零壹财经·零壹智库

数据安全问题升级：
关键领域的影响、对策与机会

研 究 机 构 | 零壹财经·零壹智库

联 合 发 布 | 中国科技体制改革研究会数字经济发展研究小组
横琴数链数字金融研究院

研究支持单位 | 欧盾链上天眼安全实验室

报 告 主 编 | 柏亮　于百程

报 告 主 笔 | 朱梅胤　赵越　李昕　温泉
赵金龙　王浙华　刘翌　王劝劝

摘 要

- ✓ 当前，数据安全已成为数字经济时代最紧迫和最基础的安全问题，加强数据安全治理已成为维护国家安全和国家竞争力的战略需要。近几年来，《网络安全法》、《数据安全法》和《个人信息保护法》等数据安全保护相关法律框架的落地或颁布，为数据安全保障提供了制度和法律支撑。
- ✓ 数据安全问题绝非只在中国存在，而是全球共同面临的问题。各国政府逐渐意识到，数据已成为与国家安全和国际竞争力紧密关联的一大要素，对数据安全的认知也已从传统的个人隐私保护上升到维护国家安全的高度。
- ✓ 我国现存“网络安全”企业共计 62.4 万家。2020 年新增 17.9 万家，同比增长 135.7%，是过去 10 年的巅峰。2021 年上半年新增 15.4 万家，同比增长 2.1 倍。
- ✓ 目前，在可统计的 225 家美国上市的中概股中，有超过七成的中概股处于破发状态。数据安全问题升级，使得中概股需要在资本市场重新做出选择。
- ✓ 随着数据安全问题甚嚣尘上，中国征信业发展也嬗变升级，征信业的政策环境、市场环境、发展模式等发生了一系列变化。
- ✓ 在法律对数据的严监管方向明确之后，隐私计算几乎是当下数据互联互通的唯一技术解，具有巨大的商业价值和应用前景。

目 录

引言

滴滴上市以及引发的一系列事件，让中国的数据安全问题和监管再次升级。

7 月 4 日，国家网信办发布通报称“滴滴出行”App 存在严重违法违规收集使用个人信息问题并下架。7 月 5 日，“运满满”“货车帮”“BOSS 直聘”被实施网络安全审查，期间停止新用户注册。7 月 10 日，国家网信办公布《网络安全审查办法（修订草案征求意见稿）》，要求掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。

这一系列事件背后，正映射着近年来国内互联网平台存在数据安全漏洞、滥用数据等乱象。数字技术促使数据应用场景和参与主体日益多样化，数据安全的外延不断扩展，数据安全治理面临多重棘手困境。

当前，数据安全已成为数字经济时代最紧迫和最基础的安全问题，加强数据安全治理已成为维护国家安全和国家竞争力的战略需要。近几年来，《网络安全法》、《数据安全法》和《个人信息保护法》等数据安全保护相关法律框架的落地或颁布，为数据安全保障提供了制度和法律支撑。

在数据安全问题升级的另一面，却是数据在经济中的重要性日益提升。

数据作为数字经济时代最核心、最具价值的生产要素，正在加速成为全球经济增长的新动力、新引擎，可以说数据正逐渐成为 21 世纪的石油。

5G、人工智能、云计算、区块链等 ICT 新技术、新模式、新应用无一不是以海量数据为基础，数据量也正呈爆发式增长态势。据 IDC 预测，2025 年全球数据量将高 175ZB。其中，中国数据量增速最为迅猛，预计 2025 年将增至 48.6ZB，占全球数据圈的 27.8%，平均每年的增长速度比全球快 3%，中国将成为全球最大的数据圈。

结合当下备受瞩目的数据发展和数据安全问题，零壹智库在本报告中将梳理中国数据和网络安全的政策、治理以及产业发展现状，并对数据安全问题影响较大的行业和技术领域，包括海外上市、征信、隐私计算等进行发展脉络、对策和机遇解读。

一、数据安全监管大势

（一）中国对于数据安全的监管与政策梳理

数据安全问题已成为当下基础的安全问题，数据安全治理也逐渐被提升到国家安全治理的战略高度。近年来，国家多次发布相关法规法案，将保障数据安全放到了重点突出的位置。据不完全统计，近 5 年来国家、地方省市以及各行业监管部门关于数据安全、网络安全已至少颁布 52 部相关法律法规。

从国家治理层面来看，2015 年颁布的《国家安全法》将数据安全纳入国家安全的范畴。2016 年发布，于 2017 年正式实施的《网络安全法》引入了网络数据的概念。

2020 年 6 月，12 部委联合发布《网络安全审查办法》，推动建立国家网络安全审查工作机制，以确保关键信息基础设施供应链安全，维护国家安全。而国家此次对滴滴出行等平台的网络安全审查，正是我国《网络安全法》《网络安全审查办法》生效之后首次公开进行的网络安全审查程序。

2020 年 8 月，《数据安全法（草案）》公开发布，从法律层面清晰定义了数据活动、数据安全，提出国家将对数据实行分级分类保护、开展数据活动必须履行数据安全保护义务承担社会责任等，明确了在我国境内依法开展数据活动。《数据安全法》将于 2021 年 9 月 1 日正式实施，其将是数据要素国家战略的基本法，强调了数据安全是数字中国重要战略举措的根本保障，体现了国家对保障数字经济安全的决心与信心。

目前我国已出台《网络安全法》、《民法典》、《数据安全法》和《个人信息保护法》四部数据安全保护基本法律框架，而围绕基本法制定的配套法规制度与相关国家规定也在加快制定出台，包括数据跨境流动、个人信息保护、新技术新应用数据安全等多个方面，部分具体法律法规情况如下。

表 1-1 国家已出台的部分数据安全法律法规

时间	发布机关	名称	内容
2016	全国人大	《网络安全法》	从“个人信息保护”“数据存储与跨境安全”“数据（信息）内容安全”和“数据系统、平台、设施安全”等角度，对数据和个人信息合规方面予以规制。

时间	发布机关	名称	内容
2020	全国人大	《民典法》	明确了隐私、个人信息的定位以及界定，明确了个人信息处理范围、主体权利、要求及原则，明确了数据活动必须遵守合法、正当、必要原则。
2020	全国人大	《个人信息安全法》	明确了个人信息处理规则、个人在个人信息处理活动中的权利、义务、履行个人信息保 护职责的部门等。
2021	全国人大	《数据安全法》	确立了数据安全管理各项基本制度；明确了数据安全保护义务及落实数据安全保护责任；强调坚持安全与发展并重，规定支持促进数据安全与发展的措施。
2020	十二部委	《网络安全审查办法》	推动建立国家网络安全审查工作机制，以确保关键信息基础设施供应链安全，维护国家安全。
2019	网信办、工信部、公安部、市场监管总局	《App 违法违规收集使用个人信息行为认定方法》	界定了手机 App 违法违规收集使用个人信息行为的六大类方法，并提出界定标准。
2019	网信办	《数据安全管理办法（征求意见稿）》	对近年来网络数据安全问题予以细化，包括个人敏感信息收集方式、广告精准推送、APP 过度索权、账户注销难等问题。
2019	网信办	《个人信息出境安全评估办法》	明确了个人信息出境安全评估的重点评估内容，规定所有个人信息出境均应当依法向网信办申报并由网信办组织开展安全评估；明确了个人信息主体在出境场景下知情权等权利履行的保障；通过系列设计加强对境外接收者的监督；全面规定了网络运营者与个人信息接收者签订的合同的具体内容。

时间	发布机关	名称	内容
2020	网信办、工信部、公安部、市场监管总局	《常见类型移动互联网应用程序必要个人信息范围规定》	明确了 39 种常见类型 APP 的必要个人信息范围，要求其运营者不得因用户不同意提供非必要个人信息，而拒绝用户使用 App 基本功能服务，旨在有效规范 App 收集使用个人信息行为并促进 App 的健康发展。
2021	网信办、工信部、公安部、市场监管总局	《移动互联网应用程序个人信息保护管理暂行规定》	确立了“知情同意”“最小必要”两项重要原则；细化了 App 开发运营者、分发平台、第三方服务提供者、终端生产企业、网络接入服务提供者等五类主体责任义务；提出了投诉举报、监督检查、处置措施、风险提示等四方面规范要求。
2020	信安标委	《个人信息安全规范》	提出了个人信息控制者处理个人信息行为的规范，旨在遏制个人信息非法收集、滥用、泄露等乱象。
2020	信安标委	《网络数据处理安全规范（征求意见稿）》	规定了网络运营者利用网络开展数据收集、存储、使用、加工、传输、提供、公开等数据处理活动应遵循的规范和安全要求。
2021	信安标委	《个人信息去标识化效果分级评估规范（征求意见稿）》	给出了个人信息标识度的四种级别，以及个人信息去标识化效果评定流程和重标识风险计算方法。

资料来源：零壹智库、数据安全治理白皮书

注：该表只列举了部分法律法规，列举顺序为数据安全相关度优先、重要性优先、时间优先的原则列举（下同）。

从地方政策的层面来看，吉林省、贵州省、海南省、广东省、天津市等省市相继出台数据相关地方法律法规，针对数据安全问题提出相应的规定。旨在探索数据开放共享与数据安全保护之间的有效平衡手段，下表展示了我国部分地方省市对于数据安全所采取的措施。

表 1-2 我国地方省市部分数据安全法律法规

时间	地方省市	名称	内容
2018	贵阳市	《贵阳市大数据安全管理条例》	保障该市辖区内大数据发展和应用的安全保护、监督管理及相关活动。要求数据安全责任单位从制度、人员、系统设备等方面对大数据安全进行保护，并要求市政府建立联席会议制度推进解决大数据安全相关重大事项。
2018	西安市	《西安市政务数据资源共享管理办法》	明确了政务公共数据权属类别，规定“政务数据资源权利包括所有权、管理权、采集权、使用权和收益权”，把政务数据作为政府的虚拟国有资产管理。
2018	天津市	《天津市促进大数据发展应用条例》	明确数据全生命周期各环节保障数据的范围边界、主体责任、具体要求；采取关键信息基础设施安全防护措施，加强防攻击、防泄漏、防窃取的技术和管理能力建设。
2019	天津市	《天津市数据安全管理办法（暂行）》	建立数据安全信息备案制度，要求组织个人信息和重要数据的数据运营者对主体信息、数据收集和使用规则、收集目的、方式、范围、类型等进行备案；建立数据安全信息通报制度，开展对监测信息、监督检查信息和上级通报信息的分析研判和风险评估，按照规定发布安全风险预警或信息通报；建立数据安全应急工作机制，定期开展应急演练，并对演练情况进行评估。
2019	海南省	《海南省大数据开发应用条例》	设立省大数据管理机构，作为实行企业化管理但不以营利为目的、履行相应行政管理和公共服务职责的法定机构；推动大数据与区块链等信息技术的融合，利用区块链技术加强数据安全保护。
2020	天津市	《天津市数据交易管理暂行办法》	建立了保障各方主体权益的数据交易全流程规范性制度；建立数据交易安全评估制度，包括数据供方出具报告对交易数据进行风险评估，数据交易机构健全第三方

时间	地方省市	名称	内容
			监督机制进行交易保护、开展事件应急处置等；健全数据交易过程的监督保障和责任追究机制。
2020	宁波市	《宁波市公共数据安全管理暂行规定》	提出数据安全政府领导原则，保护数据收集的合法性、数据的保密性以及对公共数据安全做出相关规定。
2020	深圳市	《深圳经济特区数据条例（征求意见稿）》	在诸多方面进行了大胆的尝试，设立了个人“数据权”，设置了统一的数据统筹机构，明确了公共数据作为新型国有资产，提出了各级政府设立数据工作委员会，建立决策协调机制等。

资料来源：零壹智库、数据安全治理白皮书

从行业层面来看，金融保险行业、电信和互联网行业、车联网行业、工业互联网行业近年来对数据和数据安全问题都愈加重视，中国人民银行、中国银保监会、工信部、科技部等各部门纷纷发布相应规定，旨在规范各行各业中数据安全管理工作，提高数据安全保护能力。为数据分类分级、管理能力评估、安全防护等相关工作提供了政策指导。

表 1-3 我国数据安全相关部分行业政策文件

时间	部门	名称	内容
2020	中国人民银行	《金融数据安全 数据安全分级指南》	给出了金融数据安全分级的目标、原则和范围，以及数据安全定级的要素、规则和定级过程，适用于金融业机构开展电子数据安全分级工作，并为第三方评估机构等单位开展数据安全检查与评估工作提供参考。
2020	中国人民银行	《个人金融信息保护技术规范》	将个人金融信息按敏感程度、泄露后造成的危害程度，从高到低分为 C3（鉴别信息，如银行账户、登录密码等）、C2（可识别特定主体的信息，如身份证号、用户名、交易流水等）、C1（机构的内部信息，如开户机构

时间	部门	名称	内容
			等）三个类别，对相关机构建立不同信息保护层级方面提出了更高的要求。
2020	中国银保监会	《中国银保监会监管数据安全管理办法（试行）》	围绕“信用信息采集”“信用信息整理、保存、加工”“信用信息提供、使用”“信用信息安全”及相关监督管理措施对征信业务做出规定。
2021	中国人民银行	《征信业务管理办法（征求意见稿）》	对个人信用信息采集、整理、保存和加工进行了规范；从内控制度、软硬件设备、人员管理等方面对信用信息安全和跨境流动进行了规定。明确征信机构向境外提供个人信用信息，应当符合国家法律法规的规定，包括征信机构向境外提供企业信用信息的，应当向中国人民银行备案等。
2021	中国人民银行	《金融数据安全数据生命周期安全规范》	梳理金融数据生命周期安全原则、防护要求、组织保障要求以及信息系统运维保障要求，建立覆盖数据采集、传输、存储、使用、删除及销毁全周期的金融数据安全管理框架。
2021	工信部	《智能网联汽车生产企业及产品准入管理指南（试行）》	规定了智能网联汽车生产企业应依法收集、使用和保护个人信息，实施数据分类分级管理，制定重要数据目录，不得泄露涉及国家安全的敏感信息。在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当按照有关规定在境内存储。因业务需要，确需向境外提供的，应向行业主管部门报备。
2021	网信办	《汽车数据安全管理若干规定（征求意见稿）》	明确汽车行业中重要数据的范围；对于汽车数据收集进行车内车外双场景的区分；强调最小必要原则和目的限制原则；提出数据全生命周期的处理要求；明确汽车行业数据本地化存储的原则要求和跨境数据传输的具体要求。

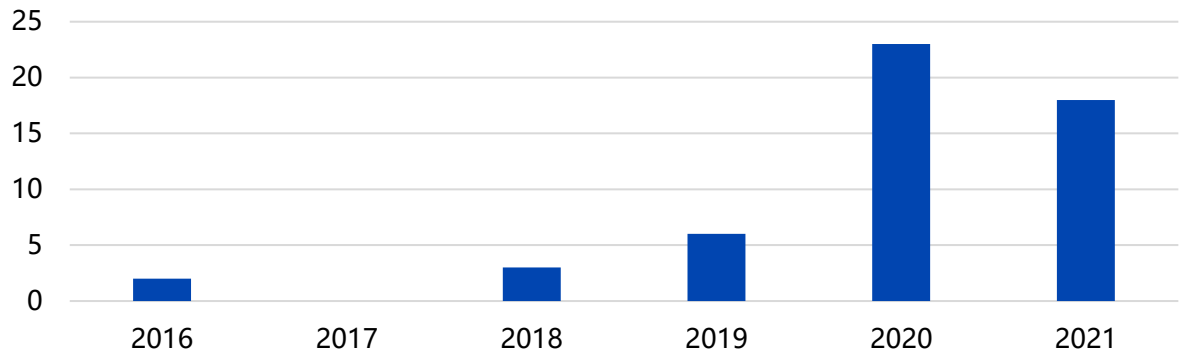
时间	部门	名称	内容
2020	工信部	《工业数据分级分类指南（试行）》	提出工业数据的基本概念，明确适用范围和原则；明确企业为数据分类分级主体，承担开展数据分类分级、加强数据管理等主体责任；按照每类工业数据遭篡改、破坏、泄露或非法利用后可能带来的潜在影响，将数据划分为 3 个级别。
2021	国家医疗保障局	《关于加强网络安全和数据保护工作的指导意见》	提出了加强医疗数据安全保护的相关要求，包括：实施数据全生命周期安全管理、实施分级分类管理、加强重要数据和敏感字段保护、强化数据安全审批管理、落实数据安全权限、推动数据安全共享和使用、建立健全数据安全风险评估机制。
2021	住房和城乡建设部	《关于加快发展数字家庭提高居住品质的指导意见》	在数字家庭系统方面，要求强化网络和数字安全保障，保障数字家庭系统安全稳定运行，防止信息泄露、损毁、丢失，确保收集、产生数据和个人信息安全。遵守密码应用规定，形成安全可控完整的产业生态系统。

资料来源：零壹智库、数据安全治理白皮书

总的来说，目前我国的数据安全相关的法律规定是基于《国家安全法》、《网络安全法》以及《民典法》建立起的，并且各省市针对地方情况会出台地方相应法律，对目前数据安全、数据跨境问题做积极探索。应对于数据应用的广泛性，各行业监管部门各司其职，对行业内数据进行管理和保护。

根据所统计已知的 52 部法律法规颁布时间，近两年数据安全的监督管理被按下了加速键，而后续法规的推出仍将持续发力。

图 1-1 截至 2021 年 6 月近几年来有关数据安全法律法规颁布数量（个）



数据来源：零壹智库、数据安全治理白皮书

2020 年之后，有关数据安全法律法规颁布数量大幅上涨，在全国各地，各行各业都对其加倍重视。到目前为止，我国数据安全监管机构机制已经初步确定，数据监管从各部门分散监管向以中央网信部门统筹协调。数据安全联合执法机制也被逐渐建立，尤其是近年来 APP 违规问题各部门联合开展整治行动，解决目前 APP、平台经济、互联网企业所存在的数据安全问题。

（二）数据安全的国际问题

实际上，数据安全问题绝非只在中国存在，而是全球共同面临的问题。各国政府逐渐意识到，数据已成为与国家安全和国际竞争力紧密关联的一大要素，对数据安全的认知也已从传统的个人隐私保护上升到维护国家安全的高度。

可以确定的是，数据安全已经成为全球性问题。国外应对数据安全的政策持续得到优化，主要体现在，一是加强数据安全顶层设计，如欧盟欧盟发布《欧洲数据保护监管局战略计划（2020-2024）》，旨在从前瞻性、行动性和协调性三方面继续加强数据安全保护，保证个人隐私的基本权利；美国发布《联邦数据战略与 2020 年行动计划》，确立了保护数据完整性、确保流通数据真实性、数据存储安全性等基本原则。二是强化数据及个人信息保护相关立法以及数据安全标准指南。

另一方面，国外数据安全保护机构设置也正不断完善，以提升执法效率，加强数据安全保护治理。得益于近几年的努力，各国推动企业数据安全保护的政策初见成效，例如，Facebook 通过开源差分隐私库加强对人工智能训练样本隐私性的保护；苹果公司通过模糊定位技术限制第三方 App 获取用户精确地理位置信息等。

国外对于数据安全的治理也正不断趋严，对大型互联网公司的数据监测、治理、执法力度持续加大，如 2019 年 Facebook 因为用户隐私问题被罚款 50 亿美元；法国、加拿大等国家也纷纷对 Twitter、谷歌等企业开出高额罚单。这种对于滥用数据优势侵害消费者隐私或进行非法数据贩卖的惩罚值得我们去借鉴。

随着数据安全逐渐上升到国家层面，各国之间数据竞争也逐渐被重视。此次滴滴被审查便存在国家层面数据泄露的可能，依据美国方面的法律，必须按照《外国公司问责法案》（Holding Foreign Companies Accountable Act）呈交以审计底稿、亦或是用户数据和城市地图为代表的部分数据，这些都是关乎国家数据主权的核心数据，可能直接影响国家安全、公共利益和社会稳定。

在大国博弈持续加剧的今天，数据作为国家重要的生产要素和战略资源，其日益频繁的跨境流动带来了潜在的国家安全隐患。一是流转到境外的情报数据更易被外国政府获取。二是我国战略动作易被预测，陷入政策被动，如美国大力推广的微观数据的汇聚分析，若在掌握我国金融数据的前提之下，便能在国际金融博弈中取得先机。三是我国以数据为驱动的新兴技术领域竞争优势被逐渐削弱，例如我国拥有全球领先的人脸识别公司商汤科技，一旦其数据被他国获取，会大大削弱我国在这一领域的竞争优势。

而某些国家尤其是美国目前正采取对中国的数据打压，将我国排除在全球数据安全治理体系之外，并可能制定针对我国的数据安全审查规则，在数据安全领域形成对我国的“包围圈”。例如，2020 年美、印、澳等多国以数据安全为由，联合对 TikTok 进行围剿，以安全调查结果违规为由，限制其使用发展。

根据 Synergy Research Group 的数据显示，截至 2020 年，全球主要的 20 家云和互联网服务公司运营的超大规模数据中心数量为 597 个，其中美国的数据中心数量远超其他国家，占比高达 40%，中国虽然位列第二但占比仅有 10%。在信息时代，这种压倒性的数据优势是极其恐怖的。中国不是“数据中心国”，但也不能沦为“数据附属国”，我们需要全力捍卫数据主权，加强数据的安全和保护。

二、网络安全、数据安全及其治理

（一）网络安全和数据安全的关系

网络安全和数据安全的关系涉及到第三个名词——信息安全。根据《数据安全架构设计与实战》一书中的论述，其发展顺序为信息安全——网络安全——数据安全。

当需要强调安全管理体系，或强调信息及信息系统的保密性、完整性、可用性，或内容合规，或 DLP（防止内部人为的信息泄露），或强调对静态信息的保护（比如存储系统、光盘上的信息）等场景时，“信息安全”一词多被使用。

当需要强调网络边界和安全域，或网络入侵防御，或网络通信系统或传输安全，或网络空间等场景时，“网络安全”一词多被使用。

当需要强调全生命周期中的数据保护，或数据作为生产力，或强调数据主权、数据主体权利、长臂管辖权、隐私保护等场景时，“数据安全”一词多被使用。

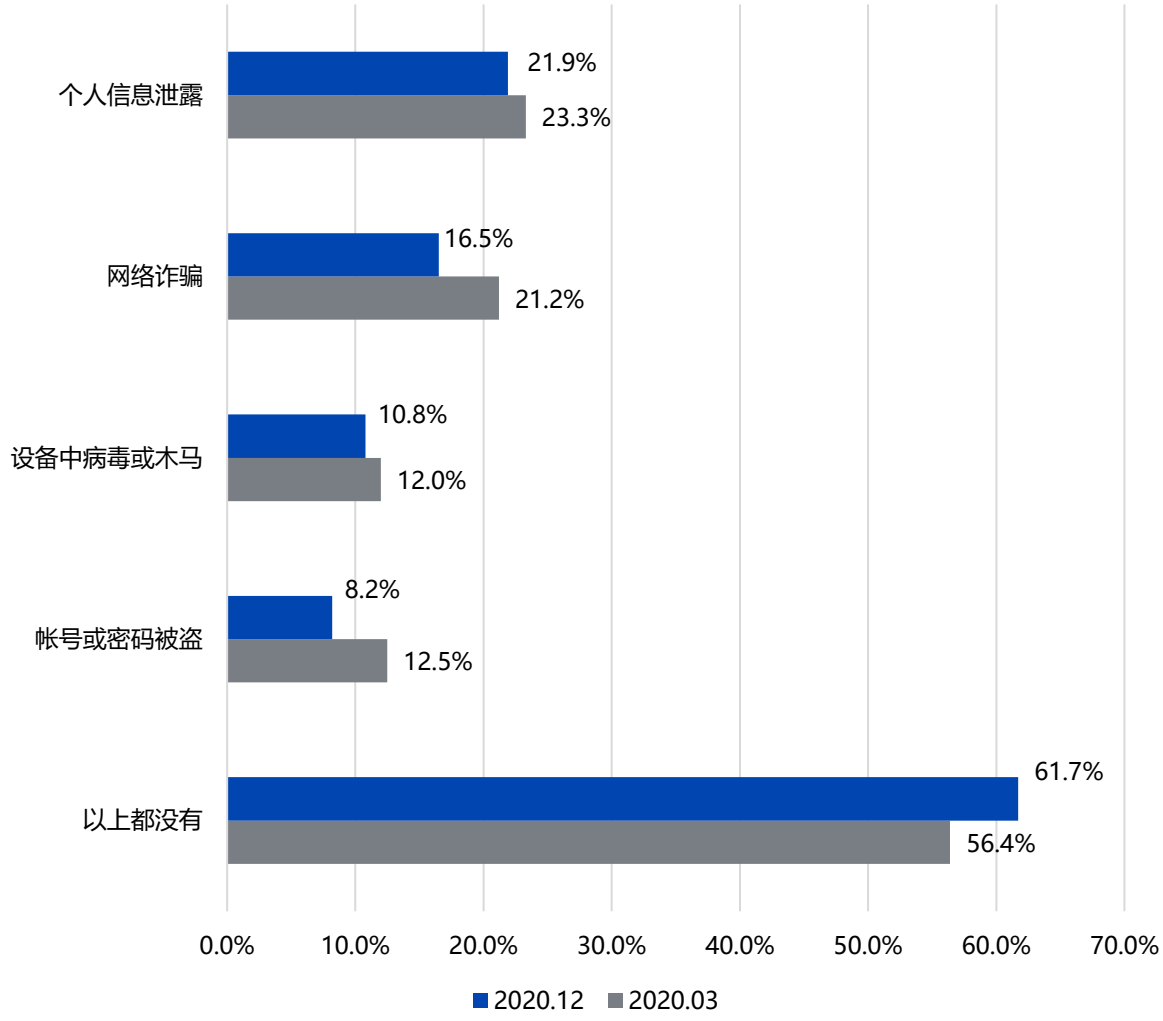
网络空间提供计算的环境，数据则作为信息的载体成为计算的对象。网络安全强调计算环境（网络空间）的安全，从而保障计算对象（数据）的安全。因此，网络安全是数据安全的前提，数据安全是网络安全的一种体现，网络安全涵盖的范围更广，而数据安全的范围更明确具有针对性。

（二）保障网络数据安全的必要性

近年来，我国网民规模不断增长，互联网普及率不断提升。根据中国互联网络信息中心和中共中央网络安全和信息化委员会办公室、中国国家互联网信息办公室联合开展的中国互联网络发展状况统计调查数据显示，截至 2020 年 12 月，我国网民规模为 9.89 亿，较 2020 年 3 月新增网民 8540 万，互联网普及率达 70.4%；我国手机网民规模为 9.86 亿，较 2020 年 3 月新增手机网民 8885 万，网民中使用手机上网的比例为 99.7%，手机网络安全成为网络安全中的关键组成部分。

随着互联网的深化普及，网络安全需求同步增长，数据安全在网络安全中的重要地位逐渐体现。同时，归功于网络安全产业的不断壮大，网络安全问题也在被不断解决。

图 2-1 我国网民遭遇网络安全问题种类及占比



资料来源：中国互联网络信息中心，零壹智库

根据中国互联网络发展状况统计调查，截至 2020 年 12 月，61.7%的网民表示过去半年在上网过程中未遭遇过网络安全问题。网民遭遇各类网络安全问题的比例均有所下降。然而，个人信息泄露仍然是最主要的网络安全问题，占比达到 21.9%，排名前四中的网络诈骗和账号或密码被盗问题都与个人信息有关，可见个人信息安全在网络安全领域中的重要地位。

根据 2021 年 4 月国家互联网信息办公室等四部门联合印发的《常见类型移动互联网应用程序必要个人信息范围规定》，国家明确规定了 39 种常见类型 App 的必要个人信

息范围，要求自 2021 年 5 月 1 日起，其运营者不得因用户不同意收集非必要个人信息而拒绝用户使用 App 基本功能服务。而在部分 App 所需的必要信息中，仍旧涉及注册用户移动电话号码、行踪轨迹、地址、证件等私密信息，加强对该类 App 的管控，确保个人数据安全的工作迫在眉睫。

表 2-1 不同 App 所需的必要个人信息

App 种类	必要信息
地图导航类	位置信息、出发地、到达地
网络约车类	注册用户移动电话号码；乘车人出发地、到达地、位置信息、行踪轨迹；支付时间、支付金额、支付渠道等支付信息（网络预约出租汽车服务）
即时通信类	注册用户移动电话号码；账号信息：账号、即时通信联系人账号列表
网络支付类	注册用户移动电话号码；注册用户姓名、证件类型和号码、证件有效期限、银行卡号码
网上购物类	注册用户移动电话号码；收货人姓名（名称）、地址、联系电话；支付时间、支付金额、支付渠道等支付信息
餐饮外卖类	注册用户移动电话号码；收货人姓名（名称）、地址、联系电话；支付时间、支付金额、支付渠道等支付信息
邮件快件寄递类	寄件人姓名、证件类型和号码等身份信息；寄件人地址、联系电话；收件人姓名（名称）、地址、联系电话；寄递物品的名称、性质、数量
交通票务类	注册用户移动电话号码；旅客姓名、证件类型和号码、旅客类型（通常包括儿童、成人、学生等）；旅客出发地、目的地、出发时间、车次/船次/航班号、席别/舱位等级、座位号（如有）、车牌号及车牌颜色（ETC 服务）；支付时间、支付金额、支付渠道等支付信息
婚恋相亲类	注册用户移动电话号码；婚恋相亲人的性别、年龄、婚姻状况

App 种类	必要信息
求职招聘类	注册用户移动电话号码；求职者提供的简历
网络借贷类	注册用户移动电话号码；借款人姓名、证件类型和号码、证件有效期限、银行卡号码
房屋租售类	注册用户移动电话号码；房源基本信息：房屋地址、面积/户型、期望售价或租金
二手车交易类	注册用户移动电话号码；购买方姓名、证件类型和号码；出售方姓名、证件类型和号码、车辆行驶证号、车辆识别号码
问诊挂号类	注册用户移动电话号码；挂号时需提供患者姓名、证件类型和号码、预约挂号的医院和科室；问诊时需提供病情描述
旅游服务类	注册用户移动电话号码；出行人旅游目的地、旅游时间；出行人姓名、证件类型和号码、联系方式
酒店服务类	注册用户移动电话号码；住宿人姓名和联系方式、入住和退房时间、入住酒店名称
用车服务类	注册用户移动电话号码；使用共享汽车、租赁汽车服务用户的证件类型和号码，驾驶证件信息；支付时间、支付金额、支付渠道等支付信息；使用共享单车、分时租赁汽车服务用户的位置信息
投资理财类	注册用户移动电话号码、投资理财用户姓名、证件类型和号码、证件有效期限、证件影印件；投资理财用户资金账户、银行卡号码或支付账号
手机银行类	注册用户移动电话号码；用户姓名、证件类型和号码、证件有效期限、证件影印件、银行卡号码、银行预留移动电话号码；转账时需提供收款人姓名、银行卡号码、开户银行信息
演出票务类	注册用户移动电话号码；观演场次、座位号（如有）；支付时间、支付金额、支付渠道等支付信息

数据来源：国家互联网信息办公室，零壹智库

表 2-2 不同 App 所需的必要个人信息（续表）

App 种类	必要信息
网络社区类、网络游戏类、学习教育类、本地生活类、邮箱云盘类、远程会议类	注册用户移动电话号码
女性健康类、网络直播类、在线影音类、短视频类、新闻资讯类、运动健身类、游览器类、输入法类、安全管理类、电子图书类、拍摄美化类、应用商店类、实用工具类	均无须个人信息 即可使用基本功能服务

数据来源：国家互联网信息办公室，零壹智库

（三）网络数据安全保障的具体措施

2019 年 6 月 28 日，工信部印发《电信和互联网行业提升网络数据安全保护能力专项行动方案》，以解决数据过度采集滥用、非法交易及用户数据泄露等数据安全问题，加快推动构建行业网络数据安全综合保障体系。

《方案》围绕加快完善网络数据安全制度标准、开展合规性评估和专项治理、强化行业网络数据安全管理、创新推动网络数据安全技术防护能力建设、强化社会监督和宣传交流五大方面提出了十四项具体任务。其中，强化行业网络数据安全管理方面的任务最为详细，要求稳步实施网络数据资源“清单式”管理、明确企业网络数据安全职能部门、强化网络数据对外合作安全管理、加强行业网络数据安全应急管理。

表 2-3：提升网络数据安全保护能力相关任务

方面	任务
加快完善网络数据安全制度标准	强化网络数据安全管理制度设计
	完善网络数据安全标准体系
	开展网络数据安全风险评估

方面	任务
开展合规性评估和专项治理	深化 App 违法违规专项治理
	强化网络数据安全监督执法
强化行业网络数据安全管理	稳步实施网络数据资源“清单式”管理
	明确企业网络数据安全职能部门
	强化网络数据对外合作安全管理
	加强行业网络数据安全应急管理
创新推动网络数据安全技术防护能力建设	加强网络数据安全技术手段建设
	推动网络数据安全技术创新发展
	加强专业支撑队伍建设
强化社会监督和宣传交流	强化社会监督和行业自律
	加强宣传展示和国际交流

数据来源：工业和信息化部，零壹智库

（四）数据要素所面临的问题与数据治理

大数据作为当下社会的一种生产要素，对人类生产产生的影响越来越重要，在数字时代更是具有独特的价值。但我国数据治理相对滞后，目前来说仍存在不少的问题。对当前问题的正确认识，也是数据安全发展必不可少的一个环节，在 8 月 1 日零壹智库“数据安全与数据治理”研讨会上，中国科技体制改革研究会数字经济小组组长陈晓华指出了目前数据要素面临四大问题。

第一，数据权属尚不明确。目前确权手段比较缺乏，现阶段还没有对数据权属问题进行过明确的法律规定。如何保障数据权属？数据交易规则？若能够交易，由于其具有可复制性的特点，数据安全又该如何保障？如何防止他人转卖自己的数据？这些无论是在技术上还是监管上都提出相应的挑战。陈晓华表示，若不能确定数据权的归

属，数据交易要走的路还很长，目前贵阳大数据交易所就面临这样的经营困窘。

第二，数据价值的问题。数据如何定价？数据作为非标品，目前很难确定它的价值，而且定价标准也尚无统一。不同的数据，针对不同的主体将会产生不同的价值，所以数据价值以何种标准界定，由谁来确定，都是亟待解决的问题。

第三，是数据隐私问题。目前数据隐私比较容易泄露，数据安全难以保障。如今数字时代，在享受数字生活给我们带来的便利的同时，数据隐私却被暴露的一览无余，对于数据隐私的保护也正是数据安全治理的重中之重。

第四，数据流通能力较弱，数据汇聚效果较差。据了解，隐私保护计算技术被视为解决数据流通不畅以及数据汇聚效果差等问题的有效手段。

对于数据治理，主要需要从三个角度进行切入。首先，最重要的还是立法，法律法规可持续，才是保障整个数据安全市场的可持续健康发展的第一要素。

第二，要从行政的角度进行管理，赋予各省市大数据管理局的相关行政权力，建议把的大数据管理局更名大数据监管局，赋予更多监管权力，以保证当前数据的安全及有效流通。

第三，要从科技的角度进行科技监管，即事前预防、事中监管、事后处置。而科技监管中最难的部分就是部委的数据共享，这在当下是一个难点，但在未来将是一个大趋势。

（五）数据安全生态加速建设

从宏观层面来看，我国在数据安全的治理，除了已出台的法规政策，以及监管机制的不断完善，数据安全产业生态建设也正在稳步推进。

一是政府积极促进企业数据安全产品和解决方案在行业场景和新基建中的应用落地。在政务、金融、交通、医疗等各行各业数据安全防护都在逐渐得到广泛应用。以专注数据安全的高新技术企业闪捷信息为例，其数据安全产品和解决方案已获取保密局、国家信息中心、公安部等权威机构认证，在商密、涉密领域均有建树，目前已与国内 1000 多家重要单位持续开展合作。

二是数据安全人才队伍正逐渐得到扩张。我国各部门组织针对数据安全问题，正通过设立相关学科与研究院、设立培训考核等方式，大力加强数据安全人才队伍建设。例如，中国信息安全测评中心成立中国网络空间安全协会大数据安全人才培养基地，并选拔国家级合作支撑单位，并开展的 CISP 数据安全治理、注册个人信息保护专业人员（CISP-PIP）认证，共同推动国家互联网网络安全大数据人才体系建设。

三是国家正大力发展数据安全示范区。数据安全产业示范区的建立会使数据安全企业与人才快速聚集，并能够对其他地区形成指导效应。2018 年，在国家认证认可监督管理委员会的支持下，贵阳经济技术开发区创建了全国首个“大数据安全认证示范区”，截止 2020 年，贵阳大数据安全示范区已聚集了大数据安全企业和相关机构约 120 家，初步形成大数据安全产业发展的生态体系，产业产值突破 18 亿元。

伴随着国家对数据安全的重视，和数据安全以及网络安全相关的企业这两年来也呈现爆发式增长。各企业面对数据安全带来的挑战都有所建树，也同样存在进步空间。第一，敏感数据识别技术向智能化发展，企业探索部署数据安全防泄露工具。数据统计，我国各大安全厂商积极研究数据防泄露技术手段，布局数据防泄露市场，2017 年我国数据泄露防护市场规模达到 7.8 亿元，同比增长 25.3%，2020 年超过 14.7 亿元。第二，结构化数据库事前、事中、事后全流程安全保障技术体系成熟，非结构化数据库安全防护手段单一。第三，数据追踪溯源技术处于研究发展阶段，大规模应用实践尚未开展，目前该技术正处在研究验证阶段，仅阿里、顺丰等部分企业探索应用，产业化应用尚不成熟。第四，数据加密技术分场景细化发展，新型加密手段逐渐涌现。第五，数据脱敏成为个人信息保护重点技术手段，企业正加强数据匿名化技术研究应用，例如阿里巴巴的数据匿名化技术已获得较大进展。

“近年来，我国网络安全产业促进政策不断加码、产品体系逐步完善、生态建设持续推进，为产业发展提供了良好环境。”中国信通院副院长王志勤日前表示。

即便如此，产业和企业的发展还是跟不上网络安全防护的需求。数据显示，2019 年美国网络安全市场规模为 447 亿美元，我国同期网络安全产业规模只有 608 亿元，仅是美国的五分之一，与我国 GDP 的体量不符。

三、数据安全典型问题和相关案例

（一）数据贩卖：大数据产业的灰色地带

随着信息技术的发展，个人数据变得愈加重要，对自己来说个人数据就如同本人身份识别，但也很有可能成为被他人利用的武器。在纪录片《监视资本主义：智能陷阱》中提到：“如果你没有为某个产品付费，那你自己本身就是产品”。换而言之，现如今使用者在享受科技时代的各种产品时，却不知自己的身份正在被“贩卖”。

目前，数据贩卖已成为大数据产业的灰色地带，个人信息倒卖黑市猖獗，对个人人身财产甚至是生命安全都造成了极大危害。

2020 年 11 月，圆通速递被曝出有多位“内鬼”有偿租借员工账号，导致 40 万条公民个人信息被泄露事件。新京报记者从知情人士获悉，涉案的为五位圆通员工，被泄露的信息中包括发件人地址、姓名、电话以及收件人电话、姓名、地址。随后，圆通发布声明进行道歉，并表示此次案件，再次敲响了信息安全风险的警钟，将持续完善信息安全风控系统和个人数据安全防护。

实际上，数据贩卖问题，甚至早已形成一条地下黑色产业链。2020 年 5 月份，江苏破获了一起特大贩卖公民个人信息案，涉案金额 2100 多万元，涉及公民个人信息 5 万多条。其中，某建设银行员工在这条数据贩卖黑色链条中发挥重要作用，自 2019 年 6 月份起开始，利用职务便利开始将相关银行卡使用人的身份信息、电话号码、余额甚至交易记录，售卖给下家，从而进行谋利。据这名员工供述，每查询一条银行卡相关信息，即可获利 80 至 100 元不等的报酬。

此外，据 2021 年 315 晚会曝光，多地商家装有具有人脸识别的摄像头，在客户毫无知觉的情况下，偷偷收集海量顾客人脸信息，涉及万店掌、悠络客、雅量科技、瑞为等公司；智联招聘、前程无忧、猎聘网等多个招聘平台业存在泄露求职者简历并被贩卖的现象，进而形成 “黑色产业链”。

数据贩卖问题持续增加，但并非是近两年才出现。2017 年 3 月，京东与腾讯的安全团队联手协助公安部破获的一起特大窃取贩卖公民个人信息案，其主要犯罪嫌疑人乃京东内部员工，盗取个人信息 50 亿条，通过各种方式在网络黑市贩卖。

如今随着数据安全防护等级提升，企业花费巨额资金保护数据不被外部盗取，然而因内部人员盗窃数据而导致损失的风险也不容小觑。此外，地下数据交易的暴利以及企业内部管理的失序诱使企业内部人员监守自盗，盗取贩卖用户数据的行为也应引起重视。

（二）数据垄断：间接引起数字权利滥用

随着数据安全内涵的延伸和扩大，对数据合法合规的收集使用也成为了数据安全的重要组成部分。当前，由于各互联网平台的业务大都由数据驱动，商业推广、精准营销、产品迭代等业务都离不开个人数据收集这个核心。各个平台利用数据在追求利益最大化的同时，也引发了个人信息滥采滥用程度加重、数据垄断乱象频发的数据安全风险。

2019 年 2 月 6 日 FCO（德国联邦卡特尔局，德国的反垄断监管机构）对 Facebook 涉嫌滥用市场支配地位行为做出处罚。在这起案件中，德国联邦卡特尔局认为 Facebook 通过用户协议条款，迫使 Facebook 用户同意公司收集和使用用户在其他平台（包括 WhatsApp、Instagram 平台以及嵌入 Facebook 插件的第三方网络平台或手机 APP）的数据，构成垄断行为。FCO 要求 Facebook 在未来四个月内调整其服务条款和数据处理活动，并提交 FCO 并接受检查监督。如果 Facebook 打算继续从社交网络外部收集数据并在未经用户同意的情况下将其合并到用户账户中，则严格控制采集的数据的处理活动，随后 Facebook 提出上诉。案件最终在 2020 年 6 月 23 日，德国最高法院做出裁定，支持 FCO 对 Facebook 滥用市场支配地位的认定以及限制其对个人数据进行处理的相关决定。

不仅仅是 Facebook，如今越来越多的 APP 出现强制授权、过度索权等数据垄断行为。同时基于数据垄断优势进行“二选一”、“大数据杀熟”等，侵犯消费者权益的行为也层出不穷。

2019 年 3 月 27 日，随着北京市消协召开“大数据杀熟”问题调查结果新闻发布会，关于大数据“杀熟”的问题终于白纸黑字被正式搬上权威台面。随着大数据“杀熟”体验调查名单的公布，飞猪、去哪儿网等平台存在不同程度的“大数据杀熟”情况。

随着类似案例与投诉的增加，2020 年“大数据杀熟”、“二选一”事件再次将各互联网平台推向风口浪尖，而后市场监管总局等相关监管部门联合对美团、拼多多等平台企业进行约谈。此外，网信办与市场监管总局、税务总局联合召开互联网平台企业行政指导会，指出信息泄露、强迫实施“二选一”，进行“大数据杀熟”等问题必须严肃整治，并要求各平台向社会公开《依法合规经营承诺》。

为预防和制止平台经济领域垄断行为，2021 年 2 月 7 日，国务院反垄断委员会制定发布《国务院反垄断委员会关于平台经济领域的反垄断指南》，强调反垄断法及配套法规规章适用于所有行业，对“二选一”、“大数据杀熟”等数据垄断问题也做了相关界定。

数据垄断将会间接引起数字权利滥用的问题，或将威胁到国家安全。因此，应当将进一步通过高额惩罚等手段对其进行约束。

（三）数据窃取：网络爬虫相关的违法案例大增

2018 年 8 月份，浙江绍兴侦破一起特大流量劫持案，涉案的新三板挂牌公司北京瑞智华胜科技股份有限公司，涉嫌非法窃取用户个人信息 30 亿条，涉及百度、腾讯、阿里、京东等全国 96 家互联网公司产品。用户在网上搜了什么、去哪儿、买了什么等这些隐秘信息，均被该犯罪团伙掌握，进而投放广告等用于商业目的，据了解，仅投放广告该公司每个月至少获利 100 万元。最终，在阿里巴巴安全部举报线索并全力协助下，警方一举将此案破获，2019 年法院公开宣判处罚罚金人民币 1000 万元，7 名被告人分别判处 3 年 6 个月至 2 年不等刑期，并处罚金。

2021 年 6 月河南商丘公开了一份判决书，显示商丘市某本科生自 2019 年 11 月起，就对淘宝实施了长达八个月的数据爬取并盗走大量用户数据。在阿里巴巴注意到这一问题前，已经有超过 11.8 亿条用户信息遭到窃取。另一名同伙利用这些信息建了 1100 个微信群，每个群 90-200 人不等，每天用机器人在群里发淘宝优惠券，赚取返利。

非法获取信息数据自互联网诞生以来便一直存在，“黑客”、不法人员通过技术手段入侵不同网站等数据源以获取信息数据，用于违法目的，甚至涉及到人身安全。随着信息技术的迅速发展，获取违法数据的技术手段逐渐提高以及获取工具的革新，门槛也相应降低。尤其是这几年“爬虫”技术的广泛应用，给予了很多不法人员对于数据窃取的可趁之机。

网络“爬虫”简单说，就是利用程序的运行实现自动的、高效的读取、收集网络数据。但由于数据性质的不同，就会造就非法爬取数据的可能。而这两年，非法爬取数据的案例大幅增长。

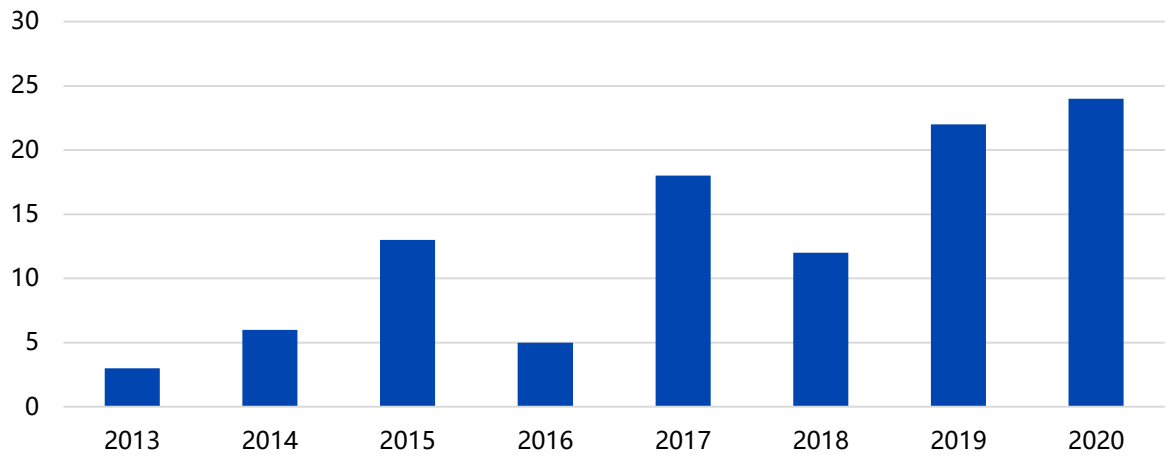
2017 年“头条视频”的前总经理宋某、视频技术负责人侯某与新东家张某合谋，利用网页爬虫技术来获取今日头条的视频数据库。该案件也是全国首例“爬虫”技术非法获取计算机信息系统数据刑事案件，于 2019 年由北京市海淀区人民法院最终审结。

2019 年 3 月份，北京警方侦破巧达科技非法获取计算机信息系统数据案，这家企业通过非法爬取用户简历并用于在网络上售卖。巧达前员工曾表示，巧达在多个网站上，建立了上千个企业账户，每天模拟人工操作访问智联招聘、猎聘等网站百万次。据悉，巧达科技非法获取的简历超过 2 亿条，而爬取的违法数据为巧达科技带来了过亿的收入。数量之大、牟利之巨，令人咋舌。最终公司法人等 36 人被检察机关依法批准逮捕。

实际上，关于网络爬虫数据窃取的违法案例远不止如此。以国内案件为范围，在通过北大法宝司法案例库全文搜索“爬虫”关键词，一共检索到案例与裁判文书 604 份；若以 “爬虫技术”关键词搜索，共检索到 124 份；若以“网络爬虫”全文搜索，共检索到案例与裁判文书 88 份。

以“爬虫技术”作为检索关键词为例，近年来的案例数量明显增多，审结年份截至 2020 年末，每年相关案例数量如下表所示。

图 3-1 2013-2020 年以“爬虫技术”关键词搜索的案例数（个）



数据来源：零壹智库、北大法宝司法案例库

同样以“爬虫技术”作为检索关键词，其案例和裁判文书按照其不同案由区分，具体数据如下。

表 3-1 2013-2021 年以“爬虫技术”关键词搜索的案例分类

案由	数量（个）
刑事	16
民事	8
知识产权	95
行政	5

数据来源：零壹智库、北大法宝司法案例库

网络爬虫获取数据最终是否构成数据窃取，主要取决于数据的合法性以及公开性。对于非法爬取网络数据的行为，也应当在政策上与技术上加强安全防护。

（四）数据泄露：2020 年全球数据泄露的数量超过过去 15 年的总和

2021 年 7 月 14 日，在第二十届中国互联网大会数据安全论坛上，中国信息通信研究院安全所信息安全部主任魏薇表示，通过研究机构统计，2020 年全球数据泄露的数量超过过去 15 年的总和。这些数据安全的风险影响范围已经从个人、企业逐步辐射到产业甚至是国家，数据安全风险隐患非常突出。

当下科技与互联网氛围，各种 APP、网页、应用内嵌小程序，都要求访问用户的位置、身份等不同信息。要求访问及获取的数据信息过多，同样会为不法分子提供可趁之机，带来数据泄露的问题。

2020 年 3 月 19 日，有用户发现 5.38 亿条微博用户信息在暗网出售，其中，1.72 亿条有账户基本信息。涉及到的账号信息包括用户 ID、账号发布的微博数、粉丝数、关注数、性别、地理位置等。主要是自 2019 年起，微博相关个人用户数据一直遭到泄露。

2020 年 4 月 27 日，联邦法院正式批准美国联邦贸易委员会（FTC）和 Facebook 之间的用户个人隐私问题和解协议，Facebook 认罚 50 亿美元。2019 年 7 月，FTC 在对 Facebook 和剑桥分析公司滥用用户数据事件进行长期调查后，就相关问题达成了和解协议。

此次事件主要是因为 Facebook 的监管失误，使得某个剑桥研究员利用自己开发在内嵌于 Facebook 的 APP，大量收集用户以及他们朋友的数据信息，最后利用这些数据信息，用于不法商业途径和政治途径。

而 50 亿美元的罚款是有史以来对侵犯隐私、泄露数据等行为对科技公司的最高罚款，或许用户数据信息在未来将会变得更“值钱”。

李彦宏曾说过“中国人为了方便，会原意牺牲一些个人隐私”。虽然用“中国人”来表达似乎有些以偏概全，但也能从侧面反映出目前用户端对信息的不重视，以及各应用对于用户信息数据收集的无理程度。

保证数据信息严密不被泄露是当下互联网企业不可忽视的一个环节，除了要求能够保证数据的全流程监控，加强目前现有风控体系之外，引入更多的新技术，打造更智能、更安全的风控系统也是必不可少的。

数据安全所存在的问题远不止如此，数据跨境流通、数据滥用、数据权归属、过度

收集用户隐私等各种问题近年来在大大小小的案例中都有所体现。可以说，目前在数据安全这个领域，无论是企业还是监管机构都还有很大的发展空间。

四、中国数据安全产业图谱

（一）数据安全产业发展的必要性

安全和发展是相辅相成的，坚持“以安全保发展、以发展促安全”一直是稳定发展的重要准则，不能单纯为了安全不发展，做好安全和发展的协调一致。在数据安全这一问题上，最终解决安全问题还是需要靠发展，一个是靠技术发展，一个是靠产业发展。

对于数据安全与数据产业发展的关系，原工信部产业政策司副司长和巡视员辛仁周在 8 月 1 日零壹智库“数据安全与数据治理”研讨会上说到：未来中国的数据产业具有巨大的发展潜力。

辛仁周表示，在过去改革开放 40 多年中，经济以 9.5%的年均增长速度稳定发展，但随着经济总量的不断扩大，尤其是技术水平和发达国家的差距正在逐渐缩小，未来的年增长率将会在 6%甚至是 5%左右。

在这种态势之下，传统经济产业在短时间内可能无法迅速拉动增长，使我们趋近甚至是超越发达国家。目前，我国存在大量产业过剩的情况，所以新兴的产业尤其物联网、人工智能、云计算等数据产业是将会是未来十几年的一大经济增长驱动点和主要发展方向。

一方面是基于数据产业巨大的市场潜力和市场需求，数据已经成为当下数字时代的硬通货，发展数据产业就是在增加国力。另一方面，基于当前外部的严峻形势和贸易战的影响，某些技术会被其他国家“卡脖子”，长期“卡脖子”对我国技术的发展极为不利，所以国家会在政策资源多方面对数据产业给予支持。

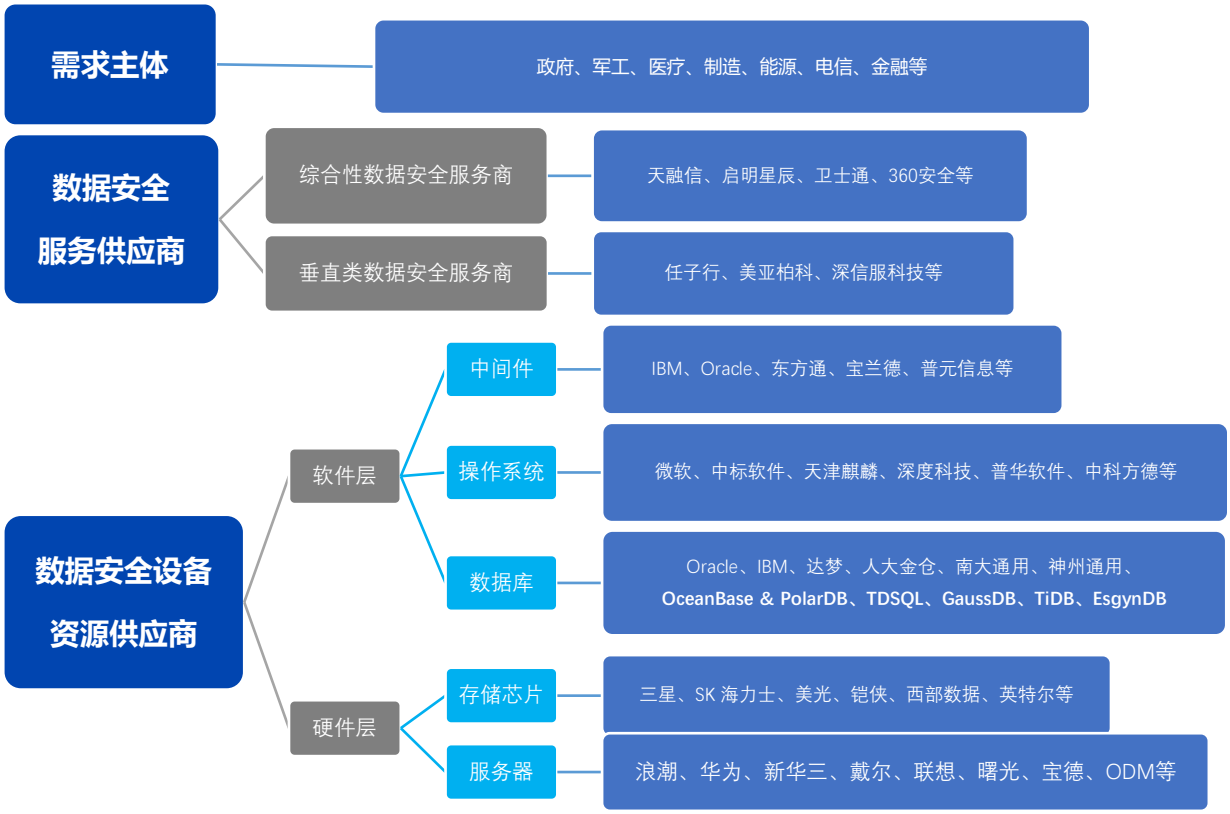
数字化、信息化时代，数据安全已经成为网络安全的重要组成部分，从数据产业目前国内的发展来看，相关产业迎来爆发式增长。据企查查数据显示，截至 2021 年 7 月 5 日，我国现存“网络安全”相关企业共计 62.4 万家。从注册量变化来看，2020 年新增 17.9 万家，同比增长 135.7%，是过去 10 年注册量的巅峰。2021 年上半年新增 15.4 万家，同比增长 2.1 倍。

数据安全在政府、金融、电信等基础设施方面有着较为广泛的应用，业务占比近 50%，且有着向医疗、制造等领域逐渐深入的趋势。据 IDC 预测，2023 年中国数据安全行业市场规模有望达到 97.5 亿美元，中国网络安全市场总体支出将达到 179.0 亿美元。[1]

庞大的市场和增长潜力，吸引了众多中上游厂商入局，产品普及度的上升也在推动

着下游需求主体购买意愿的增强。

图 4-1 我国数据安全产业图谱



资料来源：头豹研究院，零壹智库

（二）产业链上游分析

在我国，数据安全行业的上游主要是服务器、存储设备等硬件产品供应商以及中间件、操作系统、数据库等软件产品供应商。

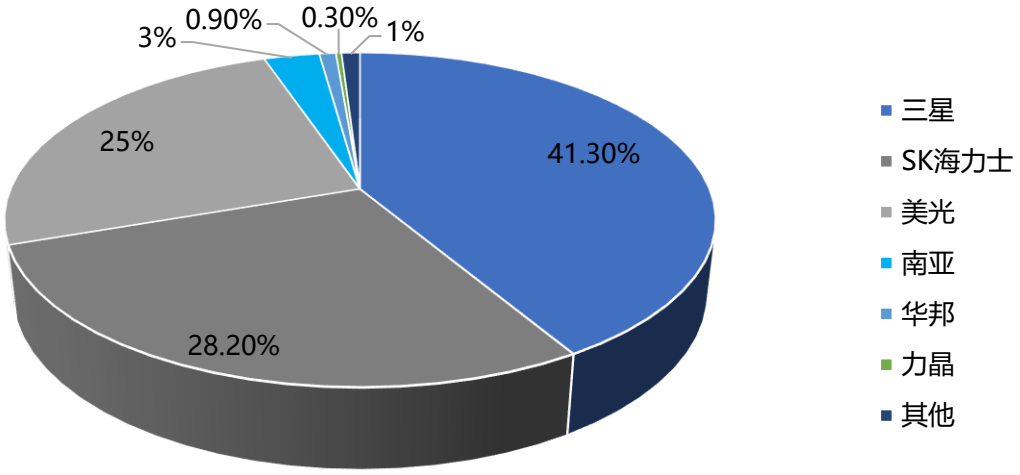
1、硬件层

存储芯片是数据安全产品的核心硬件。中国存储器厂商受限于技术以及资金实力等因素，较难满足数据安全厂商需求，对外依存度较高，采购数量占据全球存储芯片整体采购数量的 50%。

目前，全球存储器市场表现出高度集中、头部企业瓜分天下的态势，应用程度较高的主流存储器包括 DRAM 存储器和 NAND 存储器。IDC 数据显示，2019 年，DRAM 市场由三星、SK 海力士、美光三家瓜分，CR3 达 94.5%，韩国企业占七成份额。NAND 份额由三星、

铠侠（原东芝存储）、西部数据、SK 海力士、美光、英特尔六家占据，CR6 达 98.5%，其中韩国企业占四成以上。[2]

图 4-2 各企业 DRAM 市场占有份额



资料来源：前瞻研究院，零壹智库

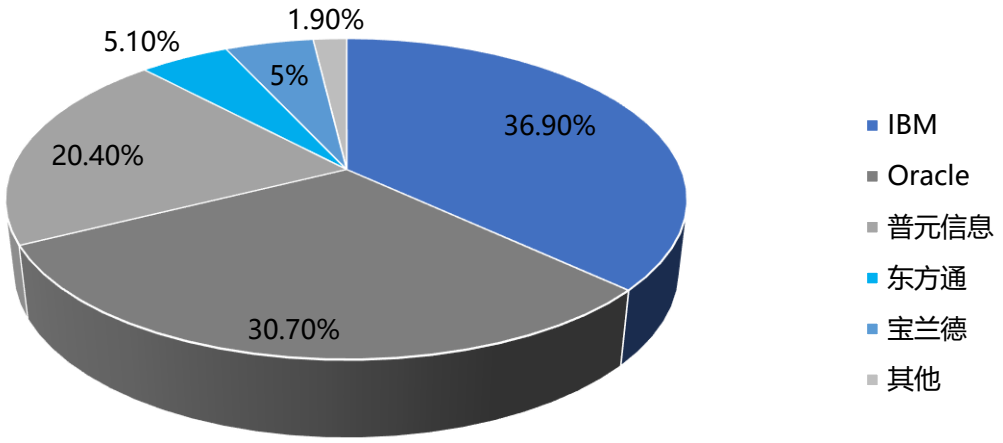
服务器是数据中心成本支出的最大部分，中国服务器行业自产率较高。IDC 数据显示，2019 年中国服务器市场前三名依次是浪潮、华为和新华三，市场份额分别为 28.7%、16.4%和 13.1%，排在后面的依次是戴尔、联想、曙光和宝德，合计占比 32.1%，ODM 厂商占比 2.9%。[3]

2、软件层

中间件是一种独立的系统软件服务程序，连接软件组件和应用。2019 年我国中间件市场总体规模达到 83.3 亿元，同比增长 15.1%。根据华为发布的《鲲鹏计算产业白皮书》，预计 2023 年，中国中间件市场空间为 13.6 亿美元，5 年复合增长率 15.7%。

我国中间件软件行业早期由国际知名厂商 IBM 和 Oracle 以领先的产品技术迅速占领了市场。随着国产中间件厂商技术的升级，以东方通、宝兰德和普元信息为代表的国产厂商赶超者，在电信、金融、政府、军工等行业客户中不断打破原有的 IBM 和 Oracle 的垄断，逐步实现了中间件软件产品的国产化自主可控，但不可否认的是，现阶段国外厂商仍然占据较大的市场份额。

图 4-3 2018 年中国中间件市场份额占比

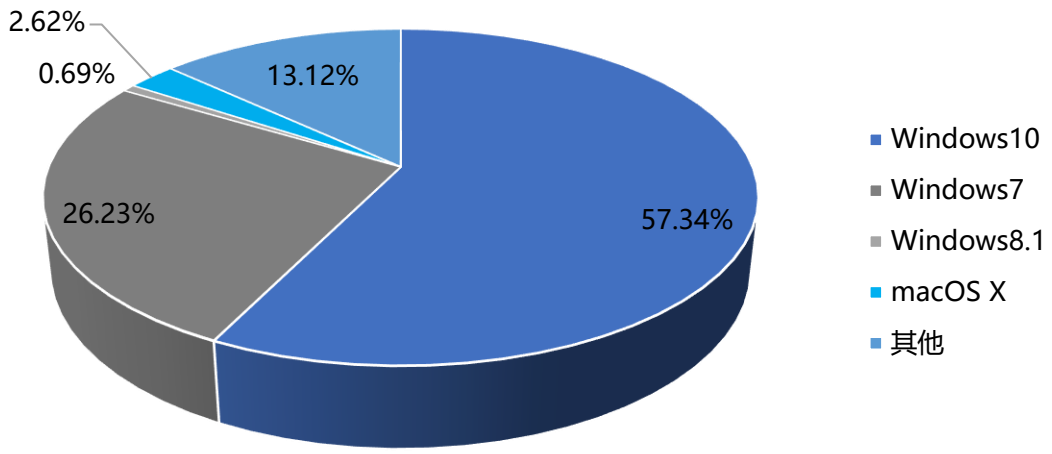


资料来源：计世资讯、天风证券研究所、零壹智库

操作系统是一个协调、管理和控制计算机硬件资源和软件资源的控制程序。Netmarketshare 数据显示，中国桌面操作系统市场中，微软的 Windows 系统一枝独秀。截至到 2020 年 3 月，Windows10 的市场份额达到 57.34%；其次是 Windows7，市场份额约 26.23%；而 Linux 系统和其他系统相加只占据 13.12%的市场份额。

在中国移动操作系统市场中，Android 系统和 iOS 系统二分天下。截至 2019 年底，Android 市场占比接近 80%，iOS 占比 20%，而其他三星、Linux、塞班等系统市场份额几乎微不足道。[4]

图 4-4 2020 年 3 月全球桌面操作系统市场企业竞争格局



资料来源：前瞻产业研究院、零壹智库

随着投入不断加大，中国的桌面操作系统也取得了重大进步，部分桌面服务器厂商完成了操作系统的自主研发和升级，如中标麒麟、银河麒麟、优麒麟等。但截止到 2020 年 3 月，Windows 系统仍占中国操作系统的 83.57%，保持垄断地位。

表 4-1 我国部分本土桌面操作系统

主流操作系统	所属企业	应用场景	芯片适配
中标麒麟	中标软件	桌面、服务器	X86、龙芯、申威、飞腾等
银河麒麟	天津麒麟	桌面、服务器	飞腾、X86
优麒麟	中国 CCN	桌面、服务器	未公布
深之度	深度科技	桌面	X86、龙芯、申威、鲲鹏等
新支点	中兴新支点	桌面、服务器、嵌入式	龙芯、兆芯、ARM 等
普华	普华软件	桌面、服务器	龙芯、申威
红旗	中科红旗	桌面、ATM	X86、ARM 等
中科方德	中科方德	桌面、服务器	兆芯
欧拉 OS	华为	桌面	X86、鲲鹏等
万里红	万里红	桌面、服务器	未公布

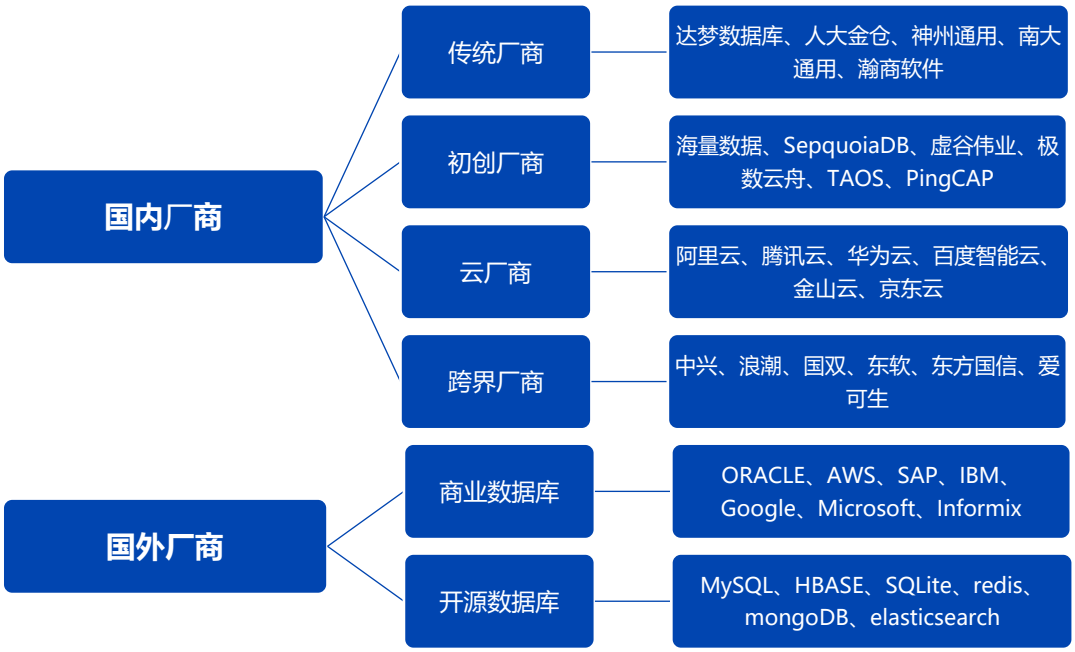
主流操作系统	所属企业	应用场景	芯片适配
一铭	一铭软件	桌面、服务器	龙芯

资料来源：头豹研究院，零壹智库

数据库是由特定软件，即数据库管理系统（DBMS）搭建、处理、维护的数据及数据间逻辑关系的集合体。它面向多种应用，可以被多个用户、多个应用程序所共享。早期，我国数据库市场主要由 Oracle 和 IBM 一统天下，21 世纪初，基于 863 计划、核高基计划等国家政策支持，一批拥有高校背景的国产厂商成立，打破了 Oracle 和 IBM 一统天下的格局。

据艾瑞统计，2020 年中国数据库市场总规模达 247.1 亿元，同比增长 16.2%。国外数据库厂商的市场份额下降至 52.6%，达梦、金仓等传统国产厂商的市场份额上升至 7.1%。在国产阵营中国，以“达梦、人大金仓、南大通用、神州通用”为代表的国产数据近年来开始发力，虽然国外数据库厂商如 Oracle、Miscrosoft、IBM 等仍占据 52.6%的市场份额，但整体市场份额正逐渐被国产数据库占领。[5]此外，阿里、腾讯、华为也投入巨资开发了自己的数据库，并逐步进入商用阶段，但市占率较低。

图 4-5 中国数据库产业图谱



资料来源：艾瑞研究院，零壹智库

（三）产业链中下游分析

1、中游分析

数据安全中游服务商通过研发、并购、合作、延伸产品线等手段丰富自身业务种类，主要包括综合型数据安全服务商和垂直类数据安全服务商。

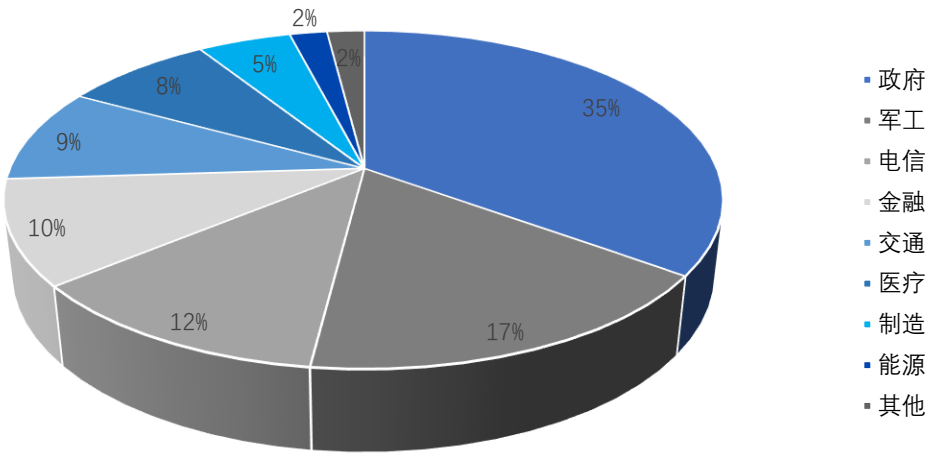
综合型数据安全服务商技术实力雄厚，通过研发、并购、合作等手段为下游各领域消费者打造全方位的数据安全解决方案，业务范围涵盖数据安全硬件、数据安全软件和数据安全服务各个方面。综合型数据安全服务商占据中游整体服务商数量的 60%，代表性企业包括启明星辰、360 企业、卫士通、天融信、绿盟科技等。

垂直类数据安全服务商深耕数据安全行业细分市场，在垂直领域的产品及服务专业化程度高于综合型数据安全服务商，垂直类数据安全服务商占据中游整体服务商数量的 40%，代表性企业有深信服、美亚柏科等。

2、下游分析

下游用户群体主要分布于政府、军工、电信、金融等领域。其中政府对数据安全的重视程度最高，在 2019 年，用户分布占行业整体的比重高达 35%；其次是军工、电信和金融领域，位居二至四位，占比均超过 10%；然后是交通领域，占比为 9%；医疗、制造以及能源领域占比分别 8%、5%、2%；而其他领域占比仅为 2%。

图 4-6 下游用户群体市场份额



资料来源：IDC，零壹智库

（四）竞争格局

1、产业巨头进军数据安全

数据安全行业的竞争促进了产品与服务的持续优化与创新，给行业技术带来了更新与迭代。我国互联网巨头入局数据安全，通过自建、投资并购协同生态发展等方式突破重围，开拓出新型产品与服务。

OceanBase 是蚂蚁金服自主研发的分布式数据库，2017 年开始对外输出，已在工行、中国移动、中国石化、中华财险、人保健康、浙商证券等机构落地应用。2008 年，阿里巴巴提出去 IOE——去掉 IBM 的小型机、Oracle 数据库、EMC 存储设备，代之以自己在开源软件基础上开发的系统，将数据安全牢牢掌握在国内企业手中。之后，阿里云多次投资与并购网络安全相关企业，包括安华金和、ThetaRay 和安恒信息等知名企业。

腾讯的 TDSQL 诞生于 2012 年，2014 年被用于 WeBank 核心系统的数据库解决方案；2015 年，作为唯一一款金融级数据库产品在腾讯金融云上正式推出，为金融、政企机构提供数据库的公有云以及私有云服务。2020 年，腾讯参与制定国家级、行业及规范，提出联合生态的力量，在数据流动过程中建立秩序。其推出的数盾是一套基于数据流的数据安全解决方案，帮助客户解决云上数据安全治理问题，满足等保合规要求的同时，也能提升数据隐私保护能力。

还有华为的 GaussDB OLAP 数据库，2015 年在工商银行上线，替代了海外的数据仓库。2018 年 GaussDB 又陆续在招行部署上线，包括综合支付交易、信用卡的重资产营销、金融科技类的项目。华为云空间为亿万终端用户提供了个人云空间功能，能够帮助用户更便捷地管理数据，并保障数据安全，保护用户隐私，这也正让数以亿万计的用户能更好地进入万物互联的智能世界和数字时代。

2、专业数据安全服务商

以安华金和、奇安信、天融信、优炫软件等企业为代表的专业数据安全服务商专注于用户核心数据保护，围绕数据资产为客户提供稳定、安全、行业领先的产品与解决方案。同时，这些专业服务商打破技术壁垒，实现单品向产线化扩张，加深产品在各应用领域的渗透率，提升自身竞争力。[6]

例如安华金和的产品由数据库加密向数据库漏扫、数据库审计、数据库防火墙布局、扩大产线范围，丰富企业类型，形成数据安全防护“产品+工具+服务”的创新型商业模式。优炫安全增强系统（RS-CDPS）通过安装在服务器的安全内核保护服务器数据，通过

截取系统调用实现对文件系统的访问控制，以加强操作系统安全性，可对 UNIX 类、LINUX 类、WINDOWS 类各种操作系统进行统一管理。

3、传统数据安全服务商

以启明星辰、360 企业、卫士通、美亚柏科等企业为代表的网络安全企业在资源方面优于其他行业参与者。例如卫士通、启明星辰在安全、管理和平台运营等业务领域拥有众多政府和军工客户资源，是传统网络安全企业中政企类业务占比最大的两家企业。

传统网络安全企业的发力方向各不相同，如卫士通专注于央企用户的运维转型，启明星辰致力于维护政府客户，市场分割较明确。部分传统网络安全企业通过投资并购布局新型安全服务领域，例如 360 企业安全集团融资金额达数十亿元，凭借资本示例和自身在终端安全、大数据处理和分析、威胁情报领域优势，快速拓展其在党政军、金融、公安、电信等行业的信息安全市场，实现销售额 4 年 6 倍的增长速度。

五、中国网络安全产业架构与发展态势

（一）我国网络安全发展概况

1、中国网络安全保障快速发展

2014 年是中国接入国际互联网 20 周年。2014 年 2 月 27 日，中央网络安全和信息化领导小组成立，国家主席习近平亲任小组组长。该小组将研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设，不断增强安全保障能力。

2014 年 11 月 19 日，中国举办了国内有史以来规模最大、层次最高的互联网大会——第一届世界互联网大会。2015 年 12 月 16 日第二届世界互联网大会举行，多国政府代表参加了大会，习近平就“中国网络空间发展和安全”发表主旨演讲。2015 年 7 月 6 日《中华人民共和国网络安全法》公布，并向社会公开征求意见。我国网络空间的治理，正式做到有法可依。

2、中国网络安全立法进程

1994 年，公安部颁布了我国首个计算机安全方面的法律——《中华人民共和国计算机信息系统安全保护条例》，标志着我国开始重视信息安全工作。21 世纪开始，随着互联网的普及和网络违法行为的增加，我国网络安全领域的立法开始加速。

从 2000 年国务院制定《互联网信息服务管理办法》，到 2016 年 11 月第十二届全国人大常委会通过《中华人民共和国网络安全法》，我国网络安全在国家安全中的地位上升到前所未有的高度。未来，我国将进一步出台《个人信息保护法》、《数据安全法》等相关法律法规，提升对公民信息数据的保障，完善网络数据安全法律体系。

表 5-1：我国网络安全立法时间线

时间	事件
2000 年 10 月	国务院出台《互联网信息服务管理办法》
2012 年 12 月	全国人大常委会通过了《关于加强网络信息保护的决定》

时间	事件
2015 年 7 月	全国人大常委会通过了《中华人民共和国国家安全法》
2016 年 11 月	全国人大常委会通过了《中华人民共和国网络安全法》，开启我国信息网络立法进程，不同于以往层位阶较低，分散化、碎片化的法规，奠定了整个信息网络立法的基础
2019 年 7 月	《云计算服务安全评估办法》正式发布，以提高党政机关、关键信息基础设施运营者采购使用云计算服务的安全可控水平
2019 年 9 月	工信部《关于促进网络安全产业发展的指导意见（征求意见稿）》公开征求意见
2019 年 12 月	网络安全等级保护 2.0 相关国家标准正式实施
2020 年 1 月	《中华人民共和国密码法》正式施行，同时《个人信息保护法》《数据安全法》被纳入 2020 年立法计划
2020 年 3 月	成都市经济和信息化局印发《成都市加快网络信息安全产业高质量发展的若干政策（征求意见稿）》
2020 年 4 月	长沙市工信局、市财政局联合印发《长沙市关于加快网络安全产业发展若干政策实施细则》
2020 年 4 月	国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、财政部、商务部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局联合制定的《网络安全审查办法》正式公布
2021 年 6 月	全国人大常委会通过了《中华人民共和国数据安全法》

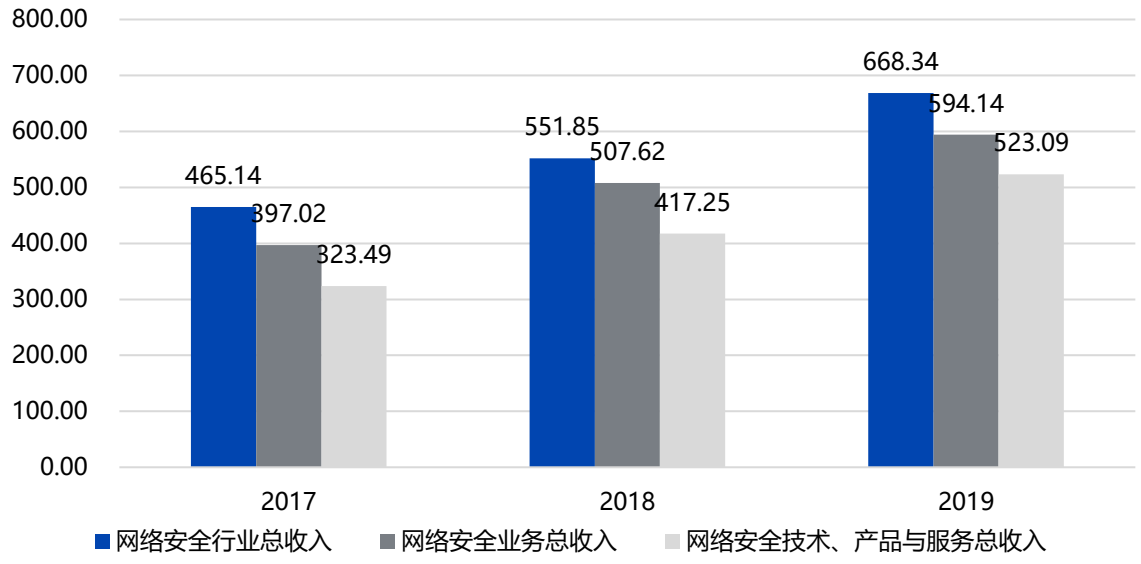
数据来源：公开资料整理，零壹智库

（二）中国网络安全产业架构

1、中国网络安全产业规模

根据工信部 2021 年 7 月发布的《网络安全产业高质量发展三年行动计划（2021-2023 年）》，到 2023 年，我国网络安全产业规模将超过 2500 亿元，年复合增长率超过 15%。我国网络安全产业规模的不断增长，同时也推动网络安全行业收入不断增加。

图 5-2 近三年国内网络安全行业及相关业务、服务总收入（亿元）



资料来源：中国网络空间安全协会，零壹智库

根据 2020 年 7 月发布的《2020 年中国网络安全产业统计报告》数据，2019 年，国内网络安全行业总收入（网络安全业务的企业的总收入）约为 668.34 亿元，同比增长 21.11%；网络安全业务总收入（网络安全行业总收入减去非安全业务收入）约为 594.14 亿元，同比增长 16.14%；网络安全技术、产品与服务总收入（网络安全业务总收入减去安全集成业务收入）约为 523.09 亿元，同比增长 25.37%。在 2017 年至 2019 年期间，网络安全行业总收入年均增长率达到 19.87%。

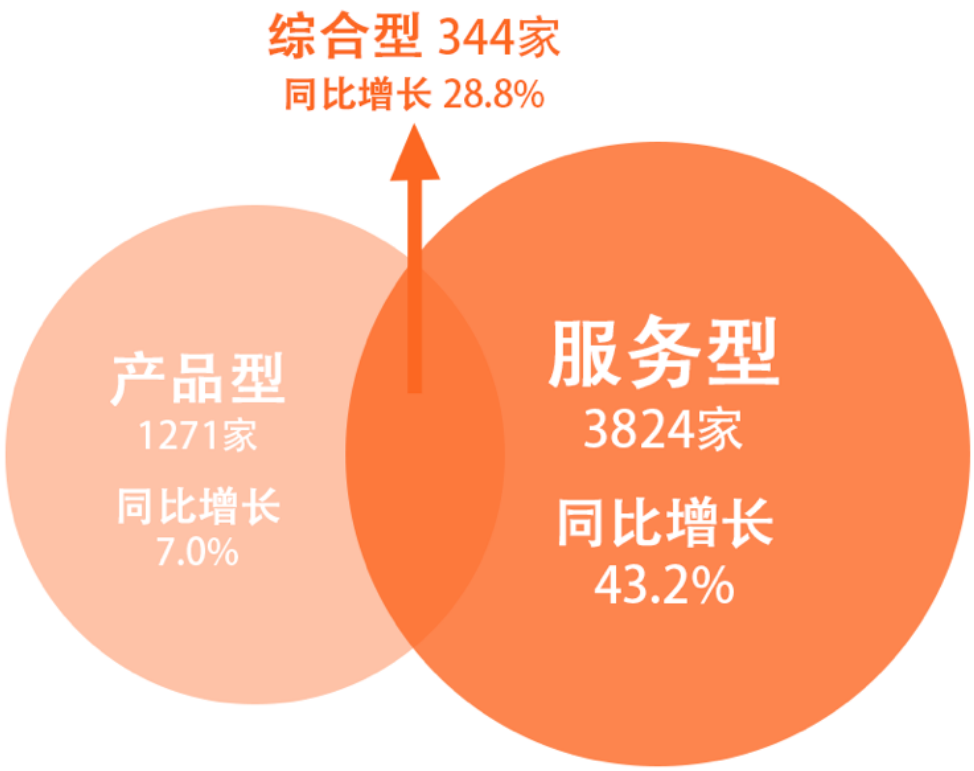
随着国家对网络安全领域重视度的提升，网络安全市场规模增速预计将进一步提升，在未来几年内保持高于 20%的平均增长率。

2、中国网络安全企业分析

1）中国网络安全企业概况

近年来，我国网络安全产业规模不断扩大背后的原因是网络安全企业数量的激增。根据中国网络安全产业联盟发布的《2021 年中国网络安全市场与企业竞争力分析》（下文简称“网安竞争力报告”）统计，2021 上半年我国共有 4751 家公司开展网络安全业务，相比上一年增长 23.1%。其中，服务型公司达到 3824 家，同比增长 43.2%，产品型公司达 1271 家，同比增长 7.0%，综合型公司（兼顾产品和服务）达 344 家，同比增长 28.8%。

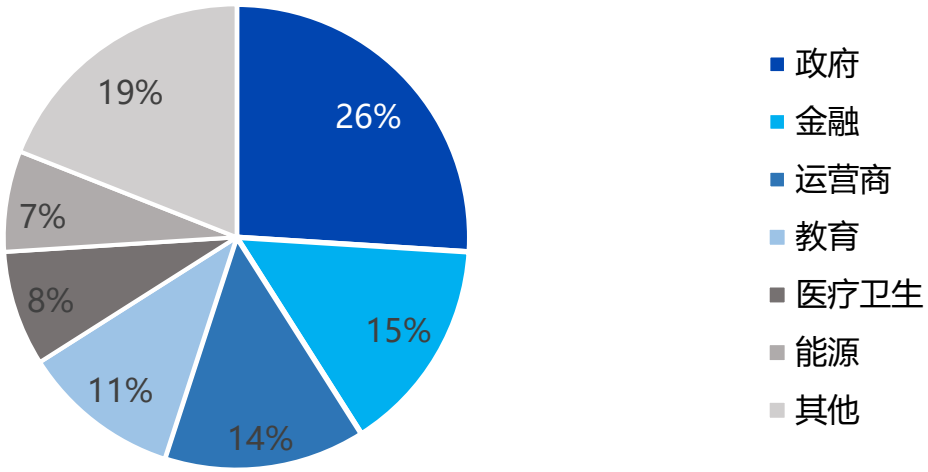
图 5-3 我国网络安全公司类型分布



资料来源：中国网络安全产业联盟，零壹智库

在 4751 家公司中，按我国网络安全企业服务的行业划分，26%的企业主要为政府服务，15%的企业主要为金融机构提供服务，排名前六的服务领域分别为政府、金融、运营商、教育、医疗卫生、能源等。可见，网络安全需求较大的领域主要为政府领域、金融领域和公共领域（如教育、医疗卫生等）。

图 5-4 我国网络安全公司服务领域分布

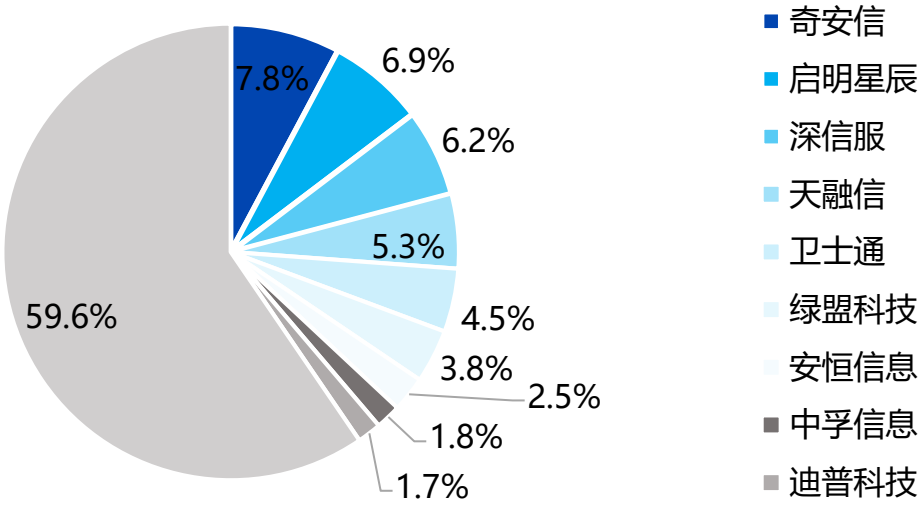


资料来源：中国网络安全产业联盟，零壹智库

2）中国网络安全头部企业分析

根据《网安竞争力报告》数据显示，2020 年中国网络安全行业主要企业中，奇安信、启明星辰、深信服等三家公司的市场占有率均超过 6%。

图 5-5 我国网络安全企业市占率



资料来源：中国网络安全产业联盟，零壹智库

市占率排名前九的企业合计占有率 40.4%，以 4751 家网络安全公司总量作为基数，显示出我国网络安全产业领域市场集中度较高。市占率排名前九的企业中，中孚信息和安恒信息的安全业务营业收入增速超过 40%，显著高于头部企业平均增速，发展态势迅猛。同时，头部企业安全业务营业收入平均增速达 27.9%，高于行业平均值，因此 2020 年头部企业市占率相比上一年小幅提升。报告预计，未来两三年内，头部企业市占率仍将保持小幅增长趋势。

表 5-6 国内头部网络安全企业安全业务营收及增速

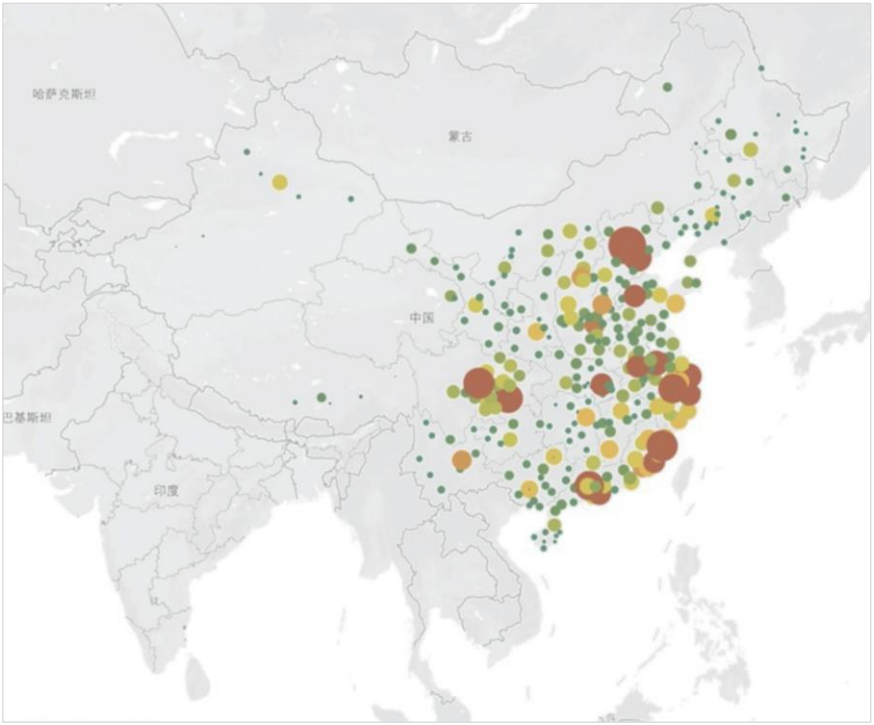
公司	安全业务营业收入（亿元）	安全业务营业收入增速
奇安信	41.6	31.9%
启明星辰	36.5	18.0%
深信服	33.5	17.8%
天融信	28.3	17.1%
卫士通	23.8	13.3%
绿盟科技	20.1	20.3%
安恒信息	13.2	40.1%
中孚信息	9.9	64.7%
平均值	25.9	27.9%

数据来源：中国网络安全产业联盟，零壹智库

3）中国网络安全客户分布

根据《网安竞争力报告》统计，2018 年至今中国网络安全客户总量超过 15 万家，其中持续在网络安全投入的客户超过 2 万家；据不完全统计，2020 年我国网络安全客户数超过 9 万家，其中新增客户数量超过 3 万家。

图 5-7 我国网络安全客户分布地图



资料来源：中国网络安全产业联盟

从客户分布情况来看，呈现聚集效应，我国网络安全的客户主要分布在京津冀地区，长三角和珠三角地区，近两年西南川渝地区客户数量增长显著，成为了新的聚集区。总体来看，我国网络安全客户分布与 GDP 有较强相关性。

（三）网络数据安全发展中的机遇与挑战

1、网络安全立法加速，法律体系日趋完善

近年来，随着个人数据遭遇滥用事件的频频发生，我国网络安全立法加速跟进，网络安全法律制度体系日趋完善。《国家安全法》从宏观角度确定了我国在网络领域的战略和方针，而《网络安全法》则更为详细地规定了网络运营者在保障数据安全、维护个人隐私方面的责任。将于今年 9 月实施的《数据安全法》在国家的网络数据保护责任、安全保护分级制度等方面与《网络安全法》衔接，与《网络安全法》相辅相成构建我国网络信息数据安全法律体系。未来，《个人信息保护法》的制定和推出将对个人信息流通和使用进行规定，进一步完善我国网络数据安全的法律法规体系。

依法治国，首选要有法可依，近年来国家不断出台信息安全、网络安全和数据安全

等领域的法律法规，为保障网络信息数据安全奠定了基础。随着我国相关法律法规的不断完善，企业、个人对于数据的运用也将更加合规，国家、企业、个人的数据和隐私安全将得到更好的保障。

2、网络安全知识普及，隐私保护意识增强

手机 App 滥用、泄露个人信息事件频发，国家网络安全立法的不断推进以及网络安全知识的不断宣传普及使得公众的个人信息、隐私保护意识不断增强。根据南方都市报大数据研究院·南都个人信息保护研究中心于 2019 年 12 月发布的《2019 个人信息安全年度报告》，95%的受访者曾遭遇个人信息泄露，其中超过一半的受访者会向 12321、消协、App 专项治理工作组等举报，其次是向相关企业客服投诉、自行在网上或找媒体曝光、请律师打官司，只有 14.92%的受访者选择无奈接受。同时，近八成受访者会主动做隐私相关的设置，有约三成受访者愿意为隐私保护付费，其中，65.07%的受访者接受每月 0 元至 30 元的付费；其次是 30 至 60 元，占 23.50%。

公民自身数据保护意识的提升，能有效减少不法分子或者是违规 App 收集、使用个人数据的机会，从源头遏制数据泄露，保护数据安全。

3、个人信息遭遇滥用，企业赴美监管困难

在信息化的时代，公众无时无刻不在使用自己的个人信息，从网站的注册登录，到 App 的信息记录，大数据甚至能够通过对某个人的数据进行分析从而获得其精准画像，而这仅仅需要采集必要信息就可以做到，如果网站或者软件违规采集用户更为广泛的数据信息，甚至把这些数据分析处理后泄露境外，将会对我国公众安全甚至国家安全造成重大威胁。

同时，部分企业远赴美股上市使得监管更加困难。在中美摩擦不断加剧的当下，我国的数据安全更需要时刻得到保障。有关部门应当对采集个人敏感数据的赴美上市企业进行严格审查，设立数据隔离机制，谨防数据泄露。

六、中概股赴美上市拐点：数据安全的影响和应对

滴滴、BOSS 直聘、运满满等上市后被实行网络数据安全审查后，传言 Keep、喜马拉雅等互联网企业均搁置赴美 IPO 计划，便利蜂也否认提交美国 IPO 的申请。随着互联网企业的数据安全已经上升到国家层面，中概股赴美上市的拐点似乎已经到来。

中概股赴美之路，已有 20 多年的历史。2000 年前后，一大批互联网企业掀起赴美上市的高潮，新浪、网易、搜狐等相继登陆美国市场，中概股群体迅速壮大。究其原因，第一是中美两国资本市场的政策差异明显，美股上市门槛更低，尤其是国内 A 股针对企业的盈利要求，互联网企业一般难以达到。第二是相较于国内市场，美国资本市场更为成熟，更有助于互联网企业的国际化战略。第三是国内的互联网企业，股东及投资者中有很大一部分来自国际投资机构，而美国资本市场一直是全球投资者聚集的摇篮。

中国企业赴美上市，募集全球资金反哺到中国市场，中国企业也因此有机会参与到全球化浪潮中。原本平衡的商业秩序却在当前国家关系中隐藏着巨大变量，二十多年的中美资本市场稳定似乎正在被悄然打破。

（一）中概股近期在美发展：情况每况愈下

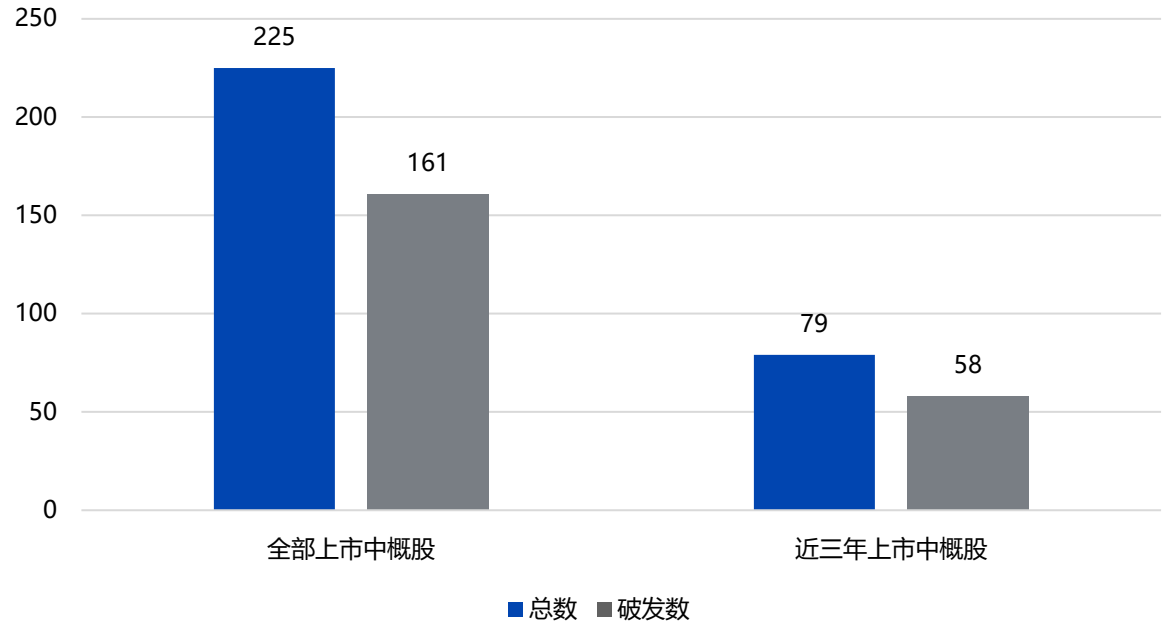
三月份，美国证券交易委员会（SEC）发布公告，称已通过《外国公司问责法案》（Holding Foreign Companies Accountable Act）最终修正法案，虽然在名义上针对的是所有在美的外国企业，但很多业界分析指出，该法案是美国针对瑞幸咖啡财务造假事件的持续发力，监管对象主要为在美上市的中概股企业。值得注意的是，处于保护国家数据安全的考虑，包括中国在内许多国家的法律法规与美国该项法案是相互冲突的。而美国方面则可能根据该法案法规条例，要求中概股企业在数据脱敏方面有一定的限制。在国家面对数据安全日益趋严的今天，数据的跨境流通，国家则保持着绝不马虎的态度。因此，基于国家安全考虑，退出美国市场不失为一种方式。例如，国内三大运营商移动、联通、电信就曾被纽交所勒令退市。

近期跨境数据安全问题之下，滴滴事件之后短短一周内国内政策频发，可见目前国家相关部门对资本市场跨境信息安全的政策早已蓄势待发，而滴滴事件正是那个导火索。从更深远来看，完全有理由相信国内数据安全的监管政策与美国资本市场所出台的法案，在将来可能仍会有更深层次的冲突，无论是已经在美上市的中国企业，还是准备在近期赴美的企业，都将更加难以同时满足双边要求。

另一方面，近些年中概股企业在美国市场的处境也变得越来越困难。根据零壹智库

统计显示，截至 2021 年 7 月 29 日，近三年赴美上市并且目前未退市的中概股约有 79 家，其中有 70%以上的企业当前处于破发状态。目前，在已统计数据完整的 225 家美国上市的中概股中，也有超过七成的中概股处于破发状态。

图 6-1 中概股目前在美市场破发表现



数据来源：零壹智库、Wind

中国企业在美国上市，无论是站在国家的角度还是站在企业自身的角度，都正在面临着前所未有的窘境。

（二）数据安全对中概股的影响与挑战：海外上市或被按下暂停键

谈起此次事件乃至后续数据安全后续发展对于海外上市的影响，就不得不回归到滴滴事件之后国家网信办发布《网络安全审查办法（修订草案征求意见稿）》（以下简称《办法》）公开征求意见。

从审查企业的质来看，《办法》指出，关键信息基础设施运营者采购网络产品和服务，数据处理者开展数据处理活动，影响或可能影响国家安全的，应当按照本办法进行网络安全审查；运营者采购网络产品和服务的，应当预判该产品和服务投入使用后可能带来的国家安全风险。影响或者可能影响国家安全的，应当向网络安全审查办公室申报网络

安全审查。

从审查的量来看，《办法》要求，掌握超过 100 万用户个人信息的运营者赴国外上市，必须向网络安全审查办公室申报网络安全审查。

此次《办法》两点新增内容几乎指向了国内多数运营 C 端产品的新兴互联网公司，同时也奠定了后期中国企业，尤其是与数据方面密切打交道的互联网或信息服务类企业赴国外上市的监管格局。在满足政策要求之下，流量型企业赴国外上市，在未来将会有明显的减缓趋势。

除了《办法》之外，中共中央办公厅、国务院办公厅所发布的《关于依法从严打击证券违法活动的意见》（以下简称《意见》）同样对中概股企业做了相关监管要求。

《意见》提出，要完善数据安全、跨境数据流动、涉密信息管理等相关法律法规，抓紧修订关于加强在境外发行证券与上市相关保密和档案管理工作的规定，压实境外上市公司信息安全主体责任。加强中概股监管，切实采取措施做好中概股公司风险及突发情况应对，推进相关监管制度体系建设。

另外，此次数据安全审查的另一个矛头则指向的是 VIE 架构，对于当前国内互联网企业普遍实行 VIE 绕开海外上市限制的做法，本身就是存在一定的安全隐患以及合规问题。距离新浪成为国内第一家通过 VIE 上市的公司已有 20 多年，中国的经济实力、资本市场环境都有了显著提升，而 VIE 一直是处于半灰色地带的创新之举。借助此次事件，SPAC 模式、反向上市进行“造壳”或“借壳上市”行为，或许也将要被监管所进一步明确。

对于中概股当下的影响，华东政法大学国际金融法律学院法学教授郑彧认为，目前我国监管政策的完善可能产生两方面影响，一是美国股东是否会找到招股说明书的漏洞，由此使得相关中概股面临集团诉讼的风险；二是因为市场对相关公司的业务增量存疑，进而可能调整对其增长评价和投资评级，如果业绩一直未达预期，公司可能触发交易类退市指标而被交易所摘牌。

随着平台经济以及互联网企业爆发式发展，海外上市近年水涨船高。据统计，2020 年共有 39 家赴美上市中概股，而 2021 年仅上半年这个数字就已经达到 37 家，完全有理由相信，若没有监管政策的“阻挡”，2021 年赴美上市的企业数将大大超过 2020 年。但随着滴滴事件和数据安全合规审查之后，各企业都将面临来自监管机构和各种诉讼的压力，可以预见的是，海外上市尤其是赴美上市正在被按下暂停键。

（三）中概股应对之举：回港或将成为主旋律

求变，将成为中国海外上市的新主题。中国与美国在面对数据时，未来很长一段时间中或仍将站在对立面，就海外上市这条路将难以回到过去，也难以揣测将来，中概股更应该考虑的是如何适应在摩擦中前进。

据郑彧分析，针对中国《网络安全审查办法（修订草案征求意见稿）》中相关约束条件，对于港交所上市并不适用，赴港上市并没有被纳入海外上市，至少在美国《外国公司问责法案》规定的期限内，踏入香港资本市场可能将是目前中概股的另一条蹊径。

实际上，港交所在这些年已逐渐成为中国企业另一个资本高地。2018 年 4 月，港交所发布了新的《香港联合交易所有限公司证券上市规则》，同时修订了“内地与香港证券市场互联互通机制”，自港交所修改上市制度以来，2019 年之后就掀起了一波中概股回港热风，阿里巴巴（09988）、百度（09888）、哔哩哔哩（09626），再到今年的携程（09961）都延续着这一势头。

在应对数据安全事件这一变量中，中概股回归或将成为常态，港交所也将成为重要选择。中概股的回港，既是应对目前监管规则发生重大变化风险的预防性举措，也反映了上市企业长期的、战略性的考量。

有行业律师曾表示，“企业在经营中应更加关注长期主义和价值主义，针对当下证券监管政策的发展趋势，有必要重点关注资本活动由海外市场转向国内的机会，以免造成因法律政策调整而造成的战略决策失误和投资损失。作为中国企业，服务本土、扎根本土、繁荣本土将是国内企业，尤其是平台型互联网企业眼见的趋势。”

未来，面对数据安全尤其是国家数据安全层面的监管仍将持谨慎态度，在登陆 A 股条件不具备的情况下，鼓励中概股赴港上市以及中概股的二次回归，不仅能够有效防范外部风险，严守数据安全底线，同时也能够巩固香港的金融中心地位，完善我国国内资本市场，这或将是未来的主方向。但是从更深层次来看，无论处身哪个资本市场，企业应时刻将国家利益放在首位，坚守数据安全的底线，坚守国家安全的底线。

七、数据安全治理背景下征信业嬗变升级

近年来，随着《网络安全法》、《数据安全法》和《个人信息保护法》等数据安全保护相关法律框架的落地或颁布，中国征信业发展也嬗变升级，征信业的政策环境、市场环境、发展模式等发生了一系列变化。

在此背景下，2021 年 1 月，央行发布《征信业务管理办法（征求意见稿）》，征信业务范围相应延展。同时，个人征信牌照的重新开闸，网络平台企业实现个人信息与金融机构的全面“断直连”，一系列举措显示征信业正迎来新的发展机遇期。

（一）数据安全：征信业发展的生命线

作为一项以数据为基础的活动，数据安全是征信行业发展的生命线。在数字经济时代，数据资源成为关键生产要素，越来越多的数据产生。数据的汇集不可避免地加大了数据泄露的风险，随着征信行业的市场化发展，一些不法机构通过非法获取、加工、售卖黑产数据而获利，不仅干扰了征信市场秩序，而且造成了个人信息数据的泄露。同时，数据安全也是判断信用主体信用水平的前提，不重视数据安全保护，滥用个人信息，会导致误判其信用水平，侵害信用主体的合法权益。

1、个人征信业务越市场化，越应高度重视数据安全

2018 年 2 月 22 日，百行征信获得我国首张个人征信业务牌照，个人征信业务市场化取得实质性突破。2021 年 2 月 2 日，朴道征信正式揭牌，标志着我国个人征信业务市场化进程的进一步加快。作为央行征信系统的有效补充，市场化的个人征信机构不仅能够大幅度拓宽征信体系的服务范围，还能为不同类型的金融机构和公司提供更多的个性化、针对性服务。

随着个人征信业务市场化的不断深入，数据安全问题应进一步被重视。第一，市场化个人征信机构作为营利机构，个人数据的挖掘和利用能够为其带来巨大的商业价值，在追求商业利益的同时，应高度重视数据安全问题，平衡商业利益与数据保护间的关系；第二，市场化个人征信机构更加注重技术创新和服务创新，在为金融机构或公司提供个性化服务的同时，还应高度注重新技术、新模式的应用所带来的数据安全风险。例如，百行征信与香港诺华诚信正式签署合作协议，即将推出跨境身份信息核验产品，跨境征信业务涉及跨境数据传递，保证数据安全是重中之重。

2、数据安全是有效判断信用主体信用水平的前提

多维度信息的有效共享，能够全方位刻画信用主体的信用水平，但信息实现有效共享的前提是能够保证数据安全。信用主体有义务让社会了解其信用行为和记录，但信用主体同样有权利保护自己的个人隐私数据或商业机密等不被泄露。

一些与征信业务边界不清的不法机构在个人数据市场上“跑马圈地”，不仅造成个人数据的滥用、泄露，还严重影响了市场的公平性，导致市场出现“劣币驱逐良币”现象，这使得个人征信市场的整体服务水平下降，信用主体的信用状况难以被有效判断。

（二）数据安全治理背景下征信业变化

随着《网络安全法》《数据安全法》等的相继实施及《个人信息保护法》的颁布，数据安全保护不断加强，同时也为征信业发展带来巨大利好，征信业的政策环境、市场环境、发展模式等发生了一系列变化。

1、信息保护相关政策标准不断出台

2021 年 1 月，央行就《征信业务管理办法（征求意见稿）》（以下简称《管理办法》）公开征求意见。《管理办法》将信用信息界定为“为金融经济活动提供服务，用于判断个人和企业信用状况的各类信息”，一定程度上拓展了信用信息的维度和范畴，同时也使得征信业务的范围也相应延展，将“信用信息服务、信用服务、信用评分、信用评级、信用修复等”均纳入了征信业务的范畴，并要求征信机构采集信息遵循“最少、必要”原则，这有利于遏制信用信息滥用现象的发生。此外，《管理办法》还对跨境征信业务及相关活动进行了相应的规定，有助于国内企业更好地“走出去”，国际机构更好地“走进来”。

在征信行业相关标准方面，随着公共信用信息等替代性信用信息的采集、共享，为保护信息安全，2020 年以来，全国社会信用标准化技术委员会制定了《公共信用信息交换方式及接口规范（GB/T 39443-2020）》《公共信用信息分类与编码规范（GB/T 39441-2020）》《公共信用信息资源目录编制指南（GB/T 39440-2020）》《公共信用信息数据元（GB/T 39445-2020）》等 8 项公共信用信息标准。同时，全国信息安全标准化技术委员会、全国金融标准化技术委员会也相继出台了《个人金融信息保护技术规范（JR/T0171—2020）》、《金融数据安全 数据安全分级指南（JR/T 0197—2020）》、《信息安全技术 个人信息安全规范（GB/T 35273—2020）》等个人信息安全标准和金融数据安全标准，不断强化数据安全保护。

2、与征信业务边界不清的机构被整顿、约谈

互联网金融的粗放发展带来了个人信息在信贷领域的滥用。2018 年，网信办约谈支付宝、芝麻信用的有关负责人时曾表示，“支付宝、芝麻信用收集使用个人信息的方式，不符合刚刚发布的《个人信息安全规范》国家标准的精神，违背了其前不久签署的《个人信息保护倡议》的承诺；应严格按照网络安全法的要求，加强对支付宝平台的全面排查，进行专项整顿，切实采取有效措施，防止类似事件再次发生。”

2019 年，大数据行业监管持续加码，魔蝎、新颜科技、白骑士、聚信立等大数据公司因通过数据爬虫侵害用户个人信息权益被整顿。这类大数据公司通常提供数据输出服务，采集个人信息的渠道一般分为三种：一是信息主体主动提供；二是提供服务的过程种缓存个人信息；三是通过共享、爬取等方式间接获得个人信息。它们提供的服务包括反欺诈、风险测评、信用评估等服务。

3、网络平台企业实现个人信息与金融机构的全面“断直连”

2021 年 4 月 29 日，央行、银保监会、证监会、外汇局等金融管理部门联合对包括腾讯、度小满金融、京东金融、字节跳动、美团金融、滴滴金融、陆金所、天星数科、360 数科、新浪金融、苏宁金融、国美金融、携程金融等在内的 13 家从事金融业务的网络平台企业进行监管约谈，并提出了七大整改要求，其中要求这些网络平台企业打破信息垄断，严格通过持牌征信机构依法合规开展个人征信业务，并且要强化金融消费者保护机制，规范个人信息采集使用、营销宣传行为和格式文本合同，加强监督并规范与第三方机构的金融业务合作等。

近日，央行征信管理局给网络平台企业下发通知，要求网络平台企业实现个人信息与金融机构的全面“断直连”。这一模式的实现将有利于个人信息保护和平台数据的规范使用，意味着个人征信相关服务必须持牌经营，网络平台企业无权直接或间接从事个人征信业务。

同时，这一政策也将改变个人征信相关服务的业务模式，当下，个人征信机构一方面通过与互联网金融机构的借贷信息的共享，提供个人征信服务，另一方面通过市场化机制，采集个人信贷信息以外的信用数据，通过对数据进行分析、整理、加工等，输出个人征信服务。在“断直连”模式下，助贷机构、网络平台提供个人征信业务只能通过申请牌照或与个人征信机构合作两种方式，后者这一合作模式则将对现有的个人征信服务模式带来改变，原来的“个人征信机构—金融机构”两者间的合作变成“助贷机构、网络平台—个人征信机构—金融机构”三者间的合作，在这种情况下，个人征信机构应该如何和助贷机构、网络平台进行合规化合作？对于助贷机构、网贷平台提供的数据又

是否能够完全采信？合作过程中，助贷机构、网络平台又该向个人征信机构提供哪种类型的数据？

（三）数据安全治理背景下征信业发展的机遇与挑战

在数据安全保护不断加强的背景下，打着大数据公司“旗号”提供个人征信服务的机构，被整顿、治理；利用自身数据优势，提供导流、助贷等个人信用服务的网络平台企业，被约谈、规范。从大数据公司，到网络平台企业，与个人信用服务相关的机构逐渐被整顿，个人征信市场正不断实现规范化、牌照化发展。

未来，个人征信牌照的价值将不断被放大。对百行征信和朴道征信来说，应在守牢数据安全底线的基础上，积极修炼内功，丰富信用信息相关维度，运用数字化手段创新征信服务新模式，不断加强产品研发，注重信用主体的多样化信用需求，提供个性化、差异化、针对化的个人征信服务。对于腾讯、字节跳动等互联网巨头来说，可以借鉴京东数科、小米等入股朴道征信的模式，与相关机构合作成立持牌化的个人征信公司，开展合规化个人征信业务。

在“断直连”这一模式下，助贷平台和银行间的授信链条中，加入了个人征信机构，助贷平台的盈利空间被压缩。对助贷机构来说，一方面可以在原有服务模式的基础上，加强自身的技术服务能力，寻找和金融机构间的合规化合作模式；另一方面，积极寻求与个人征信机构合作，避免发生监管风险、合规风险。

八、隐私计算技术加速落地，赋能数据安全应用

（一）《数据安全法》落地为隐私计算带来新机遇

2021 年 6 月 10 日，《数据安全法》正式通过并公布，并于 2021 年 9 月 1 日正式实施。该法案对数据处理活动、安全保护、开发利用提出了明确的合规要求。

在法律对数据的严监管方向明确之后，隐私计算几乎是当下数据互联互通的唯一技术解，具有巨大的商业价值和应用前景。隐私计算是面向隐私信息全周期保护的技术，通过对明文数据的加密，可以实现数据的“可用不可见”。同时，隐私计算技术可以结合人工智能，利用加密参数训练和分析模型、充分挖掘数据价值。

对数据提供方而言，《数据安全法》的出台提供了合规路径，丰富了数据市场的多样性。法规出台前，部分电信运营商和产业链上下游的大数据公司需承担交易“明文数据”的消费者投诉和网信办的查处。数据大户戒备法律风险和对公司信誉的影响，往往守着一座巨大的数据宝藏，不敢越雷池半步。数据价值被闲置，下游的数据需求方缺乏数据资源。如今，法规支持数据提供，隐私计算技术介入、搭建安全传输机制。数据提供方在保护用户隐私安全的前提下，为价值挖掘提供丰富的数据资源。

对于隐私计算厂商而言，《数据安全法》衍生了大量的市场需求。数据需求方需要数据接入和分析，以提升业务效果。为了响应合规要求，需求方急需购买隐私计算产品以实现数据在安全隐私的场景交易。因此，法案出台后，隐私计算产品应用市场迅速扩张。除此以外，融资方在衡量数据安全产品时往往考量国家政策和法规。欧盟 GDPR 法案于 2018 年出台，加州 CCPA 法案紧跟其后，中国一直缺乏数据安全领域的权威法律。《数据安全法》诞生后，隐私计算厂商将具备融资竞争力，并将获取的资金进一步投入技术研发和业务拓展。

对于数据需求方而言，《数据安全法》提高了数据利用效率和安全性。法案出台以前，需求方急于收集数据，但是否使用该数据，使用效率如何，以及能否保证数据全周期的安全可控，这些问题都不在需求方权责范围以内，反而留下了巨大的安全隐患。法案提出“各地区、各部门对本地区、本部门工作中收集和产生的数据及数据安全负责”。企业有义务保证数据的安全性，否则将面临罚金、暂停营业、吊销执照等惩罚。当数据处理各环节的安全监测落实到具体责任方，信息安全得到了进一步的维护。

所以，随着《数据安全法》的出台，整个隐私计算行业不仅更加权责分明和规范，同样也迎来资源和市场需求的增长和机遇。

（二）隐私计算目前的发展状况

2021 年，隐私计算开始尝试规模化应用。

国内隐私计算行业起源于 1982 年，姚期智先生提出“百万富翁”问题（两个百万富翁街头邂逅，他们都想炫一下富，比比谁更有钱，但是出于隐私，都不想让对方知道自己到底拥有多少财富，如何在不借助第三方的情况下，让他们知道他们之间谁更有钱？），标志着多方安全计算的诞生。

1982 年~2017 年，隐私计算市场处于萌芽阶段，集中于实验室研究。

2018 年，隐私计算市场进入启蒙阶段，中国通信标准化协会开始制定隐私计算领域的相关标准。

隐私计算市场真正启动是从 2019 年开始的。

2019 年，银监会、互联网金融风险专项整治等监管结构联合公安机关对“现金贷”数据源爬取进行了整肃，被誉为大数据风控行业史上最严的查处。公众和政府意识到“明文数据”泄露的危害性和严重性。面临个人隐私保护和公司商业发展并行的困境，“可用不可见”的隐私计算提供了技术可能性。2019 年，隐私计算产品开始出现，可用性、性能逐步提升，在某些场景下变得可用。

2020 年，介于政策上的合规避险要求，业务端挖掘数据价值的诉求，一大批隐私计算厂商在客户端市场进行大规模的概念教育和技术试点部署，较多的概念验证的产品出现。因此，2020 年被称为“隐私计算元年”。

2021 年，隐私计算开始规模化应用，主要是基于三方面的因素：

其一，市场需求启动。2019 年以来，对数据的严监管态势使得数据源和数据使用方对数据交换和使用变得谨慎，开始寻求保护用户隐私的方案。这使得隐私计算在实践中真正有了市场。此前，隐私计算技术一直存在，但是由于市场上数据滥用的现象并不鲜见，因此大部分机构对隐私计算没有需求。另外，隐私计算产品经前两年 POC（Proof of Concept，是业界流行的针对客户具体应用的验证性测试）验证，向客户端证明了隐私计算厂商对业务场景的理解能力。随着隐私计算产品在各行业的渗透，业务应用的性能和推荐的精确度、转化率得到一定程度的提升。因此，部分行业近期开启大规模招标。其中，金融行业是需求最大，预算最为充足的行业。其二，性能大幅提升。近几年来，隐私计算的性能有了大幅提升。隐私计算的性能目前不能一概而论，最快的可以达到明文计算的 3—5 倍，最慢的可能达到明文计算的上百倍。预计在未来一年左右的时间里，隐私计算的性能可以优化至明文计算的 5-10 倍。

其三，政策法规支持。一系列与数据相关的政策法规陆续出台，利好隐私计算的应用。2020 年 4 月，中共中央、国务院印发《关于构建更加完善的要素市场化配置体制机制的意见》，将数据列为生产要素，明确指出了市场化改革的内容和方向。2021 年 6 月，《数据安全法》出台，并于 9 月 1 日正式实施，各行业需合规化数据处理过程，为隐私计算行业带来了规模化商业需求。

目前，隐私计算生态主要由三方构成：甲方、乙方和丙方。甲方指的是需要用数据的机构，比如银行、保险等机构；乙方，指的是拥有数据的机构，目前数据主要集中在政府、运营商、银联、互联网巨头手中；丙方，指的是不拥有数据的服务机构，比如隐私计算厂商、云服务商、大数据服务商等。当下，最激烈的竞争是在隐私计算技术提供商之间。

（三）隐私计算的应用将带来的影响

数字经济，将是新的经济增长方式，与现有的经济增长方式相比，可能具有范式转换特征。在数字经济时代，合理保护用户隐私下发展数据产业，共享并充分挖掘数据价值是国家的核心竞争力。

隐私计算的应用，将促进数据安全合规流动，进一步释放数据价值。经由隐私计算的帮助，许多产业将迎来新的增长红利。

人工智能产业将是首先获益的产业。2012 年，深度学习理论被验证，此后人工智能技术得到飞速发展，但是目前仍处于初级阶段。人工智能的进一步提升，需要更多的数据进行训练，目前的数据孤岛限制了人工智能对数据价值的挖掘。隐私计算的应用将逐步打破数据孤岛，使得人工智能技术得到进一步飞速发展。

在具体的应用场景中，比如金融、医疗、政务领域，都有待进一步挖掘数据价值。

金融业正在经历数字化转型大潮，将金融机构内外部数据联合起来分析，提升营销和风控效果已经是大势所趋。在 2020 年 9 月的外滩大会上，蚂蚁集团数字金融 CTO 王晓航在主题演讲中表示，金融场景化是金融服务的趋势，以互联互通、数据化联营为特征的模式将会成为主流。金融和智能的结合将更加紧密，场景的产业数字化会加速。共享智能为代表的互联互通技术将打开生态之间协同的下一波合作红利，这个趋势将会更加明显。

医疗领域也正在等待隐私计算开启新纪元。传统医学是小数据的判断和决策，正确率很难保证，完全依靠医生的经验和能力。以前基于统计学意义的诊断，今后将被基于

个性化的大数据的诊断所代替。

政务领域也正等待隐私计算助力民生改善。政府掌握着其他机构无法收集的民生数据，结合隐私计算将弥补一部分数据互联市场的空白。例如，原本金融机构无法获取农民社保等信用信息，以发放小额信贷；城市规划部门难以获取居民信息、产业数据、公共信息。当隐私计算介入，政务领域将开启以“小额信贷”、“智慧城市”为例的民生红利。

（四）隐私计算未来发展面临的挑战

从基础设施建设、技术平台开发、产品落地应用场景，隐私计算产品在未来发展过程中仍面临着一系列的挑战。

1、技术挑战

隐私计算目前的安全性、性能与效果都有较大的提升空间。

首先，是安全性。隐私计算是一类技术的总称，目前应用比较多的是多方安全计算、联邦学习和可信执行环境。就每个单一技术而言，都有各自的优缺点。在安全性方面，不能排除有的技术存在一定的瑕疵，比如有的密文可以被反推出明文。因此，在实践中，这些技术需要被组合使用。在初期，市场对隐私计算技术应用的安全性存在一定顾虑。

其次，是性能。隐私计算的性能目前已经达到基本可用，最快的可以达到明文计算的 3—5 倍，最慢的可能达到明文计算的上百倍。但是，与此同时，性能仍有数十倍至百倍的提升空间。

最后，是效果。隐私计算产品处于初步应用阶段，市场需求尚未完全挖掘。大部分行业甚至由于数字化程度低、业务流程不明确，导致缺乏市场需求。因此产品距离实现大规模工业化，仍需要进一步训练和优化。在实际运用中，技术服务平台可能只提升行业共性的业务表现，隐私计算厂商需进一步研发架构、更新底层模块，以解决个性化的业务需求。因此，隐私计算技术距离满足客户整体化需求仍有距离。

2、互联互通

隐私计算本是为了促进数据互联互通而产生，但在实际中却形成了新的数据孤岛。

数据固有的分散性，以及缺乏行业认同的数据交互标准，成为数据共享的挑战。首先，数据由不同途径产生，产生个体分布于不同领域，数据拥有方亦难以统计完整范围

的数据资源。其次，各厂商研发的技术服务平台依赖差异化的底层架构、基于不同的隐私计算技术、应用于多样化的场景。底层组件的差异抑制了厂商间的数据互联。

这在实践中引发了新的问题，应用方通常需要安装好几个不同隐私计算厂商的软件才能解决问题。这将在未来带来较为棘手的问题：隐私计算应用机构，需要采购多套隐私计算系统，要使得多套系统之间的数据互联互通，连接的工作量将呈几何级数倍增。

目前，关于互联互通的尝试正在进行当中。由于各厂商统一架构程度的意愿不一，交互标准仍需经过合作的打磨。除此之外，厂商实际达成平台的互联需要一定的融资支持和研发时间。互联协议不仅停留在变更数据形式，更重要的在于对底层架构的变更。行业内建立大范围的互联互通生态具有挑战。

九、数据安全领域未来展望

随着数字经济发展，不断产生的海量数据将成为国家战略支撑点。为了确保数据战略安全健康实施，护航经济发展，需要从政府、科研、产业界、学术界、行业应用等多方面加强对数据产业、数据安全的支撑。

可以预见，《数据安全法》的正式施行，将推动落实与数据安全保护相关的一系列措施，各行业宜围绕国家数据安全战略，提升数据安全产业基础能力，加快研究和应用数据安全防护技术，健全完善数据安全法律规范与标准，构筑数据安全战略国际领先，向国际推出数据安全中国方案。

（一）法律法规在数据安全方面将得到全面强化与支撑

在立法层面，《网络安全法》、《民法典》、《数据安全法》和《个人信息保护法》将作为数据安全保护的基本法律框架，结合《网络安全法》等其他法律，将对各种数据处理活动产生重大影响。

在促进层面，除了《数据安全法》提出促进数字经济发展的大政方针外，还需要其他民事、商事法律的配套推进。在安全层面，相关的管制和管理措施的界限也将进一步得到明确。

而针对数据安全相关法律法规所引入的如数据分级分类制度、境外执法机关调取境内数据的报告制度、部分数据出口管制制度、外国歧视性措施的反制措施等制度，需要进一步细化相关制度和联动机制。除了政策之外，相关标准和指南将作为法律法规和具体实践的重要桥梁，有望解决前述的基本概念厘清、配套制度建立以及相关举措细则确定等问题。

（二）数据安全产业基础能力将得到提升

硬件层面，存储芯片等数据安全产品的核心硬件将在国家对数据产业支持之下得到迅速发展。另一方面，全闪存数据中心已成为产业共识，加速“磁退硅进”也将成为业界趋势。

软件层面，数据基础设施的基础软件应自主可控，积极推动软件产业自主创新，鼓励国内数据软件厂商自主研发，掌握核心软件技术，推动数据软件产业高质量、安全发展。

此外，政府应促进数据产业绿色节能、高效发展。数据显示，2019 年全国数据中

心耗电量达 1608 亿度，超过三峡+葛洲坝总发电量，也超过了整个上海市全年用电量。绿色节能是国家战略发展方向，政府应加快整合数据相关全产业链基础设施。

另一方面，目前各国纷纷从国家安全和产业应用角度，意识到数据作为生产要素和国家资源的重要性。对企业而言，虽然大数据业务场景众多，但尚未充分释放出应有的商业价值，数据变现能力亟待提升。

（三）数据安全升级助力相关领域发展加速

随着数据安全监管升级，与之相关的行业将同样得到加速升级。

网络安全产业方面，到 2023 年，我国网络安全产业规模将超过 2500 亿元，年复合增长率超过 15%。我国网络安全产业规模的不断增长，同时也推动网络安全行业收入不断增加。

征信业在数据合法合规得以标准化后，数据的汇集产生的数据泄露的风险将有效得到控制，征信市场秩序也能有效加以维持。数据作为征信机构卡脖子的环节，解决好数据问题就能保障好征信业的生命线。

数据安全同样为隐私计算带来了前所未有的机遇，基于隐私计算“可用不可见”这一独特的优势，可以说已经成为数据互联互通的唯一技术解。随着《数据安全法》的出台，整个隐私计算行业不仅更加权责分明和规范，同样也迎来资源和市场需求的增长和机遇。

参考资料：

[1] 数据安全治理白皮书-中国电子信息产业发展研究院，赛迪智库网络安全研究所

[2] 数据安全白皮书-工信安全，华为

[3] 嘀!数据安全监管升级-国际商报

[4] 数据安全技术发展现状及挑战解析-中国信息通信研究院

[5] 中国需要全力捍卫数据主权-环球时报

[6] 平台企业数据开发利用存严重隐忧——守护数据安全底线-经济日报

[7]存储器市场热度持续延烧 两大韩企称霸！-芯极速

[8]中国服务器行业发展研究报告-中为咨询

[9] 2020 年中国操作系统行业市场现状与竞争格局分析 国产替代仍需加速推进-前瞻经济学人

[10]中国数据库行业研究报告（2021）-艾瑞咨询

[11] 2020 年中国数据安全行业概览-头豹研究院

[12] 中国互联网络发展状况统计报告-中国互联网络信息中心

[13] 2020 年中国网络安全产业统计报告-中国网络空间安全协会

[14] 2021 年中国网络安全市场与企业竞争力分析-中国网络安全产业联盟

报告发布单位介绍

中国科技体制改革研究会数字经济发展研究小组

中国科技体制改革研究会于 1994 年 12 月，经中华人民共和国民政部批准成立，接受主管单位科学技术部的业务指导。中国科技体制改革研究会是由热心和有志于从事有关科技体制改革研究工作的人员自愿结成的全国性、学术性社会团体，是依法成立的社会团体法人，属于非营利性社会组织。

数字经济发展研究小组是于 2020 年 4 月经中国科技体制改革研究会批准成立的非独立法人智库机构。研究小组旨在深入研究全球数字经济现状、法律、趋势、挑战与机遇，数字经济重大前沿和战略问题，深度解析数字科技发展对中国科技体制改革、发展方式转变、社会转型的支持和引领作用，为探索数字经济时代的中国实现现代化的新路径建言，促进我国数字经济快速稳定发展发挥积极作用。具体工作包括以下几项：

一、联合国内各大院校及专家教授成立以 5G、区块链、人工智能、大数据等新一代和新基建为代表的课题组，深度研究相关技术对数字经济的影响；

二、加强国内外数字经济交流合作，依托科技部平台资源与其他各部委及各省市进行互连举办数字经济高峰论坛，发布数字经济行业报告；

三、深入企业调研，引导和协助国内大中型企业数字化转型；

四、组织专家深入研究数字科技在电子政务、金融、医疗、农业、交通、能源、工业互联网、房地产、新零售、贸易、供应链等领域的影响，做好我国数字科技发展战略规划与政策指导工作，为监管部门提供研究报告和相关数据支撑。

横琴数链数字金融研究院

横琴数链数字金融研究院成立于 2021 年 3 月，是在珠海市横琴新区管理委员会、珠海横琴新区金融和财政局、横琴新区金融服务中心支持下设立，由著名经济学家、横琴数链数字金融研究院学术委员会主席朱嘉明教授领衔，多位国内外专家学者支持的新兴数字金融研究平台。

研究院的成立是为了完成琴澳深度合作区所肩负的改革开放任务，在促进双循环发展的格局下，参与创建横琴和澳门作为亚太地区数字经济中心，形成以琴澳合作为中心的平台，大力推动科技、资本、信息、人才等创新要素的配置，最终实现新的历史性跨

越，建成共享型和普惠型经济示范区。

横琴数链数字金融研究院侧重琴澳数字金融发展需求，持续开展相关政策研究报告、举办相关学术论坛，协助琴澳进行产业深度合作；同时，在监管能力支持、教育培训系统、基础设施结构、空间部署和新媒体等方面提供支持。

报告研究支持单位介绍

欧盾链上天眼安全实验室

欧盾链上天眼安全实验室由欧科云链集团和南京公安研究院共同成立。双方重点围绕新型犯罪应对、智慧城市建设、社会治理等现实需求，以创新理念，推动区块链技术应用与发展，探索区块链技术在公共安全、社会治理等领域的落地应用，重点开展产品设计研发及运营、链上数据分析及服务、安全攻防对抗及风控、专项区块链技术人才培训培养等方面工作。

通过“区块链+公共安全”，为区块链产业生态构建、安全应急产业发展、社会现代化治理能力提升、城市数字化转型等做出更大贡献。

致谢

2021 年 8 月 1 日，零壹财经 • 零壹智库、数字经济发展研究小组、横琴数链数字金融研究院联合举办了首期“科技体制改革研究会数字经济研讨会”暨第 39 期“零壹智库闭门会”，会议主题为“数据安全与数据治理”。会上，专家与企业高管就当前数据安全形势和数据安全行业发展趋势进行了深入分析，并就技术升级的路径做了广泛探讨。本报告内容参考并引用了部分与会嘉宾观点，特此对以下嘉宾表示感谢（排名不分先后）。

横琴数链数字金融研究院学术与技术委员会主席 朱嘉明

中国科技体制改革研究会数字经济研究发展小组组长 陈晓华

科技部法规司原副司长 王宇

工信部产业政策司原巡视员 辛仁周

北大光华、百行征信、腾云天下征信数据分析与应用联合实验室主任 王志诚

上海交通大学数据法律研究中心执行主任 何渊

中国银行法学会理事 肖飒

建投数据副总经理 楚立山

洞见科技 PMO 总经理 方东

顺丰科技保密总监 刘森

联通数字科技有限公司数据智能事业部安全合规负责人 关泰璐

零壹财经·零壹智库

金融与科技知识服务平台

金融与科技知识服务平台，2013年成立于北京，建立了**传播+研究+数据+咨询+培训**等服务体系，覆盖金融与科技生态的主要领域，已服务超过300家机构。

零壹财经·零壹智库是中国互联网金融协会成员、北京市互联网金融行业协会发起单位并任投资者教育与保护专委会主任单位、中国融资租赁三十人论坛成员机构、湖北融资租赁协会副会长单位、广州融资租赁产业联盟理事单位。

传·播　研·究　数·据　咨·询　培·训

40+ 专业书籍　**350+** 专题报告　**700+** 数据报告　**30+** 行业峰会　**50+** 闭门研讨会

2013年 — 2020年

零壹财经官网：www.01caijing.com

零壹财经　零壹智库Pro

零壹财经·零壹智库

金融与科技知识服务平台

零壹智库信息科技(北京)有限公司
www.01caijing.com
marketing@01caijing.com
13261990570