Open Journal of Legal Science 法学, 2026, 14(5), 202-209
Published Online May 2026 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2026.145151

Hans汉斯

数字时代个人信息保护的民法困境与完善路径

——以《中华人民共和国民法典》实施为视角

施　砚

宁波大学马克思主义学院，浙江　宁波

收稿日期：2026年4月13日；录用日期：2026年4月29日；发布日期：2026年5月26日

摘　要

在数字化成为常态的时代，数字经济也如潮流一般席卷了人们的生活，最直观的改变是实体的金钱变成了手机中的一串数字，数字经济下社会生活的各方面都充斥着便利，这也是多数人所偏好和希望的。但由于个人信息本身的特殊性，它兼具人格利益与财产利益双重属性，在当下已成为社会运行与市场交易的重要资源。由于当下网络数据的获取方式使得获取本身变得更容易，导致个人信息变成了半开放甚至全开放状态。虽然说，我国《民法典》通过人格权编中的一些规定，在一定程度上明确了个人信息保护的基本规则，并在民事权益层面作为一种较为权威的规范和理论加以保障。但在具体的司法实践与社会应用中，个人信息保护仍面临着权利边界模糊不清、侵权责任认定和追责困难、举证责任分配失衡、救济机制不够完善等亟待解决的现实问题，加之技术逻辑与法律规范之间存在衔接壁垒。本文将从《民法典》中个人信息的法律定位入手，梳理当前民法保护存在的主要困境，剖析其形成原因，并从权利属性明晰、救济机制优化等方面提出建议。

关键词

个人信息保护，《民法典》，侵权责任，数字法治

Civil Law Dilemmas and Improvement Pathways for Personal Information Protection in the Digital Age

—From the Perspective of the Implementation of the *Civil Code of the People's Republic of China*

Yan Shi

School of Marxism Studies, Ningbo University, Ningbo Zhejiang

文章引用: 施砚. 数字时代个人信息保护的民法困境与完善路径[J]. 法学, 2026, 14(5): 202-209.
DOI: 10.12677/ojls.2026.145151

Received: April 13, 2026; accepted: April 29, 2026; published: May 26, 2026

Abstract

In an era where digitization has become the norm, the digital economy has swept through people's lives like a tidal wave. The most tangible change is the transformation of physical money into strings of numbers on mobile phones. Digitalization has brought convenience to all aspects of social life, which is what most people prefer and hope for. However, due to the unique nature of personal information, which possesses both personality and property interests, it has now become a critical resource for social operation and market transactions. As the means of acquiring network data have made such acquisition easier, personal information has become semi-open or even fully open. Although China's *Civil Code*, through certain provisions in the Personality Rights Book, has to some extent established basic rules for personal information protection and provides a relatively authoritative normative and theoretical guarantee at the level of civil rights and interests, specific judicial practice and social application still face pressing practical issues, such as ambiguous boundaries of rights, difficulties in determining and pursuing tort liability, imbalanced allocation of the burden of proof, and inadequate relief mechanisms. Additionally, there is a gap between technological logic and legal norms. This paper begins by examining the legal positioning of personal information under the *Civil Code*, identifies the main dilemmas in current civil law protection, analyzes their causes, and proposes suggestions in terms of clarifying the attributes of rights, reconstructing tort liability, and optimizing relief mechanisms.

Keywords

Personal Information Protection, *Civil Code*, Tort Liability, Digital Rule of Law

Copyright © 2026 by author(s) and Hans Publishers Inc.
This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).
http://creativecommons.org/licenses/by/4.0/
Open Access

1. 问题的提出

众所周知，大数据、云计算和人工智能等数字技术已与社会生活紧密结合。在个人层面，这些技术在个人信息的存储、使用、传输和交易等方面变得愈加普遍。在提高公共治理效率和推动商业创新的过程中，也伴随着信息泄露、滥用以及非法买卖等一系列风险的加剧。从日常生活中的人们收到的群发的垃圾短信、骚扰电话，到根据个人情况精准推送引发的个人隐私侵扰，再到电信网络诈骗导致的财产损失，个人信息安全问题已渗透到社会各个角落，成为全社会共同关注的法治议题。

《中华人民共和国民法典》(后文简称《民法典》)提出个人信息受法律保护，并作为人格权编的重要内容，也在第六章中进一步专门解读了隐私权和个人信息保护，逐步确立了民法保护个人信息的框架，明确了信息处理者的义务、侵权责任的基本规则，为公民个人信息权益的保护提供了根本遵循。《民法典》提出个人信息保护法的本质是领域法，数字经济时代的个人信息保护体系，不仅要体现数字化、信息化的时代特征，还要考虑个人信息整体处理系统及其环境对应用和保护方式的影响[1]。

然而，由于数字场景的复杂性、技术应用的专业性以及信息主体与处理者地位的不平等性，现行规则在具体适用过程中并没有那么理想化，存在一定程度的局限性，权利界定、责任认定、损害赔偿、举

证分配等关键问题都尚未完全明晰，导致司法实践中出现裁判尺度不一、保护力度不足等问题，所以还要通过在各种现实场景的对比使得法律不断完善。

2. 个人信息的法律界定与民法定位

2.1. 个人信息的法律内涵

《民法典》第一千零三十四条明确规定：“个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。”同时这一规定明确了个人信息的法定含义，为司法实践中个人信息的认定提供了基本标准，对理解个人信息的范围提供了清晰的法律依据。从该表述可以得出，个人信息具有三个核心特征，这也是区分个人信息与其他信息的关键，更是准确界定研究对象的基础：

一是可识别性，即锁定特定自然人可以通过信息的直接或间接指向。《中华人民共和国个人信息保护法》(后文简称《个人信息保护法》)第四条[1]对个人信息的定义也突出了个人信息判定的“可识别”特征，并据此区分了一般信息和敏感信息[2]。直接识别是指仅凭单一信息即可确定具体个人，例如身份证件号码、指纹、人脸等生物识别信息；间接识别则是指当单一信息不足以锁定个人的时候，可以通过与其他信息结合后再精准定位特定主体，例如将姓名、住址与电话号码组合使用。

二是内容广泛性。个人信息涵盖的各类信息主要体现与自然人的人身、财产有关，既包括姓名、性别、出生年月、住址等常见身份信息，也包括健康信息、生物识别信息、行踪轨迹、理财账户等敏感的个人信息。考虑到敏感个人信息一旦泄露或被滥用，极易对人身财产安全造成难以估量的风险。在风险规制范式下，风险识别是风险评估的重要前置环节，其中涉及风险标准比对关系和后续风险合规的效率与行政资源的分配[3]。因此《个人信息保护法》在规则处理上进一步做出了限制，不可避免的这种限制将会相对严格。

三是载体多样性。个人信息的载体并不限于电子形式，而是同时包含电子与非电子载体。电子形式的载体常见于手机通讯录、社交记录、网络浏览痕迹、云端数据等数字化信息；非电子载体则包括身份证复印件、个人纸质档案、业务办理的资料存根等。无论以何种方式进行记录，只要能够被识别，便属于法律保护的个人信息。

2.2. 个人信息在民法体系中的定位

《民法典》没有直接使用“个人信息权”这一表述，而是采用了“个人信息受法律保护”的说法[2]。这一内容可以归属于人格权编中“隐私权和个人信息保护”这一章节，与隐私权并列的规定展现了我国在界定个人信息法律属性时所采取的审慎态度。对于属于隐私范畴的个人信息，由于其具有强烈的人格属性，原则上也应当严格限制流通[4]。具体而言，这一定位体现了三层法理逻辑：

首先，人格利益在属性中占据核心地位。人身自由、人格尊严，这些与自然人密切相关的个人信息是重要的承载形式，也是人格利益的体现形式。无论是泄露个人健康信息造成他人歧视、滥用个人行踪信息侵犯他人人身自由，还是泄露个人隐私信息造成他人名誉受损，都可能造成自然人人格尊严受到侵害。因此，《民法典》将符合个人信息保护本质需求的个性信息纳入个性权利的汇编中，以彰显个性利益。

[1]《中华人民共和国个人信息保护法》第四条 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。
[2]《民法典》第一百一十一条 自然人的个人信息受法律保护。

其次，兼具财产利益属性。个人信息倾向于一种具有显著商业价值的重要生产要素，这是在数字经济高速发展的大背景下产生的。从多个主体的运营中可以体现出来：平台企业通过对用户个人信息的收集分析、用户画像的构建、精准广告的推送、个性化产品的开发等方式获得巨大的商业利益；通过对个人信用信息的分析，金融机构对信用风险进行评估，从而降低交易成本；通过对健康信息的分析，医疗机构开展疾病研究，优化诊疗方案，兼具公共健康价值和社会公益价值。这些做法充分表明，个人信息不仅关乎个人的权利利益，还涉及财产利益，二者构成了一个综合体。

最后，属于新型复合民事权益。个人信息所代表和体现的利益，既非纯粹的人格利益，也非纯粹的财产利益，而是兼具人格与财产双重属性的新型民事权益。相对于传统人格权(如姓名权、肖像权)而言，当前时代更突出的是个人信息的财产性、利益性；作为个人信息核心的人格利益，相对于传统的物权、债权等财产权而言，不可能脱离自然人而独立存在。

3. 个人信息民法保护的现实困境

3.1. 权利边界模糊，保护规则不够明确

首先，权益与权利的定性不清晰。《民法典》仅确认个人信息受法律保护，未明确其为独立的民事权利，仅将其界定为“受保护的民事权益”，这种模糊的定性导致实践中对个人信息的保护强度、权利行使方式、救济途径等缺乏统一标准。个人信息权益的排他性、支配性相对于物权、债权等明确的民事权利而言较弱，权利人很难像行使物权一般主张排除妨碍或恢复原状，也很难在个人信息权益受到侵害时明确自己的权利边界，导致维权缺乏明确的法律依据。例如，在司法实践中，对于平台企业擅自收集用户个人信息的行为，有的法院认定其侵害了个人信息权益，判决平台承担侵权责任；部分法院则侧重判令删除信息、停止处理，对损害赔偿请求支持较为谨慎，导致裁判尺度不一，影响法律适用的稳定性。即使平台为用户提供选择加入或退出机制，这种控制也是极其有限的，当平台与第三方分享时(服务提供商或广告商)，个体无法知晓是谁获取了其信息，更无法控制信息的流转[5]。

其次，个人信息与隐私权的界限易混淆。如前所述，个人信息与隐私权存在交叉，大量案件中二者会出现竞合，当事人存在困惑，跨专业研究者在开展研究时也容易出现概念混用、分析偏差的问题。例如，参见 2022 年 8 月 1 日作出(2021)京 0491 民初 5094 号民事判决 [3]，在该案例中，某 APP 擅自收集用户的手机通讯录信息并用于商业推送，用户起诉时既主张 APP 侵害其隐私权，又主张侵害其个人信息权益。法院在规范运用上有侧重的区别：有的法院侧重于对私密性信息的认定和私密性规则的适用；一些法院强调对个人信息保护规则的可识别性和适用性。

最后，财产利益保护不足。现行法律规则更侧重个人信息的人格利益保护，针对财产利益的配置规则与救济机制尚不健全。《民法典》仅规定了个人信息的人格利益保护相关规则，未明确个人信息财产利益的归属、行使方式、收益分配等问题。在实践中，平台企业通过收集、利用用户个人信息获取巨额商业利润，但用户作为信息来源主体，却无法主张财产性赔偿，也无法参与收益分配，导致“平台获利、用户担险”的失衡格局。

3.2. 侵权责任认定困难，举证压力失衡

第一，侵权主体难以确定。数字时代，个人信息的处理链条漫长且复杂，涉及信息收集者、存储者、加工者、传输者、第三方合作机构等多个主体，形成了“收集－存储－加工－传输－利用”的完整产业链。一旦发生信息泄露、滥用等侵权行为，往往涉及多个环节，权利人难以精准锁定具体侵权主体；且

[3]https://www.court.gov.cn/shenpan/xiangqing/474481.html

部分主体通过技术手段隐匿身份，或通过格式条款约定免责条款，进一步加大了主体认定的难度。

第二，因果关系证明复杂。个人信息侵权多发生在网络虚拟空间，网络平台是网络活动与信息交互的重要载体，已经成为落实个人信息保护政策的关键抓手和事实上的治理主体[6]。具有隐蔽性、技术性、跨地域性等特征，侵权行为的实施过程往往通过大数据算法、云计算等技术完成，普通权利人不具备相应的技术能力与取证条件，无法完整证明一种因果关系，主要是指侵权行为与损害结果之间的。比如，参见 2017 年 3 月 27 日作出(2017)京 01 民终 509 号民事判决 [4]，用户遭遇电信网络诈骗，损失了巨额财产，虽然能够证明其个人信息被泄露，但无法证明泄露的信息来自于哪个主体，泄露的路径是什么，也无法证明诈骗行为与信息泄露之间存在直接的因果关系，导致侵权责任认定在法院的认定上存在一定的难度。

第三，过错认定难度大。《民法典》对个人信息侵权采用过错责任原则，即权利人需证明侵权人存在故意或过失，才能要求其承担侵权责任。但在数字场景下，信息处理者多采用自动化算法技术处理个人信息，其行为的主观过错难以判断；且平台企业作为强势主体，掌握全部技术与数据信息，权利人根本无法获取对方存在过错的证据，导致过错责任原则举证困难、实践适用不畅。如平台企业未采取有效信息安全保护措施导致用户信息泄露，但平台往往以权利人无法举证证明平台存在过错，最终无法获得赔偿为由进行抗辩，理由是平台企业已采取合理的技术措施并尽到安全保障义务。

3.3. 救济机制不畅，个体维权成本过高

一方面，高成本、低收益的特征主要体现在民间力量的救济上。个人信息具有显著的权益复合性与侵权整体性特征，其救济渠道横跨民事、刑事与行政程序[7]。个人信息侵权具有“小额多量”的特征，单个权利人的损失往往较小，但维权需投入大量的时间、金钱、精力成本。从调查取证、与侵权人协商沟通，到提起诉讼、参与庭审，整个流程繁琐、周期漫长，普通权利人难以承受。例如，用户因个人信息被泄露遭遇骚扰电话，想要维权，需要先收集骚扰电话的证据、证明信息泄露的来源，再向法院提起诉讼，整个过程至少需要 3~6 个月，且需要支付律师费、诉讼费、鉴定费等相关费用，而最终获得的赔偿往往不足以覆盖维权成本，导致多数权利人选择“忍了算了”，形成“理性冷漠”，大量侵权行为得不到追究，公益诉讼的适用范围则相对有限。个人信息保护公益诉讼制度虽然在《中华人民共和国民事诉讼法》《个人信息保护法》中都有规定，明确检察机关、消费者协会等特定机关可以提起公益诉讼，但公益诉讼在实践中的启动门槛较高，适用场景较窄。民法上因果关系的功能在于确定损害后果由哪些主体造成，以合理分配侵权责任[8]。公益诉讼仅针对侵害众多个人信息权益、损害社会公共利益的行为，对于单个用户信息泄露、骚扰电话等分散、小额、高频侵权行为，公益诉讼不能发起；且公益诉讼审理周期长、程序复杂，权利人维权需求难以得到快速反应，不能形成常态化威慑。

同时，事前预防机制薄弱。但其实从保护实效出发，鉴于个人信息具有风险不确定性和损害不可逆性的特征，事后惩罚对于控制风险和填补损害往往无济于事，前端预防应当在个人信息保护中发挥更大作用[9]。风险社会与科技革命驱动预防型法治成为现代风险治理的关键路径，预防性规范在民法、刑法与行政法领域均广泛嵌入[10]。目前的法律规定主要关注事后损害赔偿，对于个人信息的事前保护和事中监管方面的规定相对不足，缺乏对信息处理者的强制合规要求、风险评估机制以及安全保障义务的具体细化。平台企业大多重利用、轻保护，没有建立有效的信息安全保护制度，没有进行个人信息保护影响评估，也没有制定信息泄露的应急处理机制，导致泄露、滥用信息等侵权行为频发，平台企业普遍存在安全隐患。个人信息保护影响评估机制的本质是针对“特定安全风险”进行事前评估，既不同于传统意义上的纯粹风险评估，侧重具体的风险类型识别[11]。

[4]https://www.bjinternetcourt.gov.cn/details.html?id=68

4. 困境形成的主要原因

4.1. 立法规则偏碎片化、原则化，配套制度不完善

我国当前有关个人信息保护立法存在碎片化问题，不同部门法之间衔接断层[12]。《民法典》作为民事基本法，仅确立个人信息保护的基本框架，无法细化数字场景下的具体问题，需要司法解释、行政法规等配套补充，“在前数字经济时代，我国关于个人信息保护的立法规定散布于各种规范性文件之中，立法的碎片化特征明显”。目前，即使有《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》《中华人民共和国数据安全法》这样的专门法律，在责任类型、赔偿标准等方面，与民法典的衔接并不顺畅，有抵触，也有空白；且相关司法解释、部门规章不健全，模糊规定了权利边界、举证责任等关键问题，致使司法实践中的茫然不知所措。

4.2. 信息主体与处理者地位严重失衡

个人信息处理者大多是拥有资金和技术优势，主导信息处理全过程的大型互联网平台等强势主体；而作为信息主体的普通公民，在信息的支配和话语权上处于弱势。平台通过冗长晦涩的格式条款，强制用户同意信息收集使用，用户无协商余地，只能“要么同意、要么不用”。但其实《民法典》及《个人信息保护法》中知情同意规则系处理个人信息最重要的合法性基础，其背后的法理基础是尊重私主体对信息的意思自治[13]。例如，注册 APP 时需勾选隐私政策方可完成注册，而隐私政策冗长且专业术语繁多，用户无力仔细阅读，只能被动同意，无法体现真实意愿。

4.3. 技术壁垒加剧信息不对称

大数据、算法等数字技术的专业性，进一步拉大了处理者与信息主体的信息差。平台自行控制信息收集范围、使用目的、传输路径等，普通用户无法知晓自身信息的处理情况，也难以判断处理行为是否合法。比如，平台对用户浏览记录、地理位置等信息进行隐蔽收集，用户对这些信息浑然不觉；既削弱了用户对信息的控制力，通过算法构建用户画像、推送精准广告，用户无法有效介入。

4.4. 侵权成本低而维权成本高

对于个人信息侵权行为，现行法律的惩处力度不够，形成了不良的诱因。一方面，侵权成本极低，损害赔偿与行政处罚额度远低于侵权获利，难以形成有效威慑，部分平台违规处理信息获利丰厚，却仅受到轻微处罚。另一方面，维权的费用相当高昂，个人在维护信息权利时需要投入大量的时间和金钱，普通权利者往往难以承担，加重了保护中的困境。

5. 完善个人信息民法保护的路径

5.1. 重构侵权责任规则，降低维权难度

第一，过错推定责任适用于对待平台等信息处理。优化个人信息侵权责任追究制度，实行举证责任倒置，对过错推定责任适用于平台企业等强势信息处理方。权利人仅需证明存在侵权事实、损害后果及二者间的初步关联关系，由信息处理者就其无过错承担举证责任，无法证明的应承担侵权责任。该规则可有效缓解举证失衡，降低普通用户维权难度。例如用户证明个人信息由平台泄露并遭受损失，平台若无法证明已尽安全保障义务，即应承担责任。

第二，简化因果关系认定规则。建立推定因果关系的规则，以适应数字环境技术和隐蔽性的特点。权利人能够证明信息处理者存在违规处理行为或安全防护漏洞，且其个人信息因此遭受侵害的，即可推

定行为与损害之间存在因果关系；处理者能够证明损害系不可抗力、第三人独立行为等法定免责事由所致的除外，避免权利人因技术壁垒无法举证而维权不能。

5.2. 明晰权利属性，界定保护边界

一是通过司法解释确立个人信息权利的独立性。明确个人信息权属于新型民事权利，兼具人格和财产属性，界定其包含知情权、决定权、删除权等核心内容，强化权利的支配性和排他性，明确行使权利的方式和保护强度，统一司法裁判尺度，为权利人维权提供便利。

二是对个人信息的适用边界和隐私问题进行细化。通过司法解释明确了区分标准：隐私侧重隐私与不公开，适用于私人空间、活动和信息，保护人格尊严；个人信息集中在可识别、对信息控制的保护和对整个信息处理过程的覆盖等方面。二者竞合时，允许权利人选择最优救济途径。

5.3. 完善救济机制，提升保护实效

一是降低诉讼维权成本，通过简化诉讼程序制度。民事救济的目的为实现矫正正义，刑事惩罚的目的为实现报应正义，法秩序的价值统一要求不同部门法之间协力实现各自的价值，实现部门法间的价值协调[14]。对涉及个人信息纠纷的小额诉讼、简易程序等，设立专门通道，在减少权利人时间成本的 1~3 个月内，简化流程，缩短审理周期；实行举证责任倒置和证据保全制度，对平台掌握的证据，法院可以依职权或依申请调取，减轻权利人的举证负担；为经济困难的权利人提供无偿法律服务，降低经济成本，促进维权积极性，完善法律援助和公益律师制度。同时，推行代表人诉讼制度，针对批量同类侵权案件，由权利人推选代表人提起诉讼，提升维权效率、降低整体成本。

二是激活扩大适用范围的公益诉讼制度。拓宽公益诉讼主体范围，允许符合条件的社会组织、行业协会参与个人信息保护公益诉讼，充实维权力量；降低启动门槛，不仅针对大规模群体性侵权，对骚扰电话、垃圾短信等频发小额侵权行为，也可启动公益诉讼，实现全面保护；建立公益诉讼赔偿金管理制度，将赔偿金用于赔偿受损权利人、支持公益保护事业，提升公益诉讼实效性。针对被害人损害无法得到充分赔偿的情形，建立赔偿金制度，当侵权人无法足额赔偿被害人损失时，从赔偿金中给予被害人一定的补偿，以切实保障被害人的合法权益[15]。

5.4. 打破学科壁垒，推动协同治理

个人信息保护本质上是法律、技术、管理、伦理的综合性问题，适当打破学科间的无形壁垒，有利于跨学科的协同治理，单一学科的研究并不能完全解决个人信息保护的困境。

一是加强跨学科研究与交流，搭建跨学科交流平台，推动法学、计算机、经济学、社会学、管理学等领域的学者开展联合研究，法学研究吸收信息技术知识，确保立法建议、法律适用贴合技术现实；理工、经管等学科融入法学思维，规范技术应用与商业行为，形成跨学科的研究合力。

二是构建专业辅助机制，司法所在审理案件时，为帮助司法人员理解技术逻辑、提高裁判准确率，聘请技术专家提供咨询、鉴定意见，建立个人信息保护技术专家库；为个人信息保护提供人才支撑，高校和科研单位设置跨专业课程，培养既懂法律又懂技术的复合型人才。

6. 结论

个人信息保护既是保障公民人格尊严、人身财产安全的必然要求，也是促进数字经济健康发展的重要支撑，在数字社会持续发展的大背景下，已经成为民权保障和数字经济治理的重要内容。虽然面对快速迭代的数字技术、复杂多变的实践场景，以及跨专业研究的需求，民法典奠定了个人信息民法保护的基础，确立了个人信息保护的基本框架和原则，但在界定权利、认定责任、救济程序、跨学科应用等方

面，仍存在着现实的困境。这些问题的形成，既与立法规则的原则性、配套制度的不完善相关，也源于信息主体与处理者的地位失衡、技术壁垒的存在、侵权成本与维权成本的失衡等现实因素。

民法学为构建更为完善的个人信息保护体系，应对个人信息的权利属性、保护边界等进行进一步明确；健全多元救济机制，优化诉讼程序，活化公益诉讼，加强事前防范和事中监督，增强保障实效；致力于在数字经济发展的基础上，构建政府、企业、社会组织和公民共同参与，实现其与个人信息保护良性互动的治理格局。

参考文献

[1] (德)拉尔夫·波歇尔, 周遵友, 余云霞. 数据保护权是一项权利吗——基于欧盟和美国的考察[J]. 苏州大学学报(法学版), 2024, 11(2): 153-160.

[2] 艾琳. 平台用工中个人信息保护的困境表现与规则回应[J]. 政治与法律, 2026(3): 20-32.

[3] 唐林. 个人信息保护影响评估制度的风险规制与优化路径[J]. 学习与探索, 2026(2): 93-101.

[4] 顾理平. 面子里的人格尊严: 智媒时代公民的隐私保护[J]. 南京师大学报(社会科学版), 2022(4): 128-138.

[5] 贾丽萍. 个人信息处理规则的结构性困境与路径优化[J]. 学习与探索, 2023(6): 81-90.

[6] 胡凌. 数字架构与法律[M]. 北京: 北京大学出版社, 2024: 223.

[7] 王立梅. 法秩序统一视角下的个人信息保护民刑程序衔接规则[J]. 法学论坛, 2026, 41(2): 103-114.

[8] 纪格非. 我国刑事判决在民事诉讼中预决力规则的反思与重构[J]. 法学杂志, 2017, 38(3): 31-43.

[9] 张涛. 风险预防原则在个人信息保护中的适用与展开[J]. 现代法学, 2023, 45(5): 52-72.

[10] 黄文艺. 论预防型法治[J]. 法学研究, 2024, 46(2): 20-38.

[11] 周瑞珏. 面向网络安全风险的保险合同义务理论创新[J]. 学术交流, 2024(5): 73-87.

[12] 刘艳红. 数字经济时代个人信息保护的民行刑一体化推进研究[J]. 华东政法大学学报, 2025, 28(6): 6-21.

[13] 杨勤法, 程圆圆. 劳动者个人信息权益保护的法律困境与对策[J]. 中国人力资源开发, 2022, 39(6): 94-104.

[14] 雷磊. 法秩序统一性原理之建构[J]. 法学研究, 2025, 47(1): 22-41.

[15] 贾文超, 王沁, 周璇, 等. 大数据时代下个人信息保护刑事附带民事公益诉讼的思考[J]. 征信, 2024, 42(11): 24-30.