全球数据安全观察

总第 143 期 2023 年第 24 期

（2023.08.21-2023.09.03）

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、国务院办公厅印发《政务服务电子文件归档和电子档案管理办法》

8 月 22 日，国务院办公厅印发《政务服务电子文件归档和电子档案管理办法》，要求各级政务服务机构应当依托全国一体化政务服务平台，积极推进政务服务办理系统与电子档案管理信息系统衔接。按照档案管理相关要求，做好电子档案登记、日常检查、转换、迁移、鉴定、销毁等工作，并且按照国家有关规定向档案馆移交。档案馆应当做好政务服务电子档案接收工作，提升安全管理水平，确保电子档案的真实性、完整性、可用性和安全性。

https://www.gov.cn/zhengce/content/202308/content_6899493.htm

2、财政部印发《企业数据资源相关会计处理暂行规定》

8 月 21 日，财政部印发《企业数据资源相关会计处理暂行规定》，进一步强化数据资源相关信息披露，将有助于为有关监管部门完善数字经济治理体系、加强宏观管理提供会计信息支撑，也为投资者等报表使用者了解企业数据资源价值、提升决策效率提供有用信息。

http://kjs.mof.gov.cn/zhengcefabu/202308/t20230821_3903354.htm

3、五部门发布《关于规范货币经纪公司数据服务有关事项的通知》

8 月 25 日，国家金融监督管理总局、中国人民银行、中国证券监督管理委员会、国家互联网信息办公室、国家外汇管理局发布《关于规范货币经纪公司数据服务有关事项的通知》，就四方面具体内容作出规范：加强数据治理，确保数据安全；规范提供数据标准，提高数据服务质量；明确可接受数据服务的机构范围，加强合作管理；签订服务协议，规范数据使用。

https://www.cbirc.gov.cn/cn/view/pages/governmentDetail.html?docId=1124968&itemId=861&generaltype=1

4、市场监管总局发布《市场监督管理行政执法电子数据取证暂行规定 （征求意见稿）》

8 月 22 日，市场监督总局就《市场监督管理行政执法电子数据取证暂行规定 （征求意见稿）》公开征求意见。明确电子数据收集提取、查封扣押、检查分析、证据存储等方面的规定，解决市场监管行政执法中电子数据取证难题，为市

场监管行政执法电子数据取证工作提供清晰指引和有效方案。

https://www.samr.gov.cn/hd/zjdc/art/2023/art_cdb50d1a24374b97a6e4f2ec2a9e629c.html

5、《北京市扫码消费服务违规收集使用消费者个人信息案例解析及合规指引》发布

近期，北京市网信办按照消费者真实扫码消费体验过程中可能遇到问题的先后顺序，整理出六类违规问题，制定《北京市扫码消费服务违规收集使用消费者个人信息案例解析及合规指引》，并予以公开发布。主要的六类违规问题包括强制或诱导消费者关注公众号，未通过弹窗等显著方式告知消费者隐私政策，频繁提示注册登录、干扰消费者使用，强制消费者提供与功能无关的个人信息，违规向第三方提供消费者个人信息，以及未向消费者提供删除个人信息的功能选项。

https://mp.weixin.qq.com/s/3e3dw6V4M0wds3TQlFWz6w

6、《贵州省数据要素登记管理办法（试行）》（征求意见稿）公开征求意见

8 月 31 日，贵州省大数据局发布《贵州省数据要素登记管理办法（试行）》（征求意见稿），规定了数据要素的登记内

容包括：数据要素名称、数据要素类型、数据要素适用场景、数据要素实现方式、其他应当予以登记的事项，从总则、登记机构、登记主体、登记内容、登记程序、登记类型、安全管理和附则 8 个方面提出数据要素登记管理要求。

https://dsj.guizhou.gov.cn/opinion/202308/tOpinion_14584.html

7、《信息安全技术 重要数据处理安全要求》等多项数据安全国家标准发布征求意见稿

8 月，多项数据安全国家标准发布征求意见稿，包括：《信息安全技术 重要数据处理安全要求》、《信息安全技术 数据交易服务安全要求》、《信息安全技术 数据安全风险评估方法》、《信息安全技术 基于个人信息的自动化决策安全要求》、《信息安全技术 敏感个人信息处理安全要求》。

https://www.secrss.com/articles/58208

8、深圳市地方标准《企业合规管理体系》发布

8 月 14 日，深圳市地方标准《企业合规管理体系》发布，明确了企业合规管理体系的基本原则，规定了企业合规管理体系建设中的企业环境、领导作用、策划、支持、运行、绩效评价、持续改进等方面的管理要求。

http://www.sz.gov.cn/cn/xxgk/zfxxgj/tzgg/content/post_1078334

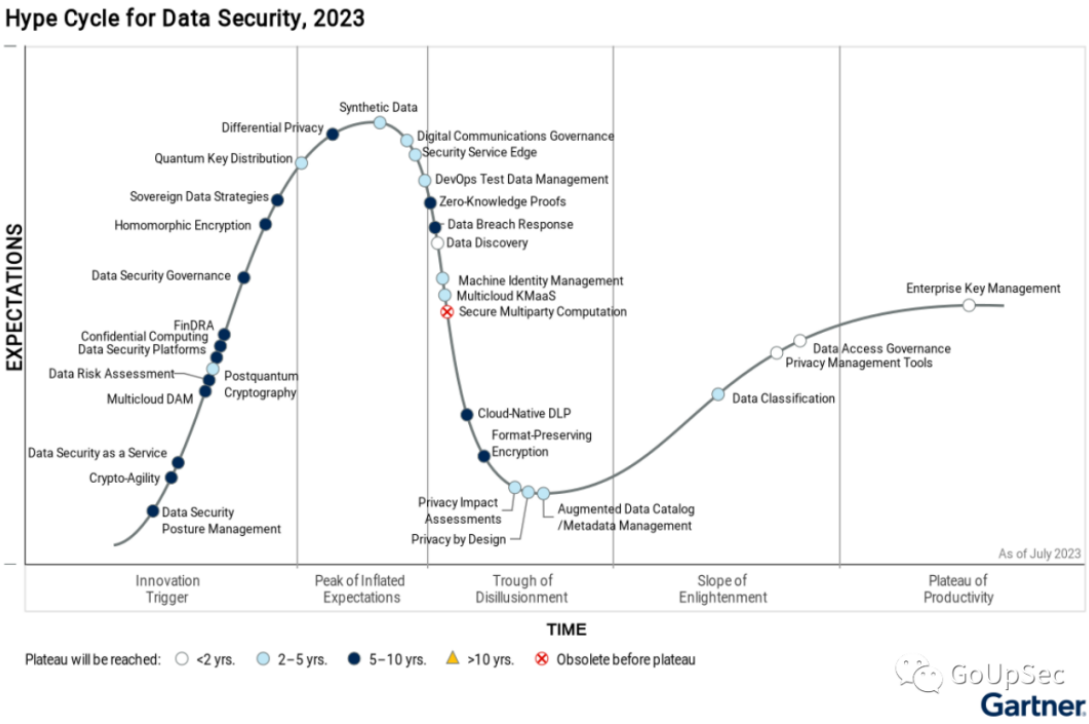
7.html

技术、产品与市场

1、Gartner：2023 年数据安全五大新兴技术

Gartner 最新发布的 2023 数据安全技术成熟度曲线（炒作周期图）增加了五项新技术：**加密敏捷性、后量子密码学、量子密钥分发、主权数据策略和数字通信治理**。此外，今年有八项技术被删除或重新分配。

Gartner 指出，一些 CISO 已经将量子计算视为一种不断变化的潜在威胁进行监控，并将监控委托给战略 IT 规划团队。Gartner 还在今年的技术成熟度曲线（下图）中引入了加密敏捷性，以满足客户对该领域尽可能多的数据和知识的要求。



Garnter 表示，企业级数据安全集成是一个艰巨的挑战，Gartner 预测这些挑战将改变或整合数据安全技术，包括数据安全态势管理(DSPM)、数据安全平台(DSP)和多云数据库活动监控(DAM)。

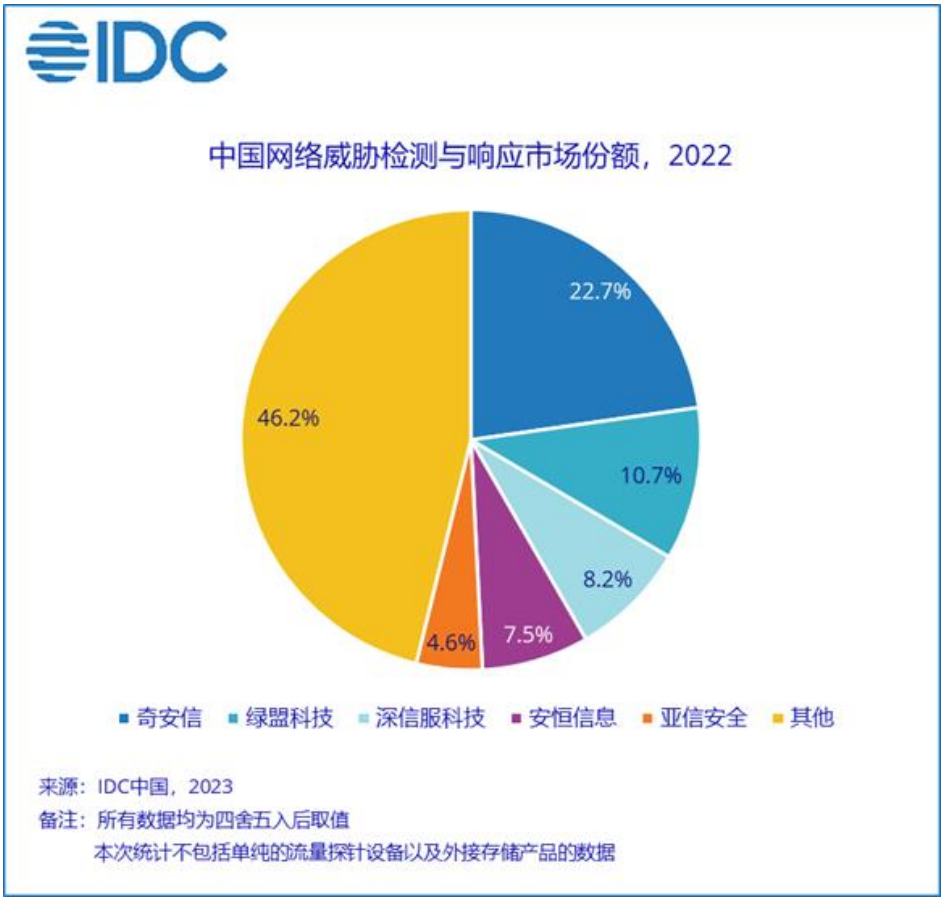
https://www.secrss.com/articles/58407

2、IDC：2022 年中国网络威胁检测与响应市场规模达到 3.5 亿美元

IDC 于近日正式发布了针对中国 NDR 的市场份额研究报告，即：《中国网络威胁检测与响应市场份额，2022：技术提升，市场下沉》（#CHC50358323）。报告针对 2022 年中国 NDR 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 NDR 产品的市场规模达到 3.5 亿美元，同比增长 13.7%。从市场份额来看，奇安信、绿盟科技、深信服科技、安恒信息、亚信安全等综合性安全厂商组成了该市场的主要玩家，具体情况详见下图：



https://www.secrss.com/articles/58067

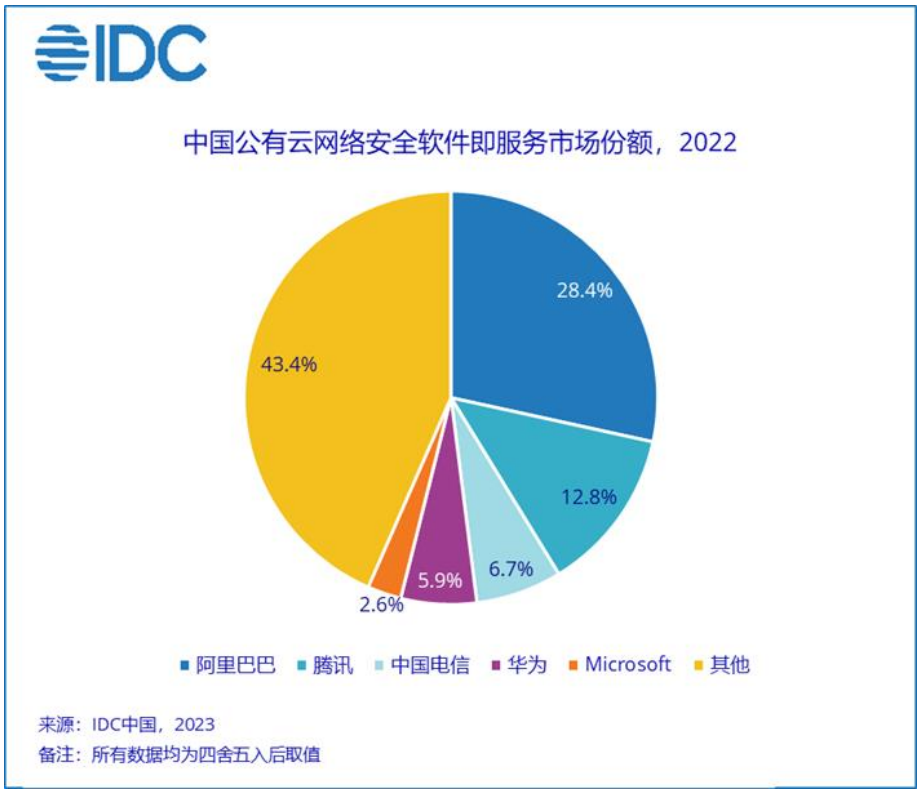
3、IDC：2022 年中国公有云网络安全软件即服务市场规模达 10.5 亿美元

全球数字化发展已经进入普及的临界点，IDC 研究显示，

到 2023 年底，全球数字化转型支出占总体企业 ICT 支出将达到 52%，全球 52%的软件应用支出也将是 SaaS 模式。2022 年，中国云计算市场迎来重要拐点，市场从规模发展向高质量发展转变，公有云网络安全软件即服务市场的发展也随之产生变化。

IDC 于近日正式发布了针对中国网络安全即服务市场份额研究报告，即：**《中国公有云网络安全即服务市场份额，2022：头部效应显著，市场期待更多强者涌现》（#CHC50357823）**。报告针对 2022 年中国公有云网络安全软件即服务市场的规模、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，中国公有云网络安全软件即服务市场在 2022 年实现了 15.5%的同比增长，规模达到 10.5 亿美元。目前，中国公有云网络安全软件即服务市场仍然以在网络安全领域持续投入的国内公有云服务提供商为主，且头部效应显著，例如阿里巴巴、腾讯、中国电信、华为等，具体情况详见下图：



https://www.secrss.com/articles/58277

4、企业警惕：浏览器插件风险高达 51%，或引发敏感数据被窃

一项新的研究发现，组织允许员工在使用软件即服务（SaaS）应用程序（如 Google Workspace 和 Microsoft 365）时使用的许多浏览器扩展可以访问高级别的内容，并存在数据盗窃和合规性问题等风险。

Spin.AI 的研究人员最近对企业环境中使用的约 300,000 个浏览器扩展和第三方 OAuth 应用程序进行了风险评估。重点是跨多种浏览器(例如 Google Chrome 和 Microsoft

Edge）的基于 Chromium 的浏览器扩展。

研究显示，所有已安装的扩展中有 51%具有高风险，有可能对使用它们的组织造成广泛损害。这些扩展程序都能够从企业应用程序捕获敏感数据，运行恶意 JavaScript，并秘密向外部各方发送包括银行详细信息和登录凭据在内的受保护数据。Spin 评估的大多数扩展（53%）都是与生产力相关的扩展。但最糟糕的——至少从安全和隐私的角度来看——是云软件开发环境中使用的浏览器扩展，Spin 评估其中 56%为高安全风险。

https://mp.weixin.qq.com/s/iroFqYWp2EcR6Q0AeURlGQ

5、《2023 联邦学习全球研究与应用趋势报告》发布

在第 32 届国际人工智能联合会议（IJCAI）上，清华大学人工智能研究院知识工程研究中心（KEG）、北京智谱华章科技有限公司、开放群岛开源社区合作发布了《2023 联邦学习全球研究与应用趋势报告》。

报告指出：中美持续引领全球联邦学习发展，研究重点逐渐转向算法模型和安全隐私技术，行业应用越来越成熟，应用方向则呈现更多与物联网、区块链、客户端、电子设备等融合的态势。中国已经成为联邦学习技术的深度参与方，国内企业和科研机构积极参与联邦学习的技术研发和应用，

以及标准制定。未来，随着人工智能技术和应用的不断升级，联邦学习的技术研发仍将较多聚焦于数据安全与隐私保护，其应用场景还将进一步扩大和深入。

https://mp.weixin.qq.com/s/A_NrJu5S1AtcKLAyp7BTwA

业界观点

1、人民时评：让人脸信息得到更有效保护

不久前，国家网信办公布《人脸识别技术应用安全管理规定（试行）（征求意见稿）》（以下简称征求意见稿），就人脸识别技术的使用条件、使用禁则、备案要求、数据保护、设备管理等向社会公开征求意见，对保护个人信息权益、维护社会秩序和公共安全具有现实意义。用好人脸识别技术，必须做好从数据收集、使用到备案、删除等全过程监管，并提供较高级别的安全保护。

规范人脸识别技术应用，“安全”应成为绝对的关键词。首先要把住信息采集入口关。征求意见稿提出，只有在具有特定的目的和充分的必要性，并采取严格保护措施的情形下，方可使用人脸识别技术处理人脸信息。这样具有很强针对性的界定，能有效防止人脸信息的非必要采集。比如，在健身房、书店等消费场景中，即便智能设备更加便捷，也应把消

费方式的选择权交给消费者，而不能把采集人脸信息作为前置条件。确有必要时，应当取得个人的单独同意或者依法取得书面同意。以当事人知情、同意为基础，确保个人信息主体享有撤回授权的权利等，有助于为新技术规范应用划清边界。

防范人脸识别技术滥用风险，要加强对数据使用的监管，全面提高信息安全保护力度。面向社会公众提供人脸识别技术服务的，相关技术系统应当符合网络安全等级保护第三级以上保护要求。第三级是除了金融机构之外，可以用到的最高等级。此外，除法定条件或者取得个人单独同意外，人脸识别技术使用者不得保存人脸原始图像、图片、视频，经过匿名化处理的人脸信息除外。将相关服务限定在最小必要的时间、地点或者人群范围内，才能把风险降到最低。

人脸识别具有独特的技术优势，是促进数字经济发展和社会治理的有效技术手段。然而，人脸属于生物识别类敏感个人信息，对此类信息的采集应出于维护公共安全的需要，并保障公民的知情权、决定权、选择权、删除权。在发展人脸识别技术的进程中，统筹发展和安全，不断完善相关法律法规，增强监管政策针对性、系统性，增强处理个人信息的敏感度，就能在有效保护个人信息的前提下，更好地促进行业健康发展，使广大群众从技术进步中受益。

http://jl.people.com.cn/n2/2023/0828/c349771-40547251.html

2、沈昌祥院士：企业家要牢记“安全可信”

8月27日，由中国电力企业联合会、中国中小企业协会、协鑫集团主办的“长三角数字能源算力大会暨专精特新产业融合发展论坛”在苏州举办。会上，中国工程院院士沈昌祥以“开创安全可信算力新生态”为题作主旨演讲。

在发展数字产业时，加工过程中只留下精品，很多“废料”数据都被扔掉了，这就是大数据。因此，我们扔掉的这些数据，一定要收集出来，再加工、再处理，成为新型的数字产品，然后继续加快产业数字化。

安全是发展的前提。我们要打造安全可信算力网络。党的二十大报告提出建设网络强国、数字中国，我们应当研究什么？算力是怎么要求的、怎么落地的？我们应当统筹规划，控制生态网络安全，推广安全可信的网络产品，保护知识产权，产学研相结合。

我建议各位企业家，牢记安全可信四个字。安全可信是计算公司进行动态全方位的保护，计算任务的逻辑组合一定要达到预期的计算目标，这相当于我们人有免疫能力，保证健康生活。

主动免疫、积极发育的保障体系，是历史的使命，是战

略的任务。我们在上世纪 90 年代初就提出，以密码为基因的城市课题，相当于网络信息具有了免疫能力，因为杀病毒、打补丁就是要全面。

我国等级保护，关键技术落实，基本要求兼容，实际要求标准，网络化、数字化、智能化，所以我们数字化的系统，体现在可信的计算环境，不仅仅是防火墙那么简单，要动态变化。

2006 年，中国提出以发展高可信网络为主的开发发展技术保障体系，因此我国重要信息系统已经安全可信了。电网、能源一定要安全可信，我们现在已经完成了产业链，公安部成立了国家等级保护 2.0，可信计算 3.0 有两款，一个是 ARM 架构的沸腾，一个是 X86 架构的。在没有可信 CPU 以前，就是一边工作一边进行检查，因此产生了巨大的产业空白。

因此，等级保护 2.0，是不同等级的安全可信强度，我们的电力系统，能源是技术的基础，必须安全可信才能保证能源稳定。

数据四要素是能源、算力、算法、数据，联合起来才是安全可信。

https://new.qq.com/rain/a/20230829A04P3100

3、北京交通大学信息管理理论与技术国际研究中心：数据要素的 20 大特性及其影响

数据具有虚拟性、非稀缺性、易复制性等 20 个独特的特性，每一个数据特性对数据产权、生产加工、流通交易、收益分配、安全监管等方面都有不同的影响。

1. 虚拟性：不同于土地、劳动力、资本等可见的、具有物理形态的传统生产要素，数据具有不可见、没有具体实物形态的特性。尽管数据需要依附于各种实物载体，但数据作用的发挥和数据价值的大小取决于数据本身。

2.非稀缺性：也称数据的无限性，主要指不同于土地、劳动力等传统生产要素，数据不仅不会因使用而耗费，反而会在使用过程中产生新的数据，并随着被使用次数的增多而新创造的数据量越来越多，因此数据是非稀缺的，数据供给也是无限的。

3.原始性：数据是构成人类知识体系中最底层、最原始、本身不具有实际价值的最基本单元。

4.易复制性：数据可以快速地以近乎零成本的方式进行复制，供多人同时使用，多次循环使用，一个人的使用可以不排斥和妨碍别人对其使用，不同人之间在使用上不存在直接的利益冲突。

5.多环节性：数据价值的形成需要经过采集、存储、加

工、流通、应用以及生态保障等不同环节。

6.非消耗性：数据不仅可以无限制地重复使用，不会因为使用而减少其价值，而且数据在使用过程中不仅不会产生消耗，反而会在数据的生产、共享和交换产生更多数据和更大的价值。

7.非排他性：也称非竞争性，是指同一个数据可被不同主体重复采集，存储在各家数据中心，数据被一个主体使用时并不影响其他主体的使用。

8.非均质性：数据的非均质性特点具有三两方面含义，一是数据价值因不同数据质量而异，相同单位量纲下的不同数据的价值完全不同；二是数据价值因应用场景而异，同一份数据对不同应用场景的价值不同；三是数据价值因使用对象而异，同一份数据对不同人的价值也不一样。

9.边际效应递增性：随着数据使用量和使用次数的增加，数据规模会越来越大、种类会越来越多、使用效用越来越大，具有边际效应递增特性。

10.交易不确定性：由于数据质量不可见、人为因素不可控、数据质量预期模糊等因素，而在数据交易过程中易产生的逆向选择、道德风险及交易对象不清等三类交易成本，造成数据交易的不确定性。

11.时效性：也称为易腐性，一方面是指数据是一种易腐

品，数据蕴含的经济价值会随着时间的流逝而迅速贬值；另一方面是指数据的贬值速度取决于数据类型、用途和具体业务场景等。

12.场景依赖性：一方面是指同一项数据在不同应用场景下的价值完全不同；另一方面是指在一种场景下的应用功能，可能会通过不同来源的数据实现。

13.“阿罗信息悖论”：“阿罗信息悖论”是诺贝尔经济学奖得主肯尼斯.阿罗于 1963 年在《不确定性与医疗保健经济学》中提出的。其基本含义是交易需要披露信息，但披露信息即意味着数据价值的丧失。无论是交易前要求部分数据内容的披露，还是交付后对交易数据不断使用与泄露，都会或多或少减少数据价值，造成数据贬值甚至数据交易买方从其他渠道低成本获取数据。

14.价值不确定性：也称数据价值易变性，一是随着时间推移变化，一些当前没有价值的数据可能会产生更大的价值；二是随着技术的进步或者可替代性数据的出现，尤其是生成式人工智能产生的大量涌现性和泛化性数据，可能会导致数据资产出现无形损耗，表现为价值降低。

15.功能替代性：不同的数据在功能上可能是相互替代的，一方面是不同数据采集机构采集的很多数据项是相同的；另一方面是来源不同的数据，其实现的功能可能是趋同的。

16.协同性：也称关联性，即来源不同的异质性数据可以带来不同的价值，由异质性数据组成的维度不同的数据集，其价值常常会超过单一数据生产价值的总和。

17.多样性：数据有单一形态数据和融合形态数据，而单一形态数据的表现形式多种多样，可以是数字、表格、图像、声音、视频、文字、光电信号、化学反应、甚至是生物信息等，融合形态数据的表现形式则更为丰富，有数字、表格、图像、声音、视频、文字等的多模态数据，也有通过数字媒体与数字制作特技产生的各种融合数据等。随着数字技术的快速进步，不同形态的数据可以互相转换。

18.规模性：数据的规模性有三方面含义：一是指数据的数量，数据的数量越大，其价值越高；二是指数据的质量，数据越完整，其价值越高；三是指数据速度，包括数据的加工速度和数据的流动速度，数据的加工速度越快，其价值越高，而数据的流动速度越快，数据就越容易贬值。

19.可加工性：虽然数据只是由 0 和 1 两个二进制数字组成的数字串和其他虚拟形态，但是，数据可以被编码、标注、记录和还原，打造一个与现实世界并行的数字虚拟世界；也可以被维护、更新、补充，增加数据规模；还可以被删除、合并、归集，提高数据质量；并还可以被分析、提炼、挖掘，形成各种层次的数据资源、数据产品和数据资产。

20.流动性：数据的流动性有两方面含义：一是数据流动起来后，能够有效贯通生产、分配、流通、消费等全过程，优化各类要素的配置组合，从而实现对经济的放大、叠加、倍增效应；二是数据流动汇聚起来后，能够呈现和反映个人、企业、社会和国家的整体整体动态和需求，为个人更便捷生活、企业更有效运营、社会更有效运转等方面提供更加全面、完整的决策依据。

https://www.secrss.com/articles/58210

4、解析银行业数据安全与隐私保护监管热点

通过对 2023 年国家及银行业最新发布的数据安全与隐私保护监管规定的解析，普华永道整理总结了如下三大监管热点：数据出境合规管理、数据安全合规管理、个人信息保护合规审计。

基于上述监管热点分析可知，国家及行业对数据安全合规的要求正持续更新且不断强化，行业监管对银行业金融机构的数据安全实践也将进行更严格的审查和监督。但银行业务场景复杂，各业务场景均可能涉及不同的内外部相关方、数据流程、数据存储系统/应用、使用目的等，数据合规需要管理非常复杂和多元的数据生态系统。如下总结了银行业数据安全合规的主要挑战：持续更新演变的监管要求、监管加

强执法力度及信息报送要求、监管加强执法力度及信息报送要求、监管加强执法力度及信息报送要求、监管加强执法力度及信息报送要求。

为有效应对银行业数据安全合规挑战，普华永道建议通过以下步骤，尽快推动银行的数据安全合规工作:

步骤一：数据资产识别与梳理

建立跨部门、跨职能的合作与协调机制，尽快梳理关键业务活动和数据场景，开展数据调研及盘点工作，包括数据类型分析、个人信息和敏感个人信息梳理、数据全生命周期流转分析等。通过前述数据资源目录(数据资产)梳理工作，银行可建立完整的数据资产清单，作为后续数据管理的基础，并应指定相关负责人持续更新该清单以反映最新情况。

步骤二：数据安全与隐私保护管理现状及合规差距识别

基于步骤一的业务及数据资产梳理，盘点适用的数据安全监管要求，包括《网络安全法》《数据安全法》《个人信息保护法》，以及网信办、工信部、中国人民银行、国家金融监督管理局出台的监管要求和金融行业指南等。银行应对标适用的监管要求，了解并分析自身当前数据全生命周期安全管理现状，识别潜在的合规差距，评估合规风险，并制定整体合规行动计划。

步骤三：数据安全与隐私保护合规整改路径规划

根据识别的合规差距，建立具体的整改方案，并根据合规风险评估结果对各项整改工作进行优先排序，明确整改完成时间，指定各项整改工作的负责人，建立具体的整改实施路线图。特别是针对合规高风险领域，如数据出境合规、数据分级分类管控、重要数据识别与定期监管报送、数据风险监测等，需要制定有效的合规方案以应对监管合规风险。

步骤四：数据安全与隐私保护管理体系完善

加强数据安全与隐私保护合规管理体系，包括完善机构内的合规管理架构与职责划分，建立数据生命周期安全管理的制度及流程，包括管理措施、技术措施以及第三方安全管理措施，个人信息保护管理流程（包括“同意”与“单独同意”管理流程、个人信息保护影响评估流程、数据主体权利响应流程、数据出境合规流程等）以及对监管机构报告及响应流程等。

步骤五：持续风险监测与合规监督

采取有效技术措施，强化数据处理活动安全风险监测和告警，加强数据安全风险情报的监测以及风险缓释措施的制定，建立数据安全事件定级判定、响应处置以及向监管报告的流程，以便实时跟踪异常活动，增强数据安全保护水平。此外，银行业金融机构应加强对数据安全与个人信息保护合规的监督管理，定期开展数据安全风险评估以及数据安全与

个人信息保护合规审计。

https://www.chnmc.com/wisdom/Insights/2023-08-24/19303.html

5、中国移动发布《智慧城市数据安全白皮书》

智慧城市是推动城市治理体系和治理能力现代化建设的重要抓手。“十四五”期间国家对数字经济和智慧城市发展进行了专项规划，智慧城市作为数字经济的重要应用场景，其数据巨大价值和重要意义得到强调和凸显。

2023 年 8 月 24 日-26 日，由四川省互联网信息办公室指导，成都市互联网信息办公室、成都高新技术产业开发区管理委员会联合主办的“2023 CCS 成都网络安全大会”在成都召开。会上《智慧城市数据安全白皮书》正式公开。白皮书梳理智慧城市数据安全需求，提出智慧城市数据安全总体框架、内外部数据安全解决方案，给出智慧城市数据安全发展建议，并基于四川成都、雄安新区、江苏无锡智慧城市数据安全实践案例，系统阐述了数据安全方案落地具体场景。展望未来城市发展，旨在为进一步推广、普及和完善智慧城市数据安全治理的理念、方法、体系与应用贡献力量。

中移雄安信息通信科技有限公司数智创新部安全技术专家李子晔在《智慧城市数据安全防护体系建设思考》的主

题分享中提到，数据要素及其安全在智慧城市建设中具有重要意义。为防范和化解智慧城市面临的各类数据安全风险，顺应未来智慧城市数据安全发展方向，保障和推动智慧城市高质量高速发展，白皮书从智慧城市顶层设计、数据处理周期安全、安全管理运营、公共领域攻击防范四个层面提出智慧城市数据安全解决方案，确保智慧城市重要数据资源的保密性、完整性、可用性、真实性、可控性、不可抵赖性，满足国家对新型智慧城市数据安全保障工作的要求。

https://www.secrss.com/articles/58206

数据安全事件

1、Fitbit 可能因涉嫌违反 GDPR 而面临 11 亿欧元的罚款

8 月 31 日，据外媒报道，谷歌旗下的健康和健身公司 Fitbit 被提出三项投诉，因为该公司强迫新用户同意将高度个人化的数据传输到欧盟以外的地区。

该公司甚至有权与第三方公司共享数据进行处理，而无需向用户提供有关此类数据共享可能产生的影响的明确信息。共享数据不仅包括用户的电子邮件地址、出生日期和性别，还包括食物、体重、睡眠、饮水或女性健康跟踪日志等数据，以及讨论板上或在论坛上给您的朋友的消息。

根据 GDPR，每个人都有权撤回对数据共享的同意。然而，Fitbit 的隐私政策规定，撤回同意的唯一方法是删除帐户，这意味着丢失所有以前跟踪的锻炼和健康数据。

相关组织已要求奥地利、荷兰和意大利数据保护机构 (DPA) 命令 Fitbit 向用户提供有关数据传输的完整信息。考虑到谷歌母公司 Alphabet 上一年的收入，相关当局可能会处以高达 112.8 亿欧元的罚款。

https://cybernews.com/news/fitbit-violates-gdpr/

2、百信银行被罚 503 万元

近日，根据中国人民银行北京市分行最新公布的行政处罚信息公示，中信百信银行股份有限公司因涉 11 项违法行为类型，被给予警告，并处罚款 503.2 万元，作出行政处罚决定日期为 2023 年 8 月 20 日。另有三名相关负责人对相应违法行为负有责任，合计被罚 33.3 万元。

具体违法行为包括：未严格落实交易信息真实、完整、可追溯相关要求；未按规定对异议信息进行核查和处理；未按规定对异议进行书面回复；异议处理超期；提供个人不良信息，未事先告知信息主体本人；未准确、完整、及时地向金融信用信息基础数据库报送个人信用信息；未按照规定履行客户身份识别义务；未按规定使用格式合同；信息披露未以适当方式供金融消费者确认接收与其切身利益相关的完整信息；未按要求向金融消费者披露与金融产品和服务有关的重要内容；投诉数据漏报。

https://mp.weixin.qq.com/s/yzDiGGfs35hXnX3ppeEICg

3、Rhysida 团伙攻击美国医疗机构 PMH 并勒索 130 万美元

据媒体 8 月 27 日报道，美国医疗保健公司 Prospect Medical Holdings(PMH)遭到了勒索团伙 Rhysida 的攻击。攻击发生在 8 月 3 日，PMH 员工称在电脑上发现勒索信。之后

该医院关闭了 IT 系统以防止攻击在内网横向移动，并被迫使用纸质病例。Rhysida 表示对此事负责，并称他们获得了 1TB 的文档和一个 1.3TB 的 SQL 数据库，其中包含 500000 个社会安全号码、护照、驾驶执照、公司文件和患者的记录，还威胁要以 50 个比特币（价值 130 万美元）的价格出售被盗数据。

https://www.bleepingcomputer.com/news/security/rhysida-claims-ransomware-attack-on-prospect-medical-threatens-to-sell-data/

4、Forever 21 披露一起涉及近 54 万员工的数据泄露事件

据 8 月 30 日报道，时尚零售商 Forever 21 通知约 54 万名参与公司健康计划的员工，他们的信息已被泄露。Forever 21 称，他们在 3 月 20 日发现一起网络安全事件。随后的调查确定，攻击者在 1 月 5 日至 3 月 21 日访问了 Forever 21 的部分系统。虽然 Forever 21 没有并没有直截了当地说有勒索要求，但他们在信中的措辞表明，不仅有勒索要求，而且 Forever 21 还向攻击者交了赎金，以获得删除数据的保证。该事件影响了 539207 个人，他们将获得 12 个月的身份监控服务。

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

5、美国 PurFoods 遭到勒索攻击约 120 万用户的信息泄露

据媒体 8 月 28 日报道，美国餐饮公司 PurFoods 露了一起影响超过 120 万人的数据泄露事件。该公司称，它于 2 月 22 日发现其网络上的可疑活动。调查确定，攻击发生于 1 月 16 日至 2 月 22 日，导致部分文件被加密。深入调查于 7 月 10 日结束，发现黑客访问了驾照、身份证号、金融账户信息、支付卡信息和治疗信息等数据。此次数据泄露影响了客户、员工以及独立承包商，涉及 1237681 人，PurFoods 将通过 Kroll 为他们提供 12 个月的信用监控和身份保护服务。

https://therecord.media/purfoods-delivery-service-reports-data-breach

6、某供应商遭到攻击导致伦敦警局近 5 万员工的信息泄露

据 8 月 27 日报道，伦敦大都会警察局正在调查关于其 47000 名警官和工作人员的信息泄露事件。泄露数据包括姓名、照片、军衔、审查级别和身份证号等。此次数据泄露是由于负责打印授权卡和员工通行证的承包商的 IT 系统遭到攻击导致的。目前尚不清楚攻击者是出于经济动机，还是专门窃取警察和工作人员的信息。由于担心泄露数据被有组织的攻击团伙利用，国家犯罪局(NCA)已被要求调查此次数据泄露事件。

https://therecord.media/metropolitan-police-data-leak-hackers-uk

7、美国家安全委员会发生数据泄露: 近万个登录凭据曝光，波及 2000 家公司

Cybernews 的研究团队发现美国国家安全委员会(NSC)网站存在漏洞，泄露了约 2000 家公司和政府机构员工的凭证信息。这一漏洞涉及众多知名企业和机构，包括化石燃料公司、电子制造商、航空航天公司、制药公司、汽车制造商、政府实体、互联网服务提供商等。暴露的凭证可能被用于撞库攻击、访问公司网络或发起其他恶意行为。漏洞首次发现于 2023 年 3 月 4 日，暴露了包括电子邮件和密码在内的用户信息。建议 NSC 用户及时更改其密码，并注意密码安全。

https://www.secrss.com/articles/58467

8、因供应商被黑，法国政府机构泄露 1000 万民众个人信息

Bleeping Computer 网站披露，法国政府失业登记和金融援助机构 Pôle emploi 通报一起数据泄露事件，该事件泄露了 1000 万名民众的个人数据信息。

Pôle emploi 在新闻稿中声称其一家供应商的信息系统遭到网络破坏，可能会泄露求职者的个人数据信息，主要影

响 2022 年 2 月登记的求职者和就业中心的前用户。

https://www.secrss.com/articles/58257

9、TopGolf Callaway Brands 遭到黑客攻击，超过一百万高尔夫球手信息暴露

9 月 1 日，据外媒报道，经营一系列高尔夫中心的美国运动器材制造公司 TopGolf Callaway Brands 的超过一百万客户的个人信息被泄露，并将被要求更改密码。

Topgolf Callaway 于 8 月 1 日注意到其计算机网络上存在异常系统活动。对此事的调查表明，用户个人资料，包括姓名、邮寄地址、电子邮件地址、电话号码、订单历史记录、帐户密码和安全问题的答案都受到了影响。共有 1,114,954 人的私人信息遭到泄露。

https://cybernews.com/security/topgolf-callaway-brands-hacked-million-golfers-exposed/

10、杭马报名系统发生数据泄露故障，报名中断

8 月 28 日杭州马拉松官网报名页面崩溃，显示大量报名者的个人信息，包括真实姓名、手机号码、身份证号等等。随后，杭州马拉松官网已紧急关闭报名入口，暂停报名。

截至 29 日早上 7 时，报名仍然没有恢复。另有网友也

在社交媒体表示，登录自己的账号查询是否成功报名，却显示了他人信息，包括姓名、身份证号、家庭住址、手机号等。

https://mp.weixin.qq.com/s/HDlgEGHiLJBzMw-rdfJ2-g

11、Akira 再次出击：Jasper 高中 60GB 数据泄露

8 月 29 日，据外媒报道，Akira 勒索软件组织声称贾斯珀高中数据泄露，此漏洞是在威胁行为者常用的暗网渠道上披露的。

因其网络攻击而臭名昭著的 Akira 勒索软件组织已扩大其受害者名单，将贾斯珀高中纳入其中。令人震惊的是，该组织声称已获得该组织 60GB 的敏感数据的访问权限。然而，威胁行为者尚未分享在贾斯珀高中数据泄露事件中被盗的文件和文件夹的确切名称。

https://thecyberexpress.com/akira-jasper-high-school-data-breach-60gb/

12、美国派拉蒙披露了一起数据泄露事件

8 月 30 日，据外媒报道，美国娱乐巨头派拉蒙全球公司 (Paramount Global) 在其系统遭到黑客攻击且攻击者获取了个人身份信息 (PII) 后披露了一起数据泄露事件。

根据调查，个人信息可能包括用户的姓名、出生日期、

社会安全号码或其他政府颁发的身份证号码（例如驾驶执照号码或护照号码）以及与派拉蒙关系相关的信息。发现该事件后，该公司采取措施保护受影响的系统，并开始调查以确定违规的程度和范围。

https://www.bleepingcomputer.com/news/security/paramount-discloses-data-breach-following-security-incident/

13、GhostSec 黑客组织曝光伊朗政府监控软件，20GB 敏感数据遭泄露

2023 年 9 月 1 日报道，GhostSec 报告了 FANAP Behnama 软件的成功入侵，他们将其描述为“伊朗政权自己的隐私入侵软件”。此漏洞导致大约 20GB 的受感染软件暴露。该组织声称，伊朗政府使用该软件进行公民监视，这代表了该国监视能力的重大进步。

作为证据，该组织分享了该软件的部分源代码，展示了其独特的面部识别功能，增强了其监控效果。在过去的两个月里，该组织声称已经逐个文件仔细分析了大约 20GB 的压缩数据。Ghostsec 的目标是确保这些信息可以随时访问，帮助隐私受到损害的伊朗公民，并坚持全面隐私保护的必要性。

https://mp.weixin.qq.com/s/EMO_RQrEqmN-APHlWn_LyQ

《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