

# 互联网法律白皮书

## (2023 年)

中国信息通信研究院

2024年01月

---

## 版权声明

---

本白皮书版权属于中国信息通信研究院，并受法律保护。转载、摘编或利用其它方式使用本白皮书文字或者观点的，应注明“来源：中国信息通信研究院”。违反上述声明者，本院将追究其相关法律责任。



## 前 言

党的十八大以来，习近平总书记高度重视互联网法治工作，强调要坚持依法治网、依法办网、依法上网，让互联网在法治轨道上健康运行。2023年是全面贯彻落实党的二十大精神开局之年，也是实施“十四五”规划承上启下的关键之年，我国互联网立法工作呈现高质量、高效率推进趋势。《数字中国建设整体布局规划》提出，要完善法律法规体系，加强立法统筹协调，研究制定数字领域立法规划，及时按程序调整不适应数字化发展的法律制度。延续《网络立法白皮书（2022年）》中提出的将互联网立法划分为“3+1”的体系架构，“3”是指数据、设施、技术三个要素，“1”是指平台。本报告围绕数据、设施、技术、平台四个方面梳理总结2023年国内外互联网立法基本情况和发展趋势。

2023年，我国深入贯彻落实党中央关于网络强国、数字中国的决策部署，积极推进互联网立法工作，不断完善相关法律制度规范，基本形成了具有中国特色的互联网法律体系，为推动互联网持续健康发展提供了法治保障。网络设施安全防护进一步加强，保障数据安全和促进数据价值释放法律制度同步推进，互联网平台发展的法治环境日益优化，新技术新模式发展逐步规范。

从全球来看，网络安全立法持续推进，数据跨境流动和数据共享流通成为新的立法关注点，互联网平台对网络信息内容的管理义务进一步强化，全球加快对人工智能等新技术新应用的立法应对，

各国加快推进互联网立法进程为保障国内发展、强化国际竞争提供制度保障。

在习近平新时代中国特色社会主义思想指引下，我国需适应数字经济发展要求，构建完善互联网法律体系，补齐法制短板；以互联网平台为抓手完善互联网法律制度，通过分类分级制度实现精准施策；应对人工智能等新技术发展风险障碍，为新技术的规范发展提供法治支撑；深入布局研究互联网立法前沿问题，探索构建数据基础法律制度。

中国信息通信研究院总结历年《互联网法律白皮书》的研究成果和发展历程，系统梳理过去一年国内外重要互联网立法活动，深入分析我国互联网立法的最新成果和国际互联网立法进展，对未来互联网立法工作进行了展望，形成《互联网法律白皮书（2023年）》。希望能为社会各界了解互联网领域立法最新趋势和动态提供有价值的参考。

# 目 录

一、我国网络空间法治化迈向新阶段 .....	1
二、2023 年我国互联网立法情况 .....	5
（一）网络设施安全持续强化，重点行业领域完善安全细则 .....	6
（二）数据安全与价值释放并重，数据法律规则体系全面构建 .....	8
（三）互联网平台责任逐步规范，平台发展法治环境日益优化 .....	11
（四）数字技术规则加速推进，新技术新应用发展逐步规范 .....	13
三、2023 年国际互联网立法情况 .....	15
（一）网络安全仍为立法重点，网络设施安全与发展齐驱 .....	16
（二）数据相关立法加快推进，数据资源博弈更为激烈 .....	18
（三）互联网平台立法不断完善，信息内容管理重点突出 .....	22
（四）数字技术立法显著增多，风险防范与创新发展并进 .....	25
四、互联网立法展望 .....	29
（一）健全数字经济发展制度，立改并举补齐法制短板 .....	30
（二）细化平台管理法律规则，分类分级实现精准施策 .....	32
（三）应对数字技术快速发展，加快人工智能立法进程 .....	33
（四）提前布局前沿制度研究，探索数据基础法律规则 .....	35
附录：2023 年互联网立法梳理 .....	37

## 一、我国网络空间法治化迈向新阶段

党的十八大以来，我国社会主义法治国家建设深入推进，全面依法治国总体格局基本形成，中国特色社会主义法治体系加快建设。在习近平新时代中国特色社会主义思想指引下，我国将依法治网作为全面依法治国和网络强国建设的重要内容，网络综合治理体系基本建成，网络安全保障体系和能力持续提升，网信领域科技自立自强步伐加快，网络空间法治化程度不断提高。我国坚实推进科学立法、民主立法、依法立法，大力推进互联网法律制度建设，互联网立法的系统性、整体性、协同性、时效性不断增强。2023 年 3 月，国务院新闻办公室发布《新时代的中国网络法治建设》白皮书，全面介绍了中国网络法治建设情况，分享中国网络法治建设的经验做法。目前，我国在网络设施安全防护、数据安全和数据价值释放、互联网平台规范、数字技术规范发展等方面不断出台和完善相关立法，为网络强国建设提供了坚实的制度保障。我国互联网法治建设取得历史性成就，基本形成了具有中国特色的互联网法律体系。

以网络设施安全防护为核心划定网络安全法律红线。网络设施是引领和支撑先进生产力的基础，网络设施安全特别是关键信息基础设施的安全关乎国家安全、国计民生和公共利益，是网络安全工作的重中之重。2016 年我国出台《中华人民共和国网络安全法》，作为我国网络安全领域的首部基础性、框架性、综合性法律，网络安全法确立了网络安全等级保护、关键信息基础设施安全保护、网络

信息安全等制度，奠定了我国网络安全基本制度框架。在此基础上，2021 年我国出台《关键信息基础设施安全保护条例》《网络安全审查办法》《网络产品安全漏洞管理规定》等相关立法，强化对关键信息基础设施的安全防护，并细化网络安全法律规则。此外，2019 年我国出台《中华人民共和国密码法》，明确了核心密码、普通密码及商用密码的管理要求，为提升密码管理科学化、规范化、法治化水平，保障网络和信息安全提供了重要制度支撑。

**以数据安全保障为基础构建数据领域法律规则。**数据是国家基础性战略资源，是数字经济时代新型生产要素。完善数据相关法律规则，需把握好和平衡好数据安全与数据技术创新发展的关系，同时强化保护相关主体数据权益。为在数据领域落实总体国家安全观，2021 年我国出台《中华人民共和国数据安全法》，确立数据分类分级管理、数据安全审查、数据安全风险评估、监测预警和应急处置等基本制度，并明确鼓励数据开发利用，建立健全数据交易管理制度，推进政务数据开放等发展要求，以安全保发展、以发展促安全。为规范和加强个人信息保护，2021 年我国出台《中华人民共和国个人信息保护法》，明确个人信息保护原则、个人信息处理基本规则以及个人在个人信息处理活动中享有的权利，健全个人信息保护工作机制，全面提升我国个人信息保护力度和水平。2019 年我国出台《儿童个人信息网络保护规定》，强化对儿童个人信息权益的保护。针对全球关注的跨境数据流动问题，2022 年我国出台《数据出境安

全评估办法》，明确了数据出境安全评估的具体流程和要求，为数据出境提供了具体指引。

**以互联网平台责任为依托全方位规范数字经济市场秩序。**平台经济在经济社会发展全局中地位和作用日益凸显的同时，也带来了平台企业垄断、侵犯用户个人信息等问题。为全面压实互联网平台主体责任，我国从信息内容管理、消费者权益保护、市场竞争秩序等多角度完善相关立法。我国 2011 年修订的《互联网信息服务管理办法》、2016 年出台的《中华人民共和国网络安全法》以及 2019 年出台的《网络信息内容生态治理规定》等立法进一步明确了网络信息内容传播要求和相关主体法律责任。2018 年我国出台《中华人民共和国电子商务法》，针对电子商务平台经营者明确了平等对待平台内经营者、信息安全、交易安全、消费者权益保护等法律义务。在此基础上，相关行业主管部门针对网络交易、网约车、在线旅游等平台经济出台规章，规范互联网平台在各行业领域的主体责任。2019 年、2022 年我国修订《中华人民共和国反不正当竞争法》《中华人民共和国反垄断法》，明确经营者不得利用数据和算法、技术等优势扰乱市场公平竞争秩序、排除或限制竞争。

**以数字技术管理为抓手防范新技术新应用安全风险。**数字技术是数字产业高质量发展的加速器，也是做强做优做大数字经济的核心力量。为实现数字技术规范发展，解决数字技术研发应用中存在的风险，我国针对新技术新应用加快构建相关法律制度。针对利用



电信网络技术实施诈骗的案件多发情形，2022 年我国出台《中华人民共和国反电信网络诈骗法》，从电信、金融、互联网等多层面明确打击和预防电信网络诈骗的具体要求。针对新技术新应用可能存在的传播违法信息内容、侵犯消费者权益等风险，我国出台《区块链信息服务管理规定》（2019 年）、《互联网信息服务算法推荐管理规定》（2021 年）、《互联网信息服务深度合成管理规定》（2022 年）等相关立法，明确区块链信息服务提供者、算法推荐服务提供者、深度合成服务提供者和技术支持者等相关主体在信息内容管理、用户权益保护、数据安全等方面的法律义务，筑牢数字技术应用安全屏障。

**以立法规划布局牵引互联网法治建设在保安全的基础上向促发展迈进。**2018 年，十三届全国人大常委会将电子商务法、密码法、个人信息保护法、数据安全法、反垄断法（修订）等互联网相关立法列入立法规划。五年来，我国加快推进互联网立法进程，基本完成了立法机关对于互联网立法工作的规划布局，在网络安全、数据安全、个人信息保护、互联网平台责任等方面明确管理要求，为构建网络综合治理体系提供了法治保障。我国运用法治观念、法治思维和法治手段有效应对互联网发展中的深层次问题，为我国从网络大国向网络强国迈进提供了坚实的制度保障，进一步丰富完善了中国特色治网之道，形成了丰富的理论成果、实践成果、制度成果。随着我国进入疫情后的经济恢复期，中央经济工作会议提出要大力发展数字经济，提升常态化监管水平。更好统筹发展和安全，全面

深化改革开放，大力提振市场信心。习近平总书记明确指出，要不断做强做优做大我国数字经济。对此，我国立法机关已经迅速开展相关立法规划工作，推动实现互联网由“管”到“治”的根本转变。2023 年 9 月发布的《十四届全国人大常委会立法规划》，将反不正当竞争法（修改）、网络安全法（修改）列入第一类项目“条件比较成熟、任期内拟提请审议的法律草案”，将电信法、数字经济促进法、网络犯罪防治法列入第二类项目“需要抓紧工作、条件成熟时提请审议的法律草案”，并提出就数据权属、网络治理等方面项目进行研究论证。基于此，今年，我国互联网法治建设继续顺应全球信息化发展大势，立足我国互联网发展实践，不断深化对依法治网的规律性认识，在保安全的基础上向促发展迈进，查漏补缺、完善制度、细化规则。

## 二、2023 年我国互联网立法情况

2023 年，我国互联网法治工作取得显著成效，互联网法律体系日趋健全完善。在筑牢国家网络安全、数据安全屏障，规范网络信息内容管理的基础上，我国重点突出互联网立法稳预期、利长远的作用，在创新构建数据价值释放和数据跨境制度、促进新技术新应用向上向善发展方面加快推进相关立法，为数字经济创新发展提供基础保障。在网络设施方面，继续推进网络安全法等相关上位法配套规则出台，在金融、交通等重点行业领域加强对网络设施的安全保护力度。在数据立法方面，呈现出促进数据价值释放的明显转变，

在推动数据跨境流动、促进数据产业发展、构建数据资产管理制度等方面进行创新性制度设计。在互联网平台方面，进一步细化数字市场竞争管理法律制度，针对重点平台业务出台管理要求，强化互联网平台在未成年人网络保护等方面的义务。在数字技术方面，立足技术产业发展实践出台人工智能等相关立法，促进安全与发展的动态平衡，在全球新技术法律规则制定中占据主动地位。

### **（一）网络设施安全持续强化，重点行业领域完善安全细则**

我国高度重视网络设施的安全防护和建设发展，出台《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》等明确对网络设施的安全防护要求。2023年，我国在现有立法基础上进一步细化具体制度规则，强化重点行业领域网络设施保护。

#### **1.持续完善重点网络安全制度要求**

一是细化商用密码安全管理规则。4月27日，国务院发布《商用密码管理条例（2023年修订）》，适应商用密码技术创新发展实践，明确对商用密码的管理要求，构建了“四级管理+专项管理”机制，促进密码科技创新与标准化，细化了商用密码检测认证实施要求，与《中华人民共和国电子签名法》衔接确立了电子认证商用密码管控要求，并明确商用密码进出口管制规定。9月27日，国家密码局发布《商用密码应用安全性评估管理办法》，进一步明确商用密码应

用安全性评估范围，确定商用密码应用安全性评估对象为重要网络与信息系统，并且明确了对网络和信息系使用商用密码技术、产品进行检测分析和验证评估的具体要求。

**二是优化网络安全服务认证规则。**3月15日，国家市场监督管理总局、中央网络安全和信息化委员会办公室、工业和信息化部、公安部联合发布《关于开展网络安全服务认证工作的实施意见》，明确了网络安全服务认证目录确定机制，以及对网络安全服务认证机构的资质、工作机制、信息公开等具体要求。

**三是强化网络安全事件管理。**12月8日，国家互联网信息办公室发布《网络安全事件报告管理办法（征求意见稿）》，规定了网络运营者对于较大、重大或特别重大网络安全事件进行报告的报告时间、报告内容等要求，并规定网络安全事件处置后需进行全面分析总结并进行上报，同时明确了运营者的法律责任。

## 2.重点行业出台网络安全实施细则

**金融、交通等重要行业领域结合行业监管现实情况出台网络安全具体规则。**2月27日，证券监督管理委员会发布《证券期货业网络和信息安全管理办法》，明确证券期货业网络和信息安全管理监督体系、网络和信息安全运行、投资者个人信息保护、网络和信息安全应急处置、关键信息基础设施安全保护等要求。6月8日，交通运输部发布《公路水路关键信息基础设施安全保护管理办法》，在《关键信息基础设施安全保护条例》基础上进一步细化公路水路关键信

息基础设施认定方法、运营者责任义务、风险隐患应急处置、事前事中事后监管等内容，提升了公路水路关键信息基础设施安全保护和监督管理水平。12月18日，工业和信息化部发布《民用无人驾驶航空器生产管理若干规定》，从唯一产品识别码、无线电发射设备型号核准、电信设备进网许可、网络与数据安全、产品信息备案等方面明确了对民用无人驾驶航空器的管理要求。

## （二）数据安全与价值释放并重，数据法律规则体系全面构建

数据作为新型生产要素，是数字化、网络化、智能化的基础。数据基础制度建设事关国家发展和安全大局。2022年底，我国发布《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》，从数据产权、流通、交易、使用、分配、治理、安全等角度提出构建有利于数据安全保护、有效利用、合规流通的数据基础制度。过去一年，我国在维护国家数据安全、保护个人信息的基础上，进一步健全数据出境规则，探索构建数据基础制度为数据价值释放提供合法依据。

### 1. 构建中国特色数据跨境流动规则体系

一是制定个人信息出境标准合同规范。2月22日，国家互联网信息办公室出台《个人信息出境标准合同办法》，细化通过标准合同向境外提供个人信息的场景，明确了个人信息保护影响评估的评估

要素，并规定了个人信息处理者对个人信息出境标准合同进行备案的要求。解决了中小型数据出境安全问题，为企业数据安全高效流通新增路径。

**二是探索为企业数据跨境流动“减负”立法。**9月28日，国家互联网信息办公室发布《规范和促进数据跨境流动规定（征求意见稿）》，规定了无需申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的情形，从“例外规定”视角进一步完善了数据出境法律制度，更精准地适配数据出境具体场景，减轻企业在数据出境中的合规压力，是我国促进数据合法有序跨境流动的积极尝试。

## 2. 构建重点领域数据安全要求

**一是工业和信息化领域加快推进数据安全管理办法实施细则出台。**1月1日，《工业和信息化领域数据安全管理办法（试行）》正式实施，确定了工业和信息化领域数据分类分级管理、重要数据识别与备案相关要求。针对不同级别的数据，在数据处理全生命周期的不同环节规定相应安全管理和保护要求。10月9日，工业和信息化部发布了《工业和信息化领域数据安全风险评估实施细则（试行）（征求意见稿）》，明确工业和信息领域重要数据和核心数据处理者开展数据安全风险评估的评估内容、评估期限、评估方式、评估报送等具体要求，为相关数据处理者开展数据安全风险评估提供了实践指引。11月23日，工业和信息化部公开征求对《工业和信息化领域数据安

全行政处罚裁量指引（试行）（征求意见稿）》的意见，对工业和信息化领域数据安全行政处罚管辖规则、处罚情形、裁量权适用规则等进行了具体规定，进一步提升数据安全相关立法的实施效果。

**二是金融领域细化数据安全具体要求。**7月24日，中国人民银行发布《中国人民银行业务领域数据安全管理办法（征求意见稿）》，明确中国人民银行业务领域数据定义，确定了数据分级分层的标准及划分级别，针对数据收集、存储、使用、加工、传输、提供、公开和删除各环节明确数据安全保护要求，细化风险监测、评估审计、安全事件处置等制度规则。

### 3. 加快推进数据要素市场依法依规构建

**一是促进数据产业规范发展。**1月3日，工业和信息化部、国家互联网信息办公室、国家发展和改革委员会、教育部、科学技术部、公安部、国家安全部、财政部等十六部门联合发布《促进数据安全产业发展的指导意见》，要求提升数据安全产业的创新能力，加强核心技术攻关，构建数据安全产品体系等，壮大不同类型的数据安全服务，推广网络安全技术产品应用。

**二是探索构建数据资产“入表”制度。**8月21日，财政部发布《企业数据资源相关会计处理暂行规定》，要求企业根据数据资源的持有目的、形成方式、业务模式，以及与数据资源有关的经济利益的预期消耗方式等，对数据资源相关交易和事项进行会计确认、计量和报告。在不改变现行企业会计准则的基础上，在资产负债表中

的“存货、无形资产、开发支出”三个项目下增设“数据资源”子项目，并对数据资源相关会计信息进行披露。

### **（三）互联网平台责任逐步规范，平台发展法治环境日益优化**

互联网平台在支持创新、促进增长、扩大需求、就业创业等方面发挥引领作用，是经济新旧动能转换和产业结构升级的有力引擎。2022 年底中央经济工作会议提出，支持平台企业在引领发展、创造就业、国际竞争中大显身手。今年以来，我国在数字市场竞争监管、网络社会管理等方面强化互联网平台主体责任，并在重点领域细化对互联网平台的管理要求。

#### **1. 强化未成年人网络权益保护**

**出台未成年人网络保护专门立法。**10 月 16 日，国务院发布《未成年人网络保护条例》，构筑了覆盖未成年人参与网络活动全链条，涵盖家庭、学校、社会、政府等多主体的网络保护体系。在网络素养促进方面，规定了政府、学校、监护人等各方主体在培育未成年人网络素养方面的责任；在网络信息内容规范方面，按照内容管理“三分法”的思路，对正能量信息、违法信息和不适宜未成年人接触的信息分别明确管理要求；在未成年人个人信息网络保护方面，明确未成年人个人信息权益的行使方式，夯实未成年人个人信息保护制度基础；在网络沉迷防治方面，对应援集资、投票打榜等诱导



未成年人沉迷网络、非理性消费的活动进行专门规范，对网络游戏、网络直播等重点应用的防沉迷规则提出细化要求。

## 2. 针对网络信息内容管理突出问题重点规范

**加快推进网络暴力规制进程。**7月7日，国家互联网信息办公室发布《网络暴力信息治理规定（征求意见稿）》，明确了网络暴力信息的定义，规定网络信息服务提供者需承担网络信息内容管理主体责任，对网络暴力信息进行监测预警、及时处置，并完善对用户的网络暴力保护机制。9月25日，最高人民法院、最高人民检察院、公安部联合发布《关于依法惩治网络暴力违法犯罪的指导意见》，对网络诽谤、网络侮辱、侵犯公民个人信息等网络暴力违法犯罪的具体情形、法律适用、定罪处罚考量等进行规定，提升网络暴力综合治理能力。

## 3. 配套出台数字市场反垄断规则

**出台实施细则配套落实反垄断法最新要求。**3月10日，为适应平台经济发展需求、提升数字平台竞争活力，国家市场监督管理总局发布《禁止垄断协议规定》《禁止滥用市场支配地位行为规定》《经营者集中审查规定》三部部门规章，明确对互联网平台垄断行为监管的具体要求。《禁止垄断协议规定》明确界定平台经济领域相关商品市场界定方法，禁止利用平台规则等达成垄断协议；《禁止滥用市场支配地位行为规定》结合平台经济特点明确认定平台经济领域经

营者具有市场支配地位的考量因素，并具体规定平台经济经营者滥用市场支配地位的具体要求；《经营者集中审查规定》明确了平台附加限制性条件减少对竞争不利影响的具体情形。6月25日，国家市场监督管理总局发布《禁止滥用知识产权排除、限制竞争行为规定》，对经营者滥用知识产权排除、限制竞争的行为进行规制，明确了知识产权领域相关市场认定方法，认定排除、限制竞争行为考虑因素。

#### 4. 细化重点领域平台管理要求

**重点民生领域强化互联网平台责任规范。**2月25日，国家市场监督管理总局发布《互联网广告管理办法》，提出互联网平台经营者在提供互联网信息服务过程中应防范、制止违法广告，并遵守记录保存用户真实信息，对违法广告进行监测、排查等义务。3月3日，国家药监局发布《化妆品网络经营监督管理办法》，明确化妆品电子商务平台经营者承担对平台内化妆品经营者进行管理的责任，包括实名登记、日常检查、违法行为处置等。

### **（四）数字技术规则加速推进，新技术新应用发展逐步规范**

近年来，数字技术创新和迭代速度明显加快，在提高社会生产力、优化资源配置的同时也带来一些新问题新挑战。过去一年，我国针对人工智能等新技术新应用带来的风险问题加快立法应对，为数字技术规范和创新提供了基本遵循。

## 1. 针对重点类型人工智能及时立法

针对重点人工智能技术应用明确管理要求和发展原则。1 月 10 日，国家互联网信息办公室、工业和信息化部、公安部联合制定的《互联网信息服务深度合成管理规定》正式实施，明确了对应用深度合成技术提供互联网信息服务的具体要求，构建了深度合成内容管理、训练数据管理以及对深度合成信息内容添加标识等具体制度。7 月 10 日，国家互联网信息办公室联合国家发展和改革委员会、教育部、科学技术部、工业和信息化部、公安部、国家广播电视总局发布《生成式人工智能服务管理暂行办法》，明确了生成式人工智能服务的基本概念，提出鼓励生成式人工智能创新应用，生成积极健康、向上向善的优质内容。同时，对生成式人工智能服务提供者的数据处理活动、保护服务使用者个人信息、及时处置违法内容等义务进行明确。

## 2. 探索构建科技伦理审查规则

以科技伦理审查构建数字技术风险事前防范制度。10 月 8 日，科学技术部、教育部、工业和信息化部、农业农村部、国家卫生健康委员会、中国科学院、中国社科院、中国工程院、中国科学技术协会、中央军事委员会科学技术委员会十部门联合发布《科技伦理审查办法（试行）》，落实科技伦理审查主体责任，明确需进行科技伦理审查的科技活动范畴，并对科技伦理审查的一般程序、简易程序、专家复核程序等进行具体规定。旨在规范科学研究、技术开发

等科技活动的科技伦理审查工作，强化科技伦理风险防控，促进负责任创新。

### 3. 针对重点类型新技术强化规制

**强化对高风险数字技术的管理要求。**5月31日，国务院、中央军委委员会发布《无人驾驶航空器飞行管理暂行条例》，明确对无人驾驶航空器、操控员及空域和飞行活动的管理要求。6月6日，国家互联网信息办公室就《近距离自组网信息服务管理规定（征求意见稿）》公开征求意见，对近距离自组网信息服务提供者、使用者的责任义务进行明确，要求服务提供者采取必要的安全管理制度和技术措施，依法处置违法信息，防范和抵制不良信息传播，保存有关记录并进行报告。8月8日，国家互联网信息办公室就《人脸识别技术应用安全管理规定（试行）（征求意见稿）》公开征求意见，重点规定了人脸识别技术的使用原则，禁止使用人脸识别技术的情形，限定使用人脸识别技术的场景，强化对人脸信息的保护。

## 三、2023 年国际互联网立法情况

2023 年，百年未有之大变局纵深演进，全球局势复杂多变，人工智能、大数据等新技术快速发展助推人类进入科技新时代，全球治理体系处于调整变革的关键时期，全球互联网立法也展现新趋势新动向。在继续强化网络设施安全防护、个人信息保护等传统互联网立法的同时，世界主要国家和地区着力以立法保障国内发展、强化国际竞争。在网络设施方面，在强调安全防护的基础上，多国在

立法和国家战略中强调促进新型基础设施建设发展。在数据立法方面，构建完善数据跨境流动管理规则，强化国际合作。在互联网平台方面，多国通过立法明确互联网平台对于网络信息内容管理、特殊群体网络权益保护的法律责任，加强对互联网信息内容管理和干预。在数字技术方面，人工智能成为今年国际立法热点，主要国家和地区加快推进人工智能立法，试图抢占全球核心规则主导权。

### （一）网络安全仍为立法重点，网络设施安全与发展齐驱

网络设施是数字经济发展的基石，是引领产业变革升级的结构性力量。今年，以美欧为代表的主要国家和地区强化网络设施安全顶层制度设计，通过发布网络设施相关国家战略、加快网络安全立法等方式强化网络设施安全防护，促进先进网络设施发展升级。

#### 1. 加强网络设施安全顶层制度设计

出台或修订相关立法、国家战略强调网络设施安全防护。1月13日，《关于在欧盟实现高度统一网络安全措施的指令》（NIS2 指令）正式生效。NIS2 指令明确了监管框架运作的最低规则、成员国主管当局之间有效合作的机制，并更新了受网络安全义务约束的部门和实体类型，还通过提供有效的补救措施和执法措施确保成员国执行指令。3月2日，美国白宫发布《网络安全战略》，将网络安全的责任从个人、小企业和地方政府转移到最有能力为所有人降低风险的组织；重新调整激励措施以支持网络安全领域长期投资；以协调的

方式使用“国家力量的所有工具”，加强在网络安全领域公私合作。4月18日，欧盟发布《欧盟网络团结法案》，促进欧盟成员国间网络安全事件和漏洞信息共享，增强欧盟整体应对网络风险能力。6月14日，德国政府通过《国家安全战略》，提出“整合安全”概念，将国家的内部安全和外部安全威胁进行整体考量。7月7日，日本总务省发布《2023年信息通信网络安全综合措施》（草案），旨在确保信息通信网络的安全性和可依赖性、提高对网络攻击的应对能力，强调公私协作，确保安全的网络空间。7月13日，美国白宫发布《国家网络安全战略实施计划》，详细阐述了相关政府部门在确保美国网络安全方面的举措和要求，并设定具体时间节点，激励关键基础设施投资。7月19日，欧洲议会工业、研究和能源委员会通过《网络弹性法案》，对数字产品提出了多方面网络安全要求，旨在以统一的法律框架来规制欧盟的网络安全问题。7月26日，巴基斯坦联邦内阁批准了《2023年电子安全法案》，旨在防止网络骚扰、网络欺凌、勒索等网络犯罪，并计划设立新的监管机构“电子安全管理局”，负责注册和监控网站、网络频道、YouTube频道和媒体公司现有网站。

## 2. 完善促进先进网络设施建设制度

**强调促进先进网络设施的发展。**2月23日，欧盟委员会通过了《千兆基础设施法案》的提案，以替代《宽带成本降低指令》，旨在减少与部署千兆网络相关的成本和管理负担，简化许可程序，并要求所有新建或翻修的建筑物都应配备光纤，保证运营商可以更低的

成本、更高效地部署网络。4月12日，英国新成立的科学、创新和技术部发布《英国无线基础设施战略》，提出为英国无线基础设施投资提供政策保障。7月12日，迪拜启动《迪拜网络安全战略》第二阶段，提出通过人才培养和促进战略伙伴关系加强数字基础设施，增强自身数字防御能力。

## （二）数据相关立法加快推进，数据资源博弈更为激烈

数字经济时代背景下，数据成为驱动各国经济发展的关键生产要素。2023年，世界主要国家和地区在强化本国个人数据保护立法的同时，加快完善数据跨境流动规则，通过立法、国际合作的方式促进数据合法流动。

### 1. 数据跨境流动立法和国家合作不断加强

一是在国内立法中明确数据跨境流动规则。1月，白俄罗斯个人数据保护中心签署了一项个人数据跨境转移规则的命令，该命令将欧亚经济联盟（EEU）成员国列入“为跨境数据传输提供适当保护的外国名单”，并明确了可将白俄罗斯国内数据转移到被认为没有提供充分性保护水平的国家的具体情形。4月24日，以色列议会的宪法、法律和司法委员会通过了《隐私保护条例（关于将信息从欧洲经济区转移到以色列的说明）》草案，明确了根据要求删除数据、删除多余的个人信息、保持个人数据的准确性以及通知数据已传输的义务等规定。8月11日，印度发布《数字个人数据保护法》，其中修

改了有关数据传输的条款，将原法案规定的仅在中央政府进行必要因素评估后通知数据受托人方可个人数据出境的规定，改为中央政府可通知限制相应个人数据出境。10月27日，泰国个人数据保护委员会根据《2019年个人数据保护法》第28条和第29条发布了两部跨境数据传输法规草案，要求数据接收方制定个人数据保护标准，并规定了在关联企业或同一企业跨国传输个人数据的相关要求。10月16日，韩国个人信息保护委员会通过《个人信息境外转移及运用规定》，规定了个人信息跨境转移评估咨询机构海外转移专家委员会运作要求，新增了个人信息向境外转移的程序及评估标准。11月，英国发布《数据保护和数字信息法案》第二次修订案，创新性规定满足英国政府的“数据保护测试”即可将英国个人数据转移至其他国家和国际组织，并认可法案生效前已经合法进行的国际贸易和数据跨境流动。

**二是通过双边、多边协议促进数据跨境流动。**4月4日，日本与欧盟结束充分性认定的首次审查，审查表明欧盟和日本的数据保护框架之间的趋同程度越来越高，并且该协议运作良好。5月24日，欧盟和东盟发布《东盟示范合同条款和欧盟标准合同条款的联合指南》，为相关公司提供了数据跨境最佳实践指引，在满足两个司法管辖区合法性要求的基础上促进数据跨境流通。7月10日，欧洲议会通过了“欧盟-美国数据隐私框架”充分性决定，明确个人数据从欧盟传输至美国企业时，美国企业不再需要采取充分性决定要求以外



的安全措施。

## 2. 个人信息保护立法进入纵深推进阶段

一是推进个人信息保护立法出台和修订。3月8日，韩国通过了《个人信息保护法》修正案，修订内容包括统一线下和线上业务的数据保护规则、降低处理个人信息的要求、引入跨境数据流动新规则等。4月，法国批准了欧洲委员会《第108+号公约》，进一步加强对数据主体权利保护，并将自动化决策等新技术应用纳入其规制范畴。4月17日，越南颁布《个人数据保护法》，并于2023年7月1日正式生效，该法规定了数据主体的权利与同意机制、数据保护影响评估以及跨境数据传输等多方面制度。8月11日，印度正式发布《2023年数字个人数据保护法》，该法明确将“数字个人数据”作为规制对象，确立了处理数字个人数据的合法性基础，阐明了数据受托人确保数据准确、防止数据泄露等义务，赋予了数据委托人知情权、更正删除权、申诉权等权利。11月，英国政府公布《数据保护和数字信息法案》第二次修订案，完善个人数据定义，增加个人数据处理合法性依据，并对电子营销、自动化决策中使用个人数据明确具体要求。

二是出台个人信息保护立法实施细则。2月24日，欧盟数据保护委员会发布《通用数据保护条例》（GDPR）第3条和第5章数据跨境条款的应用指南、向社交媒体用户建议如何识别欺骗性设计的指南、认证作为数据跨境工具的指南，进一步细化个人信息保护相

关规则。3 月，西班牙数据保护机构发布《设计隐私及默认隐私指南》，明确个人信息保护的相关要求。3 月 28 日，欧洲数据保护委员会发布了有关个人数据泄露的最新指南，更新了非欧盟机构在发生数据泄露时的通知要求。8 月 31 日，瑞士联邦数据保护和信息专员发布数据保护影响评估的信息表单，规定如果数据处理可能对数据当事人的人格或基本权利造成高风险，则必须进行数据保护影响评估。

**三是加快重点领域、新兴领域个人信息保护立法进程。**4 月 27 日，美国华盛顿州通过《我的健康，我的数据法案》，为健康数据提供更高级别的保护，引入额外的数据披露要求，授予个人删除其健康数据的权利，并禁止出售个人健康数据等。6 月 1 日，俄罗斯国家杜马一读通过了《行政犯罪法》修正草案，明确了关于违法使用生物识别数据的法律责任，最高罚款可达 700 万卢布。6 月 5 日，日本总务省和经济产业省发布《医疗信息处理信息系统和服务提供者安全管理指南 1.1 版（草案）》并征求意见，强化医疗信息的安全管理。10 月 3 日，英国信息专员办公室发布在工作场所进行合规透明监控的指南，呼吁雇主在工作场所实施任何监控之前需考虑其法律义务及员工权利，所有监控都必须符合英国数据保护法要求。

### 3.探索促进数据共享流通相关立法

**以技术、规则等手段促进数据共享流通。**3 月 31 日，美国白宫科技政策办公室发布《促进数据共享与分析中的隐私保护国家战略》，提出在数据的分析与共享中通过隐私增强技术加强对隐私的保护，

促进数据潜力释放，以技术手段推动公共和私营部门数据共享。11月9日，欧洲议会通过《数据法案》，下一步需要欧洲理事会批准后正式成为法律。《数据法案》旨在明确数据访问、共享和使用的规则，规定获取数据的主体和条件，使更多私营和公共实体能够共享数据。该法案明确了使用联网产品或相关服务（如物联网、工业机械）产生的数据进行共享的具体规则。规定了获取数据的主体和条件，还规定了云服务提供商之间进行转换的规则，并引入了防止这些公司进行非法国际数据传输的保障措施。11月15日，韩国发布《国家研究数据管理及促进利用法案》，该法案通过构建集中管理等制度促进国家研究数据充分利用和共享。

### **（三）互联网平台立法不断完善，信息内容管理重点突出**

互联网平台是数字经济时代维护数字市场秩序、规范新业态新模式的重要着力点。过去一年，国外继续推进对于互联网平台特别是超大型互联网平台企业的规制，重点强化互联网平台对网络信息内容的管理义务。

#### **1.通过立法明确互联网平台网络信息内容管理义务**

一是欧盟《数字服务法》配套规范进一步强调互联网平台网络信息内容管理义务。2月1日，欧盟发布《数字服务法》指南，指导协助企业遵守相关报告义务。4月25日，欧盟委员会划定第一批《数字服务法》中的“超大型在线平台和在线搜索引擎”，包括阿里巴巴

速卖通、亚马逊商城、苹果应用商店、脸书等 17 个超大型在线平台，以及必应和谷歌搜索 2 个超大型在线搜索引擎。从被指定之日起，这些公司必须在四个月内完成对《数字服务法》规定的全套义务的合规，包括通过指定的评估机构进行服务评估、减轻系统性风险和提供强大的网络信息内容审核工具来赋能和保护在线用户等。5 月 5 日，欧盟委员会就《数字服务法》中的独立审计规定展开了公共咨询，涉及选择审计方法和程序时应适用的主要原则，并为超大型在线平台和在线搜索引擎的审计细化规则。10 月 9 日，欧盟委员会发布《数字市场法》下超大型在线平台和在线搜索引擎合规报告模板，规定报告应“详细和透明地”披露相关信息，并在指定后六个月内提交，每年更新一次。10 月 20 日，欧盟委员会发布了有关《数字服务法》中超大型在线平台和在线搜索引擎审计报告的法律框架，包括选择独立审计师的程序和审计方法。

**二是美国加快推进网络信息内容管理立法。**3 月 9 日，美国参议院司法小组委员会达成一致，要求修改《通信规范法》第 230 条，强调平台对网络信息内容的管理责任，以保护儿童免遭网络有害内容侵害。7 月 5 日，美国联邦法官发布禁令，限制拜登政府与社交媒体平台就网络信息内容进行干预，以回应路易斯安那州和密苏里州司法部长在一项诉讼中提出的，美国政府在 COVID-19 疫情言论方面过度干预社交媒体。10 月 20 日，美国最高法院最终取消了前述对联邦政府与社交媒体公司进行沟通的限制，允许政府部门就网络信

息内容审核问题和其他事项与社交媒体平台进行沟通。

三是英国通过《在线安全法》区分不同类型在线服务提供者的网络信息内容管理义务。10月26日，英国《在线安全法》正式通过。

《在线安全法》将互联网服务划分为用户对用户服务（User-user Service）和搜索服务（Search Service）两类，规定两类服务提供者都要承担非法内容风险评估、儿童风险评估等义务。用户对用户服务提供者要承担更严格的内容安全责任，不仅需减少非法和对儿童有害的内容，还需就网络信息内容对成年人的风险进行评估，同时需保护专业性的新闻内容及具有民主价值的内容。

## 2. 重点加强对儿童等特殊群体的网络保护

一是立法强调互联网平台对儿童的保护义务。8月11日，印度《数字个人数据保护法》对18岁以下儿童提出了儿童隐私和年龄验证要求。10月26日，英国《在线安全法》对儿童风险评估义务以及相应的儿童安全保护义务进行了专门规定，对“可能被儿童访问的用户对用户服务”和“可能对儿童产生伤害的内容”进行了定义，规定互联网平台必须向国家犯罪署报告他们在其平台上发现的儿童性剥削和性虐待内容，并加大对向未成年人提供不良信息的网站的惩罚力度。

二是细化未成年人个人数据收集、使用规则。4月17日，爱尔兰数据保护委员会发布了4份儿童数据保护的指南，指南概述了儿童数据保护基本原则，包括需要父母同意才能处理儿童数据，对父

母保护儿童数据的具体建议等。6月29日，法国国家信息与自由委员会发布了有关互联网接入家长控制的两项决定，规定某些社交媒体应用程序禁止13岁以下儿童使用，要求强制性功能不得超出目的收集儿童数据。9月26日，美国和英国发布关于打击儿童性虐待和性剥削的联合声明，加强两国在打击剥削和虐待儿童方面的合作。

#### （四）数字技术立法显著增多，风险防范与创新发展并进

2023年，以ChatGPT为代表的生成式人工智能正在引发新一轮人工智能革命。生成式人工智能在助力创新发展的同时，也带来了虚假信息传播、版权保护、劳动代替等风险和问题，引发全球热议。今年，主要国家和地区根据人工智能发展情况及面临问题，持续制定、发布人工智能相关立法、政策、指南，呈现出适应产业发展、软硬手段协同、重点领域规制等趋势特点。

##### 1. 全球探索推进人工智能法律规则

一是美欧推进人工智能立法进程。10月30日，美国总统拜登签署发布《安全、稳定、可信的人工智能行政令》，聚焦人工智能对关键基础设施以及化学、生物、放射性、核和网络安全的威胁，提出制定专门标准和实践指南。要求开发对国家安全、国家经济安全或国家公共健康和安全构成严重风险的基础模型的公司向美国政府共享相关数据。提出扩大多双边合作、开发国际标准等，以确保美国在人工智能领域的全球领导力。12月8日，欧盟理事会、欧洲议会

和欧盟委员会就《人工智能法案》达成临时协议。欧盟《人工智能法案》将人工智能系统划分为低风险、高风险、不可接受风险、有限风险等不同等级。绝大多数人工智能系统都属于风险最小的类别，不做过多干预。被确定为高风险的人工智能系统将需要遵守建立数据管理制度、制定技术文件、留存记录等要求。被认为对人类基本权利构成明显威胁的人工智能系统将被禁止。《人工智能法案》对通用人工智能模型引入透明度要求，并规定可能构成系统性风险的通用人工智能模型需承担管理风险和监控严重事件、模型评估和对抗性测试等义务。此外，法案开发了促进创新的工具，除了监管沙盒之外，还同意在真实条件下测试高风险人工智能系统。

**二是多国出台人工智能官方文件。**3月15日，英国信息专员办公室更新了《人工智能数据保护指南》，涉及法律责任、透明度及合法性等内容，旨在支持英国政府对人工智能采取创新监管。4月3日，英国信息专员办公室发布了《生成式人工智能使用指南》，概述了英国将关注的八个具体领域，包括个人信息处理的合法性基础、是否经过数据保护影响测试、透明度责任、安全性保障措施等。5月25日，新西兰隐私专员办公室发布《生成式人工智能指南》，规定了企业及相关组织以尊重个人隐私的方式参与人工智能建设的相关要求。7月14日，加拿大网络安全中心发布了《生成式人工智能指南》，详细介绍了与使用生成式人工智能相关的风险，包括数据隐私问题、有偏见的内容、错误信息和虚假信息。10月16日，法国国

家信息与自由委员会发布《关于创建数据集以开发人工智能系统的操作指南》，将帮助专业人士协调创新与个人权利保护之间的关系。

**三是就人工智能规则推进国际合作。**9月9日，二十国集团(G20)提出建设由成员国和其他国家自愿共享的数字公共基础设施虚拟库，各成员国的领导人再次承诺就人工智能和隐私问题开展合作。10月，东盟拟发布《人工智能伦理与治理指南》，要求企业考虑各国的文化差异，自行确定最有效的应对措施，预计将于2024年1月底东盟数字部长会议期间定稿。10月30日，七国集团发布《广岛人工智能进程》，强调充分利用生成式人工智能带来的机遇，打造以人类为中心、包容的人工智能治理框架。11月1日，英国召开首届全球人工智能安全峰会，包括中国在内的28个国家和欧盟签署《布莱切利宣言》，承诺以安全、以人为本、值得信赖和负责任的方式设计、开发、部署和使用人工智能。11月21日，美国、英国、法国、德国、日本等45国共同启动实施《关于负责任地军事使用人工智能和自主技术政治宣言》，将围绕负责任地军事使用建立国际共识，指导各国开发、部署和使用军事人工智能。11月27日，由英国国家网络安全中心牵头，包括美国在内的18个国家共同参与制定了《安全人工智能系统开发指南》，从安全设计、安全开发、安全部署和安全运维四个关键领域提供了提高人工智能系统安全性的建议，为人工智能系统开发者在开发过程每个阶段强化网络安全要求提供了指引参考。

## 2.以立法抢占高技术领域竞争优势



一是推出芯片技术产业促进型立法。4 月 21 日，韩国国会通过《软件振兴法》部分修正案，强化软件影响评估体系以培育商业软件产业。9 月 21 日，《欧洲芯片法》正式生效，制定了一整套措施，强化欧洲芯片生产能力，建立芯片设计生态系统并支持芯片产业链创新，同时规定了危机监测和紧急应对机制。

二是在立法中明确对中国芯片产业实施歧视性打压。5 月 23 日，日本经济产业省正式公布了《外汇法》法令修正案，将先进芯片制造所需的 23 个品类的半导体设备列入出口管理的管制对象。9 月 22 日，美国商务部发布《芯片与科学法》中“护栏条款”最终规则，禁止企业在获取美国联邦政府的补贴后提高其在中国境内的特定半导体设施的产能，或与中国实体进行涉及特定先进半导体的合作研发或技术许可活动，迫使芯片行业领先企业在美国补贴与中国市场之间“选边站”，以进一步削弱中国先进半导体的产能及研发能力。10 月 17 日，美国商务部工业和安全局发布修订的《先进计算和半导体制造设备出口管制规则》，对涉华先进计算芯片和半导体行业的出口管制措施进一步升级，新规要求英伟达在内的美国半导体公司不得再向中国供应 A800 和 H800 等先进计算芯片、芯片制造设备和其他产品，全面遏制中国获取先进计算芯片。

### 3. 加大对数字技术风险的防范力度

一是强化网络诈骗打击力度。4 月 12 日，美国联邦贸易委员会发布新规则加大骚扰电话整治力度，与联邦通信委员会合作开展“网

关禁入”计划，重点打击海外诈骗者和冒名顶替者。6月1日，俄罗斯国家杜马一读通过《俄罗斯联邦行政犯罪法》修正案，规定对未在其网络上安装监控系统的电信运营商进行罚款。8月，波兰通过了新法规《打击电信滥用法》，以打击垃圾邮件和网络钓鱼等行为。

二是针对新技术新应用明确管理要求。6月1日，法国通过“网红”行业监管法案，打击误导性或欺骗性商业行为在互联网上的蔓延，违法者最高可面临两年监禁和30万欧元罚款。6月29日，美国蒙大拿州《政府使用面部识别法》生效，对警察使用面部识别使用技术产品进行全面规范。禁止“持续的”面部识别，允许执法部门使用该技术搜寻涉及“严重犯罪”案件的嫌疑人、受害者或证人。

#### 四、互联网立法展望

当前，新一轮科技革命和产业变革正在重构全球创新版图、重塑全球经济结构，数字技术全面融入人类经济、政治、文化、社会、生态文明建设各领域和全过程，给人类生产生活带来广泛而深刻的影响。抢抓数字经济发展先机，大力推动数字经济和实体经济深度融合，对于推动高质量发展、全面建设社会主义现代化国家具有重大意义。当前，我国数字经济蓬勃发展，数字经济作为经济“稳定器”与“加速器”的作用愈发凸显。而越是快速发展，越需要加强法律的规范和引导。我国需进一步健全数字经济和互联网法律法规，提高我国数字经济治理体系和治理能力现代化水平，以法治护航数字经济行稳致远。

党的二十大报告强调，要“加强重点领域、新兴领域、涉外领域立法，统筹推进国内法治和涉外法治，以良法促进发展、保障善治。推进科学立法、民主立法、依法立法，统筹立改废释纂，增强立法系统性、整体性、协同性、时效性”。法治是互联网治理的基本方式，运用法治观念、法治思维和法治手段推动互联网发展治理，已经成为全球普遍共识。下一步，要立足全球数字经济发展大势和我国网络空间法治实践，充分考虑我国经济社会发展阶段、数字技术发展演进最新趋势和数字市场竞争态势，进一步提高网络综合治理效能，构建适应数字经济和实体经济融合发展的法律体系。继续筑法治之基、行法治之力、积法治之势，在法治领域深刻践行“以安全保发展，以发展促安全”的要求，进一步健全网络法治体系，以高质量立法推动高质量发展。

### **（一）健全数字经济发展制度，立改并举补齐法制短板**

随着互联网对经济生活融入程度的不断加深，互联网立法广度和深度也在逐渐拓展。党的十八大以来，为应对互联网技术和业务的快速发展，参与数字领域国际竞争，我国互联网立法工作加快推进，互联网法治体系日益完备。但我国互联网立法在尊重和回应数字经济发展内在规律，平衡发展与监管的双重价值，应对新技术新应用带来的新问题等方面仍存一定局限。进入全面建设社会主义现代化国家新征程，互联网立法需顺应数字经济发展趋势，加紧补齐法律制度和规则短板，围绕促进数字经济发展、强化网络设施安全

发展等主题加快完善互联网法律规范体系，发挥法治固根本稳预期利长远的作用。

**专门立法制定和传统立法修订协同推进，为数字经济发展营造良好的法治环境。**一是通过促进型立法为数字经济发展提供法治保障。促进型立法是介于管理型立法和政策之间的一种新型立法，它有效地弥补了管理型立法“过刚”以及政策“过柔”的局限性。当前，我国数字经济发展中还存在核心技术受制、产业基础保障不足、产业数字化转型不平衡等问题，亟需通过相关立法巩固已有发展成果，探索创新发展路径。《十四届全国人大常委会立法规划》已经将数字经济促进法列为需要抓紧工作、条件成熟时提请审议的法律草案类型。下一步可以以全国人大常委会的立法规划为契机，立足我国数字经济和互联网发展实践，借鉴各地在促进数字经济发展方面的立法经验，加快推进数字经济促进法制定出台，考虑从数字设施、数据要素、数字技术、数字化转型等多方入手，解决数字经济发展障碍，促进数字技术和产业发展。**二是健全网络设施安全发展法律制度。**当前新一轮科技革命和产业变革加速演进，世界各国纷纷把推进网络基础设施建设作为实现创新发展的重要动能，不断激活新应用、拓展新业态、创造新模式。我国以《中华人民共和国网络安全法》《关键信息基础设施安全保护条例》等相关立法构建了网络设施安全防护法律制度。下一步，亟需从网络设施建设和发展目标出发，加快推进《电信法》等网络设施基础立法的制定出台，为我国

新一代信息通信基础设施建设提供法制保障。三是修订与数字经济发展相关的传统立法。数字经济的不断发展对传统法律规则造成挑战，特别是重点行业领域强化安全准入要求，而新技术新模式在开发应用中也存在安全风险和挑战，导致部分新技术新模式研发应用因合法性依据不足而阻滞发展创新。例如《中华人民共和国道路交通安全法》尚未明确对自动驾驶车辆的规制要求，而传统车辆测试、机动车拼装改装以及驾驶证照等规定无法适用于自动驾驶车辆，在一定程度上对自动驾驶技术和产业发展造成阻碍。我国需加快推进道路交通安全法等传统立法的修订进程，在技术产业发展成熟过程中不断完善和细化适应数字经济发展要求的法律规则。

## （二）细化平台管理法律规则，分类分级实现精准施策

互联网平台是数字经济活动的组织者和协调者，是数字经济和实体经济融合发展的关键环节。近年来，我国不断丰富发展互联网平台管理规则，强化互联网平台特别是超大型互联网平台的主体责任，在数字市场不正当竞争和反垄断监管、网络信息内容管理、个人信息保护等多领域强化对互联网平台的规范要求，相关法规政策实施效果显著，互联网平台相关专项行动接近尾声。同时，面临疫情后我国经济恢复的基础尚不牢固，外部环境动荡不安等发展挑战，我国提出充分释放平台经济的创新引领作用，以透明、可预期的常态化监管实现规范发展。2023 年 7 月，李强总理在“平台企业座谈会”上指出，各级政府要着力营造公平竞争的市场环境，完善投资

准入、新技术新业务安全评估等政策，健全透明、可预期的常态化监管制度。2023年7月19日，我国发布《中共中央 国务院关于促进民营经济发展壮大的意见》，提出加强监管标准化规范化建设，依法公开监管标准和规则，增强监管制度和政策的稳定性、可预期性。

未来，我国可适时修订互联网平台相关立法，以立法保障平台企业在引领发展、创造就业、国际竞争中发挥积极作用。一方面，完善互联网平台分类分级制度，识别核心互联网平台服务，细化超大型互联网平台划分标准，并在网络市场监管、网络信息内容管理、消费者保护等领域区分超大型互联网平台和一般互联网平台的权利义务。另一方面，加大对中小型互联网平台的倾斜保护，加快出台小型个人信息处理者个人信息保护规则，并考虑在网络安全、数据安全等相关立法中增加对中小微企业进行法律义务豁免或减轻的相关规定。

### **（三）应对数字技术快速发展，加快人工智能立法进程**

当今世界，信息技术创新日新月异，数字化、网络化、智能化深入发展，人工智能在推动经济社会发展、促进国家治理体系和治理能力现代化、满足人民日益增长的美好生活需要方面发挥着越来越重要的作用。人工智能产业在创新发展过程中存在科技伦理、侵权归责、知识产权垄断、数据安全、算法操控等多方面风险挑战，对社会秩序造成了冲击，亟需建立法律制度予以回应。同时，新技术新应用在创新发展中也面临着数据使用规则不明确、部分应用合

法性依据不足等障碍，亟需通过相关立法突破制度壁垒。当前，全球在人工智能领域加快立法，我国在全球率先进行立法探索，针对算法推荐、深度合成、生成式人工智能出台相关立法，发布《全球人工智能治理倡议》，为形成我国统一的人工智能规范体系奠定基础。

**针对数字技术和产业发展新问题加快立法应对。**针对全球共同关注的人工智能风险问题，《国务院 2023 年度立法工作计划》将人工智能法草案列入“预备提请全国人大常委会审议”的立法项目。下一步，我国需加快推进人工智能相关立法研究和制定工作。**一是**明确立法原则及立法方法，以产业发展、权利保护、伦理考量为基本原则，用系统观念和法治方法来推动人工智能技术产业在我国规范健康持续发展，促进其在“安全、可控、可解释、可问责”的基本标准下创新发展。**二是**以问题为导向，以目标为牵引，以算法、算力、数据为核心要素，在法治框架下尽快建立健全人工智能科技伦理监督管理规范，完善相应的侵权责任规范体系。**三是**构建以不同领域开发使用人工智能的风险为划分标准的规则体系，加强和改进人工智能领域数据安全保障制度，重视和强化算法管理，强化对高风险领域的管理，释放低风险领域发展活力。**四是**探索构建多元主体创新治理路径，研究探索“沙盒监管”等创新监管制度，秉持“在发展中规范”“在规范中发展”的基本制度取向，在新技术新应用治理中构建多领域、多主体、多制度、多工具协同联动治理机制。

#### （四）提前布局前沿制度研究，探索数据基础法律规则

数据是数字经济的核心生产要素，在数字经济的研发、生产、流通、分配、消费各个环节都发挥着重要驱动作用。2022 年底，我国发布《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》，提出“以维护国家数据安全、保护个人信息和商业秘密为前提，以促进数据合规高效流通使用、赋能实体经济为主线，以数据产权、流通交易、收益分配、安全管理为重点，深入参与国际高标准数字规则制定，构建适应数据特征、符合数字经济发展规律、保障国家数据安全、彰显创新引领的数据基础制度”。目前我国数据相关立法集中在数据安全、个人信息保护等领域，在数据流通共享、数据资产交易等方面尚存立法空白。下一步，我国需进一步细化数据相关制度规则，并探索构建数据基础法律制度，为合法有序推进数据要素市场建设提供立法保障。

一方面，细化数据相关法律规则，提升数据相关立法可操作性。推动出台《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》配套规则，加快推进具体行业领域出台数据分类分级规则，制定重要数据目录，强化相关主体落实数据安全义务。推动落实各行业领域个人信息保护规则与《中华人民共和国个人信息保护法》的有效衔接，强化对重点行业领域、特殊人群的个人信息保护。加快出台《规范和促进数据跨境流动规定》，构建灵活、高效的数据跨境流动制度。另一方面，研究构建数据基础法律制度，为释放数据



**要素价值提供立法保障。**以数据分类分级为前提，探索明确数据权属分配规则。结合各地大数据交易所等相关实践情况，探索构建数据定价、数据交易、数据标准制度，对数据采集、加工、交易等全链条全环节进行法律制度设计，加强数据要素应用场景指引，为数据要素的流通和交易提供规范化的市场环境。

## 附录：2023年互联网立法梳理

效力位阶	名称	发文字号	发布日期	实施日期
法律	《反间谍法（2023年修订）》	中华人民共和国主席令第4号	2023.04.26	2023.07.01
行政法规	《商用密码管理条例（2023年修订）》	国务院令 第760号	2023.04.27	2023.07.01
	《无人驾驶航空器飞行管理暂行条例》	国务院令 第761号	2023.05.31	2024.01.01
	《未成年人网络保护条例》	国务院令 第766号	2023.10.16	2024.01.01
部门规章	《个人信息出境标准合同办法》	国家互联网信息办公室令 第13号	2023.02.22	2023.06.01
	《互联网广告管理办法》	国家市场监督管理总局令 第72号	2023.02.25	2023.05.01
	《证券期货业网络和信息安全管理办法》	中国证券监督管理委员会令 第218号	2023.02.27	2023.05.01
	《网信部门行政执法程序规定》	国家互联网信息办公室令 第14号	2023.03.18	2023.06.01
	《工业和信息化行政处罚程序规定》	工业和信息化部令 第63号	2023.05.30	2023.09.01
	《生成式人工智能服务管理暂行办法》	国家互联网信息办公室、中华人民共和国国家发展和改革委员会、中华人民共和国教育部、中华人民共和国科学技术部、中华人民共和国工业和信息化部、中华人民共和国公安部、国家广播电视总局令 第15号	2023.07.10	2023.08.15
	《民用无人驾驶航空器生产管理若干规定》	工业和信息化部令 第66号	2023.12.18	2024.01.01
法律法规配套规范性文件	《关于促进数据安全产业发展的指导意见》	工信部联网安〔2022〕182号	2023.01.03	
	《关于开展网络安全服务认证工作的实施意见》	国市监认证规〔2023〕3号	2023.03.15	

效力位阶	名称	发文字号	发布日期	实施日期
	《关于推动在线旅游市场高质量发展的意见》	文旅市场发〔2023〕41号	2023.03.24	
	《关于加快推进能源数字化智能化发展的若干意见》	国能发科技〔2023〕27号	2023.03.28	
	《关于发布<化妆品网络经营监督管理办法>的公告》	国家药品监督管理局公告2023年第36号	2023.03.31	2023.09.01
	《关于加强第三方合作中网络和数据安全管理的通知》	国家金融监督管理总局	2023.06.29	
	《关于促进网络安全保险规范健康发展的意见》	工信部联网安〔2023〕95号	2023.07.02	
	《关于修订网络关键设备和网络安全专用产品安全认证实施规则》	国家认证认可监督管理委员会公告2023年第14号	2023.08.08	
	《网络平台受理处置涉企网络侵权信息举报工作规范》	中央网络安全和信息化委员会办公室	2023.08	
	《关于印发<企业数据资源相关会计处理暂行规定>的通知》	财会〔2023〕11号	2023.08.01	2024.01.01
	《关于印发<科技伦理审查办法(试行)>的通知》	国科发监〔2023〕167号	2023.09.07	2023.12.01
	《关于依法惩治网络暴力违法犯罪的指导意见》	最高人民法院、最高人民检察院、公安部	2023.09.20	
法律法规征求意见稿	《公平竞争审查条例（征求意见稿）》	国家市场监督管理总局	2023.05.12	
法律法规配套规范性文件征求意见稿	《区块链和分布式记账技术标准体系建设指南（2023版）》（征求意见稿）	工业和信息化部	2023.03.28	
	《关于行业协会的反垄断指南（征求意见	国家市场监督管理总局	2023.05.15	

效力位阶	名称	发文字号	发布日期	实施日期
	稿》			
	《工业领域数据安全标准体系建设指南（2023版）（征求意见稿）》	工业和信息化部	2023.05.22	
	《近距离自组网信息服务管理规定（征求意见稿）》	国家互联网信息办公室	2023.06.06	
	《网络暴力信息治理规定（征求意见稿）》	国家互联网信息办公室	2023.07.07	
	《铁路关键信息基础设施安全保护管理办法（征求意见稿）》	国家铁路局	2023.07.18	
	《移动互联网未成年人模式建设指南（征求意见稿）》	国家互联网信息办公室	2023.08.02	
	《个人信息保护合规审计管理办法（征求意见稿）》	国家互联网信息办公室	2023.08.03	
	《人脸识别技术应用安全管理规定（试行）（征求意见稿）》	国家互联网信息办公室	2023.08.08	
	《物联网新型基础设施标准体系建设指南（2023版）》（征求意见稿）	工业和信息化部	2023.08.18	
	《市场监督管理行政执法电子数据取证暂行规定（征求意见稿）》	国家市场监督管理总局	2023.08.22	
	《中国人民银行业务领域数据安全管理办法（征求意见稿）》	中国人民银行	2023.08.24	
	《互联网广告可识别性执法指南（征求意见稿）》	国家市场监督管理总局	2023.08.28	
	《药品网络交易第三方平台检查指导原则（征求意见稿）》	国家药品监督管理局	2023.09.04	
	《医疗器械网络销售	国家药监局	2023.09.14	

效力位阶	名称	发文字号	发布日期	实施日期
	质量管理规范（征求意见稿）			
	《规范和促进数据跨境流动规定（征求意见稿）》	国家互联网信息办公室	2023.09.28	
	《工业和信息化领域数据安全风险评估实施细则（试行）（征求意见稿）》	工业和信息化部	2023.10.09	
	《电子政务电子认证服务管理办法（征求意见稿）》	国家密码管理局	2023.10.17	
	《工业互联网安全分类分级管理办法（征求意见稿）》	工业和信息化部	2023.10.24	
	《工业和信息化领域数据安全行政处罚裁量指引（试行）（征求意见稿）》	工业和信息化部	2023.11.23	
	《网络安全事件报告管理办法（征求意见稿）》	国家互联网信息办公室	2023.12.08	
	《网络游戏管理办法（草案征求意见稿）》	国家新闻出版署	2023.12.22	

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-62301327

传真：010-62304980

网址：[www.caict.ac.cn](http://www.caict.ac.cn)

