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. 004(总第 165 期)

责编：钟力 zhongli1@360.cn

导 读

第四期《数字安全观察 数据安全专刊》对 2022 年上半年数据安全形势进行了回顾与展望，以期为读者呈现数据安全发展的整体态势，本期分为上半年政策形势总结，上半年技术、产品与市场趋势盘点，上半年数据泄露态势分析以及专题文章四个板块，主要内容如下：

政策形势方面，全球均在加快制定并完善数字经济与数据安全相关政策法规。国际方面，上半年，美国、欧盟、法国、英国、韩国、泰国等国家纷纷加紧数据安全治理相关法治建设，世界各主权国家继续以“新孤立主义”的形态开展数据安全治理，同时通过“数据盟友”等多边、区域性合作规则推进数据流动；国内方面，我国正全方位推进数据安全相关政策法规的健全与落实，截至 6 月 30 日，已发布超过 30 项国家政策法规、超过 20 项行业监管要求以及近 30 项地方政策规章，同时数十项相关标准规范在加紧制定。

技术、产品与市场趋势方面，数据安全技术不断突破，市场增长明显。技术、产品方面，一是隐私计算领域的技术与产品不断涌现，取得了重要的创新突破，可信执行环境、同态加密等技术获得了企业的重点关注；二是安全大脑的概念正逐步推广，360 于 4 月份正式推出核心安全大脑 3.0，助力用户构建“能力中枢平台”，以此带动数字时代能力体系升级。市场方面，DLP、零信任、隐私增强计算、云计算等市场均得到了快速发展，尤其是隐私计算技术，据 Gartner 预测，

2025 年 60%的大型企业机构将在分析、商业智能或云计算领域使用一种或多种隐私增强计算技术。

数据泄露态势分析方面，从泄露行业分布、泄露规模、泄露原因以及泄露类型进行了分析总结。从行业分布来看，数据泄露事件发生最多的行业为信息传输、软件和信息技术服务业，占比达 26%；从泄露规模来看，大规模数据泄露依然层出不穷，在已披露数据体量的事件中，100GB 以上体量的数据泄露总量占比高达 54%；从泄露原因来看，外部攻击仍然是大部分数据泄露的罪魁祸首；从泄露类型来看，个人信息泄露最为严重，占据了 58%的比例，主要涉及姓名、电话、身份信息、银行卡、地址等。

专题文章方面，本期收录了大数据协同安全技术国家工程研究中心的三篇文章。一是《数据出境安全评估办法》解读，从几个重点方面进行了详细解读分析，并给出数据处理者的应对之道；二是《从数据利用视角探讨数据出境安全问题》，归纳分析了典型国家地区数据出境管理做法，指出当前数据出境存在的主要问题，并结合数据利用给出了具体的应对建议；三是《数字时代的数据安全新思考》，从数据安全现状、面临的挑战、发展新趋势展望以及建议四个方面对新时代下的数据安全进行探讨。

目 录

第一部分 上半年政策形势总结

第二部分 上半年技术、产品与市场趋势盘点

第三部分 上半年数据泄露态势分析

第四部分 专题文章

一、上半年政策形势总结

2021 年，我国先后生效了《数据安全法》和《个人信息保护法》，与 2017 年生效的《网络安全法》共同构成了数据安全治理的重要法律基础与框架，推动了相关工作的法治建设。

随着数字经济的快速发展，数据作为基础性战略资源和关键性生产要素，对于生产效率的提升效应和市场创新的催化作用愈发显著，全球数据安全治理的立法、执法、“朋友圈”建立等活动更加频繁和活跃。

（一）国际政策形势

大规模数据流动带来巨大收益与价值的同时，也可能对国家安全、个人隐私等方面造成一系列冲击，2022 年上半年，世界各主权国家继续以“新孤立主义”的形态开展数据安全治理，同时通过“数据盟友”等多边、区域性合作规则推进数据流动。

1、各国加紧数据安全治理法治建设

美国国务院成立**网络空间和数字政策局（CDP）**，重点关注国家网络安全、信息经济发展和数字技术三大领域；**《2022 年算法责任法案》草案**发布，旨在为软件、算法和其他自动化系统带来新的透明度和监督；**《犹他州消费者隐私法》（UCPA）、《康涅狄格数据隐私法案》（CTDPA）**相继颁布，至此，美国共

有 5 部州级隐私法发布；首个获得两党、两院支持联邦层面数据隐私草案——**《美国数据隐私和保护法案》（ADPPA）草案**发布。

欧盟公布数据治理立法**《数据法案》（Data Act）草案**，以确保数字环境的公平性，刺激竞争激烈的数据市场，为数据创新驱动提供机会；**数据保护委员会（EDPB）**宣布启动首次联合执法行动，对公共部门使用云服务的情况展开调查；通过了**《数字服务法》（DSA）**，对大型科技企业发布的内容进行更为严格的管理；正式批准**《数据治理法案》（DGA）**，增加对数据共享的信任并为产品和服务的研究与创新建立可信的数据使用环境。

法国数据保护机构（CNIL）发布 **2022-2024 年战略计划**，专注于鼓励控制和尊重个人权利、将欧盟 GDPR 作为一项值得信赖的资产进行宣传，以及优先针对“高风险隐私问题的监管行动”；**英国国际数据传输协议（IDTA）**正式生效，确保英国的个人数据传输时得到充分的保护；**韩国**在金融服务和公共领域以外的所有领域引入 **MyData 标准化计划**；**新加坡**发布**《基础匿名化指南》**，为企业执行数据匿名化与去标识化提供指引；**泰国**发布**《个人数据保护法》（PDPA）**，参考欧盟 GDPR 的基础上，聚焦本国个人数据保护现状的进行差异化制度安排。

2、主要经济体扩大数据安全流通“朋友圈”

美国、加拿大、日本、大韩民国、菲律宾、新加坡、中国台湾正

式对外宣告成立**全球跨境隐私规则（CBPR）**论坛，将亚太经合组织(APEC)框架下的 CBPR 体系转变成一个全球所有国家都可以加入的体系。

美国同其他 60 个国家签署了**互联网未来宣言**，宣言中承诺包括“促进信息自由流动的全球互联网”和促进“对全球数字生态系统的信任，包括通过保护隐私”。

中国与哈萨克斯坦共和国、吉尔吉斯共和国、塔吉克斯坦共和国、土库曼斯坦、乌兹别克斯坦共和国等中亚五国外长会晤通过《**“中国+中亚五国”数据安全合作倡议**》，共同应对数据安全风险挑战并在联合国等国际组织框架内开展相关合作。

（二）国内政策形势

今年是我国数据安全治理立法大年的第二年，相关配套要求在不断完善、细化和健全，不完全统计，截至 6 月 30 日，已发布**超过 30 项国家政策法规、超过 20 项行业监管要求**以及**近 30 项地方政策规章**，同时**数十项相关标准规范**在加紧制定。

随着相关要求的不断完善，数据安全治理的相关执法活动也更加频繁和全面，今年上半年，**工信部**已 **4 次**组织第三方检测机构对移动互联网应用程序(APP)进行检查，对 **241 款**存在侵害用户权益行为的 APP、以及去年发现问题而今年抽测仍存在问题的 **14 款** APP 进行通报；**国家计算机病毒应急处理中心**也持续通过互联网监测，对存在隐

私不合规行为的**159 款 APP 及 1 款 SDK** 进行了违法曝光。

可见，我国在夯实参与国际数据安全治理基础的同时，正全方位推进国内数据安全治理体系的健全与落实。

1、加强数据安全治理体系引导与重视

1 月 12 日，国务院发布**《"十四五"数字经济发展规划》**，要求着力强化数字经济安全体系，提升数据安全保障水平，明确提出强化数据安全风险评估、监测预警和应急处置，建立健全数据安全治理体系，建立数据分类分级保护制度，在顶层设计规划层面再次强调对数据安全高度重视。

2 月 16 日，习近平总书记在文章**《坚持走中国特色社会主义法治道路，更好推进中国特色社会主义法治体系建设》**中指出，要加强国家安全等重要领域立法，加快数字经济等领域立法步伐，并要坚持统筹推进国内法治和涉外法治，加强涉外领域立法，进一步完善反制裁、反干涉、反制"长臂管辖"法律法规，推动我国法域外适用的法律体系建设。

4 月 10 日，国务院发表**《关于加快建设全国统一大市场的意见》**，提出加快培育数据要素市场，建立健全数据安全、权利保护、跨境传输管理、交易流通、开放共享、安全认证等基础制度和标准规范，深入开展数据资源调查，推动数据资源开发利用。

5 月 22 日，中共中央办公厅、国务院办公厅印发了**《关于推进**

实施国家文化数字化战略的意见》，明确要求在数据采集加工、交易分发、传输存储及数据治理等环节，制定文化数据安全标准制定文化数据安全标准，并要构建完善的文化数据安全监管体系。

6 月 23 日，国务院在**《关于加强数字政府建设的指导意见》**中，明确指出要构建数字政府全方位安全保障体系，强化安全管理责任、落实安全制度要求、提升安全保障能力以及提高自主可控水平。

2、推进数据安全制度建设细化与健全

2 月 15 日，修订后的新版**《网络安全审查办法》**生效实施，增加了针对数据处理活动的审查要求，明确要求影响或者可能影响国家安全的数据处理活动在审查范围内、超过 100 万用户个人信息的运营者赴国外上市应申报审查，覆盖数据被窃取、泄露、毁损以及非法利用、非法出境，以及被外国政府影响、控制、恶意利用等数据安全风险。

6 月 9 日，国家市场监督管理总局、国家互联网信息办公室发布**《关于开展数据安全管理认证工作的公告》**，基于国家标准 GB/T 41479-2022《信息安全技术 网络数据处理安全要求》及其他相关标准，对组织的数据安全管理体系进行认证并颁发证书，鼓励网络运营者通过认证方式规范网络数据处理活动，加强网络数据安全保护。

6 月 22 日，习近平主持召开中央全面深化改革委员会第二十六次会议时强调，数据基础制度建设事关国家发展和安全大局，要维护

国家数据安全，保护个人信息和商业秘密，促进数据高效流通使用、赋能实体经济，统筹推进数据产权、流通交易、收益分配、安全治理，**加快构建数据基础制度体系**。

3、加速落实重要行业、领域数据安全保障

（1）移动互联网行业

1 月 4 日，国家互联网信息办公室等四部门发布**《互联网信息服务算法推荐管理规定》**，明确算法推荐服务提供者的信息服务规范、用户权益保护要求，深入推进互联网信息服务算法综合治理，积极促进算法推荐服务规范健康发展。

4 月 8 日，中央网信办牵头开展**“清朗 2022 年算法综合治理”**专项行动，以落地落实落好**《互联网信息服务算法推荐管理规定》**，深入排查整改互联网企业平台算法安全问题，评估算法安全能力，重点检查具有较强舆论属性或社会动员能力的大型网站、平台及产品，督促企业利用算法加大正能量传播、处置违法和不良信息、整治算法滥用乱象、积极开展算法备案，推动算法综合治理工作的常态化和规范化，营造风清气正的网络空间。

4 月 18 日，中共中央办公厅、国务院办公厅印发了**《关于加强打击治理电信网络诈骗违法犯罪工作的意见》**，对加强打击治理电信网络诈骗违法犯罪工作作出安排部署，明确提出依法严厉打击电信网络诈骗违法犯罪、构建严密防范体系、加强行业

监管源头治理等方面的要求。

6 月 14 日，国家互联网信息办公室修订发布**《移动互联网应用程序信息服务管理规定》**，要求应用程序提供者和应用程序分发平台应当建立健全数据安全和个人信息保护等管理制度，规定了应用程序提供者的数据安全义务，包括建立健全全流程数据安全管理制度，采取保障数据安全技术措施和其他安全措施，加强风险监测。

此外从 4 月起，广东省通信管理局、福建省通信管理局、湖北省通信管理局、北京市通信管理局、浙江省通信管理局先后发布了关于开展 **2022 年电信和互联网行业网络与数据安全检查**的通知，对网络运行单位的数据安全保护落实、个人信息保护工作等落实情况进行检查。

（2）金融行业

去年 12 月 31 日，中国人民银行印发**《金融科技发展规划(2022-2025 年)》**，提出了对新时期金融科技发展的数据安全指导意见，明确推动数据有序共享、做好数据安全保护的要求。

3 月 15 日，银保监会消保局将组织开展**银行业保险业个人信息保护专项整治工作**，推动银行业保险业切实落实《中华人民共和国个人信息保护法》，提升对个人信息使用的规范性，保护消费者信息安全权。

5 月 18 日，中国银保监会发布**《银行保险机构消费者权益保护**

管理办法（征求意见稿）》，强调落实消费者身份识别和验证的规定，要求通过加密传输线路、安全隔离、数据加密、权限管控、监测报警等方式，严格控制合作方行为与权限，开展数据分析等方面合作应使用脱敏后的数据，防范数据滥用或泄露风险。

（3）交通运输和邮政业

3 月 29 日，工业和信息化部办公厅、交通运输部办公厅等五部门联合发布**《关于进一步加强新能源汽车企业安全体系建设的指导意见》**，提出要强化数据安全保护，要求企业要切实履行数据安全保护义务，建立健全全流程数据安全管理制度，采取相应的技术措施和其他必要措施，保障数据安全。企业要按照法律、行政法规的有关规定进行数据收集、存储、使用、加工、传输、提供、公开等处理活动，以及数据出境安全管理。

4 月 6 日，交通运输部办公厅发布**《关于做好道路客运电子客票推广普及有关工作的通知》**，要求规范电子客票相关信息的采集、传输、存储、应用流程，强化道路客运电子客票服务网络安全、数据安全和个人信息保护，确保系统安全平稳运行，严防旅客个人信息等重要数据泄露。

4 月 21 日，国家邮政局等三部门联合部署开展为期半年的**邮政快递领域个人信息安全治理专项行动**，聚焦解决突出问题，确保实现涉邮政快递领域侵犯公民个人信息违法犯罪得到明显遏制；提升打击

效能，对侵害用户信息安全行为“零容忍”，严厉打击涉寄递电信诈骗、空包“刷单”等违法犯罪行为；加大整治力度，大力推广虚拟安全号码、隐私面单、网络身份认证等技术应用。

（4）其他行业/领域

2 月 13 日，工业和信息化部对修改完善后的**《工业和信息化领域数据安全管理办法（试行）》**再次公开征求意见，新版征求意见稿在原版工业数据、电信数据的基础上，将无线电数据也纳入了工业和信息化领域数据的范畴中，并对重要数据和核心数据目录备案是否需提供数据内容本身，备案更换的条件，销毁数据备案等问题进行了进一步明确，对涉及个人信息的相关数据安全管理规定进行了补充。

3 月 22 日，科学技术部发布**《人类遗传资源管理条例实施细则（征求意见稿）》**，规定将人类遗传资源信息向境外组织、个人及其设立或者实际控制的机构提供或者开放使用可能影响我国公众健康、国家安全和社会公共利益的，应当通过科技部组织的安全审查。

5 月 11 日，国家药监局印发**《药品监管网络安全与信息化建设“十四五”规划》**，提出推进数据安全保障建设，开展数据安全顶层设计和统筹管理，明确数据安全责任主体，健全数据安全管理工作机制，通过技术手段提升数据的存储安全、传输安全、访问安全和使用安全，确保数据的机密性、完整性和可用性。建立统一高效、协同联动的数据安全风险报告及研判处置体系。

5 月 25 日，最高人民法院发布**《最高人民法院关于加强区块链司法应用的意见》**，明确要保障司法数据安全。推进人民法院电子卷宗、电子档案、司法统计报表、案件结案状态等司法数据上链存储，确保司法数据防篡改，提升数据安全水平。

6 月 14 日，国家能源局发布**《电力行业网络安全管理办法（修订征求意见稿）》**，要求电力企业应当建立健全全流程数据安全管理和个人信息保护制度，按照国家和行业重要数据目录及数据分类分级保护相关要求，确定本单位的重要数据具体目录，对列入目录的数据进行重点保护。

4、积极推动数据安全法规的本地化建设

（1）上海市

1 月 13 日，**《推进治理数字化转型 实现高效能治理行动方案》发布**，提出要按照相关法律法规要求，落实数据分类分级保护、信息安全等级保护和个人信息保护制度，健全安全风险评估、安全责任落实、安全应急处置等相关机制；加强安全技术运用，探索借助区块链、隐私计算等新技术，加强公共数据安全保护技术能力等。

1 月 30 日，上海市杨浦区检察院联合多组织出台**《企业数据合规指引》**，对企业的数据合规管理架构与风险识别处理规范作出了规定，包括数据合规管理体系、数据风险识别、数据风险评估与处置、数据合规运行与保障等内容，督促企业对数据进

行合规管理，有效惩治预防数据违法犯罪。

2 月 18 日，**《上海市未成年人保护条例》**发布，规定任何组织或者个人不得披露未成年人的个人隐私，不得违法披露未成年人的姓名、住所、单位、照片、图像以及其他可能识别未成年人身份的信息。

2 月 18 日，**《中国（上海）自由贸易试验区临港新片区条例》**表决通过，提出在临港新片区内探索制定低风险跨境流动数据目录，促进数据跨境安全有序流动。支持临港新片区推进国际数据产业发展，培育发展数据经纪、数据运营、数据质量评估等新业态，建立数据跨境流动、数据合规咨询服务、政企数据融合开发等公共服务平台。

2 月 22 日，上海首个**《餐饮行业“扫码点餐”规范指引》**正式发布，要求餐饮服务经营者收集消费者信息应当遵循合法、正当、必要的原则，在提供扫码点餐服务时，应当限于实现处理目的的最小范围，不得强制要求消费者对手机号、微信号等个人信息进行注册或授权，不得过度收集消费者信息。

4 月 20 日，**《上海城市数字化转型标准化建设实施方案》**印发，在完善基础标准中提出聚焦信息安全、链路安全、数据安全防护，研制实施数据资源全流程监测、生物特征及用户习惯采集和应用管理、数据跨境流通安全评估等标准，以标准化支撑构建城市数字化转型的大安全格局。

6 月 10 日，**《新型数据中心“算力浦江”行动计划（2022-2024 年）》发布**，明确要求加快提升数据安全防护能力。落实“谁主管谁负责、

谁运行谁负责、谁收集谁负责、谁持有谁负责、谁使用谁负责”责任要求，强化数据全生命周期安全管理机制，加强多方安全计算、联邦学习、可信执行环境等可信计算技术创新突破与推广应用，提升数据安全的监测与防护能力；开展数据中心数据安全体系建设，加强安全评估，建立数据分级分类管理制度。

（2）广东省

1 月 24 日，**《关于深圳建设中国特色社会主义先行示范区放宽市场准入若干特别措施的意见》**发布，鼓励深圳开展地方性政策研究探索，建立数据资源产权、交易流通、跨境传输、信息权益和数据安全保护等基础制度和技术标准；开展数据跨境传输（出境）安全管理试点，建立数据安全保护能力评估认证、数据流通备份审查、跨境数据流通和交易风险评估等数据安全管理机制。

2 月 7 日，**《广东省公共数据安全管理办法（征求意见稿）》**发布，公开征求意见。旨在加强广东省数字政府公共数据安全管理，规范公共数据处理活动，促进数据资源有序开发利用，保护个人、组织的合法权益，维护国家主权、安全和发展利益。

2 月 28 日，**《广东省数字政府改革建设 2022 年工作要点》**印发，提出探索运用区块链、隐私计算等新技术强化数据安全防护。建设粤港澳大湾区大数据中心，健全大湾区数据基础设施体系。

5 月，**《深圳市数字政府和智慧城市“十四五”发展规划》**发布，

提出要健全数据安全保护机制，强化公共数据和个人数据保护，提升数据安全保障能力；围绕数据全生命周期管理，编制数据资源标准规范，完善采集汇聚、数据治理、共享开放、数据安全等标准规范。

6 月 1 日，首部城市数字经济地方性法**《广州市数字经济促进条例》**开始施行，针对首席数据官、数据经纪人等创新试点提供了法律保障，明确提出建立健全部门协同、市区联动、政企合作的数据治理体制机制，探索推行首席数据官等数据管理创新制度，探索建立数据交易平台、场所以及数据入场规范、数据经纪人管理等配套制度。

（3）福建省

4 月 1 日，福建省发布**《关于印发 2022 年数字福建工作要点的通知》**，明确提出要完善信息基础设施网络安全防护能力建设，推进数据安全、个人信息保护等领域基础制度建设。建设关键信息基础设施安全保护平台，加强关键信息基础设施保护，强化数据资源全生命周期安全保护。

4 月 11 日,**《福建省做大做强做优数字经济行动计划（2022—2025 年）》**公布，在数字经济安全体系提升工程要求中，明确要强化数据安全管理，建立健全数据分类分级和隐私保护制度，定期开展安全风险检查和评估。落实网络安全和数据安全信息通报工作机制，有效防范、处置安全风险。

6 月 1 日，**《厦门经济特区数据条例（草案征求意见稿）》**发布，

明确了数据处理活动中数据安全方面的一般规定、责任制、处理者数据安全保护义务、数据安全风险评估与预警、数据安全检查协作等相关要求。

（4）四川省

3 月 23 日，**《四川省大数据发展条例（草案征求意见稿）》**公布征求意见，明确对数据安全的基本要求、监管部门与责任、处理者数据安全保护义务、数据安全风险评估与应急处置、个人信息处理活动基本原则、数据出境管控、技术创新与研究鼓励等相关要求。

4 月 14 日，**《成都市“十四五”数字经济发展规划》**发布，明确要保障数字经济数据安全，包括探索建立数据分类分级安全保护机制、加快建立全周期数据安全联动管理体系、建立健全数据安全风险预警和应急处置机制、实施数据出境安全评估、推动企业数据合规应用、强化政务数据安全应用示范等内容。

6 月 7 日，**《四川省数据条例（草案）》**提请首次审议，提出建立数据安全责任制，明确政府部门和数据处理者数据安全管理的职责义务；建立分级分类保护、风险防范预警、应急处理机制和安全评估监管等制度，构建完备的安全防护体系，筑牢数据安全底座。

（5）其他地区

2 月 10 日，**《浙江省公共数据条例》**颁布，对加强公共数据安

全管理、规范公共数据安全行为等都做出了体系化、实质性的制度设计，包括制度规范体系、技术防护体系、运行管理体系等方面的要求。

2 月 17 日，**《贵州省大数据战略行动 2022 年工作要点》**印发，明确将开展《数据管理能力成熟度评估模型（DCMM）》《数据安全成熟度模型（DSMM）》国家标准和《贵州省大数据与实体经济深度融合实施指南》贯标推广工作列为重点工作任务内容。

5 月 31 日，**《辽宁省大数据发展条例》**公布，规定实行数据安全责任制和分类分级保护制度，明确责任确定原则，搭建数据安全管理体制，并就全社会各主体建立落实数据安全保护制度、强化数据存储管理和应急处置等予以明确。

黑龙江省、河北省、江苏省、江西省等多个省市也已发布或正制定相关条例、规划，对数据处理活动的监管要求、处理者数据安全保护义务、安全防护要求等方面进行规定，推动数据处理活动的安全有序开展以保障数字经济的稳定发展。

5、不断探索与完善数据安全标准化体系

1 月 13 日，全国信息安全标准化技术委员会再次发布修订后的国家标准**《信息安全技术 重要数据识别指南（征求意见稿）》**，将旧版中“重要数据的特征”和“重要数据识别流程”合并为“重要数据的识别因素”。在内容上，新版没有详细描述重要数据特征的小类，指提出了重要数据的十四项识别因素；此外，在识别重要数据的基本原则

中，将旧版中第二项“促进数据流动”原则替换为“突出保护重点”。

2 月 8 日，全国信息安全标准化技术委员会发布国家标准**《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（征求意见稿）》**，对 App 生命周期过程和风险监测处置过程中的数据安全要求、个人信息保护要求进行了明确。

2 月 25 日，工业和信息化部印发行业标准**《车联网网络安全和数据安全标准体系建设指南》**，明确数据安全标准主要规范智能网联汽车、车联网平台、车载应用服务等数据安全和个人信息保护要求，包括通用要求、分类分级、出境安全、个人信息保护、应用数据安全等 5 类标准。

3 月 9 日，国家工业信息安全发展研究中心牵头编制的团体标准**《智能网联汽车数据安全评估指南（征求意见稿）》**发布，对数据安全评估分为数据安全风险评估、数据安全合规性评估和数据出境安全评估三种类型，对数据安全风险评估、数据安全合规性评估的流程、方法进行了明确。

3 月 25 日，天津市市场监督管理委员会发布地方标准**《网络数据安全监督检查规范（征求意见稿）》**，规定了网络数据安全监督检查的流程、内容和要求，主要适用场景为对网络数据处理者网络数据的收集、存储、使用、加工、传输、提供、公开等活动进行监督、检查、管理和评估。

4 月 15 日，国家市场监督管理总局、国家标准化管理委员会发

布国家标准 **GB/T 41479-2022《信息安全技术 网络数据处理安全要求》**，给出了网络数据处理安全的总体要求、技术要求、管理要求以及突发公共卫生安全事件时的数据处理安全要求。

4 月 15 日，国家市场监督管理总局、国家标准化管理委员会发布国家标准 GB/T 41391-2022**《信息安全技术 移动互联网应用程序（App）收集个人信息基本要求》**，围绕个人信息处理的最小必要原则，针对 App 违法违规收集使用个人信息的突出问题，结合当前移动互联网技术及应用现状，在 GB/T35273—2020《信息安全技术 个人信息安全规范》的基础上，给出了 App 收集个人信息应满足的基本要求，以及常见服务类型 App 必要个人信息的使用要求。

4 月 28 日，全国信息安全标准化技术委员会发布国家标准**《信息安全技术 互联网平台及产品服务隐私协议要求（征求意见稿）》**，规定了互联网平台及产品服务隐私协议编制程序、具体内容、发布形式，增加隐私协议的可读性、透明性，以及处理隐私协议相关的争议纠纷等方面的要求。

5 月 7 日，工信部发布行业标准 YD/T 4177—2022**《移动互联网应用程序（APP）收集使用个人信息最小必要评估规范》**，旨在对移动互联网行业收集使用人脸、通讯录、短信、位置、图片等敏感个人信息进行规范，落实最小、必要的原则。

6 月 13 日，全国信息安全标准化技术委员会发布国家标准**《信息安全技术 移动智能终端的移动互联网应用程序（App）个人信息**

处理活动管理指南（征求意见稿）》，App 在移动智能终端上的生命周期中各阶段的 App 个人信息处理活动安全风险进行了梳理，并提出了透明化展示个人信息处理活动、App 个人信息处理行为管理、用户控制 App 收集个人信息行为、预置应用软件处理个人信息行为管理等管理措施。

二、上半年技术、产品与市场趋势盘点

（一）技术、产品趋势

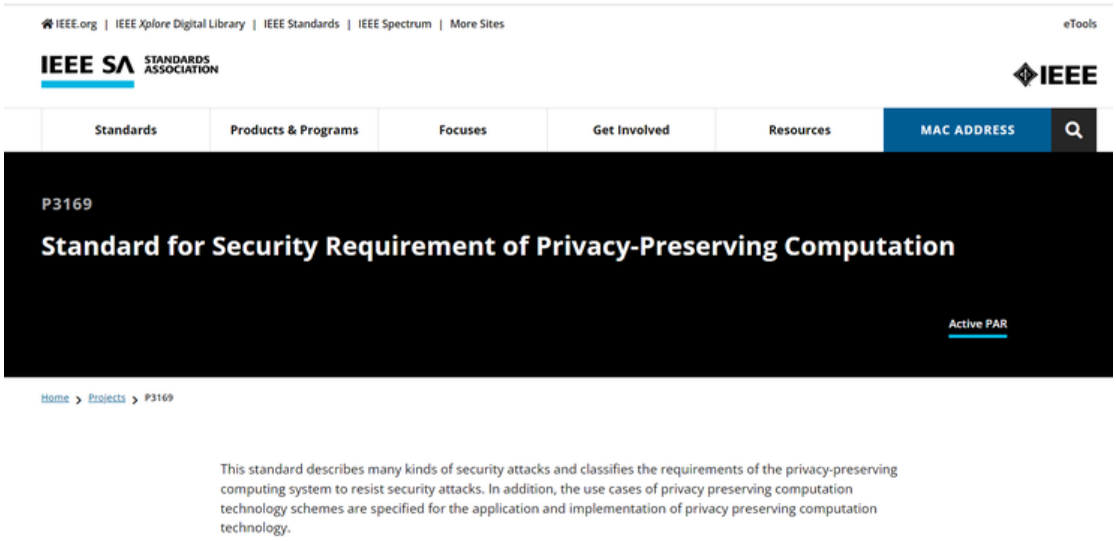
1、隐私计算重要技术持续创新，助推标准逐步完善

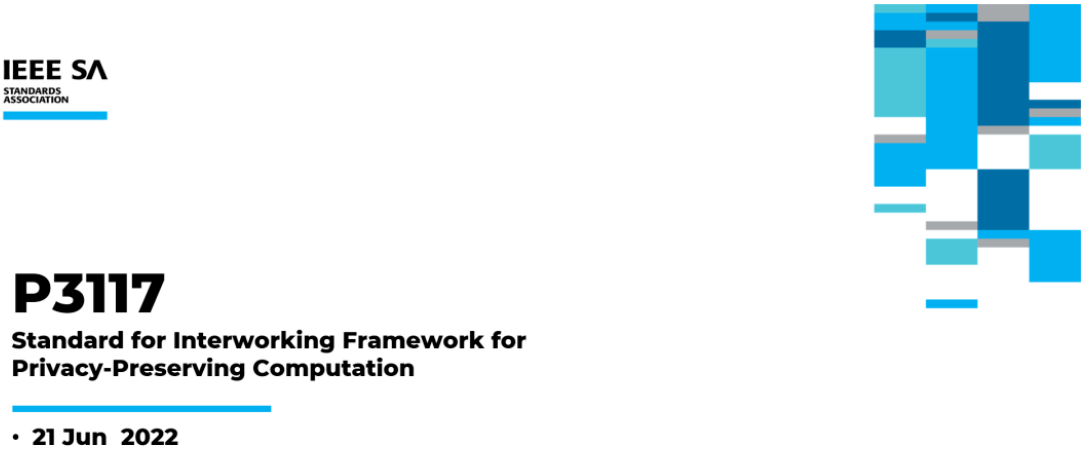
关键词：隐私计算技术创新 隐私计算标准 互联互通

隐私计算技术创新方面：一是蚂蚁集团可信密态计算（Trusted-Environment-based Cryptographic Computing，简称 TECC）领域的“分布式多方安全计算系统、方法和节点”（CN113992439B）专利被授权。该技术根据资源消耗和任务可并行拆分程度的不同，可将 TECC 的计算速度提升 10 倍到 100 倍，实现在 1 小时内完成亿级样本密态 GBDT（Gradient Boosting Decision Tree，一种树模型集成算法）建模训练，在 10 分钟内完成亿级数据密态 SQL 分析，可以为顶级数据规模带来非常友好的计算体验，达到了隐私计算现阶段最佳性能效果，也使得 TECC 计算效率接近于数据非加密的明文计算。**二是**由原语科技自主研发的隐私计算平台 Primihub 已正式在 GitHub 平台上开源：http://docs.primihub.com/。Primihub 平台融合了 MPC（多方安全计算）、FL（联邦学习）、HE（同态加密）、TEE（可信执行环境）等多种技术路线，提供多安全级别、多性能要求、多场景支持的解决方案，帮助企业用户保护数据隐私的同时，深度连接各个合作方，实现跨数据、跨行业的合作共赢。

隐私计算标准发展方面：首个“隐私计算安全

需求”国际标准立项，IEEE SA 标准委员会正式通过了“隐私计算安全需求”（Standard for Security Requirement of Privacy-preserving computation，P3169）国际标准的立项。该标准由蚂蚁集团主导，行业内专家共同参与，将对隐私计算技术本身潜在的安全隐患进行分析，并对隐私计算系统抵御的安全风险进行分级。目前，IEEE SA 已成立专门工作小组，蚂蚁集团牵头推进下一步实质性工作。全球首个 IEEE 隐私计算互联互通国际标准正式启动，6 月 21 日，IEEE SA 隐私计算互联互通标准 P3117《Standard for Interworking Framework for Privacy-Preserving Computation》（IEEE P3117）第一次工作启动会成功召开，标志着全球首个隐私计算互联互通国际标准工作组正式成立并启动标准制定工作。





（引用来源：“开放隐私计算”公众号）

2、以可信执行环境为核心的机密计算成为隐私计算赋能领域重要的解决方案，机密计算时代或将很快到来

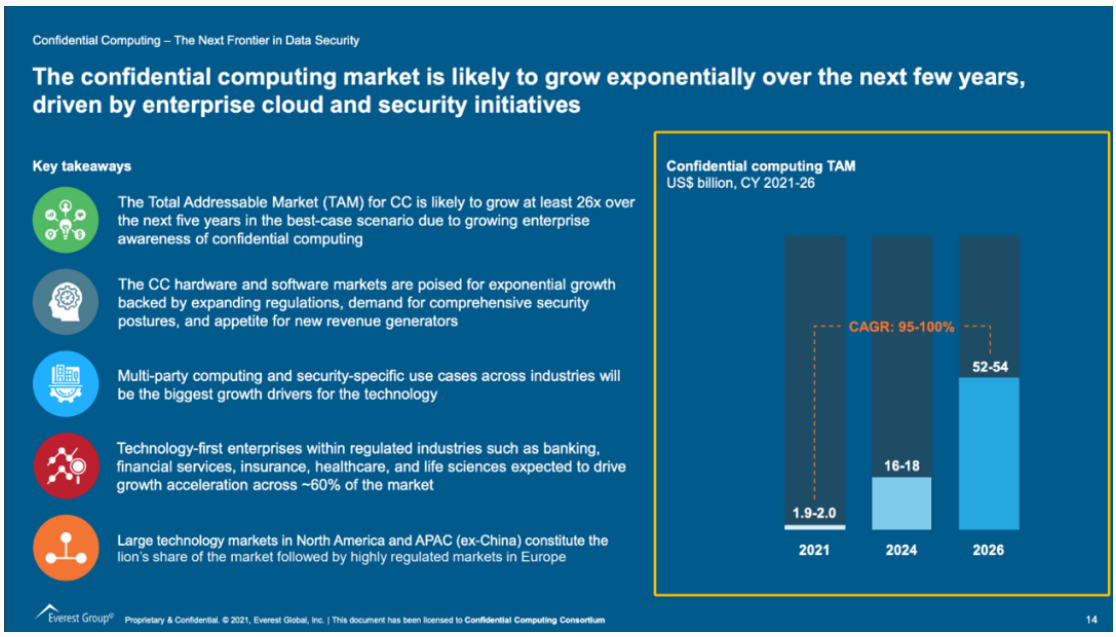
关键词：机密计算 可信执行环境 隐私计算

早在 2020 年，研究机构 Gartner 就在其年度云安全技术成熟度曲线中，将机密计算列为 33 种关键安全技术之一。有研究机构预测，机密计算技术在未来 1-2 年内就会成为安全计算的标准方法，尤其是在云计算环境中。

在企业应用需求和技术应用价值的双重推动下，机密计算概念的市场发展比预期要快很多。目前许多科技巨头纷纷入局，大力探索和开发机密计算。机密计算的产业生态也在不断完善，包括阿里巴巴、华为、AMD、微软、甲骨文、Google 等科技巨头公司在内的企业，已在 Linux 基金会下启动成立了机密计算技术应

用联盟，旨在进一步加快技术应用标准的定义和开源工具的开发。

基于 CPU 可信执行环境的机密计算技术可以在保证数据“可用而不可见”的前提下进行数据运算，成为解决数据流通安全问题的热点技术。根据国外著名信息调查机构 Everest Group 最近的一项市场研究表明，**机密计算市场预计将在 5 年内增长到 54 亿美元**。2021 年，机密计算的可触达市场空间（TAM）为 19-20 亿美元。预计到 2026 年，机密计算市场在理想的情况下将以 90-95%的年复合增长率增长，在不理想的情况下至少以 40-45%的年复合增长率增长。

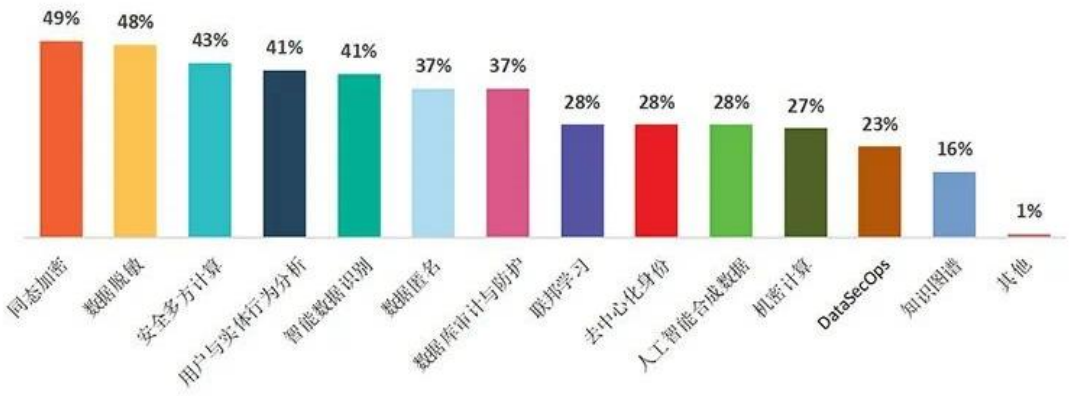


（引用来源：“隐私计算联盟”公众号）

3、同态加密已成为企业数字化转型中最热门的隐私增强技术

关键词：同态加密 数字化转型

据《2022 年中国企业数据安全现状调查报告》显示，在热门数据安全技术中，隐私增强和隐私保护相关的数据安全技术受到了企业安全主管的重点关注，这包括同态加密（第一名）、数据脱敏（第二名）、安全多方计算（第三名）、智能数据识别（第五名）、数据匿名（第六名）和联邦学习（第八名）。



同态加密作为目前市场上最强大的隐私增强保护技术之一，可以让企业在云环境中安全存储、使用和管理数据，而无需向云服务商提供对加密密钥的访问权限，同态加密可广泛应用于在数据隐私、法规合规、反洗钱、金融欺诈和数据货币化等领域，从本次调研结果来看已经成为企业数字化转型中最热门的隐私增强技术。

（引用来源：安全内参）

4、身份管理漏洞成为数字安全首要威胁

关键词：身份认证 身份管理 微软

确保身份认证及管理的安全性是确保数字安全的重中之重。当今世界，身份认证已经成为关乎每个人工作生活方方面面的关键凭证，“身份”背后存储的是每个人在浩如烟海的各类应用和服务中的全部记录。正是因为身份认证如此重要，如果没有对身份认证加以正确的安全保护，将带来巨大的潜在风险。目前以多因素认证（MFA）、无密码方案为代表的强身份认证的使用率还很低——而那些仅仅依靠密码保护的账号，常常成为黑客们最容易得手

的目标。

微软数据显示，截至 2021 年 12 月，在采用微软云端身份解决方案 Azure Active Directory（AAD）的各行业客户中，只有 22%启用了强身份认证保护措施。仅在 2021 年 1 月到 12 月的一年里，微软就阻止了 256 亿次针对 AAD 的暴力破解身份认证攻击，并通过 Microsoft Defender for Office 365 拦截了 357 亿封网络钓鱼电子邮件。

对于大多数组织来说，以多因素认证、无密码解决等方案强化身份管理，是防范各种类型安全威胁，最行之有效又简便易行的重要手段。企业和组织可以通过以下方式更好地保护自己：**（1）启用多因素身份验证（MFA）；（2）审核账户权限；（3）审查、强化和监视所有租户管理员账户；（4）建立并实施安全基线以降低风险。**

（引用来源：freebuf）

5、量子计算技术在理论与应用方面均取得显著进步

关键词：量子密钥分发技术 量子安全系统

6 月 6 日，加拿大量子安全公司 Quantropi,Inc.在加利福尼亚州旧金山举行的 RSA 大会上展示了其最新的量子安全加密产品——SEQUR™ SynQK，该产品可生成并以数字方式分发同步的量子密钥。Quantropi 的 SEQUR™ SynQK 有效地打破了几个世界记录，在 4000 到 15000 公里的距离内以 130 到 190 兆每秒的速度同时传送至少 5 个量子密钥流(5 个数据流中的每一个都相当于 Google.com 每

秒使用的 8 - 12 倍)。SEQUR™是 Quantropi 的 TrUE 加密解决方案系列中的熵产品，此产品系列提供量子密钥生成和分发功能。目前，该系列产品包括 SEQUR™ QEaaS、SEQUR™ NGen 和最新发布的 SEQUR™ SynQK。

IBM 推出了下一代大型机系统 IBM z16，搭载人工智能处理器和量子安全系统，可为人工智能、混合云、量子计算、开源等领域提供充分支持。IBM z16 **集成量子安全系统，为数据安全保驾护航**，除应对欺诈活动外，还可应用于诸如货币加密、贷款审核、防止盗窃等产业。IBM 以普及加密和机密计算技术为基础，采用网格密码学技术，在 IBM z16 上增加了一个保护组织免受未来技术，以破解当今加密文件威胁的量子安全系统。

（引用来源：信息安全与通信保密杂志社、安全内参）

6、安全大脑助力用户构建“能力中枢平台”，带动数字时代能力体系升级

关键词：安全大脑 数字安全 能力体系

在数字时代安全威胁不断演进的今天，对数字安全体系化、实战化提出了更高的要求。但越来越多政企用户清晰地看见——自身的网络安全建设存在着企业设备各自为战、生态产品难以联动、外部能力无法融合等多重协同壁垒。

在此背景下，360 政企安全集团正式推出 360 核心安全大脑 3.0。具体构成上，360 核心安全大脑 3.0 由一个安全大数据平台、一个云端赋能平台和多个安全分析引擎，以及内嵌 360 十七年经验所积累的实战方法论组成。其中安全大数据平台通过模型化管理的数据标准，接入各类安全数据使之集中管理，并在内部融合数据品类，协调数据流程决策与步骤，为安全业务提供从数据接入到存储、清洗到运算，

最终到图表展示的全生命周期一站式服务。安全大数据平台具有“运营商”级别的数据处理能力，助力提升安全运营中的数据处理效率 5 倍以上。

云端赋能平台通过云地协同、能力下沉，为安全设备提供从漏洞到资产、从情报到知识、从线索到规则、从事件到态势等百余种基础的安全数据及分析能力，可以满足各类安全设备的通用化威胁检测与分析需求。此外 360 核心安全大脑 3.0 中还预置了近百类安全分析引擎，2000 多个安全策略，可以把专业相关的分析能力通过配置组合的方式赋能特定的安全产品，应对纷繁复杂的安全业务，从多个维度指导安全设备发现、防护高级别网络威胁，提升自身网络安全能力。

（引用来源：安全客）

7、数据与隐私安全成为 RSAC 2022 十大热点议题之一

关键词：数据　　安全　隐私保护　RSAC 2022

2022 年度的全球网络安全行业盛会 RSAC 落下帷幕。RSAC 2022 的 170 余个主题演讲，主要围绕 10 大热门主题，其中包括：**数据与隐私安全**（热度 14[1]）、身份安全与零信任（热度 14）、软件供应链安全（热度 10）、勒索软件（热度 10）、AI 安全（热度 10）、威胁分析及狩猎（热度 10）、风险管理（热度 9）、云安全（热度 6）、物联网及工业安全（热度 6）、基础设施安全（热度 4）。

数据与隐私安全是近 5 年来的热点议题。随着数字经济的发展和数据流通需求的增长，其热度持续升高。数据与隐私安全融合了传统安全技术应用和创新技术应用，产生了新的需求和应用场景。数据治理、隐私计算、隐私合规成为数据安全的创新驱动力。

本届 RSAC 的**数据安全议题集中在数据保护**，如云上行业（如医疗）数据保护、企业数据保护、数据本地化保护政策，以及政府数据交易与授权访问等。在隐私安全方面，热点议题则集中在如何保障基础设施（如 5G）、设备（如汽车），以及应用（如 AI、区块链）的隐私安全方面。

（引用来源：安全内参）

（二）市场洞察

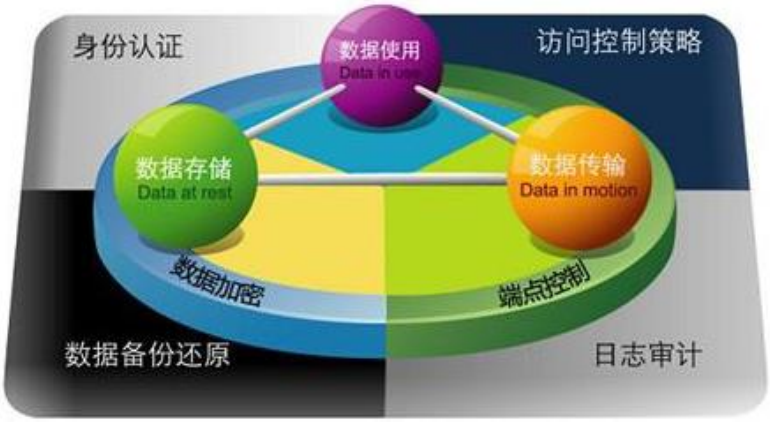
1、企业数据泄露防护 (DLP) 市场年复合增长高达 21%

关键词：DLP 市场规模

[1] 热度 14：指会议中有 14 个演讲的主题为数据与隐私安全

根据 Research And Markets 最新发布的调查数据，未来五年全球企业数据泄露防护（DLP）市场预计将以 21.03%的复合年增长率高速增长，到 **2026 年市场规模将达到 62.65 亿美元**，而 2019 年为 16.47 亿美元。

DLP 解决方案可按照网络、存储/数据中心、端点、服务、咨询、系统集成、培训等不同应用领域进行分类。根据部署模式，DLP 还可分为内部部署和云端防护两大类。由于云数据丢失防护为电子邮件、USB 驱动程序、笔记本电脑和移动电话提供了解决方案，因此预计云 DLP 细分市场将会进一步增长。



从垂直行业来看，新兴行业中越来越多地开始使用企业数据丢失防护，此外，航空航天和国防、通信和技术、政府、医疗、制造和其他行业的 DLP 市场也将以高复合年增长率增长。

（引用来源：安全内参）

2、Forrester：第三方风险管理市场将“百花齐放”

关键词：第三方风险管理 Forrester

研究咨询公司 Forrester 在最新发布的《Now Tech：第三方风险管理平台，2022 年第一季度》报告中称，第三方风险管理（TPRM）在业务优先级和风险管理优先级列表中位居前列，并将呈现“百花齐放”的发展态势。

目前，有几类供应商支撑 TPRM 市场，每一类专注于一个或多个风险领域、行业或客户成熟度级别。Forrester 的新报告《Now Tech：第三方风险管理平台，2022 年第一季度》，根据功能将 22 种主要的 TPRM 技术分为四大类，每一大类都有适合不同类型买家的供应商。

（1）专用技术。这类技术在整个第三方风险管理生命周期当中提供强大功能。它们结合领域专业知识和广泛功能，以支持所有级别的 TPRM 成熟度。

（2）GRC 平台。治理、风险和合规（GRC）平台为众多的风险和合规使用场景提供强大支持。

（3）风险信息交换中心。风险信息交换中心让组织可以访问预

先填好和验证的评估结果、多种类型的文档和证据以及分析工具。

（4）专注于垂直领域的供应商。这些提供商拥有扎实的专业技术专长、GRC 平台的广泛功能，并经常提供支持服务，但尤其关注第三方合规要求很复杂的行业。

（引用来源：安全内参）

3、零信任安全市场将在 2027 年达到 644 亿美元

关键词：零信任

据 Research And Markets 数据显示，在 COVID-19 危机中，2020 年全球零信任安全市场估计为 183 亿美元，预计到 2027 年修订后的规模将达到 644 亿美元，复合年增长率为 19.7%。

到 2020 年，美国的零信任安全市场估计为 54 亿美元。作为世界第二大经济体的中国，预计到 2027 年将达到 111 亿美元的市场规模，复合年增长率为 19%。其他值得注意的地区包括日本和加拿

大，预计在 2020-2027 年期间分别增长 17.8% 和 17%。在欧洲，预计德国的复合年增长率约为 14.4%。

（引用来源：helpnetsecurity）

4、Gartner：2025 年 60%的大型企业机构将使用隐私增强计算技术

关键词：隐私增强计算 Gartner

Gartner 日前发布了 2022 年银行和投资服务行业的三大热门技术趋势，分别是：**生成式人工智能（生成式 AI）、自主系统和隐私增强计算。**这三项趋势将在未来两到三年内继续增长，推动金融服务机构的增长和转型。

隐私增强计算（PEC）能够保障在不可信环境中处理个人数据时的信息安全，而随着隐私和数据保护法的不断发展以及消费者的日益关注，这一点正变得越来越关键。隐私增强计算运用各种隐私保护技术使金融服务机构在从数据中获取价值的同时满足合规要求。

Gartner 预测，**2025 年 60%的大型企业机构将在分析、商业智能或云计算领域使用一种或多种隐私增强计算技术。**

数据在金融服务领域的各种分析、计算和数据变现工作中都起到了不可替代的作用。金融服务机构正越来越多地在欺诈分析、智能运维和数据共享等应用中采用 PEC。

（引用来源：环球网）

5、Gartner：今年云计算支出将达到 5000 亿美元

关键词：云计算 Gartner

根据研究公司 Gartner 的数据，今年全球在公共云服务上的支出将接近 5000 亿美元，到 2023 年将达到 6000 亿美元。云原生基础设施服务的日益普及被认为是关键驱动因素之一，但疫情大流行驱动的混合工作场景的趋势也发挥了作用。

基础设施即服务(IaaS) 预计将在 2022 年实现最高的最终用户支出增长，达到 30.6%，作为云堆栈的基础级别，支撑

着每一个主要的以消费者为中心的在线产品和移动应用程序。第二高的增长将是**桌面即服务(DaaS)**，增长 26.6%，因为混合工作促使组织不再使用台式机等传统客户端计算解决方案为员工提供动力。由于对云原生功能的需求，在最终用户支出增长中紧随 DaaS 的是**平台即服务(PaaS)**，其支出达到 1096 亿美元，比 2021 年增长 26.1%。

随着核心云服务的成熟，提供商之间差异化的重点正在转移到可以直接破坏企业数字业务和运营的能力上。云计算中的新兴技术，如超大规模边缘云计算和安全访问服务边缘(SASE)，正在扰乱相邻市场并形成新的产品类别，进而为公共云提供商创造额外的收入来源。 Gartner 预计，将云与此类新兴技术相结合的组织将在其数字化转型之旅中取得最大成功。

（引用来源：theregister.com）

6、IDC：2025 年中国网络安全市场规模将超 214 亿美元

关键词：网络安全 安全服务 安全咨询

IDC 数据显示，2021 年中国网络安全相关支出有望达到 102.6 亿美元。预计到 2025 年，中国网络安全支出规模将达 214.6 亿美元。在 2021-2025 的五年预测期内，中国网络安全相关支出将以 20.5%的年复合增长率增长，增速位列全球第一。

相较于增速放缓的全球网络安全服务市场，**中国安全服务市场将以近全球两倍的五年复合增长率快速增长**。IDC 预测，在 2021-2025 的五年预测期内，中国网络安全服务市场年复合增长率将达到 20.8%，到 2025 年，其市场规模预计将超过 61.1 亿美元。其中，**安全咨询服务（Consulting Services）在未来五年仍为最大的服务子市场**，到 **2025** 年，咨询服务市场的规模将达到 **24.6 亿美元**。与此同时，在安全运营需求不断爆发的大背景下，中国托管安全服务（Managed Security Services）市场发展势头强劲，五年复合增长率预计达到 31.9%。

（引用来源：安全内参）

7、2022 年全球 IT 行业 10 大预测：网络安全、数字优先成为核心驱动力

关键词：网络　　安全　数字化　数字化转型

IDC 预计，到 2022 年，全球一半以上的经济将基于数字化或受数字化影响，因为大多数产品和服务都将采用数字化交付模式，或者需要数字化增强才能保持竞争力。为了在数字化优先的世界中赢得竞争，组织需要优先投资于数字化工具，以增强物理空间和资产。因此，到 2024 年，一半以上的 ICT 投资将与数字化转型挂钩。

根据 IDC 的最新预测，2022 年中国 ICT 市场（含第三平台与创新加速器技术）规模将达到 7,937 亿美元，比 2021 年增长 9.2%，持续高于 GDP 的增长。**2022 数字化转型支出将达到 3291 亿美元**，比 2021 年增长 18.6%，数字化转型依然是企业的核心战略。

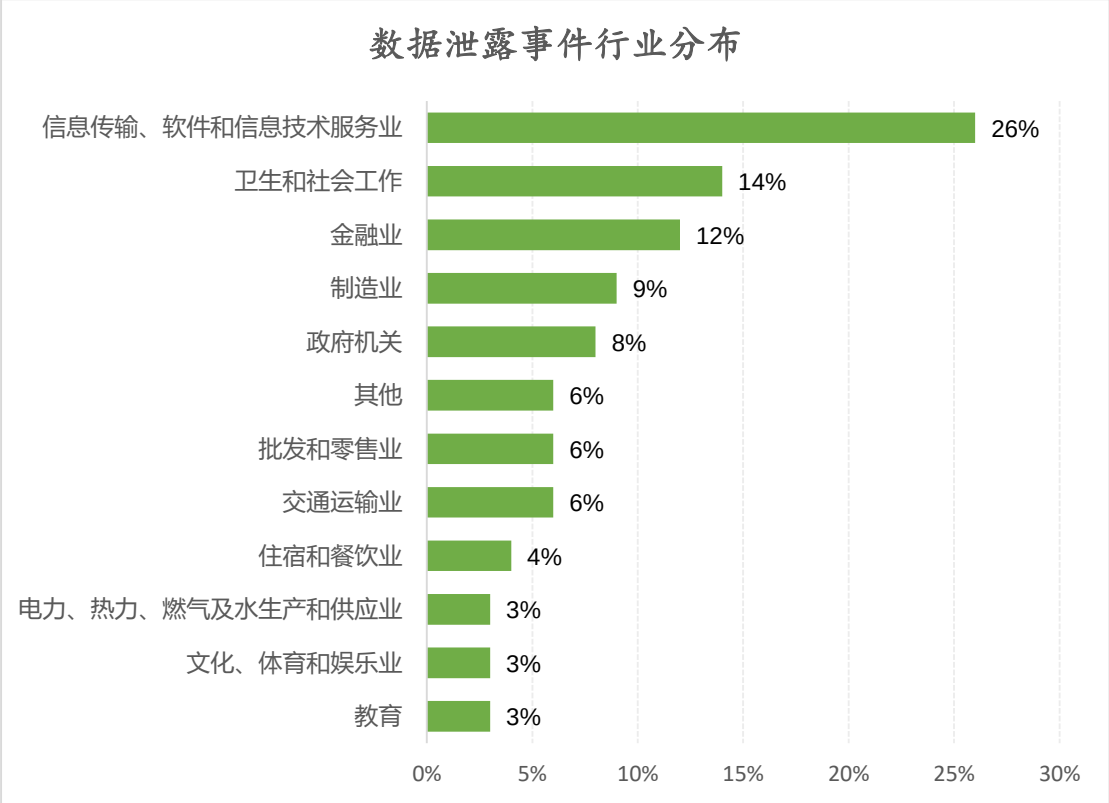
（引用来源：安全内参）

三、上半年数据泄露态势分析

本部分基于大数据协同安全技术国家工程研究中心 2022 年发布的《全球数据安全观察》周报中收录的数据泄露事件，从行业分布、泄露规模、泄露原因、泄露数据类型四个方面进行梳理和总结分析，结果如下。

（一）行业分布

本报告里事件所属行业的划分，主要参考《国民经济行业分类》（GB/T 4754-2017）。对 2022 年 1-6 月份《全球数据安全观察》周报里收录的数据泄露事件所属行业进行统计分析，结果如下：



数据泄露事件发生最多的行业为信息传输、软件和信息技术服务

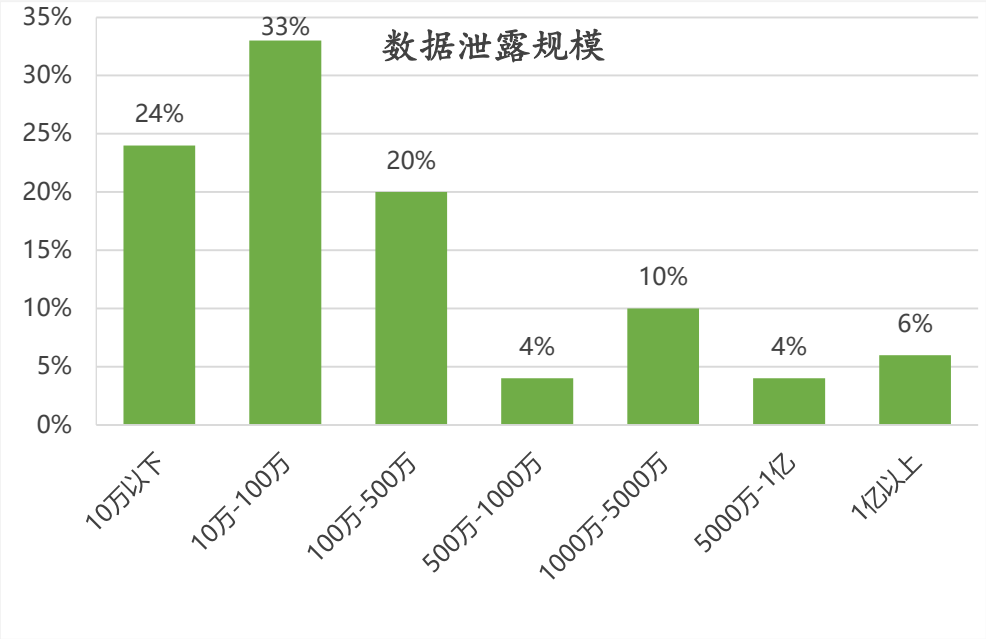
业，占比达 26%。除了涉及电商网站、数字营销公司、社交网站、网络安全公司等，还包括以互联网形式运作的金融、生产服务等企业组织；

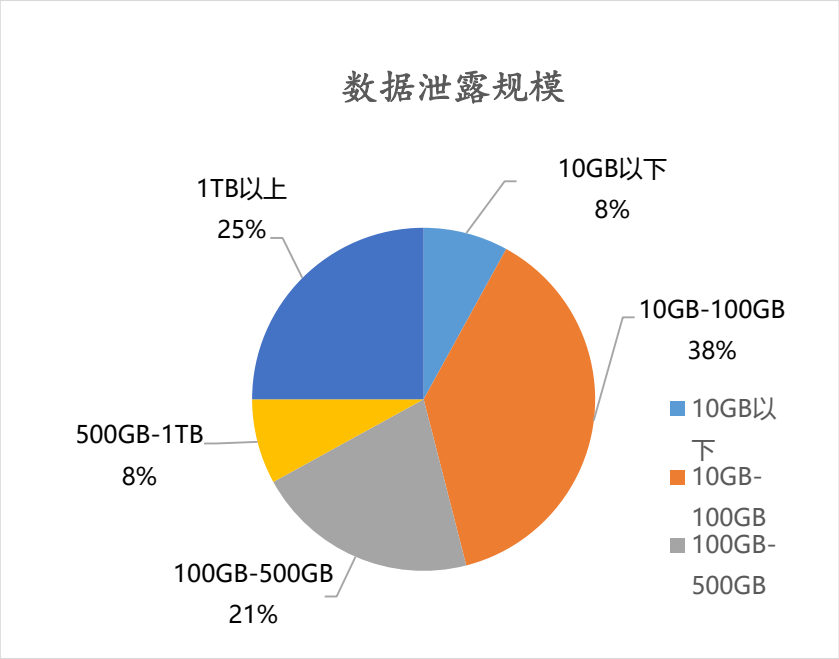
在全球疫情大背景下，医疗卫生领域信息化、智能化进程加速，其所拥有的数据仍然保持着巨大的吸引力，卫生和社会工作大类数据泄露也较为严重，在所有行业中排名第二，占比为 14%；

其次，金融业、制造业和政府机关分别以 12%、9%、8%位列第三、四、五位；电力、热力、燃气及水生产及供应业，文化、体育和娱乐业以及教育业占比最低，为 3%。

（二）数据泄露规模

统计数据中，仍然有近三分之一的数据泄露事件没有披露泄露数据量。在已知披露数据泄露规模的事件中，泄露的数据记录数量在 10 万-100 万的占比最高，为 33%；10 万以下阶段占比次之，为 24%；而泄露记录数大于 1000 万的依然有 20%的占比，不难看出，仍有不少企业组织遭受了大规模数据泄露事件。





从数据体量来说，虽然泄露规模在 10GB-100GB 的事件所占比例最大（38%），但 100GB 以上体量的数据泄露总量占比达到 54%，超过了总体的一半。可见，在大数据时代下，随着全球各行各业数据的不断积累，大规模数据泄露事件层出不穷。

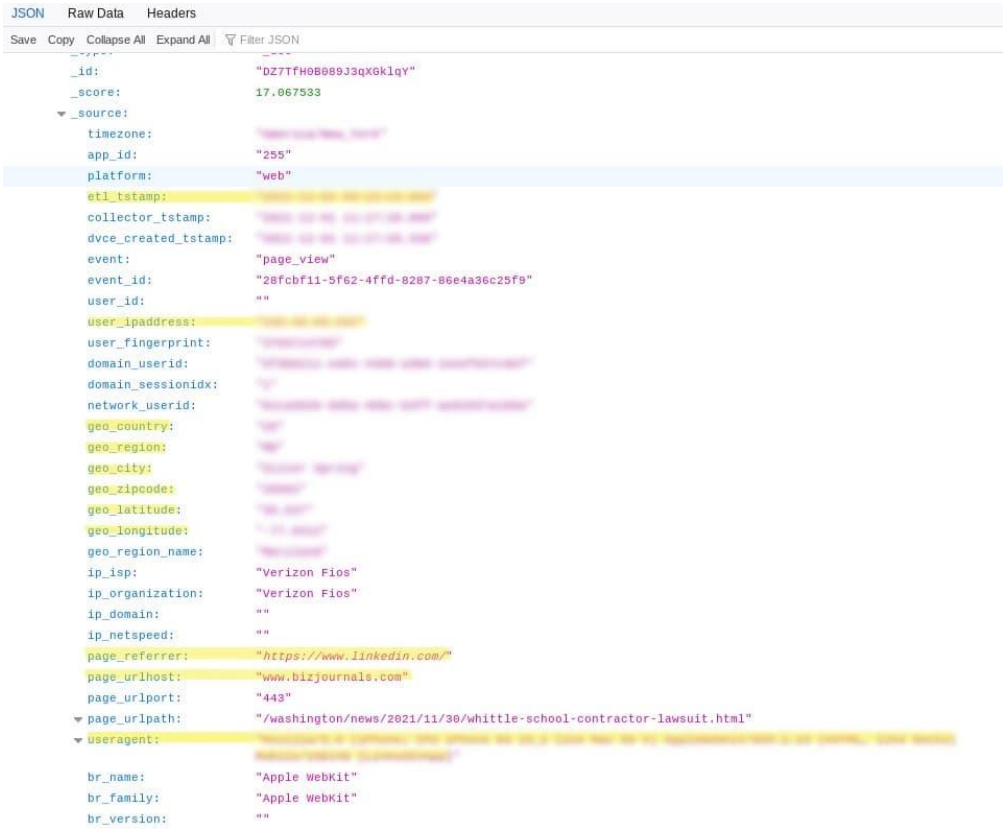
以下选取了近半年单次泄露数据量较大的代表性事件，以此警示

各组织关注数据安全防护。

1、ElasticSearch 服务器配置错误，暴露 579GB 用户网站记录

关键词：数据泄露 用户记录 配置问题

2022 年 5 月 12 日，Website Planet 的 IT 安全研究人员发现了两台暴露的 ElasticSearch 服务器，并确定服务器使用的是软件供应商 SnowPlow Analytics 开发的开源数据分析软件，该软件允许公司在其网站访问者不知情的情况下跟踪和存储信息。



据研究人员称，这两个 ElasticSearch 服务器没有任何加密或用户验证措施，意味着任何人都可以在不需要密码的情况下访问这些数据。这两个不安全的、配置错误的服务器最终暴露了大约 579.4GB 的用户记录数据（359019902 条）。暴露的服务器包含网络用户流量的

详细日志，主要包含推荐人页面、时间戳 IP、地理定位数据、访问的网页、网站访问者的用户代理数据。

（引用来源：freebuf）

2、“匿名者”入侵俄罗斯最大石油公司，窃取 20TB 数据

关键词：勒索攻击 数据泄露 关基保护

2022 年 3 月 14 日，“匿名者”声称入侵了俄罗斯能源巨头 Rosneft 德国子公司的系统，并窃取了 20TB 的数据。这一入侵的消息也得到了德国联邦信息安全局 BSI 的证实，BSI 表示支持调查安全漏洞，且已经向石油行业的其他利益相关者发出了安全警告。

据德国网站 WELT 报道，“匿名者”对俄罗斯石油公司 Rosneft 德国子公司的入侵，虽然不会影响正在进行的业务，但已经严重影响到公司系统，导致各种流程被中断，包括可能签订的合同。

“匿名者”声称已经破坏了该公司的虚拟机、不间断电源等。这次入侵很可能是在 2022 年 3 月 10 日被发现的，且数据外流也被中断。“我们的计划是提取所有可用的数据，这通过简单的 FTP 连接相对容

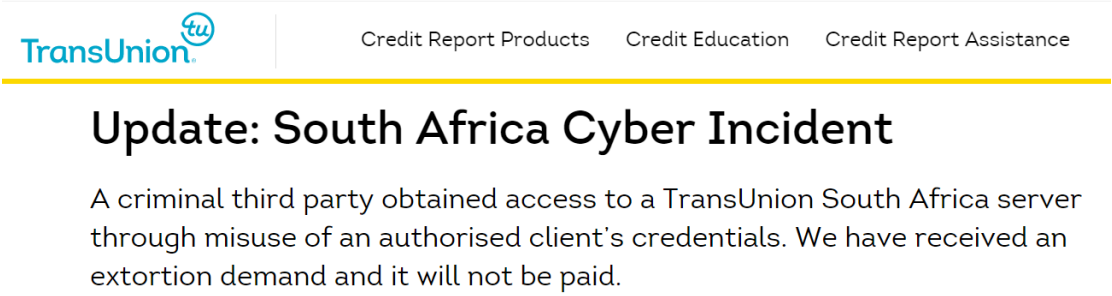
易实现，提取速度也在 5.5GB/s。然而，系统预期需要保持很长一段时间，因为人们总共可以访问近 25TB 的数据，除了备份和文件夹，还可以访问员工的 iphone 和 ipad”。

（引用来源：E 安全）

3、南非顶级征信机构 TransUnion 遭遇数据泄露，黑客索要 1500 万美元赎金

关键词：勒索攻击 弱密码 个人信息

2022 年 3 月 18 日，美国征信巨头 TransUnion 的南非公司遭巴西黑客团伙 N4aughtysecTU 袭击，5400 万消费者征信数据泄露，总数据量约达 4 TB，绝大多数为南非公民，也涉及一部分其他国家用户的记录。根据联合国统计数据，目前南非总人口为 6060 万人。

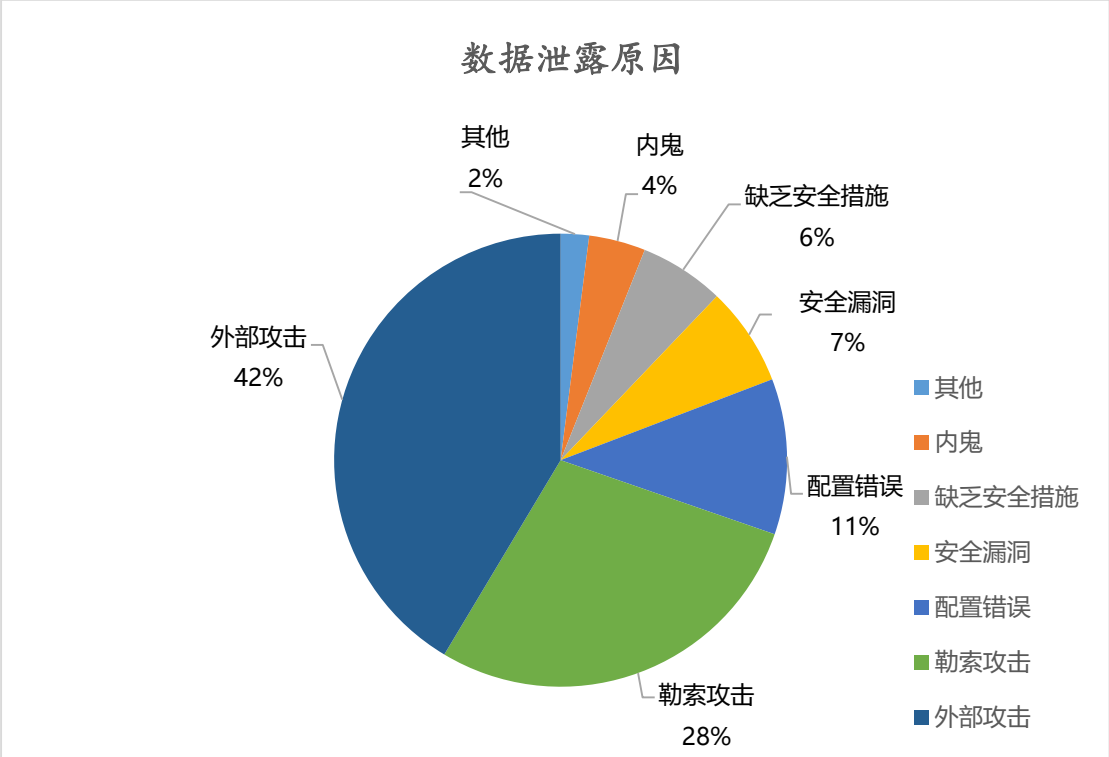


黑客团伙透露，其通过暴力破解入侵了一台存有大量消费者数据的 SFTP 服务器，该服务器的密码为“Password”，并索要约 1500 万美元的赎金。无论赎金数额是多少，此次违规事件都给所有签订过信贷协议的南非人造成了影响。TransUnion 公司称，将为受影响的消费者免费提供身份保护年度订阅服务，预计成本将超过 114 亿元。

（引用来源：bleepingcomputer）

（三）数据泄露原因

对数据泄露事件所发生的具体原因进行深入剖析，将主要原因归类为：外部攻击、配置错误、安全漏洞、内鬼、内部人员操作失误、第三方合作伙伴泄露、缺乏安全措施等，以下为主要结论。



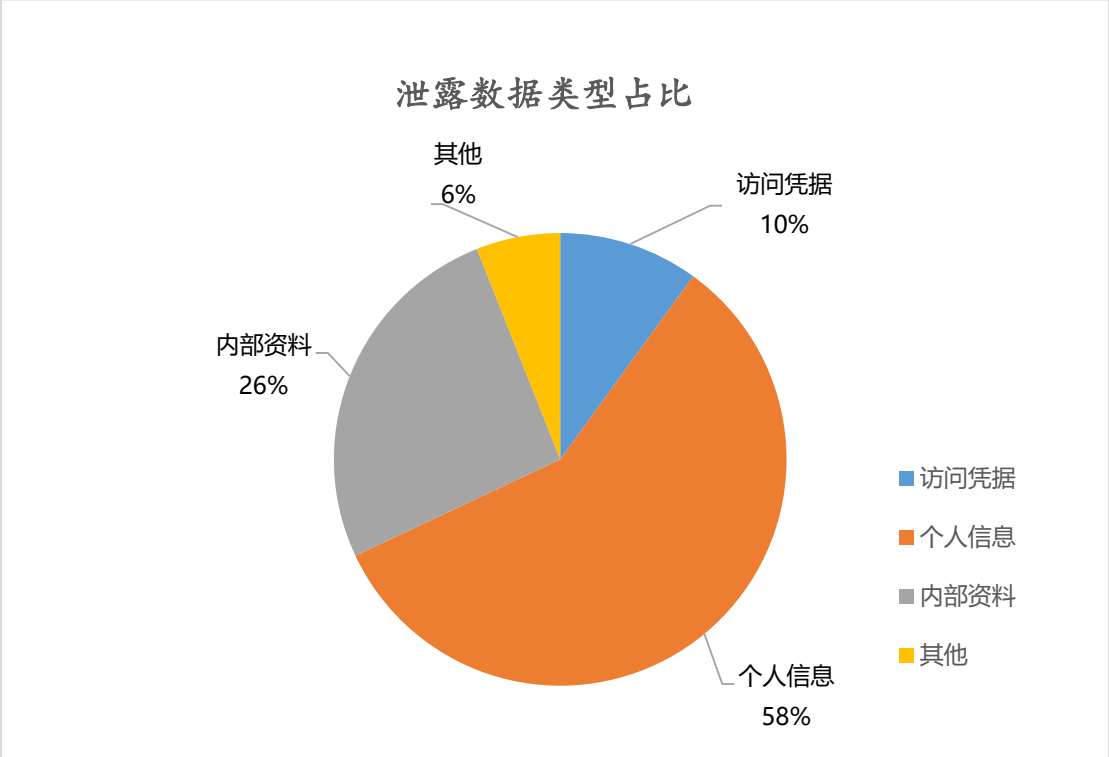
外部攻击仍然是大部分数据泄露的罪魁祸首。本报告中共有 42%的数据泄露事件可以归因为外部攻击，具体原因包括黑客入侵、网络钓鱼及未经授权访问等；

因遭受勒索攻击而导致的数据泄露占比为 28%，其中比较活跃的组织有 Anonymous、Lapsus$、Conti、LockBit 和 BlackCat 等，以数据泄露问题威胁受害者支付巨额赎金；

配置错误是导致数据泄露的第三大原因（11%），包括服务器配置不当、云存储配置错误及开发人员错误配置等；

其次，安全漏洞也是导致数据泄露的重要原因之一。本报告共有7%的数据泄露事件由安全漏洞引起，该类型主要原因包括软件本身安全漏洞、安全机制缺陷、系统缺陷或数据库漏洞等；缺乏安全措施类型占 6%，该类型主要由数据库或服务器未做任何加密等安全措施引起，使数据公开暴露而导致泄露；内鬼占比较小，仅为 4%。

（四）数据泄露类型



从泄露的数据类型来看，个人信息泄露最为严重，占据了 58%的比例，主要涉及姓名、电话、身份信息、银行卡、地址等；内部资料也是最常见的被泄露信息，26%的泄露事件涉及此类数据，其中，内部资料包括内部机密、企业商业机密信息、技术机密信息等数据；其次，10%的数据泄露涉及用户访问凭据，主要包括账号密码、口令

信息、证书及其他证明身份的信息等。

四、专题文章

《数据出境安全评估办法》如何指引数据处理者开展数据跨境活动？

大数据协同安全技术国家工程研究中心

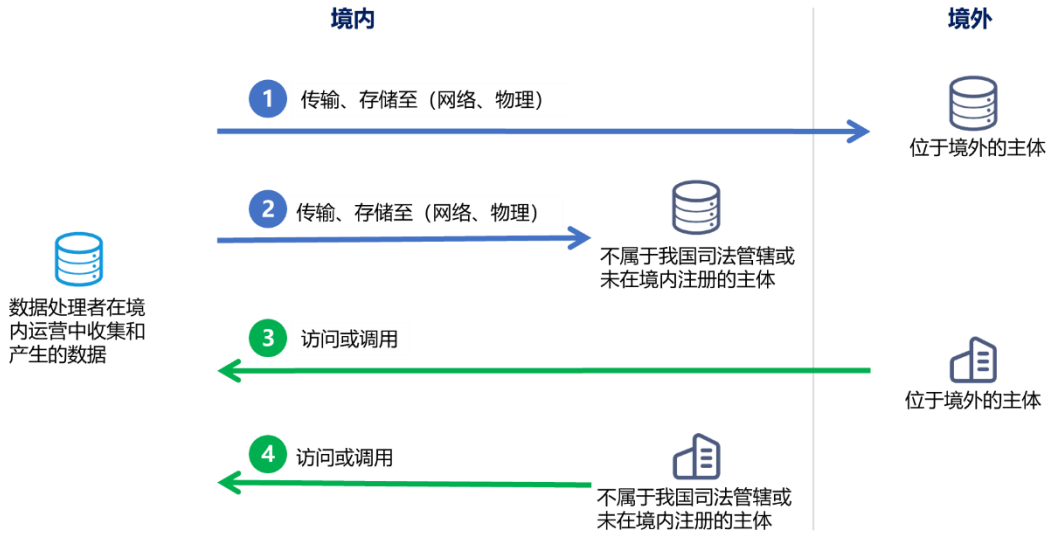
自 2016 年《网络安全法》首次提出数据出境安全评估的要求后，从 2017 年 4 月 11 日起，国家互联网信息办公室（简称“国家网信办”）三次对数据出境相关的安全评估办法进行意见征求。历时 5 年，在今年 7 月 7 日，《数据出境安全评估办法》（简称“《办法》”）正式出台，构成我国数据跨境流动安全管理制度，为数据出境提供了可操作、可落实的法律依据。

（一）什么是数据出境

《办法》第二条规定：“数据处理者**向境外提供**在中华人民共和国**境内运营中收集和产生的**重要数据和个人信息的安全评估，适用本办法。法律、行政法规另有规定的，依照其规定。”

国家网信办表示《办法》所称数据出境活动主要包括：一是数据处理者将在境内运营中收集和产生的数据传输、存储至境外。二是数据处理者收集和产生的数据存储在境内，境外的机构、组织或者个人可以访问或者调用。

结合国家标准化管理委员会在 2017 年 8 月 25 日发布的《信息安全技术 数据出境安全评估指南（征求意见稿）》中 3.7 的注释，实践中所涉及的主要场景如下所示：



1) 数据处理者在**境内运营中收集和产生**的数据，**传输、存储至**（网络、物理）**位于境外**的主体，或**传输、存储至**（网络、物理）**位于我国境内但不属于我国司法管辖**（如驻外大使馆、领事馆等）**或未在境内注册**的主体；

2) 数据处理者在**境内运营中收集和产生的数据**，可被**位于境外**的主体，或**位于我国境内但不属于我国司法管辖**（如驻外大使馆、领事馆等）**或未在境内注册**的主体**访问或调用**。

（二）申报数据出境安全评估的触发条件有哪些？

《办法》第四条对于需申报数据出境安全评估的触发条件进行了明确，包括以下 6 种情况：

1) 数据处理者向境外提供**重要数据**；

2) **关键信息基础设施运营者**向境外提供**个人信息**；

3) **处理 100 万人以上个人信息的数据处理者**向境外提供个人信息；

4) **自上年 1 月 1 日起累计向境外提供 10 万人个人信息的数据处理者**向境外提供个人信息；

5) **自上　　年 1 月 1 日起累计向境外提供 1 万人**

敏感个人信息的数据处理者向境外提供个人信息；

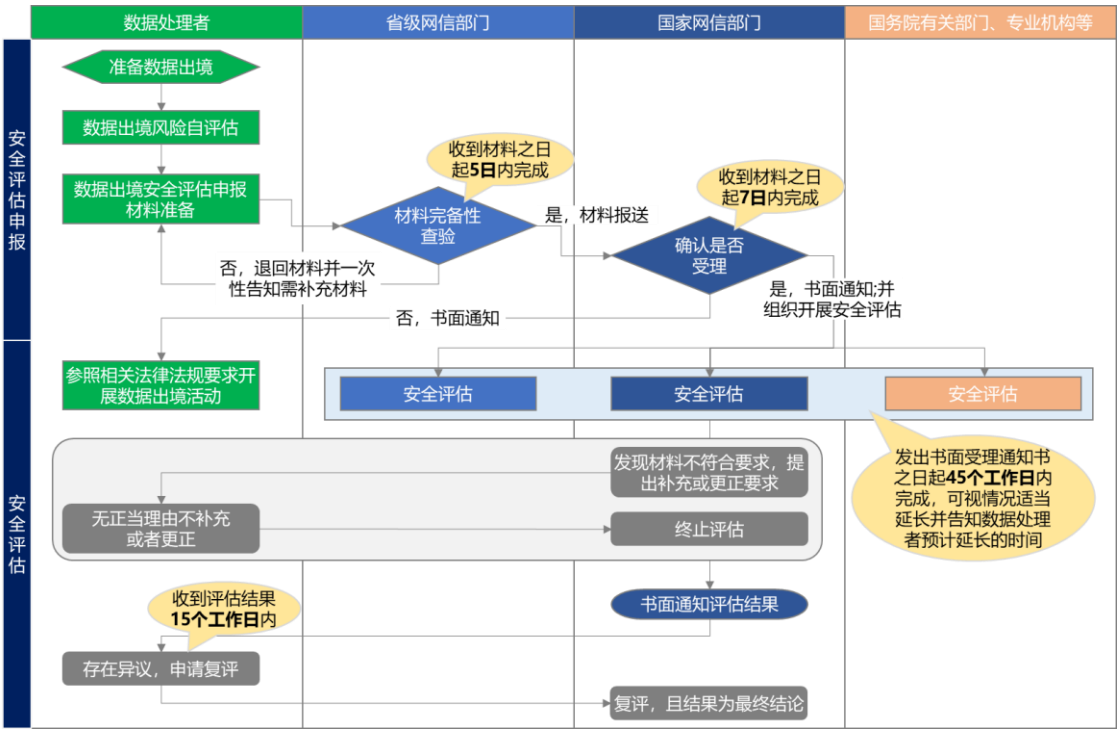
6) 国家网信部门规定的其他需要申报数据出境安全评估的情形。

以上对触发申报条件的主体性质以及提供数据的类型、规模等要求均进行了明确。

根据《个人信息保护法》第三十八条的要求，向境外提供个人信息的，可以通过**开展安全评估**、**个人信息保护认证**、**签订标准合同**、**其他条约协定**几种路径实现合规。6 月 24 日全国信息安全标准化技术委员会秘书处发布的《网络安全标准实践指南—个人信息跨境处理活动安全认证规范》，及 6 月 30 日国家网信办发布的《个人信息出境标准合同规定（征求意见稿）》，分别对**个人信息保护认证**、**签订标准合同**这两种途径进行了指导和规范。

（三）数据出境安全评估流程包括哪些事项，有哪些参与角色？

《办法》在第五、七条、十、十一、十二、十三条中明确了数据出境安全评估涉及的流程，主要包括评估申报和安全评估两个阶段，涉及的主要活动、期限及参与主体梳理如下图所示：



在第十四、十七条，明确了需要重新评估的情况及流程，主要包括三种情况：

1) **评估结果有效期满**。数据出境安全评估通过的有效期为 2 年，自评估结果出具之日起计算，到期仍需继续开展数据出境活动的，需在**有效期届满 60 个工作日前**重新申报评估；
2) **形势变化影响出境数据安全**。《办法》第十四条明确了三种影响出境数据安全的情形，若出现相关情形的，需要重新申报评估；
3) **数据出境活动违规**。若数据出境活动不符合数据出境安全管理要求的，国家网信部门发现后将书面通知数据处理者终止数据出境活动，后者需**按规整改并重新申报**评估通过后才能继续开展数据出境活动。

整个评估过程体现了第三条的评估原则：数据出境安全评估坚持**事前评估**和**持续监督**相结合。因此，在取得有效的关于数据出境安全评估通过的书面通知前，数据处理者不得开展数据出境活动。

（四）数据出境安全评估需要提交什么材料，包括哪些事项？

《办法》第五条、第八条分别明确数据安全风险自评估、数据出境安全评估的重点事项，梳理如下表所示：

关注对象	风险自评估重点事项	安全评估重点事项
	第五条 数据处理者在申报数据出境安全评估前，应当开展数据出境风险自评估，重点评估以下事项：	第八条 数据出境安全评估重点评估数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险，主要包括以下事项：
数据出境风险	（一）数据出境和境外接收方处理数据的目的、范围、方式等的合法性、正当性、必要性；	（一）数据出境的目的、范围、方式等的合法性、正当性、必要性；
数据出境风险	（二）出境数据的规模、范围、种类、敏感程度，	（三）出境数据的规模、范围、种类、敏感程度，
数据出境风险	（二）数据出境可能对国家安全、公共利益、个人或者组织合法权益带来的风险；	数据出境活动可能对国家安全、公共利益、个人或者组织合法权益带来的风险
数据接收方	（三）境外接收方承诺承担的责任义务，以及履行责任义务的管理和技术措施、能力等能否保障出境数据的安全；	（二）境外接收方的数据保护水平是否达到中华人民共和国法律、行政法规的规定和强制性国家标准的要求；
数据接收方	/	（二）境外接收方所在国家或者地区的数据安全保护政策法规和网络安全环境对出境数据安全的影响；
数据出境风险	（四）数据出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险，	（三）出境中和出境后遭到篡改、破坏、泄露、丢失、转移或者被非法获取、非法利用等的风险；
数据出境风险	（四）个人信息权益维护的渠道是否通畅等；	（四）数据安全和个人信息权益是否能够得到充分有效保障；
法律文件	（五）与境外接收方拟订立的数据出境相关合同或者其他具有法律效力的文件等（以下统称法律文件）是否充分约定了数据安全保护责任义务；	（五）数据处理者与境外接收方拟订立的法律文件中是否充分约定了数据安全保护责任义务；
数据处理者	/	（六）遵守中国法律、行政法规、部门规章情况；
其他	（六）其他可能影响数据出境安全的事项。	（七）国家网信部门认为需要评估的其他事项。

其中，风险自评估阶段重点事项在安全评估阶段均有涉及，后者从监管侧关注更宏观的数据出境风险、权益保障要求等内容。

（五）《办法》的出台，对数据处理者有什么影响？

在全球化的背景下，我国数据出境日益普遍，涉及数据出境活动的企业、组织越来越多，《办法》的出台体现国家对数据出境管控的高度重视和管控决心。对于有数据出境需求且符合安全评估要求的数据处理者，将促使其从多个方面积极建设和提升数据安全能力，包括尽快**健全自我数据安全风险防范能力**、**开展自评估**工作，**确认境外数据接收方的数据安全保护能力**，并就**双方数据安全保护责任义务达成一致**，形成符合要求的法律文件，满足出境数据安全评估通过的要求，安全、有序地进行数据跨境流动。

（六）针对《办法》提出的规定，数据处理者如何应对？

1、建立数据安全风险评估与审计机制，形成数据安全监督工作的常态化

风险是动态的，既会受数据处理者自身经营变化的影响，也会被外部合作方、市场形势、国际政策等多方面因素影响，因此建议数据处理者制定有效的数据安全风险评估和审计机制，评估与审计的对象覆盖**数据处理者自身**及**境外数据接收方**，内容包括**数据安全情况、数据安全相关承诺执行情况、个人信息保护情况**等，实现数据安全监督的持续性，以便数据处理者对于是否满足数据出境安全评估的要求进行自证，并实现第三方的数据安全监管。

2、基于数据安全能力成熟度模型评估数据出境相关责任方的数据安全保护能力

GB/T 37988-2019《信息安全技术 数据安全能力成熟度模型DSMM》根据数据生命周期，从组织建设、制度流程、技术工具、人

员能力四方面指导组织建设和评估数据安全能力。**建议国内数据处理者通过开展 DSMM 测评**评估自身数据安全防护能力，并可以基于 DSMM 对问题项、潜在风险项进行能力完善与提升；**推荐数据接收方基于 DSMM 进行数据安全能力评估**，以证明其数据安全防护能力满足数据提供方要求，具备**履行数据安全保护责任义务的能力**，以有效保障出境数据的安全。

3、及时梳理数据出境相关业务，尽快达到《办法》明确的合规要求

《办法》第二十条规定：本办法自 2022 年 9 月 1 日起施行。本办法施行前已经开展的数据出境活动，不符合本办法规定的，应当自本办法施行之日起 6 个月内完成整改。

由于数据出境安全评估需要**事前进行**，所以数据处理者要把握和利用好施行前的时间以及 6 个月的整改窗口期，厘清对于数据出境相关的合规要求、数据出境与重要数据等关键定义，盘点清楚自身涉及数据出境的业务及相关数据情况，尽快结合建议 1 和 2 明确相关部门的职责、工作流程等，达到满足《办法》要求的合规水平。

注：特别感谢北斗鼎铭律师事务所合伙人绦金伟律师对“数据出境”解释的探讨与指导

从数据利用视角探讨数据出境安全问题

大数据协同安全技术国家工程研究中心

在经济全球化与数字化的大背景下，数据流通共享成为数据要素价值充分释放的关键，必然包含国际间的数据合作。根据联合国贸易和发展会议发布的《2021 年数字经济报告》（Digital Economy Report 2021），跨境数据流动是所有数字技术的核心，全球数据流动量增长十分迅速，数据和跨境数据流动对数字经济发展的重要性与日俱增。然而，数据出境在实现全球数字经济持续性增长的同时，也可能会给一个国家、企业和个人带来很大的安全风险。因此，各国非常关注数据安全，纷纷发布数据出境安全的法规条例。

（一）典型国家地区数据出境管理做法

在各主要国家和地区的法规条例中，数据出境多被聚焦于数据的跨境流动这个维度，即数据从一个国家转移到了另一个国家。因此，各国对数据出境安全高度关切，强调数据在本国境内存储与处理、对数据出境进行安全评估。即便美国和欧盟突出数据自由流动，实质上则是采取双重标准，即数据自由流入、严控流出。

1、中国要求数据境内存储和出境安全审查

中国《网络安全法》首次在法律层面从国家安全角度对数据出境安全提出具体要求，强调在境内收集和产生的个人信息和重要数据应当在境内存储，因业务需要确需向境外提供的，应当进行安全评估。中国的《数据安全法》进一步完善了对数据出境的规定，《个人信息保护法》则具体明确了个人信息出境的管理规则。这三部上位法对数据出境安全管理的基本原则是数据境内存储和数据出境安全评估。在此基础上，中国陆续发布了数据出境安全相关的规范条例并公开征求

意见，在落地实施环节对数据跨境流动所涉及的数据处理者、数据对象、评估方法等方面给予明确指导。

2、欧盟鼓励相同规则体系下的国际数据自由流动

从 2018 年出台的欧盟《非个人数据自由流动条例》（Regulation on the Free Flow of Non-personalData）与《通用数据保护条例》（General DataProtection Regulation，GDPR）可以看出欧盟数据出境安全管理思路。欧盟致力于推动其成员国内部数据的自由流动，而对外要求其他国家只有在具有与欧盟同等保护水平的条件下，才允许将数据传输出境。“充分性认定”是欧盟核心的个人数据出境管控制度，由欧盟委员会负责对欧盟以外国家或地区的数据保护立法实施、执法能力、监管机构设置和国际条约等因素进行综合评估，最终确定数据自由流动的“白名单”国家。可以看到，欧盟这一机制促使其他国家按照 GDPR 的要求进行数据保护，以便本国企业能够与欧盟企业正常进行数据流动，进而有助于欧盟引领全球的数据合作。

3、俄罗斯强调数据本地存储、处理与严控出境

俄罗斯在《关于信息、信息技术和信息保护法》（Federal Law on Information, InformationTechnologies and Protection of Information）和《俄罗斯联邦个人信息法》（Russian Federal Law onPersonal Data）中，加强了对信息跨境传输的监管，确立了数据本地化存储的基本规则。俄罗斯对个人数据出境控制相当严苛，一是俄罗斯联邦公民个人信息和数据库需要存放在俄罗斯境内；二是对俄罗斯公民个人数据的处理活动必须使用位于俄罗斯境内的数据库；三是处理数据前履行信息告知的义务。俄罗斯同样存在与欧盟相似的“白名单”制度，要求数据接收国必须符合同等保护要求才可进行跨境数据传输，否则，只有在个人数据主体已书面同意其个人数据出境、个人数据主体作为合同

当事人履行合同等前提条件下，才可传输数据出境。

4、美国以最大化自身利益为出发点实施数据出境控制

美国基于其在数字贸易与数字技术领域的优势，极力主张全球数据自由流动，同时为遏制战略竞争对手发展，也严格限制了重要关键技术与特定领域数据出境。2010 年，美国推出“受控非机密信息”列表，并通过《出口管制条例》(ExportAdministration Regulations，EAR)，对非个人数据采取严格出境管理措施。2016 年，美国推动的《跨太平洋伙伴关系协定》（Trans-Pacific PartnershipAgreement，TPP）主张，应当允许为数据主体利益而进行的数据跨境传输，以破除许多国家所设置的数据本地化存储等市场准入壁垒。2018 年，美国出台了《澄清境外数据合法使用法案》（ClarifyingLawful Overseas Use of Data Act，CLOUD Act），通过“数据控制者”原则的适用，扩大了美国政府直接调取境外数据的权利，同时又给其他国家调取美国境内个人数据设置“符合资格的外国政府”（qualifying foreign governments）审查门槛。美国积极推行由亚太经合组织（APEC）主导的跨境商业个人隐私保护规则体系（CBPR），致力于促进 APEC 各经济体之间无障碍的跨境数据传输与流通，并与欧盟达到互认。

（二）当前数据出境及出境安全面临的困难

随着全球数字经济的发展，建立数字经济“朋友圈”的声音将会越来越大，国际间数据开放合作需求强烈。如何在安全合规的前提下促进数据出境，需要理清当前数据出境及出境安全面临的困难，才能有针对性地提出解决方案。

1、数据出境被狭义理解为数据跨境流动

当前各界对数据出境的界定仍存在差异、尚未统一。数据出境通常会被狭义地认为是物理上的跨境流动，也就是数据跨越国境，提供

给境外的主体，数据被流转到境外。随着数字经济和数据安全技术的不断发展，仅以是否跨越边境这一地理维度作为数据出境的判断标准显然已经无法适应当前各式各样的数据出境形式。实际上，数据出境至少可以有两种形式：一是通过网络传输、存储介质、开展业务、提供服务与产品销售等方式实现数据跨境流动，二是数据虽然存储在境内，但境外主体能够访问、使用和操纵境内数据。

2、确需跨境数据流动的情形有待澄清

数据跨境流动将日益频繁，无论是因投资贸易、业务合作、跨境服务而产生的数据流动，还是跨国公司内部经营管理所需要的数据转移，都是维系正常经济活动的基础，属于确需跨境流动的情况。此外，企业在面临境外司法案件时，也会需要数据跨境流动。但是，在现有的安全相关法律法规层面，并没有明确指出哪些需求属于确需向境外提供数据的情形，大多仅以“因业务需要”草草概括，这可能造成许多企业或组织无法准确识别内部数据出境场景，从而导致不必要的数据跨境流动，徒增安全风险。而且，还需明确的是数据出境目的、范围、方式和用途，这样才能消除模糊区间，有效防范数据泄露和滥用风险。

3、对重要数据的定义及范围识别难

对我国来说，并非所有的数据出境都需要安全管理，三部上位法明确了重要数据和个人信息出境应当进行安全评估。美国则强调对重要关键技术与特定领域数据出境的严格限制。因此，对重要数据的定义及识别就成为一个迫切需要回答的基础性问题。从目前的全球情况看，对重要数据的定义尚未统一，不同法域对重要数据的定义存在差异。中国国家标准《重要数据识别指南》尚处于征求意见稿阶段，离正式发布实施还有较长的路要走，而且，虽然这个指南给出了识别的基本原则和方法，但是仍需制定具体执行的实施细则，重要数据具体

目录在每个行业或地方都存在区别。

（三）对策建议

针对上述问题和困难，需要在保障数据安全和促进全球数据开放利用协调发展的原则指导下，充分利用数据安全技术进步带来的支撑，加强安全监管审计，促进全球数据合作。

1、加强安全评估，严控数据复制转移出境

采用传统的数据跨境流动方式，数据复制直接通过物理介质或互联网传输出境后，由于数据的复制和传播成本较低，数据将变得不再受控。同时，全球日益成熟的数据黑色产业链，加大了离境数据被恶意利用和买卖的风险，会给国家安全、企业利益和个人隐私带来不可估量的潜在威胁。因此，对数据复制离境这类型的出境形式，国家有关部门和行业主管部门应从严要求，将法律法规和监管要求逐项分解落实到数据出境全过程的各个环节，严格落实数据出境安全评估，确保数据跨境流动安全。

2、用隐私计算技术实现数据出境合规利用

目前，安全多方计算、可信执行环境、联邦学习等隐私计算技术和产品发展迅猛，这些作为一类希望达成数据“可用不可见”为最终效果的前沿技术，为数据出境的安全合规利用提供了一种切实可行的新方式。在隐私计算的框架下，各计算参与方的数据不出本地，能够在不泄露各自数据的前提下通过协同计算实现多源数据的跨域合作。因此，针对有出境需求的数据，通过采用隐私计算方案，在数据本身不出境的情况下，跨境进行模型训练、安全统计等多中心联合分析，可替代传统的数据复制跨境流动方式，以数据可利用实现安全合规的数据出境。

隐私计算的另一个优势在于将数据的“控制权”和“使用权”相分

离，允许参与主体以约定的使用行为对数据进行处理，同时，还可将该使用行为进行市场化交易，有效规避了权属问题。目前，我国多地大数据交易中心陆续成立，也有力地支持了这一点。因此，建议依托国际大数据交易中心，以向境外交易数据“使用权”的方式试点数据出境，既能规避数据安全风险，同时又能激励全球的数据价值挖掘。

3、加强安全监管，确保数据出境依法合规安全

无论是数据复制形式的出境以及境外仅可访问使用境内数据，还是隐私计算支持的数据跨境合作，都需要进行安全监管审计，确保数据出境行为的依法合规安全，建议构建国家级的数据出境安全监管体系，具体包括以下三个方面。

一是建设数据出境安全监管审计平台，在国家层面和各行业领域形成对各类数据处理活动特别是数据出境行为的监管审计能力，能够重点针对具有跨境业务往来的企业以及国际数据交易中心，主动对其各类关系国家安全和公共安全的数据平台进行安全监管，及时发现数据出境行为的安全风险。

二是建立专门的数据出境安全监管队伍，负责开展出境数据流通的评估、审查和监管等工作，帮助数据处理者明确各个环节的具体责任人并建立问责机制。同时，要求企业设立数据安全官岗位，负责与监管部门的对接和沟通，并做好覆盖数据出境全流程安全管理制度的整体统筹。

三是建立数据出境认定的“白名单”机制。借鉴欧盟的“充分性认定”“充分保障措施”等模式，考虑根据数据保护情况及对等措施，积极推进在“一带一路”合作框架下的双边或多边数据流通协议及机制，通过根据数据安全能力成熟度模型对数据接收方进行数据安全测评，将相关国家和地区的企业或组织纳入可自由流动的数据接收“白名

单”，构建数据出境的安全信任体系。

数字时代的数据安全新思考

大数据协同安全技术国家工程研究中心

随着数字时代发展的不断深入，数据既是驱动业务的新要素，也是创造价值的新源泉。但与此同时，数据安全问题正愈发严重，成为国家、企业等开发利用大数据的主要挑战。中国是全球数字经济最发达的国家之一，在数字经济的业务创新方面引领全球，中国也因此在数据安全领域具有最丰富的实践经验，这些对全球数据安全治理具有非常重要的参考价值。

（一）我国数据安全发展现状

数字时代的到来在促进数字经济产业发展的同时也使得数据安全进入了全球视野。我国数据安全与领先国家并无太大差距，且在数字经济规模上处于领先地位，在大数据方面具有天然优势。据联合国《2021 数字经济报告》显示，中国和美国占有全世界超大规模数据中心的一半，拥有的全球数字平台使其具有独特的数据优势。在数字技术方面，例如 5G、人工智能、计算技术等领域，中国也进入全球领先或者先进水平。因此，我国有望抓住时代机遇，在数据安全领域成为领先国家。

1、数据安全法规体系逐渐完善

随着国家大数据战略的加快实施，我国推出了一系列法律法规和相关标准加强对数据生态的监管和治理，总体来讲，我国数据安全立

法正趋于完善，法律指引日渐明确。2021 年，《数据安全法》的正式实施标志着数据安全元年的到来。作为数据安全领域的基础性法律，《数据安全法》的出台使得数据处理活动开始变得有法可依，有规可循。此后，《个人信息保护法》、《网络安全审查办法》、《网络数据安全管理条例（征求意见稿）》以及地方条例，如《上海市数据条例》、《深圳经济特区数据条例》等纷纷出台。政策法规的实施在给数据安全产业带来巨大利好的同时也使得数据安全进入了一个强监管时代。

2、数据安全逐步在国际发声

各国在数据安全领域的立法规范逐步增多，美欧等诸多国家和地区已经出台众多举措抢占国际空间数据规则的制定权，建立以本国或本区域利益为中心的数据规则体系。中国也积极探索推进全球数据安全治理规则的制定，提出营造开放、公平、公正、协作的数字发展环境的主张。2020 年 9 月，中方提出《全球数据安全倡议》，旨在为加强全球数字安全合作、推进全球数据安全治理进程贡献中国智慧。2021 年 3 月，中国同阿拉伯国家联盟签署并发表《中阿数据安全合作倡议》，双方愿以此为契机不断深化合作，共同推动全球数字治理和国际规则制定。2022 年 6 月 8 日，《“中国+中亚五国”数据安全合作倡议》通过，中国与中亚五国欢迎国际社会在支持多边主义、兼顾安全发展、坚守公平正义的基础上，为保障数据安全所作出的努力，愿共同应对数据安全风险挑战并在联合国等国际组织框架内开展相

关合作。可以看出，中国正积极构建数据安全区域合作体系，数据安全国际交流正在进入新阶段，并开始在国际发出中国声音。

3、数据安全技术、产品蓬勃发展

数据安全目前正处于高速发展的初期，在技术上，国内外都很活跃。从近几年 RSA 大会上呈现的趋势来看，数据安全热度居高不下。在 2021 年 RSAC 创新沙盒 TOP10 中，有三个企业都属于数据安全领域；在 2022 年 RSAC 中，数据与隐私安全成为十大热门议题之一，主要提及数据保护、云上数据安全、企业数据保护、数据本地化保护政策以及政府数据交易与授权访问等重点方向。国内数据安全技术、产品蓬勃发展，呈现百花齐放的态势。数据安全技术、产品体系正逐步完善，传统的数据库安全、数据脱敏、数据防泄露等技术已相对成熟，新型数据安全技术，如数据分类分级、数据资产管理、隐私计算、大数据平台安全和安全监管产品等正迎来发展良机。

4、数据安全产业投融资机会趋好

面对日益明确的政策环境，数据安全在面临强监管挑战的同时也成为了投资领域的风口，我国数据安全产业发展已经进入了快车道，数据安全的资本投入明显增多。据安全 419 的不完全统计，2022 年第一季度披露的投融资事件共有 36 起，涉及厂商 35 家，其中，数据安全领域 5 家（最多）。随着数据安全技术迭代与监管的落地实施，数据安全细分赛道投融资趋好。目前数据安全厂商都在开辟新的赛道，无明显寡头出现，数据识别、数据分类分级、数据脱敏、隐私计算和

数据安全运营等方向布局较多。

（二）数据安全面临的新挑战

数据作为新的生产要素正在成为驱动经济发展的新引擎，在数据驱动的过程中，数据安全问题也日益凸显。数据安全行业目前还处于快速发展阶段，有大量场景下的问题还有待解决，因此，数据安全行业的机会和挑战都很大。

1、数据安全事件层出不穷，大数据平台安全监管趋严

随着数字时代的到来，企业大数据平台上的数据承载量明显增多。数据量大、数据要素价值高使得大数据平台极易成为攻击的目标，数据面临着被泄露、被窃取、被滥用等风险。大数据平台往往结构复杂，且自身安全机制存在局限性，极易发生网络攻击等安全事件，数据安全关乎国家安全，数据一旦泄露将造成严重的后果。根据 IBM 发布的《2021 年数据泄露成本报告》，2021 年企业数据泄露事件的平均成本已经达到 424 万美元，同比增长 10%。为应对数据泄露等安全事件，降低数据安全风险，数据滥用识别、安全监管审计等运营安全需求已成为大数据平台的核心需求之一，针对大数据平台的安全监管与治理手段亟需加强。

2、大数据安全技术和产品亟待发展，数据安全产业创新有待加强

现在的数据安全产品只能解决局部的数据安全问题，缺乏针对数据安全的顶层设计与体系化的数据安全解决方案。大数据平台安全防

护、数据滥用防范、隐私计算、数据泄露追踪等技术的发展仍无法满足实际的应用需求，难以解决数据处理过程的机密性保障问题和数据流动路径追踪溯源等问题，大数据安全技术和产品亟待发展。此外，针对数据安全的产业创新生态建设还有待加强，目前数据创新应用场景较为单一，迫切需要提升数据安全产业竞争力，强化数据创新能力。

3、日益复杂的规则体系使得数据流通、交易和开放共享难

当前数据窃取、数据泄露、数据滥用和隐私侵犯等数据安全事件频频发生，敏感信息泄露现象非常普遍，这严重影响了社会对于数据安全和数据流通共享的信心。数据在开发利用、共享交易等动态流转过程中，也会面临敏感数据、个人信息泄露等安全风险。安全多方计算和联邦学习等新兴隐私计算技术虽然得到了广泛的研究，但都还处于初级阶段，产品运行效率难以支撑多方大数据的协同分析，实用性存在严重不足。加之数据交易流通体系建设尚未健全，仍处于探索初期，导致数据不敢开放共享，严重阻碍了数据交易和开放共享的发展。

4、数据安全人才匮乏，缺少健全的人才评价体系

当前我国数据安全人才短缺且缺少权威的数据安全专业人才培养和评价体系。随着《数据安全法》等相关法规的颁布，数据安全面临强监管与合规挑战，数据安全管理、技术等职位炙手可热。我国企业数据安全岗位大多由网络安全人员兼职，高素质的专业数据安全人才供需缺口大，特别是对于中小微企业，尤其缺乏兼具技术能力与行业经验的复合型创新人才。据 360 天枢智库《中小微企业数字安全报

告（2022 年）》分析，中小微企业极度缺乏数字安全方面的专业人员，员工安全意识和素养不足严重影响企业数字安全建设。可见，员工数据安全意识薄弱与能力不足已成为制约企业整体数据安全能力发展的关键因素。另外，我国数据安全法规制度起步较晚，对于数据安全专业人才缺乏科学分类的培养和评价体系，从而造成数据安全产业人才专业能力与安全需求脱节。

（三）数据安全发展新趋势

未来的大数据业务环境将更加开放，业务生态将更加复杂，参与数据处理的角色将更加多元，而系统、业务、组织的边界也将进一步模糊化，数据的产生、流动、处理等过程都会不同以往。

1、数据流通共享环节的安全保护和监管将得到高度关注

政府和企业都亟需对涉及关键信息基础设施的重要数据与核心数据进行严格的管控，在数据开发利用的同时，保障数据在使用和流动过程中的安全、合法、合规。具体而言，监管侧需要履行数据安全监管职责，推进事件处置式监管向常态化监管迈进；被监管的大数据相关企业或组织，则需要向监管侧证明自己具备相应的数据安全保护能力，避免在数据流通共享环节发生数据被窃取、加密勒索和泄露的情况。

2、以数据为中心的安全技术和产品将得到长足发展

数据安全将更多聚焦在数据层面的保护，一是解决因差分攻击、重标识攻击和统计推断攻击等攻击，即使是正常数据服务，也会导致

的数据泄露问题；二是解决因宽泛授权与访问控制导致的数据滥用问题；三是在云端和终端提供全面的数据处理活动的安全机制，以及数据安全统一管理、数据安全态势感知的手段和能力。

3、开放创新协同将成为适应数字时代安全领域的基本能力

新时代技术创新的复杂性不断提升，不同行业和领域的数据安全问题有很大差异性，跨界多且变化复杂。因此，拥有能够突破自己原来的领域的能力，更快速有效、更开放地学习，将成为适应这个数字时代的第一要务。利用国家工程研究中心或其他形式的开放创新平台，实现专家、问题、场景和资源等的汇聚，通过大范围开放协同创新的方式来实现持续创新，实现更好地调整和适应，必将成为数字经济时代下数据安全发展的新趋势。

（四）对我国数据安全发展的建议

首先，要意识到数据安全是个全新的问题，不能照搬之前的经验。IT 时代的安全主要是从信息系统和网络的角度关注的，数字经济时代关注的是 DT（数据技术）和数字化之后的 OT（业务技术）的安全。数据的存在形态、流动方式和频率、使用和交换方式、不同利益相关方关注的问题，都和过去完全不同。同时数字经济时代还在快速发展变化中，新技术新业务会不断出现，新的威胁手段也会层出不穷。数据安全可以参考但是完全不能依赖原来的经验。

1、积极开展并加强数据领域的国际交流与合作

全球数字经济浪潮下，数据安全问题没有国界，没有一个国家能

够置之度外、独善其身。虽然全球数据安全治理面临规则碎片化、分歧化等问题，但积极开展国内外和跨行业交流与合作，不断总结迭代，依旧是解决全球数据安全问题的关键路径。各国需要以开放包容的姿态，管控分歧，讨论建立一套普适性的数据安全治理国际合作机制，为全球数字经济发展营造公平的竞争环境。我国可以在政策、法规、标准和技术等多方面积极主导和参与，牵头经“一带一路”或国际组织形成全球共识规则及数据安全治理策略，通过数据安全能力和策略划分“朋友圈”，促进相关国家数字经济发展。与此同时，由于数据安全问题服务于数字经济的发展，涉及战略政策、法律标准、技术产品、学术教育等多个方面，而之前不同的领域相互之间交互比较少，互相并不理解。因此，未来还需要加大国内外跨行业的交流，才能实现整体上更加科学合理的数据安全创新。

2、建立以能力成熟度为核心抓手的数据安全治理机制

在发挥已有积累和保证整体协调的基础上，在全国加快推广数据安全能力成熟度（DSMM）测评咨询和专业人才培养等工作；建立科学的数据安全治理机制，基于“奖励好的、处罚坏的”原则，建立“数据安全能力强，高价值数据获取机会越多”的正向驱动关系；以DSMM为抓手，建立能力适配机制，根据数据安全能力成熟度的水平决定一个机构能够处理的数据类型和范围。依托第三方机构开展组织的数据安全治理水平评估，对于达标企业，由行业监管机构进行奖励和扶持；对未达标企业，实施项目招标和工程建设等资质方面的准入控制。以

此系统性提高我国数据安全整体水平，有效管控数据跨组织流通的安全风险。

3、加强数据安全技术和产品的建设与发展

面向城市、行业各场景下的数据安全开发利用需求，以及企业对大数据平台的安全保障要求不断提高，不断拓展的应用领域将推动数据安全技术与产品向着更加专业化、体系化的方向持续演进。行业层面，需围绕大数据平台安全、数据流通共享安全、大数据运营安全等方向，针对城市数据中台、大型平台型企业数据中心、政务数据安全等应用场景，开展数据安全顶层设计，在大力发展数据安全技术和产品的同时，实现系统建设与安全保障的有效融合与相互促进；企业层面，以数据分类分级为基础，加强特权账号管理、核心操作审计，从流量、终端、应用各方面建立数据安全能力机制，并通过实网攻防演练以及安全应急响应，做到及时改进、及时响应，而不会手足无措。

4、加大安全人才培养，鼓励人才评价创新

一是大力发展数据安全培训认证服务，扶持数据安全产业发展。由国家支持、市场运行、行业监督，加强数据安全人才培养与产业发展。支持鼓励第三方权威机构开展数据安全专业人才培训认证服务、给予数据安全企业更大的鼓励和扶持，共同推动数据安全产业发展，提供资金、人才扶持政策，为数据安全人才提供良好的就业创业环境。

二是将数据安全专业纳入高校专业学科建设。教育部增加高校数据安全学科布局，同时加强大数据安全、隐私保护、数据安全治理、

隐私计算等多个方向的研究基础。把数据安全纳入“国家关键领域急需高层次人才培养专项招生计划”支持范围，扩大研究生培养规模，并引导高校精准扩大数据安全相关学科高层次人才培养规模。

三是建立科学完善的数据安全人才评价体系。建立健全科学的人才分类评价体系，以产业需求为导向，基于岗位实际需求建立人才培养、人才评价等方面的标准体系。推进人才评价制度的创新变革，探索适应数字经济发展的数据安全人才培养新模式，建立规范的人才评价与激励机制，充分发挥人才的积极性、主动性。

《数字安全观察》版块

每周动态/政策解读/行业洞察/技术前瞻/事件分析

策略建议/国际智库精编/信创专刊/数据安全专刊/国防专刊

总编辑：杜跃进

执行编辑：张义荣 韩李云

编委会：360 天枢智库编委会

排版校对：唐会芳

如有反馈 邮件请至 dipperresearch@360.cn