健全数据安全治理体系 增强网络安全防护能力

——2024数博会数据安全交流活动嘉宾观点荟萃

8月28日，主题为“健全数据安全治理体系，增强网络安全防护能力”的2024中国国际大数据产业博览会数据安全交流活动在贵阳国际会议中心举办。此次活动由数博会执委会主办，中国互联网协会承办，贵州省互联网协会协办，贵阳经济技术开发区管理委员会具体负责。

活动中，来自全国大数据安全领域的专家学者、行业领军人物齐聚一堂，围绕安全技术应用、数据跨境流动、安全体系构建等议题深入交流，共商数据安全大计，共谋数据发展蓝图，共同探索数据安全治理的新思路、新方法、新手段，推动以高水平数据安全服务护航数字经济高质量发展。

2024中国国际大数据产业博览会数据安全交流活动现场。

国家数据局党组成员、副局长沈竹林：

建强安全治理体系 激活数据应用价值

数据开发利用既能带来新的价值增量，也伴随着海量数据的汇集，以及跨系统、跨主体的大规模流动，对数据安全治理体系建设提出了新挑战。保障数据安全是激发数据要素价值的内在要求，越是推动发展越要守住安全底线，因此，如何更好地统筹发展和安全，是必须回答的时代之问。

我认为，应从动态安全保障、治理模式探索、对外合作开发等方面，加强数据安全治理体系建设，提高数据安全系统服务水平，在安全的前提下充分激活数据应用价值。

首先要探索保障动态安全，提升治理效能。随着数据进入社会化大生产，数据安全正从静态安全转向动态安全，因此，既要加强数据流通全过程的安全防护，也要建立数据安全可信流通机制。

其次要探索新型治理模式，包容创新发展。数据是人工智能发展的重要支撑，发挥它的作用需要探讨新的安全治理机制。如数据质量不足将影响算法模型的准确性，数据污染可能导致决策偏差。因此，既要加大数据的供给，增强发展支撑，也要创新体制机制，营造新产业发展的良好环境。

最后要推动高水平开放，深化合作共赢。随着数字经济发展的全球化，数据跨境流动成为了全球焦点。应坚持合作共赢、共同发展，既要完善规则制度，实现更高水平、更加安全的国际合作，也要发挥各自优势，让世界各国共享数字经济发展红利。

在全球化背景下，探索适应数据安全发展的治理体系，是全球各国面临的问题。国家数据局愿与各方从治理规则、机制、能力等方面协同发力，共同提升数据安全的治理水平，打造安全、开放、包容的创新发展环境，为推动数字经济发展保驾护航。

在完善治理规则方面，加强机制保障。国家数据局坚持问题导向、实践先行，聚焦数据边界不明、标准不具体等问题，不断健全数据流通等机制，持续出台可操作的合规指引，加强制度保障。

在创新治理机制方面，营造包容环境。国家数据局将统筹发展和安全，统筹风险防范和产业发展，总结各地方、行业探索的实践经验，推动构建适应新技术、新产业、新业态发展的数据安全治理机制，以更小的安全治理成本实现更大的安全治理效能。

在培育安全产业方面，强化支撑能力。数据安全防护能力是提升安全治理能力的重要支撑，国家数据局将大力培育安全产业，加快数据安全核心技术创新，持续提升安全可信流通、风险监测预警能力，为数据价值的释放提供有力支撑。

深圳数据交易所总经理古亮：

开展多方合作 探索跨境数据安全流通新路

在当前的数据交易市场，最活跃的数据交易类型中，包括进出口贸易、产品设计、用户特征、交易特性及购买力等相关数据。这些数据对于不断推动产品创新和市场适应性至关重要，尤其是随着人工智能、新能源汽车等行业的发展，对这些数据的需求日益增长。

基于这样的背景，为进一步做大进出口交易，深圳数据交易所做了大量实践，并取得了一定成效。截至7月，深圳数据交易所已完成了70多笔跨境数据交易。

在这过程中，深圳数据交易所与监管机构紧密合作，确保数据流通和交易合规性，并为行业数据交易提供安全保障。同时，交易所积极构建基础设施，包括监管和数据流动的基础设施，以促进数据交易的顺利进行。

为进一步丰富数据供应，特别是国际数据流进，交易所邀请了众多境外数据供应商入驻交易所并参与到数据流通合规体系建设中。目前，已有50多款境外数据产品在交易所上架，为相关行业提供服务。

在技术保护层面，深圳数据交易所采用了多种先进技术，来确保跨境数据流动的安全，包括基本的加密技术、隐私保护技术、动态加密技术和多方安全计算等，用以保障数据可用性和隐私性。同时，交易所利用可信数据空间技术，为人工智能、医疗、新能源电池等行业提供数据流通支持；利用区块链技术进行监管和审计，以保证交易的透明性和可追溯性。

尽管取得了一定成绩，但深圳数据交易所仍面临数据确权、定价、互信和监管等方面的挑战。保障数据安全是一个持续性过程，交易所还通过“一数一码”的数据认证和授权技术研发等措施，应对新的安全挑战。

亚信安全CTO兼高级副总裁陈奋：

提升技术管控水平 应对AI时代数据安全挑战

未来，任何产业的发展都离不开AI的助力。然而，在享受AI带来的便利的同时，如何平衡数据安全与效率的关系，是一个必须直面的挑战。

从技术角度来说，首先是在数据训练阶段进行安全管控。很多企业或行业会自己训练模型，这会涉及到训练阶段的数据安全问题。在AI模型训练阶段，必须对数据的安全性、敏感性进行严格管控。无论是内部数据还是外部数据，一旦数据在训练阶段出现问题，将直接影响模型的安全性和可靠性。

对于未能在训练阶段得到充分安全保护的模型，要在模型使用阶段进行数据安全过滤。

此外，针对企业使用开源或公有云上的AI模型时可能存在的风险，建议建立内部提示词规范，防止敏感信息泄露到公有云平台。要在AI的大模型使用中实现效能与安全的平衡，关键在于采取综合性安全管控手段，确保在整个模型训练周期中，对数据安全进行全方位保护，防患于未然，从源头确保数据的安全可靠。

工业和信息化部网络安全管理局一级巡视员闫宏强：

推动数据安全与产业融合 筑牢数字中国安全屏障

随着人工智能、5G信息通信技术与传统产业的深度融合，数据作为新的生产要素，正不断塑造新发展、新动能、新优势。

我国拥有全球最大规模的通信网络与工业体系，工业和信息化领域是国家数字经济和实体经济融合发展的主阵地，每天都在产生汇聚大量关系国计民生的数据资源。同时，各细分行业领域结合实际，积极推动大数据、人工智能等技术在研发设计、生产制造、运营管理等方面的应用，帮助各行业、各领域提升生产效率和产品质量，降低运营成本和风险，塑造新的竞争优势。

在数据重要性与日俱增的同时，数据安全风险和威胁也如影随形，数据安全形势日益严峻，防护工作刻不容缓。在实体经济和数字经济深度融合中如何强化安全保障？我从四个方面提出建议。

强化政策标准供给。工业和信息化部将紧密结合工业和信息化领域，以及各细分行业的特点，积极研究制定具有针对性、可操作性的政策标准规范。如，云服务虽大幅提升了工作效率，但也带来了大规模的数据泄露和宕机风险。下一步，工业和信息化部将结合一些典型事件和案例，制定有针对性的安全合规指引。

推动重点工作落实。工信领域主体多元，数据种类丰富，应用场景复杂。应抓牢重点企业、重要数据、重点场景，指导企业始终将重要数据保护摆在首位，做好识别备案、分级保护、风险评估、跨境流动等工作，确保数据安全。同时，聚焦重点场景，围绕关键数据处理、数据要素流通等场景特征，分析薄弱环节和保护需求，打造一批数据安全保护解决方案。

积极应对新技术带来的风险挑战。人工智能、区块链等新技术的发展应用，催生了新的业态和模式，随之也产生了新的数据安全风险。全行业应进行密切跟踪，提早研究模块风险防范策略和应对措施，增强风险管理手段。

培育数据安全产业。应加强数据安全基础理论和技术研究，突破数据安全的关键核心技术，在国内统筹布局，建设数据安全产业园区，推动产学研用协同发力，着力打造良好的产业生态。

数据安全工作至关重要，要夯实数据安全基础，培育创新发展新动能，打造网络安全新格局，加快提升我国工业和信息化领域的数据安全产业核心竞争力，共同筑牢制造强国、网络强国和数字中国的安全屏障。

中国工程院院士、中国互联网协会专家咨询委员会主任邬贺铨：

加强安全技术应用 保障AI时代数据安全

AI时代的到来进一步扩展了数据安全内涵，放大了数据安全风险，数据流动管理面临巨大挑战，应加强数据安全技术应用，做好数据安全管理。

数据安全是数字经济健康发展的核心保障。数据成为重要的生产要素，如何做到既让数据流动，又确保数据安全？我认为，应从完善机制、搭建平台等方面，通过数据可靠性技术、数据安全技术、数据服务与内容安全技术等，加快提升安全管理水平，更好地支撑AI时代的数据安全流动。

在推动安全技术应用方面，政府应积极引导、扶持建立行业或区域的网络安全威胁情报共享机制，以及相应的技术支持平台，支持建设面向中小企业的第三方安全云，利用AI安全大脑协助全面守护。加快建立体系化的安全运营服务框架，面向各行各业输出数字安全能力，帮助企业构建安全防御体系，保护数据安全。

人工智能等数字技术，本身既是安全防御的重点，也是安全保障的有力手段。需要将大数据、人工智能、互联网等技术融合，提升数据安全保障能力。可通过建立数据融合的安全计算平台，实现数据融合和数据可用。然而，并不是每个企业都具备建设可信数据融合安全计算平台的能力，政府应积极支持有能力的企业搭建平台，实现数据共享和安全运用。

AI时代还存在数据可信性的问题，即便是训练过的人工智能，源头数据如果不可信，也会使AI误判。AI时代深度伪造的信息危害更大，AI被广泛应用，会增加很多前所未有的安全挑战，各方应携手加快研发推出切实有效的数据安全防护技术，共同应对AI时代带来的挑战。

上海观安信息技术股份有限公司创始人、董事长张照龙：

建好防护体系 促进数据安全跨境流通

如何促进数据跨境有序安全流动，助推高水平对外开放合作？我认为，关键是要建好数据安全防护体系，加强数据使用过程全生命周期的安全保障。

做好整体数据安全工作，要理清楚两个关系。一方面是理清人和数据的关系，数据是被人使用的，是动态的流动性过程，数据要么是内部人员在使用，要么是外部人员在共享，在用的过程要保证数据的安全性；另一方面是理清数和数的关系，在数据跨境过程中，一般是数据进行自动化收集或网端调用，这个数和数之间连接的过程，要保证数据的安全性。

在数据安全体系中，如果要实现大规模的数据治理和数据共享，要搭建四个基础体系来保障数据安全：搭建数据安全组织体系，搞清楚谁管什么，责任是什么，谁来制定制度，谁来运营；搭建制度体系，数据跨境牵扯到不同国家和区域，要建立国际合作，共同建立一套行之有效的、大家认可的统一标准，保证数据安全和合规跨境；搭建安全有效的技术保护体系，护航数据跨境；搭建一体化数据运营体系，促进数据高效运营。

在促进数据跨境安全应用中，应关注六个要点：在促进数据“聚”的过程中保护好数据安全；在算力使用和算力调用改称中保护数据安全；在数据跨境过程中保护数据安全；在网络通信过程中，根据数据不同级别进行不同级别的有效加密和传输；用人工智能算法保护数据安全，以及保护人工智能算法模型的安全；在使用过程中有效防止数据被滥用、被篡改、被违规使用。

贵阳日报融媒体记者 黄菊 蔡婕/文 徐其飞/图