

探究我国数字社会中个人信息保护的困境与未来展望

邹丛聪

青岛大学法学院, 山东 青岛

收稿日期: 2026年8月3日; 录用日期: 2026年9月2日; 发布日期: 2026年9月11日

摘要

在数字社会快速发展的背景下, 我国个人信息保护面临严峻挑战。互联网APP、小程序的泛滥及生成式人工智能的兴起, 使个人信息收集模式多元化(被动提供、主动提供、第三方共享), 但数据采集未经许可、销毁不彻底、APP过度获取权限等问题突出。生成式人工智能更打破信息分散状态, 加速信息整合与滥用风险。个人信息的商业价值推动其在精准营销、风险评估等领域广泛应用, 却也引发隐私泄露与公共秩序破坏。尽管我国《个人信息保护法》的实施标志着保护进入新阶段, 但法律法规的细化不足与技术安全威胁(如黑客攻击、企业防护薄弱)仍构成主要困境。未来需从法律完善、技术升级等层面探索更有效的保护路径。

关键词

数字社会, 个人信息保护, 收集模式, 法律困境

Exploring the Challenges and Future Prospects of Personal Information Protection in China's Digital Society

Congcong Zou

Law School, Qingdao University, Qingdao Shandong

Received: August 3, 2026; accepted: September 2, 2026; published: September 11, 2026

Abstract

Against the backdrop of the rapid development of digital society, China faces severe challenges in

文章引用: 邹丛聪. 探究我国数字社会中个人信息保护的困境与未来展望[J]. 争议解决, 2026, 12(9): 58-65.

DOI: 10.12677/ds.2026.129255

protecting personal information. The proliferation of internet apps and mini-programs, along with the rise of generative artificial intelligence, has diversified methods of personal data collection—ranging from passive provision to active submission and third-party sharing. However, issues such as unauthorized data collection, incomplete data deletion, and excessive permission requests by apps remain prominent. Generative AI further breaks down the fragmentation of information, accelerating data integration and the risk of misuse. The commercial value of personal data drives its widespread use in areas like precision marketing and risk assessment, yet this also increases the risks of privacy breaches and disruption of public order. Although the implementation of China's Personal Information Protection Law marks a new phase in protection efforts, insufficient legal detail and ongoing technological security threats—such as cyberattacks and weak corporate defenses—remain major obstacles. Moving forward, more effective protective measures must be explored through legal refinement and technological advancement.

Keywords

Digital Society, Personal Information Protection, Data Collection Models, Legal Challenges

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. 引言

当前我国互联网的 app、小程序的肆意泛滥，使我们的个人信息大量被收集，常常让我们在不知不觉中把个人信息交付于互联网公司或者其他社会主体。生成式人工智能的出现，更是对个人信息发起新的冲击。数字社会中大数据不仅给我们生产力带来巨大优势，也给我们生活带来很大的便利。目前全球各国都把发展大数据技术作为发展目标，但是也对个人信息保护提出了新的挑战。人们对于个人信息不被侵犯也提出了新的期待。随着经济社会发展，人们生活条件有了显著提高，对于深层次的权利有了更高的要求。另外应用程序等软件的发展，人与人之间的交集越来越多，彼此之间的距离也越来越近，但同时个人空间变得越来越狭窄。人们开始更加渴望能够保留自身的私人空间，而不想让自身的一切信息都被传播媒体和社会大众窥视。

个人信息保护不仅仅是信息主体的个人利益，也包含了公共利益。保护个人信息权，有利于维护社会秩序。在其他社会主体的眼中，个人信息也有商业价值。面对复杂的数字社会，个人信息保护也面临了新的困境。个人信息保护也不能像过去一样一刀切，需要寻找一个新的保护路径。作为互联网大国，我国的个人信息保护近年来也愈发得到重视，2021 年我国通过了《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》)，我们个人信息保护也进入了新的阶段，既饱含期待也存在挑战。

2. 数字社会中个人信息的收集与利用模式

数字社会中个人信息收集主要包括被动提供、主动提供、第三方共享三种模式：第一种是被动提供，主要是指在数字化生活中，个人信息主体在社会生活过程中会留下越来越多的信息痕迹，如社交媒体活动、购物记录、浏览历史等。这些信息往往被网络服务提供者通过技术手段自动收集，用于用户画像、大数据分析等。第二种是主动提供，是指在一些特定场景下，如注册账号、填写问卷、参与调查等，个人信息主体需要主动提供个人信息。这些信息可能包括姓名、身份证号、联系方式等敏感信息。第三种是第三方数据共享。随着数据交易、共享、开放等行为的日益频繁，个人信息可能在不同的个人信息处理

者之间流转。这增加了个人信息泄露或遭非法使用的风险。

数字社会中,大数据能够快速收集与储存个人信息,包含各个来源,例如互联网上的个人资料、传统的数据集,甚至部署在通信网络、电网、全球定位卫星等中的传感器收集的信息,可见,大数据对个人信息收集的规模远远大于传统软件工具对个人信息的收集、储存的速度。同时,大数据通过算法等技术,通过自动分析进行快速、高效、精准的决策。大数据技术进行数据记录或数据整合方面,也会更加深入地挖掘个人偏好、隐私、行为习惯等,这也不可避免地造成大数据对个人信息的过度收集或非法收集。个人信息会被尽可能地保存较长的时间,甚至远远超过最初的使用时间,从而重复使用。此外,大数据技术的应用并未形成明确的行业标准和统一的约束性规则,关于数据的采集、管理、共享、交易等缺乏技术标准予以规范,导致个人信息在被大数据收集的过程中面临着隐私受到侵犯的风险。当前几乎每一个手机应用都会涉及个人信息的权限获取和使用问题。手机应用不仅会搜集个人信息,更有甚者,允许略过阅读协议让用户直接同意搜集个人信息。虽然不同种类不同功能的应用程序可能侧重搜集的个人信息不同,这些个人信息杂乱无章,但最后都会绝对统一,即所有的个人信息最终都可以归属于一个主体。原本分散的个人信息虽然也存在着被泄露的风险,但是在很多情况下泄露的都只是某一类个人信息或者某个特定化场景下的个人信息,所有信息均被同一时间泄露的概率不大[1]。与此不同,在生成式人工智能出现后,分散凌乱的信息被获取,生成式人工智能可以进行快速地精确地分析与组合。生成式人工智能会使得个人信息不再分散,个人信息是否被统一只是选择问题,而享有选择权的主体可以是使用生成式人工智能的任何人。生成式人工智能加剧了个人信息的破坏,这不仅仅是对个人利益的侵犯,也破坏了社会公共秩序。

数据价值不仅在于可以从中分析出更多的个人信息,更重要的是,通过与其他数据源相结合的方式,个人信息的利用率得到极大提升。全面完整的数据不仅可以用来回答或者分析当前具体问题,还能激发新问题的提出,脱离结构化的数据库,在个人信息之间建立关联性,从而挖掘出隐匿的个人信息,甚至是个人隐私[1]。同时,数据收集者能够实现个人信息的预期利用和非预期利用,甚至会将个人信息流转至第三方手中,脱离最初收集的目的进行再利用。而作为接收个人信息的第三方根据自己的需求继续交叉比对、重复使用和加工个人信息,实现个人信息的重复循环再利用。在这一过程中,不可避免地存在着“不知道何种个人信息经过技术处理后会致个体的人格受到侵害”的情形,而这也正是个人信息在大数据时代的本质风险和保护难点。

3. 个人信息概述

(一) 个人信息的概念

关于个人信息的称谓,欧盟成员国多使用个人数据,美国则使用隐私,日本、韩国、俄罗斯使用个人信息。随着《中华人民共和国民法典》(后文简称《民法典》)中个人信息定义的出台,我国已确定使用“个人信息”这一法律概念。个人信息包括以下具体类型的信息:基本信息、生物识别信息、设备信息、账户信息、隐私信息、社会关系信息、行踪轨迹信息、财产状况、网络行为信息与敏感信息等。个人信息也称为个人信息权。第一次较为系统地集中地保护个人信息并彰显出其民事权利的属性的是德国1976年通过的《联邦数据保护法》。欧盟在《通用数据保护条例》(以下简称GDPR)中,“个人数据”是指与一个已识别或者可识别的自然人相关联的任何信息。可识别的自然人指借助姓名、识别号码、位置数据、网上标识符,或借助与该个人生理、心理、基因、精神、经济、文化或社会特征相关的一个或多个因素,可被直接或间接识别出的自然人[2]。

(二) 个人信息权与宪法的基本权利

我国《民法典》对个人信息的定性有点模糊,在《个人信息保护法》中将“个人信息”表述为“权

益”，同时《个人信息保护法》也规定了个人信息的一系列权利，立法上对个人信息的性质陷于模棱两可的定位[3]。尽管个人信息权益具有私法属性，但无法否认个人信息权具有的宪法基本权利属性[4]。《个人信息保护法》明确地指出其立法依据来源于宪法，明确了个人信息权利的基本权利属性，宪法高度的基本权利主要在于调整国家与公民的基本关系，而民法领域的权利则主要调整平等主体的权利义务关系[5]。个人信息不完全是个人的所有物，个人信息的概念当中即表明了作为原子化的“个人”与作为社会交往需要流通的“信息”的复合。个人信息兼具个体属性与公共属性。

因此，个人信息保护需要兼顾个体人格权益保护与信息流通的价值、科技发展的价值，个人信息权益的保障是平衡个人权利与公共利益的结果。因此，个人信息权没有完全绝对的支配权。个人信息具有交互性[6]、社会性、公共性等特点，难以在民法所有权逻辑下成为具有排他性的、由个人支配的权利客体。

4. 目前我国个人信息保护困境

(一) 目前个人信息保护法律存在模糊性

有学者认为，我国关于个人信息保护的法律法规灵活性程度较高，但其模糊性的缺点也无法避免。而模糊性也导致了法律不确定性程度较高[7]。个人信息保护法中的免责事由可能存在一定的模糊性，导致在实际应用中难以准确界定何种情形下可以免责。个人信息范围界定不明确，尽管《个人信息保护法》第四条对个人信息进行了定义，即“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”，但随着技术的不断进步，新型个人信息不断涌现，立法者难以穷尽列举和精确限定个人信息的类型和范围，使得在界定个人信息权利客体时存在一定的模糊性。在处理个人信息时，法律要求遵循合法、正当、必要和诚信原则，但对于某些特定场景下的具体处理方式和范围，可能缺乏明确的界定。另外个人信息保护法作为一部专门法律，某些条款可能与其他相关法律条款(如刑法、民法典等)存在协调问题，导致在实际应用中可能出现冲突或重叠的情况。这些模糊性可能给法律执行和司法裁决带来一定的困难，也增加了企业和个人在遵守法律方面的不确定性。法律条款缺乏具体性，我国已经建立了相对完善的信息主体权利规范体系，但在实际操作中，一些法律条款过于原则性，缺乏具体性和可操作性，导致在个人信息保护方面存在法律漏洞和空白，给不法分子提供了可乘之机。因此，未来在制定或修订相关法律时，有必要进一步明确和细化这些条款的规定。

法律移植确实能有效填补国内法律的空白，但欧美立法模式差异较大，我国在移植借鉴过程中应结合本国国情及社会现实进行扬弃。20世纪70年代，个人信息保护相关立法在美国和欧盟萌芽。欧盟的个人信息保护法律实施时间较早，企业和公众对个人信息保护的意识较高，欧盟的法规将通过非自动方法与自动方法获得的全部与部分个人信息数据都纳入到保护范围之内，做到了无间隙保护。欧盟法律体系详细规定了个人信息主体的多项权利，如知情权、进入权、反对权、不受约束权等，并建立了投诉机制和司法救济途径。

与国外相比，我国在个人信息保护领域，国际间的合作与协调尚不充分。不同国家和地区之间的个人信息保护法律可能存在差异，这可能导致在跨境个人信息传输和处理方面出现法律冲突和合规难题。例如，一些国家可能要求企业在跨境传输个人信息时必须获得用户的明确同意，并在合同中明确相关的安全保障措施，而另一些国家则可能没有这样的要求。这种差异可能导致企业在国际业务中面临合规风险。国家之间可以通过签订国际条约或协定，将个人信息保护法的相关原则和规定纳入其中，从而实现向国外的移植。这种方式需要国家之间的协商和谈判，以确保各方都能接受并遵守相关规定。

《个人信息保护法》在保护个人信息的同时，也可能对信息的自由流动和利用造成一定限制。例如，过于严格的个人信息保护要求可能导致企业在收集、处理和使用个人信息时面临更多的合规障碍和成本

负担,进而影响其业务的正常运营和创新发展。如何在保护个人信息的同时,促进信息的自由流动和利用,是当前个人信息保护法面临的一个重要挑战。

(二) 政府掌握公民个人信息的行为缺少相应监管

进入数字时代后,人们越来越习惯于线上处理各种社会事务,政府为了方便公民以及提高办事效率的需要,政务大多都建立了线上处理模式。电子政务方便了政府工作,也方便了我们日常生活。政府想要实现对公共事务的高效率的管理,就必须对公民的个人信息更加详细地更大规模地收集。公共行政事务日益繁杂,政府需要探寻能够提升自身行政效能的手段,而这些手段的获得需要有充足的信息作为支撑。政府为了更有效地执行政策和提供公共服务,需要对公民信息进行深入分析和了解。这些信息有助于政府识别不同群体的需求,从而制定更加针对性的政策和措施。例如,在资源配置、社会保障等领域,通过数据分析可以更精确地确定资源分配的重点区域和群体,提高公共资源的利用效率。

在实践中,政府逐渐成为现代社会公民信息的最大占有主体。因此,政府突破了其一直扮演的超然中立角色,而成为一个对公民个人信息(包括公民个人隐私信息)有着利益需求的新型社会群体^[8]。政府需要确保所掌握的公民个人信息不被泄露、滥用或遭到黑客攻击等。这需要对信息系统进行持续的安全防护和更新,以保障数据的安全性。有效地管理和保护这些敏感信息是一个挑战。政府需要建立完善的数据库和数据管理制度,确保信息的准确性和完整性,并防止未经授权的访问和使用。政府在处理公民个人信息时需要谨慎权衡个人隐私保护和公共利益之间的关系。在确保必要的信息收集和分析能力以服务于公众的同时,也要尊重和保护公民的隐私权。政府必须严格遵守相关法律法规,确保在收集、使用和处理公民个人信息时合法合规。同时,也需要接受法律的监督和社会的质询,以增强透明度和公信力。总体来说,公民隐私权的公法保护模式要更多限制政府一方的权力行使行为,对政府以公共利益为名而处理公民个人隐私信息的行为进行更严格的审查。

(三) 大数据的可标识性窃取个人信息

为了规范个人信息处理者的处理活动以实现保护个人信息的目的,《个人信息保护法》第51条规定了个人信息处理者的义务,即应建立个人信息管理制度、作业流程,并进行分级分类管理,采取加密、“去标识性”等安全技术措施。但是在数字社会中人工智能发展,人工智能能够利用再识别个人信息,通过对数据库中个人信息的重新汇合,运用统计学与其他数据挖掘技术,将本来不具有识别性或“去标识性”的信息与其他信息进行关联、筛选、比对以及匹配,从而识别出特定个人信息。大数据的可标识性意味着个人的信息可以被轻易地追踪和识别。这增加了个人隐私泄露的风险,一旦数据被不法分子获取,可能会对个人的财产安全构成威胁。由于大数据能够分析出个人的消费习惯、偏好等,一些企业可能会利用这些信息对老客户实行价格歧视,即“大数据杀熟”。这损害了消费者的权益,破坏了市场的公平性。大数据的可标识性可能导致社会透明度过高,个人隐私难以保障。这在一定程度上增加了社会的不稳定性,因为人们可能会因为担心个人信息泄露而减少在网络上的活动,进而影响社会的正常交流和运行。大数据技术的应用使得信息主体即使应用匿名化技术也难以完全实现隐匿的目的,有些信息表面上不是个人信息,但是经过大数据的处理仍然可以追溯到具体的个人,从而挖掘出相关联的其他信息。现代互联网背景下最基础的要求是对数据进行加密处理。但是当前很多数据都是以明文传输和储存在网络系统和大数据系统中,没有任何加密处理或者进行其他保障措施。

5. 个人信息保护进路

(一) 转变个人信息保护模式

在数字社会之前,立法者因公众的需求开始在法律层面将对公民的隐私保护确立为一项绝对的、对世性的防御权利。隐私权此时的防御对象主要是大众传媒和其他公众等私主体,立法者所确立的隐私权

保护模式也表现为对个体隐私权的绝对保护。这种绝对保护,直接导致法律对社会其他个体自由的限制,其中就会涉及个体之间的利益冲突和平衡。随着大数据技术的飞速发展,个人信息的收集、处理和利用变得越来越容易,但同时也给个人信息保护带来了前所未有的挑战。传统的个人信息保护模式难以应对大数据时代的复杂性和多样性。时代的新形势要求国家必须转变个人信息保护模式,并适时作出政策调整。这个阶段最重要的变化之一,是作为新型社会主体的信息业者开始迅速加入对公民个人信息(包括公民个人隐私信息)的挖掘和收集的队伍。这些信息业者通过广泛收集公民个人信息,并充分挖掘其中的商业价值来实现盈利。当人类步入数字时代,信息业者开始大量出现并逐步成为一个合法存在的社会群体,且公民的个人信息成为一种重要的社会资源时,公民对自身隐私信息的利用实际上已经逐渐从社会防御转变为合理的社会运用。随着技术的发展,个人信息的范围和类型在不断变化。立法者需要密切关注这些变化,并及时更新法律条款,确保个人信息的界定清晰、准确。立法者应继续完善个人信息保护相关的法律体系,确保法律条款的明确性和可操作性。例如,通过制定实施细则、司法解释等方式,对《个人信息保护法》中的原则性条款进行具体化和细化。立法者应推动形成跨部门协作机制,加强不同部门之间的信息共享和协作配合,这有助于打破信息孤岛,提高监管效率,确保个人信息保护的全面性和有效性。立法者应鼓励公众积极参与个人信息保护的相关活动,如举报违法行为、参与政策制定等。通过公众的参与和监督,可以推动个人信息保护工作的不断改进和完善。

(二) 对个人信息进行加密、“去标识化”

对于涉及个人信息(尤其是敏感个人信息)的数据应当通过加密和去标识化的方式进行管理。个人信息保护法第51条也要求个人信息处理者必须采取密码技术和去标识化等方式保障个人信息安全。“去标识化”的主要优点在于它能够有效地保护个人隐私。个人信息经过处理,使其在不借助额外信息的情况下无法识别特定自然人的过程。“去标识化”采用假名、加密、哈希函数等技术手段替代对个人信息的标识,但在一定程度上保留了个人信息的颗粒度。这一过程的目的是降低信息对个人的识别程度,使得单个信息不能识别到特定个人。“去标识化”后个人信息可以在一定程度上实现共享与利用,而不会侵犯个人隐私。在医疗、科研、教育等领域,大量的数据需要被收集和分析,以推动相关领域的发展。

然而,如果这些数据包含直接的个人标识符,那么共享和利用这些数据就会面临严重的隐私泄露风险。通过去标识化处理,可以在保护个人隐私的同时,促进数据的共享与利用,推动相关领域的发展。

“去标识化”还可以在在一定程度上增强数据的安全性。即使数据被非法获取,由于已经去除了直接的个人标识符,攻击者难以将泄露的数据与具体的个人联系起来,从而降低了数据被滥用的风险。此外,“去标识化”处理还可以与其他安全措施(如加密、访问控制等)相结合,形成更加完善的数据安全保护体系。随着大数据、人工智能等技术的不断发展,个人信息的保护问题越来越受到公众的关注。通过实施“去标识化”处理,企业、机构等可以展示其对个人隐私保护的重视和承诺,从而提升公众对其的信任度。

(三) 充分落实个人信息的知情同意原则

个人信息的知情同意原则是指信息主体在充分认识其个人信息被获取的渠道、披露的范围、收集的使用目的等后,做出的许可信息处理者收集并使用其个人信息的承诺。信息主体在充分了解这些信息后,有权自主决定是否同意进行信息的收集、使用或共享。“同意”是知情同意原则的核心。知情同意机制是个人信息保护制度的基石,其理论基础在于个人信息自决权[9]。在我国,该原则已成为个人信息保护立法的建构核心,在我国关于个人信息保护法律法规中,都有关于该原则更明确、更具体、更清晰的表述。

不过,知情同意原则在实际应用中面临一些困境:第一,信息处理者提供的隐私政策内容大多繁杂冗长,专业名词晦涩难懂,导致大多数信息主体不愿意认真阅读,往往直接点击“同意”。第二,信息主体难以判断风险:信息主体因技术和个人条件受限,很难根据自身经验及知识判断个人信息被收集后可

能存在的风险,难以评估对其个人合法权益造成的影响。第三,知情同意难以真正实现部分信息处理者为了加大对信息主体个人信息的利用程度,在制定隐私政策时,往往以模糊表述、写在不易被发现的位置等手段扩大收集所需信息的范围及使用目的,使得信息主体难以充分理解隐私政策,知情同意原则无法真正发挥其保障信息主体权益的功能。首先我国应当制定详细的个人信息保护法律实施细则,明确企业在履行告知义务时的具体要求,使个人信息保护治理体系有法可依。企业应当提升责任意识,在收集、使用个人信息时,应完整、主动地告知个人信息收集范围、目的、处理规则等,保障用户的知情权。加强个人信息保护宣传,提升个人对信息收集使用规则的辨别能力。例如,不轻易在 App、网站上留下重要个人信息,学会利用法律武器维护自己的合法权益。确保个人信息的同意是在充分知情的前提下自愿、明确作出的。应当避免含糊其辞或模棱两可的同意方式,保障个人的自主权。政府应加强对个人信息处理活动的监管,对违法行为进行严厉打击,确保知情同意原则得到有效执行。

(四) 个人信息与隐私权的并举

面对个人信息与非个人信息之间的界限越来越模糊一个困境,用隐私权的标准来界分个人信息有积极意义,一方面,我国民法典和个人信息保护法采纳了个人信息与隐私权界分的保护策略,个人信息的本质也是隐私权分离出的权利。另一方面,隐私权从个人本位向社会理论的转变。隐私权能够提供一个有效的红线,即隐私的核心特征在于自然人对于涉及自身内容的非公开性意愿,保护的是自然人的自主决定自由^[10]。隐私权对于保护个人信息具有至关重要的意义,主要体现在以下几个方面:隐私权是体现了对个人自由和尊严的尊重。保护隐私权意味着个人的私人生活安宁以及不愿为他人知晓的私密空间、私密活动和私密信息都受到法律的保护。这种保护确保了个人能够在不受干扰的情况下自由地发展自己的个性和生活,从而维护了个人的自由和尊严。隐私权保护能够防止个人信息被非法获取、出售或向他人提供,从而避免个人信息被滥用。这种滥用可能导致个人生活受到干扰,甚至可能引发更严重的后果,如身份盗窃、欺诈等。

在信息时代,个人信息的安全问题日益突出。隐私权的法律保护能够确保个人信息在收集、存储、使用、加工、传输等各个环节中得到充分的保护,防止信息泄露、毁损或丢失。这有助于营造一个安全、可靠的信息环境,保护个人免受信息泄露带来的风险。当个人的隐私得到充分的尊重和保护时,人们会更加信任彼此,更加愿意进行社会交往和合作。这种信任是社会稳定和发展的基石,有助于构建一个和谐、有序的社会环境。隐私权的保护有助于增强公众对信息社会的信任,促进信息的自由流动和合理利用,从而推动信息社会的健康发展,有助于构建一个尊重和保护个人隐私的社会环境,为个人的自由发展和社会的和谐稳定提供有力的法治保障。

6. 结语

个人信息保护是维护个人隐私权益的基石,也是维护社会秩序和公共安全的必要条件。每个人都有权保护自己的个人信息不被非法获取、滥用或泄露。个人信息包括姓名、身份证号、联系方式、住址等敏感数据,一旦泄露或被滥用,可能导致身份盗窃、欺诈、骚扰等一系列问题,严重影响个人的日常生活和安全。随着数字化时代的到来,个人信息成为了一种重要的社会资源。然而,个人信息的不当使用或泄露可能对社会造成重大威胁,如泄露国家机密、影响社会稳定等。

因此,保护个人信息不仅是个人责任,也是社会共同的责任。个人信息保护还有助于促进数字经济健康发展。在数字经济中,个人信息是企业 and 机构的重要资产之一。然而,如果个人信息保护不力,可能导致消费者对数字服务失去信任,从而阻碍数字经济的进一步发展。因此,加强个人信息保护有助于建立更加安全、可信的数字环境,推动数字经济的繁荣。我国应该要重视科技发展,参与更为公平合理的国际数字规则体系建构。除了制定专门的法律外,国家还不断完善个人信息保护制度,如建立个人信

息保护机构、加强个人信息保护监管等,以确保个人信息的安全和合规使用。另外信息主体也需要驱动,我们要加强保护每个主体所应享有个人信息的权益。

参考文献

- [1] 谢文辉. 个人信息权的权利属性及私法保护[J]. 山西青年职业学院学报, 2020, 33(4): 67-71.
- [2] 江必新, 郑礼华. 互联网、大数据、人工智能与科学立法[J]. 法学杂志, 2018, 39(5): 1-7.
- [3] 潘姚, 敖琪. 健康医疗数据应用中个人信息保护的欧盟实践及启示[J]. 卫生经济研究, 2025, 42(8): 32-36.
- [4] 洪丹娜. 个人信息权利在我国宪法权利体系中的定位[J]. 法学杂志, 2024, 45(3): 87-105.
- [5] 程啸. 论个人信息权益[J]. 华东政法大学学报, 2023, 26(1): 5-21.
- [6] 郑毓枫, 李晟. 我国个人信息法律保护的权利基础研究[J]. 湖北第二师范学院学报, 2018, 35(12): 64-67.
- [7] 王利明, 丁晓东. 论《个人信息保护法》的亮点、特色与适用[J]. 法学家, 2021(6): 1-16+191.
- [8] 陈锦波. 从私法到公法: 数字时代隐私权保护的 mode 延展[J]. 政治与法律, 2023(11): 24-38.
- [9] 周汉华, 主编. 中华人民共和国个人信息保护法(专家建议稿)及立法研究报告[M]. 北京: 法律出版社, 2006.
- [10] 陈怡. 健康医疗数据共享与个人信息保护研究[J]. 情报杂志, 2023, 42(5): 192-199.