



中国共产党新闻网
www.cpcnews.cn

中文简体 BIG5 藏语 维吾尔语 哈萨克语 朝鲜语 傣仂语 Sawoung

习近平系列重要讲话数据库

高层动态 人事 理论 党建 独家 滚动
中央文件 反腐 党史 综合 视频 搜索

以信息安全保障国家经济安全

孙早 王乐

2026年03月20日08:25 来源：光明日报

☆ 收藏

原标题：以信息安全保障国家经济安全

安全是发展的前提，发展是安全的保障。“十五五”规划纲要提出，“保障国家经济安全”。经济安全是经济持续健康发展的关键，也是中国式现代化建设的重要保障。随着数字技术的发展和数字产业规模的扩大，数字经济已成为经济高质量发展的重要驱动。与此同时，数字安全风险日益凸显。习近平总书记强调，“我们要坚决维护我国发展利益，积极防范各种风险，确保国家经济安全”，“要维护国家数据安全，保护个人信息和商业秘密”。在全球数字经济高速发展、数字要素成为核心生产资料的时代背景下，保障信息安全已成为捍卫经济安全的必然要求。应立足总体国家安全观，从法规政策保障、信息安全人才培养与技术研发、强化信息安全意识、国际信息安全合作等方面进行系统布局，以信息安全保障国家经济安全，为以中国式现代化全面推进强国建设、民族复兴伟业筑牢根基。

1. 健全信息安全法规保障体系

应进一步完善信息安全法律法规及配套政策体系，在数据安全法、网络安全法等现行法律框架基础上，细化配套法规与实施细则，明确各方主体在信息安全保障中的责任与义务。

强化重点领域刚性约束，优化关键行业治理模式。对关键信息基础设施、个人隐私以及国家涉密等重点领域数据，严格落实“原始数据不出域，备份数据可追溯，高敏感数据本地化”的要求。针对人工智能等重点新兴产业，一方面，聚焦安全风险制定专项规则政策，针对训练数据来源核验标准、算法歧视防控要求以及生成内容标识义务等方面制定规则细则；另一方面，加快将数据处理算法自研占比要求纳入法律框架，通过设立专项扶持资金等配套政策，引导企业攻关算法核心技术，提高企业数据处理的安全自主性。

正确处理数据安全与效益的关系，始终把安全作为头等大事来抓，规范数据流通交易行为。国内层面，制定明确的数据交易规则和流程，确保数据交易合法性、规范性与透明度，并通过数据加密、访问控制和安全审计等技术手段保障交易安全。境外层面，优化数据跨境流通监管机制：建立数据跨境流通“白名单+安全评估”的动态管理机制，明确合法接收数据的国家和地区范围，确保数据跨境流向可控可溯；构建“事前评估—事中监测—事后追溯”的全链条监管体系，要求数据运营商在境内完成信息数据的采集和存储，在出境前进行安全评估并提交相应的安全报告。

构建多主体协同保障体系，完善跨部门协调监管机制。建立联席会议机制，相关部门共享数据安全备案、流通交易、出入境管理、风险评估和事后处置等关键信息。构建国家信息安全评估平台与统一指标体系，健全信息共享机制，推动形成政府、企业、协会、科研院所等多主体共同参与的信息安全保护生态。

强化执法监管力度，完善应急响应机制。严格执行重点数据审查制度，对关键数据应用“加密传输+隐式水印”等技术，确保数据传输安全；根据数据体量、类型对数据运营商及相关企业开展网络安全检测和风险评估，定期进行专项检查，防患于未然；制定分级分类信息安全事件应急预案，在“发现—控制—评估—处理—补救—总结”的应急响应框架下，明确数据泄露、网络攻击、系统瘫痪等场景的标准化处置流程，保证应急处理的及时性和有效性。

2. 加强信息安全人才培养与技术研发

信息安全工作需要以高质量人才为支撑，以创新驱动为核心。只有一体推进教育科技人才发展，做好人才培养工作，坚持以技术研发引领产业升级，加快科技成果转化，才能以人才培养和技术研发赋能国家信息安全工作，为有效保护信息安全奠定人才和技术基础。

强化高水平人才培养，加强信息安全实践培训。应引导高校面向信息安全领域开设定制专业方向、优化培养体系，重点布局信息安全与人工智能、生物医学、经济法律等学科的交叉融合方向，培养具有交叉学科研究背景的优质人才。深化产学研协同育人，支持高校、信息安全领域的科技企业、科研机构建立稳定合作关系，通过深化信息安全领域产学研融合，培养兼具创新与实践能力的复合型人才。在数字经济示范区，支持高校、科研机构和企业共建信息安全实训基地，培育一批具有计算机、人工智能和信息安全等相关实践经历的专业技术人才。将思政教育精准融入课程教学和实践实训全过程，打造一支向党爱国、信仰坚定的高素质信息安全人才队伍。

加大政府信息安全投入，加快安全技术研发应用。首先，加大信息安全领域基础研究与核心技术研发的投入，如设立国家级信息安全技术专项

基金，出台科技创新奖励、金融支持和政府采购等政策，重点支持数据加密、安全审计、入侵检测等关键核心技术的研发工作，鼓励引导企业开展信息安全防护技术研发。其次，支持高校、科研机构与企业共建创新平台，推动信息安全领域科技创新与产业创新深度融合，打通“基础研究—技术攻关—产业应用”全链条各环节。最后，推动“安全沙箱”“数据脱敏”“零信任架构”等先进技术在信息安全领域的应用，鼓励企业使用本土化信息安全技术，实现“信息安全过滤+知识产权保护+个人信息脱敏”的结构化管理。

3. 提高信息安全意识

牢固树立国家安全意识，营造全社会注重信息安全的浓厚氛围，是有效开展信息安全工作的价值目标和实践导向。应强化企业的信息安全意识，大力提升群众信息安全素质，坚决守牢信息安全底线，形成全社会维护国家信息安全的强大合力。

分行业组建专业化信息安全治理组织，建立行业安全评估与共享机制。一方面，支持金融、能源和人工智能等重点行业成立专业化信息安全保护组织，吸纳企业负责人、科研专家和信息安全从业人员共同制定行业信息安全自律公约，明确数据采集、存储、交易等全环节行为规范。重点完善信息安全保护技术规范，细化关键技术操作要求，将“最小必要”和“知情同意”原则嵌入数据处理全流程，营造合规有序的行业生态。另一方面，由行业协会牵头开展年度安全合规评级，发布行业安全白皮书与典型风险案例，搭建跨企业安全信息共享平台，为中小企业提供风险预警服务。

强化企业主体责任，筑牢信息安全防线。鼓励企业将信息安全理念内嵌于发展战略中，开展常态化专题培训，强化全体员工的信息安全意识。推动企业建立健全数据全生命周期管理制度，实现数据采集、存储、使

用、销毁的全链条闭环监管。健全企业数字信息管理能力分级评价体系，对评级较高的企业给予政府优先采购、项目申报倾斜等激励政策，引导企业提升信息安全自主保护能力。

开展全民科普教育，提升全社会的信息安全素养。一方面，由相关部门统筹，依托电视、社交媒体和社区宣传等多种渠道，加强信息安全政策解读、风险警示与知识普及，提高全民信息安全意识和风险防范意识。另一方面，支持行业协会、信息安全企业开展免费公益咨询，为公众提供个人信息保护、网络安全问题排查等志愿帮助。此外，关注公民跨境交流中的信息泄露风险，开展专项宣传教育，发布并普及跨境信息安全指引，保障公民跨境交流的信息安全。

4. 参与国际信息安全合作

人工智能、云计算等新兴技术的快速演进，使得信息攻击手段日益多样化与智能化。面对这些共同挑战，没有哪个国家能够独善其身，也没有哪个国家能够独自解决。积极参与国家信息安全合作，达成国际共识，才能为人类发展进步提供安全的信息网络环境 and 安全有序生态。

深度参与信息安全国际规则制定，对接高标准数字经贸规则。在规则制定方面，以联合国、二十国集团、亚太经合组织等为依托，深度参与关键信息基础设施、网络安全、个人信息保护与数据安全等领域的国际标准磋商，贡献信息安全治理的中国方案。与各国政府建立高效信息安全响应合作机制，重点推动数据跨境流动“安全评估互认”“合规体系对接”等达成共识，提高对跨境信息和数据安全事件的响应和处理能力。在技术标准应用方面，依托国际标准化组织，牵头制定数据加密、匿名化处理、生成式人工智能安全标识等技术使用规范，推动我国量子安全通信、工业互联网安全等优势领域的技术方案转化为国际标准。

构建多层次多边信息安全合作，强化跨国协同治理能力。积极搭建跨国合作框架，通过高层对话、专项会议等强化互信，建立跨境数据流动国际安全合作体系。深化关键信息安全技术跨国联合研发，聚焦数据加密、匿名化等核心领域开展合作，凝聚维护信息安全的全球共识。此外，积极推动我国信息安全领域科研团队与世界顶尖机构的学术交流与合作，共同培育高素质信息安全人才。建立信息安全犯罪协作处理机制，协同打击数据窃取、个人隐私泄露、企业产权攻击等跨境非法行为。

健全企业境外权益保障体系，筑牢“出海”安全屏障。应设立信息安全维护服务平台，为境外中国企业提供信息安全评估、风险预警和法律适配等服务，指导企业应对境外数据审查与安全诉讼。分类处置境外信息安全威胁：针对一般性的境外信息安全威胁，通过双边磋商、发声等方式督促相关方及时整改；针对恶意打压、数据窃取和网络攻击等严重侵权行为，在遵守国际规则的前提下依法采取对等反制措施。

（作者：孙早 王乐，均系西安交通大学经济与金融学院教授）

（责编：黄瑾、万鹏）
