.135120

making the balance between protection and utilization a global challenge. Since the implementation of the Personal Information Protection Law of the People's Republic of China, it has played a significant role in regulating data circulation and protecting citizens' rights and interests. However, in the face of iterative artificial intelligence technologies and the expansion of the digital economy, its implementation still faces challenges such as insufficient technological adaptability and differential legal enforcement. By analyzing the data processing characteristics of personal information in the digital intelligence era, this paper reveals the dilemmas of personal information security at the levels of technology, law, and regulatory enforcement. It proposes strategies to improve the legislative system, strengthen regulatory enforcement, optimize technological empowerment, and establish a multi-stakeholder governance mechanism. These strategies provide a reference path for solving the problem of personal information protection.

Keywords

Digital Intelligence Era, Personal Information Protection, Legal Dilemma, Legal Countermeasures

1. 引言

“数智化”是在大数据、人工智能和云计算等技术加持下智能地分析和应用数据。数智时代以数字化、网络化、智能化和移动化为主要特征，是信息社会、数字时代的概念延续[1]。在当今数字化与智能化深度融合的“数智”时代，大数据、人工智能、物联网等新兴技术蓬勃发展，深刻改变了人们的生活和工作方式。从便捷的移动支付、个性化的推荐服务到智能设备的广泛应用，信息技术为人们带来了前所未有的便利。然而，在享受技术红利的同时，个人信息安全问题也日益凸显。个人信息作为一种重要的数字资产，其保护面临着严峻的挑战。大量个人信息被各类主体收集和使用，信息泄露事件频发，给个人的财产安全、隐私保护甚至人身安全带来了极大的威胁。加强“数智”时代个人信息保护，已成为社会各界广泛关注的焦点问题，也是法学领域亟待深入研究和解决的重要课题。通过对相关挑战的分析，提出有效的法律对策，对于维护公民的合法权益、促进数字经济的健康发展以及构建安全有序的网络空间具有重要的现实意义。

2. 数智时代个人信息处理的特点

探讨个人信息保护所面临的挑战时，个人信息的处理方式是一个有效的分析视角。数智时代，人们的衣食住行都离不开互联网、大数据、人工智能等数字算法领域的应用。应用这些领域的首要条件是上传个人信息，便于算法系统识别、储存和加工。随着数智技术的更迭，信息处理也呈现出新的特征。

2.1. 数据收集的时效性与处理规模的复杂性增强

数智时代，个人数据的搜集体现出实时性与持续性的特点。数智技术使个人信息的搜集突破时空限制。例如，职场中通过电子打卡、智能坐垫、办公电脑监控软件等实时记录员工的工作状态、位置轨迹甚至生物特征，形成全天候的数据流[2]。在消费领域，用户的行为数据，如浏览记录、社交媒体互动被持续追踪并存储，形成动态画像，例如短视频平台通过用户观看习惯实时优化内容推荐，购物平台根据消费习惯准确推荐广告或商品。同时，个人信息处理规模与复杂性指数也在逐渐增长。大数据技术使得

个人信息处理从单一维度转向多维关联，企业可通过整合员工的健康数据、工作绩效、社交媒体活动等，构建复杂的个人档案以预测职业风险或优化管理决策。技术的升级换代使算法数据的聚合分析能力增强，不同领域可通过跨部门数据融合实现个人信息的共享，并作出精细化决策。在企业中，这些特征表象下发生很多涉及个人隐私与组织利益的平衡的法律案例。

2.2. 算法驱动的自动化决策与法律原则不对称

人工智能算法具有自动化、复杂性与难以预料的特性。特别是生成式人工智能与自动化决策技术的广泛应用，使得个人信息处理过程呈现“黑箱化”特征。“相关研究显示，在深度学习算法的训练环节中，其参数可能会经历数百万次的微调与优化。”[3]普通用户甚至开发者均难以洞悉并预测大语言模型的工作机理与决策流程，更遑论辨析预训练阶段个人信息数据的权利归属与隐私安全隐患。开发者无法明晰大语言模型“技术黑箱”的处理方式，难以向信息主体提供详尽的告知条款，这使得“知情同意”的原则难以贯彻。其次，大数据、人工智能、区块链的学习算法能通过其卓越的数据关联分析能力，给每个网络用户树立一个“数字标签”。算法广泛应用于个人信息的筛选与评价，很多招聘中可通过 AI 筛选简历，而“数字标签”可能因数据的误差导致就业歧视。但这种云计算的学习算法需要超大体量训练数据进行大语言模型的预训练，才能实现算法的最优化，这一过程已不满足将已公开个人信息的处理活动限定在信息主体公开个人信息的初始用途之上，对个人信息处理的“目的限定”原则构成持续挑战。

2.3. 数据的规模化整合与隐私穿透风险

随着数智技术的发展，个人信息数据规模呈指数级增长，个人信息被持续采集、存储和分析，数据维度更加丰富。可通过大数据技术、物联网设备、传感器等驱动技术，还原信息主体的网络行为轨迹、生物特征、社交关系等。其次，个人信息的数据来源呈多样化，可从个人的社交、网络平台的交易、传感器分析等渠道整合文本、图像、视频、日志等素材获取。甚至可以通过数据清洗、知识图谱等技术整合不同格式的数据以构建用户画像。而通过跨平台、跨场景的数据关联，碎片化信息也可还原为完整个人画像，使匿名化技术面临失效风险，个人信息安全风险增加。

3. 数智时代个人信息保护面临的挑战

随着数字经济的不断发展，数据集聚开发应用背后的隐私侵犯、信息泄露、数据泄密等现象引起社会高度警惕和公众普遍担忧，如何应对大数据时代个人信息保护面临的挑战成为学界亟待解决的问题。而数智技术的迅速更迭，使个人信息保护相关的法律体系在实施时往往力不从心，形成技术迭代与法律规制脱节的矛盾现象。

3.1. 技术革新带来的信息安全风险

《个人信息保护法》第 4 条规定公民保护的是“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。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。”数智技术时代，大量的个人信息在网络渠道被采集，个人网络信息可识别化技术直接影响网络用户的个人信息安全。目前，数智技术可以搜集散布在各网络平台上的信息片段，通过数据汇集和综合分析，使信息主体能被识别的概率越来越高，一些数据表面上不是个人信息，但经过处理后就可以追溯到个人。比如，本不具备身份识别属性的网络设备序列号与网络购物平台收货地址、快递运营商收件人身份码等信息相结合后，关联的信息主体即可被识别[4]。同时，匿名信息的反向还原越来越容易。一些匿名行为也不能完全保护行为主体，根据匿名言论的网址，很快能锁定个人。匿名处理被还原的可能性上升，导致个人信息法律边界所依赖的标准不稳定，使得原本应

当清晰界定的法律概念和准则面临模糊化的风险。

物联网装置与生成式人工智能的广泛运用，进一步加剧了个人信息面临的安全威胁。人工智能借助机器学习与深度学习技术，对个人信息进行分析，构建“用户画像”，揭示信息主体的行为模式与消费需求，从而显著提升了个人信息被滥用的风险。智能家居、可穿戴设备等在收集与传输个人信息过程中，若安全防护措施不到位，极易导致信息被非法获取或泄露。鉴于这些设备与用户的日常生活紧密相关，包含大量个人隐私数据，一旦信息泄露，后果将极为严重。例如，智能摄像头可能遭受黑客攻击，致使用户的家庭生活场景被非法截取与传播。此外，5G 技术的快速普及显著提升了数据传输速率，为个人信息的迅速传播与滥用提供了便利。不法分子能更高效地获取并利用个人信息，从事诈骗、盗窃等违法犯罪活动。

3.2. 法律法规在个人信息保护上的衔接与认定困难

当前法律体系虽几乎广泛覆盖公民生活各领域，但仍面临立法碎片化的挑战。例如《网络安全法》聚焦于系统防护，《个人信息保护法》着重于个人权益保障，《数据安全法》则强调国家安全，法律间存在制度衔接的空隙。在新兴技术应用场景下，法律规定尚不够详尽与明确。特别是在人工智能算法监管方面，具体法律规范不完善，算法设计、运用及管理存在不规范现象的法律责任认定困难。算法的不透明性阻碍了用户理解个人信息处理流程，也难以对算法决策实施有效监督与质疑。针对个人信息跨境流动，相关法律规定亦需进一步完善。伴随数字经济全球化进程，个人信息跨境传输需求激增，但现行法律规范在跨境数据安全评估、数据主体权利保护等方面尚有不足，难以充分应对个人信息跨境流动所带来的风险挑战[5]。

此外，不同法律法规之间在个人信息保护的规定上存在一定的不协调和不一致之处。这使得在实际执法和司法过程中，容易出现法律适用的困惑和争议，影响了个人信息保护的效果。一些部门法规对个人信息的定义和范围规定不尽相同，导致在实践中对于某些信息是否属于个人信息存在认定困难的问题。数智时代，信息主体若要证明信息处理者存在“过失”，也面临着极大的挑战。首要原因在于信息处理者对个人信息拥有强大的掌控力。凭借先进的大数据分析和人工智能技术，对个人数据进行深度挖掘，并经过技术处理后进行广泛传播、销售，使个人信息被众多信息处理者所掌握。大多数人只有在信息泄露引发的侵权事件发生后，方能意识到信息的失窃，这无疑加大了信息主体提供有效证据的难度。若继续坚持单一的过错归责原则，势必会导致信息主体追求个人信息权益救济的目的落空[6]。

3.3. 个人信息安全的监管执行难题

在“数智”时代，个人信息的收集和使用涉及众多主体和复杂的业务流程，这给监管执行带来了极大的挑战。监管部门难以全面掌握个人信息的收集、存储、使用和传输情况。一些企业和机构在收集个人信息时，可能未按照规定进行明确告知，或者告知内容不清晰、不完整，监管部门难以对其进行有效监督。尽管“GB/T35273-2017《信息安全技术个人信息安全规范》中增加了明确以用户自主作出的肯定动作作为特定业务功能开启的条件，虽然从表面上否认了默认勾选，但此规定只是在强行索权的基础上增加用户自动勾选的程序。”[7]部分 APP 或网络平台在用户注册时，以极小的字体、复杂的条款向用户告知个人信息收集情况。因条款的复杂性使得很多用户根本读不懂或在未仔细阅读的情况下就点击同意，而“同意”选项并不代表用户“知情”其中具体内容，这变相是把责任转移到用户身上，而监管部门很难及时发现并制止这种行为。

针对个人信息侵权行为，监管部门的执法手段相对有限。在处理技术复杂的非法活动时，监管机构可能因缺乏必要的技术支撑与专业人才而在调查取证方面遭遇障碍。部分黑客利用尖端技术窃取个人信

息，并通过加密等手段掩盖行踪，给监管机构的追踪与打击工作带来巨大挑战。另外，不同监管部门在个人信息保护领域的职责界定不够明确，常导致监管重叠或监管缺失的问题。在处理跨部门个人信息保护事务时，可能出现部门间推诿责任、协作机制不畅的情况，进而影响了监管的效能与成果。

4. 数智时代个人信息保护的应对机制

4.1. 完善法律体系，强化法律保障

为应对数智化时代个人信息保护的新挑战，需适时更新并健全相关法律框架。针对数智时代的特性，需深化个人信息保护立法建设，制定针对新兴技术应用的专项法规，清晰界定人工智能、物联网等技术在个人信息收集、运用及处理方面的规范与准则。对于人工智能算法，应明确算法开发者及使用者的权责，确保算法具备透明度与可阐释性，保障用户享有对算法决策的知情权及异议权。构建完善的个人信息跨境流动法律机制，确立跨境数据安全评估的流程与标准，强化对数据主体权利的保障。规定个人信息跨境传输须经数据主体明确授权，并采取充分的安全措施，确保跨境传输中个人信息的安全。此外，为确保权利救济渠道的畅通，需加强司法保护体系、提升行政执法效能、强化行业自律准则及推动公益诉讼等多元化救济途径，以切实维护个人在信息利用过程中的合法权益。对现有法律法规进行整合和协调，消除不同法律法规之间在个人信息保护规定上的矛盾和冲突。统一个人信息的定义和范围，明确个人信息保护的基本原则和具体规则，为执法和司法提供清晰的法律依据。对《网络安全法》《数据安全法》《个人信息保护法》等相关法律法规进行梳理，对其中重复或不一致的条款进行修订和完善，形成一个有机统一的个人信息保护法律体系。

4.2. 强化技术赋能，提升保护效能

面向数智时代的特点，利用区块链、差分隐私等先进手段，创新性地发展身份核验、行为轨迹追踪及态势监测等隐私防护技术，以强化从预防阶段、保护过程到追溯环节的全链条风险防控效能，减少原始数据暴露风险。通过去中心化、匿名化等技术手段，强化数据脱敏与数据加密等技术在个人信息数据采集、传输、存储至使用各阶段的综合应用，以确保从数据源头至传输路径中有效防止信息泄露的风险。同时，加强算法透明度建设，创新性地引入区块链技术，利用其不可篡改的特性，对算法决策过程进行全程记录，确保每一步操作都能被准确追踪与审计。保障个体对算法决策的知情权和解释权。特别是针对算法的技术黑箱问题，需平衡披露范围与创新保护。可要求企业对高风险算法进行有限披露，同时允许低风险场景保留技术机密。

4.3. 培养监管技术人才，强化监管执行

增强监管机构的科技实力，培育专业技能人才，以提升其在个人信息保护技术领域的认知与实施能力。监管机构需装备尖端技术设施，监控并分析个人信息的采集、运用及传输动态，确保能迅速识别并阻止任何违法活动。构建专项技术监察系统，对各类应用程序、网站实施不间断监控，评估其个人信息处理行为是否符合法律法规要求。此外，应清晰界定各监管机构在个人信息保护领域的职责边界，并强化部门间的协同与信息交流。建立跨部门联合执法体系，凝聚监管力量。面对重大个人信息保护案件，网信、公安、市场监管等部门需紧密配合，协同推进调查、取证及惩处工作，从而提升监管效能。针对侵犯个人信息的行为，应加大惩罚力度，提升违法成本。对于违规收集、使用或泄露个人信息的企业与机构，依据法律严厉实施行政处罚，措施涵盖罚款、停产停业整顿、吊销执照等。对于触犯刑法的行为，则依法追究刑事责任。通过这些严厉的惩治举措，构建对个人信息侵权行为的强大震慑效应，有效遏制此类违法犯罪活动的蔓延。

4.4. 构建多方位协同治理与监督框架

在数智化时代，个人信息安全展现出日益复杂且多变的特征。单纯依赖政府的法律监管难以充分汇聚保护力量。因此，需倡导政府、企业、社会团体及个人携手参与个人信息保护，构建全面协调的治理与监督网络。政府需强化监管职能，确立清晰的行业准则与规范，并督促数智技术开发者与企业切实履行数据主体的安全责任，确保遵循国家法规与弘扬社会道德。企业应主动担当数据保护的首要责任，强化内部数据安全管理机制，运用加密、去标识化等技术强化防御，有效抵御内部操作失误及外部攻击带来的数据泄露风险。同时，需广泛且深入地开展宣传教育活动，借助学校教育、社区推广、媒体播报等多元化途径，普及个人信息保护知识及相关法律法规。公众则需提升自我保护意识，积极主动投身于个人信息保护行动，勇于举报数据泄露与滥用事件，并在日常生活中谨慎处理个人信息。在使用各类 APP 及网络服务时，应细致阅读隐私条款，审慎授权个人信息，避免在非可信平台上随意透露个人敏感数据。

5. 结语

数智时代的个人信息保护，本质上是一场技术理性与法律价值的博弈。破解当前困境，需要构建“科技向善”的价值导向、“风险可控”的技术逻辑、“权责适配”的法律框架的三重耦合机制。数智时代，随着脑机接口、元宇宙等新技术的涌现，个人信息保护或将向神经数据、数字身份等新领域延伸，要求法律对策保持动态适应性。唯有通过技术治理、法律规制、提高企业与个人的道德修养等方面协同创新，方能在数据红利与个体权利之间找到可持续平衡点，为数字经济健康发展提供制度保障。

参考文献

[1] 赵磊磊, 陈祥梅. 数智时代教育大数据风险: 表征样态与化解路向[J]. 贵州师范大学学报(社会科学版), 2022(2): 72-82.

[2] 梁栋. 数智化职场中劳动者个人信息保护的特性、价值与规则[C]//《智慧法治》集刊 2024 年第 2 卷——“东方法学新锐”研究文集. 北京: 北京理工大学法学院, 2024: 104-116.

[3] 高彩艳. 人工智能算法在个人信息保护中的应对策略[J]. 数字通信世界, 2024(11): 11-13.

[4] 李军, 慕小璐. 数字经济时代个人信息保护司法实践探析[J]. 河北法律职业教育, 2024, 2(11): 46-51.

[5] 王蕾. 企业数据跨境流动治理研究[D]: [硕士学位论文]. 南京: 南京财经大学, 2023.

[6] 郭凯. 大数据时代个人信息司法治理的困境及对策[J]. 重庆行政, 2020, 21(6): 72-74.

[7] 金泓序, 何畏. 大数据时代个人信息保护的挑战与对策研究[J]. 情报科学, 2022, 40(6): 132-140.