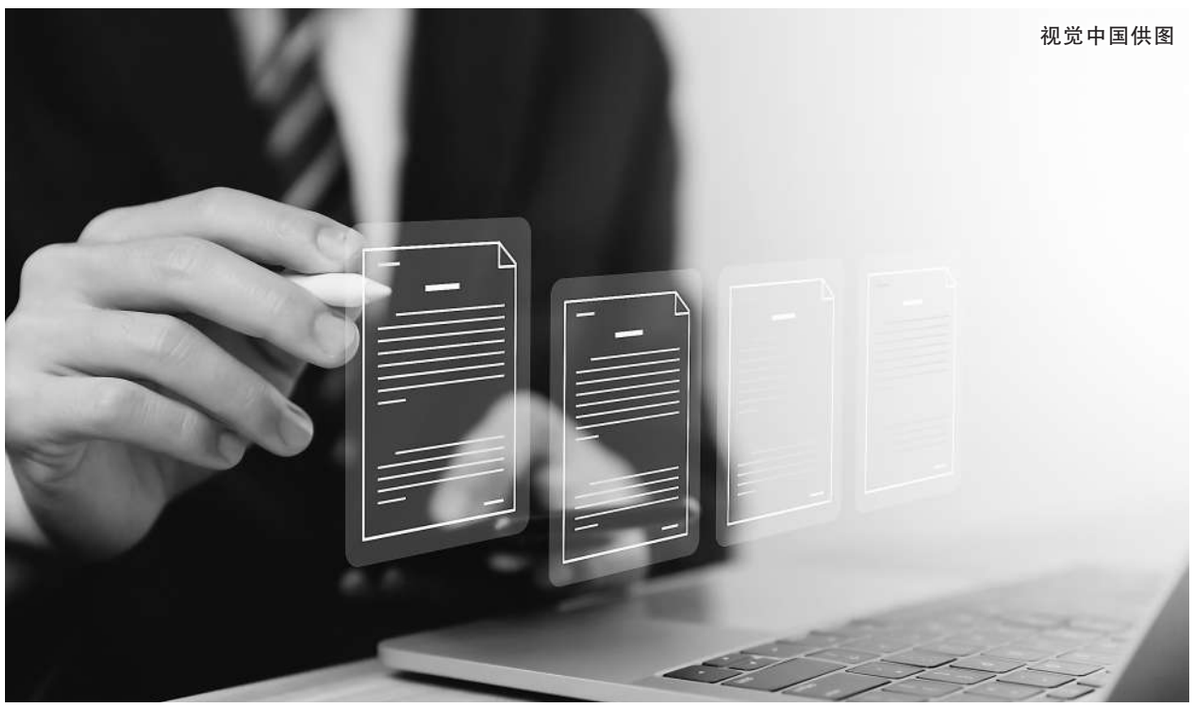
隐私计算又被形象地称为“可用不可见”的技术，是涵盖众多学科的交叉融合技术，目前主流的隐私计算技术主要分为三大类：以多方安全计算为代表的基于密码学的隐私计算技术，以联邦学习为代表的人工智能与隐私保护技术融合衍生的技术，以可信执行环境为代表的基于可信硬件的隐私计算技术。



视觉中国供图

隐私计算：让数据“可用不可见”

◎本报记者 张 晔

4月4日，北京国家金融科技认证中心公布了首批“多方安全计算金融科技产品国推认证”名单，包括蚂蚁集团两项产品在内的首批5项产品通过了该认证。

这是国内首次对多方安全计算金融领域应用展开认证工作，也是目前国内唯一针对该领域的“认证”，此次认证结果的发布，意味着数据要素市场的相关市场准入标准和监管体系迎来进一步完善。

作为隐私计算产品的重要底层技术，多方安全计算技术能够在保护数据隐私的同时，实现不同机构之间数据的合法合规融合，实现安全的多方数据查询和分析，进一步打破各方之间的数据壁垒，连接数据孤岛，有效实现数据价值的转化与释放。

为数据价值而生的隐私计算

伴随着云计算、大数据、人工智能等新一代信息技术的快速发展，数据已经成为基础性关键战略资源，同时也是数字经济时代的核心生产要素。

但是，在信息技术蓬勃发展的同时，数据也面临着一系列严峻的安全挑战，不仅包括公民个人信息和隐私的安全隐患，也包括政府和企业数据资产的泄露风险。近年来，数据泄露事件层出不穷，出于安全顾虑，数据价值链不同环节之间的流动受阻，分工协作关系脆弱，很难形成有效闭环。

大数据时代，如何在保障数据安全的同时又不影响数据要素的使用，是每一个数据生产者和获益者应该考虑的事情。

1982年，著名计算机学家、中国科学院院士姚期智提出了经典的“百万富翁”问题：张三和李四都是富翁，他们想知道谁更富有，但他们都想保护好自己的隐私，不愿意让对方或者任何第三方知道自己真正拥有多少财富。如何在保护好双方隐私的情况下，计算出谁更有钱？

在普通人看来，这几乎是一个无解的悖论。但是姚期智就此提出了“多方安全计算”的概念，即“一组互不信任的参与方在需要保护隐私信息以及没有可信第三方的前提下进行协同计算”。

近年来，我国多部与数据安全相关的法律法规落地实施，包括《网络安全法》《个人信息保护法》《密码法》《数据安全法》以及《民法典》，形成了较为完备的安全法律体系，隐私计算为需求强烈但瓶颈重重的数据流通提供了破局思路。

随着政策落地以及各方关注度的提升，隐私计算已成为当下火热的新兴技术，跻身商业和资本竞争的热门赛道，有业界人士将2020年称为“隐私计算元年”。顾问咨询公司高德纳（Gartner）发布的《2021年重要科技战略趋势》中，也将隐私计算列为未来几年科技发展的九大趋势之一。

多技术融合保护数据安全

隐私计算又被形象地称为“可用不可见”的技术。看不见数据，却又能实现对数据的计算分析，隐私计算是如何做到的？

蚂蚁集团隐私智能计算技术部总经理王磊告诉科技日报记者，隐私计算是涵盖众多学科的交叉融合技术，发展初期汇聚了多种不同种类的技术，目前主流的隐私计算技术主要分为三大类。

第一类是以多方安全计算为代表的基于密码学的隐私计算技术；第二类是以联邦学习为代表的人工智能与隐私保护技术融合衍生的技术；第三类是以可信执行环境为代表的基于可信硬件的隐私计算技术。

以多方安全计算为例，其主要逻辑是在没有可靠的第三方（中介）的情况下，各方通过事先约定的密码学协议进行交互，完成预定的计算任务，每个参与方无法得知其他方输入的信息，只能得到计算结果。

“每一类技术路线都有各自的特点，适用于不同的应用场景。”王磊说，例如联邦学习适用于对性能和规模要求较高的建模场景，多方安全计算安全性更高，基于可信硬件的隐私计算可以支持更复杂的计算需求。

但是，从近年来的技术发展趋势和行业需求来看，想要通过单一技术“包打天下”几乎不可能，现实需求往往需要不同的隐私计算技术组合使用，在保证原始数据安全和隐私性的同时，完成对数据的计算和分析任务。

王磊告诉记者，以蚂蚁集团隐私计算的技术路线为例，从最早基于矩阵掩码的数据变换方案，到基于多方安全计算和可信执行环境的两套技术路线，再到后来的多种技术融合路线，并催生了可信隐私计算开源框架“隐语”和隐语开放平台。“隐语”提供的是代码，主要面向开发者，好比把原材料都准备齐全，就看开发者怎么做出一桌色香味俱全的大菜；而隐语开放平台则可以让用户直接调用各项功能，好比平台提供了预制菜，只要根据个人需求简单加热调味即可。

金融领域应用最广泛

当前，隐私计算应用最广泛的是金融行业。例如，招商银行启动了“慧点隐私计算平台互联互通项目”，交通银行则启动了监管沙盒项目，中国工商银行、中国农业银行也不同程度的在相关业务中尝试性地应用了隐私计算工具。

“传统的金融机构风险管理模式，除了调查走访外，主要是利用本单位数据和征信系统查询用户信息，这种方式对用户的风险判断不够全面。”王磊表示，基于多方安全计算的金融风控全链路解决方案，可以调用不同机构的多个信息渠道对潜在用户的历史记录进行多维度计算分析，各金融机构、信息渠道可形成征信系统联盟，能为各方提供数据分析服务，且数据无须离开本地，调用数据的过程中，数据不再以明文（即数据不加密）形式出现，而是通过安全协议共享，任何人都无法从中窥探到原始信息，这就是隐私计算相较于传统金融机构风险管理模式所带来的重要改变。

除了金融行业，隐私计算在医疗行业、保险理赔、政务信息等领域也有非常大的应用空间。

例如，过去保险机构在理赔过程中，会向医疗机构明文查询被保险人的诊疗情况，而获得的原始数据往往涉及用户隐私。2018年，蚂蚁集团尝试将隐私计算技术应用到保险理赔场景，通过设定数据逻辑查询，利用多方安全计算等隐私计算技术，使得保险公司只获得是否理赔的结果，不会获得原始数据，从而实现数据“可用不可见”，保护理赔用户隐私。

在医疗行业，全球抗击新冠疫情数据共享也运用到了隐私计算，这使各方可以在不公布详细数据的情况下，联合其他科研人员协同进行病例样本基因组的联合分析并共享结果，实现了对病毒流行病学情况的实时追踪和对未来毒株演化的预测，成为抗击疫情的一把利剑。

王磊表示，自计算机诞生以来，数据一直是明文流通和应用，面向数字经济时代，安全地用好数据成为绕不过去的坎。今后，法规政策和技术进步都将助推数据要素告别明文流通，开启“数据密态时代”的新征程，在数据密态时代最有潜力的支撑性技术非隐私计算莫属。

迈向网络强国，下一代域名系统如何发力

◎本报记者 朱 丽

提到域名，很多人以为就是一串字符，但在字符之后还隐藏着域名系统（DNS）等一系列互联网资源和技术的支撑与保障。伴随着5G、物联网、移动互联网、卫星互联网等新一代信息技术的迅速发展，人们的生活场景愈加丰富，也让DNS迎来新的变革，行业生态正在重塑。

站在加快建设网络强国的新历史起点上，下一代DNS作为互联网的重要基础设施，在不断变化的国际格局和市场需求推动下，将发挥哪些作用？

数字经济呼唤下一代DNS

互联网基础设施和基础资源，是我国经济社会运行的基本要素和重要支撑，也是数字经济发展的坚实底座。数字技术蓬勃发展，催生了各行业数字化转型对互联网基础设施的升级需求，传统DNS已经无法满足市场需要，“发展下一代DNS，重塑网络根基”迫在眉睫。

近日，互联网域名系统国家地方联合工程研究中心（以下简称ZDNS）在成立十周年之际，宣布完成亿元C轮融资，由中科院资本、新鼎资本领投。本轮资金将主要用于推动下一代DNS技术研发和行业应用，充分发挥下一代DNS在互联网基础设施中的关键作用，为数字经济发展筑牢重要网络根基。

“我们日常生活中使用的应用软件、智能终端等，其背后都要依赖DNS进行调度。”ZDNS总经理邢志杰告诉科技日报记者，下一代DNS是涵盖网络空间、关键基础资源、软硬件系统在内的，支撑数字经济发展的重要网络根基，“向下”可对接信息网络升级，“向上”可支撑数字经济发展。

在邢志杰看来，需求牵引技术进步，ZDNS通过不断自主创新，建立起了红枫系统、白泽平台和应龙中台三大核心技术，夯实了下一代DNS技术根基，数据赋能、全面感知、可靠传输、智能分析、精准决策等能力大大提升。如今，下一代DNS技术正在试图与业务场景深度融合，让网络根基更安全、更高效、更智能。

在ZDNS团队以及投资人构筑的美好愿景中，下一代DNS按下发展加速键，正在核心技术、产品创新、网络场景和行业应用等四大方面全面推进。

创新是保障网络安全的关键

日前公布的第51次《中国互联网络发展状况统计报告》显示，截至2022年12月，我国网民规模达10.67亿，互联网普及率达75.6%。我国互联网用户人数居全球第一，是名副其实的网络大国，但关键技术受制于人，自主创新能力不强，网络安全面临严峻挑战，还不是网络强国。

在从网络大国迈向网络强国的过程中，网络安全既是根基也是关键。DNS是所有互联网服务的入口，其安全性不言而喻。然而，全球13个根服务器，中国只有镜像根运行权，没有管理权；全球1500多个顶级域名，中国拥有管理权的不足3%；很多企业的域名解析软件高度依赖进口……“断根”“断服”“断供”风险始终存在。

这就好像是一颗颗炸弹，随时都有可能被引爆。那么该如何铲除风险呢？

> 下一代DNS是涵盖网络空间、关键基础资源、软硬件系统在内的，支撑数字经济发展的重要网络根基，“向下”可对接信息网络升级，“向上”可支撑数字经济发展。
>
> **邢志杰**
> 互联网域名系统国家地方联合工程研究中心总经理

“我们历经14年自主研发的三大核心技术以及基于此进行的产品创新，正是斩断中国网络根基面临‘三断’风险的重要利器。”邢志杰进一步解释说，红枫系统通过支持区块链新型根、IPv6根扩展、本地根区副本等新技术有力支撑解决“断根”问题；基于红枫系统和应龙中台，开发和运营了全球第二大新顶级域名服务平台和面向重点行业客户的云解析、云安全服务平台，有力支持中国企业申请和运营顶级域名关键基础资源，提升企业的域名安全服务能力，为解决“断服”威胁提供有力支撑；基于红枫系统和白泽平台开发的域名解析、地址分配和地址管理等软硬件核心网络设备，全面支持国产芯片和操作系统，解决了“断供”威胁。

拥有国际互联网话语权也是网络强国的一个重要特征。当前，全球互联网核心资源包括顶级域名和互联网地址空间，正处于新一轮的分配和关键部署阶段，新通用顶级域名资源即将面向全球再次开放申请，ZDNS专家正在积极跟进新一轮顶级域名开放政策制定，为中国企业争取更多互联网关键基础资源。

“实施网络强国战略，首先要突破关键技术，创新是实现网络技术突破的灵魂。”ZDNS董事长毛伟说，未来ZDNS还将继续深耕于互联网域名、IP地址等互联网关键基础资源技术领域，努力攻克我国DNS技术“卡脖子”问题。

做好数据科学工作 是挖掘数据生产力的关键

◎本报记者 张佳星

“数字中国建设不只是存储平台、计算平台、东数西算等硬件，还需重视软实力的建设。”在“2023数据科学峰会”上，中国科学院院士，北京大学数学科学学院、光华管理学院教授陈松蹊认为，落实数字中国建设的整体布局规划，关键工作之一是通过数据科学来释放数字生产力。

日前，中共中央、国务院印发的《数字中国建设整体布局规划》要求，加快提升数据资源规模和质量，有效释放数据要素价值。

随着各行各业数智化转型的深入，数据已经成为经济社会发展的关键生产资料，如何释放数据生产力，成为推动数字技术和实体经济深度融合、加快数字技术创新应用的新命题。

“要真正把数据的生产力释放出来，光有大量的存储和算力还不行，还要搞清楚如何发挥存储、算力的最大效能，研究‘怎么算’才是关键。”陈松蹊说，用好数据要素，数据科学的研究是当务之急。

北京百分点科技集团股份有限公司董事长兼首席执行官苏萌表示，数据科学在过去50年里从1.0的小数据时代、2.0的大数据时代走入了3.0的人工智能时代，未来将迈向数据原生时代。当前新的技术和应用带来更加丰富的数据，如何使现有的海量数据可分析、可解释、可利用，进而参与到真正的预测和决策场景中，还需要数据科学的深入研究。

苏萌认为，数据科学技术将像互联网一样普惠大众，业务和决策人员将可以直接与数据进行交互，提高分析和决策效率。数据科学技术在不断地迭代升级，它将会成为重要的生产力，推动商业模式和企业组织的变革。

如何加强场景驱动的数据分析等数据科学软实力建设？陈松蹊认为，挖掘数据生产力的关键是构建数据文化。因此，数据科学团队的建设非常重要，相关研究应贯穿数据采集、数据分析到管理决策的全流程，让统计师、数据分析师从始至终介入数据的价值挖掘。其次，应重视数据科学咨询，以数据科学咨询为主体的机构需要了解企业的业务模式和核心诉求。

上海纽约大学全球杰出商学讲席教授陈宇新也认为，目前数据领域的应用型人才较多，进一步的原创性突破则需要更多的原始创新人才。对于数字经济来说，数据质量的认证将会变得非常重要，认证和确认数据源可靠性的技术或服务将会兴起。

数据科学研究是与市场联系紧密的研究领域。陈松蹊认为，实体经济中数据的价值已开始彰显，但如何把数据转化成生产力，还需要数据科学、数据企业的共同努力，例如打造专业化、智能化、个性化的数据科学方案等。

短视频成“触网”首要应用 中青年使用率更高

◎新华社记者 董小红 袁秋岳

网络视听用户规模超过10亿，短视频成网民“触网”首要应用，中青年群体网络视听使用率更高……3月30日，第十届中国网络视听大会在成都开幕。

据本次大会发布的《中国网络视听发展研究报告（2023）》数据显示，截至2022年12月，我国网络视听用户规模达10.40亿，超过即时通讯，成为第一大互联网应用。其中，短视频成为行业发展的主要增量。

中国网络视听节目服务协会副秘书长周结介绍，目前，短视频用户规模达10.12亿，已成为吸引网民“触网”的首要应用，向各类网民群体渗透，用户黏性增长明显。

周结说，短视频“纳新”能力远超即时通讯，新入网的网民中，24.3%的网民第一次上网时使用的是短视频应用，与其他应用拉开了较大距离。

短视频为何能成为网民“触网”的首选？北京交通大学语言与传播学院讲师王晓培认为，短视频的操作简单便捷，加之其视觉化、接地气的表达方式，大大降低了新网民的接受门槛。此外，短视频还具有较强的社交属性，用户可与视频内容进行互动，也可与家人、朋友分享。这种强互动性能够帮助新网民更好地融入互联网世界。

随着短视频成为重要传播工具，短视频会取代长视频吗？本次大会上，相关专家及从业者也给出了解答。

“短视频并不会取代长视频，而是随着视听行业的发展，二者互相融合起来，加快形成良性的行业生态。”北京勾正数据科技有限公司董事长喻亮星告诉记者，当前，短视频行业已经走向成熟，观众审美、行业规则、平台玩法都在不断变化，短视频需要向长视频学习，在方寸之间精细化“打磨”，取“长”补“短”，才能持续发展。

“以前，一些短视频只是简单地把长视频剪短了。现在，很多短视频内容创作者和长视频生产商达成合作，短视频对长视频进行‘二次加工’，不仅内容更优质了，也能为长视频引流，互相促进。”北京云合文化传媒有限公司创始人李雪琳说。

王晓培也认为，短视频更适合碎片化场景，在短时间内能快速吸引观众注意；长视频更能传达复杂的故事与情感。“长短视频的关系是融合互补的，现在行业中也出现这一趋势，长短视频在不同情境下发挥各自优势，相互合作。”王晓培说。

《中国网络视听发展研究报告（2023）》数据显示，高学历、一线及新一线城市的中青年群体网络视听使用率更高。尤其是，看新闻、学知识已成为短视频用户的重要需求。用户群体的变化，给从业者带来新的挑战。经过前期“野蛮生长”后，短视频的内容生态逐步进入更加严格的监管范畴，行业也在“渴求”更优质的内容。

中国移动咪咕成都公司党委书记、总经理李军指出，网络视听行业需要坚持内容创新，尤其是加强与文化、教育、旅游等相关领域的深度融合和协同发展，才能不断满足用户对多元化优质内容的需求。

“用户学历更高，思考深度和广度在提升，以往‘流量至上’的行业增长模式可能会被颠覆，从小说、诗歌等文学作品中吸收养分‘转化’而来的短视频作品，将会越来越有市场。”四川大学文学与新闻学院教授侯洪说。