Advances in Social Sciences 社会科学前沿, 2026, 15(4), 448-455
Published Online April 2026 in Hans. https://www.hanspub.org/journal/ass
https://doi.org/10.12677/ass.2026.154328

Hans汉斯

大数据时代公民隐私权法律保护研究

王若彤

大连海洋大学海洋法律与人文学院，辽宁 大连

收稿日期：2026年3月9日；录用日期：2026年4月17日；发布日期：2026年4月28日

摘　要

文章聚焦于大数据时代公民隐私权的法律保护，具有重要的现实意义。在大数据发展带来数据价值挖掘与公民隐私权保护的冲突，我国现行法律体系针对个人隐私权保护存在不足之处。国内外对隐私权的研究取得了进展，但存在差异，国内需完善相关法律法规。文章详细阐述了大数据、隐私权的概念特征，以及大数据时代隐私权的变化和侵犯隐私权的主要类型。通过对域外美国、日本的保护现状考察，得到对我国的启示，包括完善立法、提高企业自律和带动公民自我隐私保护意识等。同时，指出我国在该领域存在侵权责任主体难确定、网络服务提供者义务履行不到位等问题，并提出强化网络服务提供者的责任、明确告知义务、细化判定标准等对策建议，以加强公民隐私权保护，推动相关法律体系完善和网络空间有序发展。

关键词

大数据时代，隐私权，侵权行为

A Study on Legal Protection of Citizens' Right to Privacy in the Big Data Era

Ruotong Wang

School of Marine Law and Humanities, Dalian Ocean University, Dalian Liaoning

Received: March 9, 2026; accepted: April 17, 2026; published: April 28, 2026

Abstract

This article focuses on the legal protection of citizens' privacy rights in the era of big data and holds significant practical importance. As the development of big data creates a conflict between data value extraction and the protection of citizens' privacy rights, China's current legal system has shortcomings regarding the protection of individual privacy rights. While research on privacy rights has made progress both domestically and internationally, differences remain, and China needs to improve its

文章引用: 王若彤. 大数据时代公民隐私权法律保护研究[J]. 社会科学前沿, 2026, 15(4): 448-455.
DOI: 10.12677/ass.2026.154328

relevant laws and regulations. The article elaborates in detail on the concepts and characteristics of big data and privacy rights, as well as the changes in privacy rights in the era of big data and the main types of privacy infringements. By examining the current state of privacy protection in the United States and Japan, the article draws insights for China, including improving legislation, enhancing corporate self-regulation, and fostering citizens' awareness of self-privacy protection. At the same time, it identifies issues in China's legal framework, such as the difficulty in determining liable parties for infringements and the inadequate fulfillment of obligations by internet service providers. The article proposes countermeasures, including strengthening the responsibilities of internet service providers, clarifying disclosure obligations, and refining determination criteria, to enhance the protection of citizens' privacy rights, promote the improvement of the relevant legal system, and foster the orderly development of cyberspace.

Keywords

The Big Data Era, Privacy Rights, Infringement

1. 引言

我国隐私权领域的理论研究与法律保护实践起步相对较晚。追溯至 20 世纪 90 年代，张新宝教授刊发《隐私权研究》一文，率先明确隐私权归属于民事权利范畴，具备人格权的共性特征，这一学术成果也成为我国学界针对隐私权问题展开系统性专项研究的重要开端[1]。伴随网络信息技术的持续迭代，尤其是大数据战略全面推进的时代背景下，国内学界对网络隐私权的研究维度不断拓展、理论深度逐步深化。王利明教授在《人格权法新论》中明确指出，隐私权是一种在特定领域的排他权利，包括不为他人知悉、禁止他人干涉等，是一种基本的人格权。对于大数据时代隐私权的研究，学者们认为其具有明显的时代特征，是每个自然人在互联网上拥有的、与公共利益无关的、不被他人非法知悉、收集、侵扰、利用和公开的权利[2]。

从法律规范体系的构建层面审视，我国宪法虽未以直接条文的形式对个人隐私保护予以单列阐明，但经由其他具体条款实质上形成了对公民隐私权的保护。2021 年 1 月 1 日正式实施的《中华人民共和国民法典》对隐私进行了明确的界定，将隐私权纳入人格权编，明确了隐私权的法律地位[3]。此外，《民法典》还对个人信息进行了定义，进一步明确了个人信息的保护范围。然而，面对大数据时代背景下的隐私权保护问题，《中华人民共和国个人信息保护法》清晰划定了公民个人信息受法律保障的范畴，构建起多层次、全方位的个人信息保护机制，同时对国家机关收集、使用个人信息的行为予以严格规范，进一步健全了隐私权益遭受侵害时的法律救济渠道。然而，个人信息与隐私权在内涵上既存在包含关系，又具有相互交叉的特征，二者并非简单等同关系。在数字社会背景下，隐私权的保护对象还延伸至经由数据技术加工、分析、处理后的各类信息形态，其外延更为宽泛，因此当前我国虽已出台诸多涉及隐私权保护的法律法规，但仍存在规范分布零散、针对性不足、体系化程度不高等问题，这就导致在内容层面难以形成统一协调的隐私权保护制度体系，因而需要进一步完善。

西方发达国家对隐私权保护的研究开始较早。1890 年，美国哈佛大学法学院教授路易斯·D·布兰代斯与塞缪尔·D·沃伦在《隐私权》一文中首次提出个人隐私权的概念，认为隐私权是一项独特的权利，保障每一位公民的私人生活不受侵犯[4]。此后，隐私权逐渐受到广泛关注，并形成了研究隐私权的思潮。

大数据时代隐私权的保护是在互联网信息技术的推动下产生的，特伦斯·克雷格和玛丽·E·卢德洛夫在《大数据与隐私》一书中，通过实证研究阐述了隐私权争论从互联网时代到大数据时代的演变过程。美国则主张以行业自律的模式来保护公民的隐私权，同时辅以立法对某些特殊领域的隐私权进行保护。美国政府以“信息隐私权”为核心，建立了隐私权理论并颁布了多部法律对隐私权保护进行限制。2020 年 11 月 3 日，加州选民投票通过了《2020 年加州隐私权法》(CPRA)，该法案为消费者创造了新的数据隐私权，并要求企业和服务提供者遵守其综合性隐私框架，对企业和服务提供者施加了新的义务和责任[5]。

2. 大数据及隐私权的相关概述和主要涉及的侵权类型

2.1. 大数据的概念及大数据时代下隐私权的变化

2.1.1. 大数据的概念

大数据是在互联网技术发展背景下产生的具有复杂性、规模性、高速性、多样性和价值性等特征的数据集，它并非单纯指超过特定 TB 值的数据量，而是与普通数据库不同，具备获取、存储、管理和分析能力的数据集合[6]。如麦肯锡公司所认为的，它有着自身独特的数据处理方式，Mayer-Schnberger 在其著作《大数据时代》中阐述的大数据 4V 特性，即规模性、高速性、多样性和价值性，进一步明确了大数据的特点[7]。我国国务院在《促进大数据发展行动纲要》中定义大数据为储存大量个人信息、存取速度快、类型丰富且经济价值高的数据沉积，综合来看，大数据就像石油矿藏、钻石矿藏一样，蕴含着巨大潜力，能为企业和社会带来巨大的财富和价值，其核心在于能够快速、高效地分析和整合各种不同类型的数据，从而获取有价值的信息。

2.1.2. 大数据时代下隐私权的变化

隐私权是指自然人对其私人生活安宁和私人信息安全所享有的权利，其核心在于保护个人的私密信息不被非法探知、储存、分析、利用和公开。在大数据时代，隐私权的内涵发生了显著变化。首先，隐私权的财产属性增强，个人隐私数据被企业通过分析和利用，能够带来巨大的经济价值，使得隐私权从单纯的人格权转变为具有财产权特征的复合权利[8]。其次，隐私权的客体范围不断扩大，除了传统的个人信息如姓名、身份证号等，社交发言、聊天记录、消费记录、地理位置等网络数据也成为隐私权保护的客体。此外，大数据时代下，隐私权的保护难度增加，侵权行为更加隐蔽和复杂，个人隐私信息更容易被非法收集、分析和利用，导致隐私权的保护面临更大的挑战。

2.2. 大数据时代下侵犯隐私权的主要类型

2.2.1. 电子监控侵权

在大数据时代，随着监控技术的普及和监控系统的广泛应用，在公共场所、住宅小区、甚至私人空间中，通过摄像头等设备对个人进行不间断的监视和记录，这些监控设备收集的大量个人数据被长时间储存，并且可能被用于人脸识别、行为分析等目的。数据的收集和使用往往未经个人同意，甚至在个人不知情的情况下进行，监控数据的泄露风险也极高，一旦被不当使用或非法传播，将对个人的隐私造成更大的损害。

2.2.2. 非法买卖、利用个人隐私数据

在大数据时代，个人数据的价值挖掘吸引了众多参与者，非法收集、存储、买卖、利用个人隐私数据的行为已经形成了非法经济网络。其中，手机作为移动智能终端的典型代表，随着社交媒体和自媒体的发展，已经成为人们日常生活中必不可少的沟通交流工具[9]。非法收集、存储、买卖、利用个人隐私数据导致的隐私泄露事件，已成为大数据时代隐私安全面临的常态化风险。

2.2.3. 人肉搜索

人肉搜索通常涉及多个主体，包括个人、网络平台和网络服务提供商等，这些主体在未经当事人同意的情况下，通过网络收集、整合和公开个人的私人信息。由于人肉搜索的复杂性和隐蔽性，受害者往往难以及时发现和取证，即使发现，也难以确定侵权主体和具体责任，这使得维权变得困难。

3. 大数据时代下公民隐私权法律保护的域外考察

3.1. 美国大数据时代公民隐私权保护现状

在美国，隐私权被视为一种涵盖广泛人格利益的一般人格权，不仅包括私生活秘密和空间的保护，还涉及肖像、姓名等具体人格权。美国对隐私权的保护通过分散式立法和行业自律相结合的方式实现，源于其法律对个人自由价值的关注及对政府入侵私人领域的严格限制。在公共领域，美国针对不同社会群体的特定隐私利益采取了不同的立法保护措施，尤其是在大数据时代，政府通过一系列法律如《联邦电子通讯隐私法》《消费者隐私权法案》《儿童网上隐私保护法》和《健康保险移转与责任法》等，保护个人数据，包括儿童信息、医疗档案和金融数据。各州也有自己的隐私规范，如加利福尼亚州就有 25 部以上的隐私和数据安全法[10]。然而，联邦法律与部门法律、各州法律之间的区别和利益冲突，增加了司法和执法的难度[11]。

在非公共领域，美国采用行业自律模式，通过市场经济保持与商界及消费者团体的对话，引导和鼓励个人隐私保护。一些公司会鼓励用户上传个人数据进行交易，但在交易前会对数据进行匿名化处理。此外，美国联邦最高法院在凯茨案中提出了“合理隐私期待”原则，认为即使在公共场所，个人也有权期待隐私保护，这取决于个人的主观期待和社会的普遍观念。在信息共享中，除了征得个人同意外，还需考虑是否符合“合理预期”，特别是对于敏感个人信息，其保护范围更严格。此外值得一提的是美国加州《消费者隐私法》，针对个人隐私权规定了知情权、访问权和删除权。而后美国联邦贸易委员会于 2012 年 3 月颁布了《迅速变化时代消费主体的隐私保障：针对政策制定方与企业的建议》，“其中就给予消费主体向企业提出删除其不再需要的数据的权利，提出赋予消费者有限的数字遗忘权。”[12]该法案被称为“橡皮擦法案”，也被视为首部信息保护和确认被遗忘权的正式立法文件。确立“数据透明 + 选择退出”模式，要求企业公开个人信息收集、使用、共享的具体目的与范围，赋予用户访问、删除、限制处理的权利，进一步丰富全球告知同意的制度实践。

3.2. 日本大数据时代公民隐私权保护现状

日本在大数据时代对公民隐私权的保护采取了综合立法模式，主要通过全国性立法和部门或地方立法来进行规制。虽然日本宪法中没有对隐私权的明文规定，但宪法规定的公民追求幸福的权利成为隐私权保护的渊源。隐私权在日本民法上并非独立的民事权利，因此在侵权后的民法保护有限。然而，自“盛宴之后”案以来，隐私权开始得到宪法上的承认与保护，相关司法实务案例如京都府学联事件、律师前科照会事件等也推动了隐私权的发展。全球立法扩散：形成“告知－同意”的国际共识。

日本也出台了相关的数据保护法，均以“告知－同意”为基础规则，主要的法律文件包括 1988 年的《行政机关个人信息保护法》、1999 年的《信息公开法》，以及 2005 年的《个人信息保护法》作为基本法，对公共领域和非公共领域的个人信息处理都作出了规范。这些法律文件共同构成了日本在大数据时代对公民隐私权的保护框架，旨在适应信息化社会的发展，保护个人对其信息的控制权。

3.3. 域外公民隐私权法律保护对我国的启示

域外国家在大数据时代对公民隐私权的法律保护模式各具特色，对我国有以下启示：美国的分散式

立法和行业自律模式强调个人自由价值，通过不同法律保护不同社会群体的隐私利益，同时采用“合理隐私期待”原则，这提示我国在保护隐私权时应充分考虑个人的主观期待和社会普遍观念；日本的综合立法模式虽未在宪法中明文规定隐私权，但通过司法实践推动隐私权的发展，制定了一系列法律文件保护个人信息，这启示我国在立法过程中应注重宪法与民法的结合，通过司法实践进一步明确和细化隐私权的保护，同时根据不同领域和行业特点制定相应的隐私保护法规，以适应信息化社会的发展需求。

我国在借鉴这些模式时，应结合我国具体司法实际情况，探索出一套适合我国的隐私权保护模式。具体来说，我国应加强立法的完善，明确隐私权的定义和范围，制定统一的隐私保护法律，加强对企业和政府机构的监管，确保隐私权保护措施的有效实施。例如我国可以考虑确立经过各国立法确认和司法实践的已经日趋成熟的被遗忘权，并对此进行具体的制度建构设计。此外，还应鼓励企业进行自我监管，通过行业自律和技术创新，提高隐私保护水平。在司法实践中，应进一步明确隐私权的保护标准，加强对隐私侵权行为的惩处力度，带动公民的隐私自我保护意识，促进全社会共同参与隐私权保护。

4. 我国大数据时代下公民隐私权保护存在的问题

4.1. 侵权责任主体难以确定

在我国大数据时代下，公民隐私权保护面临的侵权主体难以确定问题主要表现在以下几个方面：一是网络活动的匿名性使得行为人可以隐藏身份进行侵权行为，如通过冒名或虚假登记实施侵权，导致被侵权人难以确定侵权者身份；二是数据的复杂性和多元性，数据收集与整合过程复杂，网络服务提供者之间存在大量数据共享行为，权利人难以确定哪些主体在收集和使用自己的隐私信息；三是技术手段的隐蔽性，行为人通过网络漏洞攻击、劫持服务器等技术手段非法获取隐私信息，侵权行为更加隐蔽，权利人难以察觉和确定侵权主体；四是法律规定不完善，“知道”与“应当知道”判定标准不清，网络服务提供者责任范围不明确，导致权利人在追究侵权责任时面临障碍；五是数据交易平台与地下产业链的隐蔽性和复杂性，非法数据交易平台和地下产业链通过匿名交易方式，使得权利人难以追踪和确定侵权主体；六是跨境数据流动的监管难题和法律适用问题，增加了侵权主体确定的复杂性。这些因素共同导致了在大数据时代下，公民隐私权保护中侵权主体难以确定的问题愈发突出。

4.2. 网络服务提供者未能充分履行应尽的审慎义务

在我国大数据时代下，公民隐私权保护存在的网络服务提供者未尽合理注意义务的问题主要体现在：网络服务提供者在数据收集环节过度收集用户信息，如要求用户提供与服务无关的个人家庭住址、身份证号等，并且未明确告知用户信息的具体用途和使用范围，导致用户对自己的信息被如何使用毫不知情[13]；在数据存储和管理环节，数据安全保障措施不足，如数据库存在安全漏洞，数据管理混乱，如数据存储、传输、共享等环节缺乏规范，导致用户数据被随意使用或泄露；在数据使用和共享环节，未经用户同意使用和共享数据，如将用户数据出售给广告公司用于精准广告投放，数据共享范围过大，如将用户数据共享给多个合作伙伴，增加了隐私泄露的风险，例如在最高法发布的典型网络服务提供者过度收集消费者个人信息案例——马某与某公司个人信息保护纠纷案中，该公司默认勾选“一揽子同意”，剥夺自主选择权。在安装 App 并首次打开时，隐私政策与用户协议默认勾选“我已阅读并同意”，无主动勾选入口；用户无法单独拒绝某一项授权，只能“全接受或全拒绝”。该 App 核心功能为词汇查询，依据《常见类型移动互联网应用程序必要个人信息范围规定》，无需收集手机号即可使用基本功能。但运营方强制要求用户提供手机号码，否则无法进入查词界面，属于超范围、非必要收集；此外，网络服务提供者用户隐私保护意识和责任意识淡薄，如未充分认识到用户隐私保护的重要性，发生隐私侵权事件时推卸责任；同时，法律监管和行业自律机制不完善，如隐私保护法律法规不够完善，网络服务行业缺

乏有效的自律机制，导致用户隐私权得不到有效保护。

4.3. 网络服务提供者“知道”与“应当知道”判定标准模糊

在我国大数据时代下，公民隐私权保护存在的网络服务提供者“知道”与“应当知道”判定标准不清的问题主要体现在：法律规定方面，《民法典》第1197条虽增加了“应当知道”的表述，但未明确“知道”与“应当知道”的具体含义及判定标准，导致实践中法官理解和适用存在差异；司法实践中，“通知－删除”规则和“红旗原则”存在局限性和适用不统一的问题，如部分法院对“明知”与“应知”认定不清，导致同案不同判的现象时有发生[14]；网络服务提供者的责任认定上，由于判定标准不清，其主观过错难以准确判断，责任范围也难以准确确定，例如在数据共享和第三方合作的情况下，网络服务提供者常以不知晓第三方侵权行为为由主张不承担责任；对权利人保护方面，由于判定标准不清，权利人在追究网络服务提供者责任时面临举证困难，责任追究不力，影响了对权利人的有效保护；此外，法律监管和行业自律机制的不足，如隐私保护法律法规不完善，网络服务行业缺乏有效的自律机制，也导致“知道”与“应当知道”的判定标准不清，影响了对公民隐私权的保护。

4.4. 过错责任原则具有局限性

在我国大数据时代下，公民隐私权保护适用的过错责任原则存在明显局限性，一方面，该原则要求以网络服务提供者主观过错为承担责任的前提，但大数据隐私侵权行为技术性强、手段隐蔽，导致过错认定困难，例如网络服务提供者常以技术中立为由抗辩，声称无法预知用户利用其服务实施侵权行为，使得权利人难以证明其存在主观过错；另一方面，过错责任原则下奉行“谁主张、谁举证”，而权利人多为普通民众，缺乏专业技术与资源，面对复杂的网络技术和海量数据，难以收集有效证据证明网络服务提供者的过错，如数据泄露事件中，权利人难以确定是因网络服务提供者的安全漏洞还是用户自身操作失误导致，这无疑加重了权利人的举证负担，导致其在维护自身隐私权时面临困境，同时，过错责任原则更多地保护了网络服务提供者的利益，容易造成网络服务提供者与权利人之间的利益失衡，不利于对权利人隐私权的充分保护。

5. 我国大数据时代下公民隐私权保护的对策建议

5.1. 化网络服务提供者的责任

在网络隐私侵权责任主体认定问题上，国家需强化个人数据保护技术投入。一方面提升加密技术水平，全方位防护数据传输与存储环节的用户隐私，规避不法分子截取、滥用数据的行为；另一方面加大安全审计与监控技术研发，通过记录分析数据访问行为，为侵权发生后追踪识别责任人提供支撑。同时，借助流量与威胁监测技术捕捉网络异常，方便相关主体及时处置，减少恶意侵权行为。

当前我国网络侵权立法采用“网络服务提供者中心主义”模式，需在立法中明确优势地位网络服务提供者的隐私保护义务，强化其自我监管与侵权惩罚力度，要求其在用户隐私受侵害时提供维权协助并承担举证责任。此外，依据网络接入服务提供者、网络内容提供商等不同角色，清晰划分各主体责任义务，避免多重主体推诿、串通规避责任的现象。

5.2. 明确告知用户信息用途和使用范围

为应对大数据时代下网络服务提供者未尽合理注意义务的问题，首先，强化告知义务的执行，网络服务提供者应在收集用户信息前，通过隐私政策或用户协议等明确告知用户信息的具体用途、使用范围、存储期限以及可能的共享对象等关键信息，确保用户充分了解其个人信息将被如何处理。其次，优化告

知内容的呈现方式，告知信息应使用通俗易懂的语言，避免专业术语和模糊描述，同时通过弹窗、页面提示等方式突出显示关键信息，确保用户能够清晰地理解和接收。再次，实施告知内容的适时更新，当个人信息的处理目的、方式或范围发生变化时，网络服务提供者应及时通过弹窗或邮件等方式通知用户，并重新获取用户的同意[15]。此外，加强告知义务的监管和处罚，监管部门应定期检查网络服务提供者的隐私政策和用户协议，对未充分履行告知义务的行为进行严厉处罚，以确保网络服务提供者切实履行其告知义务。通过这些具体措施，可以有效提升网络服务提供者在个人信息处理过程中的透明度和规范性，增强用户对个人信息处理的知情权和控制权，从而更好地保护公民的隐私权。

5.3. 明确网络服务提供者“知道”与“应当知道”的判定标准

为解决网络服务提供者“知道”与“应当知道”判定标准模糊的问题，建议从明确判定标准这一关键点入手[16]：首先，细化法律规定，在《民法典》第 1197 条的基础上，进一步明确“知道”与“应当知道”的具体含义，例如，规定网络服务提供者在接到侵权通知后未采取必要措施的，视为“知道”；对于明显存在侵权风险的行为，网络服务提供者应当采取合理措施进行预防和监控，否则视为“应当知道”。其次，制定司法解释或指导性案例，通过最高人民法院发布指导性案例，对“通知－删除”规则和“红旗原则”的适用标准进行具体说明，减少同案不同判的现象。例如，可以明确网络服务提供者在接到侵权通知后，应在合理时间内采取删除、屏蔽、断开链接等必要措施，否则将被视为“知道”侵权行为的存在。此外，对于“应当知道”的判定，可以结合网络服务提供者的业务性质、技术能力、管理能力等因素，综合判断其是否应当知道侵权行为的存在。通过这些具体措施，可以有效解决网络服务提供者“知道”与“应当知道”判定标准模糊的问题，加强公民隐私权的保护。

5.4. 创设过错责任原则与过错推定责任原则的复合归责机制

为应对大数据时代下公民隐私权保护适用的过错责任原则的局限性，建议创设过错责任原则与过错推定责任原则的复合归责机制。在网络服务提供者主观过错明晰(如未落实安全措施致数据泄露、明知侵权仍放任)，权利人可直接举证，则适用一般过错责任。过错难以直接证明的高风险场景，实行举证责任倒置，由平台自证无过错免责。过错推定法定情形可以限定于大数据隐私高风险场景，例如：处理敏感个人信息、生物识别信息；运用自动化决策、用户画像侵害隐私；数据共享、第三方合作引发隐私侵权；大规模数据泄露与隐私数据非法交易；未履行隐私保护合规义务且过错难以查实。当网络服务提供者未采取必要措施防止数据泄露时，可直接认定其存在过错；而对于复杂的隐私侵权案件，如数据共享和第三方合作中的侵权行为，若权利人难以证明网络服务提供者的过错，则可适用过错推定责任原则，由网络服务提供者举证证明其无过错。此外《个人信息保护法》第 69 条过错推定为规范基础，将复合机制纳入该条适用解释，保持立法统一。一般隐私侵权仍适用过错责任，与民法典隐私权保护规则衔接；高风险场景优先适用推定，覆盖第 69 条未明确的隐私侵害类型。明确已履行“告知－同意”、落实等保与数据安全义务、已尽合理审查与补救义务的免责事由，可推翻过错推定。通过这种复合归责机制，可为数据隐私侵权的司法适用提供清晰路径，有效减轻权利人的举证负担，加强对网络服务提供者的责任约束，从而更好地保护公民的隐私权。

6. 结论

本文通过深入探讨大数据时代下我国公民隐私权保护面临的诸多问题，包括侵权责任主体难以确定、网络服务提供者未尽合理注意义务、“知道”与“应当知道”判定标准模糊、过错责任原则的局限性等，结合域外国家在隐私权保护方面的先进经验，提出了一系列具有针对性的对策建议。强化网络服务提供者的责任有助于归责侵权主体，强化告知义务的执行能够提升网络服务提供者的透明度和规范性，明确

“知道”与“应当知道”的判定标准能够有效解决司法实践中的困境，创设复合归责机制能够更好地平衡网络服务提供者与权利人之间的利益，而加强权利人对自身隐私信息的控制力则能够从根本上提升公民的隐私保护水平。这些对策建议旨在为我国大数据时代下公民隐私权的法律保护提供有益的参考，推动我国隐私权保护法律体系的完善，促进网络空间的有序发展，保障公民的隐私权益。

参考文献

[1] 姚辉. 创建中国的人格权法理论——简评王利明教授主编的《人格权法新论》[J]. 中国法学, 1995(2): 117-118.

[2] 潘晓玲. 大数据时代公民隐私权的法律保护[J]. 法制与社会, 2021(14): 105-106.

[3] 潘星容, 黄紫妍. 论大数据背景下隐私权的法律保护[J]. 行政与法, 2020(8): 92-102.

[4] 张卓. 大数据侦查中的隐私权保护[J]. 网络安全技术与应用, 2022(5): 147-149.

[5] 刘莹莹, 史江峰. 大数据领域国内外立法及中国国家标准推进情况综述[J]. 专利代理, 2022(2): 83-87.

[6] 刘浩. 网络“爬虫”行为刑事规制的困境与转向——以实证案例分析为视角[J]. 西安电子科技大学学报(社会科学版), 2022, 32(2): 52-65.

[7] 冯莉. 大数据时代背景下行政法教学改革探讨[J]. 创新创业理论研究与实践, 2020, 3(13): 40-42.

[8] 郑艳艳, 程文佳, 文成伟. 隐私权在网络环境下之嬗变[J]. 文化学刊, 2013(1): 90-96.

[9] 顾秋丽, 徐纪周. 大数据思维的高校学生思想政治教育工作研究[J]. 学理论, 2015(14): 248-249.

[10] 彭宁波. 国内数据隐私保护研究综述[J]. 图书馆, 2021(11): 69-75.

[11] 王敏, 江作苏. 大数据时代中美保护个人隐私的对比研究——基于双方隐私保护最新法规的比较分析[J]. 新闻界, 2016(15): 55-61.

[12] 高俊. 差异与比较: 欧盟法与美国法视野中的被遗忘权[J]. 四川文理学院学报, 2016, 26(4): 24-30.

[13] 周宣辰. 自媒体著作权问题与对策研究——以微信公众号为例[J]. 淮阴工学院学报, 2018, 27(4): 32-35.

[14] 夏向荣, 张春玲. 共同饮酒人不作为侵权研究[J]. 淮海工学院学报(人文社会科学版), 2017, 15(8): 28-30.

[15] 向秦. 三重授权原则在个人信息处理中的限制适用[J]. 法商研究, 2022, 39(5): 133-145.

[16] 程一帆. 自媒体传播中“避风港”规则的适用——以“知乎”网友作品被侵权为例[J]. 青年记者, 2015(9): 62-63.