全球数据安全观察

总第 140 期 2023 年第 21 期

（2023.07.10-2023.07.23）

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、习近平对网络安全和信息化工作作出重要指示

7 月 14 日至 15 日，全国网络安全和信息化工作会议在京召开。中共中央政治局常委、中央书记处书记蔡奇出席会议并讲话，中共中央政治局常委、国务院副总理丁薛祥出席会议并传达了习近平重要指示。习近平明确坚持党管互联网，坚持网信为民，坚持走中国特色治网之道，坚持统筹发展和安全，坚持正能量是总要求、管得住是硬道理、用得好是真本事，坚持筑牢国家网络安全屏障，坚持发挥信息化驱动引领作用，坚持依法管网、依法办网、依法上网，坚持推动构建网络空间命运共同体，坚持建设忠诚干净担当的网信工作队伍。

http://www.news.cn/politics/leaders/2023-07/15/c_1129751651.htm

2、七部门联合公布《生成式人工智能服务管理暂行办法》

7 月 13 日，国家互联网信息办公室等七部门联合公布《生成式人工智能服务管理暂行办法》，明确了提供和使用生成式人工智能服务的基本原则，从技术发展与治理、服务规范等方面提出了规定，并提出对生成式人工智能服务实行

包容审慎和分类分级监管。

http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm

3、两部门印发《关于促进网络安全保险规范健康发展的意见》

7 月 17 日，工业和信息化部、国家金融监督管理总局联合印发《发布关于促进网络安全保险规范健康发展的意见》，以加快推动网络安全产业和金融服务融合创新，引导网络安全保险健康有序发展，培育网络安全保险新业态，促进企业加强网络安全风险管理，推动网络安全产业高质量发展。意见从建立健全网络安全保险政策标准体系、加强网络安全保险产品服务创新、强化网络安全技术赋能保险发展、促进网络安全产业需求释放、培育网络安全保险发展生态 5 个方面提出意见。

https://wap.miit.gov.cn/zwgk/zcwj/wjfb/yj/art/2023/art_0cc1cefdb4e74a169e0a98649c427153.html

4、人社部出台《人力资源服务机构管理规定》

6 月 29 日，人社保出台《人力资源服务机构管理规定》，对人力资源服务机构收集个人信息的范围进行明确，并要求其应当建立个人信息保护、个人信息安全监测预警等机制,不

得泄露、篡改、损毁或者非法出售、非法向他人提供所收集的个人信息，并采取必要措施防范盗取个人信息等违法行为；应当对个人信息保护情况每年至少进行一次自查，记录自查情况，及时消除自查中发现的安全隐患。

http://www.mohrss.gov.cn/xxgk2020/gzk/gz/202306/t20230630_502242.html

5、《中国人民银行业务领域数据安全管理办法（征求意见稿）》发布

7 月 24 日，中国人民银行发布了《中国人民银行业务领域数据安全管理办法（征求意见稿）》，细化明确中国人民银行业务领域数据安全合规底线要求，填补本领域数据安全管理制度保障空白。征求意见稿主要从数据分类分级、数据安全保护总体要求、数据安全保护管理措施、数据安全保护技术措施、风险监测评估审计与事件处置措施等方面提出要求。

http://www.pbc.gov.cn/tiaofasi/144941/144979/3941920/4993510/index.html

6、《中国（上海）自由贸易试验区专项发展资金支持数据要素市场发展实施细则》发布

7 月 11 日，《中国（上海）自由贸易试验区专项发展资

金支持数据要素市场发展实施细则》发布，强调支持支持浦东引领区建设国家级数据交易所，培育数据要素产业，发展高质量数字经济。实施细则鼓励数据交易场所支持企业挂牌数据产品、支持企业流通交易优质数据，对符合相关条件的予以相应的资金支持。

https://www.sh-tec.cn/ryrd/8176.html

7、《河南省实施扩大内需战略三年行动方案（2023—2025年）》印发

7月11日，河南省人民政府办公厅印发《河南省实施扩大内需战略三年行动方案（2023—2025年）》，再次强调加快培育数据要素市场，提出要求推动政务数据、公共数据、社会数据低成本采集、高效率归集与低能耗存储，加快建设数据资源池，到2025年建成10个以上全国领先的行业数据库；探索建立数据产权、流通交易、收益分配、安全治理等制度体系，完善数据质量标准规范，培育提升数据服务能力；开展数据要素价值化试点，加快建设郑州数据交易中心，支持郑州、新乡等开展公共数据确权授权试点，推动公共数据以产品或服务等形式向社会提供。

https://www.henan.gov.cn/2023/07-11/2776581.html

8、《关于印发川渝自贸试验区协同开放示范区深化改革创新行动方案（2023—2025 年）》发布

7 月 7 日，重庆市人民政府办公厅、四川省人民政府办公厅印发《川渝自贸试验区协同开放示范区深化改革创新行动方案（2023—2025 年）》，提出共同推动西部数据交易中心和西部数字资产交易中心建设，共同建设全国一体化算力网络成渝国家枢纽节点，提升中新（重庆）国际互联网数据专用通道、成都国际互联网数据专用通道覆盖范围和服务能级。https://www.cq.gov.cn/zwgk/zfxxgkml/szfwj/qtgw/202307/t20230707_12133438.html

技术、产品与市场

1、2023 年勒索软件勒索金额猛增，已达到 4.491 亿美元

根据区块链分析公司 Chainaanalysis 的一份报告，勒索软件是今年唯一出现增长的加密货币犯罪类别，而其他所有犯罪类别，包括黑客、诈骗、恶意软件、违禁品销售、欺诈商店和暗网市场收入，均大幅下降。

报告称：“勒索软件是 2023 年迄今为止唯一呈上升趋势的基于加密货币的犯罪形式。勒索赎金有望创下新的纪录。截至 6 月份，勒索软件攻击者已勒索至少 4.491 亿美元。”

2023 年上半年勒索软件的年度累计收入已达到 2022 年总收入的 90%。如果收入增长速度保持在这一水平，到 2023 年底，勒索软件攻击者将从受害者身上获利约 9 亿美元，有可能打破 2022 年创纪录的 9.4 亿美元。

分析人士认为，所谓的“大型狩猎”是勒索软件收入大幅增长背后的推动力，因为网络犯罪分子已重新瞄准可勒索大笔赎金的大型企业和机构。

https://www.secrss.com/articles/56608

2、《2022-2023 全球计算力指数评估报告》发布

《2022-2023 全球计算力指数评估报告》由 IDC、浪潮

信息和清华大学全球产业研究院联合编制。报告着重分析了美国、中国、日本、德国、印度等 15 个国家以及互联网、制造和金融等 13 个行业的计算力需求和趋势。

从国家算力指数排名看，《报告》通过综合计算能力、计算效率、应用水平和基础设施支持四个维度的评估得出评分，将国家分成领跑者国家（60 分以上）、追赶者国家（40-60 分）和起步者国家（40 分以下）三个梯队。**美国和中国依然分列前两位，同处于领跑者位置**；追赶者国家包括日本、德国、新加坡、英国、法国、印度、加拿大、韩国、爱尔兰和澳大利亚；起步者国家包括意大利、巴西和南非。

从行业来看，全球计算力水平 TOP5 的行业是互联网、制造、金融、电信和政府。制造行业首次超过金融行业，排名全球第二。同时，制造业的 IT 投入产出比表现更好，制造业全球 Top30 的企业中， IT 每投入 1 美元，可以拉动 45 美元的营收额产出，6 美元利润产出。

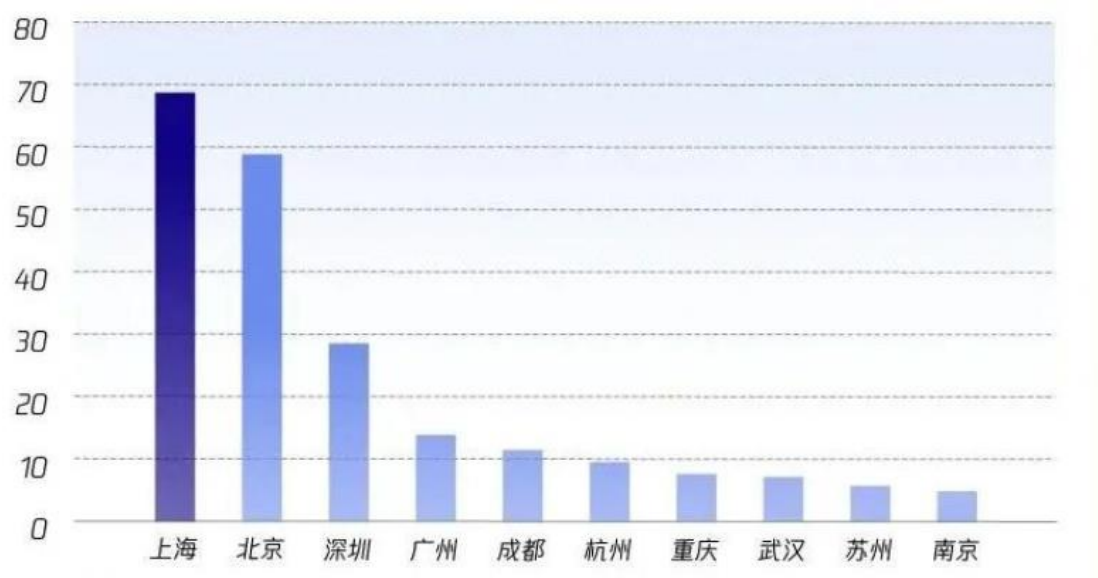
https://mp.weixin.qq.com/s/quj3yn3eCG0-ZBebjJiKXw

3、《数字化转型指数报告 2023》：上海、北京、深圳全国前三

近日，腾讯研究院联合腾讯企鹅有调、清华大学二十国

集团创业研究中心发布了《数字化转型指数报告 2023》（以下简称报告）。这是腾讯研究院连续第九年发布全国数字化指数报告，报告发现，疫情之后数字化正面临线上和线下新平衡的磨合期，而数字平台的稳定器作用更加凸显等。值得关注的是，今年还特别增加了对未来产业的研究，尝试描绘未来产业的全国布局图，以捕捉未来增长点。报告还特别发起了面向 C 端的数字化认知和使用调查，有不少有趣发现。

其中，火车头效应明显，上北深数字化转型指数规模长期处于全国前三位置，明显高于其他城市、持续领跑全国。其中，上海整体指数和基础设施指数第一，北京平台和应用指数第一，深圳指数增长在头部城市中较快。



https://mp.weixin.qq.com/s/9FEyyNnPP70wibP9oY2Kaw

4、研究：目前只有 45% 的云数据经过加密

据泰雷兹最近发布的一份研究报告称，去年有 39% 的企业在其云环境中遭遇过数据泄露，这一比例较 2022 年的 35% 有所增加。此外，55% 的受访者表示人为错误是云数据泄露的主要原因。

与此同时，该报告称，云中存储的敏感数据数量急剧增加。75% 的企业表示，存储在云中的超过 40% 的数据被归类为敏感数据。38% 的受访者将软件即服务 (SaaS) 应用程序视为黑客的主要目标，紧随其后的是基于云的存储 (36%)。

尽管据报道云中的敏感数据有所增加，但研究发现所使用的加密级别较低。只有 22% 的 IT 专业人员表示，他们在云中的敏感数据有超过 60% 是加密的。调查结果显示，目前平均只有 45% 的云数据经过加密。

该研究还发现企业缺乏对加密密钥的控制，只有 14% 的受访者表示他们控制着云环境中加密数据的所有密钥。此外，近 62% 的受访者表示他们拥有五个或更多密钥管理系统，这在保护敏感数据时增加了复杂性。

https://www.helpnetsecurity.com/2023/07/13/cloud-environments-security/?web_view=true

5、清华牵头立项 IEEE P7018《生成式预训练 AI 模型的安全性和可信性技术要求》国际标准

生成式 AI 预训练模型在取得进展的同时，也带来了安全和道德挑战。为应对这些问题，清华大学提出了 IEEE P7018 标准，旨在构建更安全、可靠的预训练 AI 系统。该标准涵盖了开发、部署和使用过程中的安全风险、隐私保护和偏见问题，并提供预防、检测和应对策略。标准的制定将提高 AI 模型的安全性、公正性和透明度，增强公众对 AI 的信任。目前，工作组公开征集专家意见，以推进标准研制工作。

https://mp.weixin.qq.com/s/B5wU1v68L257dNUFUX6fJQ

业界观点

1、《生成式人工智能服务管理暂行办法》发布，解析 AIGC 的数据合规挑战与应对之道

参考美国国家标准技术研究院于 2023 年 1 月发布的人工智能风险管理框架（AI Risk Management Framework，AI RMF），AIGC 的生命周期大体可包括模型训练、应用运行和模型优化三个阶段，文章对各阶段涉及典型数据收集形式及合规风险进行了梳理，并就我国 AI 法律框架下的五个典型数据合规问题进行分析，主要包括：

问题一：如何管理爬取数据的风险？

问题二：如何管理数据源风险？

问题三：AIGC 应用运行及模型优化阶段典型个人信息合规问题？

问题四：如何处理 AIGC 数据泄露风险？

问题五：AIGC 开发者与服务提供者如何认定数据权属及相关责任？

关于如何实现 AIGC 的数据合规，文章提出如下建议：

首先，针对 AIGC 开发者：

1) 规范数据收集活动，警惕爬虫风险。

2) 提高数据标注及清洗、模型训练阶段的透明性、可解

释性及公平性，积极应对监管。

其次，无论是 AIGC 开发者还是服务提供者，均应关注：

1) 加强第三方管理，提升可靠性与稳健性。

2) 开展个人信息保护影响评估（PIA），优先整改高风险事项。

第三，针对 AICG 集成方：

如涉及集成 AIGC 开发者技术，应梳理合作模式，厘清数据权属，明晰各方责任。

第四，针对 AIGC 服务提供者：

防止数据泄露。

最后，针对 AIGC 使用者：

1) 识别高风险应用场景，开展必要性审查并采取针对性措施。

2) 规范 AIGC 使用行为，防止数据泄露。

3) 确保在依据 AIGC 输出结果采取行动之前进行人工审查。

https://www.secrss.com/articles/56640

2、高艳东：跨境数据流动，须坚持主权至上

近年来，数据跨境流动日益受到关注。欧盟和美国刚刚达成“欧盟-美国数据隐私框架”协议，英国《金融时报》就发

文称，“在美中关系恶化的背景下，跨国公司纷纷加快脱钩中国数据”。事实上，在美国倡导的“数据自由流动”的口号下，多国数据源源不断流向美国，美国对他国的控制力日益加强。

第一，数据正在成为国家的核心竞争力之一，任何跨境数据问题都需要我们谨慎对待。

第二，应当坚决反对美国数据政策的两面性。美国利用其技术和数据优势，在全球推行两面性的数据政策。在有利于自己时主张数据自由流动，在不利于自己时则提倡监管主义。

一方面，美国对外主张数据自由流动，以强化其数据霸权。由于美国有大量互联网巨头，因而，主张数据自由流动的实质就是让全球数据流向美国，使美国成为全球数据中心。通过数据自由流动，美国获得巨额利益。

另一方面，美国以安全为名，不惜一切手段实行美国优先的政策。一旦影响了美国利益，美国就会搬出“国家安全”的大旗打压他国。在数据流向美国时，美国对自由主义持欢迎态度，但是，一旦数据要离开美国或者脱离美国控制时，美国就经常以国家安全为由实行强监管。

同样，美国最大限度地扩张其权力管辖范围，扩张数据主权的范围。根据“长臂管辖“原则，他国互联网企业不需在美国设立，也不必在美国有经营业务，只要其经营行为与美

国市场、美国企业、美国机构等有联系，华盛顿就可以按照“长臂原则”进行管辖。

第三，在数据安全问题上，中国需要做好防守反击。虽然中国数字产业近年来取得了长足发展，但与美国相比，我国有全球影响力的互联网巨头数量仍然很少。这决定了我国只能稳扎稳打。

一方面，短期内，我国的数据政策只能是“结硬寨、打呆仗”。面对美国的数据霸权，一些数据小国没有产业基础，没有技术防守能力，只能被迫放弃抵抗。但是，我国是人口和疆域大国，不可能做美国的数据殖民地，把数据主权拱手相让。为了维护数据主权，我国通过《数据安全法》，要求数据进行本地化储存，对重要数据出境进行国家安全审查。这些做法都是印度、俄罗斯等大国的惯常操作。

另一方面，未来，我国也应当倡导能够平衡数据利用和安全的国际数据规则体系。我国是全球为数不多的可以推动构建国际数据公平体系的国家之一。数据既需要自由流动，也需要有序流动。如果承认数据是一种资源，那么，一国获取他国数据资源之时，应当对他国进行补偿，这就需要对数据出境征收数字税。同时，数据是人类共有的财富，不能被某一国家独占，未来应当推动一种“数据联合国”的模式，在各国均有参与机会的前提下公平分配数据资源，打破数据垄

断，使人类能够共享数字时代的红利。

概而言之，数据无小事。在全球数据单向流动的大背景之下，我国应当在维护好自身数据安全和主权后，再进一步推动共享、共治、共利的数据国际规则体系。

https://opinion.huanqiu.com/article/4DkjVIQJYQ8

3、马晓白：加快推进政务数据有效共享

近年来，经过各方面共同努力，我国政务数据基础设施基本建成、要素壁垒逐步打通、共享开放程度不断加深、政务服务和监管效能大幅提升，政务数据共享开放工作成效显著，为加强数字政府建设打下了坚实基础，但仍存在“不敢、不愿、不能”的突出问题，数据壁垒依然存在。

（一）政务数据标准规范体系不健全，不敢开放共享

（二）政务数据统筹管理机制待完善，不愿开放共享

（三）政务数据安全保障能力待提升，不能开放共享

对此，建议聚焦数据共享“不敢、不愿、不能”的难点痛点问题，从共性基础性问题入手，夯实法律法规、统筹协调、分级分类、共享交换、数据管理、标准规范的制度基础，健全政务数据共享协调机制，促进政务数据规范有序、高效公平的开放共享和有效利用，增强数字政府效能。

（一）加快数据立法，完善制度规范

探索在数据领域统筹开展国家立法，加强政务数据领域前沿法律问题研究。建立政务数据产权保护和利用新机制，营造政务数据资源开发利用法治环境。构建政务大数据管理制度体系和标准规范体系，编制全面兼容的数据相关基础性标准规范。开展数据权属应用试点示范，探索建立数据权属界定和保护利用制度，完善数据资源全生命周期管理的规范性文件。

（二）建立“四定”制度，健全协调机制

明确政府部门数据归集的职能，形成“定职责、定机构、定人员、定职能数据清单”的“四定”制度，要求政府部门数据采集工作遵从职责、事项、数据清单三者相对应的原则，编制政府部门职能数据清单，实现政务数据应采尽采、应汇尽汇。

健全政务数据共享协调机制，加强政务数据供需对接。建立政务数据资源开发利用组织架构，开展首席数据官（CDO）试点，选择条件成熟的地区设立首席数据官，明确CDO的责任机制和激励机制，提升CDO的统筹协调和数据治理能力。完善管理规范，将系统更新和数据治理等费用纳入财政预算支持，探索将数据资源作为重要的信息化资产纳入政府资产。

（三）编制数据目录，分类分级管理

编制政务数据目录系统，全面摸清政务数据资源底数，由各地区各部门政务数据主管部门根据政务数据目录清单对本地区本部门政务数据开展分类定级，梳理数据源，明确数据更新周期，确定共享属性和共享条件、开放属性和开放条件，梳理汇总形成政务数据全量目录。依据政务数据目录清单，按照统一标准规范对各地区各部门的数据资源进行归集和汇聚。同时进一步打通各级平台的连接，持续保障数据资源一体化。

（四）提升数据质量，加强安全保障

按照“谁管理谁负责、谁提供谁负责、谁使用谁负责”的数据治理原则，建立健全数据质量管理机制，提高数据的准确性、完整性和一致性，确保数据真实可用、高效共享。

围绕数据全生命周期，明确数据安全主体责任，建立健全数据安全管理规范。加强数据安全常态化检测，提升平台技术防护能力，建立健全面向数据的信息安全技术保障体系。加大对个人隐私、商业秘密等重要数据保护力度，严格管控数据访问行为。更新老旧的信息化基础设施，基于重要数据建立数据“可用不可见”的安全可信计算环境，确保数据安全。完善数据安全运营监管保障机制，构建统一高效、协同联动的数据安全运行管理体系，形成数据安全管理闭环，筑牢数据安全防线。

（五）夯实共享机制，深化应用场景

依托全国一体化政务服务平台的数据共享枢纽，构建覆盖国家、省、市各层级的全国一体化政务数据共享交换体系，建立权责清晰、高质高效的政务数据共享协调机制。加强重点共性应用集约建设，以应用为牵引，协同推进公共服务机构、相关企业和第三方平台等数据共享，探索社会数据“统采共用”，形成横纵结合、供需互动的数据协同共享机制。进一步强化政务大数据平台的技术能力，为多元、海量的数据融合和创新应用提供基础支撑。发挥营商环境创新试点城市的示范带动作用，在数据共享和电子证照应用支撑领域先行先试，推动相关改革举措在全国复制推广。

（六）推进数据开放，探索授权运营

主动收集社会、企业的政务数据开放需求，以需求为导向制定政务数据开放清单，及时处理社会公众提出的数据开放申请和异议处理申请，不断提高政务数据开放水平。同时，根据政务数据开放安全管理的工作要求，进一步加强开放安全审查，建立开放数据全流程监管体系，对政务数据开放工作中可能出现的各类安全风险，加强研究防控和事中事后监管。鼓励各地区选择安全可控的机构依法依规开展政务数据授权运营，发挥社会力量对政务数据资源开发利用，培育数据要素市场，构建共建、共治、共享的数据治理新格局。

（七）推进数据要素与其他创新要素深度融合

数据要素的完善对于产业链升级具有重要意义，探索建立以数据链有效联动产业链、创新链、资金链和人才链的“五链协同”制度框架。一是聚焦产业链，以数据链联接创新链。二是围绕产业链，以数据链激活资金链。三是依托产业链，以数据链培育人才链。发挥大数据人才精准画像和供需匹配优势，为各层次人才提供“代理式、一站式、全天候”服务，促进数据链、人才链、产业链的同频共振。

http://www.echinagov.com/viewpoint/344344.htm

4、杜平：有效推进数据要素商品价值最大化

7 月 14 日，浙江数字经济百人会激活数据要素价值圆桌会在温州瓯海举办。国家信息中心原党委书记、常务副主任杜平就《有效推进数据要素商品价值最大化》作主题演讲。

杜平提出要坚持两个维度推进数据要素商品价值最大化，两个维度协同互补推进，这是生产要素市场化配置的基本特征所决定了的。

一是广泛深度挖掘数据资源要素使用价值。我国数字经济领域快速发展、成效显著，其主要因素就在于率先开发利用数据资源使用价值，促进数据资源要素化。在此过程中，大量数据要素使用价值得到开发利用，并且通过流通和交易

逐步实现其商品价值或货币价值。

二是加快提高数据要素商品价值是重要紧迫任务。我国数据要素商品价值化还处于早期阶段。因此，2022 年底中共中央和国务院决策推进数据要素基础制度建设 20 条，对于加快实现数据要素商品价值具有重大历史意义和鲜明的现实针对性。

同时，杜平表示要坚持数据要素场外交易和场内交易两个市场长期并存。

一是通过集中和非集中两种场景促进数据要素流通交易，都符合数据要素市场化配置的客观规律。

二是依托数据交易所推动数据要素价值化，是我国规模化、合规化、市场化实现数据要素商品价值的努力方向和主要任务。

最后，杜平强调要运用最新技术手段保障数据产品供求双方双赢发展。

一是现有技术手段可以对开发更多、更高质量、更具商业价值的入市数字产品提供保障。

二是更多运用技术手段建立健全入市数字产品（标的）市场化价格形成机制。

https://www.sohu.com/a/704969569_398084

5、李健：中小银行外部数据安全应用的探索与研究

银行在数字化转型的开展过程中，将为跨机构、跨领域的数据流动共享提供创新驱动，在深化使用外部数据，不断推进内、外部数据融合应用的同时，也为数据要素市场化配置注入充沛活力。对于中小银行而言，随着外部数据的需求越来越大，应用场景越来越多，如何进行外部数据的精细化管理，如何做好外部数据的安全应用，已经成为数据应用面临的重要挑战。主要包括:

（1）外部数据管理难度凸显。

（2）外部数据应用面临的合规性风险。

（3）外部数据应用面临的连续性风险。

（4）外部数据应用面临的可靠性风险。

（5）外部数据价值有待全面释放。

对此，应从以下几点着手应对:

（1）明确外部数据管理机制，为安全应用夯实制度基础。通过制度明确外部数据管理的职责归属，确定数据归口管理部门，整合分散重复的需求，节约成本，对外部数据进行全流程集约化管理，满足合法、稳定、准确、完整的准入要求，实现安全应用和共享，充分发挥价值。

（2）搭建外部数据管理平台，为安全应用提供标准服务。通过科学的管理和手段，将外部数据进行整合、标准化，建

设符合“统一出口、统一采集、统一服务”的外部数据服务平台十分必要。

（3）制定外部数据管理策略，为安全应用化解潜在风险。为尽可能地防范外部数据风险，确保安全可控，建议遵循以下策略实现安全应用。一是由商用数据向政务数据转变。二是由单源依赖向多源服务转变。三是由单一数据引用向交叉验证转变。四是由粗放管理向分级分类管理转变。

（4）丰富外部数据应用场景，为价值释放营造创新环境。随着接入外部数据的质量不断提升，首先是做好内外部数据的融合应用，其次是注重挖掘更多的应用场景，同时充分借鉴行业内优秀实践，不断收集整理使用外部数据的新场景及创新产品。

https://www.secrss.com/articles/56884

数据安全事件

1、谷歌与 Meta 共享私人数据，将面临数十亿美元罚款

当地时间 7 月 12 日，国会议员透露了业绩对报税公司进行为期七个月的调查。立法者发现，H&R Block、TaxAct 和 TaxSlayer 多年来与谷歌和 Meta“不计后果地共享”了数亿纳税人的敏感个人和财务数据，明显违反了禁止纳税人在未经客户同意的情况下共享纳税申报信息的法律。

国会议员的报告称，“这些公司共享了数百万纳税人的纳税申报数据，这意味着它们可能面临数十亿美元的潜在刑事责任。”来自 The Markup 的调查显示，纳税申报网站一直在与 Meta 共享客户的敏感财务信息。在被 Markup 联系后三个报税网站都证实了他们删除或禁用了收集敏感数据的 Meta Pixel 跟踪工具。

https://mp.weixin.qq.com/s/B_BV4z7k-2KQx09KKVV00g

2、浙江农商联合银行被罚 380 万，涉数据安全管理缺失等 11 项违规

国家金融监督管理总局网站 7 月 14 日披露，浙江农村商业联合银行股份有限公司因数据安全管理缺失等 11 项违法违规事实，被中国银保监会浙江监管局罚款 380 万元。该

行存在清退风险资金不及时、清算资金管理不规范、违规使用资金等问题，并对员工贷款行为管理不力。此外，还存在报表填报错误、数据安全管理缺失、审计履职不足等问题，以及漏报部分员工及其近亲属入股情况。

https://mp.weixin.qq.com/s/92E265uLxQQGsETqMWiRKw

3、双重伤害！雅诗兰黛同时遭遇两个勒索软件的攻击

7 月 19 日，据外媒报道，两个勒索软件攻击者 ALPHV/BlackCat 和 Clop 在其数据泄露网站上都将美容公司雅诗兰黛列为攻击的受害者。

在周二提交给美国证券交易委员会 (SEC) 的文件中，雅诗兰黛公司证实了其中一次攻击，称威胁行为者获得了其部分系统的访问权限，并可能窃取了数据。

Clop 勒索软件团伙利用 MOVEit Transfer 平台中的漏洞进行安全文件传输，从而获得了对该公司的访问权限。在他们的数据泄露网站上，Clop 勒索软件列出了雅诗兰黛，并注明他们拥有超过 131GB 的公司数据。

BlackCat 也将雅诗兰黛添加到了受害者名单中，该条目还附有一条消息，显示威胁行为者对该公司对勒索电子邮件保持沉默表示不满。BlackCat 暗示，泄露的信息可能会影响客户、公司员工和供应商。

雅诗兰黛对 BlackCat 的沟通没有做出回应，这表明该公司不会与威胁行为者进行任何谈判。

https://www.bleepingcomputer.com/news/security/est-e-lauder-beauty-giant-breached-by-two-ransomware-gangs/

4、因一低级漏洞，孟加拉国政府网站泄露约 5000 万公民身份数据

安全内参 7 月 12 日消息，孟加拉国出生与死亡登记主管办公室网站泄露了大量公民个人信息，包括全名、电话号码、电子邮箱地址和国民身份证号码。

6 月 27 日，Bitcrack 网络安全公司研究员 Viktor Markopoulos 意外发现了此次数据泄露，随后联系了孟加拉国电子政务计算机事件响应小组（CIRT）。

Markopoulos 表示，估计该网站泄露了约 5000 万孟加拉国公民的数据。据悉该国总人口约 1.63 亿。

https://www.secrss.com/articles/56572

5、HCA 医疗遭遇黑客攻击，泄露 1100 万患者敏感信息

7 月 11 日，Security Affairs 网站披露，HCA 医疗公司近期披露了一起网络攻击事件，约 1100 万患者的个人信息遭到泄露。

该组织于 7 月 5 日发现了这一安全漏洞，当时一名威胁行为者在一个地下论坛上声称遭受了黑客攻击。作为黑客攻击的证据，威胁行为者发布了一些患者的被盗信息，包括：患者姓名、城市、州和邮政编码、患者电子邮件、电话号码、出生日期、性别等。

https://securityaffairs.com/148371/data-breach/hca-healthcare-data-breach.html

6、Tampa General 医院遭到攻击影响 120 万患者的信息

媒体 7 月 19 日称，美国佛罗里达州的 Tampa General 医院约 120 万患者的信息泄露。该医院称其在 5 月 31 日发现其遭到了攻击，但没有透露攻击者的名字。其声明没有提及任何关于赎金要求的问题，并指出他们的安全部门能够防止文件被加密。泄露数据可能包括姓名、地址、电话、健康保险信息、社会安全号码和治疗信息等。Snatch Team 已将该医院添加到其网站中，没有提供任何勒索证据，但是声称已从医院获取了 4 TB 的文件。

https://www.databreaches.net/tampa-general-hospital-confirms-cybersecurity-incident-1-2-million-patients-being-notified/

7、Henry Ford Health 遭到钓鱼攻击近 17 万患者信息泄露

7 月 17 日报道称，Henry Ford Health 透露其遭到钓鱼攻击，导致 168000 名患者的信息泄露。受影响患者在本周一被告知，攻击者于 3 月 30 日获得了企业电子邮件帐户的访问权限。但该机构很快发现了这种访问。受影响的邮件中包含部分患者信息，这是在 5 月 16 日发现的。泄露的信息可能包括姓名、性别、年龄、化验结果、手术类型、诊断、医疗记录编号和内部跟踪编号等。该机构称其正在加强安全措施并为员工提供进一步培训。

https://www.clickondetroit.com/news/local/2023/07/17/henry-ford-health-confirms-data-breach-affecting-168000-patients/

8、今年最大规模网络攻击：受害机构数量逼近 400 家，影响人数超 2 千万

7 月 21 日消息，利用 MOVEit 文件传输软件漏洞实施的大规模软件供应链攻击已经进入第七周，受害者数量和损失持续攀升。

今年 5 月下旬，俄罗斯勒索软件组织 Clop 利用美国 Progress Software 公司旗下产品 MOVEit 的一个安全漏洞，从易受攻击网络中窃取大批文件。截至目前，已有近 400 家组织受到影响，其中不乏美国能源部等联邦机构、能源巨头

壳牌、德意志银行、普华永道、零售巨头 TJX 等知名公司机构。

据网络安全厂商 Emsisoft 统计，截至 7 月 19 日，共有 383 家组织和超过 2 千万个人遭受这次攻击。该统计的数据来源包括泄露通知、美国证券交易委员会（SEC）公告、其他公开数据及 Clop 团伙的泄露网站。

Emsisoft 团队指出，一些受到 MOVEit 漏洞影响的公司为许多其他组织提供服务。

https://www.secrss.com/articles/56932

9、明尼苏达大学遭遇数据泄露事件

7 月 21 日，据外媒报道，一名用户名为“niggy”的暗网用户在暗网论坛上声称对明尼苏达大学数据泄露事件负责。

据该用户称，该大学的数据库遭到未经授权的访问，可能会泄露敏感信息，包括超过 700 万个唯一的社会安全号码 (SSN)。

黑客声称利用 Computer Niggy Exploitation (CNE) 访问了该大学的数据仓库，其中包含自 1989 年以来数字化的记录。该数据库系统存储了有关学生、教职员工的宝贵且敏感的信息。现阶段黑客说法的真实性尚未得到证实，这让明尼苏达大学及其社区对该数据泄露事件的潜在严重程度感到

担忧。

https://thecyberexpress.com/university-of-minnesota-data-breach/

10、在线游戏平台 Roblox 遭遇数据泄露

7 月 20 日，据外媒报道，在线游戏平台 Roblox 泄露了 4000 名用户的个人信息。

Roblox Corporation 于 7 月 20 日证实了此次泄露事件。泄露的列表以 CSV 格式共享，包含 4000 个唯一的电子邮件地址，以及姓名、用户名、出生日期、电话号码以及实际地址和 IP 地址等个人详细信息。由于该数据泄露事件，许多用户已经开始收到恶意电话、短信和电子邮件。

https://www.infosecurity-magazine.com/news/old-roblox-data-leak-resurfaces/

11、VirusTotal 就影响 5,600 名客户的数据泄露事件道歉

7 月 21 日报道，上个月，由于一名员工错误地将包含客户信息的 CSV 文件上传到 VirusTotal 平台，在线恶意软件扫描服务产品 VirusTotal 因泄露 5,600 多名客户的信息而道歉。

数据泄露仅影响高级帐户客户，上传的文件包含他们的

姓名和公司电子邮件地址。据报道，泄露的 313KB 文件包含与美国官方实体相关的账户详细信息，包括网络司令部、司法部、联邦调查局 (FBI) 和国家安全局 (NSA)。

该平台主管向受影响的客户保证，该事件是由人为错误引起的，而不是网络攻击或 VirusTotal 的任何漏洞造成的。此外，只有拥有该平台高级帐户的 VirusTotal 合作伙伴和网络安全分析师才能访问泄露的文件。使用匿名或免费帐户的用户无法访问高级平台，因此无法访问泄露的文件。

https://www.bleepingcomputer.com/news/security/virustotal-apologizes-for-data-leak-affecting-5-600-customers/

12、PokerStars 扑克之星数据泄露暴露超过 11 万客户

7 月 21 日报道，全球最大的在线扑克网站 PokerStars 表示，它已成为 MOVEit Transfer 攻击的受害者，攻击者访问了敏感的用户数据。

MOVEit 零日漏洞允许恶意团伙访问 MOVEit Transfer 服务器并提取某些信息，受害者使用了这些服务器存储和共享数据。根据 PokerStars 向缅因州总检察长提供的信息，此次泄露事件暴露了 110,291 人的个人信息。暴露的文件包含个人用户详细信息，包括姓名、地址和社会安全号码。

PokerStars 扑克之星表示，到目前为止，没有迹象表明这

些数据被滥用，该公司将向受害者免费提供 24 个月的第三方身份保护服务。

https://cybernews.com/news/pokerstars-data-breach/

13、国际汽联世界耐力锦标赛车手护照数据泄露

7 月 19 日报道，Cybernews 的研究人员发现了两个配置错误（即公开暴露）的 Google Cloud Storage 存储桶。两者合计包含超过 110 万个文件。其中包括国际汽联世界耐力锦标赛（FIA WEC）车手的数百本护照、政府签发的身份证件和驾驶执照。

此类数据库的公开暴露意味着任何人都可以轻松访问并滥用敏感数据。未经授权披露个人数据的事件违反了《通用数据保护条例》（GDPR）。

https://securityaffairs.com/148587/security/fia-world-endurance-championship-data-leak.html

《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