NERCBDS 大数据协同安全技术国家工程研究中心

360

BDS 国家工程研究中心和天枢智库联合出品

数字安全观察

DIGITAL SECURITY INSIGHT

数据安全专刊 No. 007(总第 218 期)

责编：钟力 zhongli1@360.cn

导 读

第七期《数字安全观察 数据安全专刊》梳理了 2023 年第一季度的数据安全发展动态，分为政策形势、两会盘点、技术与市场趋势、安全事件分析四个板块，主要内容如下：

政策形势方面，本期选取了 2023 年第一季度数据安全领域备受关注的政策消息，从国家、地方层面分类梳理。国家层面，《党和国家机构改革方案》通过并指出将成立国家数据局，《关于促进数据安全产业发展的指导意见》对数据安全产业发展作出了全面、系统的指导。地方层面，各地持续增强数字经济布局与数字政府建设，同时杭州市、新疆维吾尔自治区、上海市临港新片区、北京市等纷纷围绕出台文件促进数据要素市场培育、数据流通释放价值等，广州市、深圳市在数据交易方面发挥先行先试的引领带动作用。

两会盘点方面，本期分类梳理了多位全国人大代表、政协委员在两会上发表的数据安全相关提案。据不完全统计，今年两会上关于数据安全的提案有近 20 条，组建国家数据局、智能网联汽车数据安全、数据要素与数据流通、数字经济与数据安全、数据安全管理与个人信息保护等是其中的热门议题。

技术与市场方面，数据加密技术和数据交易取得重大突破，成为关注热点。技术方面，清华浙大相关团队在量子计算破解 RSA 密码方面取得新进展；美国 NIST 近日宣布，名为 ASCON 的认证加密和

散列算法系列将成为标准算法，用于轻量级密码学应用。市场方面，数据交易领域的创新突破不断，数据要素市场的逻辑和规则更为清晰，数据要素流通标准体系逐步健全。投融资方面，一季度的数据安全投融资保持了较为平稳的发展态势，其中炼石网络和观安信息两家厂商完成了过亿元的融资。

安全事件分析方面，第一季度的数据安全事件主要类型集中在数据泄露、勒索攻击以及合规挑战方面。其中，政务、汽车领域的数据泄露最为严重，也是网络攻击的热门目标，如美国法警局遭遇敏感信息泄露、沃尔沃遭受勒索攻击，200GB 敏感数据被售卖等。此外，因俄乌冲突的持续，针对关键基础设施的网络攻击也引发了大规模的数据泄露。另外值得关注的是，随着执法力度的加大，出现了多起因违反《数据安全法》、《个人信息保护法》的案例，重大违法违规行为受到严厉打击。

目 录

第一部分 政策形势

第二部分 两会盘点

第三部分 技术与市场

第四部分 安全事件分析

一、政策形势

2023 年第一季度，国家和地方出台了一系列促进数字经济和数据安全发展的法规与政策指导文件，有力推动了国家数字经济持续健康发展，数据产业开始逐步步入正轨。国家层面，《党和国家机构改革方案》通过并指出将成立国家数据局，《关于促进数据安全产业发展的指导意见》对数据安全产业发展作出了全面、系统的指导，《数据安全工程技术人员国家职业标准》对数据安全工程技术人员的定位、培训考核要求进行指导，我国数字经济与数据安全产业正在全面快速推进。地方层面，各地持续增强数字经济布局与数字政府建设，同时杭州市、新疆维吾尔自治区、上海市临港新片区、北京市等纷纷围绕出台文件促进数据要素市场培育、数据流通释放价值等，广州市、深圳市在数据交易方面发挥先行先试的引领带动作用。

（一）国家政策法规

1、《关于促进数据安全产业发展的指导意见》

1 月 13 日，工业和信息化部等十六部门发布《关于促进数据安全产业发展的指导意见》，《意见》指出数据安全产业是**为保障数据持续处于有效保护、合法利用、有序流动状态提供技术、产品和服务**的新兴业态。

为贯彻落实《中华人民共和国数据安全法》，推动数据安全产业

高质量发展，提高各行业各领域数据安全保障能力，加速数据要素市场培育和价值释放，夯实数字中国建设和数字经济发展基础，《意见》从七个方面明确路径：**一、提升产业创新能力**：加强核心技术攻关、构建数据安全产品体系、布局新兴领域融合创新；**二、壮大数据安全服务**：推进规划咨询与建设运维服务，积极发展检测、评估、认证服务；**三、推进标准体系建设**：加强数据安全产业重点标准供给；**四、推广技术产品应用**：提升关键环节、重点领域应用水平，加强应用试点和示范推广；**五、构建繁荣产业生态**：推动产业集聚发展，打造融通发展企业体系，强化基础设施建设；**六、强化人才供给保障**；**七、深化国际交流合作**。

（来源：工业和信息化部）

2、《进一步提升移动互联网应用服务能力的通知》

2 月 6 日，针对部分企业服务行为不规范、相关环节责任落实不到位等问题仍时有发生等情形，工业和信息化部发布《关于进一步提升移动互联网应用服务能力的通知》。

为**提升全流程服务感知，保护用户合法权益**，《通知》指出要规范安装卸载行为、优化服务体验、加强个人信息保护、加强个人信息保护；同时，《通知》提出要**提升全链条管理能力，营造健康服务生态**，包括落实 APP 开发运营者主体责任、强化平台分发管理、规范 SDK 应用服务、筑牢终端安全防线、夯实接入企业责任。

（来源：中国政府网）

3、工业和信息化部行政执法事项清单

2 月 8 日，工业和信息化公布了《工业和信息化部行政执法事项清单（2022 年版）》，其中，第 247-261 条为依据《中华人民共和国数据安全法》相关条款增的数据安全事项，包括：

1) 对工业和信息化领域数据处理者落实数据安全保护责任义务及管理措施落实的监督检查；
2) 对工业和信息化领域数据处理者开展数据处理活动未依照法律、法规的规定，建立健全全流程数据安全管理制度的行政处罚；
3) 对工业和信息化领域数据处理者开展数据处理活动未依照法律、法规的规定，组织开展数据安全教育培训的行政处罚；
4) 对工业和信息化领域数据处理者开展数据处理活动未依照法律、法规的规定，采取相应的技术措施和其他必要措施，保障数据安全的行政处罚；
5) 对工业和信息化领域数据处理者利用互联网等信息网络开展数据处理活动，未在网络安全等级保护制度的基础上，履行第二十七条数据安全保护义务的行政处罚；
6) 对工业和信息化领域重要数据的数据处理者，未明确数据安全负责人和管理机构，落实数据安全保护责任的行政处罚；
7) 对工业和信息化领域数据处理者开展数据处理活动，未加强

风险监测，发现数据安全缺陷、漏洞等风险时，未立即采取补救措施的行政处罚；

8) 对工业和信息化领域数据处理者发生数据安全事件时，未立即采取处置措施的行政处罚；

9) 对工业和信息化领域数据处理者发生数据安全事件时，未按照规定及时告知用户并向有关主管部门报告的行政处罚；

10) 对工业和信息化领域重要数据的处理者未按照规定对其数据处理活动定期开展风险评估，并向有关主管部门报送风险评估报告的行政处罚；

11) 对工业和信息化领域重要数据的处理者报送的风险评估报告未包括处理的重要数据的种类、数量，开展数据处理活动的情况，面临的数据安全风险及其应对措施等的行政处罚；

12) 对工业和信息化领域关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，未落实《中华人民共和国网络安全法》的有关规定的行政处罚；

13) 对工业和信息化领域非关键信息基础设施运营者的数据处理者在中华人民共和国境内运营中收集和产生的重要数据的出境安全管理，未落实《数据出境安全评估办法》等有关规定的行政处罚；

14) 对从事工业和信息化领域数据交易中介服务的机构，未要求

数据提供方说明数据来源，审核交易双方的身份，并留存审核、交易记录的行政处罚；

15) 对境内的工业和信息化领域数据处理者未经工业、电信、无线电领域主管机关批准向外国司法或者执法机构提供存储于境内的数据的行政处罚。

（来源：工业和信息化部）

4、《个人信息出境标准合同办法》

2 月 24 日，国家互联网信息办公室公布《个人信息出境标准合同办法》，自 6 月 1 日起施行。《办法》对个人信息出境标准合同（以下简称“标准合同”）的适用范围、订立条件和备案要求等方面做出了具体说明，并明确了标准合同范本，为《中华人民共和国个人信息保护法》第三十八条中第三款的要求提供了具体指引。

（来源：网信办）

5、《数字中国建设整体布局规划》

中共中央、国务院印发《数字中国建设整体布局规划》，指出建设数字中国是数字时代推进中国式现代化的重要引擎，是构筑国家竞争新优势的有力支撑，而加快数字中国建设，对全面建设社会主义现代化国家、全面推进中华民族伟大复兴具有重要意义和深远影响。

《规划》提出，到 2025 年，基本形成横向打通、纵向贯通、协调有力的一体化推进格局，数字中国建设取得重要进展；到 2035 年，

数字化发展水平进入世界前列，数字中国建设取得重大成就。

《规划》明确，数字中国建设按照“2522”的整体框架进行布局，即夯实数字基础设施和数据资源体系“两大基础”，推进数字技术与经济、政治、文化、社会、生态文明建设“五位一体”深度融合，强化数字技术创新体系和数字安全屏障“两大能力”，优化数字化发展国内国际“两个环境”。

（来源：中国政府网）

6、《证券期货业网络和信息安全管理办法》

2 月 27 日，中国证券监督管理委员会公布《证券期货业网络和信息安全管理办法》，自 5 月 1 日起施行。《办法》聚焦网络和信息安全管理，强化个人信息保护，结合证券期货业特点，为相关法律法规在证券期货业的有效落地，明确实施路径，提供制度保障。

《办法》共八章七十五条，对证券期货业网络和信息安全监督管理体系、网络和信息安全运行、投资者个人信息保护、网络和信息安全应急处置、关键信息基础设施安全保护、网络和信息安全促进与发展、监督管理与法律责任等方面提出了要求。

（来源：中国证监会）

7、《党和国家机构改革方案》通过，将成立国家数据局

党的二十届二中全会通过了《党和国家机构改革方案》，深化国务院机构改革是其中的一项重要任务。其中，《方案》提到将组建国

家数据局，由其负责协调推进数据基础制度建设，统筹数据资源整合共享和开发利用，统筹推进数字中国、数字经济、数字社会规划和建设等，由国家发展和改革委员会管理。

将中央网络安全和信息化委员会办公室承担的研究拟订数字中国建设方案、协调推动公共服务和社会治理信息化、协调促进智慧城市建设、协调国家重要信息资源开发利用与共享、推动信息资源跨行业跨部门互联互通等职责，国家发展和改革委员会承担的统筹推进数字经济发展、组织实施国家大数据战略、推进数据要素基础制度建设、推进数字基础设施布局建设等职责划入国家数据局。

（来源：中国政府网）

8、《数据安全工程技术人员国家职业标准》

3 月 20 日，人力资源社会保障部、中央网信办、工业和信息化部共同制定了《数据安全工程技术人员国家职业标准（2023 年版）》，明确了数据安全工程技术人员的职业定义、培训要求以及专业技术考核要求，规定该角色需具备的职业道德、基础理论知识、技术基础知识、相关法律法规标准知识及其他知识，并对初级、中级、高级数据安全工程技术人员的专业能力要求和相关知识要求依次递进，高级别涵盖低级别的要求。

（来源：人社部）

9、文旅部：加强旅游者个人敏感信息保护

3 月 27 日，文化和旅游部发布《关于推动在线旅游市场高质量发展的意见》，围绕市场环境、市场秩序、行业发展等方面提出要求。在营造良好的市场环境方面，《意见》提出加强内容安全审核，包括：对市场主体、行政许可资质等信息进行真实性核验，督促在线旅游平台经营者及平台内经营者加强审核人员培训、**网络安全等级保护建设**和文字、图片、音视频等信息内容审核，确保平台信息内容安全；同时要保障旅游者合法权益，包括：**加强旅游者个人敏感信息保护**，防止超出合理经营需要收集旅游者个人信息，采取切实措施避免大数据杀熟、虚假宣传、虚假预订等侵害旅游者权益行为。

（来源：中国政府网）

10、《关于开展网络安全服务认证工作的实施意见》

3 月 28 日，市场监管总局、中央网络安全和信息化委员会办公室、工业和信息化部、公安部四部门发布《关于开展网络安全服务认证工作的实施意见》。《意见》从**网络安全服务认证机构**、**通过认证的网络安全服务机构**、**网络运营者**以及**监管部门**四类主体的维度，就开展国家统一推行的网络安全服务认证工作提出九点意见，对《中华人民共和国网络安全法》第十七条中**国家鼓励开展网络安全认证、检测和风险评估**等安全服务进行落实。

（来源：中国政府网）

（二）地方政策法规

1、《临港新片区国际数据产业专项规划（2023-2025 年）》

1 月 5 日，为进一步推动临港新片区国际数据港建设和国际数据产业发展，中国（上海）自由贸易试验区临港新片区管理委员会发布了《临港新片区国际数据产业专项规划（2023-2025 年）》。

《规划》从国际数据交流窗口走向开放、国内数据监管政策逐步完善、上海数据产业生态持续优化、临港新片区数据支撑底座加快成型几个方面对临港的数据产业发展概况进行总结；结合临港新片区数字经济发展定位、产业布局、城市空间布局，明确了临港数据产业规划的指导思想、基本原则、发展目标；并提出了**构筑数据要素支撑底座、打造数据产业承载区、构建繁荣有序市场生态、推进跨境数据流动服务、提升数据赋能产业价值**五大主要任务。

（来源：临港新片区管委会）

2、全国首个获批数据出境安全评估案例落地北京

自 2022 年 9 月 1 日《数据出境安全评估办法》实施以来，北京市互联网信息办公室率先开通全国首个地方申报受理咨询专线。近日，首都医科大学附属北京友谊医院与荷兰阿姆斯特丹大学医学中心合作研究项目成为**全国首个数据合规出境案例**，该项目的审批通过，标志着国家数据出境安全评估制度在北京市率先落地，为强化医疗健康数据出境安全管理，促进国际医疗研究合作提供了实践指引。

随后，北京市申报的中国国际航空股份有限公司项目作为**全国第二例**也成功获批通过，为北京市进一步指导支持更多企事业单位解决数据合规出境需求积累了经验、打通了路径，对提升北京市数据安全合规管理水平、优化营商环境具有重要意义。

（来源：网信北京）

3、《2023 年市政府工作报告重点任务清单》印发，提出推动北京数据特区建设

1 月 31 日，北京市人民政府关于印发《2023 年市政府工作报告重点任务清单》，从坚持规划引领，持续优化提升首都功能等十二个方面提出了 300 项重点任务，并明确主责单位。

其中，《清单》提出要着力建设全球数字经济标杆城市，落实北京数字经济促进条例，**推动北京数据特区建设**，开展数据基础制度先行示范。加快数字经济和实体经济深度融合，推进数字产业化和产业数字化，推动数字经济全产业链发展，创新公共数据授权运营，深化公共数据开放、数据交易流通，提升数据要素治理能力。

同时指出要培育数据要素开放共享新市场，提升国际大数据交易所能级，鼓励各类市场主体进场交易，加快汇聚行业高价值数据，打造普惠社会数据专区；培育数据评估评价、安全评估等数据要素市场机构，提供数据经纪、登记、评估等全链路服务；在服务数字贸易、数据跨境流通、对接国际数字经济规则方面先行先试。

（来源：北京市人民政府）

4、《广东省“数字政府 2.0”建设落实“实体经济为本，制造业当家”工作若干措施》

2 月 15 日，广东省政务服务数据管理局发布《广东省“数字政府 2.0”建设落实“实体经济为本，制造业当家”工作若干措施》，围绕优化营商环境、赋能实体经济提质增效、促进数据产业发展、培育数字政府产业生态、推动信创产业高质量发展、推进数字政府网络安全产业发展、营造服务实体经济良好环境等七个方面提出工作措施。

《措施》明确指出要**加强数据安全产品应用和推广**。加强政务数据安全保护，做好政务数据开放和社会化利用的安全管理。支持数据安全产业发展，培育数据安全企业、研究和服务机构。重点推动数据加密、数据脱敏、密文检索、访问控制、安全审计、数据溯源等数据安全技术产品应用和推广。

（来源：广东省政务服务数据管理局）

5、《杭州市公共数据授权运营实施方案（试行）》（征求意见稿）

2 月 17 日，杭州市数据资源管理局发布了《杭州市公共数据授权运营实施方案（试行）》（征求意见稿）公开征求意见的公告，《方案》明确了杭州市公共数据授权运营的指导思想、基本原则以及工作目标，规定了数据范围，并从公共数据资源基础、公共数据授权运营平台、公共数据授权运营工作机制、重点场景应用几个维度提出重点任务。

《方案》对公共数据加工使用主体明确了技术与安全要求：明确

数据安全负责人和管理部门，建立公共数据授权运营内部管理和**安全保障制度**；具备通过网络安全等级保护三级标准的系统开发和运维实践经验；按照《数据安全管理认证实施规则》通过数据安全管理认证规范数据处理活动，鼓励通过数据管理能力成熟度（DCMM）和**数据安全能力成熟度（DSMM）3 级**以上认证；公共数据安全体系评估结果无高风险项。

（来源：杭州市人民政府）

6、《深圳市数据产权登记管理暂行办法》（征求意见稿）

2 月 20 日，深圳市发展和改革委员会就《深圳市数据产权登记管理暂行办法》（征求意见稿）公开征求社会公众意见。

《办法》包括七章，共计三十三条，明确了登记主体的权利与义务、登记机构的管理要求，对数据产权登记进行了类型划分并规定了每种登记类型的定义及流程，同时指出了数据产权登记的监管部门、监管方式等监督管理要求。

（来源：深圳司法局）

7、《新疆维吾尔自治区公共数据管理办法（试行）》

2 月 22 日，新疆维吾尔自治区人民政府办公厅公布《新疆维吾尔自治区公共数据管理办法（试行）》，包括九章，共四十七条，明确了公共数据管理的总体原则、公共数据目录、公共数据采集与归集、公共数据共享、公共数据开放、公共数据安全等方面的管理要求。

（来源：新疆维吾尔自治区人民政府）

8、《云南省数字政府建设总体方案》

3月2日，云南省人民政府印发《云南省数字政府建设总体方案》，定义了数字政府的技术架构、业务应用架构、层级架构以及建设管理架构，围绕政府数字化履职能力体系、安全保障体系、制度规则体系、数据资源体系、平台支撑体系、建设管理体系、数字化发展等方面明确主要任务和重点工程。其中，在主要任务“构建数字政府全方位安全保障体系”提出强化安全管理责任、落实安全管理制度、提升安全保障能力的重点工程。

（来源：云南省人民政府）

9、《深圳市数据交易管理暂行办法》、《深圳市数据商和数据流通交易第三方服务机构管理暂行办法》印发

3月2日，深圳市发展和改革委员会印发了《深圳市数据交易管理暂行办法》、《深圳市数据商和数据流通交易第三方服务机构管理暂行办法》。

《深圳市数据交易管理暂行办法》共八章，总计三十五条，规定了对数据交易主体、数据交易场所运营机构的管理要求，明确了数据交易各类标的类型，规范了数据交易各环节内容，针对数据交易场所运营机构、数据卖方、数据买房、第三方服务机构等数据安全管理要求作出规定。

《深圳市数据商和数据流通交易第三方服务机构管理暂行办法》共五章，总计二十七条，对数据商和第三方服务机构规范开展业务作出规定，明确数据商数据开发及交易代理安全义务、安全保护管理体系、应急处置机制等要求。

（来源：深圳政府在线（深发改规〔2023〕3 号）、深圳政府在线（ 深发改规〔2023〕4 号））

10、《郑州市政务数据安全管理实施细则》

3 月 21 日，郑州市人民政府印发《郑州市政务数据安全管理实施细则》，共五章，总计三十九条。《细则》要求政务部门规范政务信息系统和政务数据资源管理，采取安全策略和技术措施，加强对数据收集、存储、传输、共享、开放、使用、销毁等全生命周期的安全保护，并强调加强个人信息保护。要求市政务数据主管部门会同网信、公安等部门建立应急协调机制，政务部门应按照本级政务数据主管部门和上级业务主管部门要求，建立政务数据安全应急管理机制，及时进行应急处置。

（来源：郑州市大数据管理局）

11、《“河南链”建设实施方案（2023—2025 年）》

3 月 28 日，河南省人民政府办公厅印发《“河南链”建设实施方案（2023—2025 年）》，从总体架构、公共基础平台架构、与其他业务系统的关系方面对“河南链”进行了架构设计，并提出了七项重要任

务：构建“河南链”云链融合网络、建设“河南链”数据共享链、推动“河南链”示范应用、开展“河南链”区域试点、建立“河南链”标准体系、助力数据要素市场发展、培育区块链产业生态。

其中，“河南链”数据共享链指：基于云链融合网络和省、市两级数据共享交换平台，开发建设省级数据共享主链和 19 条市级数据共享子链。根据政务数据普查结果，结合上链标准规范，统筹编制全省政务数据目录、重要数据和敏感数据清单，实现政务数据目录、重要数据和敏感数据直接或加密后上链，并进行动态维护和更新。依托上链政务数据目录，完善全省一体化政务数据目录资源体系，提升政务数据共享相关的目录索引、信息查询、信息核验、业务协同等能力，形成“河南链”和省、市两级数据共享交换平台共同对外提供数据共享服务的新模式。探索利用自主可控的标识代码体系开展数据统一编码和码链融合创新应用。

（来源：河南省人民政府）

二、两会盘点

在今年的全国两会期间，多位代表委员提出了关于数据安全的提案，为我国数字经济与数据安全发展建言献策。这些提案主要分布在智能网联汽车数据安全、数据要素与数据流通、数字经济与数据安全、数据安全管理与个人信息保护等四个方面。

（一）智能网联汽车数据安全

1、构建完善汽车数据安全管理体系

雷　军

全国人大代表、小米集团创始人、董事长兼 CEO

智能网联汽车承载的数据，既是数字经济发展的重要要素资产，也给个人隐私、国家公共利益与安全带来了挑战。目前汽车数据安全标准、认证评价、应用管理等机制仍不完善，制约了行业发展。雷军**建议：**

加快制定汽车全生命周期的数据安全标准，指导产业发展。目前国家已发布若干汽车相关的数据安全推荐性国家标准，规范了网约车服务及汽车数据采集等部分场景要求，尚无法覆盖到研产供销全业务领域，建议主管部门牵头制定涵盖汽车全生命周期的数据安全管理规范及标准，定义汽车数据分类分级规则，围绕汽车生命周期和数据生命周期两条主线，制定汽车数据安全开发、测试、风险评估及数据跨境等领域标准规范，统一基准，指导产业发展。同时鼓励企业针对特

定区域、特定场景数据的管理实践经验进行探索总结，不断丰富完善相关规范，并在行业进行应用推广。

建立汽车数据安全认证、评价机制。目前智能网联汽车数据安全认证体系仍不完善，企业推进数据安全的积极性有待进一步提高。**建议主管部门牵头出台智能网联汽车数据安全认证制度，规范认证流程；制定评价等级及对应指标，建立智能网联汽车数据安全评级及公示制度，提升行业透明度与可信度，促进企业加大数据安全的投入，引导行业企业正向发展。**

构建汽车数据共享机制及平台，促进汽车数据共享使用。当前各车企间数据尚未实现有效安全流通，数据孤岛普遍存在，数据价值无法充分发挥。**建议国家有关部门牵头行业协会、研究机构及产业链各环节厂商，针对不同场景搭建互认、互信、互通的行业级数据共享机制及平台，**在保障数据安全的前提下，实现数据可用、可信、可追溯明确数据产权归属和利用范式，将数据转化为社会生产力，为数字经济进一步发展贡献助力。

（来源：人民网）

2、关于统筹智能网联汽车数据收集与共享的建议

朱华荣

全国人大代表、长安汽车董事长

在智能网联汽车发展过程中，针对现有法规不足、汽车行业中存在数据格式不统一、严格审批监管与快速更新需求的矛盾以及重复采集造成国家层面的资源浪费、数据质量未达到让车辆数据共享的程度等问题，朱华荣提出五项改善建议：

（1）建立、健全汽车数据相关法律法规；

（2）建立汽车数据采集统一方案、数据统一标准。完善高精度地图数据策略与管理机制；

（3）制定安全可行的数据生产应用策略，建立用户申请——部委审批——地方监管的数据使用和更新机制；

（4）培育 3-5 家国资为主的国家级地图公司；

（5）建立汽车数据质量国家过检平台，提供从标准定义、质量监控、重大问题及时告警等数据质量全生命周期管理，实现对汽车数据的质量控制，驱动以监测问题为导向的持续改进，提高各车企数据质量。

（来源：新浪财经）

3、关于探索加快自动驾驶应用落地体系化保障的建议

何小鹏

全国人大代表，小鹏汽车董事长、CEO

随着自动驾驶技术的快速发展，我国现行的相关法律法规中对智能网联汽车在自动驾驶系统运行中可能发生的交通事故责任认定、产

品准入标准等问题并未完善。国家相关部委已启动开展智能网联汽车准入和上路通行试点工作。为此，何小鹏提出三点建议：

首先，**建议推动加快智能网联汽车和自动驾驶相关立法工作。**近年来，虽然国家级地方政府陆续出台相关法律法规，为智能网联汽车和自动驾驶的发展提供了一定的法律保障。但由于自动驾驶技术发展进程加快及其特殊性，相应法律法规仍需进一步完善，安全标准和技术规范亟待建立。建议完善相应法律法规的制定修订，加快相关标准、技术规范要求落地。

其次，**建议探索建立自动驾驶技术及自动驾驶汽车保险产品体系。**当前我国智能网联汽车产业发展强劲，但自动驾驶保险产品在国内尚不成熟，亟需探索建立自动驾驶技术及自动驾驶汽车保险产品体系。他建议制定自动驾驶汽车保险纲领性文件，鼓励部分地区开展自动驾驶保险创新先行先试，另外鼓励自动驾驶汽车企业参与保险产品创新。

最后，**建议推动加快城市高精地图审核流程。**高精地图是目前实现自动驾驶的重要基础设施之一。但由于我国城市道路情况 变化较快，为保证地图“鲜”度，建议优化审核流程，提升地图更新频率，加快高精地图基础设施进程。具体来说，要允许地图增量更新集中审核，要建立线上备案流程和先用后审机制，此外还要允许和鼓励众源方式更新地图。

（来源：DoNEWS）

4、建议适时启动《自动驾驶法》立法进程

连玉明

全国政协委员、北京国际城市发展研究院院长

我国现行的法律法规制度针对的是有人驾驶的传统汽车，自动驾驶汽车发展面临车辆不能入市、不能上牌、不能运营收费、车辆保险制度不完善、发生交通事故时责任无法认定、相关数据保护缺乏监管等诸多法律问题。需加快自动驾驶领域的立法，以充分发挥立法对技术创新和产业发展的引领和助推作用。为此，连玉明提出了以下三点建议：

其一，完善自动驾驶领域数据基础制度体系，强化顶层设计。

（1）制定自动驾驶数据分级分类安全规范。根据数据安全受到威胁后可能侵害个人和企业权益、社会公共利益、国家安全的严重程度划分等级，以实现差异化保护。

（2）制定自动驾驶数据共享规范。自动驾驶产业特性要求政府制定数据共享规范，不同类型的自动驾驶数据应当享有不同程度的共享水平。自动驾驶汽车在道路测试或实际驾驶运行中发生事故，产生的事故数据必须上报监管部门，同时由监管部门对社会公开共享。事故数据之外的自动驾驶数据，包括道路测试数据、仿真数据以及实际运行数据是企业竞争的基石，不宜通过法律强制要求其向行业共享。

（3）出台自动驾驶数据流通规范。自动驾驶数据中的重要数据实行分类管理。个人信息、商业秘密和国家安全以外的自动驾驶数据，

应当在符合法律规定的前提下允许自由流动，以促进自动驾驶技术和产业发展。

其二，鼓励、支持和引导地方自动驾驶领域创新实践，促进地方立法先行先试。

（1）针对自动驾驶汽车高速公路测试、无安全员驾驶、远程控制测试、载客示范、商业化试运营等先导应用，鼓励地方加快出台政策规制和专项规范，保障相关自动驾驶车辆合规上路。

（2）打破地方壁垒，消除自动驾驶汽车各地规制差异化造成的障碍，由有关部委牵头，建立各地方测试纪录与许可互认制度，为自动驾驶产业提供一个全国性的统一市场与道路测试基础。

（3）通过立法机关授权试点或制定暂行条例等方式，引导并支持代表性地区和城市逐步开展针对自动驾驶立法的先行先试。

其三，加强国外立法经验鉴别和借鉴，推进《自动驾驶法》立法进程。

（1）尽快推动《道路交通安全法》修订与颁布。现行《道路交通安全法》并没有考虑自动驾驶车辆的法律规制问题，诸多方面规定与自动驾驶车辆的测试、运营等相排斥。通过修订《道路交通安全法》，明确自动驾驶系统的合法地位，并制定人类驾驶员与自动驾驶系统的责任划分和处置机制。

（2）推进涉及自动驾驶车辆保险、交通事故定责赔偿、网络和数据安全等领域配套立法制度的更新和跟进。

（3）通过综合性的中央立法解决法律障碍，适时启动《自动驾驶法》立法进程。逐步形成自动驾驶车辆测试制度体系、运营制度体系、操作规则体系、保险制度体系、隐私权保护和数据安全漏洞防范法律体系以及自动驾驶车辆交通事故责任体系等。

（来源：南方都市报）

（二）数据要素与数据流通

1、加快构建数据知识产权保护规则

陈群

全国政协委员，民盟中央副主席、上海市委主委，上海市政协副主席

随着新一轮科技革命和产业变革深入发展，数据作为数字经济时代不可或缺的新型生产要素，正逐渐成为经济高质量发展的重要支撑。数字经济的发展离不开相关的治理体系，去年 12 月，《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》发布，系统布局了数据基础制度体系的“四梁八柱”。总体上看，我国数据治理体系建设已进入快车道，但也面临着制度体系亟须健全、交易体系有待完善、治理体系有待优化的挑战。

为促进数据有效保护和充分利用，加快发展数字经济，提出以下建议：

加快建立数据知识产权保护规则。在地方试点探索基础上，充分把握数据的特有属性和产权制度的客观规律，以促进数据要素有效流

通为关键，探索建立数据确权授权机制，合理界定参与数据生产、流通、使用等各方的合法权益，加快构建数据知识产权保护规则。同时，在国家层面进一步加强数据知识产权登记规则和登记系统的顶层设计，为构建数据要素流通统一大市场提供基础保障。此外，规则制度建设过程中，要注重衔接国际规则，推动形成体现中国特色、接轨国际发展趋势的数据知识产权保护方案，在新一轮国际竞争中赢得主动。

加快健全数据要素市场体系。进一步完善数据流通交易规则，探索数据价值评估和交易定价机制，规范数据流通交易行为，培育壮大数据交易规模。进一步创新数据交易机制，规范推进数据交易所建设，更好发挥第三方专业机构作用，鼓励拓展数据服务内涵，加强数据流通和交易全流程服务，强化数据交易平台和要素资源互联互通，提升数据要素交易流通效率和效益。进一步完善数据跨境流通管理机制，建立负面清单制度，更大力度提升数据开放共享水平。

加快完善数据治理体系。一方面，完善政府治理，在国家层面进一步明确数据管理和治理监管的部门职责，强化对数据保护和利用工作的统筹协调，聚焦数据交易准入、合规审查、跨境流通、数据安全等重点环节，进一步完善管理规则、操作细则和标准规范，建立健全监管机制，确保市场公平竞争和健康运行。另一方面，完善社会多元治理体系，鼓励市场主体、行业协会等共同参与，加强数据安全技术能力建设，推动数据要素市场自律机制和信用体系建设，切实规范数据利用行为。

（来源：新浪新闻）

2、释放数据要素潜力 更好赋能高水平对外开放

张英

全国政协委员、上海市经济和信息化委员会副主任

目前，我国在推动建立与国际经贸往来相适应的数据流动机制方面，主要有三方面不足：

一是对标高标准国际规则相对滞后，目前我国数据要素市场建设尚处于起步阶段，在面向国际的数据治理规则方面仍存在不少盲区，比如电子发票国内国际标准尚未有机衔接等。

二是数据国际合作与流动的试点路径不够清晰。近年来，我国通过自贸试验区建设探索了一条从沿海到内陆，再到全国复制推广的经贸开放新路径，但是目前仍缺少对标数字经济国际规则开展集成创新试点的试验区，创新数据流动的国际合作机制已经成为制约高水平开放的关键环节。

三是数据跨境流动缺少场景思维。当前我国数据跨境流动主要以单个企业和具体数据内容作为对象，由于缺少国际间经贸往来和交流合作场景为驱动的系统性设计，导致数据流动碎片化、个案化，面临“能出境的数据不可用，可用的数据难出境”等困境，直接影响到了企业“引进来、走出去”的成效。

就上述问题，张英建议：

一是对标 DEPA 等数字经济规则，率先在上海自贸新片区等地区，开展规则的综合集成和压力测试，设立高标准规则集成的数据国际合作试验区。积极参与数据流动、数据安全、认证评估、数字货币等国际规则和数字技术标准制定。

二是完善场景牵引下的数据流动机制和规则，聚焦全球经贸合作、高端产业开放、国际创新协同等经济数字化转型关键领域场景，完善操作指引，更好服务中国式现代化和韧性供应链体系构建。

三是创设面向国际数据合作的关键基础设施，增强国际间连接能力与算力协同，加强区块链、隐私计算等技术应用，探索“数据可用不出境”等新机制、新模式。依托上海数据交易所等国家级数据交易所，设立数据交易国际板。

（来源：中国工信产业网）

3、建议加快探索数据产权和数据空间

余晓晖

全国政协委员，中国信息通信研究院院长、党委副书记余晓晖

《中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见》(“数据二十条”)发布，以数据产权、流通交易、收益分配、安全治理为重点，系统布局了数据基础制度体系的“四梁八柱”，为充分激活数据要素潜能、做强做优做大数字经济、增强经济发展新动能指明方向。下一步，如何推动“数据二十条”落地实施成为关键。

余晓晖指出，由于数据本身可复制、能够被多主体占有或控制，数据交易存在阿罗信息悖论及数据泄露风险，因此，推动数据产权落地、增强数据交易流通互信成为落实“数据二十条”面临的首要挑战。

为此，他建议，**一方面在多层级数据要素市场建设中探索数据产权，推动数据分类分级，完善授权机制，强化确权基础。**通过探索建立三级数据交易市场，活跃产权流转机制，探索一级市场进行数据登记授权，健全数据登记和信息披露机制；二级市场进行数据流通交易，行使数据经营权、流转数据使用权；三级市场展开数据质押、数据信托等资本化交易活动。**另一方面在可信数据空间建设中探索数据流通互信，探索利用体系化的技术安排，确保数据流通协议的确认、履行和维护，解决数据流通主体间的安全和信任问题。**

建议结合数字化转型开展可信数据空间应用探索，面向制造、能源、医疗、交通等重点行业，打造行业数据空间测试床，开展应用验证；结合应用开展可信数据空间技术探索，制定技术标准，培育技术服务商；推动可信数据空间生态建设，推动可信数据空间与数据交易所、数据经纪商等现有流通模式融合发展。

（来源：中国网财经）

4、建设多层次数据要素市场，加快建设国家数字信任平台

邵志清

全国政协委员、致公党上海市委专职副主委

数据要素市场已成为国家竞争优势的重要内容。邵志清认为，我国数据要素市场处于发展初期，还存在数据交易机构统筹不足、基础设施不完善、数据资产化尚未落地等三大问题。

对此，邵志清建议，最首要的是制定加快培育全国统一数据要素市场体系的指导意见。建立分工明确、协同推进的多层次数据要素市场建设工作机制，避免各部门、各地方重复建设。明确多层次数据要素市场的总体架构和具体目标，加快建设国家数据交易所、有序推进地方数据交易中心建设、积极推动行业数据交易中心建设、引导多层次数据交易市场联动发展。完善统一数据要素市场功能，建立数据要素流通交易制度和标准体系，加强数据要素交易市场基础设施建设，加强组织保障。

针对数据交易机构建设不集中的问题，邵志清提出应当集中资源，重点支持建设国家数据交易所。支持上海、北京、深圳等条件成熟的地区建设国家数据交易所，按照“确立合法身份”和“落实法定功能”的发展阶段，完善法律、标准、政策和财政工具包。支持国家数据交易所开展数据要素基础制度创新试点，加快建设服务全国的数据基础设施，开展数据产品交易、数据资产登记、数据资产凭证管理等服务，有效链接地方和行业数据交易中心，打造全国统一数据要素市场的功能枢纽。依托国家数据交易所建设数据要素流通国家工程研究中心，加强相关理论问题与技术规范的研究。

在基础设施建设方面，邵志清建议，加快关键技术攻关，打造领跑全球、引领未来的数据要素流通基础设施。支持重点地区“云、链、网、技”建设，尽快打造多层次数据要素市场的基础设施，为场内集中交易和场外分散交易提供低成本、高效率、可信赖的流通环境。提升基础设施的效率能力，实现业务流程自动化和智能化，提高匹配效率和业务处理效率。提升基础设施的合规能力，基于区块链和可信隐私计算技术，搭建互通互联的交易系统和可信可控的交易环境。

（来源：中国电子银行网）

5、加强数据权利司法保护，更好发挥数据要素作用

连玉明

全国政协委员、北京国际城市发展研究院院长连玉明

近年来，随着《民法典》《数据安全法》《个人信息保护法》相继出台实施，为数字经济健康有序发展提供了基础制度支撑。但最为核心的数据确权问题一直没有解决。数据权利保护在司法实践层面还面临诸多困境，近期爆火的 ChatGPT 现象级应用背后就是道德伦理标准、信息隐私泄露、产品安全责任、数据跨境传输、数据产权保护等一系列新的法律问题，加强数据权利保护迫在眉睫。在这一背景下，进一步加强数据权利司法保护，对于构建适应数据特征、符合数字经济发展规律、保障国家数据安全、彰显创新引领的数据基础制度，实现数据合规高效流通使用，全面激活数据要素潜能具有重大现实意义。

研究出台数据权利保护相关司法解释和指导性案例。数据权利制度需要细化，才具有可操作性和可适用性，现行法律关于数据权利的规定较为笼统且分散。为此，建议司法机关立足审判实践，出台更具操作性的数据权利司法解释，配套出台数据权利的行政法规、部门规章和规范性文件，提高数据权利司法保护的操作性。同时，建议最高人民法院围绕数据权利保护的普遍性、规律性问题开展数据权利司法类案研究，并发布数据权利司法保护指导性案例，为各地数据保护司法实践提供参考。

加强和完善基于数据基础制度的数据产权司法保护。数据产权问题是数字经济领域亟须解决的堵点问题。加强和完善基于数据基础制度的数据产权司法保护，推动数据合规高效流通使用，关键是要进一步健全数据要素权益保护制度，依法保护数据权利人对数据控制、处理、收益等合法权益，以及数据要素市场主体以合法收集和自身生成数据为基础开发的数据产品的财产性权益，妥善审理因数据交易、数据市场不正当竞争等产生的各类案件，为培育数据驱动、跨界融合、共创共享、公平竞争的数据要素市场提供司法保障。同时，加强数据产权属性、形态、权属、公共数据共享机制等法律问题研究，按照安全至上、互联互通、公益优先、贡献定酬的原则，进一步细化完善数据产权司法保护规则。通过裁判规则的确立助力数据流通，以司法保护支持数据的价值转化、支撑数据的社会功能运转。

（来源：中国政协）

6、加快建设国家数据交易所，形成数字资产市场

张琦

全国政协委员、上海市信息投资股份有限公司董事长

数据资源化、资源产品化、产品价值化已成为数据资产化不可缺少的关键环节，但目前数据市场存在数据资产标的物不明确等困惑。“数据资源”的模糊标的无法完整反映数据资产的产品属性和价值属性，目前亟须重新明确数据资产标的物。同时，数据资产市场也未形成。

针对上述问题，张琦建议，按照“三步蒸馏法”明确数据资产标的物。

张琦解释说，“三步蒸馏法”意味着数据资产的形成有三个步骤：第一步，企业基于数据资源研发具备明确应用场景的、可持续服务的数据产品，初步形成数据资产；第二步，企业明确对内服务共享、对外流通交易为数据资产的主要运营模式，明确内部价值和外部价值都是数据资产的价值获取途径；第三步，数据交易场所将数据产品市场信息记录为基于区块链技术的数据资产凭证，作为数据资产价值确认与计量的可靠依据。

他建议，可按照“三步蒸馏法”设置更为贴切的会计科目和更为科学的计量方法，从“三步蒸馏法”出发为数据资产入表提供具体指导，加快推进数据资产入表落地。建议按照案例探索、推动示范、有序实施三步走的路径推进数据资产化。首先，探索一批数据资产入表典型

案例，由试点数据交易场所开展数据资产入表的模拟运营；其次，构建有法律效力的数据资产凭证，落实数据资产价值计量标准，已在试点数据交易场所获得数据资产凭证的企业率先入表；最后，在前期实践的基础上，不断完善数据资产会计准则，并构建起完善的数据资产凭证相关制度规范。

张琦同时建议，国资管理部门按照“三步蒸馏法”推进央企国企的数据资产化，将加工生产数据产品并通过数据交易场所流通交易作为数字化转型的重要抓手，将企业数据资产化与“发挥国有企业带头作用”结合起来。

（来源：中国证券网）

（三）数字经济与数字安全

1、推广城市数字安全服务中心模式

周鸿祎

全国政协委员、360 集团创始人

过去几年，360 在多个城市建设城市数字安全大脑，为城市管理者和监管部门提供了统一的数字安全态势感知平台，提升城市“看见”攻击的能力。但在此过程中，城市安全建设暴露了许多新的问题：一是安全建设上各自为战；二是很多单位虽然购买了大量安全软硬件，但由于养不起足够的安全运营人员导致“玩不转”、“用不好”；第三是

大量的中小企业在安全上有需求，但投资非常有限，他们需要的不是安全软硬件设备，而是安全的结果。

建议推广城市数字安全服务中心模式。建设城市安全能力应当以人为本，安全的未来一定是服务，只有通过持续的数据服务、分析服务、安全托管服务和专家服务来真正提高安全的能力，才能打造城市级的安全运营体系。此外，周鸿祎还提议组织城市数字安全服务中心优秀案例评选，围绕安全赋能、活动支撑、技术创新、人才培养、产业带动等方面，评估建设成效，发掘最佳实践，促进城市数字安全建设的模式优化。

（来源：环球网）

2、数字经济安全可持续发展亟须司法保障

巩富文

全国政协委员、农工党中央委员、陕西省高级人民法院副院长

数字经济科技创新具有更新快、迭代升级迅速等特点，对经济社会发展产生了技术、伦理和价值的多重冲击，亟需司法制度的保驾护航。

构建服务数字经济健康发展的司法保障制度，已是势在必行。巩富文建议，要确立以数字正义规制数字经济的司法价值观。

公平正义是司法的生命线和终极价值。在数字时代背景下，正义的内涵与外延也应当发生数字化迭代。要确立以科技向善为底层逻辑

的数字正义观，创设技术公平规则，实现数据正义、代码正义、算法正义，有效规制防范算法“黑箱”与“大数据杀熟”，保护公民个人数据隐私和合法权益，促进数字经济体现“以人为本”的价值导向。

同时，要促进数字经济与知识产权司法保护协调发展。妥善解决数字经济发展背景下更易受到损害的知识产权保护问题，既支持以信息数据为基础的新业态新模式新经济发展，又注重以个案裁判明确行为规则和边界，保持平台创新活力，遏制滥用市场垄断地位和不正当竞争的行为。

此外，要筑牢服务数字经济发展与安全的司法屏障，应当严格把握网络安全法、数据安全法等划定的涉及国家安全的数据安全红线，用好域外追责、刑事打击等规范跨境数据流动的司法武器，坚决保护我国享有自主知识产权的先进数字技术。

（来源：中国高新网）

3、推进数字经济融合发展，提升大湾区高质量发展水平

李民斌

全国政协委员、东亚银行联席行政总裁

随着大湾区建设进入新阶段，制度、经济、社会等各方面融通诉求愈加凸显。跨境理财通启动后，银行各类跨境金融产品也在加速上线。大湾区应整合当前条件，探索创新粤港澳三地数字经济合作机制、

合作模式，不断提升高质量发展水平，同时亦为全国提供数字经济跨境合作的鲜活经验。

对于数字化协同效应有待充分发挥、数据流通程度有待提升和数字经济融资支持有待加强三方面，李民斌提出具体建议如下：

一是加强发展数字经济的统筹协调力度。升级粤港信息化合作专责小组，建立覆盖粤港澳、由三地高层领导共同参与的大湾区数字经济发展委员会，成员包括政府官员、业界专家、学者等，强化跨部门、跨层级、跨区域的协同机制，制订大湾区数字经济发展规划、策略、重点领域，统筹三地数字经济发展事宜。同时建立统一的数字经济统计监测指标体系，为大湾区数字化发展提供决策参考。

二是推进跨境数据验证的运用。在粤澳跨境数据验证平台试运行的基础上，推动建立覆盖粤港澳三地的跨境数据验证平台。

三是完善数字经济的融资支持。一方面，建议完善大湾区数字经济融资体系，推动设立大湾区数字经济发展专项资金，带动社会资本投资。设立数字经济企业贷款补偿资金，提升对科技型中小企业的贷款贴息支持力度，支持商业银行与知识产权密集型产业园区开展战略性合作，扩大知识产权质押融资。

（来源：证券时报网）

4、数字经济是驱动产业高质量发展的关键力量

曲永义

全国政协委员、中国社会科学院工业经济研究所党委书记、副所长、研究员

我国经济发展进入新常态后，发展面临增长速度换挡期、结构调整阵痛期、前期刺激政策消化期“三期叠加”的复杂局面，由于全球地缘政治格局变化和新冠疫情冲击，发展环境发生了很大变化，我国数字经济驱动的产业高质量发展面临着重重困难，我国产业体系迈向现代化进程任重道远。

在产业创新层面我国需要持续加强全面自主创新体系建设，把数字经济发展作为推动产业高质量发展的内生动力，依靠数字创新中的数字关键核心技术自主创新，为数字经济驱动下的产业高质量发展提供核心动力和技术支撑。

他建议，当前需要瞄准我国产业发展的数字科技需求缺口，增强产业创新能力。

一是明确我国数字科技发展现状及与世界先进国家的差距，选择优先发展的关键技术群，瞄准传感器、量子信息、网络通信、集成电路、关键软件、大数据、人工智能、区块链、新材料等战略性前瞻性领域，发挥我国社会主义制度优势、新型举国体制优势、超大规模市场优势，提高数字技术基础研发能力。

二是按照产业高质量发展目标，预测技术发展趋势，形成“技术跟踪—技术预测—技术选择和规划—行动（技术开发和商业化）”的发展思路，集中突破硬性产业高质量发展的高端芯片、操作系统、工业软件、核心算法与框架等关键核心技术，加强通用处理器、云计算系统和软件关键技术一体化研发和跳跃式发展的“撒手锏”。

三是实施产业链强链补链行动，加强面向多元化应用场景的技术融合和产品创新，着力提升基础软硬件、核心电子元器件、关键基础材料和生产装备的供给水平，强化关键产品自给保障能力，完善5G、集成电路、新能源汽车、人工智能、工业互联网等重点产业供应链体系，提升产业链关键环节竞争力。

（来源：新浪科技）

（四）数据安全管理与个人信息保护

1、建议强化企业数据安全管理与评估

张金英

全国政协委员、天津市政协副主席

目前，企业数据安全评估受多部法律、法规以及地方管理条例等诸多约束和规范，企业要面对"多头监管"的复杂性现状；具体安全评估工作中，不同的数据有着差异化的保障内容和措施，其安全评估过程难以统一到一个标准化的评价体系；我国企业数据安全评估还面对一个市场化困境，国内第三方数据安全评估工作目前仍处于起步阶段，诸多核心问题亟待解决。

首先，应完善数据安全评估体系。应由工信部牵头，从企业、政府和评估单位三方需求出发，构建数据安全评估体系。一方面，考虑数据安全的定位、目标、法规、标准等内容，在概念层面构建多场景

‘综合评估模型’，以满足数据安全采集、安全传输、安全存储、安全处理、安全共享、安全交换及安全销毁等多领域、多应用需求；另一方面，通过系统调研，从科学性、有效性、精确性、适应性、现实性角度出发，给出数据安全评估‘参考指标体系’；同时，明确各项指标数据采集、核查和精度评定的技术要求，给出完整的数据安全评估‘操作技术要求’。

其次是推动数据安全合法评估。数据管理和评估的核心在于依据国家、行业的法律法规及标准要求，重点评估运营者及其他数据处理者关于数据安全的落实情况，包括个人信息保护情况、重要数据出境安全情况、网络安全审查情况、密码技术落实情况、机构人员的落实情况、制度建设情况、分类分级情况、数据安全保障措施落实情况，以及其他法律法规、政策文件和标准规范落实情况等。

同时，应突出数据安全风险防范。数据安全管理与评估需要以《中华人民共和国数据安全法》为根本出发点，以网络安全风险评估理论框架为准绳，其内容和指标都要以数据为核心对象，以发现数据安全风险为主要目的。由于数据是一类特殊的评估对象，具备动态性，数据在不同环境下的流动，面临的安全风险也有所不同。不能以某个标准为基础来设置评估项，也无需固化模式，应围绕被评估的特定数据所面临的威胁和脆弱点，综合开展风险评估，找出其在特定威胁环境下面临的风险。

最后，要明确数据安全管理要点。一是需要通过风险评估促进运营者落实数据分类分级制度体系建设和重点保护措施，做到重要数据和核心数据重点保护，明确保护对象范围，厘清保护责任和保护主体；二是需要通过风险评估找出可能导致重要数据失窃、泄露、破坏的安全隐患，降低重要数据一旦遭受攻击后可能带来的恶劣影响；三是需要通过风险评估促进数据安全防御体系的改进提升，达到"以评促建"。

（来源：网易号）

2、建议建立政府使用个人信息数据公开制度

周汉民

全国政协委员、上海市社会主义学院院长、上海中华职教社主任

近年来，我国陆续出台了相关法律，为守卫个人信息提供了法治保障，但在实践应用中，仍存在术语界定模糊、权属不清、监管滞后等短板。对此，周汉民建议进一步完善相关配套措施，优化细节，如建议建立政府使用个人信息数据公开制度，加大对违法行为的惩处力度，让个人信息保护法律真正落地生根。具体如下：

发布个人信息保护民商事指导性案例。由最高人民法院组织发布个人信息保护民商事指导性案例，分别发布有关个人信息概念界定方式、权属确认方法、个人信息保护底线等方面的指导性案例，为法官统一裁判标准、统一认定方法提供指引。在出台指导性案例后，最高法出台“个人信息保护法”司法解释，为此后修订完善“网络安全

法”“个人信息保护法”以及衔接《民法典》提供参考。

建立政府使用个人信息数据公开制度。出台“政府使用个人信息数据公开目录”，尤其在有关个人信息类型、数据要素市场以及使用方式等公开环节广泛听取社会公众意见，将公众对数据类型的需求强度纳入评判是否应使用个人信息乃至是否可进行交易流通的参考指标。另一方面，进一步加强个人信息流通的监管。

加大对违法行为的惩处力度。建立公民电子信息投诉制度，具体包括受理范围、处理流程以及投诉反馈制度。对保护公民个人电子信息确有过错的，按照过错程度责令整改和进行相应处罚，以企业为例，可考虑暂扣相关行政许可执照，以企业年、半年或季度营业收入的一定百分比分别罚款。若情节特别严重，应当移送有关部门，撤销营业所需行政许可。

（来源：新民晚报）

三、技术与市场

技术与市场方面，围绕数据加密、数据交易以及数据安全的投融资动态成为关注热点。技术方面，数据加密创新突破不断，隐私计算技术也进入快速发展阶段。行业方面，随着经济的复苏，数据要素市场的逻辑和规则更为清晰，数据要素流通标准体系逐步健全。此外，API 安全、数据安全基础设施管理平台、数据交易等方向也成为市场热点。投融资方面，据工程中心不完全统计，2023 年第一季度国内公开披露的数据安全投融资事件共有 11 起，其中炼石网络和观安信息两家厂商完成了过亿元的融资。

（一）技术趋势

1、清华浙大在量子计算破解 RSA 密码方面取得重要突破

关键词：量子计算　RSA 密码

在一项最新研究中，清华大学龙桂鲁、浙江大学王浩华等组成的团队创建了一种算法，仅用 10 个超导量子比特就实现了 48 位因式分解。该团队的最新实验表明，依靠整数因子化的公钥密码技术可能很快就会受到当今原始的 NISQ（含噪声中等规模）量子计算机的攻击。

据研究人员称，该算法是基于经典的 Schnorr 算法——使用格约化来分解整数，同时依靠量子近似优化算法（QAOA）来优化 Schnorr 算法中最耗时的部分，以提高因式分解的速度。

研究人员表示，“使用这种算法，我们已经成功地对整数 1961（11 位）、48567227（26 位）和 261980999226229（48 位）进行了因式分解，在超导量子处理器中分别使用了 3、5 和 10 个量子比特。对于 48 位的整数，261980999226229，我们也刷新了真正的量子设备中用一般方法算出的最大整数。”

使用这种算法的近期量子计算机可能能够处理更大的整数分解问题，可能打破广泛用于保护计算机数据和系统的 RSA-2048 加密方案。

（来源：“安全圈”公众号 ）

2、美国 NIST 推出物联网数据保护加密算法

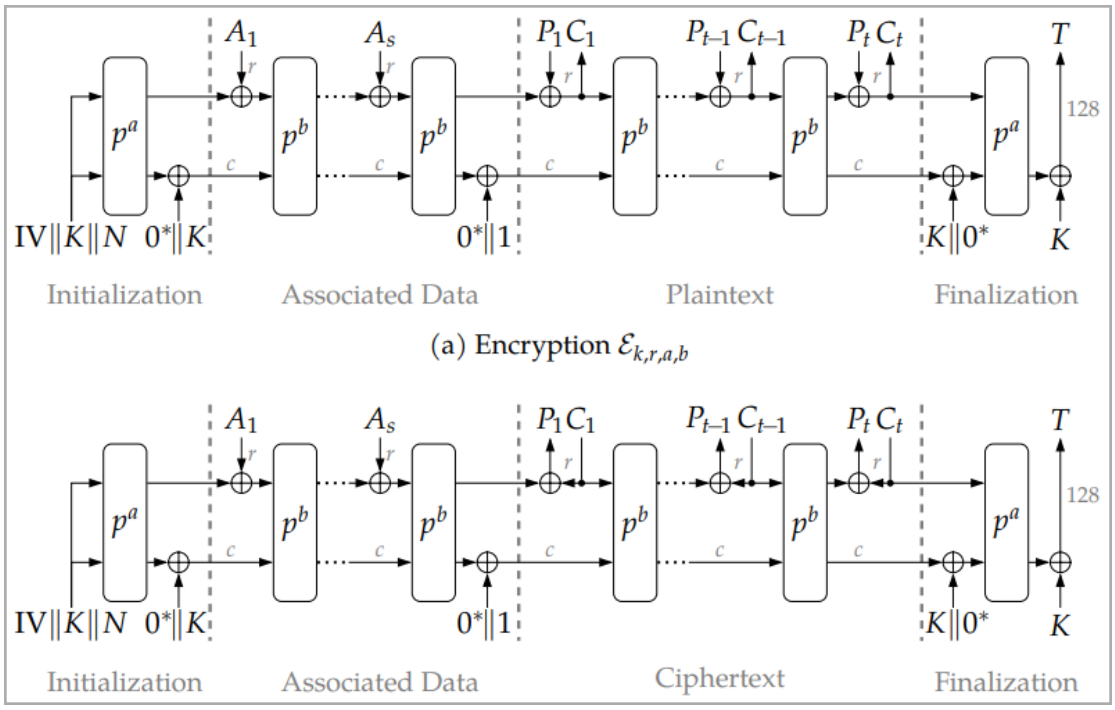
关键词：NIST ASCON

美国国家标准与技术研究院 (NIST) 近日宣布，名为 ASCON 的认证加密和散列算法系列将成为标准算法，用于轻量级密码学应用。该算法中标“轻量级密码学”计划，旨在寻找最佳算法来保护硬件资源有限的小型 IoT（物联网）设备。

小型物联网设备正变得越来越流行和无处不在，用于可穿戴技术、“智能家居”应用等。但是，它们仍然用于存储和处理敏感的个人信息，例如健康数据、财务详细信息等。也就是说，实施数据加密标准对于保护人们的数据至关重要。这些设备内部的薄弱芯片需要一种能够以极低的计算能力提供强大加密的算法。

ASCON 被选为提交给 NIST 的 57 项提案中的最佳提案，领先的密码学家进行了几轮安全分析，实施和基准测试结果，以及研讨会期间收到的反馈。整个项目从 2019 年开始，历时四年。

NIST 表示，所有 10 名入围者都表现出超越既定标准的卓越性能，而且没有引起安全问题，这使得最终选择变得非常困难。ASCON 最终被选为获胜者，因为它具有灵活性，包括七个系列、节能、在弱硬件上速度快，并且短消息开销低。



ASCON 的加密和解密操作模式 *(NIST)*

NIST 仍然推荐高级加密标准(AES)和 SHA-256 用于一般用途，但是这些不适用于资源有限的小型设备。

（来源：bleepingcomputer）

3、2023 年态势感知与安全运营十大技术趋势展望：面向数据安全的态势感知将成为新热点

关键词：态势感知 数据安全

伴随着数字化转型，数据在推动数字经济高速发展的同时，数据滥用、数据泄露等安全事件频繁发生，数据安全风险日益凸显。

国际著名咨询机构提出建议，用户必须在整个数据生命周期中规划和缓解管理风险，从而解决数据安全性，隐私性，信任与道德、数据所有权，数据恢复等一系列问题。2021 年 9 月 1 日，《中华人民共和国数据安全法》正式实施，数据安全上升到我国国家安全战略高度，并加速了数据安全体系建设。

在数据安全体系落地实践中，组织的数据安全风险迫切需要依赖系统化、产品化技术手段实现数据安全全生命周期管控，全面感知、分析、呈现数据安全风险的态势感知应运而生。

面向数据安全的态势感知围绕数据安全全生命周期管理，将数据安全技术、流程、产品和人有机的结合，融合数据资产梳理和发现、数据风险检测识别、数据风险集中分析、数据风险响应处置、数据风险态势呈现等能力，实现数据安全风险可感知、可溯源、可研判、可处置、可呈现，为数据安全运营提供基础。随着数据安全体系建设不断发展演进，面向数据安全的态势感知势将成为新热点，推动数据安全建设，助力数据安全治理 。

（来源：“数字安全助手”公众号）

4、使用神经网络，NIST 抗量子算法第四次被破解

关键词：Crystals - Kyber

近日，瑞典皇家理工学院研究团队发表论文，称其提出一种新的神经网络训练方法“递归学习”(Recursive Learning)，并通过周期性循环旋转信息，实现了对美国国家技术标准研究院(NIST)四种抗量子密码安全算法之一 Crystals - Kyber 最高 5 阶掩码的侧信道攻击，以高于 99%的概率从中恢复了信息位(message bit)。

Breaking a Fifth-Order Masked Implementation of CRYSTALS-Kyber by Copy-Paste

Elena Dubrova, Kalle Ngo, and Joel Gärtner

KTH Royal Institute of Technology, Stockholm, Sweden
{dubrova,kngo,jgartner}@kth.se

Abstract. CRYSTALS-Kyber has been selected by the NIST as a public-key encryption and key encapsulation mechanism to be standardized. It is also included in the NSA's suite of cryptographic algorithms recommended for national security systems. This makes it important to evaluate the resistance of CRYSTALS-Kyber's implementations to side-channel attacks. The unprotected and first-order masked software implementations have been already analysed. In this paper, we present deep learning-based message recovery attacks on the ω-order masked implementations of CRYSTALS-Kyber in ARM Cortex-M4 CPU for $\omega \leq 5$. The main contribution is a new neural network training method called *recursive learning*. In the attack on an ω-order masked implementation, we start training from an artificially constructed neural network M^{ω} whose weights are partly copied from a model $M^{\omega-1}$ trained on the $(\omega-1)$-order masked implementation, and then extended to one more share. Such a method allows us to train neural networks that can recover a message bit with the probability above 99% from high-order masked implementations.

Crystals - Kyber 已被 NIST 选为待标准化的公钥加密和密钥封装机制，同时也被纳入美国国家安全局(NSA)推荐用于国家安全系统的

密码算法套件，这使得评估 Crystals - Kyber 对侧信道攻击的抵抗能力变得非常重要：侧信道攻击利用从物理可测量的非主信道获得的信息，例如运行实现的设备的时序或功耗。

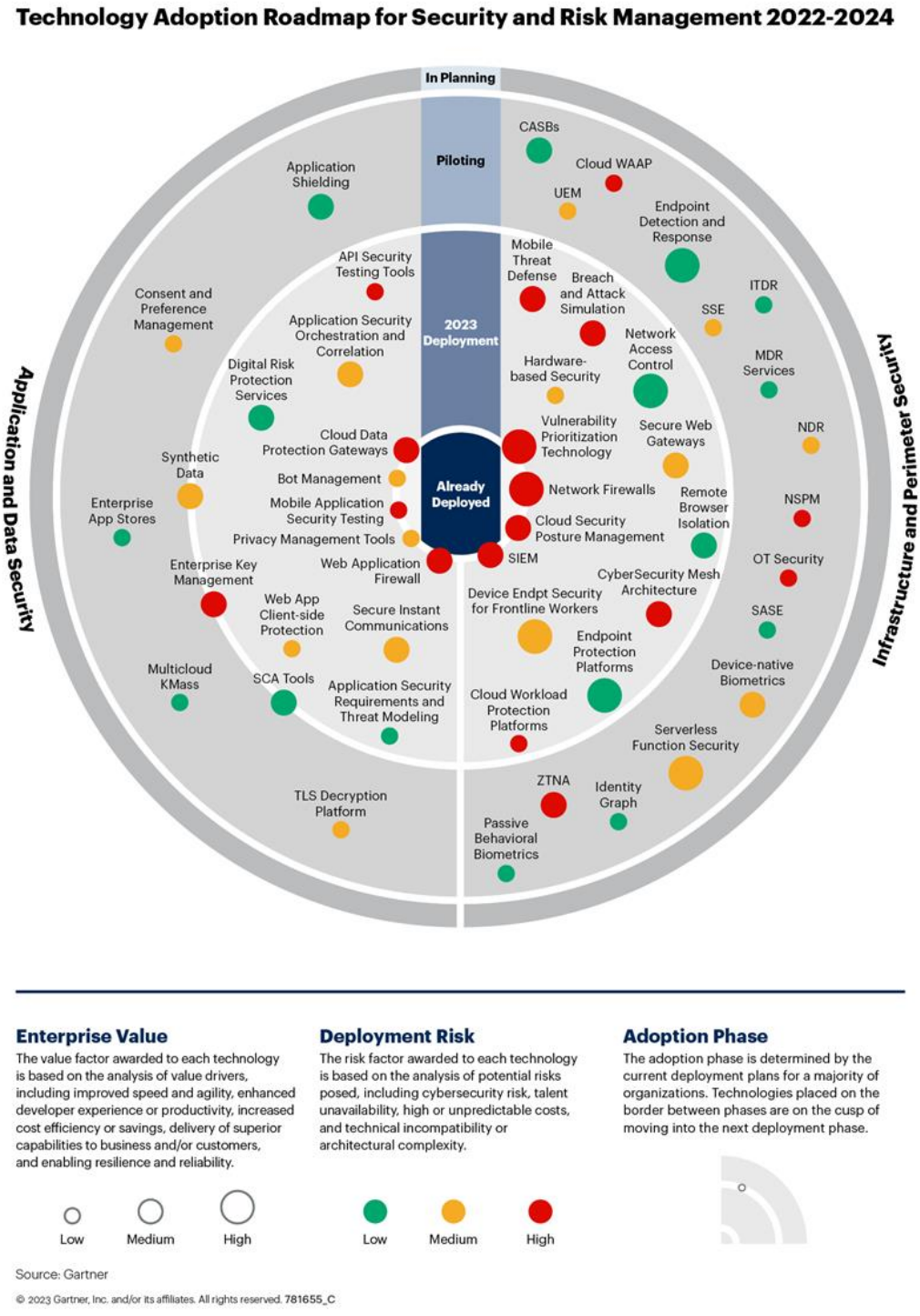
瑞典皇家科学院的研究团队开创性的提出一种使用递归学习的神经网络训练方法(Recursive Learning)，他们从人工构建神经网络开始训练，这一网络的权重是由可破解低阶的神经网络复制而来。其核心思想是将能破解低阶(ω-1)掩码的神经网络模型作为破解高阶(ω)掩码神经网络模型的基础，然后循环前进至更高阶。

（来源：安全内参）

5、Gartner 发布 2023 年安全和风险管理技术采用路线图

关键词：Gartner 安全和风险管理技术

Gartner 根据采用阶段、部署风险和企业价值，绘制了 2022 年至 2024 年间大型全球企业中 49 项安全相关技术的实施情况。安全和风险管理领导者可以使用此信息图来衡量他们的计划并根据主要趋势进行衡量。



从对技术采用路线图调查数据的分析中得出，**安全和风险管理(SRM)领导者正在近期部署应用程序和数据安全解决方案，并为基础设施和边界安全制定更长远的规划。**在我们调查涵盖的 49 项技术

中，51% 处于“部署中”，47% 处于“试验阶段”。与基础设施和边界安全技术相比，更多的应用程序和数据安全技术正在部署中，预计将在 2023 年初更快地被采用。只有一种基础设施和边界安全技术，网络防火墙，已经被大多数人部署 SRM 领导者，由于其成熟度水平。

（来源：安全内参）

6、隐私计算入选 2023 年十大科技趋势预测

关键词：隐私计算

近日，百度研究院发布“2023 年十大科技趋势预测”，隐私计算被列为十大科技趋势之一。分析认为，深度学习平台加大模型，构筑了坚实的产业智能化基座，会进一步加速产业智能化升级。数实融合，为技术底座的夯实提供了强大动力和广阔市场空间。隐私计算，成为支撑数据安全治理和数据要素市场化发展的重要基石。数据安全治理和数据要素市场化的重要性和紧迫性日渐上升，隐私计算技术进入快速发展阶段，金融、通信、医疗、互联网等领域有越来越多的机构开始自建隐私计算平台，应用场景不断拓展和深化，推进各家隐私计算平台的互联互通逐渐成为行业新趋势。在此背景下，横纵交织的可信数据流通网络初步呈现。可以预见，借助不断发展壮大的数据流通网络，未来几年隐私计算技术的应用场景将会不断推陈出新，隐私计算平台也会在多个行业成为支撑数据安全治理和数据要素市场化发展的重要基石，有助于塑造兼顾价值创造和安全可信的数据产业。

（来源：新华网）

7、九大热门 API 安全工具

关键词：API 安全

随着云计算和移动计算的快速普及，API 安全已经成为当下企业和互联网面临的最严峻的网络安全挑战之一，根据 Gartner 的研究，2022 年，超过九成 Web 应用程序遭到的攻击来自 API，而不是人类用户界面。

鉴于 API 安全问题的严重性和紧迫性，近年来 API 安全工具的数量正在快速增加。目前市场上有数十种 API 安全商业工具以及数百种免费或开源工具。

通常，根据 API 安全防护生命周期（上图），API 安全工具主要分为、检测、防护与响应、测试、发现、管理几大类；少数厂商宣称能提供完整覆盖 API 安全周期的平台工具，但如今最流行的 API 安全工具主要还是集中在“防护”、“测试”和“发现”三个环节。

CSOonline 基于全球用户和商业评论，评选出了目前九大热门顶级 API 安全工具：**APIsec、Astra、AppKnox、Cequence 统一 API 防护平台、Data Theorem API Secure、Salt Security API 保护平台、Noname Security、Smartbear ReadyAPI、Wallarm 端到端 API 安全平台。**

（来源：安全内参）

8、《数据安全风险治理成熟度评价模型》发布

关键词：数据安全风险治理成熟度

2023 年 1 月 5 日，在第二届数据安全治理峰会上，《数据安全风险治理成熟度评价模型》标准正式发布。《数据安全风险治理成熟度评价模型》将企业的数据安全风险治理按照风险治理的阶段分为 5 大能力域：分别是风险准则确立、风险要素识别、风险评估分析、风险处置解决、风险治理改进，并进一步细分成 15 个能力项。

评价模型的等级设置依据组织数据安全风险治理的覆盖范围、支撑力度进行划分。

第一级“初始级”指组织的数据安全风险治理主要依靠突发事件或临时需求驱动，具有明显的滞后性缺乏数据安全风险治理的目标、规划、依据、资源保障。

第二级“基础级”指组织的数据安全风险治理主要体现在个别业务活动或项目活动中，能主动识别法律法规与外部监管要求，使个别业务活动或项目活动中可以满足组织的数据安全保护与合规需求。

第三级“已定义级”指组织的数据安全风险治理主要体现在组织整体层面，考虑了法律法规和外部监管要求下，兼顾了组织内部发展需求，建立了覆盖数据安全风险识别、评估、处置、监控等标准化管理机制、技术和运营体系，能够保障组织数据安全风险治理工作的有序开展与规范化落地。

第四级“量化级”指在第三级的基础上对组织的数据安全风险治理效率、效果能量化分析和监控。

第五级“卓越级”指组织的数据安全风险治理成为行业标杆并推广至行业。

（来源：安全内参）

（二）标准动态

1、团体标准《数据安全合规评估方法》发布

1 月 19 日，深圳市信息服务业区块链协会发布《数据安全合规评估方法》团体标准，1 月 25 日起实施。《方法》规定了评估准备、审核、分析、评价等过程中各个环节的主要内容，从业务运营模式、数据处理主体、数据处理活动、管理措施及落实以及安全合规跟踪评估 5 各方面明确了评估内容和要求。

（来源：全国团体标准信息平台）

2、金融行业《证券期货业机构内部接口 账户管理》等 4 项标准发布

2 月 10 日，证监会发布《证券公司场外业务资金服务接口》《证券期货业机构内部接口 账户管理》《证券期货业机构内部接口 资讯数据》《证券期货业信息系统渗透测试指南》4 项金融行业标准，自公布之日起施行。

其中，《证券期货业机构内部接口 账户管理》和《证券期货业机构内部接口 资讯数据》2 项金融行业标准，分别规范了机构内部账户管理业务系统及资讯数据业务系统的数据接口，通过梳理核心业务模块之间的数据交互场景，对数据接口的数据字段、数据格式、数据交互协议提出了相关要求，对行业机构高效建立内部信息系统、实现跨平台资源共享具有指导意义。

（来源：证监会）

3、《信息安全技术 个人信息跨境传输认证要求》征求意见稿

3 月 16 日，全国信息安全标准化技术委员会秘书处针对国家标准《信息安全技术 个人信息跨境传输认证要求》征求意见稿面向社会广泛征求意见。

文件中明确了个人信息跨境传输认证基本原则，包括合法、正当、必要和诚信原则，公开、透明原则，信息质量保障原则，同等保护原则，责任明确原则以及自愿认证原则；从具有法律约束力的文件、组织管理两方面明确个人信息跨境传输基本要求，并明确了个人信息主体权利与个人信息处理者和境外接收方的责任义务。

（来源：全国信安标委）

4、多项网络安全、数据相关国家标准获批发布

根据 2023 年 3 月 17 日国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2023 年第 1 号），GB/T 42447-2023《信息安全技术 电信领域数据安全指南》等 12 项全国信息安全标准化技术委员会归口的网络安全标准以及其他与数据质量、数据采集相关的国家标准正式发布，具体内容包括：

序号	标准编号	标准名称	代替标准号	实施日期	归口部门
1	GB/T	信息技术 安全技术	GB/T	2023/	TC260（全国信息安

序号	标准编号	标准名称	代替标准号	实施日期	归口部门
	15843.3-2023	实体鉴别 第 3 部分：采用数字签名技术的机制	15843.3-2016	10/1	全标准化技术委员会）
2	GB/T 17902.1-2023	信息技术 安全技术带附录的数字签名 第 1 部分：概述	GB/T 17902.1-1999	2023/10/1	TC260（全国信息安全标准化技术委员会）
3	GB/T 20274.1-2023	信息安全技术 信息系统安全保障评估框架 第 1 部分：简介和一般模型	GB/T 20274.1-2006	2023/10/1	TC260（全国信息安全标准化技术委员会）
4	GB/T 21053-2023	信息安全技术 公钥基础设施 PKI 系统安全技术要求	GB/T 21053-2007	2023/10/1	TC260（全国信息安全标准化技术委员会）
5	GB/T 21054-2023	信息安全技术 公钥基础设施 PKI 系统安全测评方法	GB/T 21054-2007	2023/10/1	TC260（全国信息安全标准化技术委员会）
6	GB/T 32922-2023	信息安全技术 IPSec VPN 安全接入基本要求与实施指南	GB/T 32922-2016	2023/10/1	TC260（全国信息安全标准化技术委员会）
7	GB/T 33134-2023	信息安全技术 公共域名服务系统安全要求	_	2023/10/1	TC260（全国信息安全标准化技术委员会）
8	GB/T 42381.61-2023	数据质量 第 61 部分：数据质量管理：过程参考模型	_	2023/10/1	TC159（全国自动化系统与集成标准化技术委员会）
9	GB/T	数据质量 第 8 部分：	_	2023/	TC159（全国自动化

序号	标准编号	标准名称	代替标准号	实施日期	归口部门
	42381.8-2023	信息和数据质量：概念和测量		10/1	系统与集成标准化技术委员会）
10	GB/T 42383.2-2023	智能制造 网络协同设计 第 2 部分：软件接口和数据交互	_	2023/10/1	TC124（全国工业过程测量控制和自动化标准化技术委员会）
11	GB/T 42420-2023	智慧城市基础设施 突发公共卫生事件居住社区基础设施数据获取和报送规范	_	2023/10/1	TC28（全国信息技术标准化技术委员会）
12	GB/T 42446-2023	信息安全技术 网络安全从业人员能力基本要求	_	2023/10/1	TC260（全国信息安全标准化技术委员会）
13	GB/T 42447-2023	信息安全技术 电信领域数据安全指南	_	2023/10/1	
14	GB/T 42450-2023	信息技术 大数据 数据资源规划	_	2023/10/1	TC28（全国信息技术标准化技术委员会）
15	GB/T 42453-2023	信息安全技术 网络安全态势感知通用技术要求	_	2023/10/1	TC260（全国信息安全标准化技术委员会）
16	GB/T 42458-2023	智慧城市 突发公共卫生事件数据有效利用评估指南	_	2023/10/1	TC28（全国信息技术标准化技术委员会）
17	GB/T	信息安全技术 个人信	_	2023/	TC260（全国信息安

序号	标准编号	标准名称	代替标准号	实施日期	归口部门
	42460-2023	息去标识化效果评估指南		10/1	全标准化技术委员会）
18	GB/T 42461-2023	信息安全技术 网络安全服务成本度量指南	_	2023/10/1	TC260（全国信息安全标准化技术委员会）
19	GB/T 42505-2023	债券价格指标产品数据采集规范	_	2023/3/17	TC180（全国金融标准化技术委员会）

（来源：国家标准化管理委员会）

5、团体标准《数据资产价值与收益分配评价模型》（征求意见稿）

3 月 31 日，由青岛市大数据发展促进会批准制定、以青岛市大数据发展促进会为技术归口单位的团体标准《数据资产价值与收益分配评价模型》公开征求意见。据悉，该标准是全国首个“数据资产价值与收益分配评价模型”标准，规定了数据资产价值与收益分配评价模型的框架、维度及指标和评价过程。

（来源：全国团体标准信息平台）

（三）行业动态

1、IDC 发布中国 API 安全市场洞察报告

关键词：IDC　API 安全

IDC 认为，API 作为数据流转和使用的重要通道，承载着十分重要的责任。同时，API 的多样性、复杂性在不断增加，传统基于网络和主机边界安全的防护技术无法充分应对云计算和微服务技术下不断弹性部署的业务安全需要，许多用户在攻击事件发生后才意识到 API 风险。因此，API 资产的全面梳理和安全防护成为市场的迫切需求，API 的安全建设也成为企业数字化创新的基础保障。

IDC 将 API 安全定义为专门为保护 API 通信免受误用、滥用和漏洞利用而设计的解决方案，其所提供的功能包括 API 资产发现、验证和执行，动态和自适应的流量监测和模式分析、检测和阻止威胁，例如恶意软件、漏洞利用、代码注入、机器人流量、DDoS 攻击、欺诈和滥用等。目前 API 安全多以 API 安全网关、API 安全管理平台等产品形式进行交付。

IDC 认为，API 的安全防护市场在中国还处于初步发展阶段，产品和技术能力还需进一步加强。目前，国内众多网络安全厂商、数据安全厂商、云计算服务商、专业的 API 安全厂商纷纷布局 API 安全市场，且各个厂商结合自己的技术积累和行业优势推出了各具特色的产品和解决方案。

（来源：“IDC 咨询”公众号）

2、IDC 发布中国数据安全基础设施管理平台市场洞察报告

关键词：IDC　数据安全基础设施管理平台

IDC 定义下的数据安全基础设施管理平台是一个进行数据安全管理的底层平台，其从数据的发现与分类分级出发，是集成了数据合规治理、数据安全访问治理、敏感数据管理、数据防泄漏、数据加密、数据脱敏等多种数据安全产品能力的统一安全监测、管理、运营平台。该平台作为数据安全的基础设施防护底座，可不断集成并模块化多种数据安全能力。

IDC 认为，目前我国的数据安全基础设施管理平台市场方兴未艾，处于初步发展阶段，众多技术服务提供商已经意识到数据安全能力融合的大趋势，开始将其数据安全能力模块化、原子化，结合平台统一管理的优势，帮助用户从数据安全单点建设走向体系化建设。IDC 预测，未来，数据安全基础设施管理平台将逐步发展成为各组织数据安

全建设的基础设施，在最终用户的数据安全建设体系中起到“统一管理、指挥调度”的重要作用。

IDC 结合当前数据安全市场发展现状及未来趋势，为技术买家提供以下几点建议：

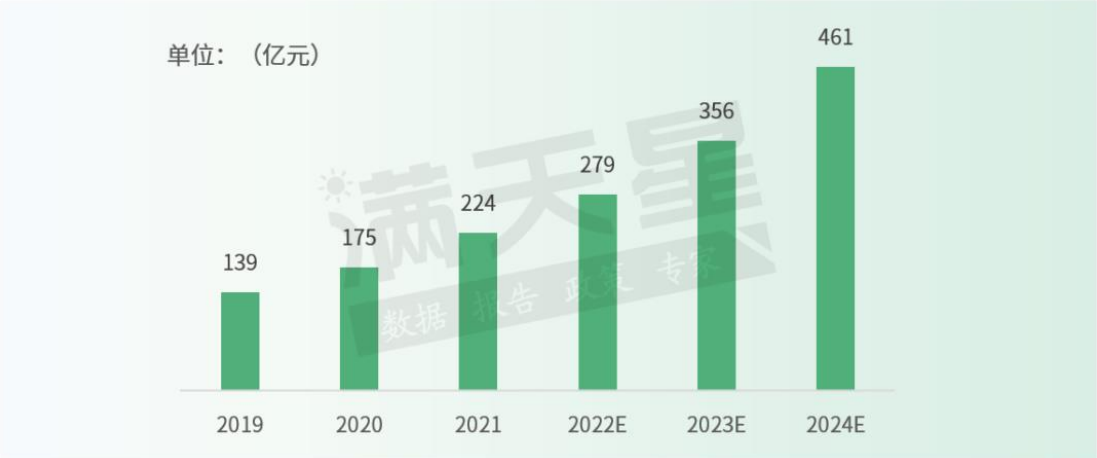
- 做好数据安全管理体系建设的顶层设计尤为重要。
- 数据资产发现和分类分级是基础能力。
- 数据安全基础设施管理平台需要与众多品牌的安全产品、能力组件对接联动，需要技术提供商能够通过更加便捷的工具、智能化的流程实现安全信息的汇聚与协同，降低产品对接的复杂度。
- 业务上云已经成为企业数字化转型的重要途经，如果企业计划或者已经拥抱云计算，则必然要考虑数据安全基础设施管理平台与云环境的适配。
- 企业应通过数据安全教育和培训加强员工数据安全保护意识，了解数据安全违规行为需要面临的法律责任，降低内部人为因素造成的数据风险。

（来源：安全内参）

3、2024 年中国数据库市场规模将达 461 亿元，本土厂商热度持续攀升

关键词：数据库

中国数据库管理系统市场保持快速增长趋势，**预计到 2024 年将达 461 亿元。**从技术架构来看，集中式关系型数据库仍然为当前市场的主流，但云数据库及分布式数据库也成为众多厂商研发的重点以及用户部署的新方向。



数据来源：赛迪顾问

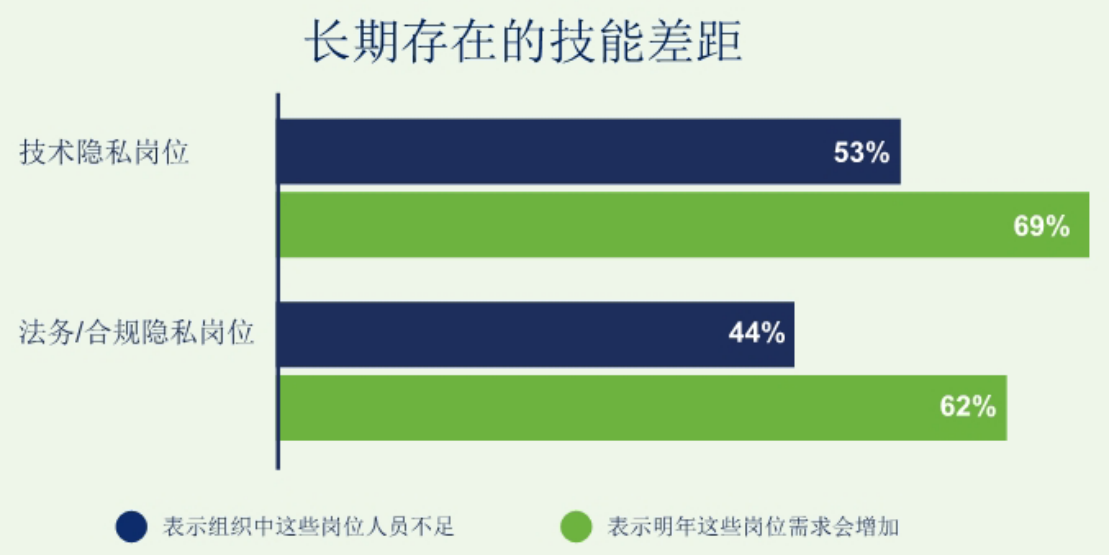
在未来的数据库选型过程中，有 53.8%的调研对象对于数据库产品的安全可靠性要求依然很高，其中大多为金融机构和政府。结合访谈结果来看，相关单位认为随着行业的发展，数据库产品的安全可靠性逐渐得以保证，未来最需要考虑的因素应该是不同产品之间的兼容性以及业务系统和数据的平滑、无损迁移。

（来源：安全内参）

4、ISACA 发布《2023 年度隐私实践研究报告》：人才短缺形势依然严峻

关键词：隐私 人才

1 月 28 日国际数据隐私日，ISACA 发布《2023 年度隐私实践研究报告》，报告显示坚持实施隐私设计的企业均大有收获，但由于隐私预算、人员配置和技能差距等问题，挑战依然严峻。ISACA 调查了全球 1890 位从事数据隐私工作或详细了解组织内的数据隐私功能的专业人员，报告总结了他们对隐私人员配置、组织结构、框架和政策、预算、培训和数据泄露的看法。



作为隐私行业的一大资源，隐私专业人员仍持续短缺，而明年对技术和法律/合规岗位的需求预计都将增加。技术隐私岗位仍然比法务/合规岗位更缺人。53% 的受访者表示所在组织在一定程度上或在很大程度上缺乏人手，法务/合规岗位缺人的仅占 44%。调查还发现，许多企业的隐私岗位没招到人（34% 受访者表示技术隐私岗位有空缺，27% 表示法务/合规岗位有空缺）。此外，与法务/合规岗位（62%）相比，技术隐私岗位（69%）在未来一年的需求更有可能增加。

调查结果显示，发生隐私事故最常见的原因是缺乏培训（49%）、数据泄露（42%）和不使用隐私设计（42%）。为了解决以上问题，

85% 的受访者表示所在组织为员工提供隐私意识培训，59%的受访者表示组织每年至少审查和修订一次隐私意识培训内容。衡量培训效果最常用的指标是完成培训的员工数量（65%）而非隐私事件的减少（54%），但 73%的受访者认为隐私培训对组织中的隐私意识产生了积极影响。

（来源：安全内参）

5、数据要素市场十大研判

关键词：数据要素

近日，上海数据交易所研究院对数据要素市场发展做了十大研判，内容如下：

研判一：数商破圈成为年度关键词。2023 年“数商”将破圈成为年度关键词，数商不仅将成为创新创业的重要赛道和政府支持相关产业的重要门类，也将成为彰显时代特色的代名词。

研判二：数据交易机构分化重组。仅在 2022 年，就有湖南、无锡、福建、郑州、苏州、广州、深圳、杭州等 8 地数据交易机构揭牌成立。2023 年新设数据交易场所将变得困难，既有的数据交易场所将围绕全国统一要素市场目标进行功能分化和结构重组，形成国家-区域-行业-场外的多层次数据要素市场体系。

研判三：场内交易发挥基础设施功能。2023 年将重点投入建设具有基础设施功能的数据交易场所，充分发挥场内交易的规范引导作用。

研判四：数据要素市场的逻辑和规则更为清晰。2023 年数据要素市场的逻辑和规则将更为清晰，各类主体将在更为清晰的市场逻辑、更为明确的流通交易规则和创新容错规则中，让数据交易不再“棘手”。

研判五：数据要素流通标准体系逐步健全。2023 年数据要素相关标准体系将逐步健全，形成分类齐全、层层递进的标准体系。

研判六：数据资产登记和入表走向现实。2023 年数据资产登记和入表将分两步走实现，全国统一的数据资产登记机构将依托数据交易机构建立，在确权登记的前提下推动数据资产入表的第二步，从而为更为广阔的数据资产应用服务提供基础。

研判七：数据产权结构性分置走向落地。2023 年将见证各层级各类制度和规范文件密集出台，推动数据产权结构性分置从理念走向落地。

研判八：公共数据授权运营激活场内交易。2023 年公共数据产品优先乃至应当进场交易将成为各地政策方向，通过公共数据产品激活场内交易，盘活带动整个数据要素市场。

研判九：数据跨境流通打通数字贸易外循环。2023 年数据跨境流通将实现更大发展，与东盟、“一带一路”国家之间的数据跨境流通将成为突破口，打通数字贸易外循环。

研判十：区块链+可信隐私计算赋能数据要素流通。2023 年区块链技术将被真正应用于数据交易系统中，可信隐私计算将继续迭代，为数据交易机构实现的更为广泛的数据要素流通提供安全可信的交付环境。

（来源：安全内参）

6、全国首个数据交易领域行业数据指数发布平台上线

1 月 13 日，全国首个数据交易领域的行业数据指数发布平台上线，广州数据交易所此次携手广东南方财经控股有限公司、广州航运交易所、中国联合网络通信有限公司广东省分公司、广东电网有限责任公司、广东省交易控股集团有限公司、广州交易集团有限公司、广州人才集团有限公司、全联集采水产品（广东）股份有限公司、北京百度网讯科技有限公司等 9 家数据商联合发布**80 余项行业数据指数**，涵盖财经金融、能源电力、交通旅游、智慧城市、船运船舶、医药健康、知识产权、公共资源、农业水产、人力管理等 **10 个行业**，将帮助市场了解行业运行情况和发展态势，洞悉未来市场发展趋势。

（来源：广东省政务服务数据管理局）

7、上海探路数据交易资产化，国内首个数据交易链问世

关键词：数据交易

3月3日，由大数据流通与交易技术国家工程实验室与上海数据交易所正式启动国内首个数据交易链的建设工作，这也是国内数据流通交易领域的新一代基础设施建设项目。

上海数据交易所数据交易系统建立了登记、挂牌、交易、交付、清结算和凭证发放六大业务环节，通过建立数据交易链，利用区块链存证和智能合约等技术使这些业务环节更加安全、高效和透明。区块链技术将数据交易系统的业务环节上链，大大提高数据交易的效率、安全性和透明度，使得交易参与主体互信互认，为各方从登记、确权到交付的交易全过程提供安全保障，体现交易所监管客观公正。

数据交易链的建设目标是构建一个技术自主可控、以平台生态完善为核心的联盟链技术体系，从而在数据产品流通交易中提供登记确权、存证防伪、数据溯源、交易监管等功能，进一步支撑数据安全合规高效流通使用，解决数据产品流通领域中权属确定、可信流通、分布式交易等多维度的难点。数据交易链将基于国内自主可控的开源区块链底链技术、智能合约开发技术、数据隐私保护技术、跨链信息互通技术等先进技术依据统筹设计、分期实施的策略建设而成。

（来源：个人信息与数据保护实务评论）

8、贵阳大数据交易所上线全国首个数据产品交易价格计算器

关键词：数据交易

为探索多样化、符合数据要素特性的定价模式和价格形成机制。近日，在国家发改委价格监测中心的指导下，贵阳大数据交易所上线全国首个数据产品交易价格计算器。

参考成熟要素市场价格机制，基于《数据产品成本评估指引 1.0》等规范，从价格形成原理出发，结合数据要素特性，该产品通过建立估价模型，以数据产品开发成本为基础，综合考量数据成本、数据质量、隐私含量等多重价值修正因子对于数据产品价格的影响，并基于预计的商业模式和市场规模，评估计算数据产品价格，为数据交易买卖双方议价提供参考，补全“报价—估价—议价”价格形成路径中的关键环节，促进数据要素高效配置、公平交易和自由流动。

（来源：贵阳大数据交易所）

9、2023 年网络安全十大发展趋势发布：涉及隐私计算、数据安全

关键词：隐私计算 数据安全

近日，中国计算机学会（CCF）计算机安全专委会中来自国家网络安全主管部门、高校、科研院所、大型央企、民营企业的委员投票评选出 2023 年网络安全十大发展趋势，其中与数据安全相关的部分如下。

趋势一、数据安全治理成为数字经济的基石：数据安全治理不仅是一系列技术应用或产品，更是包括组织构建、规范制定、技术支撑等要素共同完成数据安全建设的方法论。数据、模型算法、算力是数字经济发展的三大核心要素，其中数据是原材料。因此，发展数字经济、加快培育发展数据要素市场，必须把保障数据安全放在突出位置，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。在建立安全可控、弹性包容的数据要素治理制度后，需有效推动数据开发利用与数据安全的一体两翼平衡发展。鉴于此，夯实数据安全治理是促进以数据为关键要素的数字经济健康快速发展的基石。

趋势四、隐私计算技术得到产学研界共同关注：作为平衡数据流通与安全的重要工具，隐私计算成为数字经济的底层基础设施，为各行各业搭建坚实的数据应用基础。近年来，隐私计算产业快速增长，预计 2025 年国内市场规模将达百亿元，在巨大市场预期下，产学研界将更加关注隐私计算技术的新发展和产品应用的新场景。

趋势五、数据安全产业迎来高速增长：2023 年，《网络数据安全管理条例》有望正式出台。在政策法规和可操作性标准持续优化完善的背景下，在数据合规与企业数据保护的双重驱动下，数据安全产品和服务市场需求更加凸显，以数据为中心的安全投资将获得增长，数据安全产业的增速有望进一步加大。在下游需求及国家政策推动下，各行业对数据安全的投入占比将持续增长，尤其是政务数据管理和央企、国企在相关领域的投入增速将明显加大，有望带动网络安全市场在 2023 年实现一定程度的复苏。

（来源：中国工信产业网）

10、IDC：开源正在改写隐私计算商业逻辑

关键词：开源 隐私计算

2022 年下半年以来，在隐私计算领域，开源的趋势愈加显现。蚂蚁集团、翼方健数等相继推出隐私计算开源平台，开放群岛开源社区、FATE 开源社区、百度、腾讯云、京东科技五家企业机构共同发起了“隐私计算开源协同计划”，还有更多隐私计算开源平台获得融资，以及更多基于开源平台研发的隐私计算产品推出。

近日，IDC 发布《IDC Perspective:中国隐私计算开源市场洞察，2022》。报告通过调研中国市场上典型的在隐私计算领域进行开源实践的厂商、技术使用方以及尚未进行开源的隐私计算厂商，展现了 2022 年隐私计算在中国的开源实践以及未来的发展趋势。

IDC 经过研究发现，开源正在如下几个方面改变着该领域的商业逻辑：

（1）将隐私计算技术的门槛迅速降低——这一点正在动摇隐私计算领域商业逻辑的根本。

（2）改变隐私计算领域的人才供需状况。

（3）将催生更多数量的隐私计算产品的提供方出现，这将使得隐私计算赛道的竞争更加激烈。

（4）大量隐私计算产品的激烈竞争可能促使隐私计算产品价格迅速降低，从而进一步推动隐私计算领域的商业模式发生改变。

（5）新的行业格局与生态正在形成。

（6）在新的形势下，可能产生多种类型的隐私计算产品与服务提供商。与此对应，不同类型的提供商，在不同赛道上的致胜因素也将不同。

（来源：数据安全推进计划）

（四）投融资动态

1、炼石完成近亿元 A+轮融资

关键词：数据安全 A+轮

投资界 2 月 9 日消息，炼石宣布完成近亿元 A+轮融资，本轮融资由重庆科技成果转化基金独家投资，由清科资本担任独家财务顾问，

这是继安天科技、安云资本、国科嘉和、腾讯等多轮之后的新一轮投资。

随着本轮资金的引入，炼石将更深入研发迭代以“免改造”为创新特色的数据安全主平台，整合事前、事中、事后等多阶安全能力，深挖产品竞争力“护城河”，并布局“产品+服务”双平台战略，通过“服务拉动产品、产品固化服务”，实现对政企用户的持续价值输出。

（来源：news.pedaily.cn）

2、观安信息获 3 亿元战略投资，进入数据安全发展快车道

关键词：观安信息 数据安全 亿元级

2月3日，观安信息宣布完成近3亿元人民币的新一轮战略融资。本轮融资由上海国鑫创业投资有限公司（国鑫创投）以及国开制造业转型升级基金共同领投，卓戴投资跟投。

（来源：36 氪）

3、数据安全管理公司亿智云完成 2000 万 A 轮融资

关键词：数据安全管理 A 轮

亿智云完成 2000 万 A 轮融资，由雷石独家投资。亿智云是数据安全及服务的综合解决方案提供者，专注数据安全管理技术的新一代安全厂商，主要从事数据集成业务、IT 定制开发业务以及自有数据备份软件三块业务。在完成雷石独家投资的 A 轮融资后，亿智云将

加强对数影系列等产品的研发，提升多云、跨云、分布式的环境下对数据进行高效的保护、治理及备份能力。

（来源: donews）

4、腾讯投资企业级云数据安全厂商原点安全

关键词：原点安全　云数据安全管理

北京原点数安科技有限公司（以下简称“原点安全”）发生工商变更，新增广西腾讯创业投资有限公司为股东。同时，公司注册资本由约 890.56 万元增至约 1033.05 万元，增幅 16%。

公开资料显示，原点安全是一家企业级云数据安全（Cloud Data Security）产品服务提供商。公司成立于 2020 年 6 月，法定代表人为梁志勇，经营范围含人工智能、网络信息、通信领域内的技术开发、计算机系统服务、软件开发等。

（来源：news.cnstock）

5、日志易完成 C 轮融资，引领日志信创

关键词：日志数据分析 C 轮

国内领先的日志管理与分析平台开发商日志易完成了 C 轮融资，投资方为某知名产业投资基金。日志易成立于 2014 年，2021 年被工信部认证为国家级专精特新“小巨人”企业。公司拥有发明专利 23 项，外观专利 9 项。

日志易表示将在本轮融资后继续发力信创，进一步强化日志分析、智能运维、可观测性、数据治理以及威胁检测与响应等关键产品的核心自主知识产权研发，继续加强国内外渠道、销售及专业服务体系的建设。

（来源：news.sina）

6、大数据技术产品服务平台数字扁担完成近亿元 A 轮融资

关键词：大数据技术 A 轮

大数据技术产品服务平台数字扁担完成**近亿元 A 轮**融资，由浙报传媒控股集团旗下新干世业以及拱墅区国投联合领投。

据了解，本轮资金将主要用于基于数据编织技术的下一代数据科学平台的研发及市场化投入。

（来源：sohu.com）

7、网络安全技术初创「Drata」C 轮融资 2 亿美元

关键词：海外 C 轮

据外媒 CrunchBase 报道，总部位于圣地亚哥的网络安全技术初创「Drata」宣布筹集 2 亿美元的 C 轮资金，由 ICONIQ Growth 和 GGV Capital 联合领投。「Drata」构建了一款自动化平台，帮助企业达到安全合规方面的要求，确保企业遵守 GDPR 等法规。

（来源：36kr）

8、NsKnox 获得 1700 万美元战略融资

关键词：海外 战略投资

NsKnox 获得 1700 万美元战略融资，由 Link Ventures 和 Harel Insurance & Finance 领投，M12、Viola Ventures 和 Alon Cohen 参投。

NsKnox 是一个金融科技安全平台，旨在保护企业支付免受欺诈和数据操纵多种威胁。nsKnox 的解决方案利用了公司所谓的合作网络安全（CCS），将加密技术与来自多个组织的数据相结合。

（来源：tianyancha.com）

9、数据分析平台 BlockFenders 获得 150 万美元投资

关键词：海外 Pre-seed 轮

2 月 9 日，数据分析初创公司 BlockFenders 宣布由一系列机构投资者和天使投资者提供 150 万美元的融资以帮助他们解决当前问题。Blockfenders 总部位于帕洛阿尔托，由结交 20 年的朋友 Viraj Phanse 和 Niranjan Ingale 于 2022 年共同创立，旨在更轻松地安全地跨境交换数据。

（来源：viestories.com）

四、安全事件分析

2023 年第一季度，全球范围内数据安全威胁依旧不断，勒索软件、网络钓鱼、供应链攻击、人为错误等导致的数据被窃取或破坏的安全事件频发，对多国家、多行业、多领域造成了不同程度的影响；同时由于全球网络空间局部矛盾冲突不断，国家级网络攻击频次不断增加，关键信息基础设施所面临的数据安全形势日趋严峻，对国家安全造成严重威胁。

（一）数据安全领域执法力度持续加大，强监管进入常态化

各国持续加大数据安全的治理与执法强度，并加强针对大型互联网公司的数据安全审查与监管。1 月 5 日，法国数据保护机构对 Apple 处以 850 万美元罚款，原因是其在未征得用户同意的情况下收集用户数据用于定向广告；1 月 20 日，Meta 旗下 WhatsApp 因违规使用个人数据，违反了欧盟《通用数据保护条例》(GDPR)的规定，被爱尔兰数据保护委员会罚款 550 万欧元；2 月 8 日，韩国个人信息保护委员会对违反韩国《个人信息保护法》的 Meta 罚款 660 万韩元并要求其采取公开消息等整改措施。

放眼国内，全国在数据安全、个人信息保护等领域的执法工作持续发力增效，重大违法违规行为受到严厉打击，呈现出常态化监管的特点。2 月 10 日，因存在未经同意查询个人信息的违法违规行为，长银五八消费金融被罚款 75 万元；2 月 24 日，长沙一家信息科技公

司因未制定数据安全管理制度、未开展等级保护备案工作，用户隐私数据存在泄露风险，严重违反了《数据安全法》，被罚款 5 万元。

（二）地方政府成为热门网络攻击目标，政务部门数据泄露警钟长鸣

中央和地方政府系统中存储着大量有关公民活动的丰富信息，对于犯罪分子而言是极具吸引力的目标，同时，各类数字城市服务也为攻击者提供了更多入口。1 月 30 日，日本多个中央部门的电子邮件地址遭泄露，在暗网上遭售卖；2 月 10 日，因勒索软件攻击导致城市所有 IT 系统离线，敏感数据文件被窃取，奥克兰市宣布进入紧急状态；3 月 2 日，美国法警局遭遇勒索软件攻击，涉及执法敏感信息泄露；3 月 9 日，弗吉尼亚州韦恩斯伯勒市的官方网络门户网站受到 BianLian 勒索软件操作的破坏，350GB 的数据被窃取。

此外，政府机关普遍都缺乏明晰的数据安全战略与规划，没有定期进行风险评估并制定特定的安全策略，一旦遭遇数据威胁和攻击，很容易因此受到严重影响。1 月 31 日，因一个配置错误的亚马逊 AWS 服务器，美国交通安全管理局超过 150 万条涉恐禁飞人员和 25 万条“二级安检选中者”人员信息的禁飞名单被黑客在论坛公开泄露；2 月 26 日，美国国防部服务器因配置错误没有密码而暴露在外，3TB 敏感数据泄露，包含过去几年的大量内部军事电子邮件和敏感人员信息。这一系列触目惊心的安全事件给政务行业数据安全防护敲响了警钟。

（三）以汽车数据为核心的安全问题日益凸显，汽车数据安全事件频发

当下汽车行业正在进入数字化赋能的新时代，更多的汽车被赋予智能、互联的特性，越来越多的攻击者将攻击目标瞄准智能网联汽车、车企生产网络、运营网络和供应商网络。1 月 3 日，沃尔沃遭到勒索攻击，200GB 敏感数据以 2500 美元的价格在黑客论坛上出售；1 月 4 日，丰田、梅赛德斯、宝马等知名汽车品牌因存在 API 安全漏洞而暴露车主个人信息；1 月 18 日，日产汽车再曝数据泄露事件，或由第三方服务商配置错误所致，导致约 17998 名客户的信息受到影响；2 月 3 日，欧洲汽车经销商巨头 Arnold Clark 遭 Play 勒索软件团伙攻击，客户个人数据全部泄露；3 月 10 日，研究人员偶然发现了宝马意大利官方网站上托管的未受保护的环境(.env) 和.git 配置文件，意大利客户的数据遭到泄露。**事实上，除了用户个人隐私数据之外，随着数字化对汽车架构造成的颠覆性变革，智能网联汽车的数据安全问题也将与智慧交通、智慧城市等社会公共安全息息相关。**

（四）第三方供应商成为企业数据安全的薄弱环节，给相关组织带来巨大损失和风险

因第三方供应商造成的重大网络入侵和数据泄露事件层出不穷，犯罪分子越来越善于利用第三方为跳板从而立足于价值更高的目标。2 月 2 日，小米汽车“设计文件”因合作方对其下游供应商管理不善而

遭泄，供应商被罚 100 万元；2 月 20 日，因上游供应商遭到勒索软件攻击，全球最大的半导体制造设备和服务供应商 Applied Materials 损失超 17 亿元；2 月 23 日，澳大利亚零售商 The Good Guys 的客户数据在涉及第三方供应商 My Rewards 的安全漏洞中受到损害；3 月 9 日，美国电信巨头 AT&T 在供应商遭受黑客攻击后致 900 万客户数据泄露；3 月 16 日，LockBit 勒索软件团伙从 SpaceX 最大的零部件提供商 Max Industires 处窃取了 SpaceX 3000 张设计图纸。**据 IBM《2022 年数据泄露成本报告》研究发现，近五分之一的数据泄露是由供应链入侵造成的。总体而言，必要的持续监控和风险评估机制的缺乏，导致了第三方供应商安全风险的存在。**

（五）俄乌冲突仍在持续，针对关键基础设施的网络攻击引发大规模数据泄露

从 2022 年 2 月 24 日爆发的俄乌冲突到今天仍在持续，关键基础设施成为网络战的首选阵地，窃取其所承载的重要敏感数据是主要目标。1 月 31 日，IT Army of Ukraine（乌克兰 IT 军队）声称已经破坏了俄罗斯能源巨头 Gazprom 的基础设施，并获得了 1.5 GB 的档案数据；2 月 9 日，亲西方黑客组织“匿名者”从俄罗斯互联网服务提供商 Convex 处窃取了 128GB 数据，被盗文件包含情报部门 FSB（俄罗斯联邦安全局）进行的天罗地网监视活动的证据。**俄乌冲突进一步**

印证了，伴随着大规模数据泄露的网络攻击是现代军事行动的必要手段。

《数字安全观察》产品系列

- 每周动态：政策法规/行业动向/安全事件/技术趋势
- 深度分析：政策解读/行业洞察/市场预测/事件分析/技术前瞻/策略建议/国际智库精编
- 国防专刊：网空战略/力量建设/科装动态/空天态势
- 数据安全专刊：政策形势/安全事件/安全研究/大咖观点

总编辑：杜跃进

执行编辑：张义荣

本期编委：钟力、唐会芳、王雨薇、陈璐

如有反馈 邮件请至 nelab@360.cn、dipperresearch@360.cn