全球数据安全观察

总第 120 期 2023 年第 1 期

(2023.01.02-2023.01.08)

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、昆明市人民政府印发昆明市数字经济发展三年行动计划（2022—2024 年）

2022 年 12 月 26 日，昆明市政府官网发布《昆明市数字经济发展三年行动计划（2022—2024 年）》（以下简称《行动计划》）。《行动计划》明确，到 2024 年，全市数字经济规模翻一番，突破 5000 亿元，年均增长 25%以上，数字经济核心产业增加值占 GDP 比重超过 10%。在构建数字经济核心产业体系方面，要做大智能终端制造产业，到 2024 年，智能终端制造业产值突破 500 亿元，基本建成具有全国竞争力和影响力的智能终端制造产业高地。

https://www.km.gov.cn/c/2022-12-30/4625492.shtml

2、《厦门经济特区数据条例》发布

2022 年 12 月 27 日，《厦门经济特区数据条例》经厦门市第十六届人民代表大会常务委员会第九次会议通过，自 2023 年 3 月 1 日起施行。《条例》共七章六十五条，其中第十五条提到：厦门市大数据主管部门设立**公共数据资源平台**，作为本市公共数据汇聚、共享、开放的统一基础设施，由厦门市人民政府确定的公共数据资源管理机构负责建设、管理

和维护。政务部门、公共服务组织不得新建其他跨部门的公共数据共享、开放平台或者系统。第三十六条提出：厦门市人民政府应当**培育安全可信、包容创新、公平开放、监管有效的数据要素市场**，探索建立数据确权、资产评估、登记结算、交易撮合、争议解决等市场运营体系，促进数据要素依法有序流动。

https://mp.weixin.qq.com/s/Rz4aT_gykinJLmTHrAUqZQ

3、《贵州省数据流通交易管理办法（试行）》发布

12 月 26 日，经贵州省人民政府同意，贵州省大数据发展管理局出台《贵州省数据流通交易管理办法（试行）》。管理办法共 9 章 42 条，分为总则、部门职责、交易场所、交易标的、交易主体、交易流程、安全管理、监督管理、附则。明确制订的依据、范围、原则等内容。一是坚持政府引导、市场主导，场景牵引、释放价值，鼓励创新、包容审慎，严守底线、安全发展的原则。二是鼓励多元化数据流通交易，培育数据流通交易产业生态。

https://new.qq.com/rain/a/20230101A00TGY00

4、联盟技术规范《数据安全和个人信息保护社会责任指南》发布

为落实《数据安全法》《个人信息保护法》等法律法规中所提出关于数据安全和个人信息保护社会责任的要求，放大数据处理和个人信息使用的社会价值，由中国网络安全产业联盟归口，CCIA 数据安全委员会组织委员单位编制了联盟技术文件《数据安全和个人信息保护社会责任指南》(征求意见稿)，编号为 T/CCIA 002-2022，自 2023 年 2 月 1 日起实施。该文件为组织理解数据安全和个人信息保护社会责任以及实施相关活动提供指南。

http://www.china-cia.org.cn/AQLMWebManage/Resources/kindeditor/attached/file/20221230/20221230131850_2889.pdf

5、中国数字资产交易平台于 2023 年 1 月 1 日上线

12 月 29 日消息，全国首个国家级合规数字资产二级交易平台—中国数字资产交易平台，于 2023 年 1 月 1 日在北京举行平台启动发布仪式。据悉“中国数字资产交易平台”由中国技术交易所、中国文物交流中心、华版数字版权服务中心股份有限公司联合建设。

可以看出，“中国数字资产交易平台”是依托中国技术交

易所的国家级交易所属性，发挥交易所的交易职能，为数字资产交易业务制定完善的交易制度、规范的交易体系、科学的交易流程、安全的结算机制，夯实数字资产交易业态的底层基础设施建设，为交易全流程服务保驾护航。

https://www.cebnet.com.cn/20221230/102849637.html

技术、产品与市场

1、IDC 发布中国数据安全基础设施管理平台市场洞察报告

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。

https://www.secrss.com/articles/50795

2、《隐私计算通信应用研究报告（2022 年)》发布

近日，隐私计算联盟发布了《隐私计算通信应用研究报告（2022 年）》。

在技术发展、应用需求、政策支持的共同作用下，隐私计算技术火热发展，应用开始逐渐落地。

在技术发展方面，隐私计算的安全性持续提升，安全验证手段逐渐成熟。性能稳固增强，在部分场景中已经能够达到满足业务需求的程度；在应用需求方面，一是数据融合的需求持续增强，二是对数据保护的要求逐渐提升；在政策支

持方面，2022 年内，中共中央、国务院、国家卫健委等机构发布了一系列涉及数据要素、数据流通的相关政策，鼓励了隐私计算等安全流通技术的探索与应用。

总的来说，隐私计算通信应用主要具备应用数据多元化、应用行业广泛、应用场景集中和应用效果显著这四大特点。

在金融行业中，包括银行、证券、保险等机构都有广泛的通信数据联合应用案例 ，根据业务场景可以大致划分为联合风控、联合营销两大类型。在政务领域中，隐私计算技术在保障政务数据安全的基础上，结合通信数据维度广、数据跨度大等优势，开展了如电信反欺诈、智慧人口流动分析、公共安全态势感知等应用实践。在智慧城市建设过程中，面临大量隐私数据集中在云平台，被攻破的后果严重；跨机构、跨行业的信息流转频繁，隐私泄露风险高；数据不完整或被篡改会导致计算结果受到影响等挑战有待解决。

借助隐私计算技术，能够在保证数据安全的前提下充分发挥通信数据应用价值，助力各行业数字化发展实践，对充分释放数据要素价值和推动社会经济发展具有重大意义。在传统应用上，顺应时代趋势，增强了数据安全保护能力；在创新应用上，为解决新场景落地过程中面临的实质问题提供了较大帮助。

https://www.secrss.com/articles/50811

3、2022 年数据泄露最严重的国家 (地区) 调查

国际数字化运营服务提供商 Proxyrack 基于 2022 年度的观测数据，对全球主要国家和地区的数据泄露情况进行了统计和分析。研究结果显示，几乎所有被调研国家（地区）都在面临数据泄露引发的重大经济损失威胁，而经济发达国家的数据泄露损害将会更高。

数据泄露频率 Top10 国家：据 Proxyrack 给出的研究说明，2022 年数据泄露频率的前十大国家是按照平均每百万人的数据泄露数量排名的。统计数据显示，美国以每百万人 7221177 起数据泄露事件排名第一，法国以每百万人 6488574 起数据泄露事件紧随其后，而非洲国家南苏丹则以每百万人 6184061 起数据泄露事件排名第三。

数据泄露数量 Top10 国家：俄罗斯在 2022 年的数据泄露总数最高，泄露事件数量为 96724450 起。美国的数据泄露事件数量紧随其后，为 63716758 起。

数据泄露损失 Top10 国家（地区）：2022 年美国的平均数据泄露损失成本最高，达到 905 万美元；其次是中东地区，平均数据泄露损失成本为 693 万美元；加拿大排名第三，平均数据泄露损失成本为 479 万美元。

数据泄露影响 Top10 行业：医疗健康行业的平均数据泄露成本最高，达到 923 万美元；其次是金融行业，平均数据

泄露成本为 527 万美元。

https://informationsecuritybuzz.com/analysis-top-ten-countries-mostly-targeted-data-breaches/

4、清华浙大在量子计算破解 RSA 密码方面取得重要突破

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。

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。

https://mp.weixin.qq.com/s/HTEnfpPE1tWT1zeX7M_t_w

5、2023 年最危险的勒索软件五大家族

2022 年勒索软件生态系统发生了重大变化，从少数大型

勒索组织主导转向碎片化的勒索软件即服务（RaaS）运营模式，以寻求更大的灵活性并减少执法部门的关注。勒索软件的这种“民主化”对企业来说是个坏消息，因为这意味着勒索软件策略、技术和程序（TTP）的多样化，企业需要跟踪更多的危害指标（IOC），在尝试谈判或支付赎金时也面临更多障碍。

虽然勒索软件即服务（RaaS）的“民主化”和碎片化趋势已经不可逆转，但是在勒索软件去中心化的背后，一些最危险的勒索软件组织依然是关键目标和重大数据泄露事件的幕后黑手，以下是 2023 年值得关注的勒索软件“五大家族”:

LockBit：一马当先

Hive：勒索超过 1 亿美元

Black Basta：Conti 的变种

Royal：势头强劲

Vice Society：主要针对教育行业

https://www.secrss.com/articles/50694

业界观点

1、汤珂：完善数据全流程合规治理与监管体系，构筑数据高效安全流通屏障

数据要素与传统生产要素不同，其可复制、易修改等特征使得全流程监管体系成为其高效安全流通的保障。近日，中共中央、国务院印发《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，要完善数据全流程合规与监管规则体系。为推进数据合规治理和高效监管，需要从构建数据流通全流程规则标准体系、推进数据分类分级授权和标准化建设、积极探索数据定价机制以及强化数据监管四个维度共同发力。

（1）构建数据流通全流程规则标准体系

（2）推进数据分类分级授权使用与标准化建设

（3）探索政府指导定价、市场自主定价相结合机制

（4）严厉打击非法交易活动，强化数据监管

数据市场的发展需要数据监管的紧密协同。唯有逐步形成规范、安全的数据流通规则，构筑合理的治理和监管体系，才能实现数据要素的高效安全流通。

https://www.ndrc.gov.cn/xxgk/jd/jd/202212/t20221219_1343669.html?code=&state=123

2、方滨兴：破解数据要素流动与隐私保护相冲突的局

数据已成为国家战略资源和关键生产要素，随着数字经济时代的到来,建设安全可控的数据开放平台，培育数据交易市场成为当务之急。为此，国家提出推进政府数据开放共享，加快推动各地区各部门间数据共享交换、公共数据开放和数据资源有效流动。但是，数据安全关乎国家安全、商业机密及个人隐私,需要处理好数据开放利用与隐私保护之间的关系。我们看到，国家相继出台了《数据安全法》《个人隐私保护法》等法规政策，要求**在加快培育数据要素市场的同时，还要对数据进行分类分级的安全保护，实现数据安全与数据开放利用并重**。

实现数据安全与数据开放利用并重，其实质是多目标优化的问题，用简单的最优目标的求解方法很难达到，需要在数据要素流动和数据安全之间建立一种平衡。从数据流动和计算模式两个技术维度可以形成四大类的解决方案。

一是，在集中计算模式下实现“数据可用不可见”。典型技术如李凤华教授提出的隐私计算，通过隐私泄露代价和概率的计算模型来求得所接受的计算方法与保护结果。

二是，在协同计算模式下实现“数据可用不可见”。典型技术如姚期智院士提出的安全多方计算，允许多个数据所有者在互不信任的情况下进行协同计算，然后输出计算结果。

常见如混淆电路、不经意传输，同态加密等协同计算技术。

三是，在协同计算模式下实现“数据不动程序动”。数据不流通的情况下需要算法程序流动，典型技术如杨强教授提出的联邦学习，主要是采取联邦学习框架，将集体学习算法程序分散到各数据拥有方，然后再将训练参数传回来以实现数据利用。

四是，我们提出的在集中计算模式下实现“数据不动程序动”。其基本思想是要构造一个可信的执行环境，即通过构建“模型加工厂”为数据开放利用提供一种可用于加工模型的安全可控分析平台，保留所有权释放使用权，实现隐私保护与数据流动共存的最优目标。

https://mp.weixin.qq.com/s/kcq-yB305awi-o4cwWTLwQ

3、许皖秀：把握我国实施个人信息出境认证的几个要点

近年来，我国着力建设数据出境安全评估制度，这是一种最严格的数据出境方式。但跨境经济活动的多样性、国际贸易流通的复杂性决定了，数据出境方式必然是灵活多样的，因此，必须加快建立个人信息出境安全认证机制，作为数据出境安全评估机制的重要补充，既坚决维护国家安全，又有效促进跨境贸易、便利数据流动。此次发布的《个人信息保护认证实施规则》对此进行了积极探索，其具有以下四个特

点。

（1）首先开展数据安全认证顶层设计，个人信息出境安全认证是数据安全认证制度的其中一种应用。

（2）由国家市场监管总局和国家互联网信息办共同实施监管。

（3）“急用先上”与“稳步推进”相结合。

（4）从制度设计上强化对数据发送者和接收者的监督管理。

https://www.secrss.com/articles/50600

4、杜小勇：创新政府数据治理机制、压实企业数据治理责任

近日，中共中央、国务院印发《关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称《数据二十条》），并提出要建立安全可控、弹性包容的数据要素治理制度。数据治理是充分释放数据价值的基础性、系统性工作，要充分发挥政府和企业的创新精神和责任感，才能更好地应对日益严峻的数据危机，实现数据要素价值的可持续发挥，支撑数字经济的高质量发展。就政府和企业在数据治理中各自应该扮演的角色谈以下几点认识。

（1）释放数据价值和守住安全底线应成为数据治理的共识。

（2）要明确政府定位、创新政府数据治理机制。

（3）要发挥企业市场主体作用、压实数据治理责任。

（4）多方共创共建数据协同治理体系。

https://www.ndrc.gov.cn/xxgk/jd/jd/202212/t20221220_1343708.html?code=&state=123

5、杨强：数据跨境可信流通政策解读

数据流通的关键是价值流通，数据流通的目的是价值释放。安全、可信的数据跨境流通体系顶层设计过程，不仅包括数据安全和隐私计算技术的不断发展，还包括持续推进跨境数据审计和确权制度的完善，并构建完整的跨境数据价值交易平台，从而让数据在不出境、不可见的情况下，仍能达到价值流通与价值释放的根本目的。为了加快数据跨境可信流通体系建设步伐，进一步强化数据跨境流通法律规范，中共中央 国务院正式印发《关于构建数据基础制度更好发挥数据要素作用的意见》（以下简称《数据 20 条》），这些具备前瞻性的政策建议符合中国国情，不仅意义重大，而且具备极高的可行性，适合大力推广并践行。

（1）规绳矩墨，国际规则和数字技术标准是数据跨境可信流通的基本轨道。

（2）明堂正道，数据跨境可信流通是国际公平竞争环境

的必要条件。

（3）双管齐下，隐私计算与区块链是保护数据跨境流通安全与合规的有力武器。

（4）法成令修，法律规范为数据跨境可信流通保驾护航。

https://www.ndrc.gov.cn/xxgk/jd/jd/202212/t20221220_1343703.html?code=&state=123

数据安全事件

1、法国因 Bing Cookie 对微软处以 6000 万欧元罚款

法国隐私监管机构对 Microsoft 处以 6000 万欧元的罚款，理由是其误导性 cookie 政策违反了该国的隐私法。调查发现，微软的 Bing 搜索引擎在未经用户同意的情况下在其用户的浏览器上部署了广告 cookie。Bing 有允许用户拒绝 cookie 的机制，并且该公司故意设计其拒绝机制，使用户更容易接受 cookie 而不是拒绝它们。据 CNIL 称，微软这样做**违反了《法国数据保护法》规定的互联网用户的同意自由**。

https://www.inforisktoday.com/france-fines-microsoft-ireland-60m-euros-over-bing-cookies-a-20781

2、法国数据保护机构对 Apple 处以罚款

1 月 5 日，法国数据保护机构 (CNIL) 已对 Apple 处以 800 万欧元（850 万美元）的罚款，原因是 Apple 在未征得用户同意或未征得用户同意的情况下收集用户数据用于 App Store 上的定向广告。

这种做法被认为违反了《法国数据保护法》(DPA) 第 82 条，这是一项符合 GDPR（通用数据保护条例）的国家指令，适用于整个欧洲。

https://www.bleepingcomputer.com/news/apple/france-fines-

apple-for-targeted-app-store-ads-without-consent/

3、Facebook 因强迫用户接受定向广告而被爱尔兰监管机构罚款 4.14 亿美元

1 月 5 日，爱尔兰数据保护委员会 (DPC) 已对 Meta Platforms 处以 3.9 亿欧元（约合 4.14 亿美元）的罚款，原因是 Meta Platforms 处理用户数据以提供个性化广告，这可能对其以广告为燃料的商业模式造成重大打击。为此，隐私监管机构已命令 Meta Ireland 支付两项罚款——因违反与 Facebook 相关的欧盟通用数据保护条例（GDPR）而被罚款 2.1 亿欧元（2.225 亿美元），以及 1.8 亿欧元（1.91 亿美元）对于 Instagram 中的类似违规行为。

https://thehackernews.com/2023/01/irish-regulators-fine-facebook-414.html

4、铁路巨头 Wabtec 遭 Lockbit 勒索软件，披露数据泄露

1 月 3 日，美国铁路和机车公司 Wabtec Corporation 披露了一起数据泄露事件，暴露了个人和敏感信息。被盗数据暴露了各种敏感信息，包括：全名、出生日期、非美国国民身份证号码等。Wabtec 在年底发布的公告中表示，黑客早在 2022 年 3 月 15 日就破坏了他们的网络并在特定系统上

安装了恶意软件，这是一场勒索软件攻击。几周后，LockBit 发布了从 Wabtec 窃取的数据样本，并最终在 2022 年 8 月 20 日泄露了所有被盗数据，大概是在未支付赎金之后。https://www.bleepingcomputer.com/news/security/rail-giant-wabtec-discloses-data-breach-after-lockbit-ransomware-attack/

5、沃尔沃遭到 Endurance 的勒索攻击 200GB 敏感数据疑似泄露

1 月 3 日报道称，法国安全机构 Anis Haboubi 发现黑客在论坛上以 2500 美元的价格出售从沃尔沃窃取的数据。2022 年 12 月 31 日，论坛成员 IntelBroker 声称沃尔沃遭到了 Endurance 的勒索攻击，攻击者窃取了 200GB 的敏感数据，这些数据现在正在出售。卖家解释说，他没有索要赎金，因为他认为该公司不会付赎金。据悉，被盗数据包括数据库访问、CICD 访问、Atlassian 访问、域名访问、WiFi 点和登录、授权承载、API、PAC 安全访问、员工名单、软件许可证以及密钥和系统文件。目前，尚不清楚这一说法的真实性。https://securityaffairs.com/140258/hacking/volvo-cars-data-breach-2.html

6、勒索团伙 Hive 公开 Consulate Health Care 的 550GB 数据

媒体 1 月 7 日称，勒索团伙 Hive 泄露了 Consulate Health Care 的 550GB 数据。该团伙表示，攻击发生在 2022 年 12 月 3 日，并于 2023 年 1 月 6 日披露。起初，攻击者发布了被盗数据的样本，并声称窃取了合同、NDA 和其它协议文件、公司信息、员工信息和客户信息等。后来，研究人员发现该团伙泄露了从 Consulate Health Care 窃取的 550GB 数据，包括客户和员工的 PII。据推测，因为谈判失败了，勒索团伙没有等到计划的截止日期就公开了所有数据。

https://securityaffairs.com/140452/cyber-crime/consulate-health-care-hive-ransomware.html

7、丰田、梅赛德斯、宝马 API 漏洞暴露车主个人信息

2023 年 1 月 4 日，据报道，近 20 家汽车制造商和服务包含 API 安全漏洞，这些漏洞可能允许黑客执行恶意活动，从解锁、启动和跟踪汽车到暴露客户的个人信息。据悉，API 漏洞主要影响宝马、罗尔斯、奔驰、法拉利、保时捷、捷豹、路虎、福特、起亚、本田、英菲尼迪、日产、讴歌、现代、丰田和创世纪等其知名汽车品牌。此外，漏洞还影响汽车技术品牌 Spireon 和 Reviver 以及流媒体服务 SiriusXM。

https://www.bleepingcomputer.com/news/security/toyota-mercedes-bmw-api-flaws-exposed-owners-personal-info/?__cf_chl_tk=ygr4MT.2VGz5jSC3Nikd0aJZe1HGlxtCBcTiuianmYM-1673189212-0-gaNycGzNEZE

8、2 亿 Twitter 用户的电子邮件地址在网上泄露

2023 年 1 月 4 日，一个被描述为包含超过 2 亿 Twitter 用户的电子邮件地址的数据泄漏已经在一个流行的黑客论坛上以大约 2 美元的价格发布。这些数据集是在 2021 年通过利用 Twitter API 漏洞创建的，该漏洞允许用户输入电子邮件地址和电话号码以确认他们是否与 Twitter ID 相关联。

https://www.bleepingcomputer.com/news/security/200-million-twitter-users-email-addresses-allegedly-leaked-online/

9、社交平台 Cricketsocial.com 用户信息和管理员凭据泄露

1 月 4 日报道称，CyberNews 发现板球社交平台 Cricketsocial.com 泄露了超过 10 万条用户个人信息和凭据。该数据库由美国 AWS 托管，包含电子邮件、电话号码、姓名、用户密码、出生日期和地址等信息。其中大部分记录似乎都是测试数据，但仍然包括合法网站用户的 PII 信息。研

究人员还发现该数据库还泄露了明文形式存储的网站管理员凭据，可被攻击者用来接管平台。
https://securityaffairs.com/140329/data-breach/cricketsocial-com-data-leak.html

10、马来西亚电信称超过 25 万 Unifi Mobile 客户的数据泄露

2022 年 12 月 30 日报道，马来西亚电信（Telekom Malaysia Bhd）透露，12 月 28 日有 250248 个 Unifi Mobile 客户受到数据泄露的影响。其中既包括 Unifi Mobile 的个人客户，也包括中小型企业(SME)。泄露的数据类型主要涉及姓名、电话号码和电子邮件，没有其它信息泄露。TM 表示已通知受影响用户，并向有关当局报告此事。该公司并未说明这是何种违规行为或是如何发生。
https://www.nst.com.my/business/2022/12/865784/250248-unifi-mobile-customers-affected-data-breach-says-tm