数据安全治理白皮书

中国电子信息产业发展研究院

赛迪智库网络安全研究所

二零二一年六月

前言

在数字信息技术日新月异的发展趋势下，数据已成为数字经济发展的核心生产要素，是国家重要资产和基础战略资源。随着数据价值的愈加凸显，数据安全风险与日俱增，数据泄露、数据贩卖等数据安全事件频发，为个人隐私、企业商业秘密、国家重要情报等带来了严重的安全隐患。

当前，数据安全已成为数字经济时代最紧迫和最基础的安全问题，加强数据安全治理已成为维护国家安全和国家竞争力的战略需要。为此，国家高度重视数据安全的顶层设计：在相继发布的《促进大数据发展行动纲要》（2015）、《科学数据管理办法》（2018）、《关于构建更加完善的要素市场化配置体制机制的意见》（2020）以及“十四五”规划（2021）中，均提出发展数字经济、加快培育发展数据要素市场，应把保障数据安全放在突出位置的重要思想内涵。

面对数据安全威胁日益严峻的态势，着力解决数据安全领域的突出问题，有效提升数据安全治理能力迫在眉睫。然而，由于数字技术促使数据应用场景和参与主体日益多样化，数据安全的外延不断扩展，数据安全治理面临多重棘手困境。为此，本白皮书在分析我国数据安全风险、治理现状、治理困境的基础上，从政策、监管、产业生态建设、国际合作等方面提出综合解决路径。

目录

一、数据安全治理概述

（一）关键概念

1. 数据

数据，是用来记录客观事物或事件的符号，具体来说，是对客观事物或事件的性质、状态以及相互关系等信息进行记录的物理符号。本文中的数据包含任何以电子或者非电子形式对信息的记录，既包括网络数据，又包括线下物理场所存在的数据，并具备规模海量、类型多样、流转快速、价值巨大四大特征。

2. 数据处理活动和数据全生命周期

数据处理活动，包括数据的收集、存储、使用、加工、传输、提供、公开、销毁等，是数据处理者开展数据业务时实施的具体活动，所有数据处理活动环节共同构成了数据全生命周期。

3. 数据安全

数据安全，是指通过采取必要措施，确保数据在数据全生命周期中处于有效保护和合法利用的状态，以及保障持续安全状态的能力。数据安全保障主体包括掌握海量政务公共数据的政府部门，具备大量个人信息及商业信息的企业、持有众多国家基础重要数据的组织机构等诸多数据处理者。

4. 数据安全治理

数据安全治理，是指从决策层到技术层，从管理制度到工具支撑，自上而下建立的数据安全保障体系和保护生态，是贯穿整个组织架构的完整链条。具体来说，包含国家宏观治理和企业组织内部微观自治两个层面。**企业组织内部自治，**主要专注于数据生命周期安全的管理和技术防护措施，旨在规范企业组织数据全生命周期处理流程，保证数据处理活动的合规性和合法性。**本文所述的数据安全治理是站在国家宏观治理视角，**一方面，梳理国外数据安全治理现状，并分析其治理特色，探寻国际数据安全治理先进经验。另一方面，在从政策、监管、产业生态、国际合作等多个维度分析我国数据安全风险、治理现状、治理困境的基础上，提出我国数据安全治理路径。数据安全治理体系如图 1 所示。

5. 数据跨境流动

数据跨境流动，是指数据处理者将国家境内收集和产生的重要数据和个人信息，提供给位于境外的机构、组织、个人。数据跨境流动过程中，数据安全与个人隐私保护成为两大关键要素，世界各国对其进行明确立法的趋势也愈加明显。当前，出于保护本国数据、维护国家安全及促进国家发展目的，数据本地化存储呼声渐高，欧盟、印度、俄罗斯等诸多国家开始对关键领域数据实施本地化存储限制。

6. 数据资源、数据资产和数据资本

在数字经济的发展过程中，随着数据要素市场的蓬勃发展，数据价值的发展也分别三个阶段：**一是数据资源阶段，**数据是作为记录、反映现实世界的一种资源；**二是数据资产阶段，**数据是可创造财富的资产，且随着个人在互联网上活动的增多，积累的数据量越大，数据收益也越大。未来，数据资产可能将成为一种经数据所有者授权后，由数据管理者向使用者提供的一项服务。**三是数据资本阶段，**数据的资源和资产特性得到进一步发挥，在全社会形成巨大数据资产的基础上，可使用数据资产进行投资，将数据资产转化为数据资本。将数据资源资产化，进而资本化，对数据的所有者、管理者和使用者，均将产生巨大利益。

7.数据确权

数据确权，是指在厘清数据用途和流向的基础上，在法律上对数据权利，包括数据所有权、使用权和收益权进行明晰。

（二）数据安全治理本质

数据安全治理本质上包含“理”和“治”两个层面，先“理”后“治”，保障数据资源在安全可控的状态下充分发挥使用价值。一方面，需要“理”的内容包括数据资源的内容类型、分布流向以及不同场景下数据安全风险种类等。另一方面，需要“治”的内容包括数据安全保障制度体系、监管机制、数据安全保护生态、国际数据安全规则等。

（三）数据安全治理体系

数据安全治理体系包括政策环境、产业生态、监督管理和国际合作，如图 1 所示。**政策环境**主要是构筑数据安全顶层设计蓝图、建立稳定且具有国家强制力的法制框架、制定能够适应复杂数据利用场景的数据安全标准指南等；**监督管理**方面旨在探索构建分级分类监管体系、完善数据安全保护机构设置、联合开展专项整治行动、采取高额罚款等手段威慑数据违法违规行为、强化技术手段监管等；**产业生态建设**主要包括加大数据安全技术投资力度、推动数据安全产品和服务创新发展、加强数据安全人才队伍建设等；**国际合作**方面应积极参与并推动数据安全国际规则制定和完善、增强数据安全规则创制与话语权博弈的竞争力等。

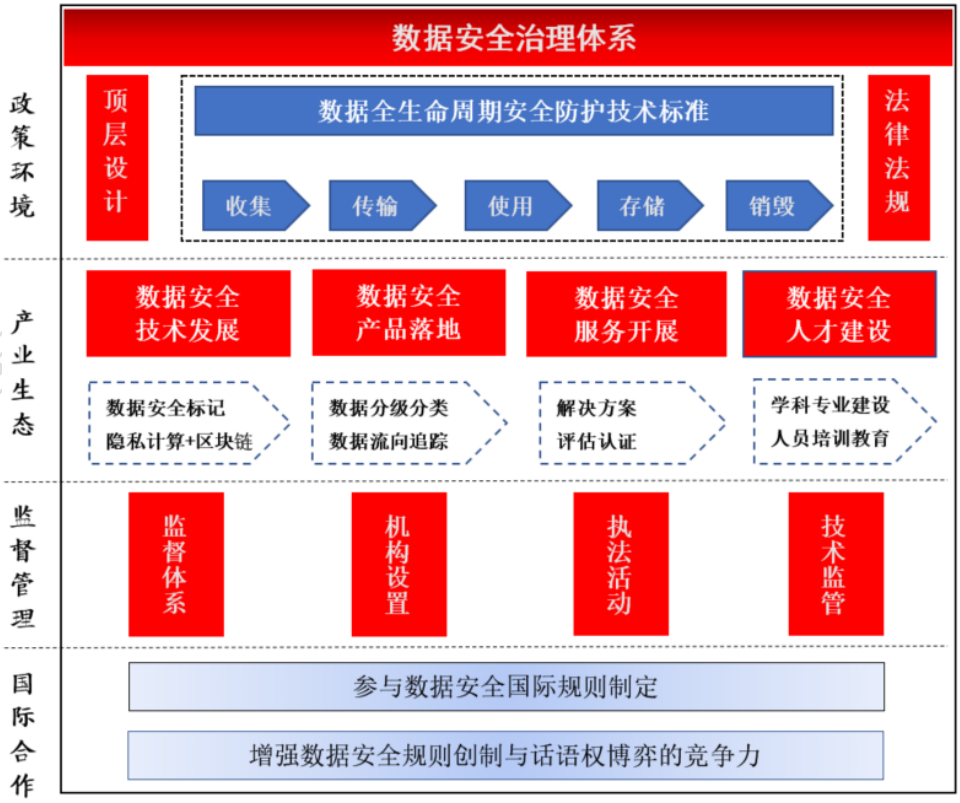

图 1：数据安全治理体系

二、国外数据安全治理现状

（一）数据安全政策环境持续优化

一是加强数据安全顶层设计。欧盟发布《欧洲数据保护监管局战略计划（2020-2024）》，旨在从前瞻性、行动性和协调性三方面继续加强数据安全保护，保证个人隐私的基本权利；美国发布《联邦数据战略与2020年行动计划》，确立了保护数据完整性、确保流通数据真实性、数据存储安全性等基本原则。**二是强化数据及个人信息保护相关立法。**阿联酋迪拜和新西兰分别出台《数据保护法》和《2020年隐私法》，加强对数据安全及个人隐私保护的规制建设；日本和新加坡分别完成了对本国《个人信息（数据）保护法》的修订，明确了个人数据权利及外部使用限制；加拿大提出《数字宪章实施法案 2020》，提出了保护私营部门个人信息的现代化框架。**三是陆续出台数据安全标准指南。**欧盟发布《为保持欧盟个人数据保护级别而采用的数据跨境转移工具补充措施》，为数据跨境流动中数据保护问题提供了进一步指导；西班牙数据保护局发布《默认数据保护指南》，阐释了默认数据保护原则的策略、实施措施、记录和审计要求等，为企业实践数据保护原则提供具体指导。

（二）数据安全保护机构设置不断完善

通过完善数据安全监管执法机构设置，提升执法效率，加强数据安全保护治理。例如，美国商务部成立提供联邦数

据服务的咨询委员会，加强联邦数据隐私保护；德国成立国家网络安全机构，负责发起网络安全创新项目、研究打击网络威胁的方法，以加强德“数据主权”；巴西总统签署法令批准建立国家个人数据保护局，负责制定相关规则、推进企业开展数据安全风险评估、调查违法违规行为、促进数据保护国际合作等；韩国成立个人信息保护委员会，负责个人信息保护与监管执法工作。

（三）推动企业强化数据安全保护技术手段初见成效

为进一步保障数据安全，各国纷纷采取措施推动企业积极响应当地政策，从数据源头、数据通道、数据运营管理等方面入手，积极运用差分隐私、区块链等技术手段强化数据安全保护，搭建具有鲜明数据安全保护特性的技术架构。例如，Facebook 通过开源差分隐私库加强对人工智能训练样本隐私性的保护；苹果公司通过模糊定位技术限制第三方 App 获取用户精确地理位置信息；亚马逊推出阻止用户敏感信息泄露的服务 Macie，保护企业云端敏感数据；新西兰企业通过区块链技术实现数据加密传输和追踪溯源，保护数据安全。

三、国外数据安全治理特色

（一）数据安全上升至国家安全层面

各国政府逐渐意识到，数据已成为与国家安全和国际竞争力紧密关联的一大要素，对数据安全的认知已从传统的个人隐私保护上升到维护国家安全的高度。美国国防部发布

《国防部数据战略》，指出战略的核心目标之一就是通过构建访问控制和最严格的安全标准来保护国防部数据安全，以实现数据推动作用下的联合全域作战，构筑国家安全保护屏障；英国发布《国家数据战略》，通过搭建国家层面的数据安全治理方案，为建设促进增长和可信赖的数据机制提供指导方向，保障国家安全；欧盟委员会相继发布《欧洲数据战略》及其配套法案《数据治理法案》提案，力求在欧盟层面建立统一的数据治理框架，保障数据安全。

（二）对大型互联网平台企业的数据执法力度持续加大

各国对大型互联网企业数据安全违法违规行为的惩治力度不断增强，美国、欧洲等国家和地区均增大了对其单笔处罚金额。例如，因 Facebook 违反用户隐私保护策略，美国对其处以 50 亿美元巨额罚款；爱尔兰也就数据非法跨境传输问题，对 Facebook 处以了高达 28 亿美元的罚款；法国、加拿大等国家也纷纷对 Twitter、谷歌等企业开出高额罚单。随着大型互联网平台企业的日益壮大，其数据垄断问题愈加严重，由此带来的数字权利滥用问题或将威胁到国家安全。因此，各国将进一步通过高额惩罚等手段对其进行约束，以防止其滥用数据优势侵害消费者隐私或进行非法数据贩卖。

（三）医疗、生物识别等个人特殊敏感数据的专项立法不断推进

当前，全球个人医疗数据泄露事件频发，人脸识别等新技术滥用导致个人生物信息长期处于高泄露风险状态，针对个人特殊敏感数据日益严峻的风险威胁，日本、美国等国家偏向于针对不同特征的个人数据采取精细化治理模式。例如，日本采用“基本法+专门法”的双重规制架构保护个人医疗信息安全。一方面，通过制定完善《个人信息保护法》等“基本法”确立个人医疗数据保护的基本原则，包括明确个人医疗数据的敏感信息特征、第三方使用的知情同意原则等；另一方面，出台《医疗大数据法》“专项法”平衡个人医疗数据的安全与使用矛盾，试图在数据安全流通的基础上，推动医疗研发进程。美国在各州及联邦层面均出台专项法案保护个人生物识别信息安全，包括为企业生物识别数据使用树立规范的联邦《国家生物识别信息隐私法案》，以及为限制公共部门生物识别技术使用的伊利诺伊州《生物识别信息隐私法案》、加利福尼亚州《加州人脸识别技术法案》等。

四、我国数据安全面临七大挑战

（一）数据贩卖严重侵害个人隐私

近些年，移动互联网技术的大力发展生产出海量数据资源，然而，大数据行业繁荣与隐忧始终并存，其中最为恶劣的影响即是数据交易地下黑色产业链的形成。目前，数据贩

卖已成为大数据产业的灰色地带，个人信息倒卖黑市猖獗，对个人人身、财产、生命安全造成了极大危害。**一是外部攻击者利用爬虫等技术窃取并倒卖个人数据。**例如，2020 年，国内第一家弹幕视频网站 AcFun 遭受黑客攻击，数千万条用户数据泄露并在“暗网”以 40 万价格出售。**二是“内鬼”常成为非法数据交易链源头。**例如，2020 年圆通快递内鬼倒卖四十万条公民姓名、地址、手机号和所购物品等个人信息。**三是平台之间实施暗箱操作，通过数据兜售进行数据商业变现。**例如，2021 年，北京智借网络科技企业未经用户允许，向下游合并公司出售包含姓名，身份证号，手机号等个人信息。**综上分析，**在数据价值利益的驱动下，数据贩卖产业链活跃程度将会进一步加深，个人隐私安全面临严重危机。

（二）数据跨境流动带来国家安全隐患

全球海量数据在网络空间中不断移动和流转，带来了经贸交易、技术交流、资源分享等跨国合作，数据的挖掘和利用释放了大数据价值、提升了经济效率、增进了社会福祉。但同时，跨境数据中不可避免地涵盖了个人敏感信息、企业运营数据和国家重要信息数据，并且随着数据规模不断的庞大、数据种类不断的丰富，数据安全风险也在日益加剧。尤其在大国博弈持续加剧的今天，数据作为国家重要的生产要素和战略资源，其日益频繁的跨境流动带来了潜在的国家安全隐患。**一是流转到境外的情报数据更易被外国政府获取。**

例如，目前拜登政府意欲采取公私合作方式开展军事网络战，实施“向前防御”战略，美私企很可能秘密将存储的我国数据提供给政府审查。**二是我国战略动作易被预测，陷入政策被动。**自 2008 年以来，美国大力推广微观数据的汇聚分析来预测金融风险，若美掌握我国海量数据，便可提前获知我国金融系统性风险，在国际金融博弈中获取先机。**三是我国以数据为驱动的新兴技术领域竞争优势将被削弱。**以人脸识别技术为例，我国具有丰富的数据资源，且相较国外文化更易收集人脸数据，因此发展出商汤科技等全球领先的初创公司，一旦我国独特的数据资源被他国获取，国外数据资源相对匮乏的短板会被迅速填补，从而实现反超，削弱我国竞争优势。

（三）高价值特殊敏感数据泄露风险加剧

近些年，除电子商务、社交等领域的用户数据发生大规模泄漏之外，政务、医疗及生物识别信息等高价值特殊敏感数据，逐渐成为了数据泄露的重灾区。**一是政务数据具有极高的社会和经济价值，黑客将其作为攻击目标可获得更高的利益回报。**例如，2015 年 30 省社保系统遭遇黑客攻击，造成数千万人信息泄露，黑客可通过数据贩卖获取高额利润，并随意修改社保待遇、停发社保金，将会造成民生混乱，影响社会稳定。**二是健康医疗数据具有高度隐私性和稀缺性，成为攻击者的关注重点。**医疗数据资产化趋势更为明显，是灰色产业中的主要交易对象。例如，2016 年全国超 330 位艾

滋病感染者信息泄露，期间患者接到诈骗电话上当受骗造成经济损失。**三是生物识别数据具有易采集和特征敏感性，成为攻击者的主要目标。**生物识别数据披露的个人特征精确，且采集门槛较低、极易获取，一旦遭到泄露、篡改或非法共享，极易造成“身份盗窃”风险。例如，2019 年深圳某企业利用街道摄像记录行人人脸图像，但却因数据库漏洞导致 250 万人脸数据泄露，使攻击者轻易掌握了行人身份及位置信息，可轻而易举实施犯罪活动。

（四）重要数据安全面临外来攻击威胁加大

一是具有政治背景的境外黑客逐渐加大对我国关键信息基础设施攻击力度，试图获取我国机密重要数据。例如，2020 年具有国家背景的印度黑客组织“白象”，以新冠疫情和全国两会新闻话题为诱饵，通过仿冒我国政府机构网站、伪造虚假政策文档等，蓄意对我国政府部门、医疗机构及其他关键信息基础设施开展网络攻击，窃取我国国情、社情、疫情等重要数据。**二是美国出台的“分层威慑战略”政策直指中国，**并已授权国防部对中国主动发起网络监视和侦察，我国关键信息基础设施或将面临着由美国主导联盟体发起网络攻击的风险，造成重要数据被监听和窃取。

（五）新技术新应用催生新型数据安全风险

新技术新应用在极大促进生产力发展和人民生活便利同时，也带来了安全方面的不确定性。以人工智能技术为例，

人工智能对分散数据的关联分析和深度发掘，可引发侵犯用户隐私、危害国家数据安全等传统安全风险，同时由于其独特的数据处理方式，还将可能引发数据污染、数据投毒攻击等一系列新型数据安全问题。

（六）互联网平台企业滥采滥用个人信息并实施数据垄断

随着数据安全内涵的延伸和扩大，除了机密性、完整性和可用性等数据本身的安全之外，对数据合法合规的收集使用也成为了数据安全的重要组成。当前，由于互联网平台企业的业务大都由数据驱动，商业推广、精准营销、产品迭代等均依赖对数据的海量收集和开发利用，数据成为了平台企业发展和盈利的核心引擎。基于数据收集使用创新商业营收模式，实现利益最大化，成为了各个平台企业追逐的商业目标，由此也引发了个人信息滥采滥用程度加重、数据垄断乱象频发的数据安全风险。例如，移动应用强制授权、过度索权等问题严重，用户个人信息自主权丧失；基于数据垄断优势进行“二选一”、“大数据杀熟”等，侵犯消费者权益。

（七）国际数据规则制定话语权与我国互联网应用领先地位严重不匹配

通过对近期美国发布的系列报告和政策文件分析，拜登政府意欲通过与理念相近国家组成“共同体”，构建网络安全联盟，掌控数据安全规则制定主导权。以美国为首的国际反

华联盟极可能以危害国家安全为由，将我国排除在全球数据安全治理体系之外，并可能制定针对我国的数据安全审查规则，在数据安全领域形成对我国的“包围圈”。例如，2020 年美、印、澳等多国以数据安全为由，联合对 TikTok 进行围剿，以安全调查结果违规为由，限制其使用发展。

五、国内数据安全治理现状

（一）数据安全政策持续加码

近些年，相关部门持续积极推进数据安全政策的制定与出台，我国数据安全相关政策布局不断提速。

数据安全相关法律法规密集出台。**一是，**目前我国已出台《网络安全法》、《民法典》、《数据安全法（草案）》和《个人信息保护法（草案）》四部数据安全保护基本法律框架。**二是，**围绕基本法制定的配套法规制度也在加快制定出台。**三是，**数据安全相关国家标准密集出炉，包括数据跨境流动、个人信息保护、新技术新应用数据安全防范、重点领域数据安全保护等方面。如表 1 所示。

表 1：数据安全相关法律法规及国家标准

时间	发布机关	名称	内容
2016	全国人大	《网络安全法》	从“个人信息保护”“数据存储与跨境安全”“数据（信息）内容安全”和“数据系统、平台、设施安全”等角度，对数据和个人信息合规方面予以规制。
2020	全国人大	《民典法》	明确了隐私定义，界定侵犯隐私权行为；明确了个人信息定义及范围；明确个人信息处理范围、要求及原则；明确个人信息主体权利，规定信息处理者义务；完善对患者的隐私及个人信息保密责任。明确数据活动必须遵守合法、正当、必要原则。

2020	全国人大	《数据安全法（草案）》	确立了数据分级分类管理以及风险评估、监测预警和应急处置等数据安全管理各项基本制度；明确了开展数据活动的组织、个人的数据安全保护义务及落实数据安全保护责任；强调坚持安全与发展并重，规定支持促进数据安全与发展的措施；建立了保障政务数据安全和推动政务数据开放的制度措施。
2020	全国人大	《个人信息安全法（草案）》	明确了个人信息处理规则、个人信息跨境提供的规则、个人在个人信息处理活动中的权利、个人信息处理者的义务、履行个人信息保护职责的部门等。
2019	网信办、工信部、公安部、市场监管总局	《App 违法违规收集使用个人信息行为认定方法》	界定了 App 违法违规收集使用个人信息行为的六大类方法，包括“未公开收集使用规则”、“未明示收集使用个人信息的目的、方式和范围”、“未经用户同意收集使用个人信息”、“违反必要原则，收集与其提供的服务无关的个人信息”、“未经同意向他人提供个人信息”、“未按法律规定提供删除更正个人信息功能”或“未公布投诉、举报方式等信息”等方面。
2019	网信办	《数据安全管理办法（征求意见稿）》	对近年来层出不穷的网络数据安全问题予以细化，包括个人敏感信息收集方式、广告精准推送、APP 过度索权、账户注销难等问题。
2019	网信办	《个人信息出境安全评估办法》	明确了个人信息出境安全评估的重点评估内容，规定所有个人信息出境均应当依法向网信办申报并由网信办组织开展安全评估；明确了个人信息主体在出境场景下知情权等权利履行的保障；通过系列设计加强对境外接收者的监督；全面规定了网络运营者与个人信息接收者签订的合同的具体内容。
2019	网信办	《儿童个人信息网络保护规定（征求意见稿）》	针对 14 岁以下的未成年人，规定了应设置儿童专门用户协议、设置专人负责、征得儿童监护人明确同意、加密存储和最小授权访问等儿童个人信息保护要求。
2020	网信办、工信部、公安部、市场监管总局	《常见类型移动互联网应用程序必要个人信息范围规定》	明确了 39 种常见类型 APP 的必要个人信息范围，要求其运营者不得因用户不同意提供非必要个人信息，而拒绝用户使用 App 基本功能服务，旨在有效规范 App 收集使用个人信息行为并促进 App 的健康发展。
2021	网信办、工信部、公安部、市场监管总局	《移动互联网应用程序个人信息保护管理暂行规定》	确立了“知情同意”“最小必要”两项重要原则；细化了 App 开发运营者、分发平台、第三方服务提供者、终端生产企业、网络接入服务提供者等五类主体责任义务；提出了投诉举报、监督检查、处置措施、风险提示等四方面规范要求。

2020	信安标委	《个人信息安全规范》	提出了个人信息控制者处理个人信息行为的规范，旨在遏制个人信息非法收集、滥用、泄露等乱象。
2020	信安标委	《政务信息共享 数据安全技术》	提出了政务信息共享数据安全技术要求框架，旨在加强政务数据共享过程中的数据安全保护。
2020	信安标委	《健康医疗数据安全指南》	提出医疗数据的分类体系、使用披露原则、安全措施等，旨在强化健康医疗数据的融合共享和开放应用过程的个人信息安全保障。
2020	信安标委	《网络预约汽车服务数据安全指南（征求意见稿）》	给出了网络预约汽车服务的数据收集、存储、使用、共享、公开披露、删除的类型、范围、方式和条件，旨在指导网络预约汽车服务运营者和相关监管部门规范服务相关的数据处理活动。
2020	信安标委	《即时通信服务数据安全指南（征求意见稿）》	给出了即时通信服务的数据收集、存储、使用、共享、公开披露、删除的类型、范围、方式和条件，旨在指导即时通信服务运营者和相关监管部门规范服务相关的数据处理活动。
2020	信安标委	《网络音视频服务数据安全指南》	给出了网络音视频服务的数据收集、存储、使用、共享、公开披露、删除的类型、范围、方式和条件，旨在指导网络音视频服务运营者和相关监管部门规范服务相关的数据处理活动。
2020	信安标委	《个人信息安全影响评估指南》	规定了个人信息安全影响评估的基本概念、框架、方法和流程，并提出了特定场景下进行评估的具体方法，旨在推动个人信息保护工作深入落地。
2020	信安标委	《电信领域大数据安全防护实现指南（征求意见稿）》	规范了电信领域大数据分类分级，基于电信领域大数据生存周期从管理和技术两方面给出了安全防护的实现指南。
2020	信安标委	《网络数据处理安全规范（征求意见稿）》	规定了网络运营者利用网络开展数据收集、存储、使用、加工、传输、提供、公开等数据处理活动应遵循的规范和安全要求，旨在为网络运营者的数据处理活动提供了更具操作性的指引，并为监督管理和认证机构的安全管理认证工作的开展提供有利参考。
2021	信安标委	《人脸识别数据安全要求（征求意见稿）》	规定了人脸识别数据的基本安全要求、安全处理要求和安全管理要求，剑指人脸数据滥采，泄露或丢失，以及过度存储、使用等问题。

2021	信安标委	《基因识别数据安全要求（征求意见稿）》	定义了基因识别数据，对基因识别数据在各场景各活动中的安全处理及安全管理要求进行了规定，旨在指导基因识别数据控制者安全开展基因识别数据业务，保证数据主体权利。
2021	信安标委	《声纹识别数据安全要求（征求意见稿）》	给出了声纹识别数据活动的四大场景，明确了声纹数据的基本安全要求、安全处理要求、安全管理要求。
2021	信安标委	《步态识别数据安全要求（征求意见稿）》	围绕个人信息安全，从全生命周期角度针对步态识别数据的特点提出相应的安全要求。
2021	信安标委	《网络支付服务数据安全指南（征求意见稿）》	规定了网络支付服务可以收集、使用、存储、共享、转让、公开披露的数据种类、范围、方式、条件等，旨在指导网络支付服务运营者和相关监管部门规范网络支付服务的数据处理活动。
2021	信安标委	《快递物流服务数据安全指南（征求意见稿）》	给出了快递物流服务的数据收集、存储、传输、使用、委托处理、删除、出境等数据处理活动的安全保护要求，旨在指导快递物流服务运营者和相关监管部门规范快递物流服务数据处理活动。
2021	信安标委	《网上购物服务数据安全指南（征求意见稿）》	规定了网上购物服务可以收集、存储、使用、交换、删除、出境的数据种类、范围、方式、条件等，旨在指导网上购物服务运营者和相关监管部门规范数据处理活动。
2021	信安标委	《移动互联网应用程序（APP）个人信息安全测评规范》	明确了开展 App 个人信息安全开展测评的实施过程以及对各项具体安全要求进行测评的方法，为第三方测评机构测评以及 App 提供者开展自测评提供指导。
2021	信安标委	《移动互联网应用程序（APP）SDK 安全指南》	规定了 SDK 提供者在 SDK 的开发、运营、个人信息处理、数据安全管理等活动中应遵循的安全要求，旨在指导 SDK 提供者和相关监管部门规范 SDK 使用。
2021	信安标委	《网联汽车 采集数据的安全要求（草案）》	规定了网联汽车采集的数据在传输、存储和跨境等环节的安全要求。
2021	信安标委	《个人信息去标识化效果分级评估规范（征求意见稿）》	给出了个人信息标识度的四种级别，以及个人信息去标识化效果评定流程和重标识风险计算方法。

各地方数据安全保护政策先行先试。以贵州省、天津市、深圳市、西安市为代表的省市最先探索数据安全治理相关棘手问题，包括贵州省出台大数据风险管理、政务数据开放共

享等相关政策文件，旨在探索数据开放共享与数据安全保护之间的有效平衡手段；西安市、深圳市出台政策文件尝试探索数据权属问题路径；天津市积极探索有效的数据交易流程，以规制数据贩卖等安全乱象。如表 2 所示。

表 2：数据安全相关地方性法规、地方政府规章、规范性文件

时间	地方	名称	内容
2016	贵州省	《贵州省大数据发展应用促进条例》	建立数据安全应急处置机制，制定应急预案，并在风险发生时开展应急演练；加强数据安全保护，鼓励大数据保护关键技术和大数据安全监管支撑技术创新和研究，支持科研机构、高等院校和企业开展数据安全关键技术攻关，推动政府、行业、企业间数据风险信息共享。
2018	贵阳市	《贵阳市大数据安全管理条例》	强化数据安全管理责任制；立大数据安全审计、应急处置、监测预警机制，实现对重要数据安全风险的全天候实时、动态监测；健全数据安全监管制度、大数据安全投诉举报制度。
2018	西安市	《西安市政务数据资源共享管理办法》	明确了政务公共数据权属类别，规定“政务数据资源权利包括所有权、管理权、采集权、使用权和收益权”，把政务数据作为政府的虚拟国有资产管理。
2018	天津市	《天津市促进大数据发展应用条例》	明确数据全生命周期各环节保障数据的范围边界、主体责任、具体要求；采取关键信息基础设施安全防护措施，加强防攻击、防泄漏、防窃取的技术和管理能力建设。
2019	天津市	《天津市数据安全管理办法（暂行）》	建立数据安全信息备案制度，要求组织个人信息和重要数据的数据运营者对主体信息、数据收集和使用规则、收集目的、方式、范围、类型等进行备案；建立数据安全信息通报制度，开展对监测信息、监督检查信息和上级通报信息的分析研判和风险评估，按照规定发布安全风险预警或信息通报；建立数据安全应急工作机制，定期开展应急演练，并对演练情况进行评估。
2019	海南省	《海南省大数据开发应用条例》	设立省大数据管理机构，作为实行企业化管理但不以营利为目的、履行相应行政管理和公共服务职责的法定机构；推动大数据与区块链等信息技术的融合，利用区块链技术加强数据安全保护。

2020	天津市	《天津市数据交易管理暂行办法》	建立了保障各方主体权益的数据交易全流程规范性制度；建立数据交易安全评估制度，包括数据供方出具报告对交易数据进行风险评估，数据交易机构健全第三方监督机制进行交易保护、开展事件应急处置等；健全数据交易过程的监督保障和责任追究机制。
2020	深圳市	《深圳经济特区数据条例（征求意见稿）》	探索数据权属定义，创设了个人数据权；设置了统一的数据统筹机构，明确了由市公安部门作为按照法律法规规定查处违法行为的行政处罚权实施机关。

行业数据安全专项保护政策陆续制定。**金融保险行业，**2020 年，中国人民银行发布、中国银保监会纷纷发布相关政策标准，旨在规范金融保险行业数据安全管理工作，提高数据安全保护能力。**电信和互联网行业，**2020 年，工信部发布系列文件指导电信和互联网行业的网络数据安全标准化工作。**车联网行业，**2020 年，工信部发布了车联网相关行业标准，旨在推动 2018 年提出的《国家车联网产业标准体系建设指南》中关于车联网个人信息保护和数据安全标准体系建设规划的立法发展。**工业互联网行业，**2020 年，工信部陆续发布了工业数据保护相关政策文件，为开展工业数据分类分级、管理能力评估、安全防护等相关工作提供了政策指导。如表 3 所示。

表 3：数据安全相关行业政策文件

时间	部门	名称	内容
2020	中国人民银行	《金融数据安全 数据安全分级指南》	给出了金融数据安全分级的目标、原则和范围，以及数据安全定级的要素、规则和定级过程，适用于金融业机构开展电子数据安全分级工作，并为第三方评估机构等单位开展数据安全检查与评估工作提供参考。

2020	中国人民银行	《个人金融信息保护技术规范》	将个人金融信息按敏感程度、泄露后造成的危害程度，从高到低分为C3（鉴别信息，如银行账户、登录密码等）、C2（可识别特定主体的信息，如身份证号、用户名、交易流水等）、C1（机构的内部信息，如开户机构等）三个类别，对相关机构建立不同信息保护层级方面提出了更高的要求。
2020	中国银保监会	《中国银保监会监管数据安全管理办法（试行）》	围绕“信用信息采集”“信用信息整理、保存、加工”“信用信息提供、使用”“信用信息安全”及相关监督管理措施对征信业务做出规定。
2021	中国人民银行	《征信业务管理办法（征求意见稿）》	对个人信用信息采集、整理、保存和加工进行了规范；从内控制度、软硬件设备、人员管理等方面对信用信息安全和跨境流动进行了规定。明确征信机构向境外提供个人信用信息，应当符合国家法律法规的规定，包括征信机构向境外提供企业信用信息的，应当向中国人民银行备案等。
2021	中国人民银行	《金融数据安全 数据生命周期安全规范》	梳理金融数据生命周期安全原则、防护要求、组织保障要求以及信息系统运维保障要求，建立覆盖数据采集、传输、存储、使用、删除及销毁全周期的金融数据安全管理框架
2020	工信部	《车联网信息服务用户个人信息保护要求》	规定了车联网信息服务用户个人信息保护的信息内容分类、敏感性分级和分级保护要求。适用于车联网相关的汽车厂商、零部件和元器件供应商、软件提供商、数据内容提供商和服务提供商等在提供服务过程中的用户个人信息保护。
2020	工信部	《车联网信息服务数据安全技术要求》	规定了车联网服务过程中数据生命周期内保护的总体要求，主要包括数据采集、传输、存储、使用、迁移、销毁、备份恢复等方面的安全保护要求。适用于车联网信息服务数据提供者或数据使用者的信息服务系统，车联网信息服务的数据提供者或数据使用者可以是汽车厂商、零部件供应商、第三方供应商、车联网服务提供商、4S 店、维修厂等。
2021	工信部	《智能网联汽车生产企业及产品准入管理指南（试行）》	规定了智能网联汽车生产企业应依法收集、使用和保护个人信息，实施数据分类分级管理，制定重要数据目录，不得泄露涉及国家安全的敏感信息。在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当按照有关规定在境内存储。因业务需要，确需向境外提供的，应向行业主管部门报备。

2021	网信办	《汽车数据安全管理若干规定（征求意见稿）》	明确汽车行业中重要数据的范围；对于汽车数据收集进行车内车外双场景的区分；强调最小必要原则和目的限制原则；提出数据全生命周期的处理要求；明确汽车行业数据本地化存储的原则要求和跨境数据传输的具体要求。
2020	工信部	《关于工业大数据发展的指导意见》	布局了 2 项重点任务，强调明确企业安全主体责任和各级政府监督管理责任，建立工业数据安全责任体系；支持安全产品开发，培育良好安全产业生态，多措并举创新和强化工业数据安全防护，筑好筑牢发展的底线和防线。
2020	工信部	《工业数据分级分类指南（试行）》	提出工业数据的基本概念，明确适用范围和原则；明确企业为数据分类分级主体，承担开展数据分类分级、加强数据管理等主体责任；按照每类工业数据遭篡改、破坏、泄露或非法利用后可能带来的潜在影响，将数据划分为 3 个级别。
2021	国家医疗保障局	《关于加强网络安全和数据保护工作的指导意见》	提出了加强医疗数据安全保护的相关要求，包括：实施数据全生命周期安全管理、实施分级分类管理、加强重要数据和敏感字段保护、强化数据安全审批管理、落实数据安全权限、推动数据安全共享和使用、建立健全数据安全风险评估机制。
2020	工信部	《电信和互联网行业数据安全标准体系建设指南》	提出基础共性、关键技术、安全管理、重点领域四大类标准，共同构成网络数据安全标准体系。
2021	住房和城乡建设部	《关于加快发展数字家庭提高居住品质的指导意见》	在数字家庭系统方面，要求强化网络和数字安全保障，保障数字家庭系统安全稳定运行，防止信息泄露、损毁、丢失，确保收集、产生数据和个人信息安全。遵守密码应用规定，形成安全可控完整的产业生态系统。

参与数据安全国际声明倡议的联合发布。近些年，我国在加强国内数据安全制度建设之外，也在积极为全球数据安全治理规则制定贡献中国方案，在加强和完善全球治理方面发挥了大国表率作用，并得到世界多国积极评价。如表 4 所示。

表 4：数据安全相关国际声明、公报、倡议

时间	名称	内容
2017	《金砖国家领导人厦门宣言》	我们将加强金砖国家在物联网、云计算、大数据、数据分析、纳米技术、人工智能、5G 及其创新应用等信息通信技术的联合研发和创新，提升五国信息通信技术基础设施建设和互联互通水平。我们倡导在基础设施安全、数据保护、互联网空间领域制定国际通行的规则，共建和平、安全的网络空间。
2018	《第五轮中德政府磋商联合声明》	双方同意双边网络安全磋商是讨论网络犯罪和网络安全合作的核心平台，同时双方可借助该磋商机制就网络立法对经济领域的影响进行交流，尤其是讨论网络给数据安全以及知识产权保护、侵犯贸易和商业秘密带来的风险和挑战。鉴于数据储存、数据使用和数据保护在未来工业核心领域发挥的重要作用，双方将在制定和实施各自网络安全法规时，为企业涉密数据保护和数据安全跨境传输提供保障。双方主管部门将直接对个案进行交流。
2018	《二十国集团领导人布宜诺斯艾利斯峰会宣言》	我们重申应对信息通信技术应用安全问题的重要性。在遵守相关法律并努力获得消费者信任、保护隐私、数据和知识产权的基础上，我们支持信息、思想、知识自由流动。我们欢迎二十国集团数字政策库，以此分享和鼓励应用创新型数字经济商业模式。我们认识到贸易和数字经济之间的关系的重要性。我们将继续推进人工智能、新技术和新商业平台方面的工作。
2020	《中俄总理第二十五次定期会晤联合公报》	鉴于数字经济对各国经济社会发展和全球治理体系的全面影响，及数据安全对各国国家安全、公共利益和个人权利的重要性，共同呼吁各国在普遍参与的基础上，达成反映各国意愿、尊重各方利益的全球数据安全规则。为此，俄方欢迎中方提出的《全球数据安全倡议》，支持中方为加强全球数据安全做出努力。
2020	《二十国集团领导人利雅得峰会宣言》	我们认识到基于信任的数据自由流动和跨境数据流动的重要性。我们重申数据对于发展的作用。我们支持营造开放、公平和非歧视环境，支持保护和赋权消费者，同时解决在隐私、数据保护、知识产权和安全方面的挑战。根据相关适用的法律框架继续应对这些挑战，我们可以进一步促进数据自由流动，并加强消费者和企业的信任。
2020	《中国—东盟关于建立数字经济合作伙伴关系的倡议》	深化网络空间合作，鼓励共建和平、安全、开放、合作有序的网络空间。双方在考虑各国法律与社会实际基础上，充分尊重网络主权，保护个人隐私和信息通信技术安全，推动建立多边、民主、透明的全球网络空间命运共同体。。共同加强数字基础设施安全保障，共建跨境网络安全事件响应信息共享体系，增进双方网络安全法律、政策理解。

2021	《全球数据安全倡议》	呼吁各国秉持发展和安全并重的原则，平衡处理技术进步、经济发展与保护国家安全和社会公共利益的关系。并提出以下倡议内容：各国应以事实为依据全面客观看待数据安全问题，积极维护全球信息技术产品和服务的供应开放、安全、稳定；各国反对利用信息技术破坏他国关键基础设施或窃取重要数据，以及利用其从事危害他国国家安全和社会公共利益的行为；各国承诺采取措施防范、制止利用网络侵害个人信息的行为，反对滥用信息技术非法采集他国公民个人信息；各国应要求企业严格遵守所在国法律。各国应尊重他国主权、司法管辖权和对数据的安全管理权，未经他国法律允许不得直接向企业或个人调取位于他国的数据；各国如因打击犯罪等执法需要跨境调取数据，应通过司法协助渠道或其他相关多双边协议解决。国家间缔结跨境调取数据双边协议，不得侵犯第三国司法主权和数据安全；信息技术产品和服务供应企业不得利用其产品和服务非法获取用户数据、控制或操纵用户系统和设备。
2021	《中阿数据安全合作倡议》	阿方欢迎中方提出《全球数据安全倡议》，支持秉持多边主义、兼顾安全发展、坚守公平正义的原则，共同应对数据安全风险挑战。双方一致认为：在全球分工合作日益密切的背景下，确保信息技术产品和服务的供应安全对于提升用户信心、保护数据安全、促进数字经济发展至关重要；各国有责任和权利保护涉及本国国家安全、公共安全、经济安全和社会稳定的重要数据及个人信息安全；欢迎政府、国际组织、信息技术企业、技术社群、民间机构和公民个人等各主体秉持共商共建共享理念，齐心协力促进数据安全。

（二）数据安全执法监督机制不断完善

数据安全监管机构机制初步明确。当前，我国数据安全监管正从各部门分散监管向以中央网信部门统筹协调，行业主管部门、公安机关等部门各司其职的监管模式转变。2020年，中央网信办成立网络数据管理局，直接负责“网络数据安全”方面的统筹监管。工信部、公安机关、市场监管总局等部门也相继在移动应用数据安全保护、数据反垄断等领域也开展了系列监管工作。此外，为夯实数据安全监管基础，

我国《数据安全法（草案）》进一步明确了各监管部门监管范围和基本职责。

数据安全联合执法机制逐渐建立。一是移动互联网应用专项整治行动升级，个人信息保护呈持续严管态势。2019 年，中央网信办、工信部、公安部、市场监管总局等四部门联合开展“App 违法违规收集使用个人信息专项治理”，旨在解决 App 强制授权、过度索权、超范围收集个人信息等问题。二是平台经济良性发展监管加强，数据垄断乱象纳入重点整治范畴。2021 年，市场监管总局等相关监管部门联合对美团、拼多多等平台企业进行约谈，剑指“二选一”、“大数据杀熟”等数据违规处理行为造成的个人数据使用风险。此外，网信办与市场监管总局、税务总局联合召开互联网平台企业行政指导会，指出信息泄露、强迫实施“二选一”，进行“大数据杀熟”等问题必须严肃整治，并要求各平台企业在一个月内全面自检自查，逐项彻底整改，并向社会公开《依法合规经营承诺》。

（三）数据安全产业生态建设稳步推进

积极促进企业数据安全产品和解决方案在行业场景和新基建中的应用落地。政府充分借助企业技术和人才优势，推动企业数据安全产品和解决方案在政务、金融、交通、医疗等重要行业数据安全防护体系建设中的广泛应用。以专注数据安全的高新技术企业闪捷信息为例，其数据安全产品和

解决方案已获取保密局、国家信息中心、公安部等权威机构认证，在商密、涉密领域均有建树，目前已与国内1000多家重要单位持续开展合作。此外，网络和数据安全是“新基建”的基础支撑，在“新基建”政策加持下，致力于自主研发的企业获得了相关部门的青睐。例如，致力于构建完整自主知识产权区块链应用体系的太一云、复杂美等企业，现已为国家多个部门的互联网应用层提供了安全稳定的区块链基础设施。

大力加强数据安全人才队伍建设。一是建设大数据安全人才培养基地，并在全国范围内与高效、企业合作开展数据安全人才培训。例如，中国信息安全测评中心成立中国网络空间安全协会大数据安全人才培养基地，并选拔国家级合作支撑单位，共同推动国家互联网网络安全大数据人才体系建设。二是设立信息安全学科、数据研究院等，致力培养数据安全专业人才。例如，复旦大学成立大数据研究院，设立培养专攻数据安全技术与理论、数据隐私保护、数据确权等方向的数据安全人才目标。三是开展系统专业认证培训及考试，为企业用人提供专业权威的参考，同时促进从业人员的专业技能提升。例如，中国信息安全测评中心开展的CISP数据安全治理、注册个人信息保护专业人员（CISP-PIP）认证，工信部电子工业标准化研究院开展的个人信息保护专业人员（PIPP）认证等。

大力发展数据安全产业示范区。数据安全产业示范区的建立会使数据安全企业与人才快速聚集，从而可快速形成强大的数据安全保护能力。为此，我国正积极推进大数据安全产业示范区建设，以奋力打造大数据安全产业发展先行先试的试验田。2018 年，在国家认证认可监督管理委员会的支持下，贵阳经济技术开发区创建了全国首个“大数据安全认证示范区”，截止 2020 年，贵阳大数据安全示范区已聚集了大数据安全企业和相关机构约 120 家，初步形成大数据安全产业发展的生态体系，产业产值突破 18 亿元。

六、我国数据安全治理面临的困境

（一）法律革新缓慢，数据行为秩序难规制

数据是数据驱动型企业的重要生产要素，对数据的占有和控制可强化企业的竞争优势，为其带来可观的商业利益。因此，在数据价值的诱惑下，部分企业利用法律的滞后性，试图脱离正常的数据行为轨道，造成了数据行为秩序的混乱。**一方面，**企业利用技术壁垒和快速革新优势，试图钻法律空子以脱离规制范围，例如，在我国尚无针对人工智能技术专项立法的现状下，部分企业利用人脸识别、深度伪造等技术滥采滥用个人数据实现利益最大化。**另一方面，**现有的法律制度难以对企业的数据商业使用行为进行有效的规制。例如，现行的《反不正当竞争法》以“因违背商业道德（如虚假宣传、仿冒商业标识等）而损

害竞争秩序”为认定不当竞争行为的基本框架，但此认定规则无法涵盖企业通过实施“二选一”对商家实施纵向约束进而独占交易的不正当竞争行为。

（二）数据权属争议大，数据产权难确立

当前，数据贩卖、数据无序竞争等行为频频发生且屡禁不止，此类数据安全乱象均是由于数据产权未确立，数据权利边界不明晰，数据利益分配模式存在缺陷所致。数据产权建设是数据安全治理的基础部分，也是数字经济健康有序发展的必要条件，“十四五”规划纲要中明确提出要加快建立健全数据资源产权基础制度。然而，由于数据的类型复杂、边界模糊、性质多样，数据相关权利体系复杂甚至冲突，导致数据产权确立困难。具体来说，不同类型的数据在权利内容上存在差异，且数据全生命周期链条上参与者众多，数据权利不完全归属于同一个主体，数据主体的不同导致利益诉求的差异性，从而引发数据权利的冲突。

（三）数据活动场景复杂，数据安全监管效能难提升

在数据全生命周期处理活动中，涉及众多数据技术、数据处理主体，且数据流动范围广，从国家内部的数据流转到跨国界的数据传输，均增大了数据活动场景的复杂性，也提升了数据安全的监管难度。**一是互联网技术日新月异，实现数据安全监管全覆盖难度大。**平台企业基于互联网技术进行数据的收集使用，并始终在技术和产品不断快速迭代中探索

全新的数据处理模式，这对监管制度的革新速度提出了高要求。**二是数据处理环节繁杂众多，进行数据安全监管定责难度大。**数据流通、应用及共享过程当中涉及了众多数据处理主体，且由于数据具有低成本的复制特性，数据泄露源头往往难以确定，为数据泄露后的安全事故定责带来了困难。**三是跨境监管没有统一国际标准，开展数据跨境流动安全监管难度大。**数据跨境流动可能导致国家关键数据资源流失，各国高度重视数据跨境流动监管这一国际性难题，但目前仍缺乏指导数据跨境流动监管的统一规范和国际规则，为我国建立数据跨境流动监管机制带来了一定挑战。

七、对我国数据安全治理建议

（一）完善数据安全法制建设，奠定数据安全保护基础

针对数据安全治理领域的痛点、难点问题，加快健全数据安全法律法规制度。**数据权属方面，**在明晰数据分级分类基本原则，各行各业进一步厘清自身行业数据的类型、特征、性质等基础上，探索数据分类确权制度，并立法对数据产权归属进行界定。**数据交易流通方面，**按照数据权属确定可交易流通数据的类型、范围和流通规则等，保护个人隐私安全。**数据垄断方面，**在反垄断法和反不正当竞争法等法律基础上，进一步完善平台企业数据垄断认定、数据收集使用管理、消费者权益保护等方面的法律规范。**关键数据保护方面，**考虑出台专项法律法规对医疗、政务、交通等行业高价值特殊敏

感数据进行分类保护，对不同关键信息基础设施运营者收集使用的重要数据分别进行单独防护，降低数据泄露风险。

（二）全面加强数据安全监督管理，促进制度落实执行

一方面，建议进一步探索建立分级分类监管机制，构建中央和地方分类监管、分级负责、权责一致的监管格局。此外，可借鉴美国、韩国、欧盟等国家和地区，针对不同数据活动场景及问题，尝试设置独立的负责机构。例如，与国际接轨、专项负责跨境数据安全风险审查与评估的机构。**另一方面，**在完善监管组织和机构职能的基础上，建议积极主动进行监管方法和流程的创新，将可能的风险点纳入监管范围，以适应复杂多变的数据活动场景。具体包括：一是组织开展数据安全风险调研。摸底调查企业、政府、组织等各主体在开展业务时面临的数据安全风险；组织开展国际跟踪研究，对新技术新应用潜在的数据安全风险进行研判。二是加强数据安全应急演练。鼓励各行业建立集中统一、上下联动的数据风险监测预警机制，定期开展数据安全风险防范演练，并组织专家针对演练中的风险进行处理效果检查。三是建立常态化数据安全专项审查行动。在现有移动 APP 专项整治行动的基础上，进一步开展生物识别技术非法使用情况审查、高价值数据非法交易的打击行动等。

（三）建立平台企业数据业务有序发展机制，保障数据合法合规使用

进一步探索政府数据安全宏观治理与平台企业内部治理之间的有效衔接机制。**一是压实平台企业数据主体的管理责任。**通过建立“事前”重要数据备案制度，组织平台企业对数据处理规则、数据处理范围进行备案，并制定针对数据备案主体的数据安全保护规范及责任制度；建立“事中”数据风险通报制度，开展信息监测和态势感知，对数据安全风险进行实时监控预警，在数据风险发布后要求平台企业及时启动应急预案、按照通报限时整改，落实数据通报制度；建立“事后”数据泄露通知制度，指导数据控制者落实个人信息泄露通知责任，将数据安全风险及时通报给相关部门和用户。**二是增强平台企业数据处理规则制定的外部参与性。**在移动应用程序数据收集使用方面，可加强对隐私协议模式和第三方服务的关注和优化。例如，将“一揽子”请求所有权限替换为动态申请服务相关所需权限；制定第三方 SDK 服务管理规则并限制其收集使用个人数据的范围。在基于大数据训练的算法使用方面，建立算法治理和监管规则，包括明确算法设计者、控制者及相关利益者披露算法设计原理、潜在漏洞的义务，并定期开展算法第三方评估等，以严格防范基于算法分析的“大数据杀熟”等数据垄断行为的发生。**三是鼓励企业提高数据安全竞争性。**强化监管的激励特性，可尝

试通过对具备成熟数据安全能力的企业进行官方宣传推广，塑造企业安全品牌优势，提升企业数据业务的安全竞争力，以激励企业强化内部数据安全能力建设。

（四）推动数据安全产业发展，构建全方位数据安全保护生态

大力推进国家大数据安全产业建设，支持产业创新发展，加快形成完整的数据安全保护产业生态链，以强化个人信息和国家重要数据的安全保障。**一是鼓励数据安全保护技术研究。**推动企业和相关研究机构积极开展区块链、密码技术、隐私计算等数据安全保障技术的研究。**二是进一步推动数据安全产品落地推广。**重点支持数据分类分级、数据共享安全监测、细粒度数据资源访问控制、数据标记及追踪溯源、数据安全威胁监控等相关产品的开发、成果转化和应用示范。并通过建立大数据安全靶场和产品检验场地，对大数据安全新应用、新产品进行测试、检验，通过开展优质安全产品使用布局，推动其在政务及关键信息基础设施等重要场景的应用。**三是培育数据安全培训、测评、认证等公共服务。**通过发展具有权威性的第三方机构，建设专业的数据安全人才培训和数据安全评估认证队伍，支持相关部门全面开展数据安全保护服务。

（五）推进全球数据安全治理，提升国际话语权

在数据安全治理领域，应继续践行多边主义理念，加强与各国的信任，共同建立数据安全治理国际合作机制，合力应对全球性数据安全挑战。**一是积极参与并推动数字领域国际规则制定和完善。**发挥政府、国际组织、企业、技术社群等各类主体作用，参与相关国际谈判与合作，推动制定符合国家利益和发展需要的数据安全国际规则。**二是加强数据安全国际治理的影响力输出。**联合中外智库、行业组织、高校通过举办数据安全治理高端论坛等，建立数据安全领域国际交流机制，并充分利用“一带一路”倡议、金砖国家、上合组织等机制和世界互联网大会、中国—东盟信息港论坛、网上丝绸之路大会等平台渠道，广泛宣传阐释《全球数据安全倡议》，积极传播中国声音。**三是鼓励企业参与国际竞争合作。**加强我国企业境外数据合规意识，鼓励我国企业开发国际化产品。同时，通过培育“走出去”联盟并搭建海外维权援助服务体系，促进我国企业“走出去”过程中加强技术、法律、政策等领域相互协调，推动产业界形成合力应对境外以数据安全为由实施的不合理政策和打压，增强企业“走出去”的风险防范和应对能力，冲破数据安全领域“包围圈”。