Advances in Social Sciences 社会科学前沿, 2024, 13(5), 648-656
Published Online May 2024 in Hans. https://www.hanspub.org/journal/ass
https://doi.org/10.12677/ass.2024.135442

Hans汉斯

网络平台隐私政策的法律规制研究

尹浩宇

阜阳师范大学法学院，安徽 阜阳

收稿日期：2024年4月14日；录用日期：2024年5月17日；发布日期：2024年5月31日

摘　要

随着我国互联网技术迅速发展，在数字中国建设背景下，互联网应用得以大面积普及，虽然便利了日常生活，但是也带来了侵犯用户隐私权、泄露个人信息等负面影响。通过深入探讨网络平台隐私政策的法律规制问题，对隐私政策的制定与实施、用户对相关政策的认知与态度、隐私保护法律规范的发展等突出问题进行研究，提出规制对策，为网络平台隐私政策的长远发展提供理论依据。

关键词

网络平台，个人信息，隐私政策，法律规制

A Study on the Legal Regulation of Privacy Policy of Online Platforms

Haoyu Yin

School of Law, Fuyang Normal University, Fuyang Anhui

Received: Apr. 14th, 2024; accepted: May 17th, 2024; published: May 31st, 2024

Abstract

With the rapid development of China's Internet technology, in the context of digital China construction, Internet applications have been widely popularized. Although it has facilitated daily life, it has also brought negative effects such as infringement of users' privacy and disclosure of personal information. Through in-depth discussion of the legal regulation of privacy policy of online platforms, the formulation and implementation of privacy policies, users' cognition and attitude towards relevant policies, the development of legal norms for privacy protection and other prominent issues are studied, and regulatory countermeasures are proposed to provide a theoretical basis for the long-term development of privacy policies of online platforms.

文章引用: 尹浩宇. 网络平台隐私政策的法律规制研究[J]. 社会科学前沿, 2024, 13(5): 648-656.
DOI: 10.12677/ass.2024.135442

Keywords

Online Platforms, Personal Information, Privacy Policy, Legal Regulation

1. 引言

21 世纪的数字化时代见证了互联网的迅猛发展，这一变革极大地改变了人类的生活方式和社会结构。网络平台作为这一时代的产物，既提供了便捷的信息交换和社交服务，也积累了海量的个人数据。同时，用户在享受这些便利时，也将个人信息(包括身份资料、行为习惯、消费记录等)暴露于网络空间。在缺乏有效监管的情况下，这些信息的积累与应用对个人隐私安全构成了前所未有的挑战。网络平台的隐私政策，作为调控平台收集、使用、处理个人数据的重要法律文件，理论上，这些政策应提供明确、透明的信息处理规则，以保障用户的知情权和选择权。然而，现实并非总是如此。许多网络平台的隐私政策内容晦涩难懂，条款繁复，使得普通用户难以完全理解其具体含义，更不用说基于平等的基础做出同意与否的决定。同时，这些政策常常赋予平台过于宽泛的权限，导致个人数据在未得到充分知情同意下被广泛使用，甚至滥用。此种情况激发了公众对网络平台隐私政策及其法律规制的广泛关注。一方面，个人数据泄露事件的频发增强了公众对个人隐私权保护的意识；另一方面，数据经济时代的到来使得如何合理利用个人数据资源的同时保护个人隐私权成为重大课题。因此，研究网络平台隐私政策的法律规制不仅挑战现有法律框架，也考验社会治理能力。《网络安全法》《个人信息保护法》的陆续出台和实施，使得网络平台隐私政策的法律规制逐渐步入正轨。然而，如何在保障个人隐私权的同时平衡网络平台的合法权益和社会公共利益，仍是一个值得深入探讨的问题。

2. 网络隐私政策的法律规制的时代价值

在信息技术快速发展的背景下，个人数据已成为数字经济的重要资源。然而，在此过程中，个人隐私权的保护问题日益突出，特别是在网络平台上。因此，法律规制作为维护个人隐私权和平衡公共利益的关键手段，其重要性显而易见。个人隐私权，作为基本法律权利，涵盖个体对其个人生活、身体、思想、信仰等方面的自主权。这一权利旨在保护个体免受不正当侵扰，确保其在社会生活中自由、独立地进行个人活动。个人隐私权的基本含义是赋予个体在信息自主权、身体自由权等方面的合法权利。

首先，个人隐私权与信息自主权密切相关。信息时代中，个人信息成为了数字经济的核心资源。个体有权决定自己的个人信息，包括其收集、使用、传播等。隐私权在此过程中保障个体的自主权，使其能更好地掌控自己的信息生态。“当我们的隐私被非法地暴露于公众面前时，我们的自尊也被摧残了，我们与他人之间的关系也受到了损害，这就是法律为什么要保护隐私的原因[1]。”其次，个人隐私权也涉及身体自由权。这意味着个体有权对自己的身体和生理状态作出自主决策，且不应遭受未经许可的侵犯。

在保护个人隐私权的同时，法律和社会必须在个人隐私权与公共利益之间寻找平衡。个人隐私并非绝对、不受限制的权利，而应在某些情况下受限，以维护社会整体利益。例如，在网络侦查中，个人隐私权可能需受限，以确保有效打击犯罪行为。一方面，我国公安信息系统详细记录了违法犯罪人员、常

住人口、暂住人口、出入境人员等数据；网吧、旅馆等施行严格的信息登记管理制度，工作人员能直接查阅公安系统信息，进行网上摸排。另一方面，网购、QQ、外卖等软件记录了个人身份、浏览痕迹、GPS定位、聊天记录等，亦可用于侦查实践。政府的以上举措，当然有助于提高政府的行政效能且实现政府对社会的精准治理，但政府在大量处理公民信息时也存在侵犯公民隐私权的极大嫌疑[2]。在这种情况下，平衡个人隐私权与社会公共安全显得尤为重要。网络隐私政策的法律规制在个人隐私权与公共利益之间建立了一种动态平衡，不仅保障了个人信息的安全和隐私，也为社会公共利益的实现提供了支撑，这种平衡是建设健康、有序的数字社会的必要条件。

3. 网络隐私政策的法律规制目前的问题

3.1. 立法保护缺乏系统性

我国目前没有颁布专门针对网络隐私权的独立法律，法律法规的分散与缺乏统一性。《宪法》间接规定了保护网络隐私权，但未提供具体保护途径，这在信息时代下无法有效保护隐私权；《网络安全法》第 4 章要求保护个人网络信息，但未详细划分信息类型，导致缺乏针对性保护和明确的保护方法；《个人信息保护法》详细规定了个人和私密信息，但现代社会隐私不仅涉及个人信息，还包括生活安宁和私密空间，仅依法律保护隐私权并不全面；虽然《民法典》确立了隐私权保护，但其原则性规定较为模糊，未明确责任追究和救济途径，也缺乏司法解释以增加实践明确性。并且我国互联网相关的法律条款多属于行政法规和行业规范，对网络隐私权保护规定不够明确，如处理措施未详细规定，缺乏可操作性，导致实际无法依据。可见，网络隐私权规定分散，法律间缺乏有效衔接，仅凭现有法律条款保护网络隐私权不足。这种情况下，法律适用复杂且耗费资源，且现有的隐私保护立法往往不能及时反映技术变革，导致目前社会的隐私问题难以得到有效解决，因此颁布独立的网络隐私权法律是迫在眉睫的工作[3]。

3.2. 网络平台隐私政策设定不规范

近年来，随着互联网技术的迅猛发展和普及，个人信息隐私安全问题日益引起关注。通常来说，隐私协议(隐私政策)是网络运营者获得用户授权同意的主要途径，说明隐私协议在本质上属于数据控制者明确告知用户收集、使用或流转用户个人信息的特别约定。但是当前的隐私政策存在剥夺用户选择权、与知情同意原则相冲突以及侵权责任不明确等问题，给用户的信息安全造成隐患[4]；通过对网络隐私政策实际披露情况的研究，也不难发现知情同意原则在网络隐私政策中存在知情原则缺位、同意原则虚化及用户事后权利难以救济等问题[5]。

3.3. 个人信息隐私的伦理问题

随着大数据时代的到来，个人信息面临了更加广泛和深入的收集和使用，伦理问题已经成为人们普遍关心的话题[6]。目前，国内关于大数据时代个人信息隐私的伦理研究主要集中在以下几个方面。

1) 数据采集、处理和使用具有复杂性

随着互联网技术和智能设备的广泛应用，个人信息被无孔不入地收集，且这一过程往往对用户而言是隐蔽的，用户难以察觉自己的信息何时被收集，以及被用于何种目的。大数据分析技术的发展使得不同来源的数据能够被关联和分析，从而推断出用户的个人偏好、行为习惯甚至敏感信息，这种数据处理的复杂性使得传统的隐私保护措施变得不再有效。同时，数据的使用往往是不透明的，算法如何驱动决策过程，数据如何被应用，用户很难得知，这加剧了用户对个人隐私的担忧。此外，数据安全风险也随之增加，数据泄露和黑客攻击事件频发，一旦个人信息被非法获取，将对用户造成严重的隐私和安全风险。技术的快速发展远远超前于伦理讨论和法律规制，导致现有的隐私保护法律和伦理准则难以适应新

情境，处理个人信息时缺乏明确的道德和法律指引。

2) 技术发展与社会伦理的矛盾需要得到平衡

技术的迅速发展，尤其是大数据和人工智能的应用，极大地增强了人类处理信息的能力，为社会进步和日常生活带来极大便利。然而，这些技术也对个人隐私构成潜在威胁，引发诸多社会伦理问题。如个人信息被收集和分析，甚至未经明确同意，用于商业目的。这既侵犯了隐私权，也违背了个体自主和尊严的伦理原则。

4. 网络隐私政策的法律规制的挑战

近年来，滥用 AI 换脸技术侵犯个人信息的行为频繁发生，这些行为包括利用换脸照片或视频编造新闻、炒作、侮辱诽谤、勒索诈骗等。AI 换脸技术，即将视频中的人物面部替换为用户自己的面部，引发了肖像权和隐私权的争议。虽然这种技术在娱乐和创意表达上令人兴奋，但它也可能用于制造虚假信息和侵犯他人隐私。在网络传播下，这些行为产生严重后果，对被侵权人造成长期、持续、难以弥补的伤害。仅用几张照片和简单操作，任何人都可能成为加害者或受害者，这不仅侵犯了个人的人格权、肖像权、名誉权、隐私权，而且对稳定的社会环境和健康的网络空间构成挑战。而这也凸显了目前存在的一系列问题。

4.1. 侵权方式和侵权者身份的具有隐秘性

目前，网络隐私侵权的隐蔽性日益受到社会关注。这种侵权的隐秘性体现在操作的隐蔽性和技术性，以及侵权者身份的难以追踪，个人隐私保护面临巨大挑战。网络隐私侵权行为通常在用户不知情的情况下悄然发生。侵权者可能使用恶意软件、钓鱼网站、数据爬虫等手段秘密搜集和窃取用户个人信息。这类侵权行为的隐蔽性使用户难以立即发现并采取有效防御。

侵权者身份的隐蔽性也是网络隐私保护面临的一个主要问题。在网络世界中，侵权者能轻易隐藏真实身份，通过伪装 IP、使用匿名账号、远程侵入他人网络系统等方式，使得追踪和定位极为困难。并且网络的跨区域属性为侵权行为带来了潜在的便利。互联网的全球化和无界限特性意味着数据可以轻松跨越国界，这使得个人信息和敏感数据的非法获取和滥用变得更加容易。同时，由于涉及多国法律体系，网络侵权行为的追究变得复杂。不同国家的法律规定和执法力度的差异，以及国际间法律合作的不足，都增加了打击网络犯罪的难度。此外，网络提供的相对匿名性加大了侵权行为的隐蔽性，使得侦查和取证更加困难。信息在网络上的快速传播和广泛影响也意味着一旦发生侵权，其负面效应会迅速扩散，给受害者带来巨大伤害。

4.2. 数据利用方式多样化

数据利用方式变得多样化，不仅用于生成视频、照片，也用于交易和贩卖，反映了科技创新和个人信息需求的增长。一方面，社交媒体平台和广告商经常利用用户网络行为数据(如浏览历史、购物习惯)定制个性化内容和广告向其推送。另一方面，零售商和在线服务提供商使用客户购物和浏览数据推荐产品或服务。并且，目前个人隐私数据的交易和贩卖事实上已成为一种盈利模式，公司收集并出售个人数据，用于市场研究、广告定向，也不可避免地用于一些不法活动，这些基于数据驱动的个性化服务在提升用户体验的同时，也为便利性与隐私保护的平衡带来新挑战，从而引发公众对隐私侵权担忧。

4.3. 损害结果多样化

数字化时代，个人信息的滥用和侵犯所引发的损害结果呈现出多样化的趋势，这些损害不局限于某

一领域，而是涵盖了从名誉损害到经济损失、从不公平对待到人身伤害等多个方面。个人隐私信息的泄露或滥用。例如，个人信息的泄露或非法窃取可能导致受害者面临身份盗用、欺诈、名誉受损，甚至人身安全受损。即使暂未直接遭受这些损害，受害者仍可能经历三种影响：首先是情绪困扰，即由信息泄露引起的各种情绪不安。其次，增加的未来伤害风险，由个人信息泄露引发，增加了身份盗窃、欺诈或其他伤害的可能性。最后，为减少未来伤害的风险，受害者不得不投入时间和财力，比如注册信用监控、联系信用报告机构及设置账户的欺诈警报等[7]。同时，随着网络交易和电子商务的普及，敏感财务数据一旦泄露，如银行账户和信用卡信息，不仅会导致直接的财产损失，还可能成为诈骗活动的工具，从而给个人带来经济上的损害。此外，数据驱动的决策过程中，个人信息的不当使用可能导致基于性别、年龄、种族等因素的不公平对待，这种基于数据的歧视正在逐渐成为社会问题。在某些极端情况下，个人信息泄露还可能直接威胁到个人的身体安全，如居住地址和行程信息的泄露可能使个人成为攻击目标。网络欺凌和线上骚扰也可能导致严重的心理健康问题，甚至自我伤害。除了这些直接后果，个人信息侵犯还可能引发一系列间接影响，比如影响个人在网络空间的自由表达和信息获取，导致社会信任度下降，进而影响网络环境的整体健康和安全。

4.4. 损害结果与行为之间的因果关系难以确定

侵权行为的隐蔽性和技术性使得损害结果与行为之间的因果关系难以确定，进而导致受害者难以获得有效的救济。网络隐私侵权行为通常以隐蔽、复杂的方式进行，这使得受害者在追踪和证明侵权行为时面临重重困难。例如，个人敏感信息被非法搜集、交易和使用时，这些行为往往在网络的深层次进行，而受害者往往难以发现自己的信息何时、如何被泄露及被谁使用，并且网络技术的专业性和复杂性使得普通用户缺乏足够的知识和技能去识别和追踪这些隐秘的侵权行为。

此外，证明损害结果与侵权行为之间的因果关系同样充满挑战。网络环境的复杂性使得侵权行为的后果可能具有间接性和长期性，个人信息泄露可能导致隐私被侵犯、财产损失或名誉受损。然而，将这些损害直接归咎于特定的侵权行为往往需要充分的证据支持，但网络上的侵权电子证据具有强流动性，可随时更新和删除，因此取证机会短暂，取证难度较高。

4.5. 公众对网络隐私保护的认识不足、意识不强

我国历史上并无保护隐私权的传统，甚至也没有隐私的概念。直到2001年《最高人民法院关于确定民事侵权精神损害赔偿责任若干问题的解释》才将隐私权作为一项独立的人格利益来进行保护[8]。许多用户对于自己的网络行为和信息安全缺乏必要的警觉性，这不仅增加了他们成为侵权行为受害者的风险，也使得他们在遭受侵权后难以及时有效应对。即便法律有明确规定，受害者在实施时仍面临诸多困难：面对侵权时无法及时反应，加之部分网站数据备份不全或备份周期短，导致证据可能无法获取；受害者可能不知道如何或者未及时公证证据，导致证据证明力下降；以及受害者对法律程序不熟悉等问题。这些原因都可能导致受害者难以有效维护自己的权益。

5. 对策与建议

针对隐私政策在公民个人信息保护领域所暴露出来的种种问题，学者普遍重视对隐私政策规制方式的研究。在宏观层面上有学者提出关于网络隐私保护立法的整体建议：“立法机关在网络隐私权保护立法中应当包括保护个人隐私、保障网络安全、明确隐私政策等原则。”在微观层面上有学者提出完善建议，一方面有从网络平台的告知同意角度，建议应适度放松其形式要求，避免同意要求的不断“升级加码”[9]；建立以分层同意、风险评估为导向的动态知情同意模式，优化个人信息保护的规范体系，采取

行政监管、公司治理与行业自治结合的治理结构[5]；在“告知－同意”的架构下，明确一般同意与特殊同意的关系、引入告知同意原则的例外情形等制度[10]。另一方面，也有学者从用户知情同意的视角，要求以“政府规制为主、行业自律为辅”模式制定隐私协议，而后通过知情方式革新和知情内容扩充提升协议质量，保障用户充分知情；在引入类型化同意模式的基础上，纳入风险评估机制，使得用户全面知悉处理全过程以及相应风险变化继而能自愿作出同意[11]。此外，也有学者从个人信息侵权责任中的因果关系角度，建议对信息本身是敏感的还是非敏感的个人信息而加以判断，进而设置不同的保护要求[12]。这些建议为未来网络隐私权保护立法和实践提供了宝贵的参考。

5.1. 隐私政策内容应完备

《个人信息保护法》要求隐私政策的完备性和公开事项的规定，是基于对个人信息处理的实际情况和风险的考量。平台需向用户明确信息处理者，并让用户了解处理的目标信息、原因和方式。这既是遵循法律上的公开透明原则，也是为了让用户了解个人信息处理的相关主体、对象和方式，确保隐私政策的合法性和合理性。如果平台方的隐私政策制定不完备，存在条款的遗漏或瑕疵，可能增加用户个人信息保护风险。隐私政策内容缺失可能导致平台在处理个人信息时超越用户同意范围，构成侵权。根据《个人信息保护法》第 13 条，除特定例外情形，“取得个人同意”是处理个人信息的合法性基础和前提条件。

实践中，个人信息处理者通常通过“取得个人同意”的方式获得授权。在需要用户同意以处理其个人信息的情形下，平台方通常通过隐私政策等文本充分说明处理规则，让用户通过点击确认或勾选同意等方式主动表示同意。在确保用户选择权的前提下，用户主动勾选确认或同意隐私政策视为其全面理解并认可其内容。

然而，如果告知同意的过程有问题，即使隐私政策再完备也可能违规。用户勾选同意的过程中必须完全保障其选择权，不能默认为同意，即同意必须是用户主动选择的结果。在实践中，应用平台在用户初次使用软件时，不得默认勾选“已阅读隐私政策”。此外，如果用户选择不同意，平台方不能因此拒绝提供服务。即使隐私政策内容与核心功能直接相关，导致不同意时用户无法使用主要功能，平台方应提供浏览模式而非使用户无法使用任何功能。平台在隐私政策中还应明确指出：若用户拒绝提供信息或授权，可能无法使用特定产品或服务，或展示相关信息，但不会影响基础功能的使用。

当个人信息的处理目的、方式或种类发生变更时，需要重新获得用户的同意。随着互联网行业的快速发展，企业需根据行业实务和政策变化持续更新隐私政策，导致个人信息处理规则也随之变更。根据《个人信息保护法》第 14 条的规定，当个人信息的处理目的、处理方式和处理的个人信息种类发生变更时，应重新取得个人同意。由此可以看出，更新的隐私政策相当于补充协议，用户同意之后，即以新条款约束平台与用户之间的关系。

5.2. 明确法律规制对网络平台隐私政策的约束作用

1) 明确网络平台隐私政策的法律效力

隐私政策属于个人信息处理规则，适用个人信息保护的相关法律规范加以调整。《个人信息保护法》第 4 条第 1 款规定，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。平台经营者作为个人信息的处理者，需遵守最小、必要和公开透明原则，而隐私政策作为一种文本形式的“沟通桥梁”，是目前平台与用户达成个人信息处理共识最普遍、最有效的方法。这要求隐私政策不仅合法、合理、透明，还要明确规定网络平台处理个人数据的范围和方式。如此，法律规制确保用户的知情权和选择权得到尊重，有效保护个人隐私权。

2) 确保网络平台操作的合规性

法律规制设定了隐私政策标准内容，如用户数据收集、存储、使用及传输方式，以及建立了相关监管机制——有效监管和审查机制要求网络平台遵循法律，包括定期审查及对违法行为的调查与处罚，即加强隐私政策执行力，设定明确法律责任，如对违规行为罚款、责令暂停或者终止提供服务、停业整顿、吊销相关业务许可或者吊销营业执照等处罚(详见《个人信息保护法》第六十六条)，以提高法律威慑力。网络平台隐私政策的法律规制既是对其操作的约束，也是保护个人隐私权和维护社会公共利益的重要手段。有效的法律规制能确保网络平台快速发展的同时保护用户基本权利，并在合法合理的框架内最大化数据利用和社会价值。

5.3. 明确网络经营者采取的处理措施

《数据安全法》第 27 条将数据处理者应采取的措施分为两类：技术措施和其他必要措施。技术措施指为确保处理活动合法并保护个人信息安全所采取的技术方法或手段。《网络安全法》第 21 条列举的技术措施包括防范计算机病毒、网络攻击、网络侵入等危害，监测和记录网络状态和安全事件，以及数据分类、数据备份和加密等。《个人信息保护法》第 51 条规定的技术措施包括数据加密和去标识化等安全措施。其他必要措施指除技术措施外，为保护数据安全所需的其他措施，包括制定应急预案等。关于数据处理者应采取的技术措施，《数据安全法》第二十七条要求“相应的”措施(详见《数据安全法》第二十七条)与欧盟《通用数据保护条例》的要求相同。“相应的”意味着数据处理者采取的措施与面临的数据安全风险相匹配，即数据处理者需根据数据类型、面临的风险等因素决定采取的技术措施[13]。如消除程序漏洞、修改密码、暂停服务等，防止数据进一步泄露或被非法窃取，避免损害他人权益和国家安全。

5.4. 促进互联网法院发展，完善救济途径

互联网法院的发展和完善是应对数字化时代法律挑战中网络隐私侵权救济的重要措施。目前传统法律体系面临诸多挑战，包括侵权行为的跨境性、技术复杂性及证据获取困难。互联网法院的出现为解决这些问题提供了新途径。互联网法院是创新的司法实践，主要职能是处理互联网相关案件。这种新型法院模式提高了审判效率，也使跨地区案件处理更便捷。以浙江杭州互联网法院为例，其受理案件类型从最初的六类增至十一类，转变为以办公智能为核心的智能化、服务型、全程性网络法院，推动了庭审制度的多元化和规范化[14]。由于传统诉讼模式程序繁琐、时间长和费用高，网络隐私被侵权人可能觉得不值得维权，影响网络环境和谐及社会稳定。互联网法院打破了这一传统，利用算法程序对公民在网络平台上描述的案情进行自动分类，为审理提供便利[15]。互联网法院在线立案、调解、审理和判决，大幅提升了司法效率和透明度，降低了诉讼成本。

互联网法院创建“双线诉讼”庭审模式。相对于“单线诉讼”，“双线诉讼”是指网上的案子在网上审，即线下的案子线上审或者线上的案子线上审[16]，分别突破了空间和时间的束缚，大大提升了庭审效率。并且，互联网法院能集聚懂得网络技术的法官和专家，利用网上审理优势，进行类型化分析和重点研究，探索适用的审判标准，如杭州互联网法院发布的《民事诉讼电子数据证据司法审查细则》，结合《最高人民法院关于互联网法院审理案件若干问题的规定》，为其他法院在相关案件审判时提供了借鉴和参考。

5.5. 提高公众隐私保护意识

个人信息泄露可能导致经济损失、影响名誉，甚至威胁个人安全。因此，增强公众对隐私保护的意识不仅是个人自保的需要，也是维护社会安全的关键。因此普及隐私保护的基础知识在日常生活中至关重要。通过教育使公众认识到保护信息安全即是保护个人安全。美国通过开展公众隐私意识教育活动，

来提高公众对个人隐私的保护意识和知识水平，加强对隐私权的尊重和保护[17]。为了加强教育和培训，学校和相关部门定期举办网络安全教育课程和讲座，向公众普及如何识别钓鱼邮件、恶意软件以及其他网络威胁的知识；也可以通过各大网络平台推广，加强法律法规宣传，让公众了解保护个人隐私的法律权利和途径，有助于提高隐私保护观念。

6. 结语

在深入探讨网络隐私政策的法律规制之后，我们不难发现，在数字化时代，随着信息技术的飞速发展和个人数据的大规模搜集与使用，网络隐私保护已经成为法律规制的重要领域。网络空间中个人隐私的概念得到新的延展和诠释，法律规制不断适应这一变化，旨在构建更安全、公平且透明的网络环境。本研究从网络隐私基本概念出发，深入分析网络隐私保护的必要性及其挑战，如技术发展迅速、跨境数据传输复杂性及公众隐私意识不足。考察不同国家和地区的网络隐私政策后发现，尽管存在差异，普遍趋势是加强个人数据保护、明确数据处理责任和权利及提高违法成本。法律规制在网络隐私保护中发挥关键作用，但同时也面临适应数字时代快速变化的挑战：法律规制不仅需保护个人隐私，也需考虑数据自由流动对创新和经济发展的重要性。因此，制定和实施法律规制需平衡各方利益，同时保护个人隐私和促进数据合理使用。最后，重要的是认识到法律规制只是网络隐私保护的一部分。提高公众对网络隐私的认识、增强自我保护能力、加强隐私保护中的技术应用，以及促进国际合作，也是保障网络隐私的关键环节。通过多管齐下的方式，我们可以保护个人隐私的同时，充分发挥网络技术的积极作用，共同推动构建更安全、健康的数字社会。

基金项目

阜阳师范大学 2023 年大学生创新创业训练项目(项目编号：202310371036)；安徽省社科联创新攻关项目“数字化视角下安徽留守儿童校园欺凌防治对策研究”(项目编号：2023CX529)。

参考文献

[1] 王利明. 生活安宁权: 一种特殊的隐私权[J]. 中州学刊, 2019(7): 46-55.

[2] 陈锦波. 从私法到公法: 数字时代隐私权保护的模式延展[J]. 政治与法律, 2023(11): 24-38. https://doi.org/10.15984/j.cnki.1005-9512.2023.11.004

[3] 晋晓彤. 我国网络隐私权的法律保护研究[D]: [硕士学位论文]. 哈尔滨: 哈尔滨商业大学, 2023.

[4] 李昕孺. APP 隐私政策的缺陷及完善[J]. 湖北经济学院学报(人文社会科学版), 2023, 20(3): 98-101.

[5] 陈科宇. 知情同意原则在网络隐私政策中的适用路径[J]. 黑龙江生态工程职业学院学报, 2023, 36(3): 94-97+130.

[6] 杨雪斐. 大数据时代个人信息隐私的伦理研究[D]: [硕士学位论文]. 兰州: 西北师范大学, 2022. https://doi.org/10.27410/d.cnki.gxbfu.2022.001466

[7] 程啸. 论个人信息权益与隐私权的关系[J]. 当代法学, 2022, 36(4): 59-71.

[8] 徐明. 大数据时代的隐私危机及其侵权法应对[J]. 中国法学, 2017(1): 130-149. https://doi.org/10.14111/j.cnki.zgfx.2017.01.008

[9] 丁晓东. 隐私政策的多维解读: 告知同意性质的反思与制度重构[J]. 现代法学, 2023, 45(1): 34-48.

[10] 张琬悦. 《个人信息保护法》中告知同意原则的问题与完善[J]. 法制博览, 2023(9): 63-65.

[11] 王佳丽. 隐私协议中用户知情同意研究[D]: [硕士学位论文]. 杭州: 浙江工商大学, 2023. https://doi.org/10.27462/d.cnki.ghzhc.2023.000227

[12] 程啸, 李西泠. 论个人信息侵权责任中的因果关系[J]. 郑州大学学报(哲学社会科学版), 2023, 56(1): 19-25+127.

[13] 程啸. 论数据安全保护义务[J]. 比较法研究, 2023(2): 60-73.

[14] 自正法. 互联网法院的运行模式、量化评估及其理性对待[J]. 政法论丛, 2022(3): 65-75.

[15] 孙梦龙. 互联网法院的价值功能与建构路径[J]. 大连海事大学学报(社会科学版), 2022, 21(4): 67-78.

[16] 樊鸳. 网络空间个人信息权益的法律保护[J]. 网络空间安全, 2023, 14(1): 1-5+15.

[17] 苏君华, 杜念. 美国公共数据开放中的隐私风险控制经验及启示[J/OL]. 图书情报工作: 1-19. http://kns.cnki.net/kcms/detail/11.1541.G2.20240104.1658.004.html, 2024-01-23.