全球化数字化背景下开展网站系统信息内容安全防护的思考

吴振峰
（中国科学技术信息研究所，北京 100038）

摘 要：网站系统作为数字经济时代的关键信息基础设施和典型组织形态，对行业、领域关键业务起到基础支撑作用。网站系统信息内容安全，已成为事关国家安全、社会稳定和人民利益的重要问题。通过阐述网站系统信息内容安全防护的国内外发展现状、面临的安全风险，分析信息内容安全防护的关键技术及相关产品，结合中国实际情况提出开展网站系统信息内容安全防护的对策。

关键词：数字经济；网站系统；信息内容安全；安全防护
中图分类号：TP309.2 **文献标识码**：A DOI：10.3772/j.issn.1009-8623.2023.06.006

近年来，互联网、大数据、云计算、人工智能和区块链等技术飞速发展，数字经济已成为中国经济发展的重要驱动力。网站系统作为数字经济时代的关键信息基础设施和典型组织形态，深刻改变了人们的生产生活方式，在优化资源配置、推动产业转型升级、赋能经济高质量发展等方面发挥重要作用。数字经济时代开展网站系统信息内容安全防护，对于维护国家安全、国家网络安全和网络空间主权，保障经济社会健康发展，维护公共利益和公民合法权益具有重要意义。

1 研究背景

信息内容安全作为信息安全领域中的一个重要分支，与物理安全、网络安全和数据安全等信息安全领域其他分支的不同之处在于，其以信息内容为主要研究载体，分析识别信息内容是否合法合规，更倾向于检测保护信息自身的安全，强化信息内容安全管控，防止非法内容的传播和利用。信息内容安全的内涵可总结为两个主要方面：一是对信息内容的保护，二是信息内容要符合政治、法律和道德层面的有关要求[1]（见图 1）。面向网站系统的信息内容安全防护，本质上是信息内容安全领域的一个子集，以网站系统的信息内容为研究对象，针对网站系统中的文字、图片和音视频等信息开展内容安全审核，监测涉政、涉黄、涉暴、涉恐等违法违规信息，防范虚假新闻、网络谣言等内容造假信息，以及错别字词、标点符号错误等不规范表述，加强知识产权保护、信息隐藏、隐私保护以及党政、科技、金融等重点领域的重要信息内容保密，及时处置可能存在的风险隐患，确保网站系统信息内容安全。

2021 年 10 月 18 日，习近平总书记在十九届中央政治局第三十四次集体学习时指出，要完善国家安全制度体系，重点加强数字经济安全风险预警、防控机制和能力建设，实现核心技术、重要产业、关键设施、战略资源、重大科技、头部企业等安全可控。因此，发展数字经济，必须把安全问题摆在更加突出的位置，把安全防护贯穿数字经济发展的全过程，做好全面风险管理和安全保障。党的十九大以来，中国数字经济规模持

作者简介：吴振峰（1991—），男，博士，助理研究员，主要研究方向为智能情报、大数据与信息安全。
项目来源：中信所重点工作项目“中国科学技术信息研究所网站系统安全防控体系建设与应用（二期）”（ZD2023-01）。
收稿日期：2023-03-01

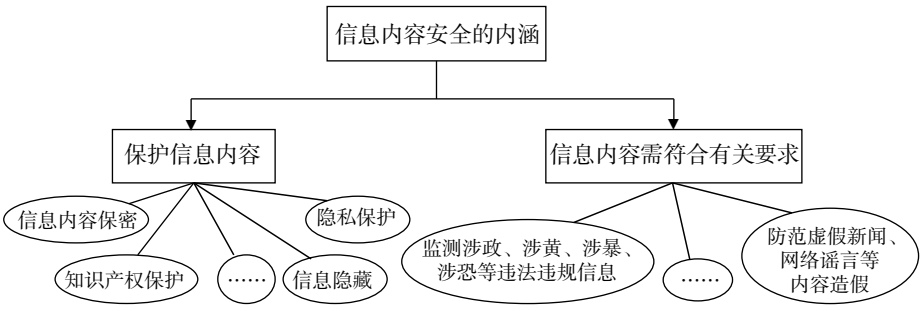

图 1　信息内容安全的内涵

续提升并实现全球领先，数据资源价值加快释放，数字社会服务更加普惠便捷。根据《数字中国发展报告（2021 年）》，2017—2021 年，中国数字经济规模从 27.2 万亿元增长至 45.5 万亿元，总量稳居世界第二位；数据产量从 2.3 ZB 增长至 6.6 ZB，大数据产业规模从 4 700 亿元增长至 1.3 万亿元；网民规模从 7.72 亿人增长至 10.32 亿人，互联网普及率从 55.8% 提升至 73.0%[2]。数字经济内涵和外延不断丰富的同时，也带动了网站类、平台类和生产业务类等网站系统建设不断提速。根据第 49 次《中国互联网络发展状况统计报告》，截至 2021 年 12 月，中国域名总数为 3 593 万个，网站数量为 418 万个，网页数量为 3 350 亿个；其中，政府网站数量为 14 566 个，仅信息公开类栏目数量就高达 22.5 万个 [3]。以此推断，若将未联网的业务系统考虑在内，中国网站系统数量以及数据规模将更加庞大，这其中既包含具有重大价值的科研数据和商业数据，也包含用户个人隐私数据，甚至可能包含影响国家安全的重要数据，对网站系统信息内容安全防护提出新的挑战。

数字经济时代，网站系统对行业、领域关键业务起到基础支撑作用，网站系统信息内容通常具有数量大、形式多样化和流动性强等特点，导致信息全生命周期管理过程中的内容安全风险随之增大。特别是近年来全球网络信息泄露、网络攻击和数据违规使用等事件频发，国内外由网站系统信息内容安全管理机制不健全、内容监测技术体系不完善等导致的内容安全问题时有发生。中国国家计算机病毒应急处理中心 2022 年 9 月 5 日发布的《西北工业大学遭美国 NSA 网络攻击事件调查报告（之一）》显示，近年美国国家安全局特定入侵行动办公室对中国国内的网络目标实施了上万次的恶意网络攻击，控制了数以万计的网络设备，窃取了超过 140 GB 的高价值数据 [4]。国际商业机器公司（IBM）最新发布的《2022 年数据泄露成本报告》显示，全球 550 家来自不同行业和地域的组织在 2021 年 3 月—2022 年 3 月所经历的数据泄露平均成本高达 435 万美元 [5]。就网站系统自身而言，部分网站系统存在违规采编发布或交易信息、散播虚假消息和网络谣言等乱象，极易扰乱网络传播秩序，泄露重要数据 [1]。由此可见，网站系统一旦遭到破坏或者数据泄露，可能严重危害国家安全和公共利益，甚至对其他行业和领域产生重要的关联性影响。网站系统信息内容安全已成为事关国家安全、社会稳定和人民利益的重要问题，信息内容安全防护更是成为网站系统生态治理的重要内容。

因此，本研究结合中国网站系统数量多、发布内容多且用户规模大的实际情况，归纳网站系统信息内容安全防护的国内外发展现状、面临的安全风险，分析信息内容安全防护的关键技术及相关产品，并重点从顶层设计、信息发布管控、信息化建设和安全人才队伍建设 4 个方面提出对策建议。

2　网站系统信息内容安全防护国内外发展现状

随着互联网和人工智能等技术的快速发展和广泛应用，全球范围内网站系统信息内容安全问题日益突出，特别是新冠肺炎疫情发生以来，网络攻击和数据泄露等事件频发，受到世界各国的高度关注。本文在广泛收集和系统梳理相关文献资料的基础上，从政策法规、项目产品和技术应用 3 个维度对国内外网站系统信息内容安全防护的发展现状进行了分析探讨。

2.1 安全立法进程不断加快，安全保护政策法规体系逐步完善

国外方面，联合国贸易发展组织统计数据显示，截至 2022 年 2 月 21 日，全球约 80% 的国家已完成数据安全和隐私立法或已提出相关法律草案。特别是 2015—2022 年，以美国、欧盟和俄罗斯等为代表的主要国家和地区相继出台相关政策法规，不断完善网络安全、数据安全顶层设计（见表 1）。例如，美国发布《关于加强国家网络安全的行政命令》，强化针对影响联邦政府信息系统或非联邦政府信息系统的重大网络事件、威胁活动和安全漏洞等的审核评估。欧洲数据保护监管局发布《欧洲数据保护监管局战略计划（2020—2024）：塑造更安全的数字未来》，明确了前瞻性、行动性和协调性三大数据保护任务，推进数字经济转型和可持续发展。俄罗斯发布《主权互联网法》，提出要建立独立于因特网的俄罗斯互联网，确保俄罗斯互联网安全、稳定和可持续运行。

国内方面，中国政府高度重视网络与信息安全工作，不断完善网络安全、数据安全领域相关制度，有力保障关键信息基础设施特别是网站系统的信息内容安全。2016 年以来，中国加快推进安全立法，相继出台《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》等多项代表性政策法规，为维护国家安全和人民群众利益提供坚实的法治保障。例如，为规范数据处理活动，保障数据安全，《中华人民共和国数据安全法》明确了数据安全保护的适用范围、支持促进数据安全与发展的措施、数据安全制度、数据安全保护义务、政务数据安全与开放，以及数据安全工作职责。为保障关键信息基础设施安全，维护网络安全，《关键信息基础设施安全保护条例》完善了关键信息基础设施认定机制，明确了关键信息基础设施范围和保护工作原则目标、监督管理体制、运营者的责任与义务、

表 1　全球主要国家和地区的代表性数据安全保护法律法规

国家 / 地区	发布年份	法律法规名称
中国	2017	《中华人民共和国网络安全法》《信息安全技术 数据出境安全评估指南（草案）》
	2019	《云计算服务安全评估办法》《数据安全管理办法（征求意见稿）》
	2020	《中华人民共和国密码法》
	2021	《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》《中华人民共和国个人信息保护法》《网络数据安全管理条例（征求意见稿）》
	2022	《网络安全审查办法》《信息安全技术 重要数据识别指南（征求意见稿）》
美国	2018	《澄清境外合法使用数据法案》
	2019	《2019 年国家安全和个人数据保护法（草案）》
	2020	《加利福尼亚州消费者隐私法案》
	2021	《关于加强国家网络安全的行政命令》《弗吉尼亚州消费者数据保护法》《统一个人数据保护法》
	2022	《计算机欺诈和滥用法（修订）》
欧盟	2018	《通用数据保护条例》《个人数据自动化处理中的个人保护公约（修订）》
	2019	《非个人数据自由流动条例》《网络安全法案》
	2020	《欧洲数据战略》《欧洲数据保护监管局战略计划（2020—2024）：塑造更安全的数字未来》
	2021	《车联网个人数据保护指南》《电子隐私条例》
	2022	《数据治理法案》《数据法案（草案）》《数字市场法案》《数字服务法案》

续表

国家 / 地区	发布年份	法律法规名称
德国	2018	《联邦个人信息保护法》
	2019	《联邦数据保护法（修订）》
	2021	《IT 安全法》《联邦数据战略》
英国	1984	《数据保护法》
	2003	《隐私与电子通信条例》
	2018	《网络和信息系统安全法规》
	2021	《通用数据保护条例》
	2022	《国家网络安全战略 2022—2030》《数据改革法案》
法国	2004	《信息技术与自由法案（修订）》
	2008	《国家安全与防务白皮书》
	2011	《信息系统防御与安全：法国战略》
	2015	《法国国家数字安全战略》
	2018	《网络防御战略评论》《个人数据保护法》《数据保护法》
俄罗斯	2006	《信息、信息技术和信息保护法》《俄罗斯联邦个人数据法》
	2008	《不使用自动化设备进行个人数据处理规定》
	2012	《个人数据相关信息系统在处理个人数据过程中的防护要求》
日本	2015	《个人信息保护法（修正案）》
印度	2022	《2022 年个人数据保护法案（草案）》
加拿大	2020	《2020 年数字宪章实施法案》

保障和促进措施，以及法律责任。

2.2 信息内容安全产业规模持续增长，项目和产品更趋多元化

国外方面，相关统计数据显示，全球信息内容安全产业规模增长较快，收入从 2018 年的 1 400 亿～ 1 600 亿元增长到 2020 年的 1 600 亿～ 2 000 亿元，其中北美、西欧和亚太地区占据产业结构的主导地位，总占比达 90%，而北美占比接近 40%[6]。面向政府管理需求，许多国家政府、科研院所或企业主导了一些代表性的信息内容安全项目，并形成相关产品。例如，美国政府层面主导了无限信息（Boundless Informant）、食肉兽（Carnivore）、锦绣（Fairview）和特别收集服务（Special Collection Service）等一系列项目，开展语音识别和关键信息提取等数据挖掘技术研究，分析全球电子信息，监听新闻网站和电子邮件等信息并进行内容分析，识别恐怖活动、欺诈等可能威胁国家安全和社会公共利益的行为。澳大利亚国家信息与通信技术研究中心主导的安全（SAFE）项目，通过目标检测等计算机视觉技术分析异常行为，预判可能的恐怖活动[6]。英国 Autonomy 公司主导的智能数据操作层（Intelligent Data Operating Layer，IDOL）服务项目，研发文本信息发掘工具，支持多语言语义检索、信息聚类、文本分类与推送等功能，并应用于实践。

国内方面，中国工业和信息化部公布的《2021 年

中国软件和信息技术服务业统计公报》数据显示，信息安全产品和服务收入增长较快，2021 年，实现收入 1 825 亿元，增速较 2020 年同期提高 3 个百分点。从全球范围来看，中国信息内容安全产业已初具规模，约占亚太地区的 7%[6]。从应用领域来看，政府、电信和金融等领域对信息安全需求规模较大，约占全国总需求份额的 60%[7]。随着国家在信息内容安全政策上的支持加大、用户需求扩大和数量增多，除北京奇虎科技有限公司、奇安信科技集团股份有限公司等信息安全领域代表性企业外，许多互联网公司和科研院所也相继加入信息内容安全领域。例如，阿里巴巴、腾讯、网易等互联网公司分别推出了云盾、天御、网易易盾等一系列内容安全产品，借助人工智能技术，检测文本、图片、视频中的涉政、涉黄、涉暴、涉恐等信息，但是面向科技领域的内容安全审核较少。中国科学技术信息研究所面向科技领域内容安全需求，推出了内容安全防控系统，能够快速自动检测党政、科技等重点领域的敏感信息和错误表述，识别科技热点话题、敏感话题并获取相关资讯，实现风险信息内容的科学研判和分级预警。

2.3 信息内容安全行业技术发展处于成长期，人工智能等技术研发及应用受到重视

国外方面，前瞻产业研究院《中国信息安全行业市场前瞻与投资战略规划分析报告》统计数据显示，2010—2020 年全球信息安全行业专利申请数量和授权数量呈现逐年增长的趋势，全球信息安全技术整体上处于成长期，截至 2022 年 1 月，美国信息安全专利申请量约占国外信息安全专利总申请量的 50%[7]。从基于人工智能的内容信息安全技术角度看，美国人工智能论文引文影响力、专利合作条约（PCT）专利数量、企业数量和融资规模等指标位居全球第一，整体实力领跑全球；欧洲、日本等主要发达国家和地区也纷纷将人工智能发展作为国家战略重点，通过加强人工智能等技术研究，赋能信息内容安全防护。例如，康奈尔大学主导的一项美国国土安全部资助项目，利用人工智能技术从收集的文本中判别蕴含的观点并寻找可能的信息来源，从而辅助决策；雅虎等公司利用大数据与人工智能分析技术过滤垃圾邮件；美国点评网站（Yelp）等社交网站利用自然语言处理技术识别虚假评论。

国内方面，截至 2022 年 1 月，中国信息安全专利申请量占全球信息安全专利总申请量的 78.33%，排名第一位，国家电网、华为、腾讯等公司的信息安全专利申请数量在全国位列前三名 [7]。近年来，中国人工智能发展迅速，综合实力不断提升，中国科学技术信息研究所发布的《2021 年全球人工智能创新指数报告》显示，中国人工智能创新水平已经进入世界第一梯队。中国科研院所和企业根据国内信息内容安全实际，积极开展基于人工智能的信息内容安全技术研发和应用示范。例如，阿里云平台、新浪微博等借助自然语言处理技术开展内容安全审核，识别垃圾文本和恶意行为，定位敏感信息 [6]。中国科学技术信息研究所内容安全防控系统通过加持网络新闻热点话题识别等人工智能技术 [8]，开展内容安全审核、科技主题研判、智能监控预警和防控定制服务，保障信息内容安全。

3 网站系统信息内容安全面临的风险

网站系统作为信息存储、交换和服务的基本载体，是网络安全的重中之重，也是可能遭受攻击的重点目标。例如，金融、能源和电力等领域的网站系统一旦遭受破坏或者发生重要信息泄露，极可能导致金融紊乱、交通中断、电力瘫痪等问题，将对经济社会稳定和国家安全构成威胁。本文从信息生命周期管理、技术谬用和滥用、网络舆情管理 3 个视角，重点梳理了网站系统信息内容安全存在的风险。

3.1 网站系统信息生命周期管理各环节存在数据安全风险

网站系统信息的采集、传输、处理、存储、传播和利用等信息生命周期管理的重要环节，存在数据篡改、违规传输、非法访问、数据泄露和数据滥用等数据安全风险 [9-10]。一是信息采集环节存在数据篡改和违规采集风险。采集的信息经过计算机或者人为的修改、增加和删除等破坏操作造成数据失真，或者未按照有关规定开展信息采集工作，影响数据的真实性和合法性。二是信息传输环节存在隐私泄露和违规传输风险。数据传输实时性要求高，由于行业和企业间存在差异，数据接口规范、通信协议不统一，加密技术和安全策略强度不足，或者

数据未按照有关规定擅自进行传输，容易导致数据传输过程追踪溯源和隐私泄露等问题。三是信息处理环节存在内容敏感和不规范风险。网站系统在信息处理过程中容易忽视党政、科技等领域敏感词汇和不规范表述的内容安全审核，导致涉及国家秘密、商业秘密和个人隐私等信息的泄露风险。四是信息存储环节存在数据篡改和数据滥用风险。数据资源整合不足、数据分级分类管理不规范、数据存储故障或被破坏等问题，会影响数据的真实性和保密性，容易导致数据泄露、篡改、丢失、不可用等风险。五是信息传播环节存在数据泄露和数据滥用风险。数据被恶意获取或者转移、发布至不安全环境，以及数据超时间、超范围和超用途使用，容易造成数据泄露风险。六是信息利用环节存在非法访问和流量异常风险。网站系统易出现数据遭到未授权访问、数据资源整合和深度分析不足、数据流量规模和内容出现异常等问题，导致身份识别和权限管理风险增加。

3.2 技术谬用和滥用对网站系统信息内容安全构成潜在威胁

随着人工智能等新技术的快速发展，“深度伪造”“大数据杀熟”等技术谬用和滥用现象，为个人和社会带来风险挑战。一是基于人工智能的内容“深度伪造”现象可能威胁公民人身和财产安全。具有极高欺骗性的“深度伪造”技术借助深度学习算法，制作或修改视频、音频、图片、文本内容，以呈现出高度逼真但与实际不符的事物，加剧了社交媒体虚假信息的传播[11]。二是“大数据杀熟”现象冲击市场和商业伦理。部分企业和商家滥用用户信息数据，对新老用户实施差异化定价手段而牟取利益，侵害消费者权益。三是算法模型自身存在安全风险。通过数据投毒攻击、神经网络后门攻击、对抗攻击和模型窃取攻击等技术手段，诱使算法模型生成误判或漏判结果，或造成数据、模型泄露，影响网站系统信息内容安全[12]。四是算法模型可解释性影响网站系统信息内容的可信度。部分网站系统使用深度学习算法模型进行数据挖掘，并提供信息服务，但是由于深度学习算法模型可解释性不足，模型预测结果透明度成为研究人员和网站系统用户关注的主要问题。五是基于智能算法的情报收集技术可能被用于国家竞争和现代战争。网站系统信息内容经过深度关联分析，极容易形成有价值的情报，威胁国家安全。

3.3 复杂传播环境下网站系统信息发布内容的网络舆情管理难度加大

新媒体技术的快速发展和广泛应用，促使网络传播环境更加复杂化、传播形态更加多样化，网络传播交互性和实时性特征凸显，重要信息泄露、虚假新闻传播等风险大幅增加，加大了网络舆情管理工作的难度。一是网站系统用户辨别能力较弱、法律意识不强等问题导致舆情复杂化。用户非理性转发传播网络突发事件信息，促使突发事件传播更快、更广，扩大了网络舆情带来的负面影响。二是网络信息碎片化和不对称性引发负面舆情风险。信息内容失真、信息观点分化，以及用户对信息获取滞后、了解缺失等现象，使得网站系统与受众之间产生认知偏差，导致负面舆情风险增加。三是网站系统信息发布制度疏漏和审核不严谨导致负面舆情风险。部分网站系统存在审核把关机制不健全、管理规范性不高、内容保障和安全保障能力不强等问题，导致错别字词和表述性错误时有发生，影响网站系统服务质量。四是网站系统中的不良信息、偏激信息影响社会稳定性。不良信息会对正确价值观产生负面影响，偏激信息在网络上传播容易导致用户产生负面情绪，影响用户对信息的价值判断。五是舆情管理机制不健全威胁网站系统信息安全。网络舆情信息收集、识别、研判、分析、预警和监督等机制不完善，信息化和智能化水平还不够高，导致复杂网络传播环境下安全漏洞和恶意攻击事件频繁发生。

4 信息内容安全防护关键技术及相关产品

信息内容安全防护旨在分析识别信息内容是否合法、规范，防止非法内容和不良信息的传播与利用，确保信息内容安全[6]。近年来，人工智能等新技术快速发展，有效提高了内容鉴别和审查能力，推进内容安全治理自动化、智能化、高效化和精准化[1]。为此，本文广泛调研国内外应对信息内容安全的经验做法，梳理了信息内容安全防护的关键技术及相关产品，为数字经济时代做好网站系统信息内容安全防护提供参考。

4.1 信息内容安全防护关键技术及应用

从防范和化解网站系统信息内容安全风险角度

出发，信息内容安全防护范畴可重点归结为信息生命周期保护、新技术安全应用和网络舆情安全管理3个方面，以下对其相关关键技术及应用进行分析。

信息生命周期保护方面，隐私计算和区块链等关键技术被用于助力数据开放共享、加强数据隐私保护、降低数据泄露风险和服务数据价值流通等实际场景中，辅助解决信息生命周期各阶段中的数据权属界定和数据安全风险等问题。隐私计算技术可在充分保护数据和隐私安全的前提下实现数据价值的转化和释放，实现多方数据“可用不可见”[13]。目前隐私计算技术有3个主流方向，分别是以多方安全计算为代表的基于密码学的隐私计算技术、以联邦学习为代表的人工智能与隐私保护技术融合衍生的隐私计算技术，以及以可信执行环境为代表的基于可信硬件的隐私计算技术[14]。区块链技术具有分布式、难篡改和可溯源等特点，确保计算过程和数据可信[15]。随着中国“东数西算”工程实施，隐私计算技术与区块链技术加速融合，用于解决数据隐私保护和数据共享之间的矛盾，助力数据可信流通。隐私计算和区块链等关键技术为实现数据安全提供了重要的技术支撑，但是它们本身的安全性和性能仍需进一步完善。

新技术安全应用方面，机器学习安全防御、虚假内容检测等关键技术被用于应对算法模型本身存在的安全风险，以及解决“深度伪造”“大数据杀熟”等技术谬用和滥用问题。机器学习在自然语言处理、计算机视觉和信息安全等领域应用广泛，但是机器学习算法模型和训练数据本身面临数据投毒攻击、模型窃取攻击等安全威胁，进而影响基于机器学习的应用系统的安全性。针对机器学习算法模型安全问题，近年来机器学习算法安全评估、训练过程防御、测试推理过程防御、数据安全隐私保护等多方面技术加速发展，旨在防御算法模型在训练和推理过程中的安全威胁[16]。针对“深度伪造”技术谬用现象，近年来涌现出大量虚假内容检测技术，着力于识别人工无法审核的内容，在虚假新闻检测和人脸资料审核等实际应用场景中发挥作用[17-18]。机器学习安全防御、虚假内容检测等关键技术有力保障了新技术的安全应用，但在多学习器安全问题和信息缺失下的系统建模和推理问题等方面仍有待深入研究[1]。

网络舆情安全管理方面，不良信息检测与过滤和社会网络分析等关键技术被用于复杂网络环境下信息内容安全审核和网络安全防护。网络舆情管理是集信息监测、分析、预警、处置和总结于一体的系统性工作，需要利用信息检索、网络爬虫、特征抽取、话题检测与跟踪以及情感分析等技术对网络舆情进行综合研判处理。同时，社会网络分析、信息内容过滤和文本自动纠错等关键技术可用于识别涉政敏感、科技敏感、低俗色情和违禁暴恐等敏感信息和不规范内容。例如，可通过对文本数据进行语义网络分析，自动识别阴谋论文本[19]。通过对网络开源信息开展针对性监测，基于开源情报分析、话题检测与跟踪等技术判断敏感信息网络暴露情况，追踪网络舆情事件发展趋势和态势。从系统网络角度来看，基于流量分析与入侵检测、恶意代码挖掘与检测等技术，对网络中各种业务流量以及系统代码进行深入分析，识别恶意流量和代码，及时开展问题溯源，保障网络信息安全。

4.2 信息内容安全防护相关产品

计算机技术的快速发展和信息化应用的广泛普及，特别是人工智能、区块链等新技术加速演进，导致网络信息安全风险概率、种类和复杂度日益增加。面对日益复杂严峻的网络安全形势挑战，中国近年来相继推出《中华人民共和国网络安全法》《中华人民共和国数据安全法》《关键信息基础设施安全保护条例》等多项政策法规，为信息内容安全产业快速发展提供了良好的政策环境和制度保障。本文对现有信息内容安全防护产品进行了梳理，重点总结了内容安全、数据安全、身份与访问安全、云安全、安全智能、网络安全、安全服务7个类别的相关产品，可以看出，信息内容安全类产品与服务的种类趋于多样化、功能趋于实用化、性能趋于智能化（见表2）。

5 开展网站系统信息内容安全防护的对策

数字经济背景下造成的网站系统信息内容安全问题，既有网站系统自身的原因，也有外部的原因，主要受网站系统自身安全防控能力不足、不能及时适应信息安全等级保护要求、信息安全环境复杂多变、防控体制机制不健全等多方面因素的影响。

表 2　信息内容安全防护相关产品与服务

产品类别	产品功能
内容安全类	借助内容审核技术，对文字、文档、图片和视频等多媒体信息进行内容过滤和分析，筛选过滤敏感信息和不规范信息，确保信息内容安全可控
数据安全类	防范网站系统数据被非授权泄露、更改、破坏或控制，确保数据的完整性、保密性和可控性
身份与访问安全类	借助身份鉴别和访问控制等技术，在用户请求访问网站系统资源时对身份进行有效性验证，确保网站系统资源不被非法访问和使用
云安全类	保障云端的服务及数据资源的安全
安全智能类	借助大数据和人工智能等技术，分析网站系统异常行为、可能存在的威胁，并开展网络攻击溯源，防范高级复杂攻击
网络安全类	面向网关安全、计算机与移动终端安全、应用安全和业务安全管理等范畴的产品
安全服务类	对网站系统运营方提供渗透测试、安全检测、风险评估、咨询规划和安全培训等服务

未来的网站系统信息内容安全防护将成为各方重点关注的问题。党的二十大报告明确指出，必须坚定不移贯彻总体国家安全观，把维护国家安全贯穿党和国家工作各方面全过程，健全国家安全体系，增强维护国家安全能力，提高公共安全治理水平，完善社会治理体系，确保国家安全和社会稳定。这为今后做好网站系统信息内容安全防护指明了前进方向，提供了根本遵循。

面对形势新变化和实践新要求，网站系统信息内容安全防护仍然存在政策体系不完善、管理责任不明晰和技术监测机制有待健全等问题。为科学应对网站系统信息内容安全面临的风险，可以重点从顶层设计、信息发布管控、信息化建设和安全人才队伍建设 4 个方面着手解决问题。

（1）加强顶层设计，完善法律法规和政策标准体系。

中国要充分适应形势新变化、实践新要求和促进新技术快速发展，加强关键信息基础设施特别是网站系统的信息内容安全立法工作，建立新的自上而下的信息内容安全法律法规和政策标准体系保障框架，从国家战略层面引导各级政府机构、非政府组织和企业等多方完善机构层面的网站系统信息内容安全管理制度，制定更加务实、可落地和操作性强的安全防控工作举措，并建立长效工作机制，强化对本行业、本领域和本区域对外发布信息内容安全的管理。网站系统责任机构要以优化机制、完善流程和强化管理为抓手，健全网站系统信息发布和更新维护、信息内容安全检测、定期备份和应急响应等信息内容安全管理制度体系，机构内各部门依据信息内容安全管理制度体系，结合实际制定相应实施细则，完善网站系统信息内容安全保护流程，明确责任分工、审查流程、审查标准、应急处置和档案管理等要求，并与时俱进更新完善。上级主管机构做好对网站系统责任机构的指导、监督和检查工作。各级网信部门和保密部门要强化网站系统信息内容安全工作协调机制，完善网站系统安全防控力量布局，构建全域联动、立体高效的信息内容安全防护体系，努力形成各单位各部门协调配合、齐抓共管的良好局面。

（2）加强信息发布管控，完善信息内容安全风险监测和评估机制。

从国家层面加快健全风险监测、评估、预警和管控机制，明确重点领域安全风险，构建一套完备的网站系统信息内容安全工作监测和评估指标体系，制定内容安全风险管理流程标准和操作指南，搭建包含识别、防护、检测、响应和恢复等功能的内容安全框架，并根据实际情况变化适时修订完善，为各级政府机构、非政府组织和企业等多方做好内容安全风险防控并及时改进工作提供重要遵循。网站系统责任机构要加强信息发布内容公开审查，坚持“先审查、后公开”的原则，严格限定公开范围及时限；要规范网站系统信息的宣传报道内

容，强化核心技术、重大项目、关键人才、重点机构、重要成果和展览展示的信息发布审查；要建立应急处置机制，制定风险防控应急预案，一旦发现内容安全风险，第一时间采取措施防止扩散并进行处理。各级网信部门和保密部门要以坚定维护国家政权安全、制度安全、意识形态安全为根本，加大监督检查力度，推进网站系统信息内容安全防控常态化，定期开展网站系统信息内容安全风险专项整治，加强重点行业、重点领域的网站系统信息发布、传播的管理和监管，以及内容安全风险信息获取、分析、研判和预警工作，及时掌握网站系统信息内容安全整体态势，严密防范安全风险。

（3）加强信息化建设，开发自主可控、安全可靠的内容安全防控系统。

考虑到机构层面的网站系统内容安全保护能力参差不齐，国家网信部门和保密部门应牵头完善网站系统内容安全风险防控体系，建设涵盖网络攻击和敏感信息等方面的高质量权威内容安全比对数据库，充分利用人工智能、隐私计算和开源情报分析等先进技术，研发有效的内容安全防控系统，能够针对网站系统中的文字、图片和音视频等信息内容开展内容安全审核，检测隐私泄露、知识产权侵权和涉政、涉黄、涉暴、涉恐等违法违规信息，党政、科技和金融等重点领域的保密或敏感信息，虚假新闻、网络谣言等内容造假信息，以及错别字词、标点符号错误等不规范表述，提升安全防控智能化、信息化水平，全面提高网站系统全域监测、智能预警和风险处置能力。网站系统责任机构要着力贯通机构内部各网站系统的底层数据，夯实网站系统数据脱敏、追踪溯源、全域扫描和实时监测等技术基础，强化网站系统中数据、技术和服务等各类要素的融合与衔接，促使数据资源分级分类管理和跨系统有序高效流动，推进技术和服务跨系统安全耦合，依托内容安全防控系统，持续监测网站系统发布信息和开源网络及社交媒体数据，提升网站系统信息内容鉴别和违规审查水平，确保网站系统数据、技术和服务等各类要素用途明确、范围可控。关键领域、易受攻击威胁和对信息技术依赖较大的机构要做好硬件设备、软件系统和关键技术的国产化更新升级，有组织、有计划地保障网站系统信息内容安全。

（4）加强安全人才队伍建设，营造人人关注安全、重视安全和参与安全的良好氛围。

考虑到网站系统信息内容安全工作具有复杂性、动态变化性等特点，政府主管部门需要与时俱进地吸收网站系统信息内容安全的创新理念、技术和管理方法，加强信息内容安全人才引进、培养等管理工作；发展壮大群防群治力量，营造安全氛围，推动构建人人有责、人人尽责和人人享有的信息内容安全治理共同体。鼓励高等院校探索信息内容安全人才培养的新思路和新机制，强化师资队伍建设和专业人才培养；鼓励企业深度参与高等院校信息内容安全人才培养工作，推动高校和企业协同育人，构建信息内容安全人才培养和技术创新助力产业发展的良好生态。网站系统责任机构要把安全文化建设作为业务工作考核的重要参考，充分调动干部职工的积极性和创造力，从根本上提升安全工作水平；加强提高网站系统信息内容安全以及处置相关突发舆情事件的保障能力，加强本单位的信息内容安全人才、技术等力量建设。各级网信部门和保密部门要加强网站系统信息内容安全教育，通过培训、宣传和研讨等形式，增强相关单位及人员维护网站系统信息内容安全的意识和能力，筑牢网站系统信息内容安全人民防线。■

参考文献：

[1] 朱世强，王永恒．基于人工智能的内容安全发展战略研究 [J]. 中国工程科学，2021, 23(3): 67-74.

[2] 中国网信网．国家互联网信息办公室发布《数字中国发展报告 (2021年)》[EB/OL]. [2022-12-12]. http://www.cac.gov.cn/2022-08/02/c_1661066515613920.htm.

[3] 中国互联网络信息中心．第 49 次《中国互联网络发展状况统计报告》[EB/OL]. [2022-12-12]. http://www.cnnic.net.cn/n4/2022/0401/c88-1131.html.

[4] 国家计算机病毒应急处理中心．西北工业大学遭美国 NSA 网络攻击事件调查报告 (之一)[EB/OL]. [2022-12-12]. https://www.cverc.org.cn/head/zhaiyao/news20220905-NPU.htm.

[5] PAGANINI P. The 'Cost of a Data Breach' report commissioned by IBM Security states that the cost of a data breach exceeded $4.2 million during the COVID19 pandemic[EB/OL]. [2022-12-12]. https://securityaffairs.co/

wordpress/120627/data-breach/cost-of-data-breach-2021.html.

[6] 杨黎斌 , 蔡晓妍 , 戴航 . 网络信息内容安全 [M]. 第二版 . 北京 : 清华大学出版社 , 2022: 3-13.

[7] 前瞻产业研究院 . 中国信息安全行业市场前瞻与投资战略规划分析报告 [EB/OL]. (2022-10-18)[2022-12-12]. https://baijiahao.baidu.com/s?id=1747021999730131373&wfr=spider&for=pc.

[8] 吴振峰 , 兰天 , 王猛猛 , 等 . 基于共享最近邻和马尔科夫聚类的网络新闻话题检测方法 [J]. 数据分析与知识发现 , 2022, 6(10): 103-113.

[9] 陈全平 . 信息生命周期管理研究 [J]. 山东图书馆学刊 , 2010(5): 15-19.

[10] 中华人民共和国工业和信息化部 . 公开征求对《工业和信息化领域数据安全风险信息报送与共享工作指引 (试行)(征求意见稿)》的意见 [EB/OL]. (2021-12-22)[2022-12-12]. https://www.miit.gov.cn/gzcy/yjzj/art/2021/art_9ed695f19c9f42f882bfdad9ba5ea0e7.html.

[11] NADIA M B, DANIEL L S. Aging in an era of fake news [J]. Current directions in psychological science, 2020, 29(3): 316-323.

[12] ANTHONY D J, BLAINE N, BENJAMIN I P R, et al. Adversarial machine learning [M]. Cambridge: Cambridge University Press, 2019: 69-103.

[13] 丁莹 . 隐私计算产业政策环境分析 [J]. 通讯世界 , 2022(4): 169-171.

[14] 隐私计算联盟，中国信息通信研究院云计算与大数据研究所 . 隐私计算白皮书 (2021年)[EB/OL]. [2022-12-12]. https://www.doc88.com/p-39239696189777.html.

[15] 法制日报 . 先进科技助攻疫情防控阻击战 [EB/OL]. [2022-12-12]. http://www.cac.gov.cn/2020-02/24/c_1584090428340042.htm?from=singlemessage.

[16] 李盼 , 赵文涛 , 刘强 , 等 . 机器学习安全性问题及其防御技术研究综述 [J]. 计算机科学与探索 , 2018, 12(2): 171-184.

[17] TOLOSANA R, VERA-RODRIGUEZ R, FIERREZ J, et al. Deepfakes and beyond: a survey of face manipulation and fake detection[J]. Information fusion, 2020, 64: 131-148.

[18] ZHOU X Y, ZAFARANI R. A survey of fake news: fundamental theories, detection methods, and opportunities[J]. ACM computing surveys, 2020, 53(5): 1-40.

[19] MIANI A, HILLS T, BANGERTER A. Interconnectedness and (in)coherence as a signature of conspiracy worldviews[J]. Science advances, 2022, 8(43): 1-9.

Countermeasures for the Information Content Security Protection of Website System in the Context of Globalized Digitalization

WU Zhenfeng

(Institute of Scientific and Technical Information of China, Beijing 100038)

Abstract: As a critical information infrastructure and typical organization form in the era of digital economy, the website system plays a fundamental role in supporting the key businesses of industries and fields. The information content security of website system has become an important issue concerning national security, social stability and people's interests. This paper introduces the development status and security risks of the information content security protection of website system at home and abroad, analyzes the key technologies and related products of information content security protection, and puts forward countermeasures for the information content security protection of website system based on the actual situation of China.

Keywords: digital economy; website system; information content security; security protection