MIN YING SHI DIAN | 民营视点

“上山”“下海”为数字经济护航

本报记者 孙 琳

“数字经济在突破传统生产要素的流动限制，促进市场效率的同时，也带来了不容忽视的信息安全问题，这就要求我们必须筑牢数字安全屏障。”

“随着数字化技术更广泛和深入地服务于社会经济，数字安全的基础性作用日益突出，一些重点领域重点问题需要破解，数字安全将面临新一轮的转型升级。”

……

在近日举行的“2022全球数字经济大会——数字安全峰会暨ISC2022互联网安全大会”上，关于数字时代如何构筑数字经济安全新长城的路径正逐渐清晰。

▶▶▶数据安全治理正加强

当前，全球经济社会正加速向网络化、数字化、智能化转型，全球数据规模呈增长态势，海量数据成为数字化转型后的重要资产，以数据为关键要素的新产业、新场景面临更加复杂的安全挑战，保障数据安全亦成为数字时代的必然课题，也是数字安全新一轮升级的必然方向。

在全国政协社会和法制委员会副主任、公安部原副部长陈智敏看来，在全面进入数字时代的当下，维护国家数据安全，保护个人信息、商业机密的任务则面临更大挑战。而这些都离不开对数据的有效安全治理。

事实上，为了保障数据安全，近年来我国已相继出台网络安全法、数据安全法、《关键信息基础设施安全保护条例》、个人信息保护法等法律法规，明确了重要数据处理者的数据安全保护义务。

更值得一提的是，近年来，国家网络基础设施安全防护水平持续提高。据工信部网络安全管理局局长隋静介绍，工信部制定了工业和信息化领域数据安全管理办法，建立工业和信息化领域数据安全风险报送与共享机制，深化电信和互联网企业数据安全合规自评，启动工业领域数据安全管理试点、工信领域数据安全管理体系。与此同时，还面向工业互联网、车联网、5G等新型基础设施，相继出台加强网络和数据安全管理的系列政策文件。

“在政策的引导下，近年来我国网络安全产业综合实力已显著增强。”隋静表示，未来还将继续完善制度规则，强化行业数据安全治理能力，加快建立数据分类分级保护、跨境数据流动监管等基本规则。

“如针对不同数据类型、不同数据用途、数据敏感程度等，完善分级分类管理办法，规范数据采集、传输、存储、处理、共享、销毁全生命周期管理；推动数据使用者落实数据安全保护责任，维护国家数据安全，保护个人信息和商业秘密，守住数据安全底线。”隋静说。

近日，国家互联网信息办公室已公布《数据出境安全评估办法》（以下简称《办法》），将于今年9月1日起施行。业界普遍表示，《办法》出台及时必要，是对数据安全治理的进一步加强，可以更好规范数据出境活动，保护个人信息权益，维护国家安全和社会公共利益，促进数据跨境安全、自由流动，真正做到“以安全保发展、以发展促安全”。

但面临新时代的数据安全问题，也需要新的防御思路。为此，陈智敏表示，要用控制论、信息论和系统论思维，来考虑数字安全或数据安全问题。

▶▶▶中小企业数字安全可通过购买服务解决

毋庸置疑，数字经济已成为重组全球要素资源，数字安全保护能力则成为数字经济稳步发展的重要基石。数字安全的基础性作用越突出越得到重视，而一些重点领域重点群体的数字安全更是得到关注。

在“2022全球数字经济大会——数字安全峰会暨ISC2022互联网安全大会”上发布的《2022中小微企业数字安全报告》显示，在过去一年中，中小微企业遭受到的网络攻击次数正在呈现上升趋势。在受访的中小微企业中，85.3%企业遇到过数字安全问题，比以前遭受网络攻击次数要多；近77.4%中小微企业自身不具备有效处置数字安全问题的能力。

而面对数字安全危机，81%中小微企业受访者认为其带领的中小微企业会在现在或不久的将来遭到黑客攻击，对未来防御网络攻击持悲观态度；而认为不会遭到黑客攻击的仅占19%。

“中小微企业在数字化业务场景、预算、安全能力、应急响应等方面都有特定的安全需求，过去适用于大企业的安全服务和产品不能照搬。面对中小微企业面临的数字安全问题，需要新思考，新方案。”360集团副总裁首席安全官杜跃进博士表示。

而从分析来看，在过去12个月中，针对中小微企业最具破坏性的数字攻击威胁分别是恶意软件入侵（68%）、勒索攻击（65.3%）、系统漏洞（64%）和网络钓鱼（42.7%）。针对这些数字安全攻击，普遍存在中小微企业应对能力不足：这一方面是缺乏资金，另一方面是缺乏专业的数字安全团队维护。

对于缺乏专业数字安全人才，中国工程院院士、ISC名誉主席邬贺铨表示，应鼓励更多的数字安全企业，从以产品为中心向以服务为中心转变，建立专业的服务队伍，为企业提供个性化安全服务。

针对中小微企业资金缺乏，全国政协委员、360集团创始人周鸿祎则表示，不同于政府和大型企业，可考虑通过“低成本模式”来提升中小微企业对数字安全的理解和重视，帮助中小微在数字化转型中防御攻击，挽回损失，消除商业风险和负面影响。同时，由于中小微企业数字体系存在分布式部署的特点，可通过SaaS服务（指通过网络提供软件服务）采用中小微企业数字安全“云上赋能”的模式，保障数字安全能力的灵活部署和可定制化。

▶▶▶“上山”“下海”协同发力

伴随着数字化进程加快，一个新升级的数字安全时代也必然来临。针对中小微企业的数字安全，360公司已制定了“上山下海助小微”战略，通过上科技高山，解决国家数字安全“卡脖子”难题；下数字化蓝海，为传统产业数字化赋能；助小微，则是通过SaaS服务免费为中小微企业提供数字化服务，助力中国数字化战略发展。

而“上山”“下海”“助小微”，对数字安全整体行业也指明了转型升级的方向。

邬贺铨提出，要提升数字安全能力基础则是需要建立我国自主可控的数字安全技术、产品和服务的完整体系；中央网信办信息化发展局副局长、一级巡视员张望也表示，各界要加强技术协作，推动网络安全和数据安全相关理论和技术的研究向纵深发展，尽快突破“卡脖子”技术。

而企业是创新的主体，对此，全国工商联党组副书记、副主席樊友山在会上提出，要发挥网络安全龙头企业自身技术、人才优势和技术创新主体作用，开展数字安全基础理论创新、重大问题研究和核心技术攻关，助力数字安全技术创新发展。

但同时，邬贺铨也提出，数字安全不再是一个单纯的技术问题，是涉及业务、管理、流程、团队等各方面的系统工程。“下一步，应建立体系化的数据安全机制，打破各自为战，实现协同联防；以强化免疫能力为本，从技术开发与网络设计之初确立同步的安全理念，数字网络安全能力需要与基础设施同步建设；同时完善数字安全的生态系统，覆盖工业企业、设备供应商、基础电信运营商等，实现危险与处置情报共享。”

而针对“下海”，周鸿祎则认为，产业数字化已成为红海中的蓝海。“随着产业互联网的到来，传统产业和政府、城市成为数字化的主角，数字安全行业要将已经成熟地服务ToC的能力体系提炼成数字安全大脑框架，更好地服务ToB市场。而除了传统网络安全，还应更多向中小微企业、政企大数据安全、人工智能安全、城市安全等迈进。”

为此，陈智敏也提出两点建议：一方面要按照和平、安全开放、合作、有序的原则，共同构建网络空间命运共同体；另一方面，数字安全防御思路要升级，从工作思路、领导指挥、力量组织、作战样式、体系协调、标准规则制定等方面作出调整。

“希望各行业部门、机构、企业等一同为国家数字安全制度的完善、数据治理体系的创新，共同发力、协力前行。”陈智敏最后说。

RE DIAN FA BU | 热点发布

北京顺义：

“两区”建设呈现“加速度”

本报记者 孙琳

作为北京探索构建新发展格局的一个发力点、重头戏，“两区”建设正在推动北京以更高水平开放，引领更高质量发展。何为“两区”建设？“两区”即国家服务业扩大开放综合示范区和中国（北京）自由贸易试验区，是党中央在构建新发展格局中赋予北京的重大责任，是构建新发展格局中赋予北京的重大机遇。

8月2日，记者从北京市顺义区举行的“两区”建设第十二次新闻发布会上了解到，2022年以来，北京市顺义区紧抓“两区”建设发展机遇，立足区位优势，坚持以“产业开放+园区开放”为主线，落实“3+7+N”发展格局，重点围绕管理体制机制改革、政策制度创新、加速项目聚集、优化营商环境等方面持续发力，“两区”建设呈现“加速度”。

营商环境持续优化 上半年新设企业2030家

筑巢引凤。随着“两区”建设的全面推进，2022年以来，北京市顺义区政策制度不断创新、优质项目加速聚集、营商环境持续优化。其中，聚力航空服务领域、金融领域、文化贸易领域、新能源智能汽车领域项目正在顺利推进。

“随着试点政策和示范项目的密集落地，顺义区在吸引市场主体方面成效显著，‘两区’建设新增市场主体数量、项目储备数量均居全市前列。”北京市顺义区商务局局长杨蓬勃表示，自“两区”建设启动以来，北京自贸区顺义组团已累计新增市场主体8159家，其中2022年上半年新设企业2030家，全市排名第一。至今，顺义“两区”项目储备数273个，在推项目137个，落地项目135个，均排名全市前列。

而促外资、稳外贸，服务外资企业复工复产，同样是顺义区“两区”建设的重点。据公布的数据显示，今年1–5月，顺义区已完成实际利用外资4.65亿美元，同比增长18.8%，全市排名第三；累计吸引合同外资9.86亿美元，同比增长9%。“顺义区正在加大各项稳外资政策落实力度，积极推动潜在外资项目落地。”杨蓬勃说。

“两区”建设脚步不停。“下一阶段，顺义‘两区’建设将加快推进新一轮44项政策任务，将继续以‘产业开放+园区开放’为主线，重点发挥三大园区主体作用，积极开展国际高水平自由贸易协定规则对接先行先试，聚焦制度创新，积极推动项目落地，带动优势领域产业集聚发展。”杨蓬勃表示。

优质金融项目组团落户 打造首都金融发展新高地

开设绿色窗口、特殊通道，仅用1小时，中国农业发展银行全资子公司——农发基础设施基金公司就获得了营业执照，正式落户北京自贸区顺义区。北京市顺义区作为首都产业金融中心，金融产业正呈现惊人速度。

据北京市顺义区金融办党组成员、顺义区金融产业发展促进中心主任赵欣介绍，2022年以来，顺义“两区”跨境金融领域频传捷报，20个“两区”优质金融项目组团落户，注册资本合计超325亿元，管理规模预计超万亿元。其中，以农发基础设施基金公司、中交商业保理公司、中航材融资租赁公司、中冶长城投资公司等为代表的央企背景金融机构达12家。

北京市顺义区产业金融发展强劲迅猛势头的背后，正是良好营商服务环境和健全完备金融产业政策体系的有力支撑。

近年来，北京市顺义区高度重视第三支柱金融产业的发展，打造了一支专业化高素质的金融招商服务团队，并推出了申请落户、登记注册等模板式指引，全程无障碍办理，创下了项目最快1天落地、平均不超8天的“顺义速度”；同时，紧抓“两区”建设契机，顺义区聚焦跨境资金流动便利化，重点推动资本项目收入支付便利化试点、重点行业跨境人民币业务和外汇业务便利化、积极开展外债一次性登记等17项“两区”金融领域试点政策全部落地实施，完成率达100%。

而对入区发展金融机构的奖励支持力度也在逐步加大。据赵欣介绍，顺义区注重“招大引强”，对持牌内外资金融机构，按实收资本规模，最高可给予6000万元一次性落户奖励；对区内金融产业发展亟须填补空白的金融机构高管团队，最高可一次性给予1000万元落户奖励；对企业因做大做强而增资、管理规模扩大的，量身定制政策支持；对全国首例、全市首例的外资金融机构，最高分别给予1000万元、800万元资金支持；对QDLP按获批和实际募集规模，最高给予1000万元资金支持；同时，对金融机构高层次人才，在人才引进、商务出行、子女上学、人才公租房等方面搭建快速通道。

“两区”建设是中央支持北京开放发展的重大政策，是构建新发展格局中赋予北京的重大机遇，同时也为顺义区迎来了发展机遇。

顺义区相关负责人表示，未来顺义区将抓住“两区”建设有利契机，进一步释放“两区”建设政策红利，按照“平原新城看顺义”目标要求，围绕首都产业金融中心发展定位，持续吸引优质中外资金融机构，努力为首都北京高质量发展贡献顺义力量。

YE JIE SHENG YIN | 业界声音

《数据出境安全评估办法》发布：

出海企业需加快对标合规

本报记者 刘艳

随着数字经济的蓬勃发展，数据跨境活动也开始日益频繁。明确数据出境安全评估的具体规定，不仅是促进数字经济健康发展、防范化解数据跨境安全风险的需要，也是维护国家安全和社会公共利益的需要，是保护个人信息权益的需要。

千呼万唤始出来。近日，国家互联网信息办公室对外发布《数据出境安全评估办法》（以下简称《办法》），自2022年9月1日起施行，《办法》一出引起了业界的关注。

绿盟科技解决方案中心高级总监、首席解决方案专家刘弘利在接受记者采访时表示，当前，我国出海企业在数据出境时确实面临一定风险，如果企业事先对跨境数据法律风险准备不足，事中对风险又不善应对，就可能会导致数据出境后因触犯境外国家法律而遭受巨额罚款。此次《办法》出台明确规定了数据出境安全评估的范围、条件和程序，为数据出境安全评估工作提供了具体指引，这也能为企业数据出境保驾护航。

为了更好结合《办法》让企业在数据出境更好合规，刘弘利表示，相关企业应尽快组建数据合规团队，严格落实数据出境的相关规范要求，制定数据出境计划，对数据出境情况进行检查与问题整改，持续提升数据出境合规化能力。“如企业在数据出境前应首先判断出境目的，如果数据出境目的不具有合法性、正当性和必要性，不得出境。在此基础上再评估数据出境安全风险，将数据出境及再转移后被泄露、损毁、篡改、滥用等风险有效地降至最低限度。”

建立数据分类分级制度十分关键。对此，刘弘利认为，可参照国家和行业领域的重要数据识别指南等文件，结合企业自身的业务数据识别重要数据与个人敏感信息。

而企业数据出境风险自评估则是数据处理者向境外提供数据的必经之路，对出境方式、数据数量、数据属性进行充分综合判断，制定数据出境计划，最终形成数据出境风险评估报告，是数据出境企业应有的能力。通过有效的自评估，不仅可以降低数据出境的合规风险，在向主管部门申报安全评估时，也有助于提高监管部门安全评估的效率。

因此，刘弘利建议，可由企业的信息安全部门、法务部门和业务部门等成员组成数据出境合规委员会，对国内外数据安全法律法规进行研究，确保在采集和处理国外数据时不违反当地的地方性法规，同时，落实数据出境的安全主体责任制，建立企业数据出境管理制度，通过常态化的数据安全风险评估，及时发现企业在管理与技术上的不足，不断完善数据跨境流动治理框架体系，以此不断提升自我评估能力。

“总之，企业应及时响应国家的监管要求，尽快建立数据跨境的安全能力，保障数据出境安全。”刘弘利最后说。

WEI YUAN SHUO HUA | 委员说话

王一鸣：打造“平台+服务”的网安保障体系

本报记者 吴志红

“没有网络安全就没有国家安全。”安全是发展的前提，发展是安全的保障。

当前，以互联网、大数据、云计算、人工智能为标志的新科技革命推动数字经济迅猛发展，不断拓展网络安全新边界、衍生网络安全新需求。与此同时，全球网络空间博弈加剧，既给我国网络安全带来日趋严峻的挑战，也为网络安全产业发展提供了重大机遇。

在全国政协委员、国务院发展研究中心原副主任王一鸣看来，面向未来，我们需要统筹发展和安全，推进网络安全技术和产品创新，提高网络安全保障能力，建立健全数据安全保障体系，加快发展网络安全产业，筑牢适应数字经济发展的网络和数据安全屏障。

谈及具体建议，王一鸣表示，“首先要推进网络安全技术和产品创新。”从现实情况来看，我国网络安全技术和产品创新成果丰硕，但与国际先进水平仍有较大差距，核心技术创新能力亟待提升。

对此，王一鸣认为，应发挥我国新型举国体制优势、超大规模市场优势，提高网络安全技术基础研发能力，加强网络安全技术和产品研发创新，攻克关键核心技术，实现高水平自立自强，把网络安全自主权牢牢掌握在自己手中。

有了核心技术还需提高网络安全整体的防护能力。对此，王一鸣认为，应加强网络安全基础设施建设，提升网络安全动态感知、威胁发现、应急指挥、协同处置和攻击溯源能力。“如加强电信、金融、交通等重点行业关键信息基础设施网络安全防护能力，开展常态化安全风险评估；强化针对新技术、新应用的网络安全管理，为新产业新业态新模式发展营造安全环境。”

当前，数据作为新型关键生产要素，已成为决定国家、地区、企业竞争力的核心资源、关键资源和战略资源，深刻改变着生产方式、生活方式和社会治理方式。保障数据安全亦成为数字时代数字安全的重中之重，而保障数据安全，不仅需要加强技术研发和推广应用，更需要建立健全各项基本制度。

王一鸣表示，应针对不同数据类型、不同数据用途、数据敏感程度等，完善分级分类管理办法，规范数据采集、传输、存储、处理、共享、销毁全生命周期管理；同时推动数据使用者落实数据安全保护责任，维护国家数据安全，保护个人信息和商业秘密，守住数据安全底线，特别是数据跨境流动的制度规范。

而网络安全产业是保障国家网络安全的重要力量，推动网络安全产业高质量发展恰逢其时。对此，王一鸣建议，要培育发展网络安全企业，创新网络安全服务模式，打造“平台+服务”的网络安全保障体系，形成网络防护、安全监管、安全服务、密码等各具特色的系统解决方案，当好国家网络安全的“守护者”；同时可建设一批网络安全产业园区，培育融合创新的产业集群，做大做强网络安全产业。

“可以预期，随着国家日益重视网络空间安全和全社会对网络安全产业需求进一步释放，我国网络安全产业将进入快速发展期，迎来高质量发展的新机遇。”王一鸣最后说。