# 迈向网络强国的网络信息内容法律治理：框架、策略与体系

赵丽莉
(山东科技大学 数字法治研究院，山东 青岛 266590)

**摘　要**：网络强国战略的实施，亟需坚实的网络安全保障作为支撑。伴随人工智能、大数据等新技术的发展和应用，网络信息内容爆炸式增长，隐私和个人信息泄露、违法虚假信息传播、网络暴力、网络恐怖主义等网络信息内容安全风险日益突出，危害隐私和信息安全、危及国家安全和社会稳定，已有法律治理规则的适用性面临新的挑战。为此，应着眼国家治理现代化对网络信息内容安全治理提出的新诉求，秉持法律治理动态平衡理念，立足网络信息内容安全法律治理多维生态，深化多方参与的综合治网格局；推进“体制之维”与“过程之维”多元协调；维系内容产业发展与安全遵从的结构平衡；促进法律治理与技术治理手段融合。

**关键词**：网络信息内容；法律治理；动态平衡；融合；多元协同

**中图分类号**：D922.16　　**文献标识码**：A　　**文章编号**：1008-7699(2025)04-0104-09

党的二十大报告中提出“加快建设网络强国”，党的二十届三中全会审议通过的《中共中央关于进一步全面深化改革、推进中国式现代化的决定》对“健全网络综合治理体系”作出系统部署，其中专门提出“加强网络空间法治建设”。网络空间构成人们生存和发展的“第五疆域”，网络成为人们获取各种信息的重要空间和主要途径。然而，具有互动性、即时性、多元性及传播成本费用低等特性的网络信息传播活动，也不断冲击网络信息内容的有效管控。网络空间成为各类违法有害、不良信息的温床，网络虚假信息、网络暴力、网络犯罪、恐怖主义等网络违法活动滋生，公共安全和利益受到不同程度的威胁。近年来，随着生成式人工智能技术的迅猛发展，网络信息内容治理面临着前所未有的机遇和挑战。为实现网络信息内容安全治理现代化，厘清法律治理在该领域中的角色与定位、探索如何通过完善治理机制保障网络信息安全以及构建多维度治理体系等，构成了亟待研究的核心命题。

## 一、网络信息内容安全治理的内涵与变革

### (一)网络信息内容安全治理的内涵

“治理”一词源于古法语，指的是治理的艺术与实施，现代含义指通过包括政府在内的多元主体的合作、互动，在协调不同利益的情况下实现公共管理的目的，涵盖包括网络治理的 7 个内容，即“公司治理、新公共管理、善治、国际间的相互依赖、社会控制论的治理、作为新政治经济学的治理、网络治理。”[1] 网络信息内容安全治理属于网络治理的下位概念。

网络信息内容安全治理作为总体国家安全观下网络安全治理的重要内容，承载着净化网络内容、营造清朗的网络空间的重要使命，是实现国家治理现代化的重要手段。网络信息内容安全治理的内涵可从治理主体、治理客体以及治理手段三个维度展开。其中，治理主体包括政府、网络信息发布者、网络信息

**收稿日期**：2024-11-21
**基金项目**：山东科技大学“智能科技安全治理创新团队”项目(2020RWB003)；山东科技大学党的二十大精神研究专项重点项目(2022A26)
**作者简介**：赵丽莉(1978—)，女，山西榆次人，山东科技大学文法学院(知识产权学院)教授，山东科技大学数字法治研究院研究员，硕士生导师.

使用者、网络平台等相关主体,即网络信息内容供给、运营、监管、使用等主体。这意味着,各网络参与主体既有维护网络信息内容安全的权利,亦同时负有维护网络信息内容安全的义务。治理客体主要侧重于违法、有害以及不良信息内容。① 网络信息内容指通过网络途径传播的具有信息符号特性的文字、图片等事物,涵盖相关数据内容。违法、有害以及不良网络信息内容则主要包括危害国家安全类信息,妨害社会管理秩序类信息,侵犯公民、法人和其他组织合法权益类信息。伴随人工智能、区块链、大数据等数字化技术的快速发展,技术逻辑在一定程度上已经可以决定信息内容的形态和生命周期,如算法推荐、内容推送、程序化过滤等技术就显著扩充了网络信息内容的外延,使得网络信息内容治理不仅在于对表层信息表述与内涵的治理,还涉及对信息背后算法、代码的治理。治理手段则主要包括法律规制、政策制定、技术措施、公共宣传等。

网络空间生态质量直接影响人们的价值观与生活态度。营造健康清朗的网络环境,必须依靠有效的价值引导与内容治理。网络信息内容安全治理致力于此,通过净化网络空间、优化网络生态、繁荣网络文化,保障每一位网络用户的健康发展。

**(二)网络信息内容安全规制方式从监管向治理的变革**

监管通常指国家作为监管主体,运用公权力主动进行干预的行为。其典型模式"命令控制型监管"的核心特征在于:监管主体具有行政优益性,而行政相对人则负有服从义务。这种监管方式的优点在于监管主体既具备民主性,又同时具备以制裁为后盾的执行效率,从而保证其可以快速实现公共利益并达成监管目的。但互联网的高速发展,使得传统上依赖知识、专业和信息优势的行政主导型政府的规制能力相对弱化。网络时代技术的高度复杂性与专业性,以及法律关系的快速演变,也导致传统的命令控制型规制模式难以适应互联网发展的需求。这不仅为政府规制带来了全新挑战,更严重制约了政府的行政裁量权与法律适用的有效性,进而增加了规制失灵的风险。简言之,在网络信息内容安全治理领域,网络信息内容发布主体、传播路径以及海量网民对于不同网络信息的多元化需求,使网络信息内容承载着不同的价值内涵,也由此导致内容物的良莠不齐。而且自媒体、人工智能等技术的持续创新,推动了网络信息内容生产与传播的多元化、专业化和智能化。这不仅显著拓展了网络信息内容安全治理的边界与复杂度,更因算法、区块链等底层技术所固有的高门槛与隐秘性特征,对政府的治理能力提出了全新的、更高维度的挑战。

至此,新型治理困境使得网络信息内容治理越来越强调"从传统的行政管理向公私伙伴关系的治理路径转变"。[2]更强调以政府、网民、企业和行业组织为网络内容治理主体的多中心合作共治。政府将不再是"控制的中心",而只是其中的一个治理成员,[3]网络空间涉及的企业、网民、信息发布者、信息接受者等各个主体,都会在追求各自利益偏好与具体需求的过程中对治理效果产生影响。概言之,互联网时代,对于网络信息内容安全的治理不能只注重政府的强有力管控,也不能只依靠技术本身的发展,而是需要构建一个包括政府、网民、相关行业等在内的多元主体协同共治体系,形成一个网络信息内容安全治理共同体,在此基础上细化网络信息内容治理的不同主体责任,实现多层面协同治理,营造良好的网络生态空间。

## 二、网络信息内容安全治理对法律治理的深化

法律治理,是指运用法律规范对社会主体行为及其构成的社会关系进行规范与调节,并在政治、经济、社会、文化、生态等各领域明确界定各方主体的权责边界,从而发挥法律的社会规范功能,最终实现社会关系规范化、法治化的过程。相比较其他治理手段,法律治理以其法律规范性体现出更强的强制力和权威性。尽管网络信息内容治理已经从单一的行政垂直监管模式转变为多维主体多头监管模式,但实践中仍面临治理模式僵化、权力与权利边界不清、法律适用困难等问题。[4]故此,法律在保护和鼓励创新及促进社会发展中发挥着框架和支撑作用,可通过法律控制、消除和减少技术创新消极面及其负面影响。

① 具体内容可以参见《网络信息内容生态治理规定》第五条的内容。

在网络内容安全治理领域,提出要深化法律治理,实质即社会治理理念和机理在网络空间领域的具体体现,其不仅指运用法律规范实施治理的行为,也意蕴协同治理、多元共治的理念与机制重塑,以期最终实现网络内容安全治理领域的良法善治。[5]

**(一)根本目的:规范网络信息内容安全秩序**

互联网的普及在加速信息传播的同时,也带来诸多安全隐患,构建完善的网络信息内容安全法律治理体系,规范网络信息内容传播,保障公民权益、国家安全和社会稳定,成为当前网络信息内容安全法律治理建设的重要任务。展开而言,当虚假新闻、煽动性言论可能激化社会矛盾,境外势力利用网络进行意识形态渗透、破坏国家统一时,网络信息内容安全法律治理必须确保网络信息内容符合国家安全要求;当网络诈骗、人肉搜索、数据泄露等行为严重侵害个人隐私、名誉权、财产权等公民权益时,网络信息内容安全法律治理需明确责任主体,保障公民免受网络信息侵害;当虚假广告、商业诋毁、数据滥用等行为扰乱市场秩序,阻碍数字经济发展时,网络信息内容安全法律治理应规范网络信息传播,营造公平竞争的市场环境。故此,构建安全有序的网络信息传播环境,首要目标就是要确保网络信息内容传播合法合规,防止违法和不良信息扩散,打击虚假信息;遏制暴力恐怖信息;保护个人隐私,防止数据泄露和非法收集等。

**(二)本质要求:共建共治共享目标实现**

当治理需要多主体共同实施,并以正式与非正式制度有机结合共同作用于特定领域,强调通过法律来组织和规范社会生活时,治理本身便构成了法律体系的内在价值。事实上,即便在强调通过法律控制社会生活或将法律秩序作为社会秩序主要保障的情形下,也从未否认或排除其他社会主体、机制和规范的作用领域与功能。社会治理规范的来源具有多样性,法律并不排斥道德等其他社会规范。相反,在认识到法律与道德存在差异,强调两者在生成逻辑和作用机理上不同的同时,反而更需关注其相互影响与作用。

从综合治理角度看,强调共建共治共享,必然要求突出法治、德治和自治的作用。其中,法治在网络空间法律治理中发挥核心与框架作用。网络空间法律治理反映了我国公权力配置及行政管理体制的特点。例如,对网络传播暴力恐怖音视频的规制,就涉及立法、司法与行政多个环节,在行政管理层面,需公安、文化、网监、新闻、教育等多个主管部门协同发力,本身就存在跨部门协调与合力形成的问题。在行政管理领域,不同行政主管部门各有其执法依据和职权来源,且不同的行政法规范通常由不同的行政机关执行。因此,如何在信息网络安全治理领域构建有效的治理体系,是网络空间法律治理的应有之义。

从社会治理角度看,网络空间的治理主体除公权力机关外,还应包括网络空间的利用者(用户)、社会自组织等多元社会性参与者。因此,在构建网络空间法律治理体系时,必须贯彻并体现这一治理理念与机制。

**(三)依法治网:以《中华人民共和国网络安全法》为核心的法律体系架构**

单就法律规范的制定和运用而言,其来源具有多层次性及灵巧治理等特点。不仅存在效力位阶不同的法律规范,也存在大量效力位阶较低、却能有效指引治理实践的操作性规则。换言之,单一的部门法资源和调整手段难以达到网络内容安全的治理目标。故此,网络空间的法律治理具有鲜明的“领域法”①特征,强调突破部门法的壁垒,综合运用多元调整机制与跨学科知识,以实现特定领域的综合治理。[6]在依法治网过程中,注重并强化对违法有害信息的法律治理,既是新时代互联网法治思想的基本要求,亦是法治中国建设的关键内容。《中华人民共和国网络安全法》(以下简称《网络安全法》)《网络信息内容生态治理规定》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等一系列与上述精神相关的法律与法规陆续发布,共同构建了以《网络安全法》为核心的依法治网体系,持续深化着网络信息内容法律

① 领域法学(Science of field law),是以问题为导向,以特定经济社会领域全部与法律有关的现象为研究对象,融经济学、政治学和社会学等多种研究范式于一体的整合性、交叉性、开放性、应用性和协同性的新型法学理论体系、学科体系和话语体系,具有研究目标的综合性、研究对象的特定性以及研究领域的复杂性等特征。

治理体系和内容。具体分析如下。

《网络安全法》出台之前,《全国人民代表大会常务委员会关于维护互联网安全的决定》《全国人民代表大会常务委员会关于加强网络信息保护的决定》等规范亦涉及对网络信息内容安全的相关规定,但大多以行政法规为主,立法层级低且覆盖内容有限。《网络安全法》一出台就成为了我国治理网络安全领域的基础性法律,明确将网络信息内容安全纳入专章规范,明晰了网络运营者、服务者在网络信息内容安全保护中的义务和要求,划定了基本的保护规则和基线。如明确规定了网络用户信息保护制度、网络信息内容安全监督管理制度、关键信息基础设施保护制度、监测预警与应急处置制度。除此以外,《网络安全法》也推进了自身与《中华人民共和国刑法》《中华人民共和国治安管理处罚法》的衔接,如违法窃取网络数据,通过网络窃取或者非法获取、出售、提供个人信息,利用网络发布或者传播违法有害信息等,均与《中华人民共和国刑法》中非法获取计算机信息系统罪、侵犯公民个人信息罪、非法利用信息网络罪等内容相衔接。在此之后出台的《网络信息内容生态治理规定》提出了网络信息内容生态治理的概念,明确了政府、企业、社会、网民等治理主体,以及违法、不良等网络信息内容的具体范围,也明确规范了网络信息内容生产者、服务平台、服务使用者应遵循的基本义务以及相应法律责任,该规定成为网络综合治理体系的重要规范。《中华人民共和国民法典》《中华人民共和国个人信息保护法》等关于个人信息权益保护、个人信息处理活动规范的规定,则细化了个人信息的内涵,明确了个人信息保护的基本原则,构建了以“告知同意”为核心的个人信息处理规则,强化信息处理者的基本义务,进一步完善了对网络空间涉个人信息内容安全的法律治理。此后,大数据、人工智能、云计算等新兴技术推动数字经济快速发展,使数据成为重要的新兴生产要素,《中华人民共和国数据安全法》应运而生。其核心在于通过规范网络空间数据处理活动行为,保障网络空间数据安全,内容涵盖了对于数据分类分级的保护、数据处理者数据安全责任、数据跨境流动的管理、数据安全的审查与监督。

当然,伴随技术的持续变革——诸如生成式人工智能技术的演进、大语言模型的广泛应用、数据要素市场的深入挖掘与拓展——新型网络信息内容安全风险与威胁不断涌现,并可能因此冲击既有法律治理规范的适用性。既有法律治理规范亦面临一系列新问题,例如:如何有效界定与识别新型风险威胁;如何提升政府监管与应急处置能力;如何重新配置各治理主体间的权益;如何界定新型损害赔偿责任。为适应网络信息内容安全治理的新挑战与新要求,法律治理体系需持续深化与完善。

## 三、网络信息内容安全法律治理的基本原则

鉴于网络时代违法有害信息传播具有动态性,为实现网络信息内容安全治理的“全方位”目标,应秉持系统思维与过程控制相结合、统筹“安全”与“发展”价值取向、坚持网络社会与现实社会治理相协调的基本原则。

### (一)坚持系统思维与过程控制相结合

法律治理作为社会治理的一种手段,因其治理基础是法律规范,所以具有不同于其他治理的特点,更强调协作性、确定性、意志性、普遍性、动态性。网络社会治理需要创新,那么,针对网络社会的安全风险防范理念和机制同样需要与时俱进。网络内容安全风险防控的特点决定了,治理行为的实施不能等到出了问题之后才进行,风险防控规制也不能只是理解为“命令和控制”的指令,或者预先设定的可对结果进行评价的规则种类。[7]由此,综合考虑网络空间的规制难点和重点,提出基于控制论和系统论的网络安全风险预防与控制理念。这一理念的实施涉及三个层面:预测风险和隐患、形成和公布预警方案、实施应对网络安全危机的措施。同理,在网络空间中,为避免网络信息内容遭受破坏、泄露、篡改及不可用造成的危害和损失,杜绝违法有害信息在互联网进行传播,需要实时监测网络内容安全状态。这就要求用于保障网络信息内容安全的法律制度应当高度重视对网络信息内容安全风险的动态防控。两个相互关联的规制内容因此将被涉及:一是,预防、阻止、检测、限制、纠正、恢复和监视网络信息内容安全事件;二是,确

保网络信息系统功能的整全性,以及信息内容的可控性。

作为网络空间安全的重要部分,网络信息内容安全风险具有动态特征,这就要求对这类风险实施整体性预防与控制,推动法律治理实现三重转向:治理重点从结果转向过程,规制手段从惩罚转向预防,治理视野从静态转向动态,以破解"结果控制型"防控实践的局限性。因此,强化预防性措施、提升实时态势感知能力、完善过程控制机制、落实责任主体"协同治理",成为网络内容生态治理的必然要求。基于此理念构建防控违法有害信息传播的法律治理机制,就既要重视前端预防,阻断违法有害思想的初期传播,又要优化中端控制,强化对违法有害信息网络传播的实时识别、阻断与控制,更要加强后端惩治,依法严惩制作、传播违法有害信息的违法犯罪行为,从而构建立体式综合防控机制。可见,以"预防与控制"为核心的治理规则,强调在科学预测与风险评估的基础上,聚焦防控违法有害信息传播风险,据此确定调整对象与手段,构建融合"预防、控制、惩治"功能的"过程控制型"规范体系。

综上,网络信息内容安全法律治理所确立的防控体系与规制措施,应坚持系统性谋划、综合性治理、体系化推进,设置具有事前控制特点和动态防控功能的治理机制,以弥补法律治理因法规范自身的滞后性和静态性所产生的不足。

**(二)坚持"安全"与"发展"相统筹的价值取向**

无论是现实社会还是虚拟社会,无论是发达国家还是欠发达国家,"发展"都是社会的永恒需求。但不同国家甚至同一国家的不同时期,将因为不同的"安全"压力而面临不同的发展环境,并且在"发展"与"安全"之间作出不同的价值选择。在网络信息内容安全治理方面,坚持"安全"与"发展"统一并重的价值理念,注重"安全"与"发展"的统筹已成为我国网络空间建设的基本价值取向。

在网络信息内容安全治理中,"安全"是最基本的价值向度,其包含三层含义:一是,系统层面的数据信息安全,指保护网络系统中的硬件、软件及相关数据,使其免受偶然或恶意破坏、篡改与泄露,从而保障系统持续可靠运行及网络服务不中断。二是,社会层面的网络信息安全,指维护社会秩序稳定,防止因网络信息外部性引发社会失序、动荡或破坏。此处的"网络信息外部性",指特定社会主体使用或发布网络信息对其他主体产生的非预期影响。三是,国家层面的安全,亦称国家网络安全,指国家捍卫网络主权,防范外部网络攻击对国家核心安全信息造成损害或颠覆。以网络涉恐信息传播、关键基础设施被攻击、大规模重要数据泄露和窃取、深度伪造技术对金融信息安全的威胁、人工智能训练数据对知识产权成果的侵犯等为代表的典型风险场景,均严重威胁网络信息内容安全,并可能进一步冲击社会秩序与国家安全。故此,坚持总体国家安全观所确立的"安全"根本遵循,是网络信息内容安全治理的核心准则。

网络信息内容安全治理的另一个基本价值向度是"发展",它代表着互联网治理的目的性和"硬道理"。首先,从信息网络技术演化的长时段看,网络内容必须要抢先发展,否则会"不用则退"。如依托于互联网基础设施(WEB1.0)推动了以门户网站为中心节点的网络信息产品的产生、传播,提升了使用网络信息的潜力,可支持新闻组、电子邮件、信息检索、在线论坛的开发和运行。但如果它不能在网络内容上抢先发展,就会随着信息网络技术的演化被"2.0 版本"所淘汰,从而出现"有技术、无发展"的"不用则退"现象。其次,从同一技术时代的短时段看,网络内容必须要繁荣发展,否则就会"不用则废"。如 WEB2.0 技术可产生即时通讯传播工具,打通线上线下界限,变革信息内容的推动模式;生产式人工智能技术的出现则可提升生成效率、推动产业升级;大数据技术的出现进一步促进数据聚合,赋能生产力转型升级,提升服务精准度从而有效防范社会风险隐患、优化海洋气象预报、保障金融安全。但若不能发挥新型技术在网络内容建设方面的积极作用,就可能出现"有平台、无繁荣"的"不用则废"现象。故此,就网络信息内容建设而言,持续发展创新依然是基本要务,亦是网络强国建设的重要内容。

**(三)坚持网络信息内容治理与现实社会治理相协调**

如何理解网络信息内容治理与现实社会治理的关系,不仅影响网络信息内容治理体系、信息内容质量监管模式的构建,还影响负面清单的制定。在互联网与社会相互嵌入的环境下,网络信息内容治理的

关节点在于:能否以互联网这一巨型工具的内在规定性为基础,成功地构建起与现实社会相适应的网络信息内容安全治理模式。网络内容治理应具有与现实社会治理相协调的价值顺位,且网络信息质量监管的负面清单应该与现实社会治理呈现出一致性的价值表达。在网络空间,与现实社会相一致的网络伦理和法律规则发挥着重要的基础功用。无论是主题社区还是公共平台,都要共享基本的伦理规则和法律规则,它们是网络内容治理的基础和内核。这些伦理规则和法律规则也是人们在实际行动中自觉服从的行为准则,在总体上构成一组规则集。从过程上看,一个网络社区的形成必然伴随着现实规则的移入,那些与现实社会相融的行为规范会随时间推移占据主导地位。总之,只有立足实践,守好国家安全和法律法规的现实底线,才能有助于塑造和凝聚共治。[8]

## 四、网络信息内容安全法律治理的多维生态机制构建

### (一)深化多方参与的综合治网格局

多元治理机制作为一项重要的治理机制,在实践中持续发挥着关键作用。以合作为核心的网络治理模式,为参与预防、缓解和应对网络威胁的公共与私营部门提供了重要的发展机遇。当前,网络信息内容安全问题日益复杂多元,有效维护网络安全亟需建立一套行之有效的综合治理体系。国内外网络内容安全治理实践表明,面对快速迭代的互联网技术、不断演进的产业业态以及由此衍生的安全风险与威胁,单靠政府管控机制已力有不逮。政府治理在技术手段、信息收集与分析、风险控制等方面存在局限性,因此必须推动政府、企业、社会组织之间实现资源与治理方式的优势互补。

网络信息内容安全治理强调政府主导下的多主体协同监管,聚焦信息质量,要求所有利益相关者共同参与、责任共担、利益共享,即实现政府部门、互联网企业、网络媒体及全体网民的协同共治。其中:内容生产者与服务平台掌握技术、信息和数据资源,熟悉行业生态;行业协会关注行业可持续发展,推动自律;用户既是信息内容的生产与传播主体,也是使用者,是网络秩序构建的重要参与者。因此,向政府之外的主体合理分配风险控制责任,可提升网络信息内容安全治理的效率,也可有效弥补政府单一治理的局限性。

至此,强化以多方参与为目标的综合网络信息内容安全治理格局,发挥治理主体的协同效能,实现“互动常态化、秩序化、制度化”,[9]是提升治理效能的重要前提。一方面,需积极推进政企间信息共享与技术合作。另一方面,应主动引导产学研力量参与治理工作。可组建由民间团体、网络企业、新闻媒体组织和学术界代表组成的专家小组,协助政府管理部门制定抵制虚假信息传播的政策法规文件,开展违法有害信息的识别分析工作。此外,还应构建保障企业内容安全的责任体系,巩固并深化群防群治的网络信息内容安全治理格局。在推进网络信息内容安全治理现代化进程中,除积极发挥各主体在内容治理方面的重要作用之外,还应明确各主体间权责的边界性,即清晰的权、责、利应是持续探讨的问题。

### (二)平衡网络内容产业发展与安全遵从间的互动关系

发展是安全的基础,安全是发展的条件。既要重视发展问题,也要重视安全问题,这是坚持总体国家安全观的基本内涵。换言之,创新发展与安全可控是建设安全稳定繁荣网络空间的应有之义。伴随信息技术的持续变革与互联网内容产业的迭代更新,网络信息内容、产品及服务的创新发展,既是互联网产业发展的基本属性,也是适应技术创新、谋求长远发展的必然之举,若网络信息内容和服务停滞不前,则无法匹配新技术变革驱动下的内容产业升级诉求,终将面临淘汰风险。内容生产者、服务者及其投资者,为规避风险责任、获取互联网收益,必然主动推进内容创新发展。

与此同时,确保内容安全是网络内容治理的核心价值取向。鉴于互联网及其安全问题具有高度关联性与复杂性,一旦内容安全失守,国家安全、社会公共安全以及用户数据与隐私安全均可能被置于风险之中。例如,微短剧、短视频平台“二次创作”兴起的同时,亦暴露出内容低俗、质量参差不齐、虚假信息泛滥、价值观偏离、版权侵权、平台监管与责任界定等问题;生产式人工智能内容生产产业的发展,亦面临训

练数据合理使用、生产内容版权侵权、训练数据质量确保、虚假有害信息产生等新型内容安全风险。不仅如此,重要信息也面临被窃取或泄露风险,以及涉暴力恐怖等违法不良信息在互联网上快速传播风险,尤其是大数据、人工智能等技术的广泛应用,极有可能加剧隐私泄露、外部攻击以及数据存储与保护等安全问题,这均使国家安全与社会公共安全面临严峻挑战。由此,产业发展与数据隐私保护之间,信息内容的生产、服务、利用与数据安全之间的矛盾日益凸显,应审慎权衡网络内容产业发展与安全遵从,在二者间寻得平衡。第一,持续加强落实法规底线安全监管,在已有规范基础上,设置安全底线,从源头上把控内容质量,明析符合"合理使用"规则的二次创作条件,防范虚假有害信息、价值观渗透,明确网络内容生产者、网络服务提供者的信息安全遵从义务。第二,重视发挥头部网络服务提供者的安全保障作用,强化其内容安全审查义务。尤其是面对人工智能等新型技术带来的内容生产便捷性,大量用户利用人工智能生产违法有害内容并通过平台传播,这使得网络服务提供平台成为内容安全治理的重要参与主体,应进一步细化和明确其责任边界。第三,重视新型平台在内容安全风险方面的特殊性,设置适应性规则。以生成式人工智能平台为例,其运营涵盖数据训练、内容生成和内容传播等多个环节,不同环节可能产生不同的侵权风险,因此,其责任界定需区分不同环节。第四,利用技术赋能建立"动态合规"机制,推进发展效率与风险控制的协同。如设置自动识别侵权内容的技术措施,运用先进的算法检测和过滤不良信息等。如此,既确保内容安全又促进产业发展,可实现两者的安全互动。

**(三)持续加强多元治理机制的协调性**

面对现有网络信息内容安全协同治理中存在的"层级规制难协调、主体协同动力不足"等问题,[10]坚持"系统治理、依法治理、综合治理、源头治理"(简称"四个治理")为提升多元协同治理效能提供了重要指引。据此,网络信息内容安全治理应着力推进以下四个维度的协调统一。第一,强化系统治理。网络信息内容风险的动态演变特性要求治理行为的实施基于"过程控制"理念,不仅如此,网络信息内容间的高度关联性也凸显了对系统治理的内在需求。第二,突出源头治理。追查和控制违法有害信息,最有效的方式是源头管控,从源头实现及时识别、阻断与制止。然而实践表明,技术迭代的快速性、信息传播的跨境性与自动化、内容生成的海量化以及网络空间的不可控性等挑战,均使风险与威胁的源头追溯面临困境。例如,对暴恐信息、虚假信息、诈骗信息等传播源头、技术手段和涉案人员的追查,在实践中常面临源头难追溯、证据难固定等问题,严重阻碍了对此类行为的有效治理与打击。第三,落实综合治理。单一的行政治理模式已难以适应实践需求,构建综合治理体系与机制,已成为网络空间治理的普遍共识。第四,坚持依法治理。依法治理是网络信息内容安全治理的应有之义,法律手段是关键的治理工具和保障基础。上述各治理维度均需法律的有力支撑和规范约束。

网络信息内容安全治理不应只是关注治理效能,还应重视各治理维度间的协同互嵌关系。各治理维度应保持协同,具体治理措施的设计更需体现整体性。例如,在打击治理煽动颠覆国家政权、煽动分裂国家、煽动民族仇恨、制造社会混乱等类别的暴恐信息网络传播方面,鉴于此类音视频大多通过境外向境内流入,单纯的境内移除和拦截访问无法有效解决跨境数据流动问题,这就需要:加强对境外暴恐信息制作、传播技术的实时追踪,强化风险识别、评估与预测,实施源头治理;加强对其网络传播的过程控制,突出系统治理;依法打击违法犯罪传播行为,实施依法治理,并综合发挥行政、司法、行业协会、互联网平台、用户等多元主体的治理作用,实施综合治理。由此可见,持续推进"四个治理"间的协同协调性,是网络信息内容安全治理现代化进程中的关键要素。

**(四)重视强化法律治理与技术治理的融合性**

网络信息内容安全法律治理在强调政府主导作用的同时,需引导多元主体参与网络空间安全治理。一是明确各责任主体的法律义务。例如,网络服务提供者(含运营商)应承担的社会责任(如内容审核)及协助执法义务等。这要求在法律制度层面明确其应尽的注意义务、审查义务和协助义务,并厘清相应的法律责任分配机制。二是明确"专群结合"的治理协同规则。在网络空间治理中,多元治理主体间的协

同,即专门机关与用户的协同、行政执法机关之间的协同、执法与司法之间的协同,这些协同关系的构建与运行,均亟需法律发挥其规范与保障作用。

面对新技术对网络信息内容安全的负面冲击,单纯依靠管理,可以在特定时期和范围内解决信息安全问题,但如果缺乏坚实的技术支撑,则难以从根本上予以根除。技术是信息安全保障工作的物质基础,为信息安全管理提供核心手段与支撑。唯有坚持"以技术对抗技术"的策略,持续加强技术控污能力,方有可能有效清除那些同样由尖端技术催生的网络污染物。相关研究指出,在迈向"智能 3.0"时代的进程中,依托数字化基础及以算法为驱动核心的网络空间,其治理工作已使得数据与算法上升为关键治理要素;[11]主张网络信息安全治理应尊重内嵌于"代码"的网络技术规则,治理方式转型与网络技术换代应同步进行,[12]需高度重视信息技术的应用[13]。故此,无论在理论层面还是实践层面,技术治理均被认为是网络信息内容治理不可或缺的重要手段与核心依赖。

总而言之,"综合治网格局"强调法律与技术手段相融合,重视法律治理与技术治理的融合并进。以 ChatGPT 为代表的生成式人工智能技术所产生的虚假信息,其深度合成与自适应传播逻辑显著区别于传统技术。由此,对此类虚假信息的治理既需要厘清其技术生成逻辑、生成虚假信息的特征、产生的特殊风险,又需要分析其对已有法律治理规则的冲击,进而提出有针对性的法律治理措施。诸如创新网络安全风险评估方法、实施网络安全审查、加强信息通报与能力共享机制建设、强化对违法有害信息的追踪识别与拦截过滤等治理诉求,既需法律治理确立规范框架与权责边界,更需技术治理提供实时高效的解决方案与执行能力。唯有二者的有机融合,方能有效应对新型技术带来的复杂挑战。

## 五、结语

网络信息内容安全关乎国家安全和社会稳定,《网络安全法》《中华人民共和国数据安全法》等系列法律法规的颁布实施,初步构建了网络信息内容安全法律治理的体系框架。党的二十届三中全会强调要"加强网络空间法治建设,健全网络生态治理长效机制"并"加强网络安全能力建设",这对构建网络信息内容安全法律治理的长效机制提出了更高要求。当前,面对以信息技术、生成式人工智能、大数据为代表的新技术迅猛发展,以及随之加剧的网络攻击威胁、数据隐私泄露、虚假信息识别难度增大等新型挑战与风险,亟需在法律治理理念、模式与机制上进行创新突破。网络信息内容安全治理的基本目标具有多维性与层次性,加强其法律治理,治理体系是核心支撑、社会共治是机制创新、政策法规体系是制度保障。为此,必须持续发挥政府、社会组织、企业等各类主体在信息内容安全治理中的差异化角色与作用,综合运用社会治理、技术治理和法律治理等多种路径,切实实现维护总体国家安全观的根本目标。

**参考文献:**

[1] RHODES R A W. Governance and public administration[M]//PIERRE J. Debating governance. New York: Oxford University Press, 2000: 54-90.

[2] 宋华琳. 论政府规制中的合作治理[J]. 政治与法律, 2016(8): 14-23.

[3] 冉连, 张曦. 网络信息内容生态治理: 内涵、挑战与路径创新[J]. 湖北社会科学, 2020(11): 32-38.

[4] 任家诚, 杨青达. 网络信息内容的多维治理: 现状、困境及完善[J]. 互联网周刊, 2024(15): 16-19.

[5] 张敏, 马民虎. 企业信息安全法律治理[J]. 重庆大学学报(社会科学版), 2020, 26(5): 143-155.

[6] 刘剑文. 论领域法学: 一种立足新兴交叉领域的法学研究范式[J]. 政法论丛, 2016(5): 3-16.

[7] MULLIGAN D, PERZANOWSKI A K. The magnificence of the disaster: Reconstructing the SONY BMG rootkit incident [J]. Berkeley technology law journal, 2007, 22: 1161-1162.

[8] 支振锋, 刘佳琨. 互联网信息内容治理的中国方案[J]. 江西社会科学, 2023, 43(11): 176-187.

[9] 王泽坤. 协同困境及其破解: 对网络内容共同治理的考察——基于多重制度逻辑的视角[J]. 理论探索, 2023(6): 68-75.

[10] 周毅, 张雪. 网络信息内容生态安全风险整体智治的理论框架与实现策略研究[J]. 图书情报工作, 2022, 66(5): 44-52.

[11] 何邦武. 数字法学视野下的网络空间治理[J]. 中国法学,2022(4):74-91.
[12] 何明升. 中国网络治理的定位及现实路径[J]. 中国社会科学,2016(7):112-119.
[13] 郑智航. 网络社会法律治理与技术治理的二元共治[J]. 中国法学,2018(2):108-130.

## Legal Governance of Network Information Content Towards a Network Power: Framework, Strategy, and System

ZHAO Lili

(*Institute of Digital Law, Shandong Universityof Science and Technology, Qingdao, Shandong* 266590, *China*)

**Abstract**: Implementing the strategy to build a strong cyber nation urgently requires solid cybersecurity as support. With the development and application of new technologies such as artificial intelligence and big data, there is an explosive growth in network information content. Risks to network information content security, such as privacy and personal information leaks, the spread of illegal and false information, cyberbullying, and cyberterrorism, are becoming increasingly prominent, infringing on privacy and information security and threatening national security and social stability. Existing legal governance rules face new challenges in their applicability. Therefore, we should address the new demands for network information content security governance arising from the modernization of national governance. We should uphold the dynamic balance of legal governance, focus on the multi-dimensional.

**Key words**: network information content; legal governance; dynamic balance; integration; multidisciplinary collaboration

(责任编辑:魏 霄)