全球数据安全观察

总第 142 期 2023 年第 23 期

(2023.08.07-2023.08.20)

大数据协同安全技术国家工程研究中心

NERCBDS
大数据协同安全技术
国家工程研究中心

目录

政策形势

1、国务院关于进一步优化外商投资环境加大吸引外商投资力度的意见

8 月 13 日，国务院印发《关于进一步优化外商投资环境加大吸引外商投资力度的意见》,提出 6 方面 24 条政策措施。其中明确了要探索便利化的数据跨境流动安全管理机制，包括高效开展重要数据和个人信息出境安全评估，促进数据安全有序自由流动；支持试点探索形成可自由流动的一般数据清单，建设服务平台，提供数据跨境流动合规服务。

https://www.gov.cn/zhengce/content/202308/content_6898048.htm

2、网信办发布《人脸识别技术应用安全管理规定（试行）（征求意见稿）》

8 月 8 日，国家网信办就《人脸识别技术应用安全管理规定（试行）（征求意见稿）》公开征求意见。规定了人脸识别技术的使用原则、合法基础，并对该技术使用的场景、规范性要求等进行了明确。

http://www.cac.gov.cn/2023-08/08/c_1693064670537413.htm

3、上海市印发《立足数字经济新赛道推动数据要素产业创新发展行动方案（2023-2025 年）》

8 月 15 日，上海市人民政府办公厅印发《立足数字经济新赛道推动数据要素产业创新发展行动方案（2023-2025 年）》，着力建设具有国际影响力的数据要素配置枢纽节点和数据要素产业创新高地。方案提出强化数据安全保障，包括建立数据分类分级保护制度，制定重要数据目录；建立数据安全监测预警和应急处置机制；发展数据安全产业，推动数据识别、质量管控、血缘分析等技术创新，加快隐私计算、密码等产品研发和解决方案应用，培育数据安全规划咨询等第三方机构；创新可信流通服务，完善平台架构，打造低成本、高效率、可信赖的流通环境。

https://www.shanghai.gov.cn/nw12344/20230814/e946902bdcaf40e292602ac6e8818f61.html

4、《贵州省数据流通交易促进条例（草案）》（征求意见稿）发布

8 月 16 日，贵州省大数据发展管理局就《贵州省数据流通交易促进条例（草案）》公开征求意见。条例对数据交易场所建设和管理进行规定，并提出支持贵阳大数据交易所建设国家级数据交易所，突出其公共属性和自律合规监管功能，

面向和服务全国统一大市场，负责数据流通交易平台日常运营，实现与贵州公共资源网上交易大厅互联互通，推动与其他数据交易场所互联互通。同时，条例对数据授权使用、数据权益保护、收益分配、数据流通交易生态培育、安全保障等内容进行了规范。

https://dsj.guizhou.gov.cn/opinion/202308/tOpinion_14498.html

5、《信息安全技术 大数据服务安全能力要求》等国标发布

8 月 6 日，国家市场监督管理总局、国家标准化管理委员会发布 431 项推荐性国家标准和 2 项国家标准修改单，其中，包括全国信息安全标准化技术委员会归口的 4 项国家标准：《GB/T 35274-2023 信息安全技术 大数据服务安全能力要求》、《GB/T 42884-2023 信息安全技术 移动互联网应用程序（App）生命周期安全管理指南》、《GB/T 42888-2023 信息安全技术 机器学习算法安全评估规范》、《GB/Z 42885-2023 信息安全技术 网络安全信息共享指南》。

https://std.sacinfo.org.cn/gnoc/queryInfo?id=CD3E02C22A1721C5BF7E8DF7A2EF4996

6、《个人支付信息保护指引》发布

8 月 9 日，中国支付清算协会印发团体标准《T/PCAC:

0001-2023 个人支付信息保护指引》，对个人支付信息的分类分级、处理基本原则、安全框架、安全保护范围进行了规定，并提出了支付业务主体的基本要求、支付业务主体的管理要求、支付业务主体的人员要求、支付业务主体的系统要求、不同业务场景的保护要求。

https://www.pcac.org.cn/eportal/ui?pageId=607975&articleKey=618267&columnId=596609

7、印度通过《2023 年数字个人数据保护法案》

8 月 9 日，印度通过《2023 年数字个人数据保护法案》（The Digital Personal Data Protection Bill, 2023），对于科技公司如何处理用户数据作出规定。该法律将允许公司将部分用户数据转移到国外，同时赋予政府向公司寻求信息的权力，并指示联邦政府任命的数据保护委员会打击不当内容。此外，该法案还赋予政府豁免国家机构的权力，以及赋予用户更正或删除其个人数据的权利。对于违规行为，印度政府可处以最高 25 亿卢比（约合 3000 万美元）的罚款。

http://www.globaltechmap.com/document/view?id=36876

技术、产品与市场

1、谷歌推出首个抗量子硬件密钥

谷歌 8 月 16 日宣布推出首个开源的抗量子（量子弹性）FIDO2 安全密钥，该产品是谷歌 OpenSK 安全密钥计划的一部分。

谷歌研究人员 Elie Bursztein 和 Fabian Kaczmarczyck 表示："该密钥的开源硬件优化实现使用了一种新颖的 ECC/Dilithium 混合签名模式，该模式受益于 ECC 面对常规攻击的安全性以及 Dilithium 抵御量子攻击的弹性。"

抗量子硬件密钥的问世是网络安全业界推广和普及抗量子加密算法的一次重大突破。与 Chrome 的混合机制（X25519 和 Kyber-768 的组合）类似，谷歌提出的 FIDO2 安全密钥实现是椭圆曲线数字签名算法（ECDSA）和最近标准化的抗量子签名算法 Dilithium 的混合。

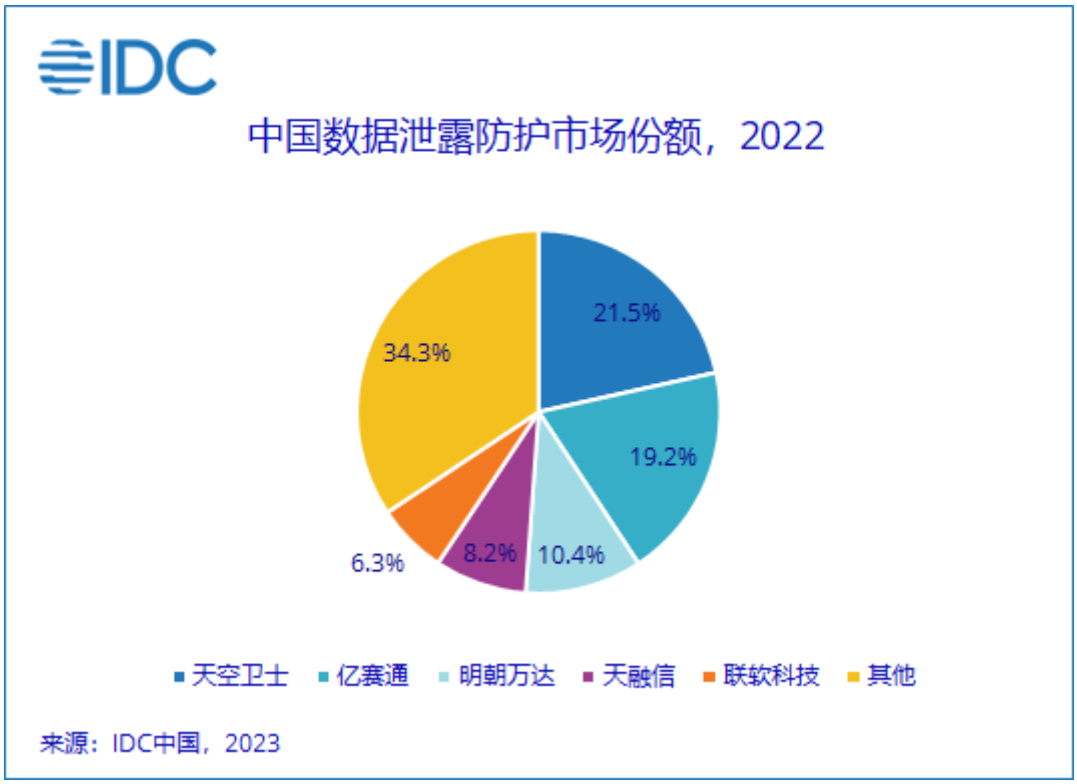
https://www.secrss.com/articles/57876

2、IDC：2022 年中国数据泄露防护市场规模达到 1.31 亿美元

2023 年 8 月 14 日，IDC **发布了《中国数据泄露防护市场份额，2022》报告**，报告针对 2022 中国数据泄露防护市场

的规模、增长速度、主要玩家、市场与技术的发展趋势等内容进行了详细研究。**IDC 数据显示，中国数据泄露防护市场在 2022 年实现了 4.8%的同比增长，规模达到 1.31 亿美元。**

专业数据安全技术提供商如天空卫士、亿赛通、明朝万达继续主导市场。报告指出，未来趋势包括整合云计算和移动设备支持、强化机器学习和人工智能分析、强调法规合规性、数据分类和标识改进、强化实时监控和响应能力。IDC 建议技术供应商提供更细致的数据保护功能以满足企业日益增长的数据安全和合规性需求。



https://mp.weixin.qq.com/s/2aWcz5MmAtc_XNF63cUmaA

3、研究：数据泄露现在是网络勒索的首选策略

据 Akamai 的数据显示，与 2022 年第一季度和 2023 年第一季度相比，过去六个月中 0-day 和 1-day 漏洞的滥用导致受害者数量增加了 143%。

报告还发现，勒索软件组织越来越多地以文件泄露、未经授权提取或传输敏感信息为目标，这已成为勒索的主要来源。这种新策略表明文件备份解决方案不再是防范勒索软件的充分策略。

Akamai 企业安全高级副总裁兼总经理 Pavel Gurvich 表示："勒索软件攻击背后的对手不断发展其技术和策略，通过泄露关键和敏感信息来攻击组织的核心。组织必须了解对手部署的技术和工具，以保护其关键资产、保持对品牌的信任并确保业务连续性，这一点至关重要。"

https://www.helpnetsecurity.com/2023/08/09/ransomware-groups-extortion-source/?web_view=true

4、研究：37%第三方应用存在高风险权限

据 Abnormal Security 称，自今年年初以来，电子邮件攻击的复杂性和数量均有所增加。

2023 年上半年（1 月至 6 月），集成的第三方应用程序数量持续增加，在此期间，Abnormal 观察到商业电子邮件泄

露 (BEC) 和供应商电子邮件泄露（VEC）攻击总体有所增加。

Abnormal 的研究显示，平均每个组织将 379 个第三方应用程序与电子邮件集成，这个数据自 2020 年以来增加了 128%。对于拥有 30,000 多名员工的大型企业，集成的第三方应用程序数量平均飙升至 3,973 个。其中包括用于协作、生产力、开发、社交网络、安全等的应用程序。在集成的第三方应用程序中，37% 的应用程序具有高风险权限，例如创建和删除电子邮件或用户的能力，甚至重置用户密码的能力。

https://www.helpnetsecurity.com/2023/08/10/third-party-applications-risk/?web_view=true

业界观点

1、王延川等：通用人工智能的价值、创新方向与风险防范

通用人工智能的发展对提高社会生产力水平、实现推进国家治理体系与治理能力现代化、增强国际竞争力以及维护国家安全具有重要意义。

通用人工智能是一把“双刃剑”，在促进经济效益和社会进步的同时，也会诱发技术滥用风险，给经济安全、社会安全等带来挑战。发展通用人工智能应正确处理创新与安全之间的关系，在营造良好的创新生态的同时注意防范其中的各种风险。

完善指南、法规和伦理等治理规范体系，引导通用人工智能规范发展。坚持“科技向善”的行为准则，通过制定全国统一的人工智能技术规范指南，明确从业人员的行为规范，引导通用人工智能技术规范发展。完善通用人工智能在应用过程中的各项法律法规，充分保护个人信息安全、隐私安全，防止算法歧视、算法偏见扰乱正常的社会生活秩序。完善通用人工智能伦理规范，要求通用人工智能的设计者、开发者、使用者必须遵守基本的伦理规范和行为规范。通过完善自上而下的治理规范体系，引导通用人工智能健康持续发展。

构建以国家监管为主导的多元共治监管体系，实现对整

个产业生态的可持续性动态监管。通用人工智能技术更迭迅速，场景应用多元性突出，仅依靠法律法规和安全技术革新难以跟上它的发展步伐。建议通过建立国家级统一的监管机构统筹通用人工智能的各项监管举措，明确各级部门的监管职能。在此基础上，探索建立以行业监管、企业自治、社会监督为协同的多元共治体系，回应通用人工智能技术迭代以及场景更新所带来的各种新风险和新挑战，充分保障社会公共利益和国家安全。

加快人工智能安全关键技术研发，提升抵御通用人工智能风险的能力。人工智能技术安全涉及人工智能技术自身的安全与人工智能技术应用安全两个方面：一方面，通过隐私计算、算法攻防、深度防伪等技术的研发提高通用人工智能自身防范技术安全漏洞的能力，开发人工智能生成内容技术监测系统，提升通用人工智能自我纠偏能力；另一方面，通过研发人工智能对抗技术，以“杀毒软件”等形式为用户端提供模型安全性量化测评以及安全性提升服务，增强人工智能技术应用的安全性，有效抵御恶意入侵行为。建立禁止问题库，对用户询问的具有风险的问题导流至客服和网络监管部门。完善规范体系、构建以国家监管为主导的多元共治监管体系，织密通用人工智能安全网。

https://mp.weixin.qq.com/s/jbGBM5hJziXmAbAEw_u-iQ

2、李庆霞等：共建数据网络安全环境 推动数字经济可持续发展

数字经济的发展离不开数据安全的保护，加快推动数字经济可持续发展，必须维护和保障好数据安全和网络安全，加快提升数字技术核心技术的研发和网络监管能力，共建数据安全和网络安全新态势，为数字经济的发展保驾护航。

实现高质量数据治理。必须坚持改革创新、系统谋划，以维护国家数据安全、保护个人信息和商业秘密为前提，以促进数据合规高效流通使用、赋能实体经济为主线，以数据产权、流通交易、收益分配、安全治理为重点，推动各项意见建议落实落地，大力提升数据要素配置的整体性、系统性、协同性、融合性。同时，优化各相关管理部门的数据治理分工协作，全方位应对和解决好数字经济发展中遇到的数据与网络安全问题，维护公平公正的数据交易市场秩序，优化网络安全行业发展环境，全面提升数据和网络安全保护水平，为推动高质量发展、推进中国式现代化提供有力数字支撑。

坚持数据安全与发展并重。以国家安全、公共安全以及个人隐私安全为底线，合理把握数据应用开放的界限，促进数据资源的流动和利用，更好实现数据要素价值。在大力提升数字技术与经济发展的适配度的同时，必须加强对数据全生命周期安全的维护和保障，强化对国家机密、商业秘密和

个人信息等数据的保护，避免造成信息泄露和黑客入侵等网络安全问题。同时，在国家层面上也要加强对重要数据出入境安全管理，强化对网络安全和信息安全的风险评估机制，定期对相关信息材料和网络安全进行排查和防护，最终达到捍卫数据安全和网络安全的目的。

突破数据安全领域关键核心技术。信息领域关键核心技术是网络安全和信息化工作的“命门”，关键核心技术受制于人势必失去发展主动权、削弱发展安全性，只有突破关键核心技术，才能从根本上保障网络安全、经济安全、国家安全。因此，走好自主创新道路，持之以恒突破关键核心技术，是保障数据与网络安全的关键所在，也是保障依法管网、依法办网、依法上网的关键所在，能够从根本上筑牢国家网络安全屏障，为提升网络治理体系和治理能力现代化水平提供坚实的技术支撑。

https://mp.weixin.qq.com/s/njqPgDOiNHIh9_OyZmDFdg

3、冯涛：加快数据安全治理体系构建刻不容缓

当前，数据安全面临诸多挑战。数据安全治理已成为贯彻落实总体国家安全观、守住数据要素流通交易红线和底线、保障企业数字化转型的重要保证。

随着数据作为基础性战略资源的地位不断凸显，数据安

全治理体系缺失已成为制约大数据发展的短板之一；数据安全法律法规滞后于数据业务发展，难以保障各项制度措施落地；此外，当前我国市场驱动下的数据安全技术研发滞后于业务发展，二者之间发展不平衡。

对此，冯涛建议：

首先，在国家层面，加快数据安全治理体系的顶层设计，为各行各业的数据安全治理提供指导。其次，要逐步完善数据安全监管机制，结合数据业务特点，分类实行相应的监管规则和标准。再次，还要加快出台重要数据保护、数据流通等相关配套规章制度，逐步完善数据安全法律法规体系，充分发挥行业协会力量，加快完善互联网、能源、交通、教育等行业管理要求和标准制定，更加全面地保障国家安全在各行业、各领域有法可依。最后，在行业层面，一要加大产业投入，明确数据安全在各项投资中的占比，政府、国企、民企等主体协同配合，激发数据安全核心技术攻关的内生动力，撬动全社会资源优化、高效配置；二要在国家课题和项目中，从项目数量和资金方面增加对工业控制芯片、工业控制系统等关键技术研发的投入，着力解决关键基础技术的“卡脖子”问题；三要通过政府部门、科研机构、高等院校、企业等多方主体联合培养、建立数据安全试验基地等手段，培育全方位、多层次的复合型数据安全优秀人才。

http://www.npc.gov.cn/npc/c30834/202308/1d6251398b0742ab8c6897440c8580be.shtml

4、吴国舫等：证券期货业数据出境监管模式探索与研究

证券期货行业数据出境主要集中在出境开展业务、出境经营管理以及出境监管与司法诉讼等三个方面。通过对行业数据出境场景梳理与分析，发现行业数据出境需求主要集中在交易、资讯、研报、客户信息、集团信息共享等几个方面，从数据特点来看，跨境数据普遍具有行业特色，从专业性上给数据出境的评估及后续监管带来了一定难度，为了更好地促进行业的双向开放，在整体行业数据出境监管设计上建议遵循如下五点原则。

1) 构建数据出境流动治理体系，兼顾安全性和流动性之间的平衡；
2) 配套出台证券期货业数据出境流动规制，保障数据出境的安全性和可操作性；
3) 构建证券期货业数据出境流动监管体系，提升跨境数据监管的协同性和有效性；
4) 完善证券期货业数据出境流动安全评估体系，进行数据出境试点，平衡数据出境的审慎性和灵活性
5) 构建以尊重为基础的证券期货业数据出境合作共建

新模式。

为了能在《数据出境安全评估办法》的框架下，合规且高效落地数据出境评估流程，建议探索行业监管部门主导的行业数据出境监管路径。

（一）落地证券期货业数据出境管理规章制度

建议证券期货业由证监会牵头与网信办申请获得证券期货业数据出境评估及监管的授权，授权应包括以下事项：授权开始的时间及有效期；授权进行数据出境评估的数据范围，如证券期货业数据等；授权方式，包括全权授权与部分授权。全权授权指网信办将行业数据出境评估职责全部授权予证监会，不参与评估工作；部分授权指行业数据出境评估工作由证监会主导，但国家网信办仍将参与评估工作。同时参照网信办颁布的《数据出境安全评估办法》，落地行业数据出境管理规章制度。

（二）证券期货业数据出境监管权责

建议构建证监会行政监管、证券期货业协会自律监管、证券期货业从业公司自查，以及数据接收者配合、协助相结合的法律规制体系。

在行政监管方面，构建由证监会统筹、派出机构落实的行政监管机制。当前，行业归口监管是我国数据出境流动的基本体制，证监会及其派出机构作为证券期货业数据出境监

管主体，负责证券期货业数据出境管理办法制定、数据出境评估、审查、监管及评价等工作。其中证监会对数据出境进行统筹管理，证监会各地派出机构负责所辖区域的具体落实与管理。

在行业自律监管方面，构建证券期货业协会等自律组织参与安全评估的合作机制，细化数据出境管理自律秩序。作为国家行政监管的重要补充，证券行业协会、交易所、中国证券登记结算有限公司在证券期货业数据出境监管中必将发挥重要的作用。构建证券期货业数据出境管理秩序的关键要素就是对数据出境流动的合规与安全性进行评估，在这方面我国可借鉴美国经验，引入第三方机构评估证券期货业数据出境安全水平，并及时从以下方面规范第三方评估市场。第一，对评估机构进行评估能力、评估资质的认证；第二，监督管理第三方评估机构评估的形式、过程及方式；第三，明确第三方评估机构失职或造成损失的责任。引入第三方评估机构并规范其运作方式，以此提升数据出境流动的评估水平。行业自律组织可利用自身优势，广泛参与并组织对第三方评估机构资格认定规范的制定，并在证监会的领导下，组织第三方机构对证券期货业跨境流动进行安全评估，以控制和规避数据出境流动合规及安全等风险。

在证券期货业数据处理者的自觉监管方面，应明确证券

期货业数据控制主体在国家安全、数据保护等方面的自律自查责任。规范证券期货业数据出境流动，除了完善立法和加强公权力监管及合理发挥自律组织作用之外，证券、期货、基金公司作为证券期货业数据的主要收集者和处理者，同样也产生了重要影响。建议采用“问责制”原则，各证券、期货、基金公司应根据自身实际情况确定证券期货业数据保障义务，并通过行业规章及公司制度加以具体落实。证券、期货、基金公司应当充分考虑如下内容，获取数据的途径是否合法合规；处理数据时是否保障数据的真实性和安全性；是否采取了足够的安全保障措施审慎保管掌握的数据；数据出境流动时是否保障了数据主体的知情权；数据接收国的法律能否做到对跨境流动的数据进行安全保障；被侵权的有力救济措施等。相较于处罚、救济等事后监管行为，风险事先预防实施成本更低，效果更明显。在此方面可以借鉴 CBPRs（跨境隐私规则体系）尝试设立激励机制，并将自评估作为一项评价指标纳入行业机构诚信评价体系，鼓励证券、期货、基金公司自评估，并定期向社会公布评估报告。

在数据接收方的监管方面，应遵从我国及数据接收所在国数据出境相关规制要求。数据接收方对接收到的跨境数据具有保护义务，应对接收到的数据进行严格控制管理，保证所接收的数据只用于协议约定的使用目的，不能侵害相关数

据主体的权利。应对接收的数据内容按照数据安全等级进行分级管理，对重要和敏感数据进行加密存储。当存在数据被非法使用时，数据接收方有义务配合数据输出机构进行追责。

数据接收方应遵守归属地法规，同时严格按照和数据处理者签署的协议处理数据，必须保证数据处理相关人员能够遵守有关数据保密的要求，并在数据安全、数据泄露、数据保护影响评估等方面对数据控制者提供协助。如果没有数据控制者的同意，数据接收者不得将跨境数据传输给第三方。经过数据控制者授权后，数据接收者可以将跨境数据传输给第三方，如果第三方发生了变化，数据接受者有义务及时告知数据控制者，数据控制者有权提出反对。数据接受者对第三方的数据处理活动完全负责，有义务将数据保护的要求施加给第三方。数据接收者在数据处理服务终止时，应当删除相应数据，除非根据法律要求必须保留这些数据。

https://k.sina.com.cn/article_7072825535_1a592c0bf00101520u.html

5、唐林垚：以技术手段破解数据合规难题

数据合规的前沿技术风险包括三个方面：

前端风险在于诱发人机对抗。技术手段下数据合规具有“白盒特性”，各参与方都可以直接获取完整的技术参数，恶

意攻击者同样可以利用该特性伪装成诚实参与方窃取运算结果、扭曲模型训练、破解可信环境或生成恶意低代码。参与方自愿提供数据、消耗算力参与数据合规实践，其具有强烈的自利动机，轻则通过参与获得技术使用权，重则掠夺中间数据和源头数据。依据危害性由低到高的顺序，将数据合规的参与方划分成三种类型。此种划分方式表明，随着利益需求的不断变化，各参与方的角色定位也可能发生改变。

中端风险在于加剧算法歧视。算法歧视主要源于数据集偏差或数据缺陷，在数据合规场景中，不同来源数据间的强搭和错配可能对联合数据造成冲击与扰乱，使算法歧视规模性放大。除了数据投毒等极端手段，诚实但好奇参与方的数据输入因数据梯度同其他参与方相差过大，也可能间接导致模型被“污染”，输出歧视性结果。单次歧视的即时危害虽不易被察觉，却足以在更长时间维度和更长数据链条上产生积累式影响。例如，当不同学校的毕业生数据被用于训练招聘筛选系统，或者当男性占绝对多数的 IT 行业数据和其他行业数据被共同用于训练升职评价系统时，同身份紧密捆绑的群体歧视将借由算法“共训”之名，从数据向模型蔓延。

后端风险在于催生逆向淘汰。在各类促进数据合规的技术大规模部署前，面对受众，智能应用被限制在各自为政的领域，彼此之间没有交流与协作，更多的是算法间的良性循

环，即效率高、服务好、安全稳定的智能应用将获得更高市场份额，榨取用户剩余的智能应用将面临被淘汰或整改的命运，因严重违法违规收集使用个人信息而被强制下架的各类APP即为典型事例。由于披上了“合规”的外衣，数据合规科技可能逐渐导致“算法趋同”，在技术黑箱的掩护之下，过去算法间的“朝上竞争”极有可能向“逐底竞争”转变。对数据规整性要求不高、通信成本更低、算法可解释性匮乏的智能应用，或将随着技术手段下数据合规的不断发展，逆向淘汰相对保守的传统智能应用。

基于此，破解数据合规的应对措施包括:

为应对前端风险，应引入声誉概念作为衡量参与方信任度的核心指标。多权重主观逻辑模型使基于声誉的可信赖客户端之间的“朝上竞争”成为可能，配合区块链技术的不可篡改特性，分布式信誉管理将成为现实。例如，主导方可围绕深度强化学习设计激励策略，在开源分布式特殊场景中推行资源“按劳分配”，以达到边缘节点的最佳训练水平；利用区块链技术跟踪全局模型更新，对积极贡献用户给予丰厚奖励，实现局部模型的更高稳定性。此外，契约理论可被用于各参与方算力投入和模型质量的衡量。不过，技术互嵌的解决方案有时也存在相互掣肘，技术方需“量力而行”。例如，区块链技术的公共账本特性存在通信延迟、数据吞吐量大等问题，

必然对通信设备、服务器带宽以及主机算力等提出更高要求。为此，可通过对通信成本和模型准确性之间进行表征的多节次方程式对二者的权衡取舍予以指导。

为应对中端风险，应构建数据清洗过程适用的缺省性数据筛选机制。避免算法歧视“群体化”需要深入数据处理的社会性聚合机制，尤其需拷问作为多方安全计算、联邦学习和低代码参与方的自身禀赋、行业特点和地域限制在何种程度上影响了数据样本的生成。无论如何清洗，来源于同一主体的数据通常会被打上难以察觉的烙印，具有隐性的身份化表征，在无形之中限定了数据合规的应用格局。不同数据间集体身份在数据合规实践中相互排斥和博弈越明显，得出的运算结果、训练出的公共模型和成型的低代码模块就越有可能产生歧视。简言之，原本稀松平常的数据，可能由于同其他非适配数据的联合，导致数据池难以自洽。在数据处理的过程链条上，被污染的数据池无法充分发挥技术潜力，甚至可能造成数据共享机制和自动化决策机制一同组成的整体解决方案的走样。歧视源于数据，因此，主导方应在数据清洗过程中主动去除冗余、不相关、不合格数据，在降低通信成本的同时提升运算精度，避免各参与方因“数据饥渴”而“来者不拒”，以期从源头“掐断”算法歧视群体化的苗头。

为应对后端风险，应确立智能应用开发和投入市场的基

础伦理标准。引导科技向善、避免智能应用出现“劣币驱逐良币”的有效手段，是通过法律将标准和原则植入技术的底层行动逻辑。在投入市场前，任何技术应用都应满足伦理先行原则，不得游走于现有法律体系的灰色地带进行监管套利。因汇聚了海量大数据，技术方极有可能经不住诱惑，利用算法压榨个体，摄取不成比例的回报。伦理先行原则表明，技术目标的选择不应是简单的效益至上或是性能择优。在数据合规场景中，各参与方的效益增长势必会同步拉动社会公共利益的福祉提升。此外，对于数据主体而言理应共享技术红利，技术方必须兑现用户授权时所抱有的信赖利益，否则数据主体有权主张数据处理合同自始无效。

http://www.cbdio.com/BigData/2023-08/11/content_6174621.htm

数据安全事件

1、罚款 85 万元！南昌某高校发生大量数据泄露案件

近期，南昌公安网安部门工作发现，南昌某高校 3 万余条师生个人信息数据在境外互联网上被公开售卖。

南昌公安网安部门立即开展一案双查，成功抓获犯罪嫌疑人 3 名。同时，对涉案高校不履行数据安全保护义务违法行为开展执法检查。

经查，涉案高校在开展数据处理活动中，未建立全流程数据安全管理制度，未采取技术措施保障数据安全，未履行数据安全保护义务，导致学校存储教职工信息、学生信息、缴费信息等 3000 余万条信息的数据库被黑客非法入侵，其中 3 万余条教职工、学生个人敏感信息数据被非法兜售。

https://www.secrss.com/articles/57836

2、江西一 IT 公司存在数据泄露风险，当地通管局依据数据安全法罚款 15 万元

近日，根据上级部门通报，赣州某信息技术公司业务系统疑似遭受黑客攻击，存在数据泄露风险。江西省通信管理局立即依法组织开展案件调查，查明该公司在开展网络营销代理业务中未有效落实网络和数据安全保护主体责任，未依

法采取相应的技术措施保障业务系统数据安全，该行为违反了《中华人民共和国数据安全法》相关规定，省通信管理局对赣州某信息技术公司给予警告、罚款 15 万元，对直接负责的主管人员和直接责任人各罚款 1 万元。

https://www.secrss.com/articles/57924

3、北海某公司因泄露约 22 万条个人信息数据被罚款 20 万元

近日，北海某网站存在数据泄露问题，约 22 万条个人信息数据被挂在境外论坛售卖，该公司及其直接负责人被北海公安机关分别处以罚款 20 万元、3 万元的行政处罚。

据了解，北海公安网安部门在查处一起涉个人信息保护违法案件时发现，涉案公司建设有一网站，主要提供网上咨询服务，在日常工作中收集了个人和企业等大量公民信息，但未能按照《中华人民共和国数据安全法》《中华人民共和国网络安全法》以及有关等级保护工作要求落实网络安全保护主体责任。

办案民警介绍，该网站服务器安全防护措施不足，存在被多个境外 IP 攻击入侵的情况。同时，涉案公司未采取数据加密等有效的技术保护措施来确保其收集的个人信息安全；在发现个人信息泄露后，未及时告知用户，也未主动向公安

机关报告；还存在网络日志留存不足 6 个月及相关安全管理制度缺失等问题。

https://m.gmw.cn/2023-08/14/content_1303479409.htm

4、房源数据服务商遭勒索软件攻击，美国房地产市场陷入混乱

安全内参 8 月 16 日消息，过去五天，美国加州一家房源挂牌服务提供商遭遇网络攻击，导致全国各地房屋买家、卖家、房地产经纪人和房源网站业务受阻。该公司提供一项关键在线工具，帮助房地产专业人士挂牌房源、查看待售房源、追踪挂牌房源。

这次攻击始于 8 月 9 日，袭击对象是位于加州的软件和服务提供商 Rapottoni 公司。该公司为加州乃至全美各地区房地产集团提供多重房源挂牌服务（也叫 MLS），房地产经纪人可以实时获取各类房屋的销售数据，包括即将入市的房屋、购房报价以及已入市房屋的销售信息。多重房源挂牌服务在买家与卖家、经纪人和房源挂牌网站之间架起了重要桥梁。

https://www.secrss.com/articles/57835

5、IBM 遭到攻击导致科罗拉多州 HCPF 超过 400 万人的信息泄露

据媒体 8 月 14 日报道，美国科罗拉多州医疗保健政策与融资部(HCPF)向超过 400 万人发出通知，称数据泄露事件影响了他们的个人和健康信息。HCPF 澄清说，他们的系统没有遭到攻击，但是他们的承包商 IBM 遭到了针对 MOVEit 的攻击。6 月 13 日调查发现，IBM 使用的 MOVEit 应用上的部分 HCPF 文件在 5 月 28 日左右被访问，攻击者可能窃取了包含某些 Health First Colorado 和 CHP+会员信息的文件。总共影响了 4091794 人，HPCF 将通过 Experian 为受影响用户提供两年的信用监控服务。

https://www.bleepingcomputer.com/news/security/colorado-warns-4-million-of-data-stolen-in-ibm-moveit-breach/

6、Discord.io 约 76 万用户的数据在黑客论坛被出售

据媒体 8 月 14 日报道，Discord.io 约 760000 名会员的信息泄露，导致服务暂时关闭。Discord.io 不是官方 Discord 网站而是第三方服务，被服务器所有者用来创建自定义邀请。8 月 13 日，黑客 Akhirah 在论坛 Breached 上出售了 Discord.io 的数据库，并公开了其中的 4 条用户记录作为攻击证据。据攻击者称，该数据库包含 760000 名 Discord.io 用户的信息。

不久后，Discord.io 证实了泄露数据的真实性，并关闭其服务，取消所有付费会员的资格。

https://www.bleepingcomputer.com/news/security/discordio-confirms-breach-after-hacker-steals-data-of-760k-users/

7、芝加哥贝尔特铁路公司遭到 Akira 的攻击 85GB 数据泄露

媒体 8 月 12 日称，芝加哥贝尔特铁路公司称其正在调查勒索攻击导致的数据泄露事件。该公司由美国和加拿大的六家铁路公司共同拥有，每家铁路公司都使用该公司的转运和换乘设施，是美国最大的中间换乘终点站铁路。8 月 10 日，Akira 将该公司添加到其网站，并表示已获取 85 GB 数据。发言人称，此次事件并未影响公司的运营。去年，多家铁路公司遭到了网络攻击，美国 TSA 试图对铁路等重要基础设施采取更强硬的措施。

https://therecord.media/belt-railway-chicago-ransomware-data-theft-akira

8、英国政府承包商 MPD FM 泄露大量敏感数据

8 月 12 日，据外媒报道，MPD FM 是一家为英国各政府部门提供服务的设施管理和安全公司，该公司的一个公开

实例暴露了员工护照、签证和其他敏感数据。

据调查，暴露的亚马逊存储服务 (S3) 数据文件库，向任何有能力扫描开放网络的人开放了 16,000 多个敏感文档。被曝光的文件包含大量极其敏感的信息，泄露的 MDP FM 员工信息包括：护照、身份证、驾驶执照、出生证明、审核报告、工作权检查、工作合同、地址证明、银行对账单等。

https://securityaffairs.com/149440/security/mpd-fm-data-leak.html

9、普华永道因 MOVEit 存在安全漏洞，致银行 8 万名储户的信息被泄露

8 月 14 日，波多黎各自治区最大的银行——人民银行向缅因州司法部长提交了一份客户信息泄露报告。该报告指出，由于供应商普华永道使用的 MOVEit 软件存在安全漏洞，导致银行 82217 名储户的个人信息被泄露。

目前，波多黎各人民银行已经陆续通知了数千名银行用户，向其告知数据泄露的安全风险，并表示普华永道会计师事务所一直为银行提供相应的审计服务，双方已经连续合作超过二十年。由于其工作性质和要求，使得该银行必须要和普华永道贡献客户信息，以便后者可以完成财务报表方面的独立审计工作，从而造成了此次客户数据泄露事件。

https://www.freebuf.com/news/375127.html

10、微软：欧德神思软件曝出 15 个漏洞，可致电厂关停、数据窃取

8 月 15 日报道，近日，微软安全专家透露，德国工业软件巨头欧德神思（Codesys）的系统中存在 15 个高危安全漏洞，可导致电厂关停或重要关基系统信息被窃取。

这 15 个安全漏洞的编号为 CVE-2022-47379 到 CVE-2022-47393，均属于高危评级，其中多数评分为 8.8/10，可被用于拒绝服务 (DoS) 攻击或远程代码执行 (RCE)。其中的 12 个漏洞为缓存溢出漏洞，可用于对 PLC 实现远程代码执行。但需要攻击者可以绕开身份验证，以及绕过数据执行保护（DEP）和地址空间配置随机加载（ASLR）措施。

https://www.secrss.com/articles/57788

《全球数据安全观察》周报

政策形势： 政策法规/地方动态/标准动态

技术、产品与市场： 技术研究/行业洞察/市场趋势

业界观点： 大咖观点/业界报告

数据安全事件： 合规事件/数据泄露/数据勒索

编委会： 钟力、唐会芳、王雨薇、陈璐

如有反馈 邮件请至 nelab@360.cn