筑牢数据安全屏障

数据作为新型生产要素，是数字化、网络化、智能化的基础。随着数据要素向深度应用拓展，规范数据流动、保护个人隐私、保证网络安全等问题也面临考验。2022年12月19日，中共中央、国务院发布《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，统筹发展和安全，贯彻总体国家安全观，强化数据安全保障体系建设，把安全贯穿数据供给、流通、使用全过程。本期特邀专家围绕相关问题进行研讨。

智库圆桌（第2期·总121期）

主持人 本报理论部主任、研究员 徐向梅

数据共享应用成效显著

主持人：数据作为新型生产要素，有何特点及优势？我国数据开发利用现状如何？

唐建国（北京市大数据中心副主任、北京市经济和信息化局大数据应用与产业处处长）：2020年3月，中共中央、国务院发布《关于构建更加完善的要素市场化配置体制机制的意见》，第一次把数据要素作为第五大生产要素提出，对数字经济发展具有划时代的里程碑意义。

数据，是对客观事物的逻辑归纳。在数字时代，数据成为表达信息、知识和智慧的主要载体。数据要素，是指经过清洗、加工和治理后，直接拿来可用并具有交易价值的数据资源。用土地作比喻的话，数据要素本质上是一块达到“七通一平”条件、能够在市场交易的“熟地”，也是高价值可用数据资源的代名词。从资源、要素、资产到资本，数据在形态演进中实现价值跃升。

从生命周期看，数据可分为零次数据（收集生成）、一次数据（清洗比对）、二次数据（统计分析）、三次数据（研判预测）等类别，具有无限衍生的可能。从自身构成看，数据具有类似于波粒二象性的二元化结构特征。从法律视角，数据分为载体和内容，数据权属可以分解为载体权利和内容权利。从技术视角，数据可分为信息和价值，基于隐私计算技术信息进行加密处理，可将数据计算价值进行流动。从生产资料角度看，数据要素具有可复制、可再生、海量获取、消费中增值、边际成本接近零、在应用中产生价值等特点。利用数据要素，人们可以形成新的洞见，具备超范围协同、超时空预判、精准调控、双向触达等新能力，打破传统生产要素有限供给对经济增长的制约。

2015年国务院印发《促进大数据发展行动纲要》提出，加快政府数据开放共享。2022年12月，中共中央、国务院发布的《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，建立数据资源持有权、数据加工使用权、数据产品经营权等分置的产权运行机制。近年来，各地在数据资源开发利用方面进行制度探索，北京、上海、深圳、浙江、广东等地出台数字经济或数据条例，对数据的采集、共享、开放、交易等活动设定权利义务，明确了数据具有财产性权益，为数据开发利用提供了法制保障。

公共数据开放方面，我国不断加大开放共享力度，截至2021年10月，已有193个政府数据开放平台，其中省级平台20个，城市平台173个。截至2022年8月，北京市公共数据开放平台浏览量累计3.8亿次，公共数据开放总量约59.86亿条，其中无条件开放8496个数据集，约1.48亿条数据，累计数据下载总量突破30万次，有条件开放数据集3555个，约58.38亿条数据，整体水平居全国前列。

数据应用方面，国家政务服务平台、粤省事、随申办、浙里办、北京通等App或小程序，通过整合健康服务、市民办事、行政审批等各类业务数据，为百姓提供多样便捷的政务和城市服务，实现了“让数据多跑腿”“让百姓少跑腿”。截至2022年9月，北京通App累计下载量5000万次，累计用户1300万人，月活用户320万人，对外提供5177项政务和公共服务，汇聚576类电子证照1.24亿张。

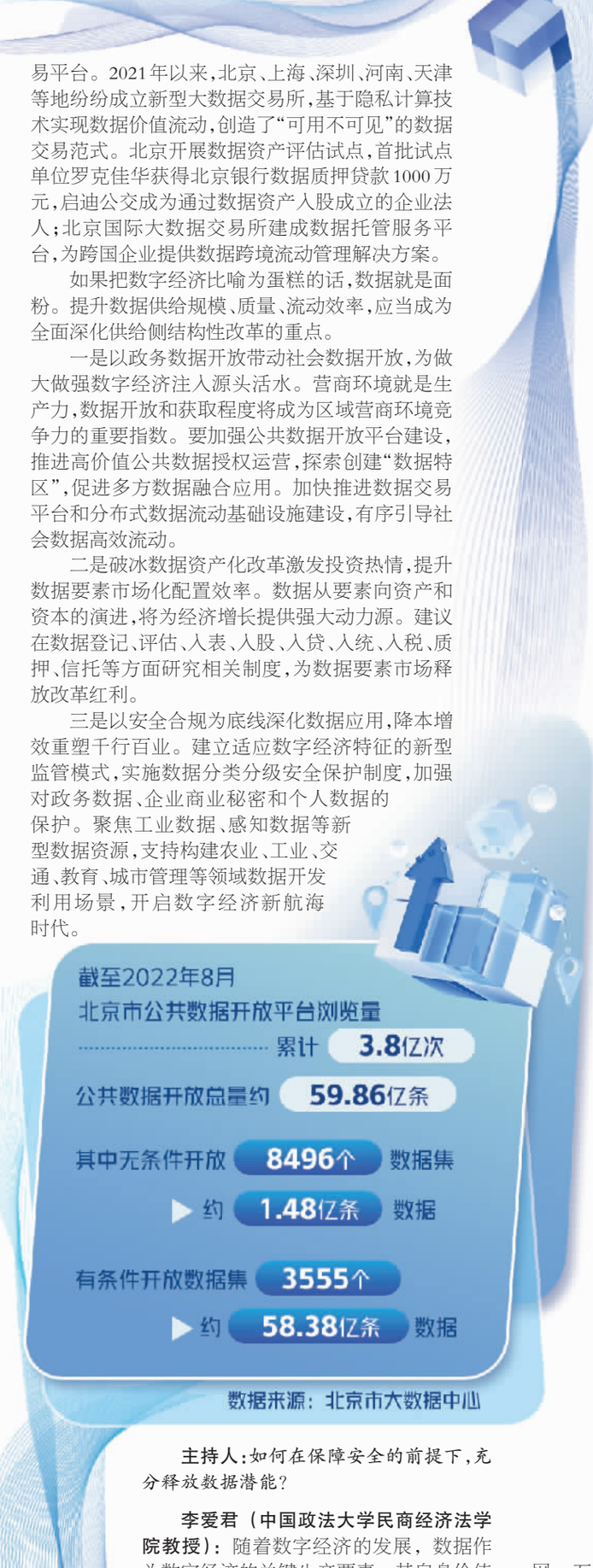
数据要素市场方面，全国有40家左右数据交易平台。2021年以来，北京、上海、深圳、河南、天津等地纷纷成立新型大数据交易所，基于隐私计算技术实现数据价值流动，创造了“可用不可见”的数据交易范式。北京开展数据资产评估试点，首批试点单位罗克佳华获得北京银行数据质押贷款1000万元，启迪公交成为通过数据资产入股成立的企业法人；北京国际大数据交易所建成数据托管服务平台，为跨国企业提供数据跨境流动管理解决方案。

如果把数字经济比喻为蛋糕的话，数据就是面粉。提升数据供给规模、质量、流动效率，应当成为全面深化供给侧结构性改革的重点。

一是以政务数据开放带动社会数据开放，为做大做强数字经济注入源头活水。营商环境就是生产力，数据开放和获取程度将成为区域营商环境竞争力的重要指数。要加强公共数据开放平台建设，推进高价值公共数据授权运营，探索创建“数据特区”，促进多方数据融合应用。加快推进数据交易平台和分布式数据流动基础设施建设，有序引导社会数据高效流动。

二是破冰数据资产化改革激发投资热情，提升数据要素市场化配置效率。数据从要素向资产和资本的演进，将为经济增长提供强大动力源。建议在数据登记、评估、入表、入股、入贷、入统、入税、质押、信托等方面研究相关制度，为数据要素市场释放改革红利。

三是以安全合规为底线深化数据应用，降本增效重塑千行百业。建立适应数字经济特征的新型监管模式，实施数据分类分级安全保护制度，加强对政务数据、企业商业秘密和个人数据的保护。聚焦工业数据、感知数据等新型数据资源，支持构建农业、工业、交通、教育、城市管理等领域数据开发利用场景，开启数字经济新航海时代。



各国前所未有重视信息安全

主持人：国际上对于信息安全保护有哪些可借鉴经验？

支振锋（中国社会科学院法学研究所研究员）：信息安全领域宽泛，既包括网络空间得以安全稳定运行的互联网基础设施安全，也包括在新技术新应用新业态中起基础性驱动作用的数据安全，还包括对国家政治和社会稳定有重大影响的内容安全。美国“棱镜计划”被斯诺登披露之后，世界各国前所未有地重视信息安全，并在战略设计、技术创新和法规政策上取得一系列进展，其中有不少可借鉴经验。

信息安全成为国家安全和发展战略的重要部分。近半个世纪以来，美国通过《第12065号总统行政令》《关于通信和自动化信息系统安全的国家政策》《转变中的国防：21世纪的国家安全》《网络空间安全国家战略》等举措，国家信息安全政策渐成体系。近10年来，其国家信息安全政策不断扩张，2011年《网络空间行动战略》将网络空间与陆海空天并列为行动领域，2021年增强国家网络安全的行政命令签署、2022年《网络安全战略规划2023—2025》发布，进一步将网络安全置于国家安全优先位置。由于特殊战略环境，俄罗斯对信息安全同样敏感，1995年在讨论《俄罗斯联邦信息安全纲要》时提出信息安全概念，1997年《国家安全构想》提出信息安全是经济安全的重中之重，2000年《国家信息安全学说》为构筑未来国家信息安全政策大厦奠定基础。2014年以来，俄罗斯在信息安全国家战略和法规政策上不断出台新举措，2021年发布新版《国家安全战略》，为维护国家安全奠定了更加坚实的基础。

关键信息基础设施安全成为信息安全的重中之重。现代社会数字化程度日益加深，公共通信和信息服务，以及能源、交通、水利、金融、电子政务等重要行业和领域信息系统一旦遭到破坏、丧失功能或数据泄露，可能严重危害国家安全、国计民生、公共利益，是需要重点保护的关键信息基础设施。20世纪末美国出台关键信息基础设施领域保护的政策，确立保护机构，明确职责分工，此后相继发布第14028号行政令《提升国家网络安全》和《改善关键基础设施控制系统网络安全的国家安全备忘录》《关键基础设施网络安全事件报告法》；欧盟高度重视整体层面的网络攻击防御和复原能力，2021年通过《关于欧盟数字十年网络安全战略的决议》，重申为欧盟关键基础设施建立新的、强大的安全框架的重要性；新加坡《2021年网络安全战略》进一步明确和强化关键信息基础设施保护过程；澳大利亚《2022年安全立法修正案（关键基础设施保护）法案》就关键信息基础设施保护进行了新的探索；俄罗斯强调关键信息基础设施的保护和防御，要求关键信息基础设施部门自2025年1月1日起全面禁用外国软件，政府在最短时间内建立一个现代化的国产电子元件基地。

数据安全成为信息安全的基础性问题。数据承载着个人、市场主体与国家的大量信息，关系到公民人格权益、市场主体财产权益以及国家安全和社会公共利益。美国在数据与个人信息保护方面立法较为碎片化，但联邦和州层面通过专门立法，已形成数据安全保护的制度体系。欧盟特别注重数据和个人信息保护，通过《数据保护指令》《通用数据保护条例》《数字服务法》《数字市场法》，形成了极具特色的严密数据安全法律体系。在数据跨境流动问题上，不同国家地区之间在数据安全方面存在信任危机，2022年3月美欧达成《跨大西洋数据隐私框架》，10月美国签署《关于加强美国信号情报活动保障措施的行政命令》，12月欧盟委员会启动《欧盟—美国数据隐私框架充分性决定草案》推进进程。

内容安全成为信息安全的焦点议题。剑桥分析丑闻引发了美国对大型社交媒体平台的警惕，开始讨论《通信规范法》第230条对平台责任的豁免问题，2020年签署《防止在线审查行政令》。欧盟、英国、法国、德国、俄罗斯、巴西等纷纷出台法律，对社交媒体进行规范，强化内容治理。

供应链安全成为信息安全的重要内容。由于现代产品和服务依赖于供应链，产品的组件和软件来源众多，设备可能在一个国家设计而在另一个国家制造，这意味着产品可能包含恶意软件、易受到网络攻击，而供应链本身的安全漏洞也会影响公司安全基线。美国一直以来重视供应链安全，不断完善产业链供应链安全体系的战略设计，关注重点也逐步由灾难性风险转向大国政治博弈风险。2021年美国对半导体、新能源电池、关键矿物和医药用品四大关键领域的供应链弹性进行评估，此后通过《两党基础设施法》强调供应链安全。英国、欧盟以及其他国家和地区也都把产业链供应链安全视为国家安全的重要内容而投入大量立法、规制和政策资源。

信息安全是一项长期、复杂、系统的综合工程，我们要以新安全格局保障新发展格局，加快建设网络强国，以高水平信息安全促进高质量发展，构筑竞争新优势。

主持人：大数据背景下，信息保护面临怎样的挑战？我国在数据安全治理方面有哪些举措？

郭雳（北京大学法学院教授）：数字经济已成为推动经济高质量发展的新引擎。算法、区块链、人工智能等新兴技术广泛应用于数据收集、加工和分析，大数据正深刻改变着国家治理能力、社会生活形态和经济运行方式，也对信息保护、数据安全提出新的挑战。

首先，随着不同场景中海量数据的收集与使用，数据侵害来源呈多样化趋势。例如，出入小区时人脸数据不规范采集、网购联系方式遭到营销短信轰炸等，个人数据安全问题遍布日常生活。在人脸识别相关案件中，人脸数据具有高度敏感性，不当收集程序及后续滥用、泄露风险，将对个人人身、财产安全产生重大的威胁，案件激起的个人数据信息安全话题，值得社会各方思考。

其次，数据处理者在数字化转型进程中面临数据安全问题。以金融数据为例，一些传统金融机构特别是中小金融机构缺乏与数据价值创造相匹配的重视并保护数据的意识与能力，引发了内部数据管理系统不健全、数据泄露或越界使用等问题。从2021年金融监管部门统计的涉数据违法处罚来看，金融机构因“未按规定收集使用个人信息”“泄露客户个人信息”等问题共收到罚单千余张，金额超10亿元。

再次，数据安全与数据商业化利用、公共价值创造之间如何平衡。数据安全固然重要，但也并非规范数据产业发展和企业数据处理行为的终极目的。数据要素是经济发展的基础性、战略性资源，其易复制、可共享等特征为经济发展带来强劲动力。数据要素不仅是数字经济深化演进的核心特质，还具有保障社会安全、提升社会福祉、维护国家数据主权等多重功能定位。如何在保障数据安全基础上充分利用数据商业化价值、实现数据要素的公共价值，是新时代数据治理核心命题。

最后，大规模个人数据跨境流动给国家信息安全带来新的挑战。某大型网约车平台公司赴境外上市风波即是典型事例，2022年7月有关部门公布了对该公司的处罚。类似地，美国近年来也通过《澄清境外数据的合法使用法案》扩大了美国外资投资委员会的审查权，限制特定领域外国投资的数据跨境流动。一系列数据执法案例表明，数据安全已融入内涵丰富的总体国家安全观。维护国家主权、数据主权与国家安全，成为大数据背景下个人信息保护和国家数据治理的底线。

在立法层面，近年来我国在个人信息与数据安全保护领域取得了丰硕成果，网络安全法、数据安全法、个人信息保护法等法律及配套法规相继出台，丰富和细化了民法典这一基础性法律中的基本原则与相关制度，形成了网络空间与现实世界并重、国家数据安全与个人数据安全并重的现代化数据安全法律体系。在此基础上，行政监管部门鼓励和引导行业组织、高等院校、从业机构共同参与，推动多元主体在标准制定、文件论证、文化建设等方面与政府开展合作，形成了大量数据安全标准、科技伦理指引、数据治理倡议。这些软性约束与法律的刚性色彩相呼应，勾画出数据安全的“柔性边界”。

在执法层面，《中华人民共和国个人信息保护法》第六十条将国家网信部门作为负责统筹协调个人信息保护工作和相关监督管理工作的机构，建立了网信办统筹协调、有关部门在各自职责范围内执法的跨部门、跨行业、跨领域监管体制机制，一系列“净网”“清朗”等专项行动取得显著成效。同时，该法赋予数据执法者包括询问、调查、查阅、复制、现场检查、查封和扣押等措施在内的执法工具箱。另外，随着数字政府建设不断深入，监管科技已成为高效发现和追踪数据违法行为的新法宝。

在司法层面，目前已形成私益与公益诉讼相结合的司法救济体系。违约之诉、侵权之诉是个人数据被侵害时的私益救济方式。不过，由于其举证难度、救济成本、救济效果等方面的局限，使传统私益诉讼容易陷入困境。因此在私益诉讼之外，个人信息保护法专门设置了公益诉讼条款，将个人信息保护纳入检察机关公益诉讼的范围之内。2021年，全国检察机关共提起2000余件公益诉讼案件，一定程度上改善了个人提起诉讼的“行动难”问题，公益诉讼与私益诉讼一道构成数据安全司法救济途径。

主持人：如何在保障安全的前提下，充分释放数据潜能？

李爱君（中国政法大学民商经济法学院教授）：随着数字经济的发展，数据作为数字经济的关键生产要素，其自身价值和潜能日益凸显。为充分释放数据潜能，党的十九届四中全会首次提出将数据作为生产要素参与分配，《“十四五”数字经济发展规划》指出，数据对提高生产效率的乘数作用不断凸显，成为最具时代特征的生产要素。数据价值挖掘已成为推动我国经济转型的新动力，同时也是新经济增长点和新动能。

大数据精准分析和科学决策有效促进了教育、医疗、电子商务、工业、农业效率和经济效益提升。例如，医疗行业通过多部门对个人健康信息、职业、行为等数据与医疗数据关联处理，提供个性化和精细化医疗服务；政府通过政务数据共享和开发应用，提高了决策科学性、服务便民性和治理效率，同时提升了突发事件应对能力和动态预警水平，实现了人民生活安全和幸福指数增长。产业方面，大数据开发和应用可形成新产业链、新消费、新经济内循环和新服务模式，例如“互联网+政务服务”、智能交通、智慧医疗和智慧养老等，促进了经济增长和经济结构转型。国际竞争方面，我国具有数据规模优势，2017年至2021年，我国数据产量从2.3ZB（计算机术语，十万亿亿字节）增长至6.6ZB，全球占比9.9%，位居世界第二，大数据产业规模从4700亿元增长至1.3万亿元。如果充分利用数据规模优势，提升数据规模、质量和应用水平，未来我国在数字经济时代将具有巨大发展空间和竞争优势。

大数据、云计算、人工智能、物联网、互联网等技术为人类提供便利的同时，对个人信息保护、公共利益和国家安全也带来挑战。现实生活中，个人信息数据泄露和滥用情况时有发生，数据要素处理和使用过程中的安全问题若得不到有效解决，将会造成社会对数据和信息安全的担忧，降低社会成员提供个人信息意愿，叠加组织机构之间数据共享与开放壁垒，进而阻碍数据价值挖掘和潜能释放。

提高数据安全保障能力既是对数据发展优势的保障，也是国家竞争力的体现。数据安全与发展的平衡是释放数据潜能的关键，我国在维护数据安全方面已确立网络安全法、数据安全法、个人信息保护法等一系列法律法规。但数据安全法和个人信息保护法分别以保障数据安全和保护个人信息合理利用为立法目标，在促进数据潜能释放方面的基础制度仍供给不足。数据基础制度建设事关国家发展和安全大局，要以维护国家数据安全、保护个人信息和商业秘密为前提，促进数据高效流通使用、赋能实体经济，统筹推进数据产权、流通交易、收益分配、安全治理，加快构建数据基础制度体系。

构建数据安全与发展平衡的基础制度体系主要包括以下五个层面。一是确立数据财产权制度。数据是一种财产，应通过设立财产权的方式实现对数据财产的法律保护。数据财产权是指合法获得对数据控制的主体享有的财产权利，财产权利内容包括控制权、处理权、处分权和收益权，这些权利的行使受数据所记录信息的相关法律法规规范。

二是构建数据供给制度。构建以开放公共数据向市场供应数据生产要素的制度，公共数据开放应作为国家数据要素市场供给侧来源补给的主要手段，公共数据开放制度应围绕开放公平、部门职责、开放标准、开放范围、开放类型、开放方式、开放程序、安全保障和监督机制展开。

三是搭建数据流通制度。数据流通是释放数据潜能的重要方式，目前平台交易是多层次的：第一层次是有国家级资质的数据交易所，第二层次是由地方政府赋予资质的数据交易中心，第三层次是没有任何资质的数据交易平台。未来应进一步完善和规范数据流通制度，根据数据分级和分类，不同类别数据可在相应层次交易流通。

四是建立数据治理制度。数据治理是在保障数据安全前提下使数据资产化，数据资产化是数据治理目标。建立数据治理制度要从微观管理角度着手，实现数据安全与发展的平衡，包括治理组织架构（决策架构、管理架构、执行架构、监督架构）、权责边界明确的责任制度、安全保障、质量标准等。

五是构建数据源供给主体制度。建立数据源供给主体制度的目的，在于解决数据需求方获取数据成本高、数据供给方维权成本高和国家对数据安全与个人信息保护监管缺乏实效性等问题。建议通过对数据源主体准入资格和内部治理结构规制，赋予数据源供给主体相关权利与义务，有效解决上述问题。

以法

加快构建数据基础制度体系

本版编辑 谢 慧 美 编 倪梦婷 来稿邮箱 jjrbjjzk@163.com