CAICT 中国信通院

# 数据安全技术与产业发展研究报告

（2021 年）

中国信息通信研究院安全研究所

2021 年 12 月

# 版权声明

# 编制说明

本蓝皮报告由中国信息通信研究院撰写，限于撰写组时间、知识局限等因素，内容恐有疏漏，烦请各位读者不吝指正。

在本报告的研究过程中，得到以下单位的支持协助，在此表示感谢（以企业名称笔画为序）：上海观安信息技术股份有限公司、山石网科通信技术股份有限公司、中国移动通信集团有限公司、中国电信集团有限公司、中国联合网络通信集团有限公司、中国工商银行数据智能中心、贝壳找房（北京）科技有限公司、北京天融信网络安全技术有限公司、北京安华金和科技有限公司、北京启明星辰信息安全技术有限公司、北京炼石网络技术有限公司、北京数安行科技有限公司、北京信安世纪科技股份有限公司、北京天空卫士网络安全技术有限公司、北京中安星云软件技术有限公司、北京大学粤港澳大湾区知识产权发展研究院、成都思维世纪科技有限责任公司、闪捷信息科技有限公司、华为技术有限公司、全球能源互联网研究院有限公司、全知科技(杭州)有限责任公司、亚信安全科技股份有限公司、杭州世平信息科技有限公司、杭州天宽科技有限公司、杭州美创科技有限公司、郑州信大捷安信息技术股份有限公司、金砖国家未来网络研究院（中国•深圳）、奇安信科技集团股份有限公司、恒安嘉新（北京）科技股份公司、浙江御安信息技术有限公司、浙江华途信息安全技术股份有限公司、深圳腾讯计算机系统有限公司、珠海高凌信息科技股份有限公司、绿盟科技集团股份有限公司、深信服科技股份有限公司、维沃移动通信有限公司、博瑞得科技有

限公司。

# 前　言

近年来，国内数字经济和信息产业蓬勃发展，5G、大数据、人工智能、区块链等技术不断落地应用。2020 年我国数字经济规模达到 39.2 万亿元，占 GDP 比重达 38.6%[1]。新业态新技术在推动经济转型升级的同时，数据规模不断扩大，数据泄露、滥用等风险日益凸显，防范数据安全风险、构建数据安全保护体系成为各方共识。习近平总书记多次作出重要指示批示，提出加快法规制度建设、切实保障国家数据安全等明确要求。党的十九大报告、十四五规划等重要文件提出推动发展数据战略，统筹数据开发利用、隐私保护和公共安全，规范数据有序流通，推进数据资源整合和开放共享，保障数据安全。落实数据安全离不开数据安全技术和产业的有力支撑。在新冠肺炎疫情常态化发展和国际形势风云变化的关键时期，系统性梳理展望我国数据安全技术与产业现状以及未来发展趋势，对促进我国数据安全健康有序发展意义重大。

基于此，本研究报告通过调研访谈的方式研究梳理我国数据安全技术、产品和服务的发展驱动力以及现状，形成总体的数据安全技术与产业发展视图。同时，分析总结数据安全技术发展存在的问题和挑战，并对数据安全技术及产业发展进行了趋势研判，为相关企业开展数据安全技术手段建设过程中提供一些参考。

[1] 来源：《中国互联网发展报告 2021》

# 目 录


第一部分 数据安全技术.....1
一、 数据安全技术进入快速发展期.....1
二、 数据安全技术总体视图.....1
三、 数据安全关键技术发展分析.....3
（一） 数据加密技术.....3
（二） 数据脱敏技术.....4
（三） 数据识别技术.....6
（四） 数据标记技术.....6
（五） 数字水印技术.....7
（六） 隐私计算技术.....9
第二部分 数据安全产业.....10
一、全球数据安全产业发展概况.....10
（一） 新形势推动国外数据安全产业发展.....10
（二） 数据安全产品向体系化智能化发展.....11
（三） 产业投融资迎来大爆发.....14
二、我国数据安全产业发展现状.....16
（一） 数据安全产业顶层设计思路逐渐明晰.....16
（二） 数据安全产品及服务发展态势向好.....21
（三） 国内数据安全企业迎来高速发展机遇.....26
（四） 数据安全产业生态环境持续优化.....28
三、我国数据安全产业发展的驱动力.....34
（一） 数据安全重视程度持续提升.....34
（二） 数据泄露成本上涨推升企业数据安全需求.....34
（三） 监管行动扩大数据安全合规需求.....35
（四） 产业数字化步伐加快推动数据安全产业发展.....36
（五） 新兴领域技术迭代引领数据安全产业成长.....37
第三部分 未来展望.....38
一、 数据安全成为战略布局重点.....38

二、 数据安全保护规则体系进一步细化.....38
三、 数据安全企业将迎来快速发展机遇.....39
四、 数据安全技术将不断突破创新.....40
五、 数据安全产业生态将稳步推进.....40

# 图 目 录

图 1　2017-2021 年 Gartner 萌芽期技术对比分析图.....1
图 2　数据安全技术总体视图.....2
图 3　近十年国外数据安全企业投融资情况图.....15
图 4　国内数据安全产业增长曲线图.....27
图 5　近年数据泄露成本趋势图.....35

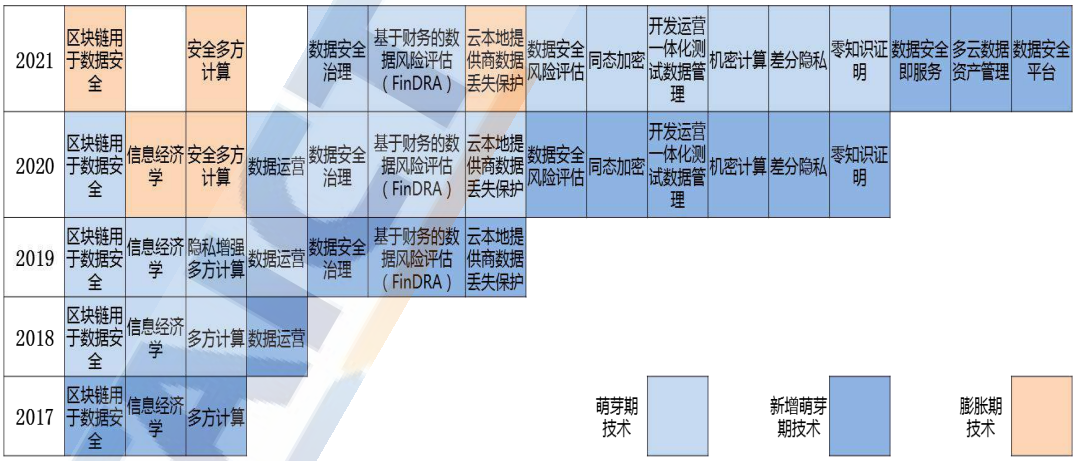
# 表 目 录

表 1　国外数据安全产品调研表.....12
表 2　2020 年国外数据安全领域企业投融资情况表.....15
表 3 部分数据安全厂商安全服务情况统计表.....25

# 第一部分　数据安全技术

## 一、 数据安全技术进入快速发展期

数据安全技术最初是网络安全技术的一个分支，随着数字经济的发展和信息技术的演进，逐渐形成一套独立的技术体系，成为热点研究领域，进入快速发展期。近几年的 RSA 大会上，数据安全在十大热议话题、创意沙盒十强中的占比和热度逐年提高。从 2017-2021 年 Gartner 发布的数据安全技术成熟度曲线研究报告来看，新兴数据安全技术呈现逐年递增的趋势。尤其是 2020 年，数据安全新技术迅猛增加，处于萌芽期的新技术增加了 6 项，其中安全多方计算、同态加密、差分隐私等隐私增强计算技术近两年发展势头强劲，安全多方计算已经从萌芽期发展到了期望膨胀期，同态加密、差分隐私技术尚处于萌芽期。

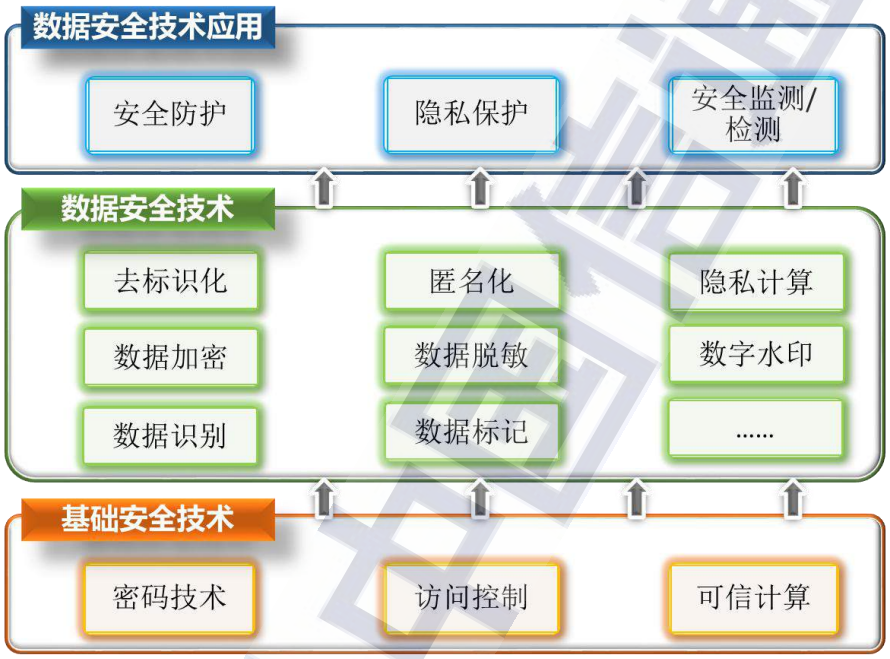



来源：2017-2021 年 Gartner 数据安全技术成熟度曲线

图 1 2017-2021 年 Gartner 萌芽期技术对比分析图

## 二、 数据安全技术总体视图

当前数据安全技术快速发展，技术领域不断细分，技术体系不断完善。在借鉴 Gartner DSG 模型、ISO38505-1 数据治理应用模型、GDPC 模型等国际主流数据安全技术框架的基础上，结合数据安全技术发展实际现状，依据技术内涵、主要功能及应用场景，本报告提出数据安全技术总体视图如下。




来源：中国信息通信研究院

图 2 数据安全技术总体视图

数据安全技术视图总体可以分为三层，其中，基础安全技术层包括密码技术、访问控制、可信计算等共性安全技术，是网络安全与数据安全技术体系构建的基础，在网络安全领域，这些技术用于保护网络与信息系统的安全；在数据安全领域，这些技术用于保护计算对象——数据的安全。数据安全技术层是以数据为核心，围绕数据要素在全生命周期中的安全需求，对数据实施识别、变形、标记、计算等操作的技术集合，包括采集阶段的数据识别、分类分级

标记，存储与应用阶段的加密、脱敏、去标识化，以及共享流通阶段的隐私计算、数据水印等。数据安全技术应用层利用一种或多种数据安全技术组合，实现数据安全保护、安全检测/监测、隐私保护、追踪溯源等应用场景下的数据安全功能。

## 三、 数据安全关键技术发展分析

在数据安全技术总体视图中，数据安全技术层中所列出的这些关键技术一方面是实现数据安全保护目标的核心技术手段，另一方面又为数据安全技术应用层所要实现的安全监测、隐私保护等目标提供了技术支撑。因此，有必要对数据安全技术层的一些典型技术进行具体展开分析。基于目前数据安全技术应用的热点，本报告选择数据加密、数据脱敏、数据识别、数据标记、数字水印和隐私计算六种关键技术，开展技术发展现状梳理和发展展望，以期为数据安全技术发展提供前瞻性思考。

### (一)数据加密技术

数据加密技术是以密码技术为基础对数据进行编码转化的保护方法，是网络安全和数据安全领域的通用关键技术。在网络安全领域，加密技术一般用于静态文件加密、数据库加密以及数据传输加密等场景，解决的是信息系统的边界防护和传输通道安全问题；在数据安全领域，加密技术用于满足数据全生命周期的存储、应用、共享流通等各个环节的安全需求，并兼顾数据安全性与可用性的平衡。随着数字经济的高速发展，应用领域日趋复杂多样，传统加密技术的效率、强度、灵活性等无法满足多变的业务需求。因此，一

方面，**随着数据共享流通场景保护需求的不断增加，数据加密技术从静态数据加密向动态数据加密扩展**。在数据流转场景下，数据加密操作需要嵌入到业务流程中，并且要根据细化的访问控制需求，提供多场景细粒度的加密策略和密钥管理方法。另一方面，**目前数据加密技术因为新兴领域的需求不断变化，而产生新的演进方向**[2]。以云计算环境为例，数据拥有者的敏感数据在云端以加密形式存储，而在数据使用和共享过程中，由于数据拥有者对云端不完全信任，不能将解密密钥发送到云端，由云端解密后再进行应用和共享，这给数据拥有者的数据共享业务开展带来不便。因此，云环境下的密文检索、代理重加密、密钥协商等技术应运而生。其中，代理重加密技术使得云端可以直接将密文转化为可用另一方私钥解密的密文，既无需接触数据拥有者的敏感数据，又可满足数据共享的需求[3]。目前，基于身份和属性的代理重加密技术在可重复性、非交互性、单向性、可验证性等方面相对成熟，基于区块链的代理重加密技术刚刚起步[4]。

### （二）数据脱敏技术

**数据脱敏技术可以在不泄露敏感信息的前提下保留数据源的可用性，是目前应用最多的数据安全保护技术手段**。数据脱敏技术的核心是脱敏算法的选择，目前脱敏算法主要分为如下三类：第一类是标准的加密算法，数据加密后完全失去业务属性，算法开销大，

[2] 詹榜华，新时期新密码新发展，信息安全与通信保密，2020
[3] 沈剑等，云数据安全保护方法综述，计算机研究与发展，2021
[4] 鲁金钿等，云数据安全研究进展，电子与信息学报，2021

适用于机密性要求高、不需要保持数据业务属性的场景。第二类是基于数据失真的算法，一般不可逆，如随机干扰、乱序等，通过这种算法可以生成“看起来很真实的假数据”，适用于群体信息统计或需要保持数据业务属性的场景。第三类是置换算法，兼具可逆和保持数据业务属性的特点，可以通过位置变换、表映射、算法映射等方式实现。表映射方法应用起来相对简单，但是随着数据量的增大，相应的映射表同量增大，其应用具有局限性；算法映射不依赖映射表，通过预先设计的算法实现数据的变换，满足大规模数据映射的需求。**在选择业务系统的脱敏算法时，可用性和隐私保护的平衡是关键**，既要满足业务对数据可用性的需求，又要兼顾最小可用原则，最大限度的保护敏感信息。

**目前来看，数据脱敏技术应用模式成熟，随着对数据开发利用需求的不断增长，数据脱敏技术的应用将更加广泛。**数据脱敏技术分为静态脱敏和动态脱敏两种应用模式。静态数据脱敏技术一般是通过脱敏算法，将生产数据导出至目标存储介质，可以支持源库脱敏、跨库脱敏、数据库异构脱敏、数据库到文件脱敏、文件到数据库脱敏、文件到文件脱敏等场景。动态数据脱敏通过解析 SQL 语句匹配脱敏条件，通过改写或拦截 SQL 语句，返回脱敏后的数据到应用端，可以支持实时运维管理、应用访问等场景。从 Gartner 2017-2020 年的《数据脱敏市场指南》可以看出，企业对于数据脱敏技术的使用从 2017 年的 15%增加到了 2018 年的 20%，预计在 2022 年将达到 50%。

### （三）数据识别技术

数据识别技术主要目标是识别和发现敏感数据，从而能够更有效地实施敏感数据保护，是精准数据安全防护的基础。目前，数据识别技术广泛应用于数据分类分级、数据安全监测、数据脱敏等技术产品中。传统的数据识别技术以关键字、字典和正则表达式匹配为主，这种方法再辅以人工的帮助可以适用于结构化数据的识别。在大数据场景下，随着数据量的剧增，数据格式更加丰富多样，**传统的数据识别技术对于非结构化数据难以适用，对于结构化数据也无法满足日益复杂的识别需求。**在此需求驱动下，引入机器学习和自然语言处理等技术，可以在一定程度上自动生成识别规则，解决上述难题。目前常用的模型算法包括 HMM 模型、CRF 模型、BiLSTM 模型和 BiLSTM-CRF 模型等，但各类模型的运算开销比较大，还不能满足大规模应用的需要，算法的成熟度以及准确度也有待提升，智能数据识别技术应用并不广泛。**未来，数据识别技术将倾向于将传统方法与智能化方法结合，**兼顾识别覆盖率、效率与准确率，降低人工参与的比率，逐步向自动化、智能化不断演进[5]。

### （四）数据标记技术

数据标记技术是指对需要保护的数据增加标记信息，是实现数据分类分级安全防护的基础。**目前，数据标记技术处于探索研究阶段，**学术界对于数据标记技术的研究相对较少，产业界运用的数据标记技术也并不是一种特有的技术，而是将能够实现类似效果的技

[5] 唐建,基于自然语言处理的敏感数据识别技术研究与实现,电信科学技术研究院研究生论文,2021.

术应用到实际业务场景中，一般可以分为分离式和嵌入式两类。分离式标记即标记信息和原始数据分开，只建立两者间的映射关系，主要通过扩展元数据信息或数据库表结构、建立索引表等方式实现，适用于数据访问控制、加密等场景；嵌入式标记即将标记信息和原始数据融合形成新的带有标记信息的数据，主要通过密码标识、数字指纹、数字水印、数字隐写等技术实现，适用于数据审计和追溯等场景。**虽然数据标记技术已在产业界初步应用，但在企业落地过程中还存在一定困难。**一方面，企业很难兼顾数据标记技术的适用性和应用成本。对于新建信息系统，企业可以按照场景需求和数据类型等选择适当的数据标记技术；但对已有信息系统增加标记时，若需改变已固化的数据结构，投入成本较大，企业很难下决心做大规模的升级改造，只能退而选择对系统影响较小的标记技术。另一方面，如何实现全局场景下统一的数据标记也是企业全面落实数据分类分级管控过程中面临的难题。一般来说，企业内各系统标记信息各自独立且分散，可在各自应用场景中被识别、利用，但跨系统的异构标记信息传输和识别，仍是技术实现上的难题。未来，数据标记技术仍需要学术界和产业界持续跟踪研究[6]。

### （五）数字水印技术

R. G. van Schyndel 等人在 1994 年首次定义了数字水印技术[7]，数字水印（Digital Watermarking）技术是永久镶嵌在其它数据（宿

[6] 来源：深度分析| 在落实数据分类分级保护中数据标记方法的现状分析和建议 https://mp.weixin.qq.com/s/_rNkl7ZXFN7Xth5qDPBhHQ

[7] VAN SCHYNDEL R G,TIRKEL A Z,OSBRNE C F. A digital watermark[C].IEEE International Conference on Image Processing,1994:86-90.

主数据或载体数据）中具有可鉴别性的数字信号或模式，且不影响宿主数据的可用性[8]。除某些特殊要求外，水印信息一般要求是不可见的，并有相应的标准来评判其不可见性或透明性。**数字水印技术发展至今，已经逐渐由传统的理论研究阶段发展到实际应用阶段，且为了增加其安全性，常与密码学相结合**[9]。数字水印技术最早主要应用于知识产权保护、票据防伪等场景，随着互联网的迅猛发展以及网络欺骗行为的频繁发生，人们越来越怀疑数据的真伪，对数据的真实性要求越来越高，数字水印技术恰巧可以应用到数据的隐藏标识和篡改提示、隐蔽通信及其对抗、数据追踪溯源等场景，为数据泄露追责、数据篡改等提供解决方案。但数字水印技术在关系型数据库中的发展还不尽如人意,这是由于关系型数据库中的冗余空间很小，元组和属性都具有无序性及数据库自身经常需要更新操作等原因造成的[10]。

**目前，无论是在结构化还是非结构化数据应用场景下，数字水印技术在鲁棒性和抗攻击方面都存在一些共同的技术难题。**例如：数字水印的鲁棒性和透明性如何兼顾，如何应对几何攻击等新的攻击方式[11]。**因此，水印鲁棒性提升和水印抗攻击方法是研究的重点方向。**目前，学术界研究证明，人工智能方法的引入是提高水印算法鲁棒性和抗攻击性的有效途径[12]。

---

[8] VAN SCHYNDEL R G,TIRKEL A Z,OSBRNE C F. A digital watermark[C].IEEE International Conference on Image Processing,1994:86-90.

[9] 吴海涛,詹永照,数字水印技术综述,软件导刊,2015.

[10] 程虹,对关系数据库数字水印技术的研究,郑州大学硕士学位论文,2009.

[11] 邵晓根,孙天凯,丁宾,王兴元.基于神经网络分类的图像水印算法.计算机应用,2011.

[12] 张颖君,陈恺,周赪,吕培卓,刘勇,黄亮.神经网络水印技术研究进展.计算机研究与发展,2021.

## （六）隐私计算技术

**隐私计算是在提供隐私保护的前提下，实现数据价值挖掘的技术体系**[13]。隐私计算作为涉及多领域交叉融合的跨学科技术体系，包括联邦学习、安全多方计算、机密计算、差分隐私和同态加密等，能够提供数据计算过程和数据计算结果的隐私安全保护能力。目前，隐私计算多用于实现多方数据所有权、管理权、使用权分离时的数据“可用而不可见”，从而达到数据联合使用以及隐私保护的目的。**随着隐私计算应用范围渐广，各类隐私计算技术之间出现相互融合的趋势。**例如，联邦学习技术架构的底层往往会使用不经意传输、秘密分享等安全多方计算技术，以及同态加密技术、差分隐私技术，以确保各方数据交换过程中的隐私性。**在安全性上，隐私计算技术仍存在问题。**现有的安全多方计算、联邦学习技术框架尚难以应对恶意安全假设下的多数合谋，且学术界仍不断发现隐私计算的新安全风险。因此，隐私计算技术中的安全解决方案仍需不断与时俱进。**计算效率上，隐私计算技术已达到可用状态，但仍需提高。**以安全多方计算技术为例，其计算过程相对明文计算增加了电路转换、加密解密等过程，需要付出额外的计算开销，目前最前沿的安全多方计算框架计算 64 位整数的两个 10 万元素向量内积的时间随算法不同在 $10^{-2}$ 秒级至 101 秒级浮动[14]，与明文计算仍存在差距。

---

[13] UN Handbook on Privacy-Preserving Computation Techniques

[14] Marcel Keller, MP-SPDZ: A Versatile Framework for Multi-Party Computation, CCS '20: Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security, 2020

# 第二部分　数据安全产业

## 一、全球数据安全产业发展概况

伴随全球数字化进程日益加快及新冠肺炎疫情影响，全球数据体量呈现指数型增长态势，不断扩大的数据规模促使社会各方将注意力投向数据安全，资本市场对数据安全企业的关注度明显提升。同时，目前国外有近四百家企业提供了数据安全和隐私保护相关产品及服务[15]，数据安全产品呈现出快速适应新场景、新模式并不断迭代优化等特点。

### （一）新形势推动国外数据安全产业发展

**一方面，新冠肺炎疫情持续蔓延反而为数据安全产业发展提供新契机。**新型冠状病毒及变种在全球迅速传播，各国政府部门及企业不得不选择远程办公、居家办公等模式，网络在线活动及相应的数据大幅度增加，公众对于数据安全和个人信息保护的担忧刺激了数据安全产品和服务需求的快速增长。与此同时，疫情防控措施进一步加快社会数字化转型步伐，保障转型过程中的数据安全成为数据安全产业发展的重要动力。**另一方面，西方主要发达经济体相继发布数据战略，利用数据基础设施建设、人才培养等手段促进产业需求。**2020 年，欧盟发布《欧洲数据战略》，战略提出更新法规政策以提供更多数据安全产品需求、进一步投资数据安全技术创新等愿景，明确关注社会数据安全治理，提升数据中心、边缘安全、数

[15]来源：全球数据安全服务企业名录 https://airtable.com/shrLZ7JIsSEnysQOw/tbl8m2hIajtIOfpC2

据托管、处理、使用和兼容等方面的能力和基础设施建设，扩大欧盟数据安全人才规模，进一步提高欧盟全域数据安全能力。2020 年，美国发布《联邦数据战略和 2020 年行动计划》，该计划提出促进数据流通、保护数据完整性、提高数据处理透明度、增强数据管理分析能力和促进数据访问途经多样化等四十项具体数据管理实践，建立了一致化的数据基础设施和标准实践，提升了社会对于数据安全的重视程度，进一步促进了政府部门及企业对数据安全产品和服务的需求。

### （二）数据安全产品向体系化智能化发展

**一是“大厂”布局数据安全产品生态建设。**亚马逊、因特尔、微软、惠普等国外数据安全“大厂”自身拥有雄厚的资金和强大的研发团队及产品设计实力，重点布局数据安全解决方案的生态建设，提供从数据安全硬件到核心软件到人员培训等数据安全整体解决方案，全面覆盖用户身份管理、数据安全动态感知、零信任体系架构建设、数据分类及数据风险评估、员工培训等重要方面，系统性提升企业数据安全。**二是数据风险可视化、云数据安全等细分领域崛起。**随着数据规模扩大和新技术发展，国外数据安全产品内涵不断丰富，竞争日益激烈。相关企业不仅提供数据库安全防御、数据防泄漏、数据容灾备份及数据脱敏等传统数据安全产品，更关注云存储安全、数据风险动态评估、跨平台数据安全、数据安全虚拟防护等前瞻领域并推出针对性解决方案。**三是人工智能、大数据等新技术持续赋能数据安全。**伴随数字技术不断发展，人工智能、大数据、

云计算等新技术不断成熟落地，IBM 等国外头部厂商充分利用人工智能等技术在算法优化、数据处理、漏洞分析、响应速度等方面的优势，研发并推出了“人工智能+数据安全”等数据安全解决新方案，持续赋能数据安全产品在物联网、智能驾驶等复杂场景中的全面应用及快速迭代，以期更加高效和快速的响应、解决数据安全风险。目前国外主要数据安全产品基本情况可见表 1。

表 1 国外数据安全产品调研表

| 序号 | 企业/产品名称 | 数据安全产品 | 数据安全产品简介 | 企业网站 |
|---|---|---|---|---|
| 1 | IBM CLOUD SECURITY | ➢ IBM 云数据盾；<br>➢ IBM 密钥保护等； | 提供跨越数据存储、云计算服务等跨平台的数据保护服务，提供数据权限管理服务等。 | https://www.ibm.com/cloud/security |
| 2 | Amazon | ➢ 数据加密及秘钥管理；<br>➢ 威胁检测和持续监控；<br>➢ 身份识别和管理<br>➢ 关键数据存储管理 | 提供全面系统的云数据安全保护体系，包括数据分析自动化识别、数据安全标准构建、数据安全生态建设以及数据安全合规评估等。 | |
| 3 | CODE42 | ➢ 数据内部风险检测与响应 | 快速准确发现系统数据安全风险，并及时采取相应措施予以解决。 | https://www.code42.com/product/ |
| 4 | COMMVAULT | ➢ 数据风险监测；<br>➢ 数据合规管理；<br>➢ 敏感数据识别及管理；<br>➢ 数据备份与恢复<br>➢ 数据存储优化； | 通过数据管理和保护、数据安全、数据合规与治理、数据流转保护、数据分析等手段，利用统一的数据平台解决关键业务数据挑战，保障企业数据安全 | https://www.commvault.com/ |
| 5 | ORCA SECURITY | ➢ 漏洞管理；<br>➢ 恶意软件检测；<br>➢ 敏感数据检测；<br>➢ 身份和访问管理等 | 敏感数据检测 通过对敏感数据的风险，验证最重要的数据的安全性。 | https://www.orca.security |

| | | | | |
|---|---|---|---|---|
| 6 | REDWARE-CLOUD NATIVE PROTECTOR | ➢ 数据中心保护；<br>➢ 云恶意软件防护服务；<br>➢ 应用程序保护等 | 专注于云数据安全，提供云数据安全咨询、数据安全软件开发等服务。 | https://www.redware.comx |
| 7 | DATAFLEETS | ➢ 私有和分布式数据分析平台；<br>➢ 数据生命周期管理；<br>➢ 数据集成分析、个人信息去标识化管理等 | 为处理敏感数据团队提供全面的分析，实现灵活的用户身份识别和访问管理，保护企业重要数据安全 | https://www.datafleets.com/ |
| 8 | DELL EMC DATA PROTECTION | ➢ 数据备份；<br>➢ 电源设备保护；<br>➢ 数据管理器等 | 提供从归档到物理防护、虚拟防护和云防护的持续可用性，提供全方位的数据保护。 | https://www.delltechnologies.com |
| 9 | PRIVITAR | ➢ 数据去标识和数据匿名；<br>➢ 数据生命周期保护；<br>➢ 数据安全合并共享等 | 建立数据隐私平台-用于保护和治理的全面数据隐私管理解决方案；建立零信任平台，安全地共享数据并实施第三方协作。 | https://www.privitar.com/ |
| 10 | OKTA | ➢ 多重身份验证；<br>➢ 用户管理；<br>➢ 数据生命后期管理；<br>➢ API 访问管理等 | 利用快速的用户身份识别设定相应权限，对敏感信息的访问及处理设定更加严格的标准，采取充分的数据安全风险控制和审计手段，保障企业数据安全。 | https://www.okta.com/initiatives |
| 11 | symantec | ➢ 数据防丢失；<br>➢ 云安全访问；<br>➢ 数据加密；<br>➢ 数据合规评估等 | 对私有云和物理数据中心的数据进行持续监控，包括基础设施监控、权限监控及快速识别和评估违反规定的行为和可疑活动。 | https://securitycloud.symantec.com/cc/landing |
| 11 | DATADOME | ➢ 智能机器人保护；<br>➢ 无代码 SDK 集成 | 提供人工智能数据保护服务，定期筛查人工智能数据系统漏洞及风险，及时报警并处理。 | https://www.datadome.co |
| 12 | GRETEL | ➢ 数据合成；<br>➢ 数据去标识和数据匿名化；<br>➢ 数据目录等 | 创建具有差异隐私保证的合成数据扩充数据源、提高机器学习准确性，降低学习偏差，同 | https://www.gretel.ai |

| | | | | |
|---|---|---|---|---|
| | | | 时创建个人信息目录，通过目录管理保障数据安全。 | |

来源：中国信息通信研究院整理

### （三）产业投融资迎来大爆发

**国外受疫情长期蔓延、相关法规持续出台以及技术迭代等诸多因素影响，数据合规、数据容灾备份、数据防泄露、安全培训教育等产品或服务领域投融资活动持续活跃。**根据国外研究机构crunshbase统计数据显示，2019 年全球对隐私和安全公司的投资接近100 亿美元，是过去十年的历史新高，具体如图3 所示。2020 年受新冠肺炎疫情影响，相关数据虽然降至70 亿美元左右，但是近两年数据安全投融资规模总体仍比2010 年的17 亿美元增长了四到五倍[16]。2020 年国外数据安全领域企业投融资情况可见表2。具体来看，伴随GDPR、CCPA 等数据安全和个人信息保护法规影响力不断扩大，隐私保护和数据合规领域异军突起，拥有合规产品或服务的企业所获得的融资量占据总体的大多数。另外受疫情影响，网络在线活动频繁，数据规模持续扩大，由此带来的数据存储压力使得数据容灾备份、数据防泄露、身份识别管理等领域成为重点投资领域。

[16] 来源：https://news.crunchbase.com/news/almost-10b-invested-in-privacy-and-security-companies-in-2019/


来源：crushbase 信通院整理 单位：十亿美元

图 3 近十年国外数据安全企业投融资情况图

表 2 2020 年国外数据安全领域企业投融资情况表

| 类型 | 企业名称 | 融资方式 | 时间 | 金额 | 投资方 |
|---|---|---|---|---|---|
| 隐私保护和数据合规 | BigID | D 轮融资 | 2020.01 | 5000 万美元 | Clearsky 等 |
| | Cyral | B+轮融资 | 2020.01 | 1100 万美元 | RedpointVentures 等 |
| | VGS | 战略融资 | 2020.01 | 未披露 | Visa |
| | OneTrust | B 轮融资 | 2020.02 | 2.1 亿美元 | Insight Partners 等 |
| | Privitar | C 轮融资 | 2020.04 | 8000 万美元 | 荷兰银行等 |
| | CyberSmart | A 轮融资 | 2020.07 | 550 万英镑 | IQ Capital 等 |
| | DiviceLock | 并购 | 2020.07 | 未披露 | Acronis |
| | K2View | 融资 | 2020.08 | 2800 万美元 | Forestay Capital 等 |
| | Skyflow | A 轮融资 | 2020.12 | 1750 万美元 | Canvas Ventures 等 |
| | eXate | 种子轮 | 2020.12 | 230 万英镑 | Outward VC 等 |
| | OneTrust | C 轮融资 | 2020.12 | 3 亿美元 | TCV 等 |
| 数据库安全 | jSonar | 并购 | 2020.10 | 未披露 | Imperva |
| 容灾备份 | Veeam | 并购 | 2020.03 | 50 亿美元 | Insight Partners |
| | Actifio | 并购 | 2020.12 | 未披露 | Google |
| | Trilio | B 轮融资 | 2020.12 | 1200 万美元 | SKK Ventures 等 |
| 身份识别与管理 | Trusona | B 轮融资 | 2020.01 | 2000 万美元 | 微软等 |
| | AimBrain | 并购 | 2020.02 | 未披露 | BioCatch |
| | Youverify | 种子轮融资 | 2020.03 | 150 万美元 | OrangedigitalVentures 等 |
| | BioCatch | C 轮融资 | 2020.04 /2020.09 | 1.65 亿美元 | 花旗银行、贝恩资本等 |

| | | | | | |
|---|---|---|---|---|---|
| | ForgeRock | E 轮融资 | 2020.04 | 9350 万美元 | Riverwood Capital 等 |
| | Jetstack | 并购 | 2020.05 | 未披露 | Venafi |
| | Alloy | B 轮融资 | 2020.09 | 4000 万美元 | Canapi Ventures |
| | Symphonic | 并购 | 2020.11 | 未披露 | Ping Identity |
| | Beyond Identity | B 轮融资 | 2020.12 | 7500 万美元 | NEA 等 |
| 加密 | Enveil | A 轮融资 | 2020.02 | 1000 万美元 | C5 Capital、万事达卡 |
| | Ubiq | 种子轮融资 | 2020.11 | 640 万美元 | Okapi Venture Capita |

来源：虎符研究院

## 二、我国数据安全产业发展现状

### （一）数据安全产业顶层设计思路逐渐明晰

#### 1.国家统筹布局数据开发利用和大数据产业发展

**近年来，国家在数字经济发展、大数据行动计划等战略和顶层设计文件中，对数据安全产业做出了相应的工作部署，但尚未形成专门针对数据安全产业的国家顶层规划，我国数据安全产业发展政策有待进一步明确细化。**2015 年 8 月，国务院印发《促进大数据发展行动纲要》（简称行动纲要）。行动纲要旨在加快建设数据强国，释放数据红利、制度红利和创新红利，以“加快政府数据开放共享，推动资源整合，提升治理能力”和“推动产业创新发展，培育新兴业态，助力经济转型”为重要抓手，立足我国国情和现实需要，实现推动大数据发展和应用在未来 5 到 10 年逐步实现打造精准治理、多方协作的社会治理新模式；开启大众创业、万众创新的创新驱动新格局；培育高端智能、新兴繁荣的产业发展新生态等目标。同时，行动纲要提出国内力争在 2020 年，形成一批具有国际竞争力的大数

据处理、分析、可视化软件和硬件支撑平台等产品；培育 10 家国际领先的大数据核心龙头企业，500 家大数据应用、服务和产品制造企业等。

2020 年 4 月 9 日，中共中央、国务院公布了《关于构建更加完善的要素市场化配置体制机制的意见》（以下简称《意见》），明确提出“加快培育数据要素市场”，解决数据自由流动的体制机制障碍，深化数据要素价格改革，加快建立健全数据治理体系，充分发挥数据这一新型要素对其他要素效率的倍增作用，培育发展数据要素市场，推进政府数据开放共享，强化数据隐私保护和安全审查，推动设立数据分类分级制度，对释放数据红利、推动数字经济高质量发展具有十分重要的战略意义。

2021 年 3 月 11 日，全国人大表决通过《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》（简称十四五规划）。十四五规划说明要统筹数据开发利用、隐私保护和公共安全，加快建立数据资源产权、交易流通、跨境传输和安全保护等基础制度和标准规范。加快推进数据安全、个人信息保护等领域基础性立法，强化数据资源全生命周期安全保护。完善适用于大数据环境下的数据分类分级保护制度。加强数据安全评估，推动数据跨境安全有序流动。加快推动数字产业化，培育壮大人工智能、大数据、区块链、云计算、网络安全等新兴数字产业，提升通信设备、核心电子元器件、关键软件等产业水平。

2016 年 12 月，工业和信息化部发布《大数据产业发展规划

（2016-2020 年）》。规划明确坚持安全与发展并重，强化数据安全技术保障能力，建立健全数据安全技术防护体系，加强数据安全监督管理和行业自律，促进数据有序、规范流动。在数据挖掘、分析和应用算法等技术领域实现突破，满足国家战略重要应用需求。

2021 年 7 月 12 日，工业和信息化部发布《网络安全产业高质量发展三年行动计划 2021-2023（征求意见稿）》并向社会公开征求意见。行动计划要求要优化数据安全管理技术，提升数据识别、分类分级、质量管控等基础性技术产品准确性和智能水平。完善数据应用安全防护技术，推进数据脱敏、数据防泄漏、细颗粒度访问控制等技术产品升级，保障数据安全可控。突破数据共享安全保障技术，推动安全多方计算、联邦学习、同态加密、差分隐私等技术应用化部署和普及应用，促进数据要素安全有序流动。

2.数据安全法律法规相继出台

**随着《网络安全法》《数据安全法》《个人信息保护法》陆续出台，我国在数据安全和个人信息保护领域已形成较为完备的法律规范体系。**2016 年 11 月十二届全国人大常委会第二十四次会议正式通过《网络安全法》，并于 2017 年 6 月 1 日正式实施。该法要求建立网络安全等级保护制度，明确采取数据分类、重要数据备份和加密等措施防止数据泄露或被篡改。网络运营者应当在收集、使用个人信息时遵循合法正当必要原则，强调进行必要的个人信息匿名化处理和个人信息泄露报告等措施保障用户个人信息安全，规定任何组织和个人禁止非法获取、非法出售、非法提供个人信息。同时鼓

励开发网络数据安全保护和利用技术，促进公共数据资源开放，进一步推动技术创新和经济社会发展。

2021 年 6 月 10 日，全国人大常委会会议通过《数据安全法》，自 2021 年 9 月 1 日正式实施。该法第二章以专章篇幅梳理数据安全与发展关系，进一步明确数据安全与发展并行原则，提出支持数据开发利用和数据安全技术研究工作，鼓励数据开发利用和数据安全等领域的技术推广和商业创新，培育、发展数据开发利用和数据安全产品、产业体系等。并且，该法明确了国家层面建立数据分类分级，数据风险评估、数据安全应急处置和数据安全审查等制度，全面加强重要数据保护，降低数据安全风险。并且要求数据处理者建立健全全流程数据安全管理制度，组织开展数据安全教育培训，采取数据安全技术研发、数据安全风险检测、定期数据安全风险评估等措施，保障数据安全。

2021 年 8 月 20 日，全国人大常委会通过《个人信息保护法》，自 2021 年 11 月 1 日正式实施。该法将合法、正当、必要与最小必要、透明公开、安全保障作为个人信息活动基本原则，明确个人信息跨境处理要求，充分保障用户对个人信息处理的知情权和控制权，赋予用户删除、查询、更正、补充个人信息等权利，明确个人信息处理者应当遵循履行告知、个人信息分类、个人信息安全加密、敏感个人信息事前影响评估等义务，保障用户个人信息安全。该法兼顾个人信息保护与利用，通过法律规范建立权责明确、保护有效、利用规范的制度规则，在保障个人信息权益的基础上，促进数据依

法合理有效利用，推动数字经济持续健康稳定发展。

**可以看出，今年出台的两部法律在立法目的和原则当中都强调了统筹兼顾发展与安全的指导思想，对我国数字经济繁荣和数据安全产业发展都在法律层面提供了制度保障。**

3.区域性数据安全相关法规政策接连发布

**天津、贵州、深圳等省市加快建立完善数据安全管理制度，进一步细化落实数据安全管理要求，鼓励技术培育和人才建设，夯实数据安全产业发展基石。**2019 年 7 月 18 日，天津市网信办发布《天津市数据安全管理办法（暂行）》。办法坚持安全与发展并重、管理与技术兼顾的原则，针对不同类型数据运营者，对普适性、基础性、一般性数据安全保护方法和技术措施作出规定。此外，办法还对数据全生命周期管理、数据服务外包及信息通报与应急处置工作等都作出了明确规定。鼓励支持教育、科研机构和企业参与数据安全的国家标准、行业标准和地方标准的研究、制定。鼓励高等院校、科研机构和企业开展数据安全人才培养工作，实现数据安全人才培养、技术创新、产业发展的深度融合。

2019 年 8 月 1 日，贵州省发布《贵州省大数据安全保障条例》。条例明确单位应当设立数据安全责任人，负责数据全生命周期过程中安全问题的监督管理。梳理明确数据安全监管主体和对应职责，进一步落实数据安全风险评估、数据审查等手段。鼓励建立数据安全产业基地，要求县级以上政府设立数据安全专项基金对数据安全技术研发及成果转化应用、安全监测预警平台建设等给予支持。

2021 年 7 月 6 日，深圳市正式出台《深圳经济特区数据条例》。条例规定数据安全管理遵循政府监管、责任主体负责、积极防御、综合防范的原则，坚持安全和发展并重，鼓励研发数据安全技术，保障数据全生命周期安全。及时稳步推动构建数据收集、加工、共享、开放、交易、应用等数据要素市场体系，促进数据资源有序、高效流动与利用。鼓励充分开展数据价值评估和数据安全评估。鼓励建立数据交易平台，探索建立数据生产要素统计核算制度等，实现数据安全与发展协同共进。

## （二）数据安全产品及服务发展态势向好

数字经济飞速发展的同时，数据泄露、滥用事件层出不穷。近几年数据安全法律法规、监管政策不断出台，企业数据安全防护、监测、监管、隐私保护等需求逐步显现，推动数据安全产品和服务快速发展。2021 年上半年，我们对 50 多家数据安全企业、应用企业和科研机构开展了数据安全产品和服务现状调研，本报告以调研结果为基础，分析我国数据安全产品和服务发展现状。

### 1.数据安全产品体系逐步完善，总体处于快速发展期

目前，国内数据安全产品已经从单一的数据库加密、审计扩展到数据资产管理、安全防护、监测/检测、共享流通安全、隐私保护、追踪溯源等数据全生命周期的方方面面，随着企业数字化进程的推进，数据安全产品的应用场景越来越丰富，也推动了数据安全产品的快速迭代和发展。

（1）数据资产管理、分类分级、安全监测等产品形态未定型，产品命名和对应功能未形成共识

**数据资产管理、数据分类分级产品市场需求明显，但产品名称五花八门，产品功能各异，产品性能不尽如人意。**此类产品的核心技术是数据识别，包括数据库、服务器等系统中静态数据识别和传输流动中的动态数据识别。本次调研中有多家企业推出了类似产品，产品名称各不相同，同时产品功能差别明显。部分企业的“敏感数据发现系统”，在数据资产识别、分类分级、可视化等基础功能之上，增加了脱敏检测功能；而“敏感数据发现与风险评估系统”则增加了流量监控、审计等功能，“数据分类分级与风险评估系统”在基础功能之上又增加了数据库防护功能。**数据资产管理相关产品应用过程中，需要与业务有深度磨合，需要较多人工干预。例如，**分类分级产品在交付过程中，企业数据字典的建立、识别规则的建立和工具个性化配置等工作是产品在实际环境中真正发挥作用的关键环节，需要数据安全技术人员与业务人员共同完成，一般需要数月甚至更长的时间才能正常运转。数据安全监测预警相关产品也存在上述类似情况。

（2）数据库安全、数据脱敏、数据防泄漏产品进入成熟期

根据 2020 年数据安全技术成熟度曲线，数据库加密、数据库审计与防护、动态数据脱敏等技术已经进入成熟期。相应的，**数据库加密、数据库防护、数据库审计，动/静态数据脱敏，数据防泄漏（DLP）等安全产品也进入成熟期。各家产品的功能基本相似，应用场景明**

**确，应用行业广泛。**例如，数据库审计产品，已经在政府、能源、金融、教育、医疗等行业领域得到应用；数据脱敏产品已经应用于政府、金融、医疗、电力、运营商、互联网等多个行业领域。**随着数据库国产化进程的不断推进，适配多种数据库是此类产品未来的发展方向。**2020 年，国产数据库市场份额占 47.4%[17]，众多软件厂商、集成商、运营商等推出了自研数据库，且各种数据库的衍生、变种多种多样，数据库类安全产品在部署过程中必须要逐一匹配用户的数据库环境，才能真正发挥产品的作用，满足客户的业务需求。

（3）数据水印、数据溯源等产品处于萌芽期

根据本次调研情况来看，仅有 15%的企业推出了数据水印、溯源产品，相比之下，有 56%企业提供数据脱敏产品，由此可见，数据水印、溯源等产品仍处于研究探索阶段。并且，**数字水印技术在数据追踪溯源中的应用是新的研究领域，仍存在一些技术难题亟待解决。**对于结构化数据，目前实现方案是增加冗余数据，例如增加伪行或伪列。但冗余数据容易被识别或被清洗，使用效果不理想。对于非结构化数据，数字水印可以应用于数字图像、音频、视频、文本、条码等数据信息中，在数据外发的环节加上隐蔽水印，可以追踪数据扩散路径。但当前这类方案大多还是针对静态的数据集，满足数据量巨大、更新速度极快场景的水印方案尚不成熟。

（4）隐私计算产品商用化处于起步阶段，安全隐患不容小觑

**目前隐私计算产品的商业化应用主要集中于金融行业，其他行**

[17] 来源：艾瑞咨询，《2021 年中国数据库行业研究报告》

**业应用较少。**隐私计算产品在金融行业的应用集中在智能风控、智能营销、反洗钱等少数几个场景。在其他行业里，因为使用隐私计算成本过高，且企业对数据共享的监督能力较弱，隐私计算产品尚未得到广泛应用。**市面上多数隐私计算产品存在隐蔽性安全问题。**根据我们对市场上主流的20余款隐私计算产品的安全检测结果，80%的产品在算法与交换协议方面存在安全隐患，可能导致数据泄露，使得“数据可用不可见”成为空谈。而且这类问题多出现在产品技术设计底层，具有较高隐蔽性。

### 2.数据安全服务占比相对较低，总体趋势向好

数据安全与业务紧密关联，即要满足安全需求又要兼顾数据正常的应用与流转，数据安全服务是将安全专业技术与业务系统相融合，在不影响业务正常运营的前提下，满足企业数据安全合规、防护、监测等需求的主要途径。**目前国内市场上的数据安全服务主要涵盖数据安全合规评估、数据安全规划咨询、数据安全治理（分类分级）三大类，数据安全托管、数据安全运维、数据安全测评、数据安全防护能力评定等服务开展较少。**本报告统计了部分安全厂商数据安全服务在总销售额中的占比，如表 8 所示，大概为 20%左右，占比水平较低。其原因主要有两方面：**一方面，数据安全服务应用方对数据安全服务的认识不准确，**认为通过传统网络安全的防护系统，即“硬件设备+专用软件”的模式就可以解决数据安全的问题，对软性的数据安全服务认可度不高。**另一方面，目前数据安全服务缺乏标准化的规范指导，**尚未建立成熟的服务评价体系，企业在选

择过程中缺乏参考指导。与网络安全服务相比，数据安全服务刚刚起步，业务模式不成熟，积累比较少，市场整体来说处于开拓阶段，需要逐步培育。但数据安全服务的市场总体向好，受调研企业中，2019 年到 2020 年销售额增长率大部分在 50%左右，增长势头迅猛。数据安全厂商安全服务情况具体见表 3。

表 3 部分数据安全厂商安全服务情况统计表

| 序号 | 企业名称 | 数据安全服务类型 | 产品和服务营收占比 |
|---|---|---|---|
| 1 | 华途信息 | 数据安全咨询、数据安全检测、数据安全产品、整体解决方案 | 7:3 |
| 2 | 炼石科技 | 数据安全咨询与解决方案，产品交付与定制开发 | 8:2 |
| 3 | 数安行 | 主要依托自研产品为企业或者第三方评估机构提供咨询或评估服务，目前以私有化模式为主，未来会提供 SaaS 模式 | 9.5:0.5 |
| 4 | 上海观安 | 数据安全合规评估、数据安全治理服务 | 平台：产品：服务=6:3:1 |
| 5 | 珠海高凌 | 在数据分层治理阶段提供租户权限服务，在数据共享开放阶段提供 API 服务 | 8.5:1.5 |
| 6 | 中安星云 | 数据安全风险评估服务、数据安全培训服务、应急响应服务、安全巡检服务、数据安全体系架构建设等数据治理服务 | 7:3 |
| 7 | 博瑞得 | 数据安全资产梳理、数据安全策略规划、数据安全治理 | 7.5:2.5 |
| 8 | 信安世纪 | 数据加密安全，数据传输安全，和数据来源认证安全等技术服务支持 | 6:4 |
| 9 | 全知科技 | 数据安全管理体系规划、数据安全风险评估、数据安全评测服务，数据出境评估、数据分级分类 | 7:3 |
| 10 | 思维世纪 | 数据资产和分类分级咨询、数据安全合规评估、数据安全法律法规对标、数据安全检测、数据安全管理咨询、数据安全培训宣贯等 | 4:6 |

| | | | |
|---|---|---|---|
| 11 | 安华金和 | 数据安全治理服务 | 9.5:0.5 |
| 12 | 绿盟科技 | 数据分类分级、规划类的（例如：按照数据安全成熟度模型）、数据安全管理体系建设、数据安全评估、个人信息安全影响评估、数据安全培训 | 7:3 |
| 13 | 亚信安全 | 咨询规划、数据分类分级、数据安全治理 | 8:2 |
| 14 | 深信服 | 数据安全治理服务、数据资产梳理、数据分类分级、数据风险评估、数据安全管理制度咨询、数据安全能力评估、数据安全应急处置、数据安全培训宣贯 | 7:3 |
| 15 | 山石网科 | 数据安全评估 | 9.5:0.5 |
| 16 | 杭州美创 | 数据安全治理、数据安全咨询、数据安全风险评估、数据安全运维、数据安全意识培训 | 7.2:1.8 |
| 17 | 恒安嘉新 | 数据安全治理 | 7.5:2.5 |
| 18 | 世平信息 | 数据安全规划咨询、数据安全治理、数据安全评估、数据安全运维、数据安全审计 | 8.5:1.5 |

来源：中国信息通信研究院

## （三）国内数据安全企业迎来高速发展机遇

根据中国信息通信研究院发布的《中国网络安全产业白皮书（2020）》以及部分机构对我国数据安全产业规模的测算，2020 年我国网络安全产业规模约为 1702 亿元，同年数据安全产业规模约为 50 亿元左右[18]，不到网络安全产业规模的百分之三。**但过去三年我国数据安全产业发展增速明显。**根据计世资讯[19]的数据统计，2018 年到 2020 年我国数据安全产业同比增速分别为 29.6%、32.7%、33.2%，

[18] 数据来源：计世资讯预测 2020 年我国数据安全市场规模为 52.5 亿元，头豹研究院预测 2020 年我国数据安全市场规模为 46.2 亿元

[19] 来源：http://www.ccwresearch.com.cn/

呈逐年快速上升趋势。**数据安全产业强劲的发展态势带动数据安全企业的发展进入快车道。**


来源：计世资讯

图 4 国内数据安全产业增长曲线图

**一方面，企业数据安全产品服务收入呈现爆发式增长态势。**根据奇安信、中孚信息、天融信等国内相关上市企业披露的 2021 年企业半年财报显示，2021 年上半年，国内安全企业数据安全收入呈现大幅度增长态势。其中，奇安信上半年数据安全产品收入同比增长超 100%，大数据安全与隐私保护、零信任数据安全增长率均超 60%，电子数据取证收入增长超 300%，以终端安全、边界安全、数据安全、实战型态势感知为核心的新赛道产品营收占主营产品收入比例超 70%，同比增长近 60%。天融信 2021 年半年报披露，企业 2021 年上半年数据安全产品在研发、渠道方面持续发力，收入同比增长 46%左右。

**另一方面，企业全力支持数据安全技术研发，力图进一步扩大**

**产品服务优势。**技术研发投入方面，企业注重数据安全技术研发投入。根据对闪捷信息、全知科技、美创科技等 8 家企业调研访谈显示，2020 年上述企业平均研发投入经费 2839.7 万元，占 8 家企业全年平均营业收入的 28%，根据中国信息通信研究院发布的《中国网络安全产业白皮书（2020 年）》，科创板上市的 5 家网络安全企业，2019 年企业平均研发投入 2.99 亿元，占企业全年平均营业收入的比例也是 28%，数据安全企业研发投入与科创板上市的安全企业投入持平。

### （四）数据安全产业生态环境持续优化

#### 1.数据安全标准体系逐步健全完善

**一方面，数据安全国家标准相继出台，有力支撑相关法律法规的落地实施。**2016 年，全国信息安全标准化技术委员会（SAC/TC260，简称“信安标委”）成立大数据安全标准化特别工作组，正式启动了数据安全相关国家标准研制工作。目前，TC260 已发布数据安全和个人信息保护标准 9 项，在研标准 22 项。**已发布标准涉及大数据服务安全、政务信息共享、个人信息安全等多个重要标准化方向。**《GB/T 35274-2017 大数据服务安全能力要求》《GB/T 37932-2019 数据交易服务安全要求》《GB/T 37973-2019 大数据安全管理指南》《GB/T 39788-2019 数据安全能力成熟度模型》《GB/T 39477-2020 政务信息共享 数据安全技术要求》和《GB/T 39725-2020 健康医疗数据安全指南》，针对大数据服务安全管理基本要求、数据生命周期保护措施、数据安全能力的成熟

度模型架构、政务信息共享技术实施方案和医疗数据安全管理提出了具体技术规范要求。《GB/T 37964-2019 个人信息去标识化指南》《GB/T 35273-2020 个人信息安全规范》以及《GB/T 39335-2020 个人信息安全影响评估指南》，分别对个人信息去标识化的目标、原则和手段措施，个人信息收集处理活动应当遵循的规则，个人信息安全影响评估原理和实施流程提出了规范要求。**重点领域在研标准项目广受各方关注。**《数据出境安全评估指南》《网络数据处理安全要求》《人脸识别数据安全要求》《个人信息告知同意指南》《移动互联网应用程序（App）SDK 安全指南》等国家标准在研项目，因与数据安全法律法规政策落实紧密联系，产业界各方主体的参与积极性和主动性颇高，相关标准化研制工作正在加紧推进。

**另一方面，各行业数据安全标准陆续发布，有效指导行业数据安全实践工作。**电信和互联网领域，2020 年 12 月，工业和信息化部正式印发《电信和互联网行业数据安全标准体系建设指南》，该指南通过标准体系的顶层设计，制定政府引导和市场驱动相结合的数据安全标准体系建设方案，加强标准制定工作的统筹协调，对已出台数据安全相关法律法规的管理要求进行补充和细化，促进标准在保障数据安全、推动行业健康有序发展中的引领和支撑作用。在此基础上，《YD/T 3813-2020 基础电信企业数据分类分级方法》《YD/T 3867-2021 基础电信企业重要数据识别指南》《电信网和互联网数据安全评估规范》等重要标准陆续发布，分别针对电信企业数据分类分级原则和具体实施步骤、重要数据识别原则和注意事

项以及电信和互联网企业数据安全评估范围、模式和流程等进行指导，进一步细化行业数据安全管理工作，落实数据安全管理要求，基本满足行业数据安全保护需要。

工业领域，《YD/T 3865-2021 工业互联网数据安全保护要求》《YD/T 3751-2020 车联网信息服务 数据安全技术要求》《T/CCSA 278-2019 工业互联网平台 制造企业数据质量治理技术要求》等已发布标准分别对制造企业数据质量治理的目标和技术框架、工业互联网数据安全保护的范围及数据类型、工业互联网数据重要性分级与安全保护等级划分方法、数据质量治理的顶层设计、数据质量治理环境、数据质量治理域等提出了具体要求。

金融领域,《金融数据安全 数据生命周期安全规范》(JR/T 0223—2021）《金融数据安全 数据安全分级指南》（JR/T 0197—2020）《个人金融信息保护技术规范》(JR/T 0171—2020)等数据安全和个人信息保护标准持续发布，规定了金融数据收集、存储、共享等生命周期管理方式和注意事项以及金融数据分级的目标、原则和范围等，明确了个人金融信息全生命周期保护原则和措施，给予企业更加明确充分的数据安全和个人信息保护指导。

### 2.数据安全行业自律活动百花齐放

**一是产业多方力量聚集，数据安全专业组织或平台相继成立，在标准研制、技术创新、治理规则、人才培养等方面持续发力。**2020年7月10日，中国信息通信研究院、中国电信、中国移动、中国联通等40余家企业共同成立《中国互联网协会数据治理工作委员会》，

该委员会将持续促进成员单位完善数据管理、数据质量控制、数据价值挖掘、数据流通和数据隐私安全等相关工作。2021 年 7 月，中国网络安全产业联盟和中国计算机行业协会相继成立了数据安全工作委员会，均致力于促进数据安全产业持续健康发展。此外，2021 年 2 月，中国信息通信研究院正式启动“卓信大数据计划”。该计划作为数据安全领域政、产、学、研、法交流平台，主要致力于打造业内权威的数据安全治理的全要素解决方案，从构建数据安全基础设施、完善数据安全保障体系、探索数据安全应用创新三个方面出发，通过安全测试、安全认证、人员培训等服务为企业数据安全保驾护航。**二是数据安全和个人信息保护论坛、研讨会吸引各方关注，成为思想交流、碰撞的主舞台。**中国互联网协会连续两年成功举办中国互联网大会数据安全分论坛。2021 年 7 月，第二十届中国互联网大会数据安全分论坛上来自工业和信息化部网络安全管理局、中国信息通信研究院、阿里巴巴、北京师范大学的领导及专家学者纷纷针对国内数据安全典型问题发表观点意见，建议从提高政治站位、加强顶层设计、强化技术创新，鼓励产业发展等方面提高我国数据安全整体水平。今年 9 月 26 日，2021 年世界互联网大会网络数据治理论坛在乌镇举行，论坛以“数据治理与个人信息保护”为主题，相关部门领导、国内外数据领域知名专家学者以及产业界共话数据治理，探讨数据安全与发展、数据治理与个人信息保护问题。**三是校企合作设立数据安全联合研发项目，研究讨论数据安全典型前沿问题。**上海观安、安恒、奇安信、天融信及全知科技等数

据安全企业与复旦大学、北京理工大学、上海交通大学、南开大学、天津大学等高等院校、国家工业信息安全发展研究中心等相关单位联合开展数据安全领域技术研究，有效整合双方优势资源，培育数据安全技术人才，推动人工智能、量子安全通信等典型前沿技术在数据安全领域的深度应用，引领我国新一代数据安全技术发展。

### 3.数据安全国际交流合作进入新阶段

**一是加强自由贸易区建设，探索数字经济发展新路径。**2019 年，国务院印发《中国（上海）自由贸易试验区临港新片区总体方案》，方案提及拟在临港自贸区试点开展数据跨境管理的各项举措，包括开展数据跨境流动的安全评估，以及建立数据保护能力认证、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，力图在促进全球跨境数据流动方面发挥积极作用。2020 年 9 月，国务院印发《中国(北京)自由贸易试验区总体方案》，方案将创新数字经济发展环境，提升数字贸易国际竞争力作为主要目标。方案要求对标国际先进水平，探索符合国情的数字贸易发展规则，加强跨境数据保护规制合作，促进数字证书和电子签名的国际互认。探索制定信息技术安全、数据隐私保护、跨境数据流动等重点领域规则。探索创制数据确权、数据资产、数据服务等交易标准及数据交易流通的定价、结算、质量认证等服务体系，规范交易行为，全方位多角度的探索数字经济发展新路径，进一步提升我国数字经济发展水平。**二是积极构建参与区域合作体系，协同共促数字经济发展。**2020 年 11 月 15 日，东盟十国、中国、日本、韩国、澳大利亚及新西

兰共 15 个国家共同签署《区域全面经济伙伴关系协定》（RCEP），RCEP 要求缔约方之间加强合作交流，共同促进数字贸易的发展[20]。该协定限制成员国政府利用数据本地化存储等手段对数字贸易施加限制，鼓励在保障公共利益以及采取合理措施保护个人信息安全的情况下促进数据跨境流通。该协定对电子认证和电子签名、垃圾邮件处理等领域也进行了规范，鼓励相关行业进一步发展。2021 年 9 月，我国宣布正式申请加入《全面与进步跨太平洋伙伴关系协定》(CPTPP)， CPTTP 对数据跨境流动进行了原则性规定,即除为“正当公共政策之目的”外,应允许为数据主体利益而进行的数据跨境传输，进一步释放数据价值。**三是强化全球数据安全治理，贡献中国方案。**2020 年 9 月我国发布《全球数据安全倡议》，倡议呼吁各国秉持发展和安全并重的原则，平衡处理技术进步、经济发展与保护国家安全和社会公共利益的关系，寻求各方一起共同加强数据安全、个人隐私和国家安全的协调发展，促使各国更加重视网络安全和数据安全建设，推动全球数字经济产业的发展与合作。2021 年 3 月 29 日,我国与阿盟成员国共同发布《中阿数据安全合作倡议》，该倡议支持秉持多边主义、兼顾安全发展、坚守公平正义的原则，共同应对数据安全风险挑战，推动在多边主义基础上共建和平、安全、开放、合作的网络空间，树立了发展中国家参与全球治理的范例，为世界各国在全球数字治理领域寻求最大公约数贡献了智慧和力量。

[20]:https://kns.cnki.net/KXReader/Detail?TIMESTAMP=637679022590380425&DBCODE=CJFD&TABLEName=CJFDLAST2021&FileName=ZGLT202108003&RESULT=1&SIGN=Qd3H5mOcDFLiyJ4q0%2b8jo%2bXieEg%3d

## 三、我国数据安全产业发展的驱动力

### （一）数据安全重视程度持续提升

数据规模迅猛增长，对经济发展、社会治理、人民生活产生了重大而深刻的影响，数据安全已成为事关国家安全与经济社会发展的重大问题。习近平总书记多次作出重要指示批示，提出加快法规制度建设、切实保障国家数据安全等明确要求。党的十九大报告提出加强关键信息基础设施网络安全防护，增强网络安全防御能力和威慑能力，加强网络安全预警监测，切实保障国家数据安全。推动实施国家大数据战略，加快完善数字基础设施，推进数据资源整合和开放共享，保障数据安全。十九届中央政治局第二次集体学习明确要切实保障国家数据安全，强化国家关键数据资源保护能力，增强数据安全预警和溯源能力。要加强政策、监管、法律的统筹协调，加快法规制度建设。此外，《数据安全法》《个人信息保护法》等法律陆续出台，建立了权责明确、协调统一的数据保护规则体系，明确了数据安全和个人信息保护的基本制度，完善了数据开发利用规则，对提升我国数据安全治理和数据开发利用水平，促进数字经济发展提供了坚实的法律保障。中央领导人批示以及国家顶层设计屡次提及数据安全，凸显了数据安全的重要性，提升了社会各界对数据安全和个人信息保护重视程度，成为数据安全产业发展快速发展的重要前提。

### （二）数据泄露成本上涨推升企业数据安全需求

由数据泄露引发的企业成本损失近年来不断增长，企业采购成

**熟数据安全产品和服务的紧迫性和必要性逐渐提高。**2021 年 8 月，IBM 发布《2021 年数据泄露成本报告》。根据该报告，2020 年至 2021 年，企业数据泄露事件成本平均已经达到 424 万美元，同比增长 10%。数据泄露事件导致的最大损失是业务损失，平均为 159 万美元，占比为 38%。并且，统计数据显示，近年来企业数据泄露事件成本不断增加，增长幅度也呈现明显上升趋势，具体可见图 5。


图 5 近年数据泄露成本趋势图

为应对高涨的数据泄露事件成本、降低数据安全泄露事件发生的频率、控制影响程度，65%左右的企业开始采购数据安全风险检测、风险事件及时响应工具、风险自动化处理系统等数据安全产品和服务，庞大的采购需求为相关产品和服务的发展带来了新的机遇。

### （三）监管行动扩大数据安全合规需求

**行业主管部门密集开展数据安全和个人信息保护专项工作，安全测评、人员培训、能力认证等安全合规需求进一步增加。**自 2019 年 1 月，中央网信办、工业和信息化部、公安部、国家市场监管总局四部门在全国范围组织开展 App 违法违规收集使用个人信息专项

治理活动，对 App 运营者收集使用用户信息行为进行监督管理，严格查处违法违规收集使用个人信息行为。2020 年治理活动持续深入，重点关注针对面部特征等生物特征信息收集使用不规范，App 后台自启动、关联启动、私自调用权限上传个人信息，录音、拍照等敏感权限滥用等问题。截止目前，工作组已针对 2300 余款 App 开展深度评估、问题核查，对用户规模大、问题突出的 260 款 App，有关部门采取了公开曝光、约谈、下架等处罚措施。同时，自 2019 年 11 月以来，工业和信息化部组织开展“App 侵犯用户权益专项整治行动”等一系列 App 个人信息保护监管工作。2021 年全年，工业和信息化部已累计通报 10 批 1494 款侵害用户权益行为的 App，累计下架 205 款 App。**上述对 App 个人信息保护的强有力监管，促使相关技术检测、人员培训等安全服务市场活跃度明显上升。可以预见，随着《数据安全法》深入落地实施，数据安全产品和服务的需求也将不断释放。**

### （四）产业数字化步伐加快推动数据安全产业发展

**国内企业面临“数字化”转型机遇，对数据资产管理、分类分级、安全监测等数据安全产品和服务提出更高要求。**我国经济结构调整和产业升级面临生产要素成本上升、人口老龄化及资源环境制约的挑战，加之新冠肺炎疫情发展进一步影响传统企业生产，企业“数字化”转型已经成为解决发展瓶颈的重要突破口。2019 年，国务院国有资产监督管理委员会印发了《关于加快推进国有企业数字化转型工作的通知》，就推动国有企业数字化转型做出全面部署。

国有企业的数字化转型，需要依托数据要素，在开发和利用数据的过程中，必然需要专业化的数据资产管理、数据安全监测、安全存储、风险评估、隐私计算等数据安全产品和服务作为支撑和保障。相较于国有企业，中小企业更需要通过数字化网络化智能化实现复工复产，增添发展后劲。在数据安全保障能力建设方面，采购、租赁云化部署的数据安全一站式产品或服务，更符合中小企业的实际情况。

### （五）新兴领域技术迭代引领数据安全产业成长

**人工智能等新兴技术快速演进、交叉融合，“技术—产业”迭代交互效应持续增强[21]，正在深刻影响数据安全产业发展。**当前人工智能、云计算、车联网、工业互联网、5G、物联网、区块链等新领域新业态快速发展，多元算力将成为未来的主要生产力，人工智能、5G 等新兴技术将替代传统信息技术和产品，传统数据安全思维与数据安全手段面临着全新的转变。以人工智能为例，人工智能领域数据安全技术的应用环境已经从传统的 APP、接口等深入到算法层面，该领域面临的数据安全风险不仅囊括了数据泄露、数据破坏等传统风险，还包括了数据投毒等新型数据安全风险。这种变化促使数据安全企业需要紧跟业务发展趋势，结合区块链、云计算等新兴技术特点及优势，优化数据去标识、数据匿名等传统数据安全手段，加快差分隐私、同态加密、秘密分享、不经意传输等数据安全保护新技术落地速度，升级创新数据安全产品、服务，进一步带动数据安

[21] :https://m.thepaper.cn/baijiahao_13615812

全产业发展。

# 第三部分　未来展望

## 一、数据安全成为战略布局重点

伴随疫情常态化发展，全球数据规模爆发式增长，线上交易、电子商务、远程医疗、在线娱乐等数字经济新模式和新业态蓬勃发展，数据价值日益凸显。**一方面，全球数据安全博弈加速白热化，数据安全成为影响国家竞争力的关键因素。**近年来，数据安全逐渐演化成为一个跨领域、跨专业的综合性议题，数据治理能力成为国家竞争力的重要体现。数据基础设施建设、数据存储、数据跨境流动和新兴技术安全等问题成为各方关注焦点，科技力量千帆竞发勇进者胜。**另一方面，新冠肺炎疫情已进入常态化防控阶段，稳定和促进经济发展成为各国政府下一步工作重心，这为数据安全产业发展带来了千载难逢的机遇。**在此背景下，我国也需要抓紧窗口期，落实《数据安全法》关于数据安全产业的工作布局要求，分析国外数据安全产业发展趋势，全局统筹谋划数据安全产业发展方向，加快数据安全先进技术研发落地，构建数据安全产业发展新格局。

## 二、数据安全保护规则体系进一步细化

伴随《数据安全法》《个人信息保护法》相继出台，我国数据安全和个人信息保护规范体系框架已经基本形成。**数据分类分级、数据安全评估等制度将进一步细化，配套的数据安全规范和标准体**

**系也将进一步完善。**未来，我国将出台细则落实数据安全审查、数据安全监测、数据交易等制度，进一步细化数据分类分级、重要数据目录、数据风险评估、数据出境等重点工作的相关规范要求，进一步明确国家核心数据、重要数据保护手段。**个人信息出境安全评估、安全认证、个人信息侵权案件公益诉讼等重要制度也将逐步落实，成为个人信息保护的有力抓手。**下一步，企业层面也需要建立健全个人信息合规体系，落实敏感个人信息保护、个人信息影响评估、合规审计等法定保护义务，重点对自动化决策、未成年人个人信息保护、个人信息主体的权利实现等方面加强企业内部管理制度机制建设。

## 三、数据安全企业将迎来快速发展机遇

**数据安全市场规模不断扩大，未来 3 到 5 年内将保持继续高速增长态势。**随着我国社会数字化转型步伐加速，数据规模持续扩大，金融、医疗、交通等重要市场以及智能汽车、智能家居等新兴领域数据安全投入持续增加，稳定增长的市场需求将吸引越来越多的传统安全企业以及新兴安全企业推出数据安全相关产品和服务，抢占市场份额，引领行业发展。**数据安全产品将向专业化、体系化方向不断迈进，为专业型企业发展带来新机遇。**数据安全产品和服务垂直细化的趋势愈加明显，促使数据安全企业的产品结构愈加周密，专业程度愈来愈高，企业与企业之间、行业与行业之间的独立性越来越强，专业化聚焦基础上的“差异化共存”成为商业主流，以“需求定制”为驱动的专业型产品供给时代正在到来，专业型数据安全

企业将迎来创新发展新机遇。

## 四、数据安全技术将不断突破创新

**基础通用技术的不断发展为数据安全技术创新提供了有力支撑。**在国家对技术创新支持力度不断提升的大背景下，产业链各环节相关主体将持续加大在人工智能、区块链、密态计算等基础通用技术方面的研发投入，为数据识别、数字水印、隐私计算等数据安全关键技术的能力提升和创新发展提供有力支撑。**应用领域的逐步拓展将推动数据安全技术的持续演进。**数据要素市场化背景下，联邦学习、密文检索、多方安全计算等处于萌芽期的新兴技术，为解决数据利用与数据保护之间的矛盾提供了新的解决方案，应用需求旺盛。随着应用领域的不断扩展和需求的不断释放以及理论研究的不断深入，这类技术在运算效率、互联互通、安全性等方面的问题将逐步得到改进，实现核心技术的持续演进。

## 五、数据安全产业生态将稳步推进

**一是数据安全产业扶持政策的制定出台将提上日程。**《数据安全法》中明确提出要“培育、发展数据开发利用和数据安全产品、产业体系”，可以预见，相关部门将制定出台专门的数据安全产业发展政策，为我国数据安全产业发展创造良好发展环境。**二是数据安全标准体系将进一步健全完善。**为增加标准有效供给，支撑和引领数字经济高质量发展，可以预见，国家和各行业相关标准化组织将加快重要数据的识别与保护、数据安全风险评估与监测预警、重

要数据和个人信息出境安全评估等领域数据安全标准研制工作，进一步完善数据开发利用技术和数据安全标准体系建设。**三是行业自律活动稳步推进。**随着数据安全专业组织和平台不断发展壮大，相关组织将在技术发展、人才培养、能力认证等方面持续发力，整合技术优势和资源优势，以行业自律的形式形成并推广高质量的数据安全产品和服务最佳实践，促进数据安全政策、技术、人才多要素良性互动。**四是数据安全人才培养将受到进一步重视。**为解决当前数据安全人才缺口的问题，政府部门、科研机构、高等院校、企业等各方主体必然将加强人才培养力度，发挥政策、技术和资源等优势，充分采取多方联合培养、建立数据安全实训基地等手段，发掘培育全方位、多层次的复合型数据安全优秀人才，夯实数据安全人才队伍建设。

中国信息通信研究院 安全研究所

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-62308070

传真：010-62300264

网址：www.caict.ac.cn