

计算机应用

数据安全大事记整理及展望

数据安全顶层设计趋于完善，互联网、工控及电信领域数据安全政策细节催化需求，数据安全市场规模及落地速度或超预期。1) 顶层设计趋于完善，部分公司已接受调查，2021年6月10日，《中华人民共和国数据安全法》审议通过，并于2021年9月1日起施行。《个人信息保护法》(“个保法”)于8月20日表决通过，将于2021年11月1日起施行；2) 监管细节催化落地，2021年9月15日，工信部发布《关于加强车联网网络安全和数据安全工作的通知》，2021年9月30日，工信部发布《工业和信息化领域数据安全管理办法(试行)(征求意见稿)》。共同推动数据敏感企业建立数据全生命周期管理制度，针对不同级别数据，明确制定数据收集、存储、使用、加工、传输、提供、公开等环节的具体分级防护要求和操作规程。

展望数据安全发展趋势：1) **数据是互联网企业最重要生产资料，有望率先展开合规动作。**由于监管环境变化、数据安全需求迫切，且自身技术实力领先，有望成为数据安全合规典型行业，部分头部互联网企业如腾讯、百度，已率先在数据安全保护领域加大投入，用户行为数据在人群提取、转化统计、程序化创意、oCPA等领域应用影响仍待观察；2) **金融、医疗、能源等关保行业数据安全潜在空间巨大。**金融数据天然具有商业价值，需加强监管。通过分析金融交易相关“敏感个人信息”总结、归纳、演绎后得到的“衍生个人信息”，对于风控及业务价值巨大；智能医疗设备供应商将收集越来越多样化的数据，其使用必将面临强监管，随实体医院将诊疗活动延伸至互联网端，数据流通成业务刚需，关乎患者隐私、种类繁多的医疗数据也迫切需求安全监管；以自动驾驶为代表的AI技术日益普及，汽车数据处理量级及能力日益增强，汽车数据依法合理有效利用同时维护了国家安全利益与个人合法权益；3) **产业市场规模及落地速度有望超预期。**《数据安全法》正式实施，《个人信息保护法》等政策实施在即，叠加用户隐私安全意识加强，监管诉求、企业自身合规需求迫切，产业落地及总规模有望超预期。

监管政策加码与大数据加速应用驱动数据安全发展，短期百亿市场以技术服务收入为主，长期SAAS运营收入有望达千亿。近期《数据安全法》、《关保条例》、《个人信息保护法》等法律法规密集发布并实施，仅从数据安全的组成部分隐私计算来看，据Gartner预测，2023年，全球80%以上的公司将面临至少一项以隐私为重点的数据保护法规，2024年隐私驱动的数据保护和合规技术支出将在全球突破150亿美元。随《数据安全法》等落地、数据交易市场快速发展，KPMG预计2023年国内数据安全技术服务有望达百亿，随IT架构走向云化，长期将撬动千亿级的数据安全SaaS运营收入。

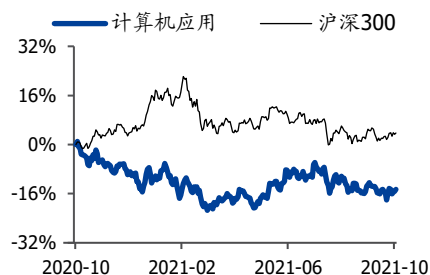
隐私安全：卫士通、安恒信息、奇安信。

网络安全：奇安信、卫士通、安恒信息、深信服、天融信、启明星辰、绿盟科技。

风险提示：行业竞争加剧风险；政策力度不及预期风险；宏观经济风险；测算可能与实际存在误差。

增持（维持）

行业走势



作者

分析师 刘高畅

执业证书编号：S0680518090001

邮箱：liugaochang@gszq.com

相关研究

- 1、《计算机应用：挂钩收入大额罚款开启，互联网治理时代来临》2021-10-09
- 2、《计算机应用：数据安全政策密集发布，千亿产业爆发拐点已至》2021-10-07
- 3、《计算机应用：数据安全，后互联网时代的盛宴》2021-09-26

内容目录

《数据安全法》，需求落地的最强催化剂	3
《个人信息保护法》，2018 年的 GDPR.....	4
展望一：互联网数据安全需求最迫切，已加大投入力度	7
展望二：金融、医疗、汽车、能源等数据安全潜在市场巨大	10
展望三：数据安全市场规模及落地速度有望超预期	11
风险提示	13

图表目录

图表 1: 《数据安全法》要点概览.....	3
图表 2: 网络安全领域重要政策法规梳理	4
图表 3: 个人具有数据处置权.....	5
图表 4: 数据跨境提供的规则.....	5
图表 5: GDPR 中处理个人数据的基本原则.....	5
图表 6: GDPR 中对合法处理数据的定义.....	6
图表 7: GDPR 监管企业	6
图表 8: 判罚的严重程度要素.....	7
图表 9: 腾讯数据安全中心功能	8
图表 10: 腾讯数据脱敏解决方案功能.....	8
图表 11: 百度 APP 安全解决方案	9
图表 12: 史宾格安全及隐私合规平台功能	9
图表 13: 金融结构涉及相关个人信息.....	10
图表 14: 互联网医院面临的主要数据安全风险.....	10
图表 15: 我国车联网安全监管机制现状.....	11
图表 16: 数据安全 2023 年规模上限超百亿	12
图表 17: 隐私计算商业模式	12
图表 18: Snowflake 基于三朵公有云的云原生分析型数据仓库	13

《数据安全法》，需求落地的最强催化剂

数据是国家基础性战略资源，没有数据安全就没有国家安全。6 月 10 日，《中华人民共和国数据安全法》由中华人民共和国第十三届全国人民代表大会常务委员会第二十九次会议审议通过，自 2021 年 9 月 1 日起施行。确立了数据分类分级管理，数据安全审查，数据安全风险评估、监测预警和应急处置等基本制度。

近期网络安全政策持续加码，2021 年 7 月 2 日，网信办依法宣布对某“用车平台”实施网络安全审查，7 月 4 日、5 日多家公司 APP 被依法下架、暂停新用户注册，7 月 10 日，网信办又发布《征求意见稿》补缺了此前网络安全审查仅针对关键信息基础设施的采购审查短板，审查范围从关键信息基础设施运营者扩大到了全部数据处理者，要求掌握超过 100 万用户个人信息的运营者赴国外上市，必须审批。

此前已颁布多部法律法规，《数据安全法》将进一步完善数据安全要求。如与《网络安全法》相比，仍存在基本法缺位、“数据主权”地位尚未确立，数据经营难有效监管等问题。“网络安全法”主要是针对网络层面的安全规范，但未能从数据信息全维度进行规范，相关配套政策文件法律层级低，要求较为分散，难以系统性解决数据安全保障问题。

对于数据本身而言，“数据”已成为和土地、资本、劳动力并列的“生产要素”，具有重大价值。一旦数据被破坏或者被泄露，这些数据信息被利用后将对国家安全、公共利益等造成损害。另一方面，《数据安全法》中也明确规定了未履行数据安全保护义务将承担法律责任。对于监管者和执法者来说都需要引起高度重视。

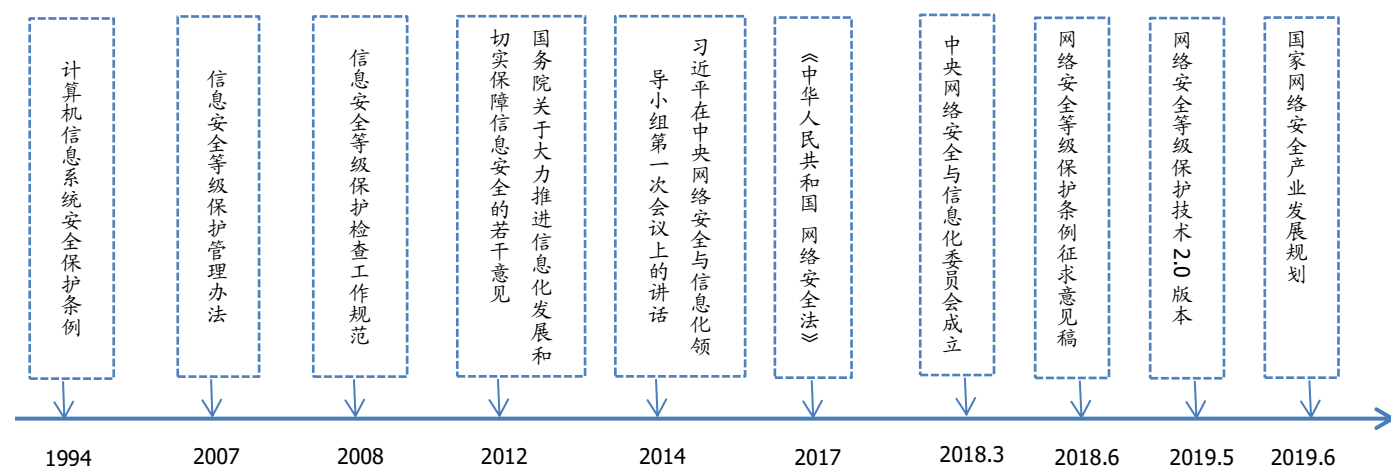
图表 1: 《数据安全法》要点概览

序号	内容
要点一	完善数据分级分类保护制度
要点二	新增强化等保在数据安全保护要求中的基础作用
要点三	调整数据安全负责人和管理机构的要求
要点四	新增重要数据出境的管理规定和对应的法律责任
要点五	调整数据处理相关服务的资质要求
要点六	加强对向境外司法或执法机构提供数据的监管
要点七	大幅加重不履行数据安全保护义务的法律责任
要点八	新增明确拒不配合数据调取的法律责任

资料来源：中伦视界，国盛证券研究所

政策合规方面，还有《网络安全法》、等保 2.0、护网行动力度加大、关键基础设施保护条例（草案）等一系列积极因素影响。等保 2.0 于 2019 年 12 月 1 日正式实施，年初疫情使各级政府财政收入受到一定影响，部分合规产品需求采购后移。但攻防演习范围从中央直属部委、国企总部延伸至分支机构，攻防演习投入保持韧性；随着关键基础设施保护条例预计的出台，涉及国计民生、公共利益的政府机关和能源、金融机构，大型公共信息网络服务单位将会给网络安全行业带来增量收入。

图表 2: 网络安全领域重要政策法规梳理



资料来源: 各级政府网站, 国盛证券研究所

《个人信息保护法》，2018 年的 GDPR

《个人信息保护法》围绕规范个人信息处理活动、保障个人信息权益，构建了以“告知-同意”为核心的个人信息处理规则，借鉴以《通用数据保护条例》（GDPR）为代表的国外个人信息保护立法，我国《个人信息保护法》赋予个人的权利种类、框架基本一致。亮点如下：

- 1) 个人信息保护法明确处理个人信息应当在事先充分告知的前提下取得个人同意，个人信息处理的重要事项发生变更的应当重新向个人告知并取得同意。同时，针对现实生活中社会反映强烈的一揽子授权、强制同意等问题，个人信息保护法特别要求，个人信息处理者在处理敏感个人信息、向他人提供或公开个人信息、跨境转移个人信息等环节应取得个人的单独同意，明确个人信息处理者不得过度收集个人信息，不得以个人不同意为由拒绝提供产品或者服务，并赋予个人撤回同意的权利，在个人撤回同意后，个人信息处理者应当停止处理或及时删除其个人信息。
- 2) 随着越来越多的企业利用大数据分析、评估消费者的个人特征用于商业营销。有一些企业通过掌握消费者的经济状况、消费习惯、对价格的敏感程度等信息，对消费者在交易价格等方面实行歧视性的差别待遇，误导、欺诈消费者。其中，最典型的就是社会反映突出的“大数据杀熟”。对此，个人信息保护法明确规定：个人信息处理者利用个人信息进行自动化决策，应当保证决策的透明度和结果公平、公正，不得对个人在交易价格等交易条件上实行不合理的差别待遇。
- 3) 个人信息保护法将生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息列为敏感个人信息。个人信息保护法要求，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，方可处理敏感个人信息，同时应当事前进行影响评估，并向个人告知处理的必要性以及对个人权益的影响。

《个人信息保护法》违法成本较欧盟标准更高，国内数据安全需求落地确定性强。触犯规定的违法行为，情节严重的，由省级以上履行个人信息保护职责的部门责令改正，没收违法所得，并处五千万元以下或者上一年度营业额 5% 以下罚款，并可以责令暂停相关业务或者停业整顿、通报有关主管部门吊销相关业务许可或者吊销营业执照。

图表 3: 个人具有数据处置权

个人有权请求删除的情形

- 1、处理目的已实现、无法实现或者为实现处理目的不再必要;
- 2、个人信息处理者停止提供产品或者服务, 或者保存期限已届满;
- 3、个人撤回同意;
- 4、个人信息处理者违反法律、行政法规或者违反约定处理个人信息;
- 5、法律、行政法规规定的其他情形。

资料来源: 中国《个人信息保护法》, 国盛证券研究所

图表 4: 数据跨境提供的规则

个人信息跨境提供的规则

- 1、依照本法第四十条的规定通过国家网信部门组织的安全评估;
- 2、按照国家网信部门的规定经专业机构进行个人信息保护认证;
- 3、按照国家网信部门制定的标准合同与境外接收方订立合同, 约定双方的权利和义务;
- 4、法律、行政法规或者国家网信部门规定的其他条件。

资料来源: 中国《个人信息保护法》, 国盛证券研究所

2016 年 4 月 14 日, 欧洲议会投票通过了商讨四年的《一般数据保护法案》(General Data Protection Regulation (GDPR)), 新法案由 11 章共 99 条组成, 该法案将于 2018 年 5 月 25 日正式生效, 将取代现有的《数据保护指令》(Data Protection Directive 95/46/EC), 统一欧盟成员国关于数据保护的法律法规。

此外, GDPR 新规是在 28 个欧盟成员国统一实施生效的, 这将使 28 个欧盟及欧洲经济共同体成员国的隐私保护法更具有一致性和现代性。GDPR 作为一套用来保护欧盟公民个人隐私和数据的新法规, 其颁布意味着欧盟对个人信息的保护及监管达到了前所未有的高度, 堪称史上最严格的数据保护法案。

图表 5: GDPR 中处理个人数据的基本原则

GDPR 中处理个人数据的基本原则

- 1、合法、正当、透明
- 2、处理数据的目的是有限的
- 3、仅处理为达到目的的最少数据
- 4、确保数据准确、及时更新
- 5、存储数据的期限不得长于为达到目的所需要的时间
- 6、采取技术和管理措施以保护数据的安全
- 7、数据控制者有责任并应能够证明做到了以上几点

资料来源: 欧盟《一般数据保护法案》, 国盛证券研究所

图表 6: GDPR 中对合法处理数据的定义

GDPR 适用企业

- 1、数据主体同意为了特定目的处理其数据
- 2、处理数据是为了签订或履行合同的需要
- 3、处理数据是为了遵守法定义务的需要
- 4、处理数据是为了保护数据主体或其他自然人的至关重要的利益
- 5、处理数据是为了公共利益或行使政府授受的权力
- 6、处理数据是为了追求数据控制者的合理利益，但不得损害数据主体的利益

资料来源：欧盟《一般数据保护法》，国盛证券研究所

欧盟 GDPR 法案具有域外效应。也就是说，GDPR 赋予了欧盟在个人信息安全方面的域外管辖权。

主要受影响的企业为以下四类：

图表 7: GDPR 监管企业

GDPR 适用企业

- 1、设立在欧盟境内的企业（控制者、处理者）
- 2、未在欧盟境内设立，但向欧盟境内的数据主体（自然人）提供产品和服务的企业（控制者、处理者）
- 3、未在欧盟境内设立，但涉及监控欧盟境内数据主体（自然人）行为的企业（控制者、处理者）
- 4、未在欧盟境内设立，但在欧洲成员国法律适用的地方设立的企业（控制者、处理者）

资料来源：欧盟《一般数据保护法》，国盛证券研究所

总结来说，GDPR 不仅适用于位于欧盟境内的企业组织机构，也适用于位于欧盟以外的企业组织机构，无论机构所在地在哪里，只要其向欧盟数据主体提供产品、服务或者监控相关行为，或处理和持有居住在欧盟境内的数据主体的个人数据，都将受到 GDPR 法案的监管。

一旦数据泄露，数据控制者应在 72 小时之内向监管机构报告个人数据的泄露情况。当数据泄露可能会给数据主体的权利或自由带来巨大风险时，数据控制者必须毫不延误的通知数据主体，以便数据主体及时采取措施。

不遵守信的数据隐私法规的后果就是会受到严厉的制裁和巨额的罚款。

GDPR 的处罚并不是像网上传的那样直接就罚全球营收的 4%。而是有两个等级的征收行政性罚款的规定：

- 1) 对于一般性的违法，罚款上限是 1000 万欧元，或者在承诺的情况下，最高为上一个财政年度全球全年营业收入的 2%（两者中取数额大者）；
- 2) 对于严重的违法，罚款上限是 2000 万欧元，或者在承诺的情况下，最高为上一个财政年度全球全年营业收入的 4%（两者中取数额大者）；

判罚的严重程度是基于以下因素：

图表 8: 判罚的严重程度要素

判罚的严重程度要素

- 1、违规的性质、严重程度和违规的持续时间
- 2、违规是故意的还是因疏忽造成的
- 3、对个人身份信息的责任心和控制程度
- 4、违规是单个事件还是重复事件
- 5、受到影响的个人资料的种类范围
- 6、数据主体遭遇的损害程度
- 7、为了减轻损害而采取的行动
- 8、由违规产生的财务预期或收益

资料来源：欧盟《一般数据保护法案》，国盛证券研究所

展望一：互联网数据安全需求最迫切，已加大投入力度

数据已成为互联网企业最为重要生产资料。用户会在网站、应用等场景发生一些行为，如浏览商品、收藏内容、完成关卡等。接入行为数据可以帮助广告主了解用户在其网站或应用采取的操作，继而利用这些数据进行广告营销活动。

行为数据接入到 DMP 后，可以用于人群提取、转化统计、程序化创意、oCPA 等。

人群提取，广告主可根据其上传的用户行为数据提取出符合特定条件的用户人群，用于广告定向等。假如广告主上报了一条“某用户某时刻在某个应用内购买了价格 300 元的女装”的行为数据，那么广告主可以在 DMP 中创建一个“最近 7 天在应用内发生过购买行为，商品类型是女装，商品价格>200 ”的行为人群。

转化统计，广告主可把其上传的用户行为数据与广告进行关联，从而统计广告的转化效果。在 DMP 上传用户行为数据后，广告主可以在投放端创建转化规则，在投放端即可看到转化数据报表。转化行为包括“搜索”、“加入购物车”等。

程序化创意帮助广告主通过简单的设置，实现自动化个性化的创意投放及优化，同时享受更低的创意成本和持续的创意优化效果。广告主接入用户数据后，DMP 可以按照用户行为提取人群，用于程序化创意，让不同人群看到不同的广告创意。

oCPA 智能出价模式，让广告主在成本可控的前提下，更具效率和效果地完成广告 ROI 管理。广告主在 DMP 上导入转化数据后，可以选择期望优化的用户行为，如移动应用激活或下载，并提供对该用户行为期望的平均转化成本，然后系统即可通过预估每一次展示的转化价值，自动出价，按照点击扣费。最终帮助广告主实现转化成本控制及出价自动化，提升投放效率。

腾讯数据安全中心（Data Security Center, DSGC）依据《数据安全法》，帮助企业自动梳理数据资产，对企业云上数据进行分类分级和安全风险评估，并协同腾讯云各安全能力，形成闭环的数据安全防护网，帮助企业最大化提升安全效益。

图表 9: 腾讯数据安全中心功能



资料来源：腾讯安全官网，国盛证券研究所

腾讯数据脱敏（Data Masking, DMask）是一款敏感数据脱敏与水印标记工具，可对数据系统中的敏感信息进行脱敏处理并在泄漏时提供追溯依据，为企业数据共享、迁移、分发提供安全保护措施。共享数据时，基于保护企业产权或用户隐私的需求，往往要对数据进行一定的变换，数据脱敏帮助企业实现数据共享脱敏，既能达到合作目的，又不会造成核心数据泄漏。

图表 10: 腾讯数据脱敏解决方案功能

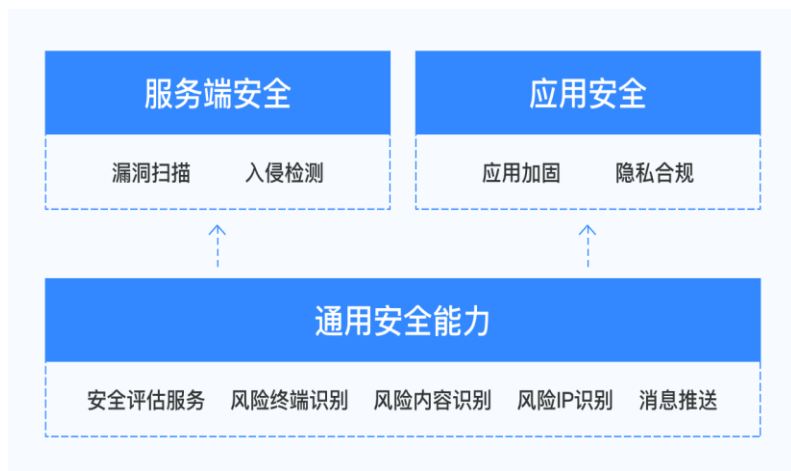


资料来源：腾讯安全官网，国盛证券研究所

百度推出“史宾格”安全和隐私合规平台，基于 AI 检测技术，比照《App 违法违规收集使用个人信息行为认定方法》《工业和信息化部关于开展 App 侵害用户权益专项整治工作的通知》《工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》《信息安全技术个人信息安全规范》等规范性文件、国家标准，提供隐私风险项检测、

隐私专项检测、场景检测、权限过度收集与使用情况检测等产品服务，助力监管机构、应用市场、大型企业、App 开发者等完成 App 隐私合规自查，发现隐私违规风险。

图表 11: 百度 APP 安全解决方案



通用安全能力

包括APP的综合安全评估以及部分通用的安全能力，APP可以通过集成这部分能力提高访问风险识别、内容能力和消息推送到达率等。

应用安全

解决应用端安全问题。主要解决应用被逆向破解可能造成的业务数据泄露等风险，以及滥用隐私等不符合相关监管规范的问题。

服务端安全

聚焦服务端安全问题。发现服务端的安全漏洞以及识别入侵风险，提升服务端的安全防护等级。

资料来源：百度官网，国盛证券研究所

图表 12: 史宾格安全及隐私合规平台功能

		扶持版	专业版
每天检测次数		5次	无限制
可检测App数量		15款App	无限制
测试手机使用时长		累计15小时	无限制
使用期限		1年	1年
隐私检测专项	《工信部App侵害用户权益专项整治8项要求》	✓	✓
	《中华人民共和国网络安全法》	×	✓
	《信息安全技术个人信息安全规范》	×	✓
	《App违法违规收集使用个人信息行为认定方法》	×	✓
	《App违法违规收集使用个人信息自评估指南》	×	✓
隐私检测功能	权限代码分析	✓	✓
	第三方SDK分析	✓	✓
	个人信息收集行为分析	×	✓
	隐私行为分析	×	✓
隐私风险项检测	违法违规行为隐私风险分析7项	✓	✓
安全服务	病毒检测	✓	✓
	恶意吸费检测	✓	✓
	强行捆绑无关软件检测	✓	✓
	漏洞扫描	×	✓
	漏洞代码溯源	×	✓

资料来源：百度官网，国盛证券研究所

展望二：金融、医疗、汽车、能源等数据安全潜在市场巨大

金融机构在客户所掌握的“个人信息”，依据其获取途径和发挥作用的不同，在《信息保护法》之下可归于不同的类型，相应地由金融机构进行不同程度的保护。

图表 13: 金融结构涉及相关个人信息

金融机构“个人信息”	《个人信息保护法》下“个人信息”类型
员工个人信息	个人信息
客户相关信息	敏感个人信息
业务合作方相关个人信息	
衍生个人信息	非个人信息

资料来源：《个人信息保护法》，国盛证券研究所

随着实体医院将诊疗活动延伸至互联网端，数据共享和流通成为刚性业务需求，静态的隔离保护措施难以控制数据在流动中的风险，关乎患者隐私、种类繁多的医疗数据也迎来愈加严峻的安全挑战，互联网医院需要通过动态变化的视角分析和判断数据安全风险。

图表 14: 互联网医院面临的主要数据安全风险



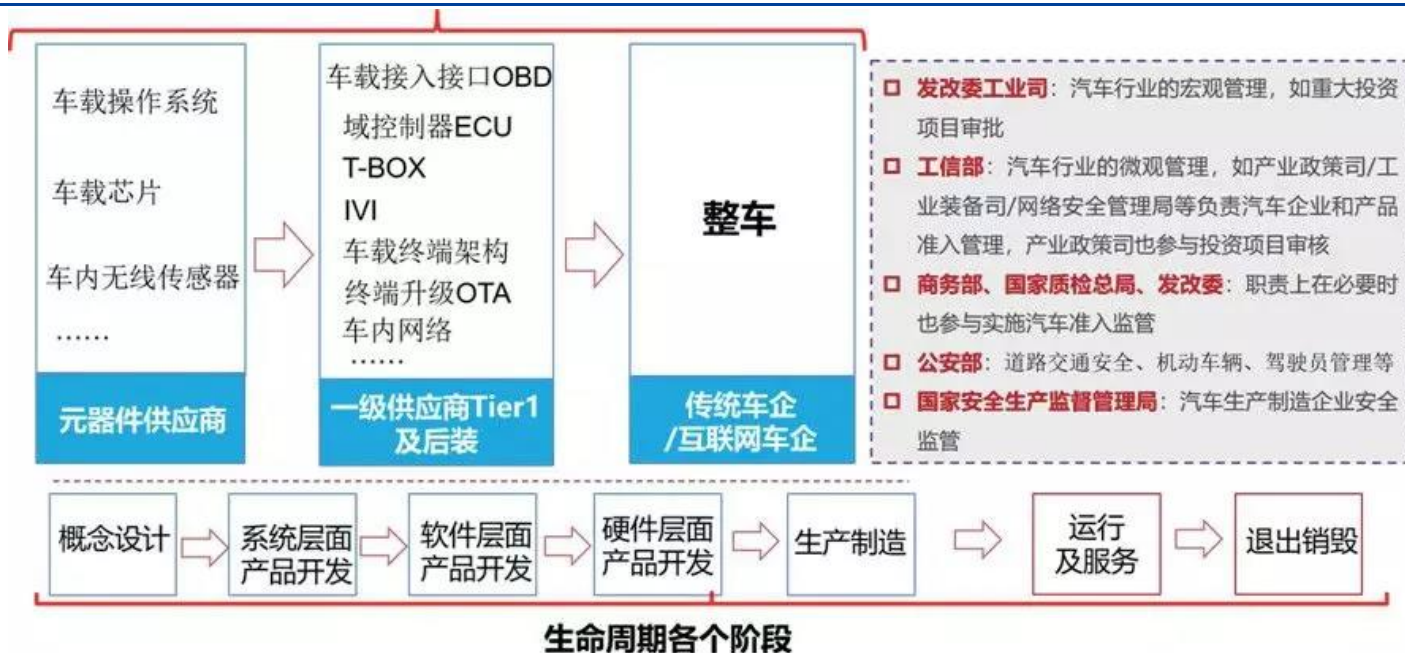
资料来源：医疗数据安全，国盛证券研究所

随着智能汽车产业、车联网技术的快速发展，以自动辅助驾驶为代表的人工智能技术日益普及，汽车数据处理能力日益增强，暴露出的汽车数据安全风险和隐患日益突出。在汽车数据安全领域出台有针对性的规章制度，明确汽车数据处理者的责任和义务，

规范汽车数据处理活动，是防范化解汽车数据安全风险、保障汽车数据依法合理有效利用的需要，也是维护国家安全利益、保护个人合法权益的需要。

《规定》明确，汽车数据处理者应当履行个人信息保护责任，充分保护个人信息安全和合法权益。开展个人信息处理活动，汽车数据处理者应当通过显著方式告知个人相关信息，取得个人同意或者符合法律、行政法规规定的其他情形。处理敏感个人信息，汽车数据处理者还应当取得个人单独同意，满足限定处理目的、提示收集状态、终止收集等具体要求或者符合法律、行政法规和强制性国家标准等其他要求。汽车数据处理者具有增强行车安全的目的和充分的必要性，方可收集指纹、声纹、人脸、心律等生物识别特征信息。

图表 15: 我国车联网安全监管机制现状

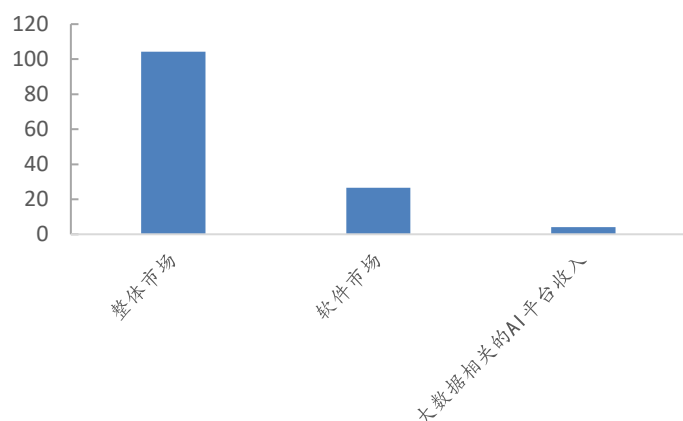


资料来源：信息安全与通信保密杂志社，国盛证券研究所

展望三：数据安全市场规模及落地速度有望超预期

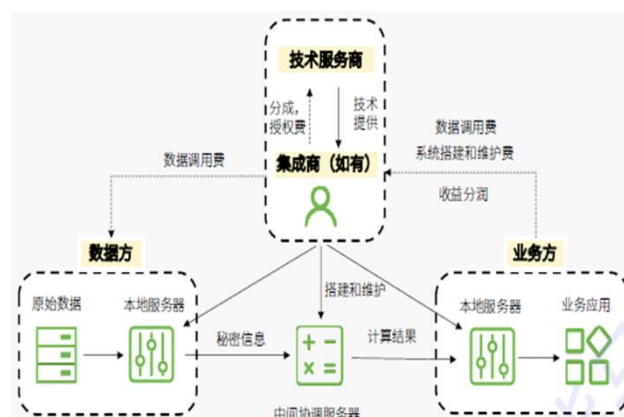
数据安全市场空间测算，依据大数据市场中 AI 平台收入推算仅计算环节 2023 年有望达百亿，数据安全全生命周期长期潜在空间有望达千亿。数据安全计算模块常见于大数据服务场景，添加至 AI 计算平台，并且与 AI 应用同样以数据为基础，进行安全、存储以及计算等服务，故以 AI 平台收入为隐私计算产值上限，根据 IDC 预测 2020 年我国大数据市场约 104.2 亿美元，其中软件市场规模为 26.5 亿美元，AI 平台收入约 4 亿美元，IDC 预测 2018 至 2024 年 AI 产业年均复合+39%，则 AI 平台收入 2024 年有望达 15 亿美元，则数据安全方案上限近百亿人民币。

图表 16: 数据安全 2023 年规模上限超百亿



资料来源: IDC, 国盛证券研究所

图表 17: 隐私计算商业模式



资料来源: KPMG, 国盛证券研究所

数据深度价值挖掘过程中需要兼顾数据应用和安全，平衡效率和风险，在保障安全的前提下发挥数据价值。以多方安全计算（Secure Multi-Party Computation, MPC）、可信执行环境（Trusted Execution Environment, TEE）、联邦学习（Federated Learning, FL）等为代表的隐私计算技术为解决了数据流通过程中的“可用不可见”难题，有助于破解数据保护与利用之间的矛盾，已在金融、医疗、政务等领域开始推广应用：

- 1) 对于个人消费者，隐私计算应用有助于降低隐私数据在应用过程中的泄密风险；随着信息化程度不断提高，个人信息被采集和广泛应用，同时也面临着信息泄露风险，而隐私计算在很多场景的应用，可以提升对个人信息的保护水平，降低个人信息在应用过程中泄露的风险。
- 2) 对于 B 端企业，隐私计算兼顾数据协作过程中的安全性与效率性，监督企业履行数据保护义务。企业内部借助隐私计算，能够切实保护企业在采集、存储、分析等过程中的关键信息。另一方面，隐私计算能够促进企业的跨界数据合作，由于隐私计算能够实现数据可用不可见，能够帮助不同企业和机构与产业链上下游的主体进行联合分析。
- 3) 对于 G 端政府、社会机构，隐私计算可促进数据价值和社会福利最大化。一是借助隐私计算能够在政府数据开放过程中，在采集、存储、协作等方面提升数据安全和隐私保护水平，在保障数据安全的同时增强全社会的数据协作，通过数据的应用最大化社会福利。二是借助隐私计算推动数据要素赋能产业升级

随 IT 架构上云，长期数据安全 SaaS 运营收入有望达千亿，商业模式改善带来估值提升机遇。以消费贷款场景为例，假设 2030 年金融机构信用风险建模使用联邦学习渗透率达 60%，服务费率为 1%，国内短期消费信贷市场 2019 年已达 9.92 万亿元，假设直到 2030 年年化复合增速为 8%，则 2030 年市场有望达 21.42 万亿元，数据安全收入有望达 1285 千亿元，考虑互联网、医疗及政务大数据等场景，空间巨大。

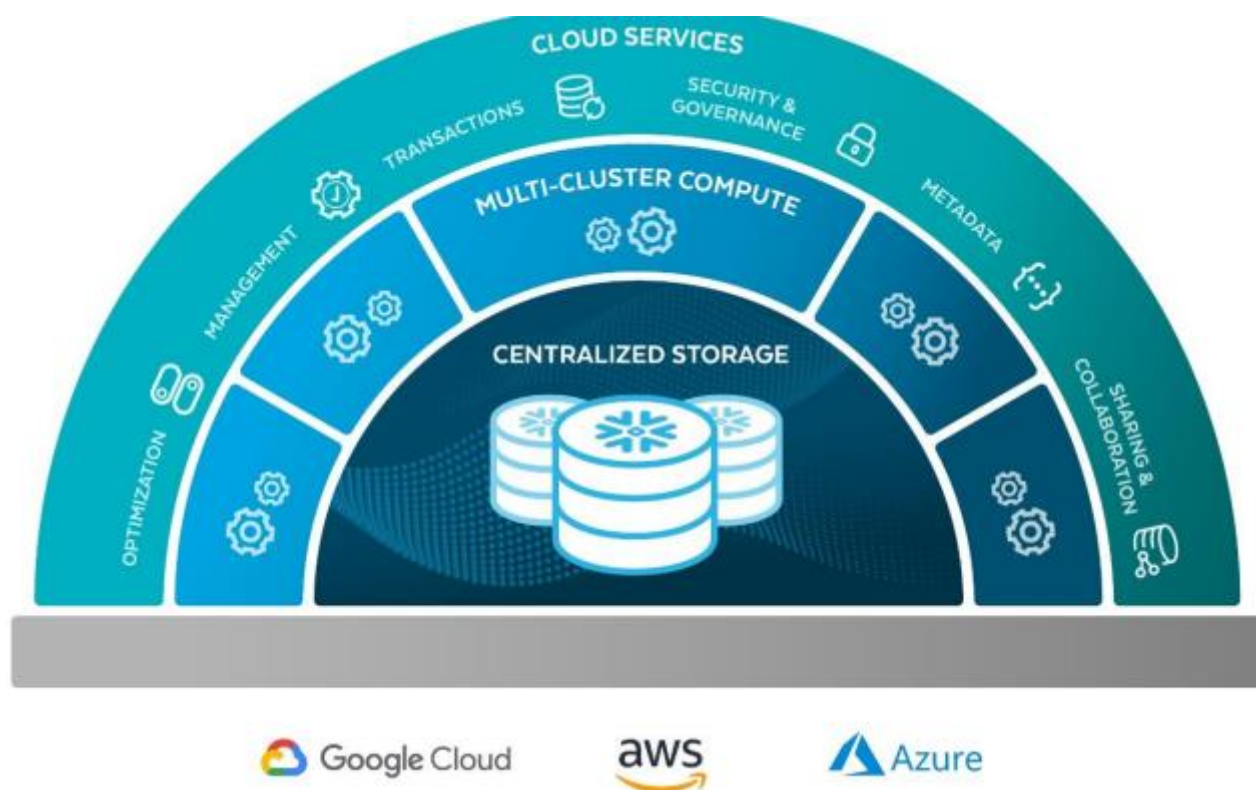
平台经济垄断本质是数据垄断，通过数据协作运用打破垄断过程中的安全性愈发重要，未来隐私计算领军企业除具备完备隐私计算服务能力外，还将具备“Snowflake+CrowdStrike”特征，即同时具备“DaaS+SECaaS”能力。

Snowflake 提出 Data-Warehouse-as-a-Service (DaaS) 概念，即云原生并专注于分析型数据仓库的 SaaS 服务。Snowflake 将各类客户的各类数据整合至云数据平台，方便用户进行数据分析，简化了数据共享，还能够将数据管理和合规问题的风险降到最低。

Snowflake 可以解决的痛点包括：数据孤岛、数据更高效的搜索和维护、数据分析的速度和成本。相较于传统的硬件服务器存储传输、单一 IaaS 厂商而言，其优势在于：可伸

缩性、易操作、SaaS 订阅模式、多云架构，商业模式天然具备网络效应等。

图表 18: Snowflake 基于三朵公有云的云原生分析型数据仓库



资料来源：公司招股说明书，国盛证券研究所

风险提示

行业竞争加剧风险：网络安全行业竞争激烈，如果行业行业竞争进一步加剧，或对毛利率产生不利影响。

政策力度不及预期风险：等保 2.0、护网行动等合规政策执行力度若不及预期，将影响企事业单位对于网安产品及服务的需求。

宏观经济风险：疫情影响下，宏观经济面临下行风险，可能导致各行业企业网安支出受到影响。

测算可能与实际存在误差：目前隐私计算仍处于初始发展期，存在落地节奏及渗透不及预期风险。

免责声明

国盛证券有限责任公司（以下简称“本公司”）具有中国证监会许可的证券投资咨询业务资格。本报告仅供本公司的客户使用。本公司不会因接收人收到本报告而视其为客户。在任何情况下，本公司不对任何人因使用本报告中的任何内容所引致的任何损失负任何责任。

本报告的信息均来源于本公司认为可信的公开资料，但本公司及其研究人员对该等信息的准确性及完整性不作任何保证。本报告中的资料、意见及预测仅反映本公司于发布本报告当日的判断，可能会随时调整。在不同时期，本公司可发出与本报告所载资料、意见及推测不一致的报告。本公司不保证本报告所含信息及资料保持在最新状态，对本报告所含信息可在不发出通知的情形下做出修改，投资者应当自行关注相应的更新或修改。

本公司力求报告内容客观、公正，但本报告所载的资料、工具、意见、信息及推测只提供给客户作参考之用，不构成任何投资、法律、会计或税务的最终操作建议，本公司不就报告中的内容对最终操作建议做出任何担保。本报告中所指的投资及服务可能不适合个别客户，不构成客户私人咨询建议。投资者应当充分考虑自身特定状况，并完整理解和使用本报告内容，不应视本报告为做出投资决策的唯一因素。

投资者应注意，在法律许可的情况下，本公司及其本公司的关联机构可能会持有本报告中涉及的公司所发行的证券并进行交易，也可能为这些公司正在提供或争取提供投资银行、财务顾问和金融产品等各种金融服务。

本报告版权归“国盛证券有限责任公司”所有。未经事先本公司书面授权，任何机构或个人不得对本报告进行任何形式的发布、复制。任何机构或个人如引用、刊发本报告，需注明出处为“国盛证券研究所”，且不得对本报告进行有悖原意的删节或修改。

分析师声明

本报告署名分析师在此声明：我们具有中国证券业协会授予的证券投资咨询执业资格或相当的专业胜任能力，本报告所表述的任何观点均精准地反映了我们对标的证券和发行人的个人看法，结论不受任何第三方的授意或影响。我们所得报酬的任何部分无论是在过去、现在及将来均不会与本报告中的具体投资建议或观点有直接或间接联系。

投资评级说明

投资建议的评级标准		评级	说明
评级标准为报告发布日后的 6 个月内公司股价（或行业指数）相对同期基准指数的相对市场表现。其中 A 股市场以沪深 300 指数为基准；新三板市场以三板成指（针对协议转让标的）或三板做市指数（针对做市转让标的）为基准；香港市场以摩根士丹利中国指数为基准，美股市场以标普 500 指数或纳斯达克综合指数为基准。	股票评级	买入	相对同期基准指数涨幅在 15%以上
		增持	相对同期基准指数涨幅在 5%~15%之间
		持有	相对同期基准指数涨幅在 -5%~+5%之间
		减持	相对同期基准指数跌幅在 5%以上
	行业评级	增持	相对同期基准指数涨幅在 10%以上
		中性	相对同期基准指数涨幅在 -10%~+10%之间
		减持	相对同期基准指数跌幅在 10%以上

国盛证券研究所

北京

地址：北京市西城区平安里西大街 26 号楼 3 层
 邮编：100032
 传真：010-57671718
 邮箱：gsresearch@gszq.com

南昌

地址：南昌市红谷滩新区凤凰中大道 1115 号北京银行大厦
 邮编：330038
 传真：0791-86281485
 邮箱：gsresearch@gszq.com

上海

地址：上海市浦明路 868 号保利 One56 1 号楼 10 层
 邮编：200120
 电话：021-38124100
 邮箱：gsresearch@gszq.com

深圳

地址：深圳市福田区福华三路 100 号鼎和大厦 24 楼
 邮编：518033
 邮箱：gsresearch@gszq.com