（2024 年 11 月）

目录

一、法规速递

1. 《工业和信息化领域数据安全事件应急预案（试行）》

发文机关：工业和信息化部

发布日期：2024.10.29

生效日期：2024.11.01

时效性：现行有效

1. 总则

1.1 编制目的

建立健全工业和信息化领域数据安全事件应急组织体系和工作机制，提高数据安全事件综合应对能力，确保及时有效地控制、减轻和消除数据安全事件造成的危害和损失，保护个人、组织的合法权益，维护国家安全和公共利益。

1.2 编制依据

《中华人民共和国突发事件应对法》《中华人民共和国数据安全法》《中华人民共和国网络安全法》《中华人民共和国个人信息保护法》《网络数据安全管理条例》等法律法规和《工业和信息化领域数据安全管理办法（试行）》等相关政策制度。

1.3 适用范围

在中华人民共和国境内发生的工业和信息化领域数据安全事件应急处置活动，应当遵守相关法律、行政法规和本预案的要求。

工业和信息化部对重大活动期间数据安全事件应急处置工作另有规定的，从其规定。

1.4 事件定义

本预案所称数据安全事件，是指数据遭篡改、破坏、泄露或者非法获取、非法利用，对国家安全、公共利益或者个人、组织合法权益造成危害的事件。

1.5 事件分级

根据数据安全事件对国家安全、企业网络设施和信息系统、生产运营、经济运行等造成的影响范围和危害程度，将数据安全事件分为特别重大、重大、较大和一般四个级别（见附件 1）。

1.6 工作原则

数据安全事件应急工作应当坚持统一领导、分级负责。坚持统一指挥、密切协同、快速反应、科学处置。坚持“谁管业务、谁管业务数据、谁管数据安全”，落实数据处理者的数据安全主体责任。坚持充分发挥各方面力量，共同做好数据安全事件应急处置工作。

2．组织体系

2.1 领导机构与职责

在国家数据安全工作协调机制统筹协调下，工业和信息化部网络安全和信息化领导小组（以下简称部网信领导小组）统一领导数据安全事件应急管理工作，负责特别重大数据安全事件的统一指挥和协调。

2.2 办事机构与职责

在部网信领导小组统一领导下，工业和信息化领域数据安全工作机制（以下简称数据安全机制）负责统筹开展工业和信息化领域数据安全应急处置工作；及时向部网信领导小组报告数据安全事件情况，提出特别重大数据安全事件应对措施建议；负责重大数据安全事件的统一指挥和协调处置；根据需要协调较大、一般数据安全事件应急处置工作。

数据安全机制具体工作由工业和信息化部网络安全管理局牵头承担。

2.3 地方和数据处理者职责

各省、自治区、直辖市及计划单列市、新疆生产建设兵团工业和信息化主管部门，各省、自治区、直辖市通信管理局和无线电管理机构（以下统称地方行业监管部门）负责组织开展本地区本领域数据安全事件应急处置工作，结合实际根据本预案分别制定本地区本领域数据安全事件应急预案。

工业和信息化领域数据处理者负责本单位数据安全事件预防、监测、应急处置、报告等工作，应当根据应对数据安全事件的需要，制定本单位数据安全事件应急预

案。

中央企业应当督促指导所属企业在数据安全事件应急处置工作中履行属地管理要求，并负责全面梳理汇总企业集团本部、所属企业的数据安全事件应急处置相关情况，按要求及时报送工业和信息化部。

2.4 应急支撑机构与职责

工业和信息化部及地方行业监管部门（以下统称行业监管部门）根据需要遴选部级与属地两级专业数据安全应急支撑机构，负责开展数据安全事件预防保护、监测预警、应急处置、攻击溯源等工作。

2.5 协同联动

行业监管部门按照有关法律、行政法规，与有关部门加强协同联动，依法配合有关部门开展数据安全事件应急处置工作。

3．监测与预警

3.1 预警监测和报告

地方行业监管部门、工业和信息化领域数据处理者、数据安全应急支撑机构应当按照《工业和信息化领域数据安全管理办法（试行）》、工业和信息化领域数据安全风险信息报送与共享等要求，加强数据安全风险监测、研判和上报，分析相关风险发生数据安全事件的可能性及其可能造成的影响。

地方行业监管部门认为可能发生重大及以上数据安全事件的，应当立即上报数据安全机制。

工业和信息化领域数据处理者、数据安全应急支撑机构认为可能发生较大及以上数据安全事件的，应当立即向地方行业监管部门报告（模板见附件 2）。

3.2 预警分级

工业和信息化部统筹建立数据安全风险预警机制，根据紧急程度、发展态势、数据规模、关联影响和现实危害等，将数据安全风险预警等级分为四级：由高到低依次用红色、橙色、黄色和蓝色标示，分别对应可能发生特别重大、重大、较大和一般数据安全事件。

行业监管部门及时汇总分析数据安全风险和预警信息，必要时组织数据安全应

急支撑机构、专家、相关企业进行会商谈判，明确预警等级。

3.3 预警发布

认为需要发布红色、橙色预警的，由数据安全机制报部网信领导小组同意后统一发布，红色预警同步报国家数据安全工作协调机制办公室；认为需要发布黄色和蓝色预警的，由相关地方行业监管部门在本地区本领域内发布。

发布预警信息时，应当包括预警等级、起始时间、可能的影响范围和造成的危害、警示事项、应采取的防范措施、处置时限要求、发布范围和发布机关等。

3.4 预警响应

发布黄色和蓝色预警后，地方行业监管部门应当针对即将发生的数据安全事件特点和可能造成的危害，采取下列措施：

(1)要求涉及预警信息的数据处理者及时收集、报告有关信息，加强数据安全风险监测；

(2)组织数据安全应急支撑机构加强预警信息分析评估与事态跟踪，密切关注事态发展，提出下步工作措施；

(3)组织专家加强风险研判及原因、影响等分析，提出应急处置方法和整改措施建议。

发布红色和橙色预警后，数据安全机制除采取黄色和蓝色预警响应措施外，还应当针对即将发生的数据安全事件特点和可能造成的危害，采取下列措施：

(1)要求地方行业监管部门、涉及预警信息的数据处理者等相关单位加强值班值守，相关人员保持通信联络畅通；

(2)组织研究制定防范措施和应急工作方案，组织专家会商研提意见，协调各方资源，做好各项准备工作；

(3)要求相关数据安全应急支撑机构进入待命状态，针对预警信息研究制定应对方案，检查应急设备、软件工具等使用情况，确保处于良好状态。

3.5 预警调整和解除

数据安全机制、地方行业监管部门发布预警后，应当根据事态发展，适时调整预警级别并按照权限重新发布。经研判不可能发生事件或风险已经解除的，应当及

时宣布解除预警，并解除已经采取的有关预警响应措施。

4．事件响应

4.1 响应分级

数据安全事件应急响应分为四级：I 级、II 级、III 级、IV 级，分别对应发生特别重大、重大、较大、一般数据安全事件的应急响应。

4.2 事件监测和报告

工业和信息化领域数据处理者一旦发现数据安全事件，应当立即先行判断，对自判为较大及以上事件的，应当立即向地方行业监管部门报告，不得迟报、谎报、瞒报、漏报。

数据安全应急支撑机构应当通过多种途径监测、收集数据安全事件信息，及时向行业监管部门报告。

地方行业监管部门初步研判为特别重大、重大数据安全事件的，应当在发现事件后按照“电话 10 分钟、书面 30 分钟”的要求向数据安全机制报告。

数据安全机制按照有关规定将涉及重大及以上的数据安全事件报送国家数据安全工作协调机制办公室。

报告事件研判信息时，应当说明事件发生时间、初步判定的影响范围和危害、已采取的应急处置措施和有关建议。

4.3 先行处置

数据安全事件发生后，工业和信息化领域数据处理者应当立即启动应急响应工作，组织本单位应急队伍和工作人员采取应急处置措施，开展数据恢复或追溯工作，尽可能减少对用户和社会的影响，同时保存相关痕迹和证据。

4.4 应急响应

行业监管部门视情组织数据安全应急支撑机构、专家等进行研判，确定事件级别和响应等级，启动应急响应。

4.4.1 I 级响应

根据国家数据安全工作协调机制有关决定或经部网信领导小组批准后启动，由数据安全机制统一指挥、协调。

数据安全机制在发现事件后按照“电话 20 分钟、书面 40 分钟”的要求将事件情况向部网信领导小组报告；进入应急状态，加强值班值守，相关人员保持联络畅通，相关单位派员参加数据安全机制工作；视情设立应急恢复、事件溯源、影响评估、信息发布、跨部门协调、国际协调等工作组；召开紧急会议，听取各相关方面情况汇报，研究紧急应对措施，对应急处置工作进行决策部署，指导相关地方行业监管部门、数据处理者开展应对工作；视事件严重程度和涉事数据处理者整改处置情况，评估是否开展现场检查。

地方行业监管部门立即启动本地区本领域数据安全事件应急预案，进入应急状态，加强值班值守，相关人员保持联络畅通，派员参加数据安全机制工作；加强事件跟踪监测、研判分析和排查处置，全面了解本地区本领域相关数据处理者受事件影响情况。

涉事数据处理者立即进入应急状态，数据安全第一责任人（本单位法定代表人或主要负责人）牵头组建事件应对工作专班，组织研究应对措施，统筹开展应急处置工作。数据安全直接责任人（本单位数据安全工作分管领导）对应急处置工作进行具体部署，组织专班加强值班值守，相关人员保持联络畅通；持续加强监测分析，跟踪事态发展，评估影响范围和事件原因，采取有效整改处置措施，并及时汇报工作进展和处置情况。

相关部级与属地数据安全应急支撑机构进入应急状态，加强值班值守，相关人员保持联络畅通；持续加强监测分析，跟踪事态发展变化、处置进展情况，评估影响范围。

组织专家加强安全事件研判分析，配合开展会商研讨，提出应急处置决策建议。

4.4.2 II 级响应

由数据安全机制决定启动，并负责统一指挥、协调。

数据安全机制在发现事件后按照“电话 20 分钟、书面 40 分钟”的要求将事件情况向部网信领导小组报告；进入应急状态，相关人员保持联络畅通，相关单位派员参加数据安全机制工作；召开紧急会议，听取各相关方面情况汇报，研究紧急应对措施，对应急处置工作进行决策部署；视事件严重程度和涉事数据处理者整改处置

情况，评估是否开展现场检查。

地方行业监管部门立即启动本地区本领域数据安全事件应急预案，进入应急状态，相关人员保持联络畅通，派员参加数据安全机制工作；加强事件跟踪监测、研判分析和排查处置，全面了解本地区本领域相关企业受事件影响情况。

涉事数据处理者立即进入应急状态，数据安全直接责任人牵头研究应对措施，统筹部署开展应急处置工作，相关人员保持联络畅通；持续加强监测分析，跟踪事态发展，评估影响范围和事件原因，采取有效整改处置措施，并及时汇报工作进展和处置情况。

相关部级与属地数据安全应急支撑机构进入应急状态，相关人员保持联络畅通；持续加强监测分析，跟踪事态发展变化、处置进展情况，评估影响范围。

组织专家加强安全事件研判分析，配合开展会商研讨，提出应急处置决策建议。

4.4.3 III 级响应

由相关地方行业监管部门按照本地区本领域数据安全事件应急预案决定启动，并负责指挥、协调。

相关行业监管部门组织涉事数据处理者、数据安全应急支撑机构等加强事态跟踪研判、开展事件处置，及时将事件进展及重要情况报数据安全机制，通知可能受影响的其他区域做好数据安全应急处置工作。

涉事数据处理者持续开展监测分析，跟踪事态发展，评估影响范围和事件原因；加强相关业务系统应用安全加固措施，提升数据安全防护能力，采取有效整改处置措施，并及时汇报工作进展和处置情况。

相关属地数据安全应急支撑机构持续加强监测分析，跟踪事态发展变化、处置进展情况，评估影响范围。

4.4.4 IV 级响应

涉事数据处理者应当按照行业数据安全保护相关政策标准及时采取有效措施处置事件，加强数据安全防护。

4.4.5 响应级别调整

涉事数据处理者可根据事态发展等情况，向属地行业监管部门申请调整事件响

应级别。

地方行业监管部门根据涉事数据处理者的申请情况或者事态发展情况等，适时调整事件响应级别，涉及 I、II 级响应级别调整的应当报数据安全机制同意。

数据安全机制根据地方行业监管部门上报情况或者事态发展情况等，适时调整事件响应级别。

4.5 舆情监测

行业监管部门组织监测公开信息发布渠道，密切关注数据安全事件舆情信息，跟踪掌握事件影响程度和范围。

4.6 结束响应

事件的影响和危害得到控制或消除后，I 级响应应当根据国家数据安全工作协调机制有关决定或经部网信领导小组批准后结束；II 级响应由数据安全机制决定结束，并报部网信领导小组；III 级响应由相关地方行业监管部门决定结束，并报数据安全机制；IV 级响应由相关涉事数据处理者决定结束。

5．事后总结

5.1 事件总结上报

重大及以上数据安全事件应急工作结束后，涉事数据处理者应当及时调查事件的起因、经过、责任，评估事件造成的影响和损失，总结事件防范和应急处置工作的经验教训，提出处理意见和改进措施，在应急工作结束后 5 个工作日内形成总结报告（模板见附件 3），报地方行业监管部门。地方行业监管部门汇总审核后，在应急工作结束后 10 个工作日内形成报告报送数据安全机制。

5.2 事件警示

行业监管部门应及时向社会发布与公众有关的警示信息，引导做好数据安全风险防范。

6．预防措施

6.1 预防保护

工业和信息化领域数据处理者应当根据有关法律法规和标准的规定，建立健全数据安全管理制度，建设数据安全应急技术手段，重要数据和核心数据处理者应当

每年至少开展一次数据安全风险评估和自查自纠，及时消除风险隐患。

行业监管部门依法开展数据安全监督检查，指导督促相关单位消除风险隐患。

6.2 应急演练

行业监管部门应当定期组织开展数据安全事件应急演练，提高数据安全事件应对能力。

工业和信息化领域数据处理者应当积极参与行业监管部门的应急演练，开展本单位数据安全事件应急演练，提高数据安全事件应对能力。重要数据和核心数据处理者应当加强应急演练。

6.3 宣传培训

行业监管部门应当组织开展数据安全事件应急相关法律法规、应急预案和基本知识的宣传教育和培训，提高相关单位和社会公众的数据安全意识和防护、应急能力。

工业和信息化领域数据处理者应当面向本单位员工加强数据安全应急宣传教育和培训，鼓励开展各种形式的数据安全应急相关竞赛。

6.4 手段建设

工业和信息化部统筹建设工业和信息化领域数据安全监测预警与应急处置相关技术手段，对数据泄露、篡改、非法访问、违规传输、流量异常等安全风险和事件进行监测预警，并及时开展应急处置。

地方行业监管部门建立本地区本领域数据安全监测预警与应急处置能力，组织相关企业开展数据安全风险和事件监测预警工作，及时开展风险和事件应急处置。

工业和信息化领域数据处理者等单位应当开展数据安全风险和事件监测，积极配合行业监管部门开展数据安全风险监测和技术能力联动等工作，及时排查安全隐患，采取必要的措施防范、处置数据安全风险和事件。

6.5 重大活动期间的预防措施

在国家重大活动期间，行业监管部门组织指导数据处理者、数据安全应急支撑机构等加强数据安全风险监测、威胁研判和事件处置，强化风险防范与应对措施。相关重点单位、重点岗位加强值班值守。

7．保障措施

7.1 落实责任

工业和信息化部加强数据安全事件应急处置工作督导和落实。地方行业监管部门、工业和信息化领域数据处理者、数据安全应急支撑机构应当把数据安全应急工作责任落实到单位负责人、具体部门、具体岗位和个人。

7.2 奖惩问责

工业和信息化部对数据安全事件应急处置工作中作出突出贡献的集体和个人给予表扬。

对未按照本预案开展数据安全事件应急处置工作的，行业监管部门依法依规对数据处理者进行约谈或给予行政处罚。

7.3 经费保障

行业监管部门、数据安全应急支撑机构等为数据安全事件应急处置工作提供必要的经费保障。

工业和信息化领域数据处理者应当安排必要的专项资金，支持本单位数据安全应急队伍建设、手段建设、应急演练、应急培训等工作开展。

7.4 工作协同

行业监管部门与其他相关部门加强沟通协调，支持相关企业、科研院所、高等学校开展应急技术攻关、产品服务和能力供给，培养数据安全应急技术人才，形成应急响应工作合力。

7.5 物资保障

行业监管部门和应急支撑机构应当加强对数据安全应急装备、工具的储备，及时调整、升级、优化软件硬件工具，不断增强应急技术支撑能力。

7.6 国际合作

工业和信息化部根据职责建立国际合作渠道，必要时通过国际合作应对数据安全事件。鼓励相关企业、科研院所、高等学校、工业和信息化领域数据处理者等开展数据安全国际交流与合作。

7.7 保密管理

行业监管部门、应急支撑机构工作人员对在履行职责中知悉的个人信息和商业秘密等，应当严格保密，不得泄露或者非法向他人提供。

8．附则

8.1 预案修订

本预案原则上每年评估一次，根据实际情况由工业和信息化部适时进行修订。

8.2 排除条款

涉及军事、国家秘密信息等数据安全事件应急响应的，按照国家有关规定执行。

涉及国防科技工业、烟草领域数据安全事件应急响应的，由国家国防科技工业局、国家烟草专卖局负责，具体制度参照本预案另行制定。

涉及工业和信息化领域政务数据安全事件应急响应的，由工业和信息化部另行规定。

8.3 预案解释

本预案由工业和信息化部负责解释。

8.4 实施日期

本预案自 2024 年 11 月 1 日起实施。

附件：

1．工业和信息化领域数据安全事件分级

2．数据安全事件上报（模板）

3．数据安全事件应急处置工作总结报告（模板）

4．　数据安全事件应急处置流程图

2. 《推动数字金融高质量发展行动方案》

发文机关：中国人民银行,国家发展和改革委员会,工业和信息化部,国家金融监督管理总局,中国证券监督管理委员会,国家数据局,国家外汇管理局

发布日期：2024.11.21

生效日期：2024.11.21

时效性：现行有效

做好数字金融大文章，加快金融业数字化转型，高质量服务数字经济和促进数实融合，对于建设金融强国、巩固和拓展我国数字经济优势具有重要意义。为深入贯彻落实党的二十届三中全会和中央金融工作会议决策部署，推动数字金融高质量发展，制定本方案。

一 、总体要求

（一）指导思想。以习近平新时代中国特色社会主义思想为指导，完整、准确、全面贯彻新发展理念，坚持金融服务实体经济和以人民为中心，把握机遇、重视安全，以数据要素和数字技术为关键驱动，加快推进金融机构数字化转型，提高金融服务的便利性和竞争力，保留必要的现金等传统金融服务方式，完善数字金融治理体系，提高数字化监管能力和金融消费者保护能力，积极稳妥推行数字人民币，助力金融强国建设，支持做强做优做大我国数字经济。

（二）工作目标。到 2027 年底，基本建成与数字经济发展高度适应的金融体系。金融机构数字化转型取得积极成效，数字化经营管理能力明显增强。形成数字金融和科技金融、绿色金融、普惠金融、养老金融协同发展的良好局面，数字化金融产品服务对重大战略、重点领域、薄弱环节的适配度和普惠性明显提升。数字金融治理体系基本形成，数字金融基础设施基本齐备，相关金融管理和配套制度机制进一步健全。

二 、系统推进金融机构数字化转型

（三）加强战略规划和组织管理。指导金融机构制定全方位数字化转型战略规划，明确目标路径和实施策略。建立数字化转型“一把手”负责制和统筹协调机制，

指定牵头工作部门，加强经费保障，加快推进数字化转型步伐。建立健全与数据驱动下智能化战略决策、运营决策、创新决策相适应的运营管理机制。建立数字化转型成效评价体系，完善激励考核机制。

（四）强化数字技术支撑能力。合理评估金融机构数字化进程，指导具备条件的金融机构建立跨科技部门和业务部门的任务型团队，建立前端业务部门需求驱动的数字技术开发模式，提高科技开发敏捷响应能力。落实科技自立自强战略，开展前沿技术研究，加快重点领域专利布局，持续提升科技核心系统自主可控能力。建设证券期货业数字化公共服务平台，为金融机构数字化转型提供数据和技术支撑。

（五）夯实数据治理与融合应用能力基础。指导金融机构健全数据治理体系，完善数据治理制度和数据质量管控机制，积极参加数据管理国家标准（DCMM）贯标评估。加强数据资产积累，全面整合内外部数据，实现全域数据的统一管理、融合共享。强化数据挖掘分析和数据可视化能力建设，形成对业务经营、风险管理、内部控制的基础数据支撑。推进金融领域“数据要素×”试点，运用大数据、隐私计算等科技手段，融合应用多维数据，优化金融产品和风控模型，提升金融服务和风险管控质效。

（六）建设数字金融服务生态。鼓励金融机构合理布局数字生态场景体系，构建数字生态运营体系。坚持人民至上，以服务大众为价值目标，构建零售数字金融生态，在做好金融消费者适当性管理的基础上，有效提高金融产品服务的可获得性和普惠性。支持金融机构参与数字政府建设，助力提升政府管理服务水平。推动区域性股权市场数字化转型，加快数据资源整合运用。推动互联网保险规范发展，增强线上承保理赔能力。

（七）提升数字化经营管理能力。支持金融机构提高数据驱动的业务决策和资源配置能力。利用流程机器人、数字化客户营销触达工具、集约化作业模式等数字化手段，赋能高强度操作性岗位提质增效。健全数字化人才培养、选拔和使用机制，完善数字化人力资源考核激励机制。运用数字技术优化风险管理系统，实现风险智能预警和动态捕捉，推动风控从“人防”向“技防”“智控”转变。鼓励有条件的地方支持有能力、有意愿的中小金融机构结合自身定位探索数字化转型特色模式，优先选

取影响程度深、范围广、价值高的业务领域或环节加快转型，实现成本可承担、业务可持续。

三 、运用数字技术提升重点领域金融服务质效

（八）助力科技金融提质增效。鼓励金融机构充分运用内外部数据和大数据技术对科技型企业全景画像，提升客户筛选和营销对接效率，促进金融服务触达更多初创期、成长期企业。支持金融机构依托创新积分、专精特新企业高质量发展评价指标等“技术流”信息，借助数字手段，提高对科技型企业的风险评估能力。建立科技金融风险监测模型，动态掌握科技行业趋势和企业市场变化，开展智能化风控和监测。发挥国家产融合作平台作用，依托智能算法模型更好支持制造业发展。

（九）赋能绿色金融深化发展。推动金融机构基于企业碳账户、碳排放数据以及环境、社会和公司治理（ESG）评分等，探索创新金融产品和服务模式。运用数字技术开展定性定量分析，提高绿色企业、绿色项目智能识别能力。加强与外部机构合作，运用数字技术探测收集碳足迹信息，提升碳减排计量、核算和披露水平，提高绿色金融风险管理能力。

（十）大力发展数字普惠金融。深入推进“信易贷”工作，完善以信用信息为基础的普惠融资服务体系,优化中小微企业信贷服务。有序推进全国中小微企业支付资金流信用信息共享平台建设，支持银行在有效防控风险基础上，探索运用交易数据创新“脱核链贷”业务模式，提升供应链金融服务数字化水平。深化实施金融科技赋能乡村振兴示范工程,建立健全乡村振兴领域数字一体化平台,推动涉农信息整合，打造金融综合应用场景。加强动产融资统一登记公示系统建设应用，支持金融机构探索运用数字技术加强对活体、生产设备等押品管控，拓宽动产融资业务范围。

（十一）持续丰富养老金融服务。鼓励金融机构加强金融科技应用，深度挖掘信息数据资源，对养老企业精准画像，在风险可控前提下，开发养老专属纯信用信贷产品，充分满足普惠养老服务机构的合理融资需求。聚焦老年人群日常生活中的高频金融场景，持续健全金融无障碍服务体系，加快数字服务的适老化改造，推出“关怀模式”“长辈模式”，加强相关产品服务的宣传普及和推广应用，提升老年人群享受数字金融服务便利度。

（十二）支持提升数实融合水平。加快数字金融创新，发挥科技创新和技术改造再贷款作用，引导金融机构将金融服务嵌入工业互联网、“人工智能+产业”等数字化场景，助力数字经济核心产业发展和产业数字化转型。支持金融机构搭建数字化金融服务平台，围绕重大项目、重点企业和重要产业链，加强场景聚合、生态对接，实现“一站式”金融服务。鼓励金融机构发挥金融科技优势，输出技术、平台等服务资源，促进中小企业数字化转型。鼓励金融机构搭建跨境金融数字平台，助力航运贸易数字化。

四 、夯实数字金融发展基础

（十三）营造高效安全的支付环境。提高应对特殊情景的支付系统应急处置能力，加强支付系统业务连续性管理，确保支付系统安全、稳定、连续运行。完善系统功能，丰富业务场景，提升支付系统服务质效，持续完善广泛覆盖、高效安全的现代支付体系。稳妥推进数字人民币试点，持续完善数字人民币受理环境，丰富数字人民币使用场景。强化数字金融业务反洗钱监管。

（十四）培育高质量金融数据市场。发挥金融信用信息基础数据库、全国信用信息共享平台各自功能，加大涉企信用信息归集力度，进一步优化信用信息的开发应用机制。推动各级融资信用服务平台按照公益性原则依法依规向金融机构提供信息共享服务，降低金融机构数据收集运用成本。加强金融领域数据资源开发利用，探索开展金融行业数据空间建设。积极稳妥推动市场化征信和信用评级机构发展壮大，为金融“五篇大文章”提供多元化征信和信用评级产品服务。健全覆盖各金融市场的交易报告制度与交易报告库。在依法安全合规前提下，支持客户识别、信贷审批、风险核查等多维数据在金融机构间共享共用和高效流通，建立健全数据安全可信共享体系。促进和规范金融数据跨境流动，统一监管合规口径，给予金融机构规则指引。

（十五）加强数字金融相关新型基础设施建设。指导有条件的金融机构规划建设绿色智能金融数据中心，推动新增算力向国家枢纽节点集聚，支持海量数据存储和实时数据调用。建设优化高可靠冗余的网络架构，提高金融网络健壮性和服务能力，为金融数字化转型架设通信高速公路。布局先进高效的算力体系，加快云计算、

人工智能等技术规范应用，探索运用边缘计算和量子技术突破现有算力瓶颈，为金融数字化转型提供精准高效的算力支持。

五 、完善数字金融治理体系

（十六）强化数字金融风险防范。指导金融机构加强数字金融业务合规管理，实施创新业务合规审查并定期开展风险评估。多维度开展新技术应用适配测试与安全评估，强化技术风险管理，保障业务连续稳定运行。完善激励和容错机制，引导金融机构持续提升信息系统安全可控水平，化解核心技术“卡脖子”风险。强化模型和算法风险管理，健全模型安全评估和合规审计体系，及时披露算法信息，提升算法可解释性、公平性和安全性。督促金融机构加强外包风险管理，建立外部合作方准入管理、持续评估和退出机制。

（十七）加强数据和网络安全防护。指导金融机构严格落实数据保护法律法规和标准规范，完善数据安全管理体系，强化数据安全的商用密码保护，建立健全全流程数据安全管理机制。组织金融机构定期进行数据和网络安全风险评估，识别潜在风险，接入金融行业相关网络安全态势感知平台，推动相关平台互联互通。开展网络安全相关压力测试，提升网络安全防护体系建设水平。搭建证券业数据和网络安全公共服务平台，加强基础、共性安全支撑。

（十八）加强数字金融业务监管。密切跟踪数字金融新产品、新业务、新模式，按照功能监管和穿透式监管的原则，依法依规全部纳入监管。持续完善数字金融相关业务规则和监管制度，及时补齐监管制度短板。落实“管合法更要管非法”“管行业必须管风险”责任，严密防范和严厉打击数字金融相关非法金融活动。充分运用金融科技创新试点和监管工具，强化金融科技创新行为全生命周期管理，为数字金融创新提供包容审慎、富有弹性的真实市场环境。积极参加国际货币基金组织、国际清算银行、金融稳定理事会、国际证监会组织等国际机构组织的数字金融监管国际合作。

（十九）提升金融监管数字化水平。推动监管流程数字化再造，增强关键监管活动的规范性和透明度。加强智能分析工具研发，提升风险监测预警和识别研判能力。推进监管大数据建设，加强工商、司法、舆情等外部数据引入，完善监管数据

和执法信息共享机制。打造兼具信息展示、智能分析、流程管控、智慧决策功能的数字化监管平台。

（二十）健全金融消费者保护机制。督促金融机构结合数字金融业务模式和特点，健全金融消费者权益保护机制。畅通金融消费者投诉渠道，建立健全金融纠纷多元化解机制。组织开展针对数字金融的教育培训和知识普及，增强消费者金融素养，提升数字金融产品使用能力和风险防范意识。督促金融机构保留现金等传统服务模式，提升现金服务水平，弥补数字鸿沟，保障老年人等公平享受金融服务的权利。

六 、做好统筹协调和组织保障

（二十一）建立工作联动机制。中国人民银行、国家数据局会同国家发展改革委、工业和信息化部、金融监管总局、中国证监会、国家外汇局等部门建立工作联动机制，在数字经济发展部际联席会议下召开专题会议，加强政策协同和信息共享，共同推动金融业数字化转型，组织开展常态化融资对接，支持数实融合和经济社会高质量发展，同时密切监测和防范相关金融风险。各金融管理部门按照职责分工推动本行业领域的数字金融工作。

（二十二）强化监测评估。组织开展金融机构数字化转型评估，对金融机构数据挖掘能力和数字技术应用水平进行评价。探索建立数字金融相关统计标准和制度，指导金融机构开展常态化数据报送，做好统计监测工作，研究将相关统计结果纳入金融机构评价体系。

（二十三）加强总结宣传。探索建立数字金融业务试点，加大对数字金融政策的宣传和培训力度，加快形成可复制可推广的经验。及时总结推动数字金融发展工作情况，梳理提炼发展数字金融的经验做法、典型模式，加大宣传推广力度，形成良好数字金融发展氛围。

3. 《关于开展“清朗·网络平台算法典型问题治理”专项行动的通知》

发文机关：国家互联网信息办公室,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,国家市场监督管理总局

发布日期：2024.11.12

生效日期：2024.11.12

时效性：现行有效

各省、自治区、直辖市党委网信办、通信管理局、公安厅（局）、市场监管局（厅、委），新疆生产建设兵团党委网信办、公安局、市场监管局：

《关于加强互联网信息服务算法综合治理的指导意见》（以下简称《指导意见》）《互联网信息服务算法推荐管理规定》等政策文件印发以来，各部门各地区加强组织推进，网站平台积极落实有关管理要求，算法应用生态日益规范，但仍存在一些需要持续加强治理的典型问题。为进一步深化互联网信息服务算法综合治理，现决定自即日起至 2025 年 2 月 14 日开展“清朗·网络平台算法典型问题治理”专项行动。有关工作方案如下：

一 、主要任务

聚焦网民关切，重点整治同质化推送营造“信息茧房”、违规操纵干预榜单炒作热点、盲目追求利益侵害新就业形态劳动者权益、利用算法实施大数据“杀熟”、算法向上向善服务缺失侵害用户合法权益等重点问题，督促企业深入对照自查整改，进一步提升算法安全能力。

1.深入整治“信息茧房”、诱导沉迷问题。构建“信息茧房”防范机制，提升推送内容多样性丰富性。严禁推送高度同质化内容诱导用户沉迷。不得强制要求用户选择兴趣标签，不得将违法和不良信息记入用户标签并据以推送信息，不得超范围收集用户个人信息用于内容推送。规范设置“不感兴趣”等负反馈功能。

2.提升榜单透明度打击操纵榜单行为。全面公示热搜榜单算法原理，提升榜单透明度和可解释性。完善榜单日志留存，提高榜单算法原理可验证性。健全水军刷榜、水军账号等违规行为、账号检测识别技术手段，严管不法分子恶意利用榜单排

序规则操纵榜单、炒作热点行为。

3.防范盲目追求利益侵害新就业形态劳动者权益。严防一味压缩配送时间导致配送超时率、交通违章率、事故发生率上升等问题。详细公示时间预估、费用计算、路线规划等算法规则。搭建畅通的申诉渠道，及时受理劳动者因交通管制、交通事故、恶劣天气等不可控因素导致的配送超时等申诉。

4.严禁利用算法实施大数据“杀熟”。严禁利用用户年龄、职业、消费水平等特征，对相同商品实施差异化定价行为。提升优惠促销透明度，清晰说明优惠券的领取条件、发放数量和使用规则等内容。客观如实说明优惠券领取失败原因，严禁以“来晚了”“擦肩而过”等提示词掩盖真实原因。

5.增强算法向上向善服务保护网民合法权益。持续优化完善面向未成年人、老年人的算法推荐服务，便利未成年人、老年人获取有益身心健康的信息。建立健全算法在赋能优质内容传播、违法行为识别发现等方面的社会治理应用。持续提升生成合成信息检测识别能力，及时发现处理违法违规生成合成信息。

6.落实算法安全主体责任。健全算法机制机理审核、数据安全的管理制度和技术措施。确保算法的训练数据具有合法来源，及时检测修复代码安全漏洞和算法逻辑缺陷，定期对算法模型的可用性、可控性、可解释性以及数据处理、模型训练、部署运行等环节开展安全评估。

二 、工作目标

1.算法导向正确。健全完善正能量优质内容池，优化算法推荐服务机制，积极传播正能量，促进算法应用向上向善；建立健全用于识别违法和不良信息的特征库，积极探索应用于识别违法和不良信息的算法、技术，防范和抵制传播不良信息。不得设置诱导用户沉迷、过度消费等的算法模型。不得利用算法干预信息呈现，实施影响网络舆论或者规避监督管理行为。

2.算法公平公正。不得利用算法实施垄断和不正当竞争行为。保护劳动者合法权益，完善平台订单分配、报酬构成及支付、工作时间、奖惩等相关算法。保护消费者公平交易的权利，不得利用算法在交易价格等条件上实施不合理的差别待遇。

3.算法公开透明。优化检索、排序、推送等规则的透明度和可解释性，预防和减

少争议纠纷。以适当方式公示算法推荐服务的基本原理、目的意图、主要运行机制等，确保简单、清晰、可理解。

4.算法自主可控。关闭算法推荐服务的选项操作便捷、功能有效。向用户提供选择或者删除用于算法推荐服务的针对其个人特征的用户标签的功能，便利用户自主选择兴趣领域。

5.算法责任落实。建立健全算法安全管理制度和技术措施。定期审核、评估、验证算法机制机理、模型、数据和应用结果等，常态化开展算法安全自评估。算法“应备尽备”，备案信息发生变更的及时办理变更或者注销手续。

三 、工作安排

专项行动自即日起至 2025 年 2 月 14 日，具体安排如下：

1.组织企业自查自纠（即日起至 2024 年 12 月 31 日）。通过下发通知、召开专题会议等形式，部署属地重点网站平台对照重点任务，举一反三排查安全风险问题，简单问题立即整改，复杂问题明确整改举措和期限。

2.核验企业自查情况（2025 年 1 月 1 日至 2025 年 1 月 31 日）。积极落实属地管理责任，对照《算法专项治理清单指引》（附件），对企业自查自纠情况进行深入评估。对自查不认真、整改不彻底的企业，及时组织技术力量进行核查并督促整改。

3.深入评估治理成效（2025 年 2 月 14 日前完成）。各地网信部门会同有关部门，总结专项行动实施成效，结合专项行动开展情况，全面评估《指导意见》印发以来的算法治理举措及取得的积极成效，深入分析难点问题，制定今后一段时期的务实举措。

4.开设举报受理渠道（专项行动期间）。各地网信部门在专项行动期间要及时公开算法问题举报渠道。对网民举报线索进行监测核实，督促存在问题的网站平台及时整改，并向网民反馈整改结果。

四 、工作要求

1.抓好组织落实。各地网信部门要发挥统筹协调作用，牵头开展专项行动。加强与属地电信、公安、市场监管等相关部门联动，细化工作分工，压实工作责任。

运用好央地各方有效技术支撑力量，积极有效推动各项任务落实，确保取得工作成效。

2.依法依规处置。要依法依规对违反有关法律法规的网站平台进行处置处罚，精准区分违法违规情形、影响、性质，实现宽严相济、过罚相当、有力有效。

3.压实平台责任。要督促相关企业落实算法安全主体责任，认真梳理风险隐患，排查问题漏洞，客观真实反映存在的问题，及时深入开展整改。

4.推动长效治理。要常态化开展算法服务安全风险监测防范工作，及时发现网站平台违规问题线索，并综合运用督促整改、现场检查、处置处罚等措施，提升算法常态化治理水平。

4. 《上海市数据产品知识产权登记存证暂行办法》

发文机关：上海市知识产权局,上海市数据局

发布日期：2024.11.08

生效日期：2024.12.08

时效性：现行有效

第一条（目的和依据）

为促进数据要素有序流通和数据价值充分实现，推进数据产品知识产权登记试点工作，根据《“十四五”国家知识产权保护和运用规划》《上海市知识产权保护和运用“十四五”规划》以及相关规定，结合上海实际，制定本办法。

第二条（适用范围）

本办法适用于自然人、法人或者非法人组织向上海市知识产权局申请数据产品知识产权登记以及相关管理服务活动。

第三条（定义）

本办法所称数据产品知识产权，是指自然人、法人或者非法人组织对其合法获取的数据资源，经过实质性加工和创新性劳动后形成的具有智力成果属性和商业价值的数据加工集合、数据加工产品、数据技术算法等数据产品享有的权益。

第四条（总体要求）

上海市知识产权局在国家知识产权局指导下，贯彻落实关于数据产品知识产权试点工作部署，开展数据产品知识产权登记的审查、监督、管理等工作，为国家试制度、探新路积累先行先试经验。

上海市数据局支持建设上海市数据产品知识产权管理平台和上海市数据存证中心知识产权分中心。

数据产品知识产权登记遵循依法合规、自愿登记、公平有序、诚实信用、安全高效的原则，确保国家安全、社会公共利益、商业秘密和个人隐私不受侵犯。

数据产品知识产权登记、变更、撤销和注销的，上海市知识产权局应当进行公告。

第五条（申请方式和材料）

申请数据产品知识产权登记的，应当通过上海市数据产品知识产权管理平台（简称“管理平台”）提出申请，并提交以下材料：

（一） 数据产品知识产权登记申请表；

（二） 数据产品概述；

（三） 对数据进行实质性加工和创新性劳动的说明；

（四） 应用场景说明；

（五） 数据产品知识产权权益归属声明以及数据产品不涉及国家秘密、不侵害他人个人信息和知识产权承诺书；

（六） 数据产品信息。

第六条（登记审查）

上海市知识产权局应当依据本办法和制定的审查指南对登记申请进行审查。

申请材料不齐全或者不符合规定要求的，上海市知识产权局应当在接到材料 3 个工作日内，一次性告知登记申请人需要补正的材料，申请人应于 10 个工作日内予以补正。

登记申请人无正当理由逾期不补正的，视为撤回登记申请。

第七条（不予登记的情形）

有下列情形之一的，不予登记并告知申请人：

（一） 数据产品涉及国家安全、侵犯国家秘密或者损害社会公共利益的；

（二） 数据产品侵害他人个人信息或者隐私的；

（三） 数据产品系非法获取或者侵害他人知识产权的；

（四） 数据产品权属不清或者存在争议的；

（五） 登记申请人隐瞒事实或者弄虚作假的；

（六） 重复申请登记或者登记申请主动撤回后 3 个月内无正当理由再次提出登记申请的；

（七） 其他不符合法律法规规定的情形。

第八条（公告异议程序）

数据产品知识产权登记申请经审查通过的，由上海市知识产权局发布公告。

自公告之日起 15 日内，利害关系人认为登记申请具有本办法第七条第二项至第四项规定情形之一的，或者任何自然人、法人或者非法人组织认为登记申请具有本办法第七条第一项、第五项至第六项规定情形之一的，可以向上海市知识产权局提出异议。

上海市知识产权局应当对异议进行审查，在 60 日内作出异议处理决定，并告知异议人和登记申请人。情况特殊、复杂的，异议处理期限可以延长 60 日。

公告期满无异议或者异议不成立的，由上海市知识产权局予以登记，通过区块链技术予以上链存证，并颁发登记证明文件。

第九条（登记证明文件）

登记证明文件包含以下内容：

（一） 文件名称；

（二） 证书编号；

（三） 登记号；

（四） 数据产品名称；

（五） 登记主体；

（六） 证件号码；

（七） 申请日期；

（八） 登记日期；

（九） 其他需要在登记证明文件上载明的内容。

第十条（变更登记）

已登记数据产品知识产权的转让、质押、许可使用以及登记内容变更的，应当通过管理平台进行变更登记。

数据产品知识产权转让的变更登记应当由双方共同申请，属于下列情形之一的，可以由单方申请：

（一） 继承、接受遗赠取得权利的；

（二） 生效的法律文书等设立、变更、转让、消灭权利的；

（三） 权利人姓名、名称或者自然状况发生变化的；

（四） 法律法规规定的其他情形。

第十一条（撤销登记）

数据产品知识产权登记后，上海市知识产权局发现已登记的数据产品知识产权具有本办法第七条规定情形之一的，应当予以撤销，告知权利人。

利害关系人认为已登记的数据产品知识产权具有本办法第七条规定情形之一的，可以向上海市知识产权局申请撤销。

上海市知识产权局经审查，应当在 30 日内作出撤销或者不予撤销登记决定，并告知权利人和利害关系人。

第十二条（注销登记）

权利人可以向上海市知识产权局申请注销已登记的数据产品知识产权。

因生效的法律文书等情形导致原权利人相关权利灭失的，由新权利人进行注销或者变更登记；无新权利人的，由上海市知识产权局进行注销登记。

第十三条（登记有效期及续展登记）

数据产品知识产权登记有效期为 3 年，自数据产品知识产权登记之日起计算。

涉及变更登记、撤销登记、注销登记的，登记部门要将相关信息及时传送存证。

数据产品知识产权登记存证有效期满，权利人应当在期满前 30 日内办理续展登记手续。每次续展登记的有效期为 3 年，自上一有效期满次日起计算。

第十四条（施行时间）

本办法自 2024 年 12 月 8 日起施行。

5. 《国家数据基础设施建设指引（征求意见稿）》

发文机关：国家数据局

发布日期：2024.11.22

时效性：草案/征求意见稿

前 言

党的十八大以来，以习近平同志为核心的党中央，敏锐把握新一轮科技革命和产业变革的新机遇，统揽中华民族伟大复兴的战略全局和世界百年未有之大变局，对发展数字经济作出重大部署，擘画了新时代数字中国建设的宏伟蓝图。

党的二十届三中全会明确提出“建设和运营国家数据基础设施，促进数据共享”。各地区各部门认真贯彻落实习近平总书记重要指示精神，积极探索数据基础设施建设，为数据要素市场化配置改革、建设全国一体化数据市场奠定了良好基础。同时也要看到，数字经济蓬勃发展对数据流通利用和价值释放提出了新的更高的要求，迫切需要更好发挥有为政府和有效市场作用，构建兼顾效率和公平、适应数据要素特征、发挥数据价值效用的国家数据基础设施。

按照党中央、国务院决策部署，国家发展和改革委员会、国家数据局、工业和信息化部在充分调研的基础上，组织编制了《国家数据基础设施建设指引》，力争在当前情况下，说清楚数据基础设施的概念、发展愿景和建设目标，指导推进数据基础设施建设，推动形成横向联通、纵向贯通、协调有力的国家数据基础设施基本格局，打通数据流通动脉，畅通数据资源循环，促进数据应用开发，培育全国一体化数据市场，夯实数字经济发展基础，为数字中国建设提供有力支撑。

一 、概念内涵

纵观人类经济发展史，每一轮产业变革都会孕育新的基础设施。农业经济时代，基础设施主要是农田水利设施。工业经济时代，公路、铁路、港口、机场、电力系统等成为新的基础设施。数字经济时代，网络设施、算力设施、应用设施等构建了数字基础设施。当前，数据成为关键生产要素，催生新的技术–经济范式，重塑产业发展方式，推动数字基础设施向数据基础设施延伸和拓展。建设和运营国家数据基

础设施，进一步促进数据“供得出、流得动、用得好、保安全”，对于支撑数据基础制度落地、构建全国一体化数据市场、培育发展新质生产力具有重要意义。

国家数据基础设施是从数据要素价值释放的角度出发，面向社会提供数据采集、汇聚、传输、加工、流通、利用、运营、安全服务的一类新型基础设施，是集成硬件、软件、模型算法、标准规范、机制设计等在内的有机整体。国家数据基础设施在国家统筹下，由区域、行业、企业等各类数据基础设施共同构成。网络设施、算力设施与国家数据基础设施紧密相关，并通过迭代升级，不断支撑数据的流通和利用。

二 、发展愿景

（一）主要目标

国家数据基础设施是数据基础制度和先进技术落地的重要载体。在数据流通利用方面，建成支持全国一体化数据市场、保障数据安全自由流动的流通利用设施，形成协同联动、规模流通、高效利用、规范可信的数据流通利用公共服务体系；在算力底座方面，构建多元异构、高效调度、智能随需、绿色安全的高质量算力供给体系；在网络支撑方面，构建泛在灵活接入、高速可靠传输、动态弹性调度的数据高速传输网络；在安全方面，构建整体、动态、内生的安全防护体系；在应用方面，支持传统行业转型升级，赋能人工智能等新兴产业发展。总体实现“汇通海量数据，惠及千行百业，慧见数字未来”的美好愿景。

（二）推进路径

当前，我国数据基础设施处于起步建设阶段，围绕流通利用业务场景，各地方各行业各领域探索形成多种有针对性的技术方案和解决路径，并在不断迭代发展。在推动技术设施化过程中，要注重发挥有为政府和有效市场双重作用，坚持自上而下布局、自下而上探索双向协同，鼓励大胆创新，支持先行先试，加快技术收敛，推动技术规模化部署、系统化应用，为构建高速互联、高效调度、开放普惠、安全可靠的国家数据基础设施奠定坚实基础。

2024–2026 年，利用 2–3 年左右时间，围绕重要行业领域和典型应用场景，开展数据基础设施技术路线试点试验，支持部分地方、行业、领域先行先试，丰富解

决方案供给。制定统一目录标识、统一身份登记、统一接口要求的标准规范，夯实数据基础设施互联互通技术基础。完成国家数据基础设施建设顶层设计，明确国家数据基础设施建设的技术路线和实践路径。

2027–2028 年，建成支撑数据规模化流通、互联互通的数据基础设施，数网、数算相关设施充分融合，基本形成跨层级、跨地域、跨系统、跨部门、跨业务的规模化数据可信流通利用格局，实现全国大中型城市基本覆盖。

到 2029 年，基本建成国家数据基础设施主体结构，初步形成横向联通、纵向贯通、协调有力的国家数据基础设施基本格局，构建协同联动、规模流通、高效利用、规范可信的数据公共服务体系，协同构筑数据基础设施技术和产业良好生态，国家数据基础设施建设和运营体制机制基本建立。

三 、总体功能

数字中国、数字经济、数字社会建设提出了数据要素化、资源化、价值化要求，国家数据基础设施围绕打造高速互联、高效调度、可信流通、安全可靠的体系化能力，持续赋能各行业数据融合与智能化发展。

（一）数据可信流通：开放普惠的数据流通

国家数据基础设施需要打造低成本、高效率、可信赖的流通环境，便于人、物、平台、智能体等快速接入，在符合统一目录标识、统一身份登记、统一接口规范的基础上，实现数据在不同组织、行业之间安全有序流动，精准匹配数据供需关系，面向电子商务、金融支付、跨境物流、航运贸易等典型场景创新融合数据应用，同时符合相关法律法规、社会伦理、个人隐私保护等要求。

（二）高效算力供给：多元异构的算力协同

算力资源多元异构、异地分布、动态变化，给大规模计算任务的统一调度与任务协同带来挑战。面向“东数西算”等场景中对异属异构异地算力的调度需求，需要建立多元异构算力统筹调度的能力，实现算力和运力的高度融合，实现算力资源之间的无缝对接与协同计算，提高整体计算效率与资源利用率，实现算力最优配置与动态调整。

（三）数据高速传输：高效弹性的数据传输网络

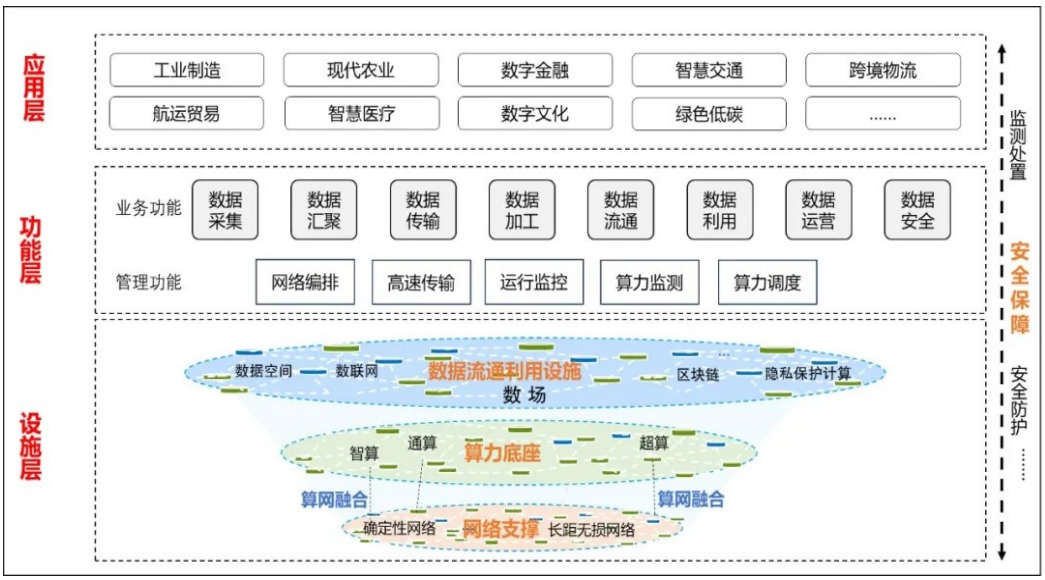
高效弹性的传输网络可为数字金融、智慧医疗、交通物流、大模型训练和推理等核心场景数据传输流动提供高速稳定服务。国家数据基础设施在高效弹性传输网络的支撑下，能够显著提升数据交换性能，降低数据传输成本，为数据大规模共享流通提供高质量通道。

（四）全程安全可靠：动态全面的安全保障

数据采集、汇聚、传输、加工、流通、利用、运营等多样化活动，涉及多方主体、多个环节，需要在开放环境下对数据进行整体、动态保护。国家数据基础设施需要构建标准化、多层次、全方位的安全防护框架，推动安全防护由静态保护向动态保护、由边界安全向内生安全、由封闭环境保护向开放环境保护转变，形成贯穿数据全生命周期各环节的动态安全防护能力，系统保障数据基础设施相关的网络、算力、数据安全。

四 、总体架构

（一）技术架构



国家数据基础设施具有数据采集、汇聚、传输、加工、流通、利用、运营、安全八大能力。在数据采集方面，支持通过传感器、业务系统等手段采集相关数据。在数据汇聚方面，通过标识编码解析、数据目录等，对数据进行高效接入、合理编目，实现数据广泛汇聚、存储和发布。在数据传输方面，支持节点即时组网、数据

高效传输。在数据加工方面，为参与方提供高效便捷、安全可靠的数据清洗、计算服务，建立数据质量控制和评估能力，提高数据处理环节效率。在数据流通方面，通过数据分类分级策略实现共享、交易等流通功能，为不同行业、不同地区、不同机构提供可信流通环境。在数据利用方面，为数据应用方提供数据分析、数据可视化等能力，进一步降低数据应用门槛。在数据运营方面，提供数据登记、监督管理、数据认证、合规保障等功能，有效支撑数据要素市场有序运行。在数据安全方面，提供动态全过程数据安全服务，包括防窃取、防泄露、防破坏等。在赋能方面，促进数据多场景应用、跨主体复用，赋能工业制造、现代农业、跨境数字货币、数字金融、智慧医疗、智慧交通、跨境物流、航运贸易、绿色低碳等行业领域。

其中，数据流通利用设施是国家数据基础设施的重要组成部分，为跨层级、跨地域、跨系统、跨部门、跨业务数据流通利用提供安全可信环境，包括可信数据空间、数场、数据元件、数联网、区块链网络、隐私保护计算平台等技术设施。网络设施、算力设施适应数据价值释放需要，向数据高速传输、算力高效供给方向升级发展。安全保障体系是国家数据基础设施安全可靠运行的保障，包括监测预警、信息通报、应急处置等相关制度、能力和队伍建设。

（二）主要构成

国家数据基础设施以行业、区域数据基础设施为主体，以企业数据基础设施为重要组成。企业数据基础设施是指服务企业生产、运营、管理的数据平台，包括采集、存储、处理、管理等相关硬件和软件系统，以及企业整合、协同关联数据方形成的数据服务平台。行业数据基础设施是指覆盖某一行业领域，服务行业内企业、用户及利益相关者，实现数据要素化、资源化、价值化的各类设施，包括行业数据流通交易平台、行业数据归集平台、行业数据公共服务平台等。区域数据基础设施是指覆盖本地区，服务区域内企业、用户及利益相关者，实现数据要素化、资源化、价值化的各类设施，包括数据归集平台、数据资源管理服务平台、公共数据运营平台等。国家在企业、行业、区域数据基础设施的基础上，组织建设基于统一目录标识、统一身份登记、统一接口要求的数据流通利用底座，搭建数据流通利用基础设施管理平台，以及建设数据产权登记、公共数据运营、数据资源管理、数据流通交

易、算力资源监测调度等基础公共服务的平台。这些设施相互贯通、协同推进，共同促进国家数据基础设施建设发展。

五 、重点方向

（一）建设数据流通利用设施底座

按照统一目录标识、统一身份登记、统一接口要求，建设数据流通利用设施底座。建立覆盖政府、行业、企业等主体及国家、省、市、县等层级的全国一体化的分布式数据目录，形成全国数据“一本账”，支撑跨层级、跨地域、跨系统、跨部门、跨业务的数据有序流通和共享应用。建立全国一体化的分布式数字身份体系，规范身份标识生成、身份注册和认证机制。建立统一的数据凭证、交易凭证结构、生成与验证机制，支持利用区块链、加密技术、智能合约等手段提高凭证的可溯性和信任性。构建标准化、规范化的交互接口，实现数据基础设施的互联互通。建设数据泛在接入体系，支持数据资源、参与主体、第三方服务更大规模接入。建立与 IPv6 等网络标识兼容的数据标识体系。建立数据目录分类分级管理机制，加强数据分类管理和分级保护。

（二）建设数据高效供给体系

在数据标注产业的生态构建、能力提升和场景应用等方面先行先试。链接各类公共数据、企业数据、个人数据以及各类高质量数据集，对社会形成统一的数据资源开放目录。研究制定高质量数据集建设相关标准，从数据生成、注释定义到数据管理的全过程，确保数据标注的准确性和数据模型的专业性。制定高质量数据标注与交付规则，提高训练数据质量。支持农业、工业、金融、自然资源、卫生健康、教育、科技、民航、气象等行业领域打造高质量数据集。因地制宜推进公共数据运营平台集约化、标准化建设，推进公共数据的规模化、常态化供给。推进数据资源管理服务平台互联互通，完善平台标准，促进平台间互操作，实现全国数据资源的跨领域、跨层级、跨区域流通利用。支持各地积极建设政务服务大模型，推动政务服务智能化。

（三）建设数据可信流通体系

建立高效便利可信的数据流通机制，促进数据大规模、低成本、安全自由流通。

支持建设企业可信数据空间、行业可信数据空间，探索建设城市可信数据空间、个人可信数据空间、跨境可信数据空间。支持基础好、有条件、意愿强的行业和城市，先行先试数场建设。鼓励行业、地方积极探索建设区块链、隐私保护计算等新技术设施。支持因地制宜，探索数联网、数据元件等数据流通基础设施建设。支持建设数据流通交易公共服务平台。支持探索建设数据跨境流动基础设施。建立数据流通准入标准规则，鼓励探索数据流通安全保障技术、标准、方案。

（四）建设数据便捷交付体系

加强数据交易场所体系设计，统筹数据交易场所优化布局。支持数据交易场所创新发展，鼓励各类数据进场交易。构建集约、高效的数据交付基础设施，为场内集中交易和场外分散交易提供低成本、高效率、可信赖的数据交付环境。促进各类交易所、交易平台互联互通。推动数据价值贡献度评估、数据集推荐匹配、数据产品差异性分析等技术创新，实现供需精准匹配和便捷交付。鼓励各地提升数据加工、测试、建模验证、安全实验等社会化服务能力，打造产学研用“一公里”工作圈。

（五）建设行业数据应用体系

加强场景牵引，建设面向工业制造、现代农业、数字金融、智慧医疗、智慧交通、跨境物流、航运贸易、卫生健康、绿色低碳等重点行业领域的数据应用基础设施，促进行业数据应用创新。培育基于数据要素的新产品和新服务，促进数据多场景应用、跨主体复用，实现知识扩散、价值倍增。

六 、算力底座

（一）推进算力资源科学布局

加快推动通用算力、智能算力、超级算力等多元异构算力的绿色发展、有机协同。促进各类新增算力向国家枢纽节点集聚，强化枢纽节点国家算力高地定位。建设全国一体化算力网监测调度平台。探索采用存算分离架构建设新型智算中心和新材料大数据中心。

（二）推进东中西部算力协同

加强新兴网络技术创新应用，优化网络计费方式，降低东西部数据传输成本，促进东部中高时延业务向西部转移。构建算力多级调度策略引擎，实现跨平台、跨

层级、跨区域的算力资源混合部署和统一调度，促进算力资源高效对接，提升数据汇聚、处理、流通、交易效率。推动国家枢纽节点和需求地之间 400G/800G 高带宽全光连接，引导电信运营商提升“公共传输通道”效能，推进算网深度融合。

（三）推进算力与数据、算法融合创新

推动实现“瓦特”产业向“比特”产业转化，不断壮大数算产业生态体系，助力打造具有国际竞争力的数字产业集群。推动行业数据和算力协同，实现数据可信流通，提升数据处理能力和治理水平。建立健全算法开发利用机制，积极开展大模型创新算法及关键技术研究，提升数据分析能力，降低大模型计算的算力消耗水平。

（四）推进算力与绿色电力融合

强化枢纽节点与非枢纽节点的协同联动，支持绿电资源丰富的非枢纽节点融入全国一体化算力网建设。加强大型风光基地和算力枢纽节点协同联动，把绿色电力转换成绿色算力。积极推进风光绿电资源消纳，助力实现碳达峰碳中和。支持利用“源网荷储”等新型电力系统模式。加强数据中心智慧能源管理，开展数据中心用能监测分析与负荷预测，优化数据中心电力系统整体运行效率。探索绿电直供新模式，有序开展绿电、绿证交易。

（五）推进算力发展与安全保障协同

推动建设国家算力网基础安全服务保障平台，打造一体化的安全保障服务能力。打造网络和数据安全攻防演习靶场，推动国家枢纽节点地区定期开展网络和数据安全攻防演习。建设算力网安全应用技术试验场。强化国家枢纽节点自主防护能力，统一应急处置、统一安全监测、统一运行监控，构筑全生命周期的安全管控措施。

七 、网络支撑

建设高速数据传输网，实现不同终端、平台、专网之间的数据高效弹性传输和互联互通，解决数据传输能力不足、成本较高、难以互联等问题。支持基础电信运营商叠加虚拟化组网、网络协议创新和智能化任务调度等云网融合技术，形成多方快速组网和数据交换能力，支持面向数据传输任务的弹性带宽和多量纲计费。

推动传统网络设施优化升级，有序推进 5G 网络向 5G-A 升级演进，全面推进 6G 网络技术研发创新。在东中西部地区均衡布局国际通信出入口局，加快扩展国际

海缆、陆缆信息通道方向。建设时延确定、带宽稳定保障、传输质量可靠的确定性网络。布局“天地一体”的卫星互联网。

八 、安全防护

国家数据基础设施安全保障体系建设重点是构建多层次、全方位、立体化的国家数据基础设施安全保障框架，贯穿数据生命周期全流程，帮助各参与方提升数据安全保障能力，确保数据的可信性、完整性和安全性。

在国家数据基础设施安全保障层面，实现可信接入、安全互联、跨域管控和全栈防护等安全管理，建立网络安全风险和威胁的动态发现、实时告警、全面分析、协同处置、跨域追溯和态势掌控能力，提供芯片、软件、硬件、协议等内置后门、漏洞安全威胁的内生防护能力。加强对合作伙伴、运维人员、平台用户等数据安全内部风险的防范应对。加强对入侵渗透、拒绝服务、数据窃取、勒索投毒等外部威胁的应急响应。

在数据流通利用安全层面，综合利用隐私保护计算、区块链、数据使用控制等技术手段，保证数据的可信采集、加密传输、可靠存储、受控交换共享、销毁确认及存证溯源等，规避数据隐私泄露、违规滥用等风险。加强算法、模型、数据的安全审计，增强模型鲁棒性和安全性，保证高价值、高敏感数据“可用不可见”“可控可计量”“可溯可审计”，确保贯穿数据全生命周期各环节安全。

九 、组织保障

（一）健全政策保障体系

建立健全数据基础制度体系，加快出台数据产权、流通交易、收益分配、安全治理等政策文件。在新型基础设施规划安排下，研究制定国家数据基础设施建设规划。加大中央投资对国家数据基础设施建设的支持力度。各地区、各部门要在数据基础设施规划布局、资金安排、课题研究方面给予重点支持。积极引导社会资本力量参与国家数据基础设施建设。

（二）加快技术创新探索

支持有条件的行业和地区开展先行先试探索建设数据基础设施。鼓励企业和科研机构加大研发投入，加快数据流通利用关键技术攻关和重大成果转化。通过国家

重点研发项目课题立项、揭榜挂帅、数据技术创新大赛等方式推动技术创新。

（三）强化标准和人才支撑

强化标准支撑，研究制定数据基础设施相关标准规范。鼓励企业、社会团体、科研机构参与数据基础设施国际标准的制定工作。加强与 ISO、IEC、IEEE、ITU、3GPP 等国际标准化组织的合作，推动数据领域高水平专家在国际组织任职。推动人才队伍建设，建立数据人才评价标准和评选机制。

附录：

技术术语解释

（一）数据流通利用技术

在数据流通利用领域，目前常用的技术路线主要包括隐私保护计算、区块链、数据使用控制等。

1.隐私保护计算

隐私保护计算指在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算的一类信息技术，保障数据在产生、存储、计算、应用、销毁等数据流转全过程的各个环节中“可用不可见”。隐私保护计算的常用技术方案有安全多方计算、联邦学习、可信执行环境、密态计算等；常用的底层技术有混淆电路、不经意传输、秘密分享、同态加密等。

2.区块链

区块链是分布式网络、加密技术、智能合约等多种技术集成的新型数据库软件，具有多中心化、共识可信、不可篡改、可追溯等特性，主要用于解决数据流通过程中的信任和安全问题。

3.数据使用控制

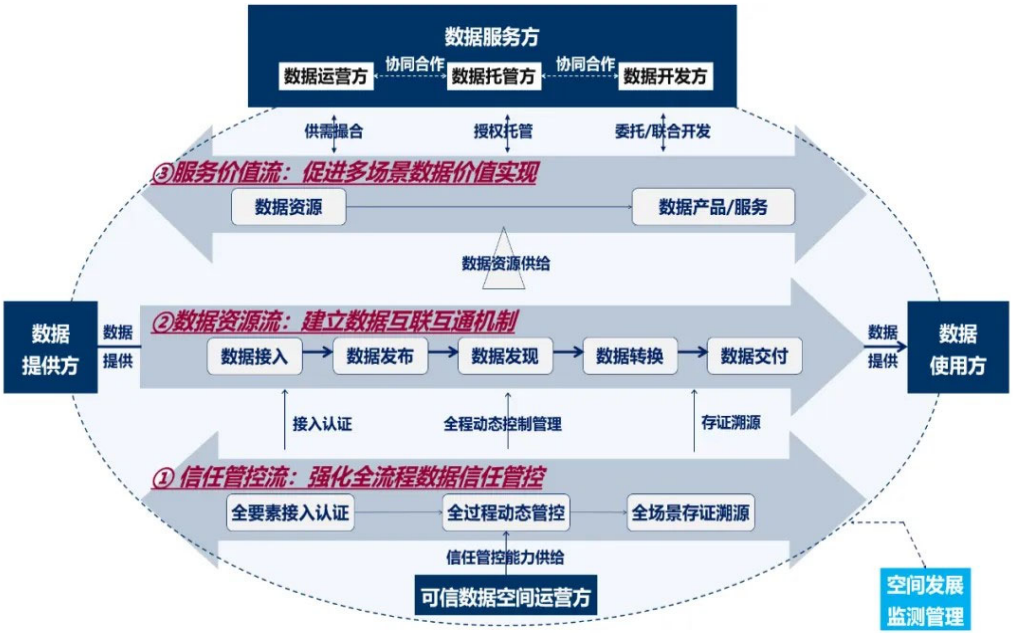
数据使用控制是指在数据的传输、存储、使用和销毁环节采用技术手段进行控制，如通过智能合约技术，将数据权益主体的数据使用控制意愿转化为可机读处理的智能合约条款，解决数据可控的前置性问题，实现对数据资产使用的时间、地点、主体、行为和客体等因素的控制。

（二）数据流通利用实践方案

在数据流通利用领域，目前业界的实践方案主要包括可信数据空间、数场、数联网、数据元件等。

1.可信数据空间

可信数据空间是指数据资源开放互联、可信流通的一类数据流通利用设施，其以数据使用控制为核心，以连接器为技术载体，以实现数据可信交付，保障数据流通中“可用不可见”“可控可计量”为目标，具备数据可信管控、资源交互、价值创造三大核心能力。

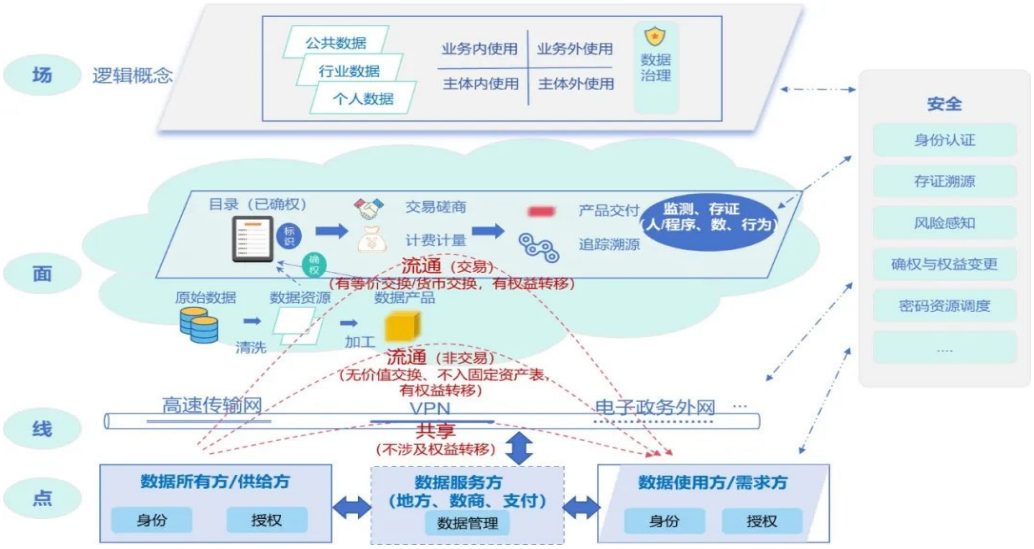


2.数场

数场是依托开放性网络及算力和隐私保护计算、区块链等各类关联功能设施，面向数据要素提供线上线下资源登记、供需匹配、交易流通、开发利用、存证溯源等功能，支持多场景应用的一种综合性数据流通利用设施。以高效流通、价值释放、繁荣生态为核心，实现数据可见、可达、可用、可控、可追溯，具备开放性、融合性、扩展性等特点。

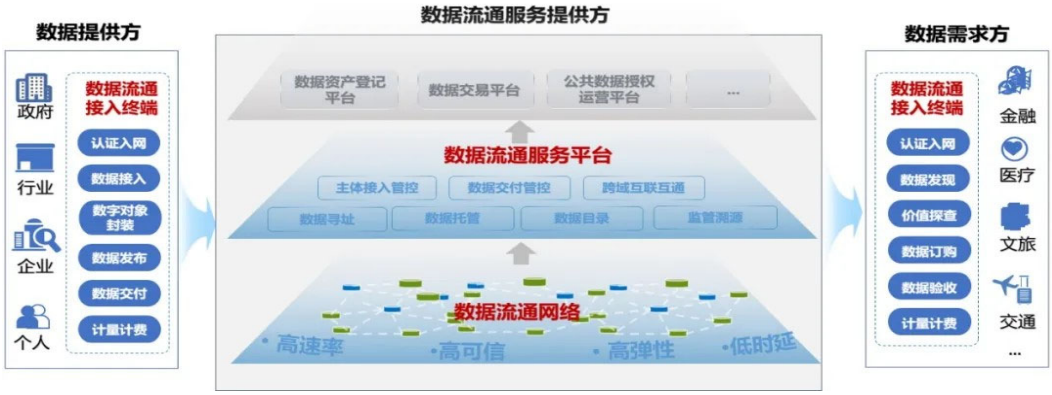
数场从点、线、面、场、安全五个维度构建标准化技术框架。点是数据主体进入数场的接入点。线是数场内连接各主体、各平台的数据高速传输网，实现数场内各主体之间的互联互通。面是数场中数据主体、传输网络的集合，是实现数据大规模流通、高效安全利用的核心。由点到线、由线到面构成数场基础设施。场是基于

数场基础设施构建的数据应用、场景化创新，以及相关能力、流程、规范的统称。安全是覆盖点、线、面、场的动态全流程保护措施。数场在技术架构上包括接入点、功能平台、管理平台、安全保障、网络传输等基础服务平台。



3.数联网

数联网由数据流通接入终端、数据流通网络、数据流通服务平台构成，提供一点接入、广泛连接、标准交付、安全可信、合规监管、开放兼容的数据流通服务。



4.数据元件

数据元件提供统一标准、自主可控、安全可靠、全程监管的数据存储和加工服务，支持采用标准化工序完成数据产品规模化加工、生产和再利用，适用于大规模数据加工和生产场景。数据元件作为连接数据供需两端的“中间态”，将原始数据与数据应用“解耦”，基于数据元件相关组件，实现从数据归集到数据元件加工交易全

生命周期的数据要素开发和管控。

（三）数据安全技术

数据安全技术为数据收集、存储、处理、传输、共享和销毁等全生命周期提供安全保障，包括数据备份与恢复、应用数据加密、数据泄露检测、流转监测、身份认证与访问控制、数据脱敏、数据水印、数据安全态势感知等。

6. 《关键信息基础设施商用密码使用管理规定（征求意见稿）》

发文机关：国家密码管理局

发布日期：2024.11.15

时效性：草案/征求意见稿

第一条【目的依据】 为了规范关键信息基础设施商用密码使用，保护关键信息基础设施安全，根据《中华人民共和国密码法》、《中华人民共和国网络安全法》、《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》、《商用密码管理条例》和《关键信息基础设施安全保护条例》、《网络数据安全管理条例》等有关法律、行政法规，制定本规定。

第二条【适用范围】 依据《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》等法律、行政法规和国家有关规定认定的关键信息基础设施的商用密码使用管理，适用本规定。

第三条【管理部门职责】 国家密码管理部门会同国家网信部门、国务院公安部门负责规划、指导和监督全国的关键信息基础设施商用密码使用管理工作，建立关键信息基础设施商用密码使用管理信息共享机制。

县级以上地方各级密码管理部门会同网信部门、公安机关负责指导和监督本行政区域的关键信息基础设施商用密码使用管理工作。

第四条【保护工作部门职责】 关键信息基础设施保护工作部门（以下简称保护工作部门）在职责范围内负责监督管理本行业、本领域关键信息基础设施商用密码使用工作，单独编制本行业、本领域商用密码使用规划或者纳入本行业、本领域的关键信息基础设施安全规划并组织实施，指导本行业、本领域关键信息基础设施运营者（以下简称运营者）做好商用密码相关制度、人员、经费等保障。

保护工作部门应当于每年 3 月 31 日前向国家密码管理部门、国家网信部门、国务院公安部门报告上一年度本行业、本领域关键信息基础设施商用密码使用管理情况。

关键信息基础设施发生涉及商用密码的重大网络安全事件或者发现涉及商用密

码的重大网络安全威胁时，保护工作部门应当及时向国家密码管理部门报告。

第五条【运营者总体责任】　运营者应当按照相关法律、行政法规和国家有关规定，遵循国家商用密码管理、网络安全等级保护、关键信息基础设施安全保护等制度要求，使用商用密码保护关键信息基础设施，同步规划、同步建设、同步运行商用密码保障系统，并定期开展商用密码应用安全性评估。

运营者应当于每年 1 月 31 日前向所属的保护工作部门报告上一年度关键信息基础设施商用密码使用情况。

第六条【制度保障】　运营者应当加强关键信息基础设施商用密码使用制度保障，建立商用密码使用、应急处置、重大事件报告等关键信息基础设施商用密码使用管理制度。

运营者的主要负责人对关键信息基础设施商用密码使用管理负总责，负责关键信息基础设施商用密码使用和涉及商用密码的重大网络安全事件处置工作。

第七条【人员保障】　运营者应当加强关键信息基础设施商用密码使用人员保障，配备取得密码相关专业学历或者密码相关国家职业技能等级认定证书的专业人员分别承担密钥管理员、密码操作员等职责，配备具有安全审计专业能力的人员承担密码安全审计员职责。

运营者应当对密码相关专业人员进行安全背景审查，并定期组织其参加密码相关业务技能培训，提高密码相关专业人员的商用密码使用能力。

第八条【经费保障】　运营者应当加强关键信息基础设施商用密码使用和应用安全性评估经费保障，将商用密码使用和应用安全性评估经费纳入网络安全和信息化经费安排。

第九条【商用密码技术、产品、服务使用要求】　关键信息基础设施使用的商用密码产品、服务应当经检测认证合格，使用的密码算法、密码协议、密钥管理机制等商用密码技术应当通过国家密码管理部门审查鉴定。为关键信息基础设施提供的商用密码服务，其商用密码使用要求应当不低于其服务的关键信息基础设施。

运营者采购涉及商用密码的网络产品和服务，影响或者可能影响国家安全的，应当按照《网络安全审查办法》进行网络安全审查。

第十条【数据安全保护、个人信息保护要求】　关键信息基础设施应当按照国家数据安全保护、个人信息保护有关要求，使用商用密码对其存储、使用、传输的核心数据、重要数据和个人信息进行保护。

第十一条【规划阶段要求】　关键信息基础设施规划阶段，其运营者应当依照相关法律、行政法规和标准规范，根据商用密码应用需求，制定商用密码应用方案，规划商用密码保障系统并纳入关键信息基础设施安全规划统筹部署。

运营者应当自行或者委托商用密码检测机构对商用密码应用方案进行商用密码应用安全性评估。商用密码应用方案未通过商用密码应用安全性评估的，不得作为商用密码保障系统的建设依据。

第十二条【建设阶段要求】　关键信息基础设施建设阶段，其运营者应当按照通过商用密码应用安全性评估的商用密码应用方案组织实施，落实商用密码安全防护措施，建设商用密码保障系统。建设过程中需要调整商用密码应用方案的，应当重新开展商用密码应用安全性评估，评估通过后方可按照调整后的商用密码应用方案继续建设。

关键信息基础设施运行前，其运营者应当自行或者委托商用密码检测机构开展商用密码应用安全性评估。关键信息基础设施未通过商用密码应用安全性评估的，运营者应当进行改造，改造期间不得投入运行。

第十三条【运行阶段要求】　关键信息基础设施建成运行后，其运营者应当自行或者委托商用密码检测机构每年至少开展一次商用密码应用安全性评估，确保关键信息基础设施商用密码的正确使用和商用密码保障系统的有效运行。关键信息基础设施未通过商用密码应用安全性评估的，运营者应当进行改造，并在改造期间采取必要措施保证关键信息基础设施运行安全。

第十四条【过渡安排】　本规定施行前正在建设的关键信息基础设施，其运营者应当加强商用密码应用方案编制论证，建设完善商用密码保障系统，并按照本规定第十二条开展商用密码应用安全性评估。

本规定施行前已经投入运行的关键信息基础设施，其运营者应当按照本规定第十三条开展商用密码应用安全性评估。

第十五条【商用密码应用安全性评估要求】　开展关键信息基础设施商用密码应用安全性评估，应当符合《商用密码应用安全性评估管理办法》有关规定。

关键信息基础设施商用密码应用安全性评估应当与关键信息基础设施安全检测评估、网络安全等级测评加强衔接，避免重复评估、测评。

第十六条【商用密码运行安全管理】　国家密码管理部门负责建设和管理国家关键信息基础设施商用密码运行安全管理基础设施，统筹保护工作部门建设本行业、本领域关键信息基础设施商用密码运行安全管理基础设施，会同国家网信部门、国务院公安部门分析研判关键信息基础设施商用密码运行安全态势，协同做好重大商用密码运行安全威胁应对措施。

第十七条【商用密码使用情况监督检查】　密码管理部门应当定期组织开展关键信息基础设施商用密码使用情况监督检查。保护工作部门应当定期对本行业、本领域关键信息基础设施商用密码使用情况进行检查并提出改进措施，必要时可以自行或者委托商用密码检测机构等专业机构进行商用密码应用安全性评估。

运营者对密码管理部门和保护工作部门开展的关键信息基础设施商用密码使用情况监督检查应当予以配合，根据监督检查意见及时进行整改并向保护工作部门报告整改情况，保护工作部门应当将整改情况向国家密码管理部门报告。

开展关键信息基础设施商用密码使用情况监督检查应当加强协同配合、信息沟通，避免不必要的检查和交叉重复检查。监督检查不得收取费用，不得要求被监督检查单位购买、使用指定单位或者指定品牌的商用密码产品、服务。

第十八条【保密义务】　密码管理部门、有关部门、商用密码检测机构及其工作人员对其在履行职责中知悉的国家秘密、商业秘密和个人隐私承担保密义务，不得泄露或者非法向他人提供。

第十九条【违反商用密码使用要求罚则】　运营者违反《中华人民共和国密码法》、《中华人民共和国网络安全法》、《商用密码管理条例》、《关键信息基础设施安全保护条例》和本规定有关条款，有下列情形之一的，由密码管理部门责令改正，给予警告；拒不改正或者有其他严重情节的，处 10 万元以上 100 万元以下罚款，对直接负责的主管人员处 1 万元以上 10 万元以下罚款：

（一）未按照要求使用商用密码保护关键信息基础设施，同步规划、同步建设、同步运行商用密码保障系统的；

（二）关键信息基础设施使用的商用密码产品、服务未经检测认证合格的；

（三）关键信息基础设施使用的密码算法、密码协议、密钥管理机制等商用密码技术未通过国家密码管理部门审查鉴定的；

（四）关键信息基础设施规划阶段，未制定商用密码应用方案，或者未对商用密码应用方案进行商用密码应用安全性评估的；

（五）关键信息基础设施建设阶段，未按照通过商用密码应用安全性评估的商用密码应用方案建设商用密码保障系统的；

（六）关键信息基础设施运行前，未开展商用密码应用安全性评估，或者未通过商用密码应用安全性评估且未进行改造的；

（七）关键信息基础设施建成运行后，未定期开展商用密码应用安全性评估，或者未通过定期开展的商用密码应用安全性评估且未进行改造的。

第二十条【违反安全审查要求罚则】 运营者违反《中华人民共和国密码法》、《中华人民共和国网络安全法》、《商用密码管理条例》、《关键信息基础设施安全保护条例》和本规定第九条，使用未经安全审查或者安全审查未通过的涉及商用密码的网络产品或者服务的，由有关主管部门责令停止使用，处采购金额 1 倍以上 10 倍以下罚款；对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款。

第二十一条【违反监督管理配合义务罚则】 运营者违反《中华人民共和国密码法》、《中华人民共和国网络安全法》、《商用密码管理条例》、《关键信息基础设施安全保护条例》和本规定第十七条，无正当理由拒不接受、不配合或者干预、阻挠密码管理部门、有关部门的商用密码监督管理的，由密码管理部门、有关部门责令改正，给予警告；拒不改正或者有其他严重情节的，处 5 万元以上 50 万元以下罚款，对直接负责的主管人员和其他直接责任人员处 1 万元以上 10 万元以下罚款；情节特别严重的，责令停业整顿。

第二十二条【违反商用密码保障责任罚则】 运营者违反本规定，有下列情形

之一的，由密码管理部门、有关部门依据职责责令改正：

（一）未按照要求报告上一年度关键信息基础设施商用密码使用情况的；

（二）未建立关键信息基础设施商用密码使用管理制度的；

（三）未按照要求配备密钥管理员、密码操作员、密码安全审计员的；

（四）未保障关键信息基础设施商用密码使用和应用安全性评估经费的。

第二十三条【监督管理人员罚则】　从事关键信息基础设施商用密码使用监督管理工作的人员滥用职权、玩忽职守、徇私舞弊，或者泄露、非法向他人提供在履行职责中知悉的商业秘密、个人隐私、举报人信息的，依法给予处分。

第二十四条【激励措施】　国家密码管理部门会同国家网信部门、国务院公安部门、保护工作部门定期通报表扬关键信息基础设施商用密码使用先进单位和突出事迹。

第二十五条【制度衔接】　属于国家政务信息系统的关键信息基础设施，除应当遵守本规定以外，还应当按照《国家政务信息化项目建设管理办法》〔国办发〔2019〕57 号〕等有关规定要求开展商用密码使用管理工作。

第二十六条【施行日期】　本规定自××××年××月××日起施行。

二、数安热点

1. 11 月 1 日起 13 项网络安全国家标准开始实施

11 月 1 日起，《网络安全技术 信息技术安全评估准则》等 13 项网络安全国家标准开始实施。

《网络安全技术 信息技术安全评估准则 第 1 部分：简介和一般模型》《网络安全技术 信息技术安全评估准则 第 2 部分：安全功能组件》等 6 项推荐性国家标准，是对软件、硬件、固件形式的 IT 产品及其组合进行安全测评的基础标准，为产品消费者、开发者、评估者提供了基本的安全功能和保障组件，内容吸纳了国际网络安全评估领域模块化评估、多重保障评估、供应链分析等最新理念，将为我国具有安全功能 IT 产品的开发、评估以及采购过程提供指导。

《网络安全技术 无线局域网客户端安全技术要求》《网络安全技术 无线局域网接入系统安全技术要求》2 项推荐性国家标准，规定了无线局域网客户端与接入系统的安全功能要求和安全保障要求，给出了无线局域网客户端与接入系统面临安全问题的说明，能够为无线局域网客户端产品与接入系统的测试、研制和开发提供指导。

《网络安全技术 零信任参考体系架构》《网络安全技术 证书应用综合服务接口规范》2 项推荐性国家标准，分别规定了零信任参考体系架构以及面向证书应用的综合服务接口要求和相应验证方法，对于采用零信任体系框架的信息系统的规划、设计，公钥密码基础设施应用技术体系下证书应用中间件和证书应用系统的开发，以及密码应用支撑平台的研制和检测具有重要意义。

《网络安全技术 软件供应链安全要求》《网络安全技术 网络安全众测服务要求》《网络安全技术 软件产品开源代码安全评价方法》3 项推荐性国家标准，分别确立了软件供应链安全目标，规定了软件供应链安全风险管理要求和供需双方的组织管理和供应活动管理安全要求，描述了网络安全众测服务的角色以及职责、服务流程、安全风险、服务要求，规定了软件产品中的开源代码成分安全评价要素和评价流程，对软件供应链中的供需双方开展风险管理、组织管理和供应活动管理具

有引领和促进作用，将为网络安全众测服务活动提供帮助指导，助力各方对软件产品包含的开源代码成分进行静态安全评价。

2. 全国数据标准化技术委员会拟制修订 37 项重点标准

为发挥标准在规范数据基础设施建设、促进数据资源高质量供给、推动数据高效有序流通、引领数据技术迭代创新、形成多元数据融合应用新格局的基础和支撑作用，围绕数据治理、数据流通利用、数字化转型、数据技术、数据基础设施等重点领域，全国数据标准化技术委员会提出了 2024—2025 年拟制修订的 37 项重点标准项目。

全国数据标准化技术委员会

2024-2025 年拟制修订的重点标准项目清单

序号	拟制修订的标准名称
1	《数据 术语》（修订）
2	《高质量数据集格式规范》
3	《高质量数据集类型与质量要求》
4	《数据流通匿名化效果评估方法》
5	《数据流通匿名化实施指南》
6	《数据基础设施 参考架构》
7	《数据基础设施 通用要求》
8	《枢纽节点公共传输通道网络传输服务与技术能力要求》
9	《算力网一体化监测调度》
10	《城市全域数字化转型 城市数据有效利用水平评估模型》
11	《数据服务能力评估 第 2 部分：流通交易类能力评估模型》
12	《数据服务能力评估 第 3 部分：第三方服务类能力评估模型》
13	《数据服务能力评估 第 4 部分：咨询服务类能力评估模型》
14	《数据服务能力评估 第 5 部分：应用创新类能力评估模型》
15	《数据服务能力评估 第 6 部分：产品平台类能力评估模型》
16	《数据服务能力评估 第 7 部分：资源集成类能力评估模型》

17	《数据服务能力评估 第 8 部分：加工分析类能力评估模型》
18	《数据服务能力评估 第 9 部分：安全技术类能力评估模型》
19	《公共数据 授权运营 第 1 部分：参考架构》
20	《公共数据 授权运营 第 2 部分：管理规范》
21	《公共数据 授权运营 第 3 部分：服务目录和服务规范》
22	《公共数据 授权运营 第 4 部分：绩效评估要求》 （拟更名为《公共数据 授权运营 第 4 部分：监测评估要求》）
23	《公共数据资源登记 实施指南》
24	《数据要素型企业能力要求》 （拟更名为《数据企业认定及评估规范》）
25	《数据登记平台通用技术要求》
26	《数据质量评价系统通用要求》
27	《数据空间 参考架构》
28	《数据空间 能力基本要求》
29	《数据空间 应用成熟度评价》
30	《城市全域数字化转型 术语》（修订）
31	《城市全域数字化转型 技术参考模型》（修订）
32	《城市全域数字化转型 顶层设计指南》（修订）
33	《面向分析和机器学习的数据质量 第 1 部分：概述、术语及示例》（采标）
34	《面向分析和机器学习的数据质量 第 2 部分：数据质量度量》（采标）
35	《面向分析和机器学习的数据质量 第 3 部分：数据质量管理要求和指导原则》（采标）
36	《面向分析和机器学习的数据质量 第 4 部分：数据质量过程框架》（采标）
37	《面向分析和机器学习的数据质量 第 5 部分：数据质量治理框架》（采标）

3. 北京互联网法院通报涉个人信息及数据相关案件审理情况

为深入贯彻落实党的二十大报告精神，加强《民法典》《个人信息保护法》和《网络数据安全管理条例》的实施落地，回应数字时代人民群众对个人信息保护的诉求，10 月 30 日上午，北京互联网法院召开新闻通报会，通报涉个人信息及数据相关案件审理情况及八起典型案例，并提出对加强个人信息保护和数据合理利用的建议。

党组成员、副院长赵瑞罡首先通报了涉个人信息及数据相关案件审理情况。自 2023 年 10 月至 2024 年 10 月，北京互联网法院共受理个人信息保护纠纷案件 113 件，已审结 104 件。经调研，此类案件侵权主体以互联网企业为主，涉诉个人信息类型多样，侵权形态主要涉及个人信息的知情权与决定权。从案件呈现的主要特征来看，个人信息保护与数据合理利用价值存在张力，权益主体主张的个人信息类型日益丰富，“AI 换脸”人工智能等新类型侵权案件不断涌现。通过案件审理发现，个人信息保护与数据合理利用中存在以下问题：一是个人在多元化在线场景中的个人信息保护意识和能力有待提升，二是个人信息处理者未严格履行法定义务引发信息安全风险，三是监管部门执法手段与风险预警措施需进一步加强。对此，北京互联网法院提出建议，应增强广大人民群众个人信息保护意识和能力，落实个人信息处理者的保护义务和责任，并进一步加强个人信息的保护与监管力度。

综合审判三庭法官王红霞通报了八起典型案例，包括“必要个人信息范围应结合相关规范性文件、服务性质、处理必要性等因素进行认定”“未经消费者同意，线下商店的线上小程序无权获取消费者的线下交易信息”“企业对经过去标识化处理后的个人信息进行访问所形成的访问记录，依法受法律保护”“信息处理者未尽到个人信息安全保障义务致他人个人信息权益被侵害的，应与侵权用户承担连带责任”等。

市人大代表邬光荣、刘克友、李丽萍、张向军、袁民、钱旻坤参加了本次通报会。通报会由综合审判三庭庭长颜君主持。央广《中国之声》、人民网、光明日报、中国日报、法治日报、法治周末、北京日报、北京新闻广播、新京报等媒体记者通过线上、线下方式进行参会、报道。

4. 快手公司因短视频中存在违法信息等问题被公安机关警告处罚

近日，针对快手公司短视频中存在违法信息等问题，公安机关依据《网络安全法》规定，依法给予快手公司警告处罚。经查，快手公司存在对法律、行政法规禁止发布或者传输的信息未及时处置，以及落实青少年模式不到位等情况，导致违法信息扩散，危害未成年人身心健康，违反了《网络安全法》相关规定。公安机关依法对快手公司给予行政处罚，责令其全面落实青少年模式，全面排查清理违法信息，并依法依规处置违法违规账号。

公安机关要求各互联网平台引以为鉴，举一反三，切实履行信息网络安全管理主体责任，严格落实网络实名制，加强源头治理、综合治理，有效防止违法信息传播，坚决防范违法信息对未成年人造成侵蚀危害。

5. 网信办提出全球数据跨境流动合作倡议

伴随数字技术渗透到人类生产生活的方方面面，全球数字经济快速发展，数字社会逐步成为人们分享文明进步的新空间。数据作为数字经济的关键要素，在创新发展和公共治理中正在发挥越来越重要的作用。数据跨境流动对于各国电子商务、数字贸易乃至经济科技文化等诸多方面至关重要，不仅可以有效降低贸易成本，提高企业开展国际贸易的能力，还有助于促进贸易便利化，加快产业数字化转型，弥合数字鸿沟，实现以数据流动为牵引的新型全球化。目前，国际社会正在积极探索形成全球数字领域规则和秩序，联合国制定发布《全球数字契约》、世贸组织电子商务谈判以及《全面与进步跨太平洋伙伴关系协定》（CPTPP）、《数字经济伙伴关系协定》（DEPA）等多双边实践正在开展，这些均体现了推动全球数据跨境流动合作、促进数据跨境流动已经成为各国或地区共同的意愿和选择。

我们注意到，在推动全球数据跨境流动实践的同时，各国普遍关注国家安全、公共利益、个人隐私以及知识产权等风险。我们认为，国际社会应在充分尊重各国、各地区因具体国情、社情而采取的不同政策法规和实践基础上，认真听取各方数据安全与发展的利益诉求，通过协商的方式推动国家间、地区间数据跨境流动规则形成共识。

我们呼吁各国秉持开放、包容、安全、合作、非歧视的原则，平衡数字技术创新、数字经济发展、数字社会进步与保护国家安全、公共利益、个人隐私和知识产权的关系，在推动数据跨境流动的同时实现各国合法政策目标。我们期待政府、国际组织、企业、民间机构等各主体坚守共商共建共享理念，发挥各自作用，推动全球数据跨境流动合作，携手构建高效便利安全的数据跨境流动机制，打造共赢的数据领域国际合作格局，推动数字红利惠及各国人民。

为此，我们倡议各国政府：

——鼓励因正常商业和社会活动需要而通过电子方式跨境传输数据，以实现全球电子商务和数字贸易为各国经济增长和可持续增长提供新的动力。

——尊重不同国家、不同地区之间数据跨境流动相关制度的差异性。支持不涉及国家安全、公共利益和个人隐私的数据自由流动。允许为实现合法公共政策目标

对数据跨境流动进行监管，前提是相关监管措施不构成任意或不合理的歧视或对贸易构成变相限制，不超出实现目标所要求的限度。

——尊重各国依法对涉及国家安全、公共利益的非个人数据采取必要的安全保护措施，保障相关非个人数据跨境安全有序流动。

——尊重各国为保护个人隐私等个人信息权益采取的措施，鼓励各国在保护个人信息的前提下为个人信息跨境传输提供便利途径，建立健全个人信息保护法律和监管框架，鼓励就此交流最佳实践和良好经验，提升个人信息保护机制、规则之间的兼容性，推动相关标准、技术法规及合格评定程序的互认。鼓励企业获得个人信息保护认证，以表明其符合个人信息保护标准，保障个人信息跨境安全有序流动。

——鼓励探索建立数据跨境流动管理负面清单，促进数据跨境高效便利安全流动。

——合力构建开放、包容、安全、合作、非歧视的数据流通使用环境，共同维护公平公正的市场秩序，促进数字经济规范健康发展。

——提高各类数据跨境流动管理措施的透明度、可预见性和非歧视性，以及政策框架的互操作性。

——积极开展数据跨境流动领域的国际合作。支持发展中国家和最不发达国家有效参与和利用数据跨境流动以促进数字经济增长，鼓励发达国家向发展中国家，特别是最不发达国家提供能力建设和技术援助，弥合数字鸿沟，实现公平和可持续发展。

——鼓励利用数字技术促进数据跨境流动创新应用，提高保障数据跨境高效便利安全流动的技术能力，推动数据跨境流动相关的技术与安全保障能力评价标准的国际互认，做好知识产权保护工作。

——反对将数据问题泛安全化，反对在缺乏事实证据的情况下针对特定国家、特定企业差别化制定数据跨境流动限制性政策，实施歧视性的限制、禁止或者其他类似措施。

——禁止通过在数字产品和服务中设置后门、利用数字技术基础设施中的漏洞等手段非法获取数据，共同打击数据领域跨境违法犯罪活动，共同保障各国公民和

企业的合法权益。

我们愿意在以上倡议基础上与各方开展和深化数据跨境流动领域的交流合作，我们呼吁各国、各地区通过双多边或地区协议、安排等形式呼应、确认上述倡议。欢迎国际组织、企业、民间机构等各主体支持本倡议。

6. 未按照要求完成整改 广东下架3款侵害用户权益APP

近日，广东省通信管理局发布关于下架3款侵害用户权益APP的通报。全文如下：

依据《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》等法律法规，按照工业和信息化部《关于进一步提升移动互联网应用服务能力的通知》（工信部信管函〔2023〕26号）等工作部署，广东省通信管理局持续开展APP隐私合规和数据安全专项整治行动。截至通报规定时限，经核查复检，尚有3款APP未按照要求完成整改反馈（详见附件）。

为严肃处理上述APP的违规行为，广东省通信管理局决定对该APP予以下架。相关应用商店应立即组织对该APP进行下架处理，并举一反三，排查反复出现问题的APP开发运营者，严格落实分发平台主体责任，把好上架审核关。广东省通信管理局将对通报APP持续跟踪，视情况进一步采取断开网络、行政处罚、纳入电信业务经营不良名单等后续处理措施。

同日，广东省通信管理局公开通报14款未按要求完成整改APP。全文如下：

依据《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》等法律法规，按照工业和信息化部《关于进一步提升移动互联网应用服务能力的通知》（工信部信管函〔2023〕26号）等工作部署，广东省通信管理局持续开展APP隐私合规和数据安全专项整治行动，发出《违法违规APP处置通知》责令APP运营者限期整改，并通知相关应用商店协助督促APP运营者整改。截至目前，尚有14款APP未完成整改（详见附件），现予以通报。

被通报的APP应在10月10日前完成整改及反馈工作。逾期不整改的，广东省通信管理局将依法依规采取下一步处置措施，切实维护APP用户合法权益和网络安全秩序。