EY安永
Building a better working world

SICSI
CYBER RESEARCH INSTITUTE
赛博研究院

全球数据合规与隐私科技发展报告

2022

Global Data Compliance and Privacy Technology Development

版权声明

COPYRIGHT STATEMENT

出品方

安永（中国）企业咨询有限公司

上海赛博网络安全产业创新研究院

编写组成员

高轶峰　安永（中国）企业咨询有限公司大中华区网络安全和隐私保护服务主管合伙人

惠志斌　上海赛博网络安全产业创新研究院院长，首席研究员

王瑾　　安永（中国）企业咨询有限公司网络安全和隐私保护咨询服务高级经理

周雪静　上海赛博网络安全产业创新研究院高级研究员

蒋采玲　安永（中国）企业咨询有限公司网络安全和隐私保护咨询服务经理

王龙飞　上海数据安全协同创新实验室秘书长

吴梦庭　安永（中国）企业咨询有限公司网络安全和隐私保护咨询服务顾问

李顾元　某公司隐私合规专家

孙思瑄　某公司隐私合规专家

2022 年是中国数据合规全面发展的一年，也是隐私科技进一步从概念走向落地的一年。回顾近一年的发展，安永与赛博研究院联合发布第二期年度《全球数据合规与隐私科技发展报告》。本报告全面梳理了国内外数据安全与算法应用的合规体系，对隐私科技的概念、内涵和外延进行更新，并通过对近百家头部企业的问卷调研，覆盖金融、科技、媒体与通信、消费品、生命科学、制造业等行业，客观了解企业数据合规的现状与隐私科技的需求，最后为国内外企业数据合规实践提供参考案例与创新思路，供业内参考。

主要发现

- 全球近 100 个国家和地区已制定数据保护相关法律，数据安全、算法应用有关立法进程加快，合规本地化的全球性趋势将进一步加强。

- 全球数据合规领域执法力度加强，截至 11 月 30 日，GDPR 执法总数 1216 起，罚款总额超 20 亿欧元。企业面临合规人员招聘、安全产品及服务采购等合规成本与监管罚款等不合规支出的双重压力。

- 企业更加重视数据合规与隐私保护，完善数据合规与隐私保护职能和管理体系，提升数据合规与隐私保护汇报层级，加大数据合规与隐私保护的人员和资金投入。22% 的企业直接向高级管理层汇报工作，82% 的企业认为在过去 12 个月的投入满足需求。

- 更多企业发现隐私计算的价值并付诸实践，隐私计算在更多风险控制和数据流通等业务场景中发挥着重要作用，并在元宇宙、工业互联网与区块链等新兴科技中崭露头角。在未来十二个月，更多企业选择保持对隐私科技的投入水平，力图稳中求进。

- 从隐私科技产业发展来看，数据分类分级、数据流通监控、数据风险与隐私影响评估、数据与隐私综合治理是当前的热门细分赛道。后续围绕提高数据的匿名化程度，增强算法可解释性，加强落实伦理先行原则，将进一步赋能隐私科技的合规能力。

CONTENTS | 目录

P-A-R-T 01

数据经济时代的安全与隐私挑战

PART 1

数据经济时代的安全与隐私挑战

当前，大数据正在迅速改变全球的经济面貌。在数字经济的发展过程中，企业和个人持续依赖大数据与不断更迭的数字技术，驱动数据处理活动、探索数据创新。然而，繁荣背后隐藏风险，数据的价值吸引内外部的恶意攻击与频繁掠夺，数据的流通引发个人隐私担忧与合规警惕。从漏洞攻击到数据窃取，从经济损失到合规成本，从系统安全到隐私保护，以安全与隐私为主题的风险正成为影响数字经济发展的关键因子。对此，企业正在积极采取措施，运用“数据 + 算法”、“隐私 + 合规”等技术与服务手段，制定应对安全与隐私挑战的安全战略与整体解决方案。

1.1 “隐私科技”概念界定

在 2021 年发布的《2021 全球数据合规与隐私科技发展报告》中，我们将隐私科技定义为：用于支撑隐私保护与合规的日常运营流程，且嵌入到 IT 架构和业务场景中的一系列技术解决方案，在保证个人信息全生命周期的增强保护和个人信息处理活动规范化的基础上，实现保护个人信息权益、提升数据流通、共享与开放、促进个人信息合理开发利用的目的。

图 1 隐私科技概念图示（2022 版）

今年，基于对国内隐私科技厂商的普遍性研究，《全球数据合规与隐私科技发展报告（2022）》对隐私科技框架进行了更新与完善，主要体现在①凸显应用场景的重要性，强调隐私科技在数据处理全生命周期中的应用，以及在金融、医疗、政务等重点行业的实践趋势；②对隐私科技解决方案与底层支撑技术进行梳理与更新。现将隐私科技定义更新为：**在日常运营流程中，通过嵌入 IT 架构和业务场景支撑主体数据合规和隐私保护的一系列工具、服务及技术解决方案。**通过将隐私科技应用于个人信息全生命周期或各行业个人信息处理场景中，在增强保护个人信息、规范个人信息处理活动的基础上，实现保护个人信息权益，推动数据流通、共享与开放，促进个人信息合理开发利用的目的。

1.2 全球数据合规与隐私保护挑战

数字世界里，合规与隐私保护作为反复出现的话题，也是企业在经营、上市、融资、发展过程中的“必经之路”。当前企业为满足数据合规与隐私保护需要，面临诸多挑战，包括满足来自监管的迫切要求，应对围绕数据处理全生命周期的外部攻击与内生安全风险。

（1）遵守不断发展变化的法律法规

随着与数据相关的法律体系的不断完善，企业面临的首要挑战是来自国际监管环境的变化。首先是适应全球不断发展变化的法律法规，包括遵守已经生效、即将生效的数据合规要求——涵盖当地数据合规与个人信息隐私保护、跨境数据传输安全合规要求等。由于法律法规要求众多且持续更迭，企业及其内部合规团队不得不面临合规制度不完善、合规要求更新不及时、合规措施落实困难等现实挑战。

其次是适应“当地”法律法规，由于各国在数据安全方面的立法存在标准不一、条款冲突的情形，因此跨国企业需重点关注业务经营所在国家的法律合规要求，加强监测预警，规避和降低跨国经营合规风险。在不损害国家安全、公民个人信息安全的前提下，以“安全合规本土化”为原则，提升企业境外市场的综合竞争力。

（2）高昂合规成本带来的经济压力

鉴于全球监管格局的不断变化，企业为了适应日益严格的监管与处罚，面临更大的经济压力。**一是表现在不合规成本支出上，**即支付因违规带来的高额罚款。截至 2022 年 11 月 30 日，《通用数据保护条例》（简称“GDPR”）执法总数 1216 起（相较去年 9 月 30 日的统计数据，增加 322 起），GDPR 罚款总额超 20 亿欧元（增加约 7 亿欧元），最高的一笔罚款暂时还未刷新，仍为 2021 年针对某国际电商巨头开出的 7.46 亿欧元罚款。不仅 GDPR 的执法强度大、频次高，其他国家的监管处罚也不容小觑。以我国为例，伴随执法常态化发展，监管措施涵盖公开通报、应用下架、罚款到实施网络安全审查、过渡性指导措施等多种手段。监管处罚对象不仅包括企业，还覆盖到高管及相关责任人，处罚方式主要体现为警告与罚款。譬如 2022 年 7 月，国家互联网信息办公室对某出行平台处人民币 80.26 亿元人民币罚款，对公司董事长、总裁各处人民币 100 万元人民币罚款。**二是表现在企业在数据合规与隐私保护工作上投入更多预算。**企业通过技术、工具和组织架构的调整提升整体合规能力，具体包括组建

数据安全团队，设置 CDO（首席数据官）制度，配备专职隐私保护人员及合规法务人员，应用隐私计算等技术，采购第三方合规风险评估服务等。其中，在人才需求方面，由于国内法律法规对于开展相关业务的企业提出数据安全管理相关要求，《个人信息保护法》更是明确指出处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人。然而，囿于当前数据合规与隐私保护的专业人员仍然存在较大的市场缺口，导致部分企业仍然因为缺乏人才，无法满足实际的数据合规和隐私保护工作需求。

整体来看，数据安全预算的增加一定程度上给企业带来了额外的成本，尤其是对于初创企业或中小企业来说。然而，根据《2022 全球隐私基准报告》研究显示，数据监管不合规的成本是合规成本的 2.71 倍，因此仍有 42% 的公司打算在隐私计划上花费超过 100 万美元，采取更多措施促进隐私保护。此外，根据 IBV 发布的《网络经济中的繁荣》研究显示，网络安全成熟度最高的组织在五年内的收入增长率比最不成熟的组织高出 43% ，数据安全在一定程度上也可以被视为企业经济和价值增长的措施。因此承担合规成本对于企业长期发展而言是必要的。

（3）复杂的第三方风险管理挑战

企业不仅面临自身的内外部安全威胁，还需要做好第三方风险管理。第三方数据处理者因供应链攻击或数据安全合规能力不足而产生的风险，正在对企业造成直接影响。**从供应链角度来看，**第三方数据处理者包括了企业直接合作的公司，如材料供应商、分包商、网络托管公司、安全产品提供商、数据服务提供商等可以访问企业系统或数据的第三方主体。由于供应链攻击是网络空间攻防对抗的焦点之一，即便企业自身安全建设成熟度高，攻击者也能利用供应链上下游企业的任一脆弱环节实现入侵。伴随供应链攻击的往往还有企业核心数据、重要数据泄露，让企业防不胜防。**从数据处理关系来看，**企业的数据源包括内部自主收集以及与第三方产生的数据共享、委托处理、转让，后者既有企业与企业之间的数据共享，也有企业和政府之间的数据共享。在数据传输、存储、处理过程中，第三方的网络安全防护能力以及数据安全保障能力，也是企业需要重点评估的方面。当前，大多数企业都需要重新审视第三方风险管理，尤其在网络安全、数据合规、隐私保护方面。

（4）数据频繁流通引发的安全威胁

伴随数字化转型，数据的价值与日俱增，数据的流通性也成为创新发展的必然要求。在此基础上，企业采用 AI 技术、自动化工具、混合云部署等多种手段，加快数据从本地向云上，从内网向外网，从境内向境外流通。借助数据流通，推动因开展业务需要而收集与产生的数据的共享与开发利用，进而为市场创造新的价值。与此同时，政府机构也与企业一起，推动发挥数据要素生产力，构建功能齐全的数据要素市场。

然而，在数据流通利用过程中，也存在诸多风险隐患。部分企业由于安全管控措施不足、数据可信流通能力建设滞后，导致企业的风险暴露面增加。例如面临联网系统、云上资产等遭受攻击所引发的数据泄露；企业与第三方机构合作共享数据时，数据因明文流通或复制滥用而导致大量隐私泄露；企业因跨境业务需要等原因启动数据出境工作，可能因涉及重要数据，或一定规模的（敏感）个人信息外传，直接危及国家安全、企业合规与个人信息安全。综上，面对复杂的数据流通场景，企业亟须探索基于隐私保护的数据流通解决方案，在安全合规的前提下，促进数据在企业内外部的流通以及拓展数据开发利用的深度和广度。

P-A-R-T 02

全球数据安全立法及监管现状

PART 2

全球数据安全立法及监管现状

目前全球已有近 100 个国家和地区制定了数据安全保护相关法律，数据安全保护专项立法成为国际惯例。Gartner 预测，到 2024 年，全球 75% 的人口将在其个人数据方面受到隐私法规的保护。以中国、美国、欧洲各国为例，中美欧持续围绕数据安全、算法安全立法及监管进行探索与实践。

2.1 数据安全立法现状与动向

各国持续将数据安全立法作为工作重点，逐步推进实施有关法律法规。**值得关注的是，随着数据作为生产要素的价值愈发凸显，数据立法不仅针对个人信息保护，而是已经广泛地涵盖公共数据开发利用、企业数据共享流通、个人数据保护（包括个人信息及个人隐私数据）等多场景。**

在数据安全与个人信息保护方面，以欧洲、美国、中国为代表的区域 / 国家在 2022 年以前已经形成了较为清晰、具备特色的法律体系与框架。**（1）欧盟以 2018 年生效的《通用数据保护条例》（简称“GDPR”）为核心，构筑统一的数据安全治理框架：**GDPR 与《非个人数据自由流动条例》构成数据安全领域的关键立法体系；《电子隐私条例》作为 GDPR 在电子通信领域起细化和补充作用的特别法，两者在监管规则上保持一定的一致性；《电子证据条例》侧重科技企业向政府部门提供数据协助，同时保障数据安全；《为保持欧盟个人数据保护级别而采用的数据跨境转移工具补充措施》为数据跨境流动中的数据保护问题提供进一步指导。**（2）美国立法体系分为联邦立法和州立法，呈现多级多行业监管特征。**1974 年，美国实施的《隐私法案》对政府机构应当如何收集个人信息、收集到的个人信息如何向公众开放及信息主体的权利等做出了详细规定。此后，美国采取分行业的分散立法模式，在金融、健康、教育、消费等行业领域制定数据保护规范。同时，美国多个州在其原有的个人信息保护法律基础上作出修订，进一步扩展“个人信息”定义，补充数据安全法律法规细节。仅 2021 年，美国 38 个州就出台了 160 多项与消费者隐私相关的法案 。值得注意的是，美国还通过数据安全立法为其执法机构的域外数据管辖提供依据。2018 年正式签署的《澄清境外数据的合法使用法案》意味着，美国执法机构在认为可能存在危害美国国家安全的情况下，可以要求跨国企业将存储在他国境内服务器中的与调查事件或者案件相关数据传输至美国执法机构。这意味着执法数据跨境获取需求日益增加的背景下，美国的执法效力将扩展至全球，同时出海企业需要进一步研判多国数据安全法律法规，规划部署数据

存储地，减少合规冲突。整体来看，美国的数据安全立法错综复杂，但仍缺乏统筹性的数据安全法案。**（3）我国基于《网络安全法》《数据安全法》与《个人信息保护法》，开展综合性立法。**目前，我国的这三部法律分别适用于境内所有网络运营者的包含处理个人信息及数据在内的行为、所有主体处理网络数据和非网络数据的行为、个人信息保护行为。在行政法规、部门规章、地方性法规及标准文件方面，我国也已逐步形成体系，广泛适用不同的行业及数据使用场景。

2022 年以来，全球数据安全相关立法进程再次提速，一方面通过推动数据流通、共享、开发利用充分释放数据红利，另一方面通过分行业分场景分企业推动重点监管。

一是在隐私保护立法与规范方面，一方面基于原有的数据安全立法基础，美国、英国等国家正在把握机会，在个人信息保护、消费者隐私等细分方向提出具有统筹性、影响力的专项立法。美国参议院和众议院于 6 月 3 日发布了《美国数据隐私和保护法》草案。多级多行业监管之下，缺乏一个统一、全面的联邦数据隐私保护法律一直以来是美国所面临的一大问题。作为第一个获得两党两院支持的美国联邦全面隐私提案，《美国数据隐私和保护法》意味着在美国在制定全面数据隐私框架上的努力。虽然《美国数据隐私和保护法》仍有待商榷，但 2020 年 11 月通过的《加州隐私权利法案》（CPRA）将于不久后（2023 年 1 月 1 日）生效，同年 7 月 1 日执行，也意味着美国在隐私保护问题上的强监管趋势，新法案势必对企业施加更为严格的隐私保护义务，并增强消费者权利。与此同时，脱欧后的英国也在推动《数据保护和数字信息法案》，试图对数据保护框架进行更新并取代英国 GDPR。另一方面，从合规认证的角度推动隐私保护规则完善，欧盟委员会今年推出首个获批的欧盟通用数据保护条例（GDPR）认证体系——Europrivacy（欧洲隐私）。作为第一个符合 GDPR 规定的官方认证机制，Europrivacy 用于评估、记录、认证和评价企业的合规情况。基于评价、认证规则，企业将进一步加强合规评估，减少不合规的个人数据处理行动，同时还可以依赖 Europrivacy 评估企业跨境数据传输的充分性。

二是在数据出境安全问题上，以《个人信息出境安全评估办法（征求意见稿）》《信息安全技术数据出境安全评估指南（征求意见稿）》为基础，我国先后于 6 月 30 日、7 月 7 日、8 月 31 日出台《个人信息出境标准合同规定（征求意见稿）》和《数据出境安全评估办法》《数据出境安全评估申报指南（第一版）》，明确了数据出境安全评估的流程和要求，为促进数据依法有序流动提供关键指导。目前数据出境合规路径主要分为三条，包括数据出境安全评估、专业机构个人信息保护认证、签署标准合同。此外，各国之间也在频繁开展关于数据出境方面的磋商，如部分国家达成数据跨境协议、一些国际组织成员国已经联合签署与数据安全有关的贸易协定。

以美欧为例，自“隐私盾”失效后，今年 3 月，美欧就新的“跨大西洋数据隐私框架”达成原则性协议，新框架标志着美国方面做出了前所未有的承诺——根据“跨大西洋数据隐私框架”，美国将制定新的保障措施，以确保信号情报监视活动在追求确定的国家安全目标方面是必要的和相称的，并且承诺建立一个有约束力的两级独立补救机制，加强对信号情报活动的严格分层监督。此后，美国又于 10 月发布

了一项加强美国信号情报活动的行政命令，旨在促进欧盟和美国之间未来的数据传输。虽然美欧在数据隐私保护方面仍然存在分歧，并且缺乏一个可行的法律结构来兑现美国对于隐私保护的承诺，但通过数据跨境国际协议、协定构建数据流通仍然是应对数据出境安全问题的一个重要思路。

三是在公共数据共享利用方面，包括我国在内的多个国家都在积极探索公共数据的共享、开发利用，试图激发公共数据的潜在价值，为市场化运作、创新研究等提供数据支撑。在释放公共数据红利的同时，各国政府也在加快公共数据有关法律条例文件的制定与出台，守好安全底线，做好重要数据、商业秘密与个人信息保护。今年，在《欧洲数据战略》指导下，欧洲《数据治理法案》正式公布并将于 2023 年陆续实施。该法案将在数据共享、开发利用问题上，进一步平衡公共数据的流通使用与安全合规问题，增加欧洲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。

四是在个人与企业数据共享方面，共享范围、权限分配、隐私保护等都是亟待解决的问题。目前欧洲在数据共享方面开展了更多的探索。欧盟委员会于 2 月 23 日公布《数据法案》草案全文，重点聚焦企业之间以及企业与政府之间的数据共享。其中，重点推进消费者和企业对其拥有的数据拥有更多的控制权，自主决定如何使用数据。5 月 3 日，首个欧洲健康数据空间正式启动，促进针对个人健康数据的访问与流通。通过充分利用健康数据，为诊断治疗、科研创新等决定提供数据支持，增强欧盟公民对其个人健康数据的控制权。据了解，继欧洲健康数据空间之后，欧洲下一个政策目标将放在交通领域，并计划于 2023 年上半年推出交通公共数据空间 。

欧洲促进个人与企业数据共享的方式主要分为 3 种，包括企业依法为个人提供其使用相应产品或服务所产生的数据；个人出于个人需要（如为获取第三方服务）可主动选择与第三方进行数据共享；依托数据中介机构（数据经纪人、数据利他主义组织等）生态开展数据交易共享。不论是依循上述哪种思路，均需确保数据在共享过程中的可信、安全。为此，有关数据安全责任界定与安全保障有关的法律制度也在探讨之中。2022 年，除了欧盟《数据法案》，《数字市场法》《数字服务法》的立法进程也显著加快。6 月 15 日，大西洋另一边的美国则提出了《健康和位置数据保护法案》，提出禁止数据经纪人出售位置和健康数据等敏感信息。该提案对交易共享的数据类型进行了限制，试图平衡个人与数据中介之间的利益关系。总体来看，在个人信息尤其是个人敏感信息的共享流通机制上，通过立法手段管控市场主体之间的数据交易、加强政府引导，构建公平、

2.2 算法应用合规现状与趋势

当前的个人信息保护法律进路在于通过赋权模式，为自然人赋予个人信息主体权利，这就导致在大多数个人信息应用场景下，征求个人信息主体的授权同意成为唯一的合法性基础，由此为企业主体带来了一系列的合规义务，包括知情同意、最小必要、公开透明等。而算法作为数据生产力转化的重要引擎，也同时引起监管重视，从全球范围来看，算法的监管模式还不成熟，但是普适性算法监管制度供给不断涌现。

2021 年 4 月，欧盟委员会公布了《关于“欧洲议会和理事会条例：制定人工智能的统一规则（人工智能法案）并修订某些联盟立法”的提案》，确立了算法应用主体和政府在算法应用过程中应遵循的底线原则，并界定了基于风险等级的算法应用场景。2022 年，欧盟《数字服务法案》《数据治理法案》和《数字市场法案》对互联网数据应用规则进行全面改革，加强构建平台型企业的算法责任体系。为促进数据再利用，《数据治理法案》欲将建立数据中介服务机制，并强调数据的利他主义，为欧盟单一数字市场奠定基本的数据使用管理规则，平衡企业数据利用和公民个人数据保护之间的利益诉求。

类似地，为解决算法自动化决策所引起的社会公众不满问题，美国一直以来也高度关注算法监管问题，2017 年 12 月签署通过了美国立法史上第一个对公用事业领域算法进行问责的法案，即《算法问责法案》；2019—2022 年，美国立法者相继提出并持续更新《算法责任法案》，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方式。其中《2019 年算法问责法案》强制要求相关实体针对高风险自动化决策系统进行数据保护影响评估，提高数据应用的透明性和规则的可解释性。

我国近年来也愈加重视算法监管，2021 年 9 月，国家互联网信息办公室等部门联合印发《关于加强互联网信息服务算法综合治理的指导意见》，提出算法安全监管体系，规定了算法备案、算法监督检查、算法风险监测、算法安全评估等四项举措。其中，算法备案是算法安全监管的抓手和基石；算法监督检查和算法风险监测相辅相成、互为补充，检查是现场监测，监测是线上检查；算法安全评估是出口，是算法安全监管的落脚点。

2.3 监管路径与发展趋势

聚焦数据、算法层面的立法现状与监管动向，各国明显加快数据保护及算法治理相关工作，优化法律基础，构建强监管环境。

第一，大型跨国科技公司成为重点监管对象。一方面，大型跨国科技公司基于业务需要所收集、存储与处理的数据，在数据量和数据重要程度上一般会高于普通公司，具有更高的数据价值与潜在风险。例如，近年来国内外的大型跨国科技公司侵犯个人隐私、滥用数据、数据泄露等问题层出不穷，使得更加严格的监管势在必行；另一方面，数据安全不仅要以监管机构为主导，还需要社会、企业、群众等主体共同发挥作用，而大型跨国科技公司具备一定的社会影响力，由其开展的最佳实践或倡议行动都有助于建设更好的数据安全环境。因此，将

跨国互联网巨头作为数据保护监管的重点对象，不仅有利于海量数据保护，而且在执法层面也更具有示范和预警效果。

第二，数据出境活动成为重点监管情形。数据本地化趋势在全球范围内尤其是发展中国家愈发凸显。关键信息基础设施的运营者、大型跨国企业或开展海外业务的企业需要重点关注围绕“跨境数据传输”“数据本地化存储”“数据隐私保护”的当地法律规定。目前跨境数据流动治理及监管暂未形成全球性规制体系，但包含中国在内的部分国家已经出台相应法律法规。以我国 9 月 1 日起施行的《数据出境安全评估办法》为例，明确了数据出境的具体流程。一是事前评估，数据处理者在向境外提供数据前，应首先开展数据出境风险自评估。二是申报评估，符合申报数据出境安全评估情形的，数据处理者应通过所在地省级网信部门向国家网信部门申报数据出境安全评估。三是开展评估，由国家网信部门收到申报材料之日进行评估。围绕数据出境的监管，重点在于出境这一活动是否对国家安全、公共利益、个人或者组织合法权益带来风险。

第三，安全审查成为关键领域数据安全强监管的重要举措。网络安全审查一般是针对关系国家安全和社会稳定的信息系统中所使用的信息技术产品与服务开展审查与监督。当前美国、中国等多个国家已设置审查制度，并且随着安全态势变化，审查范围也在进一步拓展。以美国为例，其网络安全审查涵盖外国投资、关键基础设施保护、供应链安全管理等。目前，全球网络安全审查更聚焦于关键领域及信息科技行业。值得注意的是，国家将安全审查作为重要监管手段之一，以实现数据安全这一最终目的，但考虑到不同国家的网络安全审查制度和体系可能存在法条竞合或法条冲突，需要企业进行预先自审自查。

第四，合规性评估与安全检查成为数据安全日常监督的举措。在日常监管工作中，除了网信办、工信部、各地通管局等部门围绕违法违规收集使用个人信息等情形定期对 App 开展技术检测，开展通报、批评、下架处理等执法活动。数据安全检查专项活动也取得了阶段性成效，成为主要监管举措。2022 年，浙江省、广东省、北京市、上海市等多省市已经开展电信和互联网行业或车联网行业的网络与数据安全检查工作，重点聚焦企业的数据安全保护落实情况、个人信息和用户权益保护工作情况。数据安全合规评估作为检查的一部分，对于企业自查自改具有全面指导意义，同时既可以作为数据安全符合性成果报告，也可以作为直接向监管部门提供的企业履行数据安全合规评估工作的证明。

第五，算法监管的未来趋势将从个人信息保护基本原则出发不断提高其数据的可溯源性和规则的可解释性。从各国的算法监管思路来看，个人信息保护要求下的个人信息处理规则公开透明和个人信息自主决定权与算法黑箱模式形成冲突，虽然技术中立，但是算法的设计和数据的筛选都掺杂的人为因素，如果没有中立的第三方进行算法治理和监管，容易导致算法歧视和舆论引导，对部分群体的权益造成影响。其中，数据的可溯源性，指数据的来源无瑕疵，对于个人信息的处理，需要取得个人信息主体的授权，这就要求，算法的数据提供方需要在数据收集时充分告知个人信息主体关于数据收集的种类和应用目的，如果需要向第三方共享，还必须向其告知共享的第三方主体基本信息。根据我国《个人信息保护法》对个人信息的定义，将匿名化后的

信息排除在外，这为隐私计算的发展提供了发展窗口，即通过“数据可用不可见”的方式实现数据的流通和利用将成为算法合规路径之一。

规则的可解释性同样映射出个人信息主体权利的要求，由于法律对个人信息人格性权益的认可，个人信息主体参与到数据的权益配置链路中，算法的使用主体应当承担相应的披露义务，明确告知公众关于算法使用的基本逻辑，接受公众的监督，保障个人信息主体对算法使用的知情权。

附：数据合规监管处罚典型案例（2022 年）

时间	案例简介	适用法律	风险点
1 月 10 日	某银行因违反信用信息采集、提供、查询及相关管理规定，被中国人民银行上海分行罚款 1674 万元人民币	《个人信息保护法》《征信业务管理办法》	不正当采集、使用用户的个人信息
3 月 10 日	意大利的数据保护机构宣布对一面部识别公司违反欧盟法律的行为处以 2000 万欧元罚款。该公司从互联网上搜集自拍，积累了约 100 亿张脸的数据库，积累了约 100 亿张脸的数据库，为其出售给执法部门的身份匹配服务提供数据支持	《通用数据保护条例》（GDPR）	非法处理用户的个人数据
5 月 25 日	某社交平台因不当使用用户数据，达成 1.5 亿美元庭外协议。除罚款外，该平台还必须接受对其数据隐私计划的审计以及其他限制	美国《联邦贸易委员会法》	未经用户同意使用个人信息；未明示收集、使用个人信息的目的、方式和范围
7 月 21 日	因存在 16 项违法事实，国家互联网信息办公室对某出行平台处人民币 80.26 亿元人民币罚款，对公司董事长、总裁各处人民币 100 万元人民币罚款	《网络安全法》《数据安全法》《个人信息保护法》	过度收集个人信息、个人敏感信息；超范围获取用户权限，未告知用户个人信息处理目的等；存在严重影响国家安全的数据处理活动
7 月 26 日	某公司对于日常经营活动采集到的驾校学员个人信息未采取去标识化和加密措施，系统存在未授权访问漏洞等严重数据安全隐患。广州警方依法处以警告并处罚款人民币 5 万元人民币的行政处罚	《数据安全法》	未建立数据安全管理制度和操作规程
8 月 24 日	某著名化妆品品牌就其侵犯消费者隐私一事达成和解协议，决定支付 120 万美元的罚款，并在隐私政策中披露其向第三方出售消费者个人信息的事实，为消费者提供个人信息出售的退出机制	美国《加州消费者隐私法案》	出售、非法提供消费者个人信息

时间	案例简介	适用法律	风险点
9 月 5 日	因涉嫌不当处理青少年相关数据（如青少年用户的账户状态被默认设置为“公开”；平台收集青少年用户的电话号码或电子邮件地址数据），某社交平台将被爱尔兰数据保护委员会（DPC）处以 4.05 亿欧元（约合 4.02 亿美元）罚款	《通用数据保护条例》（GDPR）	不当处理未成年人数据
9 月 14 日	韩国个人信息保护委员会（PIPC）对两大公司合计处以 1000 亿韩元（约合 7190 万美元）的罚款，这是该委员会对个性化广告数据收集的首次处罚，也是有史以来韩国因涉嫌违反个人信息保护法而被处以的最高罚款金额	韩国《个人信息保护法》	未经用户同意收集个人信息；不正当使用用户个人信息用于个性化在线广告和其他目的
9 月 26 日	某社交平台可能在没有适当的父母同意的情况下处理了英国 13 岁以下儿童的数据。该公司还涉嫌没有以简洁、透明和容易理解的方式向其用户提供适当的信息，并在没有法律依据的情况下处理特殊类别的数据。英国信息专员办公室（ICO）将对其罚款 2700 万英镑	英国《数据保护法案》	未经监护人同意处理未成年人信息；不正当处理个人敏感信息
10 月 13 日	某科技公司在处理政务类数据时违规操作，导致数据存在泄露风险。上海网信办对该公司责令改正，给予警告，并处以人民币五万元罚款的行政处罚	《数据安全法》	违规操作且未采取相应的技术措施和其他必要措施保障数据安全，导致数据存在泄露风险
10 月 20 日	某跨境电商平台在英国面临 8.89 亿英镑的诉讼，被控其滥用主导地位，操纵算法偏袒自身产品	英国《垄断法》	算法垄断

2.4 从算法监管看隐私科技的破局思路

在算法监管规则日渐明晰的背景下，隐私科技的市场需求与日俱增，但是市场应用还难以推广。除了因为技术本身不成熟、缺乏可靠的技术标准以及多方数据融合处理需求不明晰等技术和应用层面的原因外。更重要的原因在于，在当前个人信息保护规则下，个人信息的概念外延不断扩大，法律除保护可用于直接识别自然人的信息外，算法应用中被加工的数据也受到同等法律保护，这类数据被称

为与个人信息主体相关联的信息。无形中增加了数据应用的合规难度和算法的透明度要求。

隐私计算作为隐私科技中的核心技术能力体现，为了实现在安全的前提下促进数据的可持续流通，其破局思路具体要从法律规则层面进行先行引导和规划：

（1）提高数据的匿名化程度

我国《个人信息保护法》中将匿名化定义为“个人信息经过处理无法识别特定自然人且不能复原的过程”，并将匿名化处理后的信息排除在个人信息之外，这为算法类应用的发展提供了合规思路，即通过隐私计算实现数据的匿名化处理效果，在匿名化的前提下实现数据的“可用不可见”。但是随着大数据技术的发展和数据的泛在化，完全做到匿名化可能是个伪命题，典型的例子是搜索记录的重新识别，美国在线网站曾经公布 2000 多万条匿名化处理的用户搜索记录，有研究人员通过把其中多条记录联合分析后，很容易就识别出特定个人的姓名和身份。在当前法律和行业标准尚未界定匿名化实现方式和验证标准的前提下，隐私科技技术需要对匿名化数据的重识别行为做出约束，通过规则设计避免算法运行过程中的中间态数据被重新识别到特定个人。

（2）增强算法规则可解释性

数据作为新型生产要素，打破了“一物一权”式的传统物权体系下的主客体对应关系，这就导致算法的开发方和利用方需要向个人信息主体披露数据处理的逻辑，以达到合规的要求。隐私科技技术在实现匿名化信息处理的前提下无疑也增加了算法可解释性的难度。例如在多方安全计算中，由于数据供给方互相并不知道对方的数据特征和群体特征，用于算法训练的数据仅限于中间态计算结果，数据黑箱导致算法计算最终结果的可解释性变差，因此，即便是“心怀善意”的技术提供方，也会因为数据的不完全透明导致数据的虚假乃至错误应用。隐私科技如何实现算法的可解释性，降低算法偏差将成为合规必须攻破的难题。

（3）遵循应用伦理先行原则

由于算法与决策直接相关，从本质上来讲，算法是客观规律的数学表达和理性预测，但是算法的运算逻辑和数据输入都是由人来完成的。在隐私科技加持下的算法虽然一定程度提高了数据匿名化的程度，但是增加多个数据处理环节和应用主体，包括数据提供方、技术提供方和数据应用方，其中数据提供方可能涉及跨行业多个主体，这多方主体彼此之间难以对算法开发过程中的信息做到完全披露和理解，信息的不对称同样也会影响技术的中立性，从而导致计算偏差和算法歧视，算法不仅会将代码中固有的决策保存下来，还会在预测过程中不断固化歧视而创造出新的现实。因此隐私科技的推广必不可缺少中立第三方对数据源、算法模型的伦理审查，通过降低信息不对称性和融入社会学分析，加强算法的伦理审查，以促进隐私科技的向善发展。

P-A-R-T 03

企业隐私保护及隐私科技应用现状调研

PART 3

企业隐私保护及隐私科技应用现状调研

在数字化时代，数据合规与隐私保护一直是企业关注的一大重点，企业开展数据合规与隐私保护工作不仅是为了遵守全球不断发展变化的法律法规要求，也是为了增强客户体验。在这两大目标驱动下，不少企业将数据合规和隐私保护视作企业的生命线。在《数据安全法》和《个人信息保护法》施行一年有余，本报告再次发起调研，了解和分析企业数据合规与隐私保护现状和趋势，包括数据合规与隐私保护人员、组织、流程和技术等方面。

本次调研涉及百家余家头部企业，覆盖金融、科技、媒体与通信、消费品、生命科学、制造业等行业。

3.1 企业数据合规与隐私保护概况

1. 数据合规与隐私保护职能所属部门呈多元化

今年有更多的被调查企业（98%）具备了数据合规和隐私保护职能，而去年该数值为 89%。《数据安全法》第四章明确了企业应遵循的数据安全保护义务，《个人信息保护法》第五章规定了企业作为个人信息处理着的义务，基于此越来越多企业在内部设立数据合规与隐私保护职能，推动企业内部履行合规义务。

信息安全部门、法务部门和合规部门仍然是数据合规与隐私保护工作的主要责任部门。调查结果显示，48% 的被调查企业信息安全部门需要担任部分数据合规与隐私保护职能，39% 的被调查企业合规部门和 38% 的被调查企业法务部门也需要担任部分职能。企业在考虑将数据合规与隐私保护职能安置到哪个部门时，可结合自身业务和组织架构进行设定，以更加符合和适应企业的需求。考虑到数据合规与隐私保护工作的复杂性和学科交互性，48% 的被调查企业数据合规与隐私保护工作由多部门共同负责。

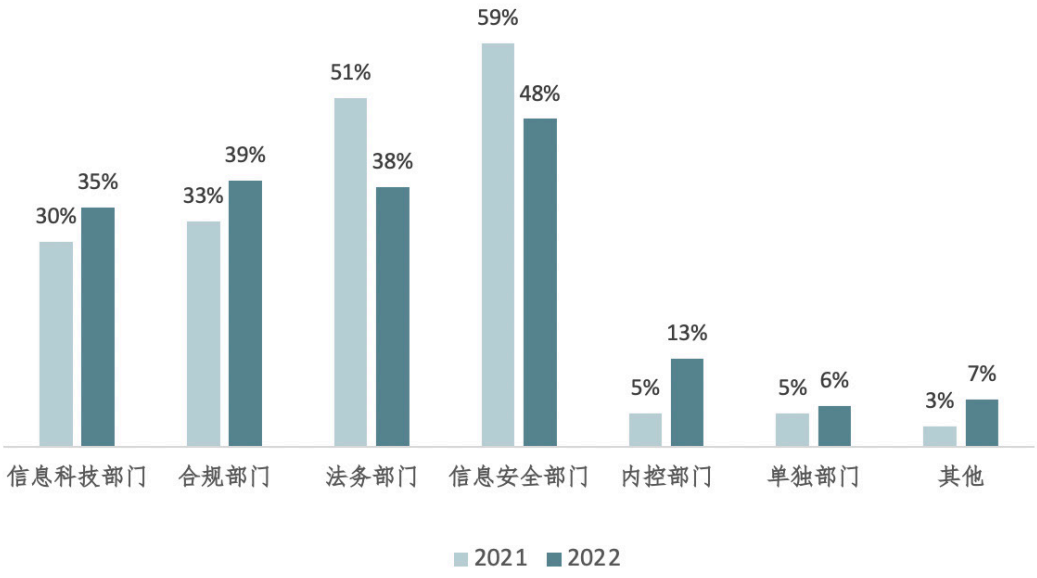

图 2 企业数据合规与隐私保护职能所属部门

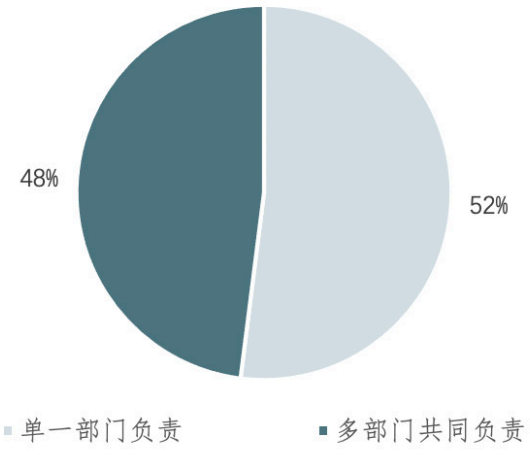

图 3 企业数据合规与隐私保护职能模式

与去年相比，信息安全部门和法务部门的占比有所下降，而合规部门、信息科技部门和内控部门等占比轻微上升。这些转变的出现可能是因为数据合规与隐私保护的多学科性。除了常见的安全风险和法律合规风险，一些企业信息科技部门担任部分数据合规与隐私保护职能，可能是为了将数据合规与隐私保护工作左移，在产品设计初期就考虑数据合规与隐私保护，并且通过信息科技部门实施更多的隐私科技以支持内部数据合规与隐私保护工作；一些企业内控部门担任部分数据合规与隐私保护职能，可能是为了在企业内部形成数据合规与隐私保护的第三道防线，检查企业内部设置了数据合规与隐私保护控制并运行有效。

2. 数据合规与隐私保护工作直接汇报层级越来越高

- 首席信息官 /IT 总监仍然是当前数据合规与隐私保护工作的主要汇报对象，其次是企业高级管理层。根据调查统计，29% 的被调查企业的数据合规与隐私保护工作是向首席信息官 /IT 总监进行汇报，与去年相比有轻微的下降趋势。

- 22% 的被调查企业数据合规与隐私保护职能直接向企业高级管理层（董事会或企业法人）汇报，而去年仅有 9% 的企业直接汇报到高级管理层，是去年的两倍有余。这些变化说明，随着《个人信息保护法》和《数据安全法》施行以及监管部门的一系列执法行动，越来越多企业将数据合规与隐私保护工作视为企业高级管理层应重点关注的事项。个保法第六十六条明确“严重违法行为可处五千万元人民币以下或者上一年度营业额百分之五以下罚款，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”，违法违规事项不仅可能影响企业经营，也会影响消费者对企业的信任。

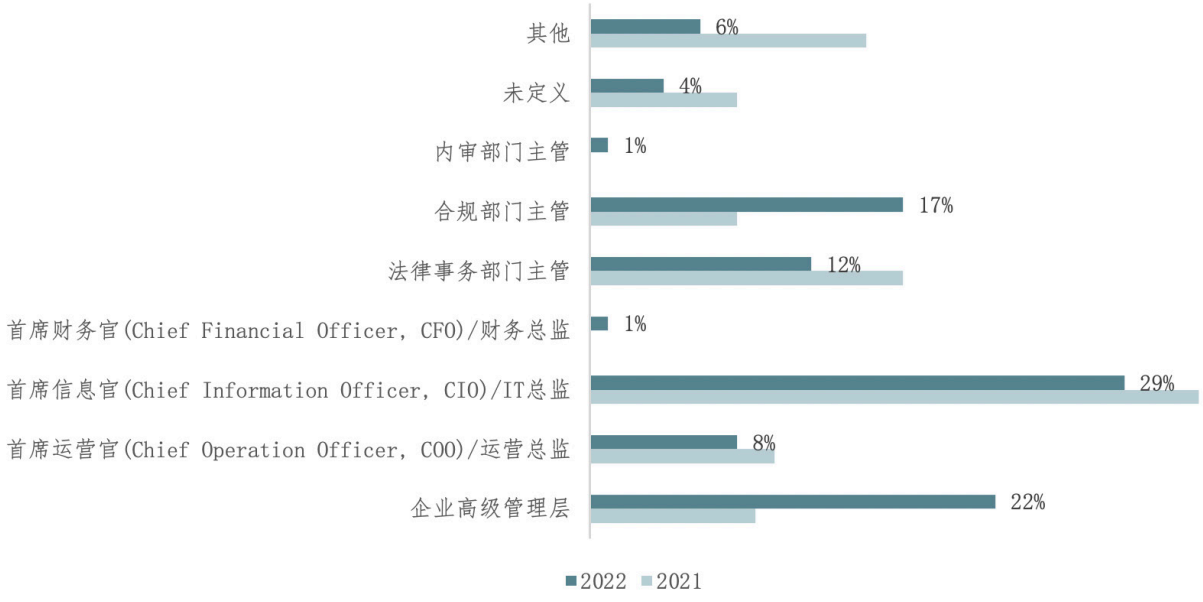

图 4 企业数据合规与隐私保护职能直接汇报工作的角色比例

3. 大部分企业已委任数据安全负责人和个人信息保护负责人

根据《数据安全法》第二十七条“重要数据的处理者应当明确数据安全负责人和管理机构”及《个人信息保护法》第五十二条“处理个人信息达到国家网信部门规定数量的个人信息处理者应当指定个人信息保护负责人。”，满足法律规定情形的企业应设立数据安全负责人和个人信息保护负责人。本次调研发现，大部分被调查企业已委任数据安全负责人（90%）和个人信息保护负责人（88%）。

然而具体如何设置数据安全负责人和个人信息保护负责人在法律法规中并未明确规定。通过调研发现，被调查企业更多地选择 CIO/IT 总监（25%）、CISO（19%）、DPO（15%）担任数据安全负责人。而对于个人信息保护负责人，被调查企业更多地选择由合规主管（18%）、CIO/IT 总监（17%）、DPO（16%）担任。同时，部分企业选择由 CEO 担任数据安全负责人（7%）和个人信息保护负责人（6%）。可见，目前数据安全负责人和个人信息保护负责人的任命未成定式，企业可根据自身组织架构以及业务与产品设立相应岗位，落实保护和监督责任。

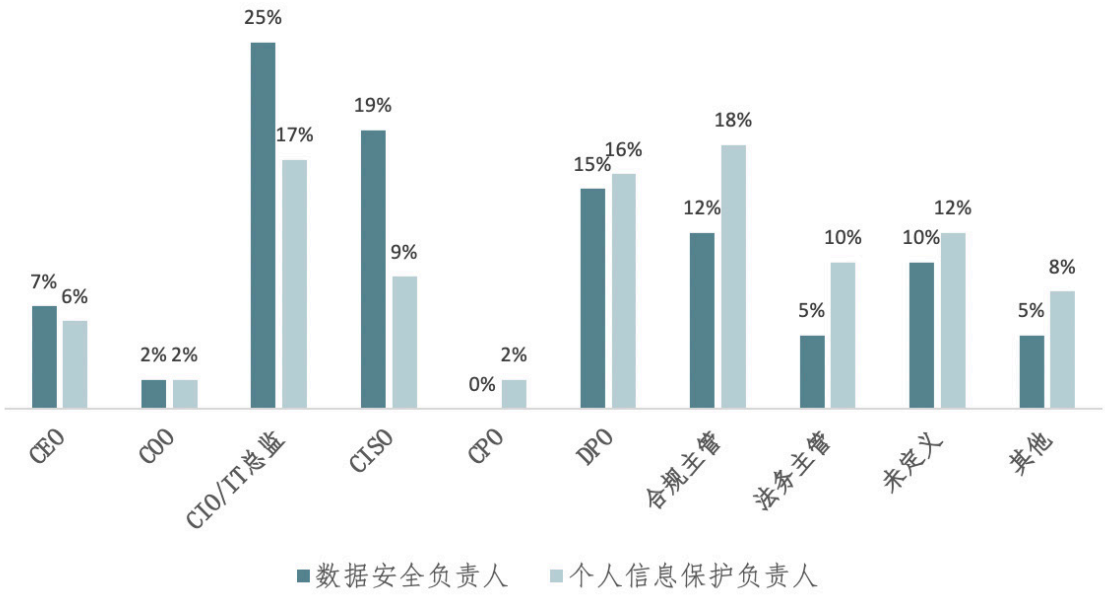

图 5 数据安全负责人和个人信息保护负责人的设立

4. 企业负责数据合规与隐私保护工作的人员数量逐年提升，但仍存在人才缺口

去年企业负责数据合规与隐私保护工作的人员数量“大于 20 人”“11–20 人”“6–10 人”的占比仅为 6%、2%、6%，而今年企业负责数据合规与隐私保护工作的人员数量“大于 20 人”“11–20 人”“6–10 人”的占比相比去年均有所上升，为 15%、6%、12%，说明企业需要更多的数据合规与隐私保护人员以满足监管和消费者对数据合规与隐私保护日趋强烈的需求。

13% 的企业没有全职人员负责数据合规与隐私保护工作。2022 年 9 月工业和信息化部人才交流中心和工业和信息化部网络安全产业发展中心牵头，联合多家单位共同研究编制的《网络安全产业人才发展报告》（2022 年版） 正式发布，报告显示随着合规和业务安全需求的提升，网络安全领域人才仍然供不应求，其中数据安全相关人才尤为紧缺。对于大部分企业尤其是中小型企业来说，数据合规与隐私保护的专业人员仍然存在较大的缺口，人员问题也成为了部分企业无法满足实际的数据合规和隐私保护工作需求的原因之一。

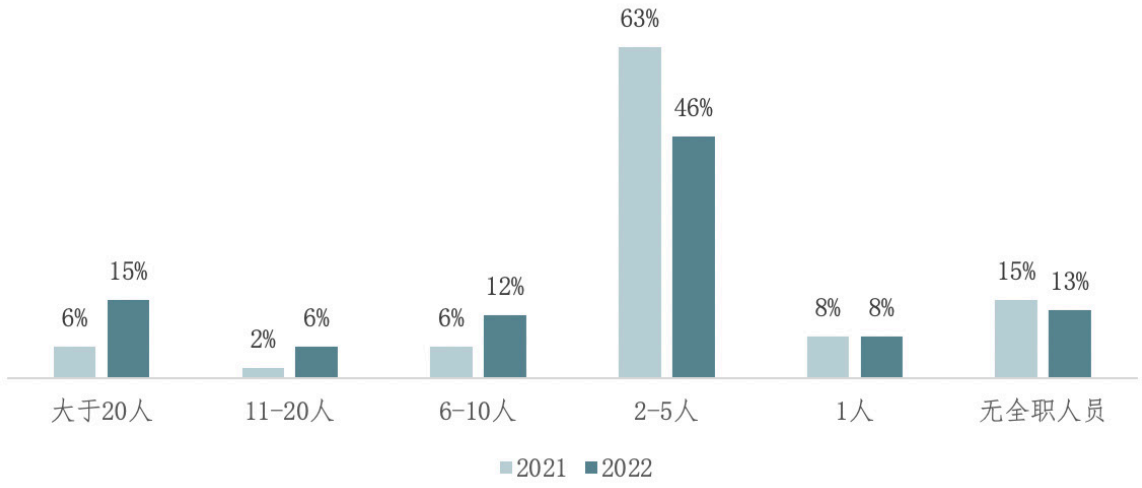

图 6 企业数据合规与隐私保护工作的人员数量

数据合规与隐私保护工作人员数量随着企业营业额增加而增多。60% 的“营业额大于 1000 亿元人民币”被调查企业，拥有 6 人及以上的数据合规与隐私保护工作人员；而 83% 的“营业额小于 100 亿元人民币”被调查企业，拥有 5 人及以下的数据合规与隐私保护工作人员。

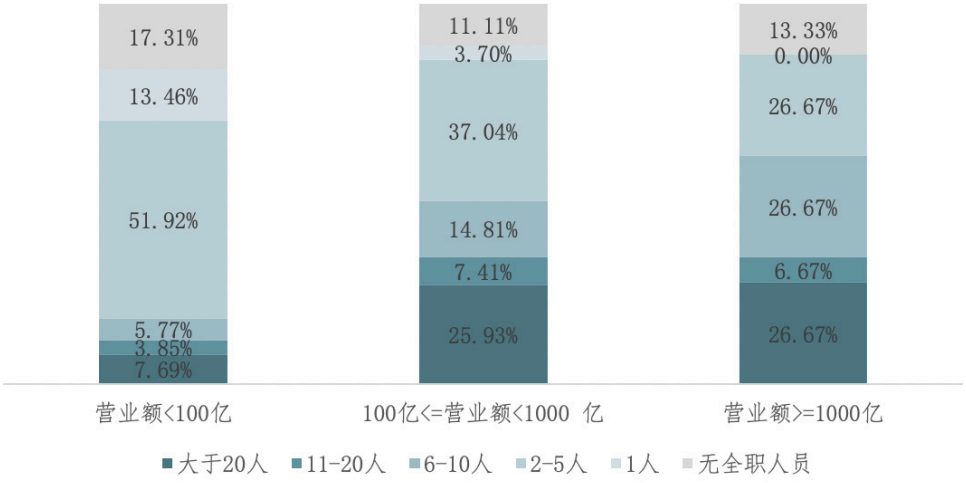

图 7 企业数据合规与隐私保护工作的人员数量分布图（单位：人民币）

5. 数据合规与隐私保护的投入日趋满足实际需求

- 数据合规与隐私保护的投入一直是数据合规与隐私保护工作者关注的重点，通过对比，了解自身数据合规与隐私保护的投入是否与同等规模企业一致。调查发现，68% 的被调查企业过去 12 个月在数据合规与隐私保护的投入大于 100 万元人民币。
- 企业数据合规与隐私保护的投入随着营业额的增加而增多。52% 的“营业额 <100 亿元人民币”被调查企业过去 12 个月在数据合规与隐私保护的投入小于 100 万元人民币；66% 的“100 亿元人民币 <= 营业额 <1000 亿元人民币”被调查企业在数据合规与隐私保护的投入在 100 万元到 500 万元人民币之间；而 54% 的“营业额 >1000 亿元人民币”被调查企业在数据合规与隐私保护的投入大于 500 万元人民币。

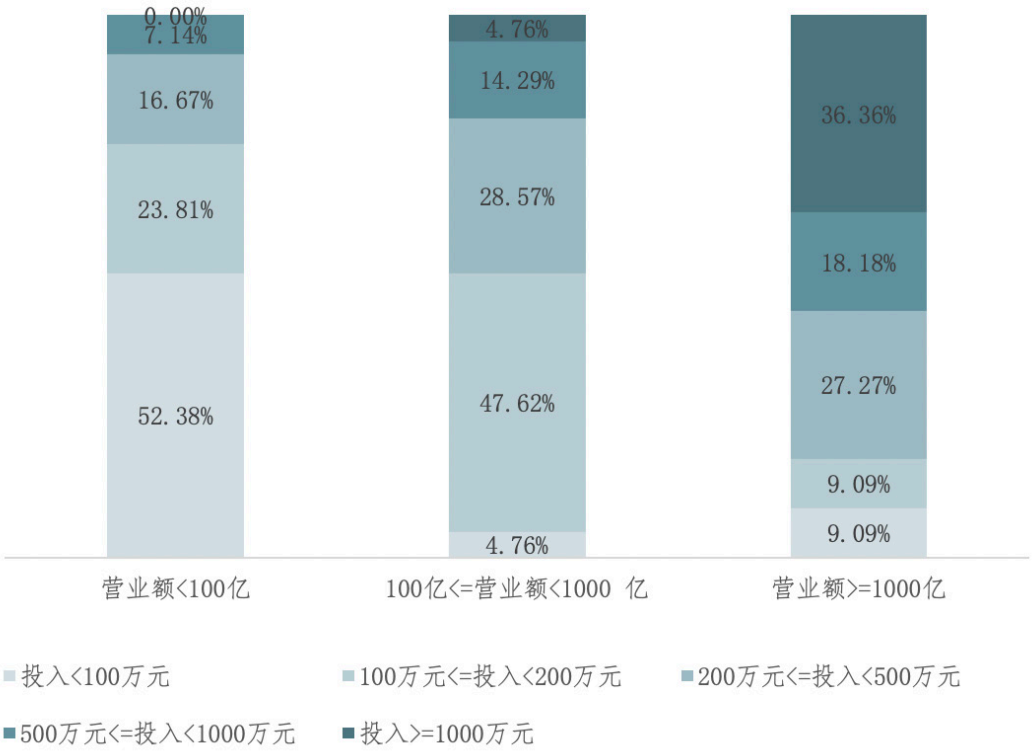

图 8 过去 12 个月企业数据合规与隐私保护的投入分布图（单位：人民币）

- 数据合规与隐私保护的投入日趋满足实际需求。82% 的被调查企业认为公司在过去 12 个月内数据合规与隐私保护方面的投入基本满足需求或超出需求，而去年仅为 52% 的被调查企业这么认为。可见随着国内数据安全和隐私保护压力增大，企业在数据安全和隐私保护方面的投入逐步增加，更加积极主动地应对合规风险。

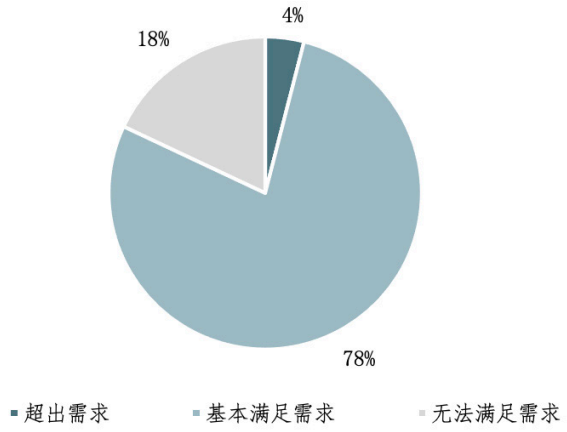

图 9　过去 12 个月企业数据合规与隐私保护的投入满足需求程度

6. 数据合规与隐私保护成熟度逐步提升

制度与流程是数据合规与隐私保护体系的重要组成部分，也是基础性工作。大部分企业在启动数据合规与隐私保护工作时，会从制度与流程建设着手，对内部管理进行标准化、规范化，设立运营流程以保证数据处理活动符合相关法律法规要求。

- 在制度建设方面，已有 92% 的被调查企业定义了相关方针政策以及管理制度与操作规程，并且有 42% 的被调查企业认为公司已制定了完善的管理制度和操作规程。

- 在制度执行情况和效果方面，大部分（81%）被调查企业对制度要求进行了落实执行，相比去年（74%）有所提升。今年，63% 的被调查企业认为执行效果有待提升，而仅 18% 的被调查企业认为公司有效执行和落实了数据合规与隐私保护制度和流程，尽管如此，这一数值相对去年的 3% 仍有很大提升。这些转变表明随着企业数据合规与隐私保护工作的深化，企业对于制度和流程落地的需求越来越强烈，企业数据合规与隐私保护成熟度不断提升。

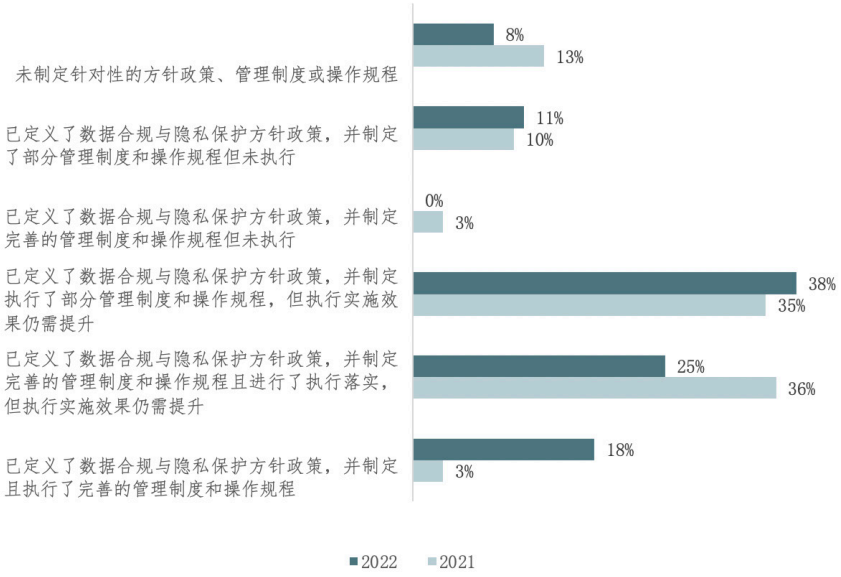

图 10　企业数据合规与隐私保护的制度定义与执行情况

7. 企业积极开展数据出境安全评估工作

2022 年 9 月 1 日《数据安全评估管理办法》正式施行，以支持企业履行《数据安全法》第三十一条重要数据出境和《个人信息保护法》第三十八条个人信息出境相关义务。《数据安全评估管理办法》明确指出，办法施行前已经开展的数据出境活动，不符合办法规定的，应当本办法施行之日起 6 个月内完成整改。对此，适用该办法的企业，大部分（75%）被调查企业进行了积极响应，其中 42% 的被调查企业处于数据出境安全评估工作前期，即正在开展数据出境自评估，17% 的被调查企业已完成子评估，16% 的被调查企业已经开始进行安全评估申报。

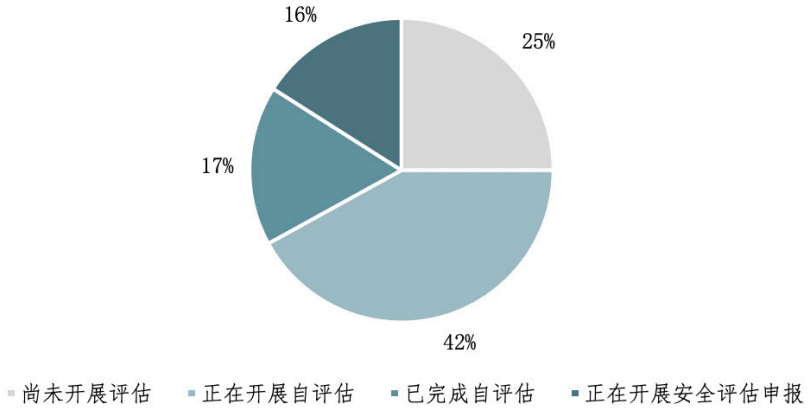

图 11　企业数据出境安全评估工作的进度

由于国内数据出境安全评估工作刚开始启动，企业在评估过程中存在许多挑战。在已经启动数据出境安全评估工作的被调查企业，71% 的被调查企业认为公司数据出境场景复杂，很难梳理清楚。另外，46% 的被调查企业认为公司人员缺乏数据出境评估技能和知识，难以支持评估工作的开展；40% 的被调查企业认为公司缺乏隐私技术开展数据出境安全评估。

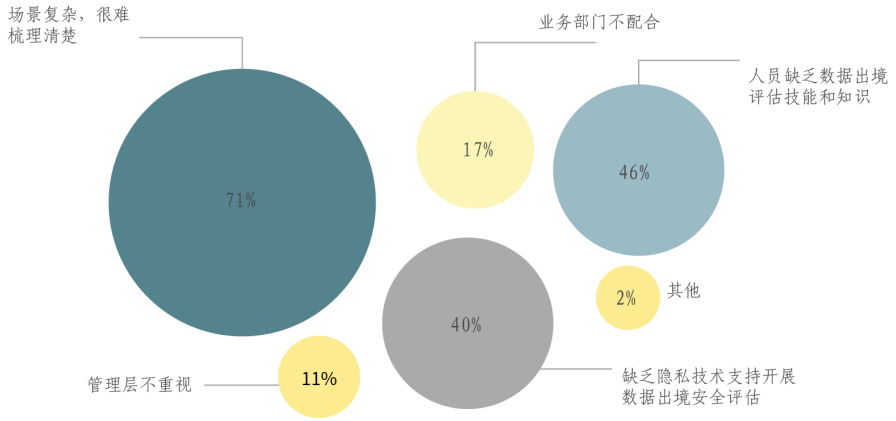

图 12　企业开展数据出境安全评估工作面临的挑战

针对这些挑战，短期可以借助内外部资源，对公司现有数据出境场景和风险进行梳理和评估。长期来说，可以从流程、技术和人员三方面入手，逐步完善企业在数据出境安全管理能力。流程方面，建立数据出境安全评估机制，在开展业务时若涉及数据出境应进行内部申请和自评估，必要时还需进行外部申报。技术方面，一是借助“数据自动化发现、分级分类与标识”和“数据流动监控”隐私科技解决方案掌握公司个人信息和重要数据的分布、流动、出境等情况，这与目前企业对数据合规与隐私技术解决方案迫切需求一致；二是通过“数据合规与隐私风险评估平台”将数据出境安排评估流程线上化，并将其嵌入业务活动设计阶段，形成关键控制卡点。人员方面，通过开展数据合规与隐私保护职能人员的技能培训和全员意识培训，增强人员数据出境安全评估能力和意识。

随着《数据安全法》和《个人信息保护法》的施行，我国在数据安全和个人信息保护方面的监管不断增强。今年，除了数据出境需根据《数据出境安全评估办法》的要求向网信办申报，汽车数据安全管理也需根据《汽车数据安全管理若干规定（试行）》的要求向网信办报送。另外，银保监会下发《关于开展银行保险机构侵害个人信息权益乱象专项整治工作的通知》，要求银行保险机构在个人信息保护方面进行自查自纠，并报送书面自查整改工作报告；各地通管局也发布《电信和互联网行业网络和数据安全检查的通知》要求企业自查自纠并上报总结报告。相信未来，数据合规与隐私保护企业自查整改上报、监管重点抽查的趋势将越来越明显，企业需不断提升自身数据合规与隐私保护水平。

3.2 企业隐私科技应用程度

个人信息保护和数据安全法律法规和监管日渐成熟的同时，企业的数字化进程也未曾放缓脚步。在日益增加的数据量和愈发复杂的业务场景下，技术手段成为企业隐私保护与数据安全治理的必要手段。因此，越来越多的企业开始了隐私科技解决方案的实施，将先前的规划付诸实践。在去年的调研中我们发现，有 57% 参与调研的企业正在实施部分隐私科技解决方案，而到了今年，这个比例增长到了 65% 以上，其中更是有 38% 的参与调研的企业已经实施了部分隐私科技解决方案。

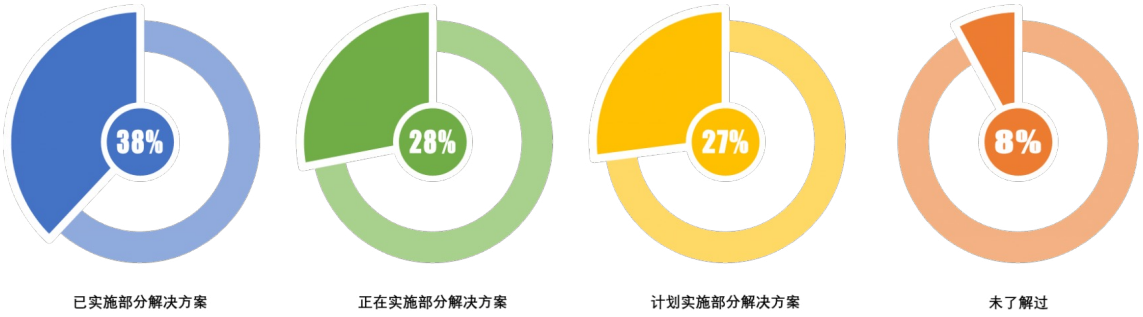

图 13 企业隐私科技解决方案实施程度

针对常见的隐私科技解决方案，除隐私计算平台外，所调研的其余九类隐私科技解决方案的整体实施程度较高的（即实施中、部分已实施和已较完备实施的解决方案）企业占比均超过了 50%，其中排名前三的有：个人信息主体授权同意管理（66%）、个人信息主体权利响应管理（63%）、隐私事件响应（62%）、隐私风险与合规评估平台（62%）。另外，隐私计算平台（41%）和数据流动监控（52%）这两个在去年的调研中实施程度最低的隐私科技解决方案在今年仍然是最低，但其实施程度相较去年均有明显增长，其中，隐私计算平台从 29% 增长到了 41%，数据流动监控从 33% 增长到了 52%。综合来看，尽管各类隐私科技解决方案在企业中达到"已较完备实施"的程度仍然都不高（均未超过 18%），隐私科技在企业中的整体实施现状仍然处在起步阶段，但经过了过去一年的实施后，隐私科技解决方案在企业中的整体实施已经取得了长足的发展和进步。

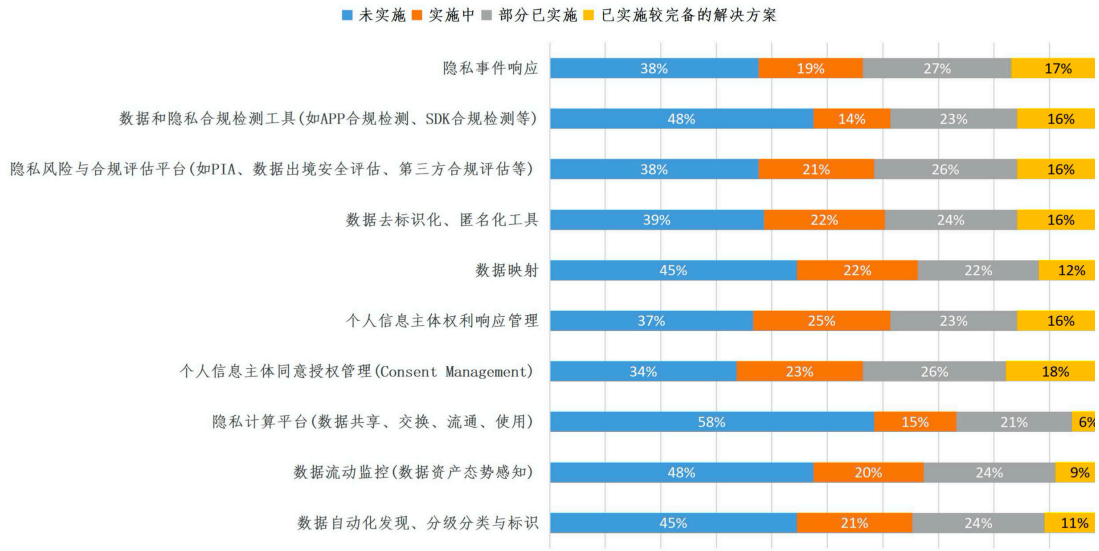

图 14　企业隐私科技解决方案实施现状

数据资产管理是同时飘在甲方和乙方头上的一朵"乌云"。在去年的调研中我们发现，企业需求最迫切的三类隐私科技解决方案是，数据自动化发现、分级分类与标识（60%），数据流动监控（52%），数据去标识化、匿名化技术（38%）；而在今年，数据自动化发现、分级分类与标识（62%），数据流动监控（51%）仍然是企业最迫切的需求，但数据去标识化、匿名化技术仅排在 23% 的企业最迫切的"三甲"榜单之上。这与隐私科技解决方案实施现状的调研结果也是吻合的，在今年有 16% 的企业实施了较完备的数据去标识化、匿名化技术，而去年仅有 5%，企业通过一年的实施，已部分满足了需求。而相比去年，数据自动化发现、分级分类与标识和数据流动监控的实施程度、需求迫切程度均未明显改善，其中数据自动化发现、分级分类的实施程度甚至有显著降低。这说明企业对数据隐私与安全愈

发重视的同时，隐私科技市场仍未出现较好的帮助企业识别与监控“有什么数据”和“数据在哪里”等问题。同时我们发现，数据自动化发现、分级分类与标识与数据流动监控也是企业自开发率最低的两类技术，分别为 47% 和 48%。这说明，隐私科技市场无法较好满足企业需求的同时，企业也较难依赖自己的研发能力来解决数据资产管理的难题。

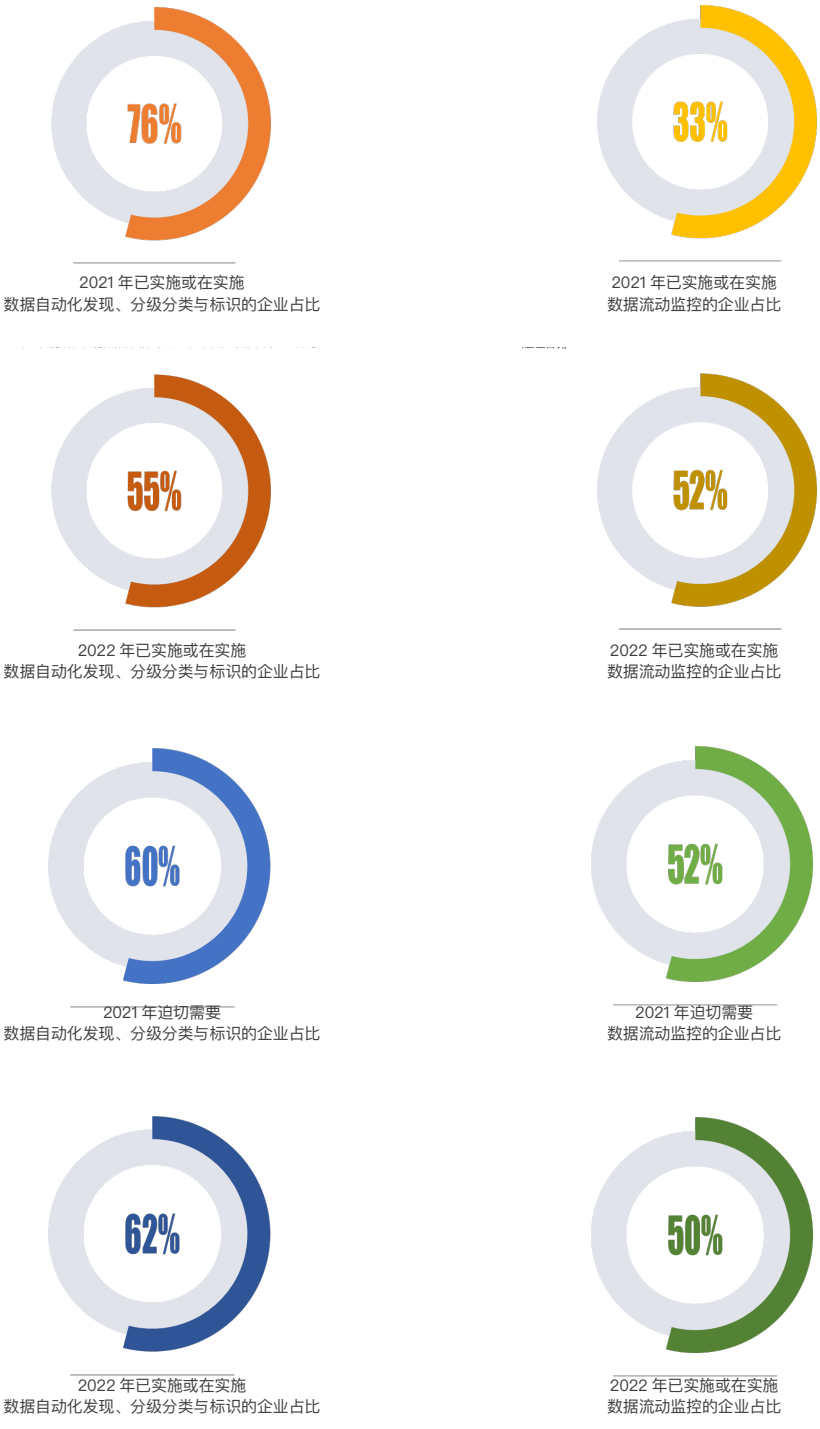

图 15　企业隐私科技解决方案需求与实施现状

隐私计算平台在金融与 TMT 行业中有着较大发展潜力。替代数据自动化发现、分级分类与标识成为企业最迫切需要的隐私科技解决方案的是隐私计算平台，有 40% 的企业表示迫切需要这类解决方案。在这些企业中，大部分企业来自金融业（占全部表示迫切需要隐私计算平台的企业的 28%）和 TMT 行业（占全部表示迫切需要隐私计算平台的企业的 8%）。无独有偶，隐私计算平台实施程度最高的两个行业（已较完备实施、已实施部分解决方案）同样是金融业（占全部隐私计算平台实施程度较高企业的 33%）与 TMT（占全部隐私计算平台实施程度较高企业的 22%）。可见，尽管金融业与 TMT 行业已经走在了隐私计算平台实施的前列，但仍有巨大的增长空间。

越来越多的企业开始选择自研。在去年的调研中我们发现，针对与已有系统环境存在紧耦合关系的解决方案，自开发比例会明显高于外采，包括个人信息主体同意授权管理（自开发率 70%）、个人信息主体权利管理（自开发率 65%），数据去标识化、匿名化技术（自开发率 63%）；而对于技术门槛较高、管控规则需长期沉淀的解决方案，大部分企业选择购买成熟产品来进行实施。今年，企业自开发率进一步提高。除了数据自动化发现、分级分类与标识（自开发率 47%）、数据流动监控（自开发率 48%）、数据和隐私合规检测工具（自开发率 44%）以及隐私风险与合规评估平台（自开发率 50%）以外，其余隐私科技解决方案的自开发率均超过了 60%，其中隐私事件响应的自开发率高达 75%。综合各项隐私科技解决方案，今年参与调研的企业的平均自开发率从去年的 47% 提高到了 57%。在各行业中，研发能力较强的 TMT 行业各项隐私科技的自研比例均显著高于外采比例。此外，62% 的企业认为隐私科技解决方案无法满足需求的原因是产品无法有效地与管理流程或 IT 环境整合，因此，高度定制化、高集成度也许是企业更多地选择自研方案的原因之一。

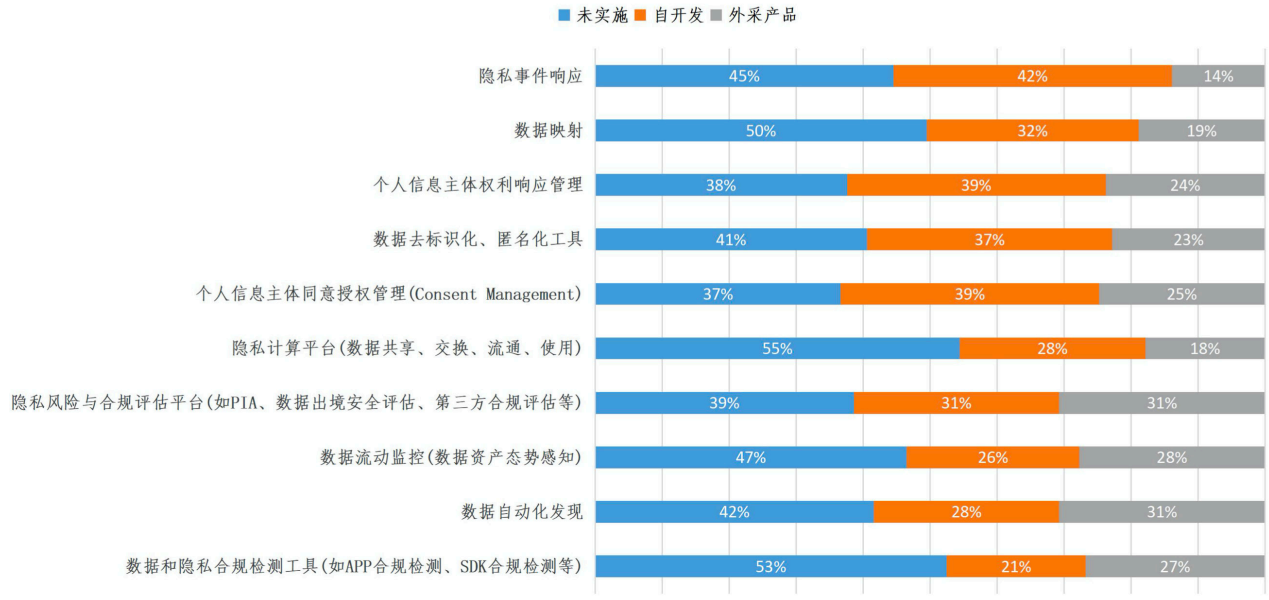

图 16　企业已实施的隐私科技技术自研与外采情况

数据合规与隐私保护管理平台的实施程度提高，且取得了良好的实施效果。去年的调研显示，企业在隐私保护管理平台的功能实现与实际需求存在较大差距。企业对数据合规与隐私保护安全意识培训（93%）、数据 / 个人信息安全事件应急响应（92%）和数据安全与个人信息保护合规自评估（90%）等功能有较大的需求，但是大部分功能仍处于未实施的状态，各项功能平均实施率仅有 35%。在今年的调研中，需求最高的三个功能分别是数据合规与隐私保护安全意识培训（92%）、数据安全与个人信息保护合规自评估（88%）和数据 / 个人信息安全影响评估（87%），而平均实施率提高至 47%，且每项功能的实施率均有所提高。

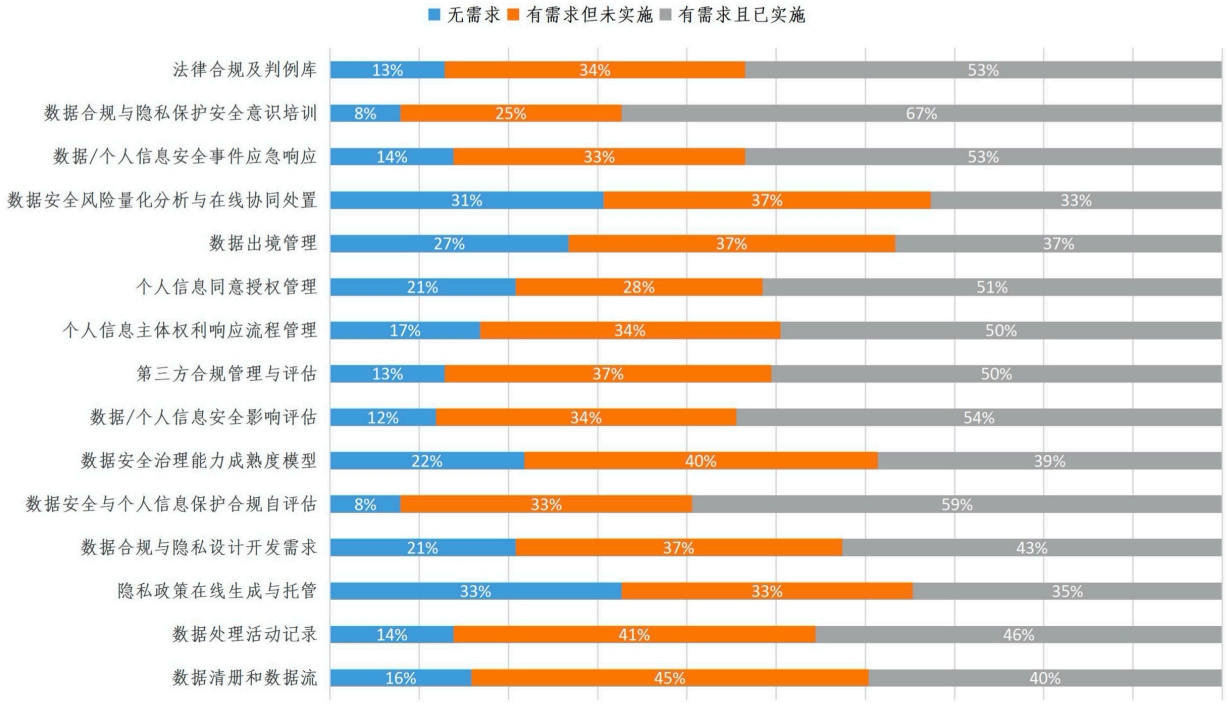

图 17　有需求的企业对数据合规与隐私保护管理平台所支撑功能的实施现状

而在已实施数据合规与隐私保护管理平台功能的企业中，功能能够满足需求或超出预期的情况也较高，所有已实施的功能需求满足率均达到了 70%。

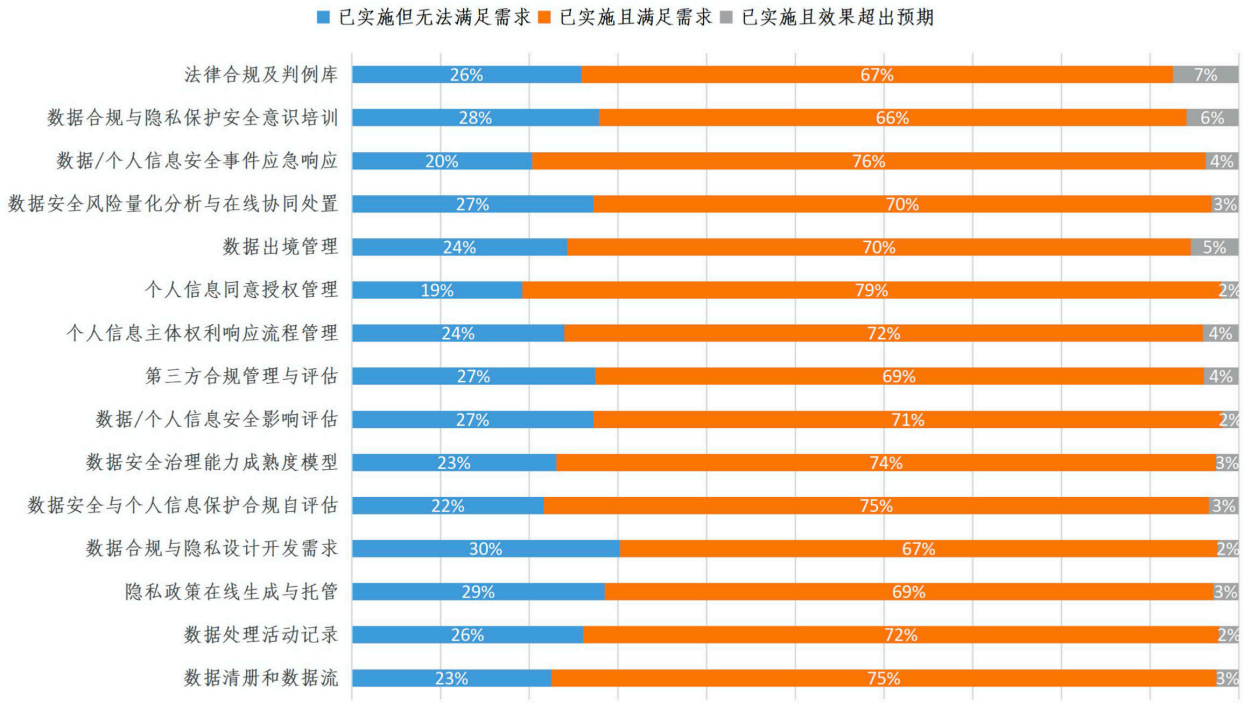

图 18　已实施的企业对数据合规与隐私保护管理平台所支撑功能的实施现状

隐私计算平台的用途更加广泛，且各类隐私计算技术均有用武之地。在今年的调研中，有 52% 的企业有了隐私计算技术的应用场景，远高于去年的比例（29%）。在参与调研的企业中，隐私计算平台除了在控制企业风险的场景中发挥着作用，也真正做到了为业务赋能，让在严格的监管环境、越来越高的数据安全要求以及保障知识产权的前提下难以开展的业务安全有序进行。隐私计算平台最常用的三大场景分别是风险控制（61%）、联合营销（50%）与反欺诈（44%）。在企业所采用的的隐私计算平台中，各类技术均达到了一个可观的使用比例，其中使用比例最高的是让数据可用不可见的多方安全计算（66%）与联邦学习（40%）。

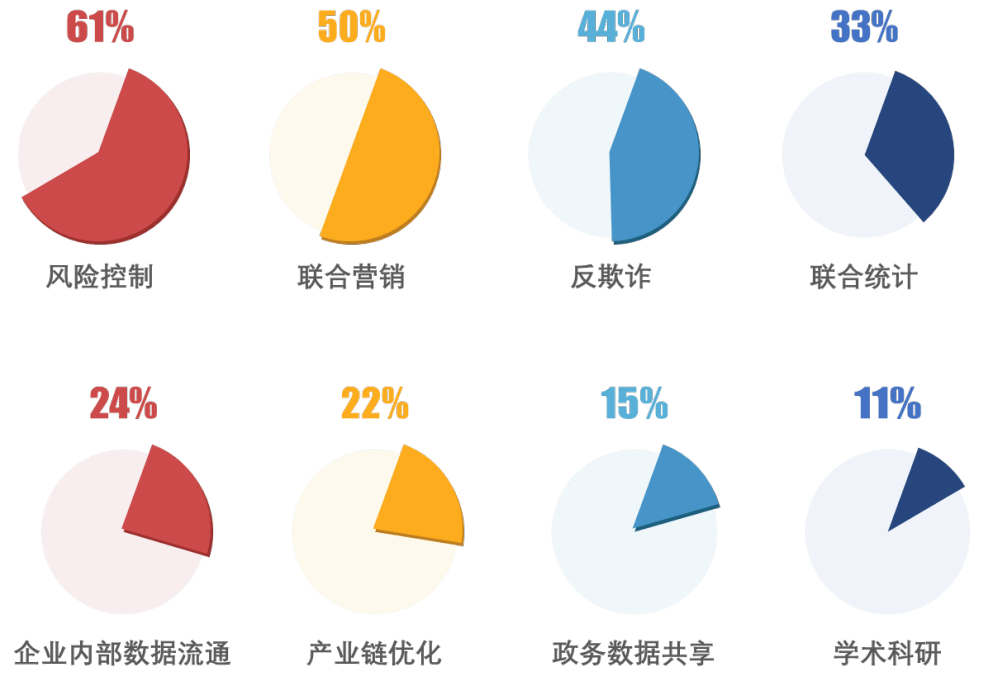

图 19 已实施的隐私计算平台所支撑业务场景

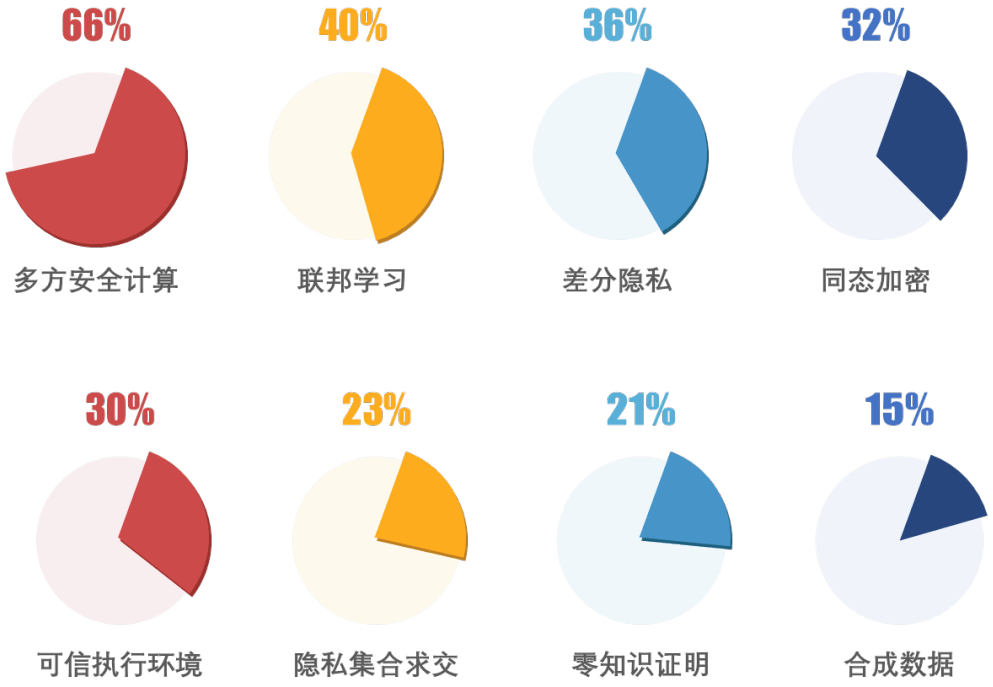

图 20 已实施的隐私计算平台中隐私计算技术的采用情况

隐私保护与数据安全已应用到了新兴科技中。隐私计算技术在元宇宙、工业互联网和区块链中也发挥着重要作用。根据调研结果，在已开展元宇宙项目的企业中，53% 的企业正在元宇宙项目中或已在元宇宙项目中实施了隐私科技技术；在已开展工业互联网项目的企业中，32% 的企业正在工业互联网项目中或已在工业互联网项目中实施了隐私科技技术；在已开展区块链项目的企业中，50% 的企业正在区块链项目中或已在区块链项目中实施了隐私科技技术。

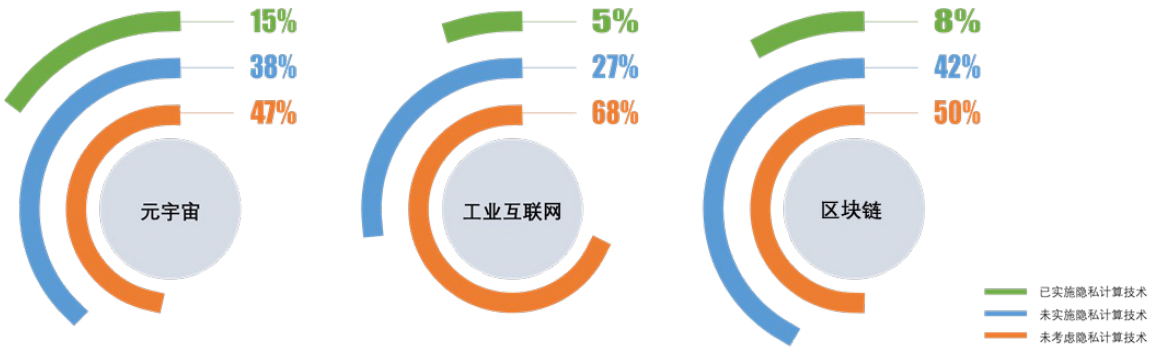

图 21 隐私科技在新兴技术中的实施情况

3.3 企业隐私科技投资趋势

尽管受到经济环境的影响，很多企业都在缩减预算，但很多企业仍然在为数据合规与隐私保护持续投入。在去年的调研中，有 46% 的参与调研的企业认为公司投入无法满足需求，但今年这个比例降低到了不足 18%，更有 4% 的企业认为投入已经超出需求。

然而，对于数据合规与隐私保护的持续投入并未完全体现在对隐私科技的投入上。在去年的调研中，61% 的参与调研的企业表示将会在未来 12 个月内增加对隐私科技解决方案的预算 5% 以上，但根据今年的调研结果，企业在过去 12 个月在隐私科技上的投入占比仍然不高，技术投入占公司数据合规与隐私技术方面投入超过 10% 的企业由去年的 27% 下降至今年的 22%。且在今年参与调研的企业中，表示会在未来 12 个月内增加 5% 以上的隐私科技解决方案预算的仅占总数的 43%，而表示会降低此方面预算的企业由去年的 4% 增加到了 8%，一半的企业表示对数据合规和隐私技术投入将保持平稳（预算变化 ±5% 以内）。

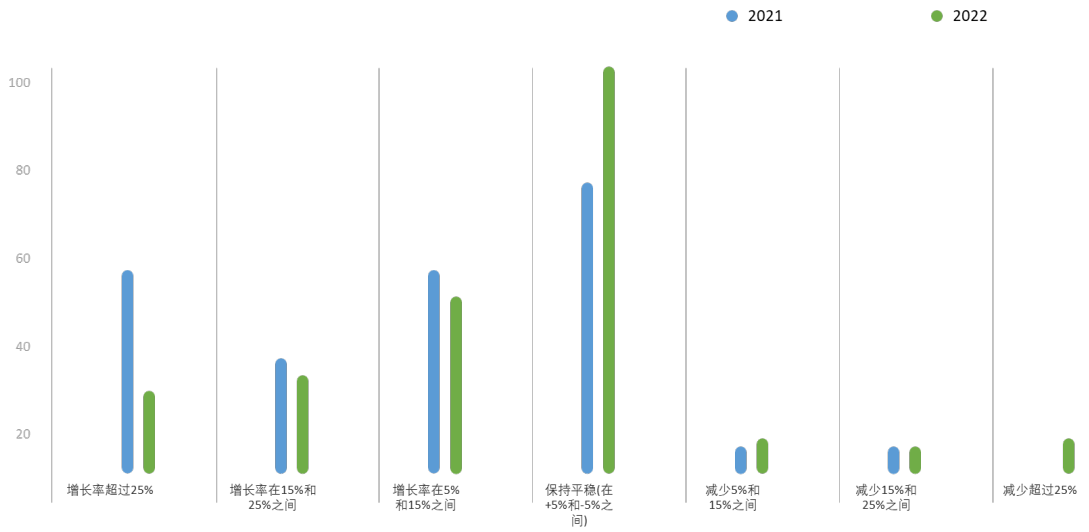

图 22 过去两年企业在隐私科技的投入意愿变化情况

企业在具体到特定解决方案的投入时也更加谨慎了。在去年的调研中，除了零信任仅有 38% 的企业愿意增加投入外，每一项隐私科技解决方案都有超过 40% 的企业愿意增加投入，而在今年，除数据自动化发现、分级分类与标识有 41% 的企业愿意增大投入外，没有一项隐私科技解决方案这项数据超过 35%，而选择不投入、减少投入的企业的比例均有所增长。

在停滞不前的隐私科技投入面前，仍有四分之一（24%）的被调查者认为未来 12 个月内对隐私科技的投入调整无法满足实际需求。隐私科技作为数据合规与隐私保护的基础能力之一，可以帮助企业更加高效、有效地控制合规风险，为业务保驾护航，因此企业仍需做好规划、合理分配资源，选择适合自己的隐私科技解决方案。

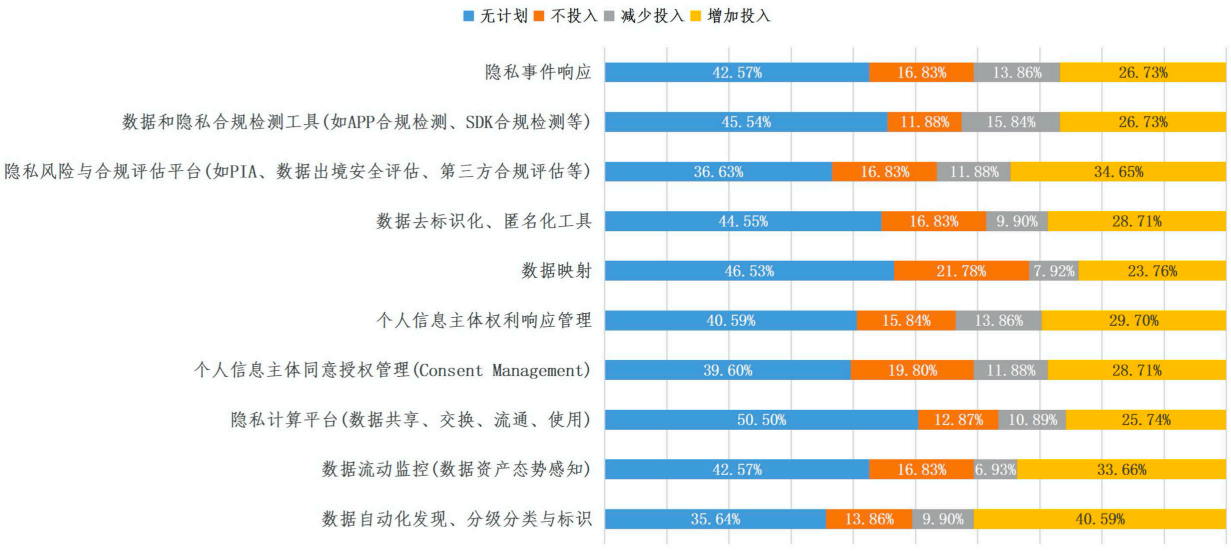

图 23 企业在隐私科技解决方案的投入意愿情况

3.4 企业对国内隐私科技市场的期望

隐私科技投入的停滞原因可能有多种，如过去两年的前期实施让部分产品、方案已进入业务稳态，维护费用低于前期实施费用；企业更多的自研使成本分摊在了信息技术或数字化部门的其他业务预算中；今年新出台的法律要求使得企业花费了更多预算用于合规评估等非技术类工作上等等。但更重要的是，随着国内合规要求日渐成熟且明确，我国数据合规与隐私保护法律提出了诸多相比欧洲、美国、新加坡等地独特的要求，我国的市场环境、业务场景和数字化程度也有着鲜明的特色，因此很多企业在期待更加贴合本地需求的国内隐私科技解决方案。根据调研，仅有 5% 的参与调研的企业在未来 36 个月内不会考虑国内的隐私科技解决方案，更是有 24% 的参与调研的企业表示会在未来 12 个月内考虑国内的隐私科技解决方案。

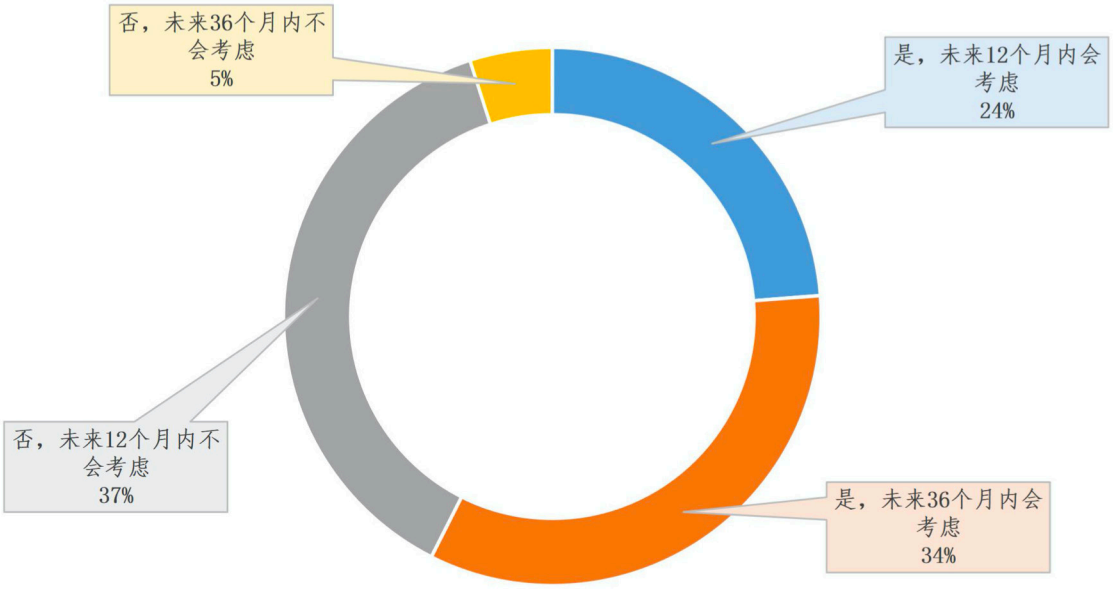

图 24 企业对国内隐私科技解决方案的考虑意愿

然而，大部分参与调研的企业均认为目前国内隐私科技市场仍处于早期阶段，仅有不到 10% 的参与调研的企业认为国内隐私科技市场大部分技术已进入商业化模式或认为整个市场已经成熟，90% 以上的企业认为市场仍不成熟，甚至有 22% 的企业认为所有技术均处于概念性阶段，无法有效落地。而在未来 36 个月内会考虑购买国内隐私科技解决方案的企业中，更是有 40% 的企业认为目前国内隐私科技市场的技术均无法有效落地。

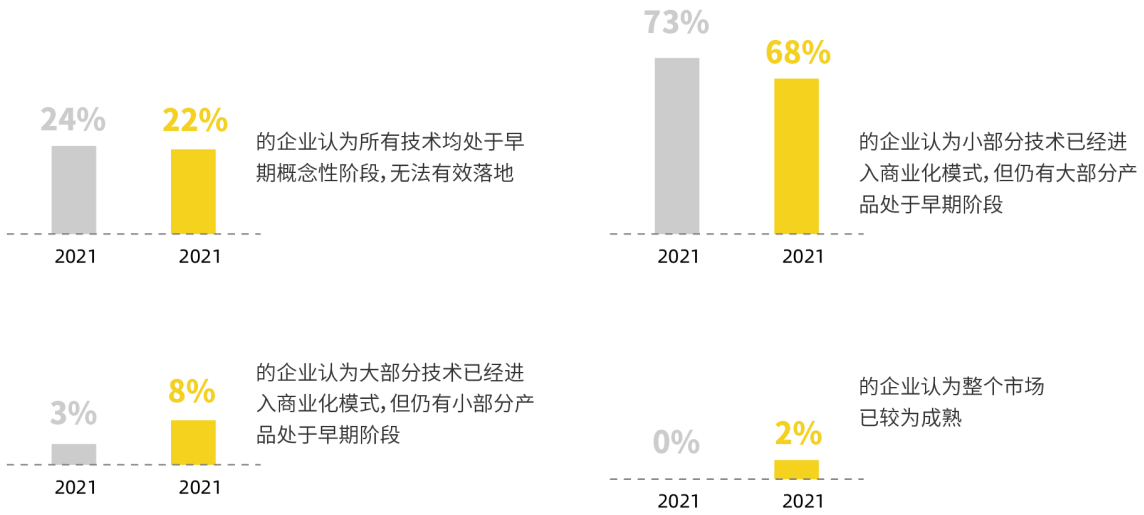

图 25　企业对国内隐私科技市场成熟度的评价

对比去年的数据，我们可以观察到国内隐私科技市场成熟度的提高，但提高幅度有限。这些数据既说明目前隐私科技市场仍处于非常初期的阶段，更代表着企业对国内厂商的期待与长期看好。在数据合规与隐私保护的浪潮下，厂商应当进一步理解企业需求、加大研发力度，做好企业数据合规与隐私保护的守护者。

3.5 企业实施隐私科技所面临的挑战

在企业的数据合规与隐私保护治理中，人员、流程与技术三者均不可或缺且紧密关联。实施隐私科技除了在技术上给企业带来挑战之外，同时也对企业的人员能力与意识、制度流程规范提出了更高要求。在去年的调研中，参与调研的企业表示实施隐私科技最大的挑战是产品无法有效地与现有管理流程或 IT 环境进行整合（84%），用户体验差、导致业务部门对产品的抵制使用（41%）和缺乏相应资质或技能的人员有效支撑运营（36%）。根据今年的调研结果，企业实施隐私科技解决方案的三大挑战分别是产品无法有效地与现有管理流程或 IT 环境进行整合（62%）、缺乏相应资质或技能的人员有效支撑运营（47%）和后期运维成本高、无法及时对产品、规则和流程进行更新（39%）。

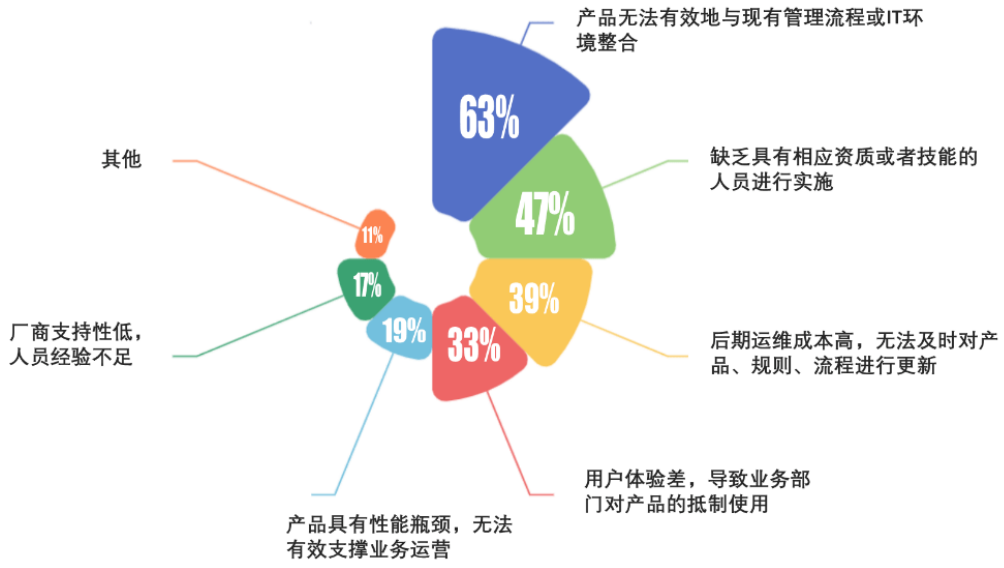

图 26 企业实施隐私科技面临的挑战

产品无法有效地与现有管理流程或 IT 环境进行整合

尽管产品无法有效地与现有管理流程或 IT 环境进行整合仍然是最大的挑战，但情况有所好转。这需要全行业的共同努力方可进一步改善、解决。在市场进一步提高对企业技术环境、业务场景的理解和加强对技术难关的攻克的同时，企业也需要进一步建设、优化相应的治理体系与技术架构，选择适合自己的解决方案。

缺乏相应资质或技能的人员有效支撑运营

在企业内建设运营隐私科技解决方案，对人员的技术能力、法律理解和企业管理知识都有着较高要求，然而这样的人才目前十分稀缺，随着法律法规的发展，人才缺口问题也变得愈发突出，是全行业都亟待解决的挑战。

后期运维成本高、无法及时对产品、规则和流程进行更新

这个挑战其实是前两个挑战的综合体现，产品本身在实施过程中就没有很好地兼容企业现有治理体系和技术架构，那么在产品、监管环境、企业内部环境产生变化时，产品的扩展性很可能变成突出问题，企业需要花费额外的人力财力去进行维护、变更，甚至宣布项目失败；与此同时，运营人才的缺失更加加剧了运维的难度。

挑战之外，我们同时也看到了进步。今年的调研发现，隐私科技解决方案的用户体验同样得到了长足的改善，仅有 33% 的参与调研的企业认为这是隐私科技解决方案无法满足需求的原因，这一项也跌出了无法满足需求的原因的前三名，同时产品性能问题也得到了改善，仅有 19% 的企业认为产品具有性能瓶颈、无法有效支撑业务运营，而这项数据在去年高达 34%。

P-A-R-T 04

产业发展洞察与典型实践

PART 4

产业发展洞察与典型实践

目前，隐私科技被广泛应用于金融、政务、医疗等重点行业，随着市场应用的增长，隐私科技产业发展迈入深度实践阶段。与此同时，由数据源、数据使用方和数据服务方构成的隐私计算生态，由安全厂商、数据合规与隐私保护服务方构成的数据合规生态，成为隐私科技产业生态的核心支撑。

4.1 隐私科技产业发展

隐私科技的产业及应用发展是各企业、机构充分践行国家数据战略，满足监管与数据共享的结果。由于隐私监管工作在全球范围内的扩展，越来越多的组织看到开始隐私工作的必要性。

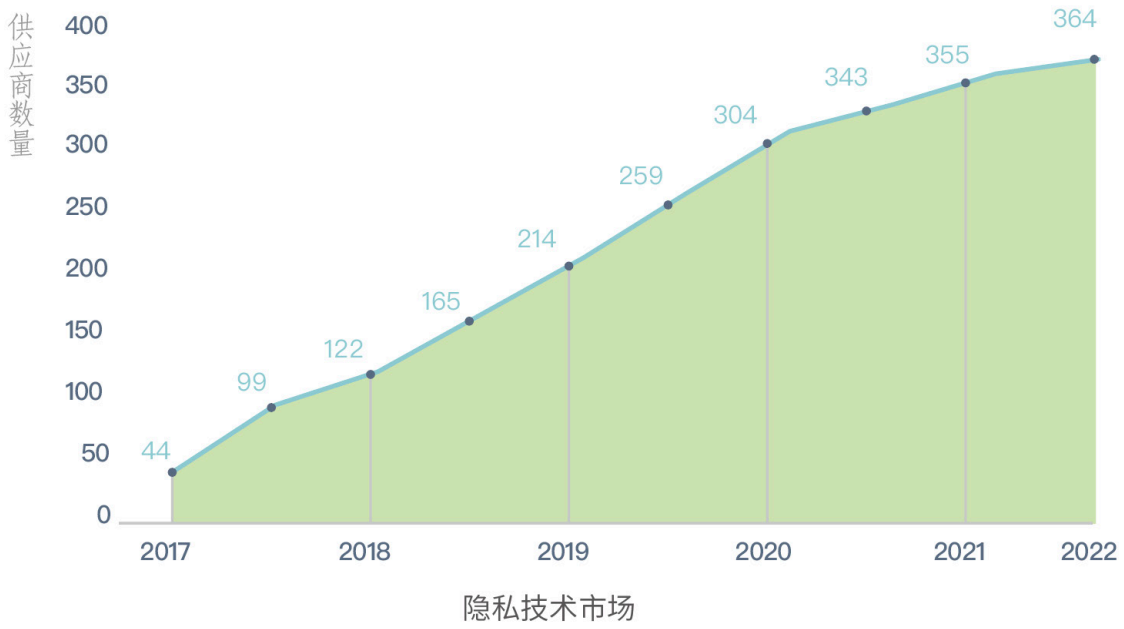

图 27 2017–2022 年隐私技术供应商增长情况（IAPP）

市场需求拉动下，全球隐私科技市场整体趋于稳固发展，我国则进入追赶型发展阶段。根据 IAPP 年度隐私技术供应商报告（Privacy Tech Vendor Report），2022 年共计收录来自全球各地的隐私技术供应商为 364 家，对比 2021 年的 365 家在供应商数量上基本持平。当前，全球范围内的主要隐私科技供应商处于深耕行业、稳固发展阶段，该领域头部企业角逐趋于明朗。聚焦国内市场，隐私科技产业伴随一批数据安全法律法规的颁布、生效迎来快速发展期，既涌现了一批隐私科技创新创业企业，同时逐步孵化国内隐私科技领头企业，其中既包括传统网络安全企业借助原有安全基础，在数据安全方面加大投入，孵化新的产品及服务，也有较早入局的隐私科技企业在数据安全、数据合规或隐私计算等方向选择侧重点突破，提供更为成熟的服务体系和产品类型。国内隐私科技供应商处于百花齐放，百舸争流的多元发展阶段，尚未涌现全球及中国头部企业。

从产业分类来看，数据分类分级、数据流通监控、数据风险与隐私影响评估、数据与隐私综合治理是隐私科技产业的热门细分赛道。与此同时，随着安全产品、安全服务向集中式平台汇聚的趋势增强，市场上涌现了更多通用型数据安全与合规平台、隐私计算平台。平台型解决方案通过整合或替换单一功能的数据安全产品，成为支撑企业数据安全与合规常态化运营工作的重要方式。目前主要集中应用在以数据驱动为核心的金融、互联网行业，以及拥有大量数据源和数据流通需求的医疗、政务等领域。

从市场应用来看，隐私科技企业的进入市场实施阶段的产品比例逐年提升。以隐私计算相关技术和产品为例，根据隐私计算联盟统计，进入实施阶段的产品已由 2020 年的 38% 上升至 2021 年的 48%，且部分产品能够支持较大规模应用的实施。此外，隐私科技相关技术的开源生态逐步形成，这也进一步推动合规解决方案的落地与应用。

在产业结构丰富、企业快速发展的背景下，隐私科技产业的投融资整体向好。2022 年上半年，我国隐私应用平台已经涌现千万级融资，隐私计算服务领域出现亿级融资，可以预估我国隐私科技产业在近 3 年将快速新增一批估值数亿到十亿级别的产品与服务提供商。

4.2 典型案例 1：运营商行业数据分类分级

随着电信行业的快速发展，新技术、新模式得到广泛运用，用户个人信息的泄露风险和保护难度不断增大。运营商行业相关政策法规相继出台，数据安全方面，《电信网和互联网数据安全通用要求》（YDT 3802–2020）、《基础电信企业数据分类分级方法》（YDT 3813–2020）相继出台，针对基础电信企业数据分类分级提出了示例，并规范了数据采集、传输、存储、使用、开放共享、销毁等数据处理活动及其相关平台系统应遵循的原则和安全保护要求，同时，明确了对运营商数据安全组织保障、制度建设、规范建立等管理要求以及相关配套技术要求。《2020 年省级基础电信企业网络与信息安全工作考核要点与评分标准》要求包括运营商在内的相关行业按照《2020 年电信和互联网企业数据安全合规性评估要点》完成数据安全合规性评估工作，形成评估报告，并针对 2020 年内应组织落实的要点

内容，及时进行风险问题整改。

与此同时，工业和信息化部《关于做好 2020 年电信和互联网行业网络数据安全管理工作的通知》也对运营商行业数据安全防护提出了更高、更具体的要求，包括：持续深化行业数据安全专项治理、全面开展数据安全合规性评估、加强行业重要数据和新领域数据安全管理、加快推进数据安全制度标准建设、大力提升数据安全技术保障能力、强化社会监督与宣传培训。

对于运营商来说，需要满足通信行业安全合规政策检测要求，提高自身数据安全防护能力，针对全行业有序实施数据安全治理建设。

（1）运营商行业数据安全痛点

大数据新技术带来客户信息安全挑战。众所周知，大数据平台数据量大、数据类型多样、大数据平台组件设计之初存在高解耦性等，面对大数据环境下，数据的采集、存储、处理、应用、传输等环节均存在更大的风险和威胁。在运营商大数据安全管理层面，存在缺乏客户信息衡量标准，运营商的安全管控系统和安全管理职责不明确等风险，特别是在运营商大数据对外业务合作过程中，数据传输、使用的过程中留存等诸多的安全漏洞。在安全运营层面，也存在着供应链、业务设计、软件开发、权限管理、运维管理、合作方引入、系统退服等安全风险。

数据信息的分类分级较难。数据信息包括客户的信息和企业业务数据信息。客户信息中又涵括了用户身份和鉴权信息、用户数据及服务内容信息、用户服务相关信息等三大类，而在这三类信息中，又包含了身份标识、基本资料、鉴权信息、使用数据、消费信息等诸多不同类型的数据。这就导致在实际工作落地中，运营商往往很难进行全量的识别，致使对这些客户信息进行管理时，无法进行全部监控，因而不能在第一时间发现风险。运营商的业务数据信息中由于内部业务系统复杂，各区、省、市、县业务数据信息存在非常高的业务属性，对比客户信息更加繁杂，而且各业务系统的开发厂商也存在各自的专有标签，这些数据信息存在分散、数据量大、业务属性强，都导致数据分类分级难以推行实施，使敏感信息无法准确定位、定级发现，导致整体的数据信息环境存在安全隐患。

数据大集中导致风险集中爆发。随着近些年来，目标明确、精准打击的高级持续性威胁攻击行为带来越来越大的风险，电信行业受到了越来越多更加隐蔽、更加深度的威胁。目前大数据平台、云计算环境尚处于起步阶段，基于新模式新场景下的数据安全防护手段和措施仍然欠缺，同时由于电信企业大数据环境存在宝贵的海量数据资产，因此更容易成为不法分子的目标，带来数据安全难题。

（2）运营商行业客户信息保护

为了使客户信息得到保护，电信运营商必须要加强对大数据环境下客户信息保护的要求工作，深入探索大数据安全，开展大数据安全保障体系规划，同步推进大数据安全防护手段建设，保障大数据环境下安全可管可控。在治理大数据客户信息安全的过程中，需要从安全策略、安全管理、安全运营、安全技术、合规评测、服务支撑等层面，建立大数据客户信息安全管理总体方针，加强内部和第三方合作管理过程把控，强化数据安全运营和业务安全运营的过程要求，夯实对大数据平台系统的安全技

术防护手段，定期开展大数据客户信息安全评估工作，强化大数据客户信息安全治理过程。

- **推动数据分类分级**

对于电信运营商企业信息，全面开展对客户敏感信息的识别和分类分级。通过对业务数据的分类分级，实现业务系统的分级安全建设标准，只有这样才能够在大量的客户信息和业务信息中，有效地分析出敏感信息，并科学管理这些信息，打造出安全的数据流转环境。

基础电信企业数据分类方法：参照 GB/T 10113–2003 中的线分类法为基础进行分类。按照业务属性或特征，将基础电信企业数据分为若干数据大类，然后按照大类内部的数据隶属逻辑关系，将每个大类的数据分为若干层级，每个层级分为若干子类，同一分支的同层级子类之间构成并列关系，不同层级子类之间构成隶属关系。

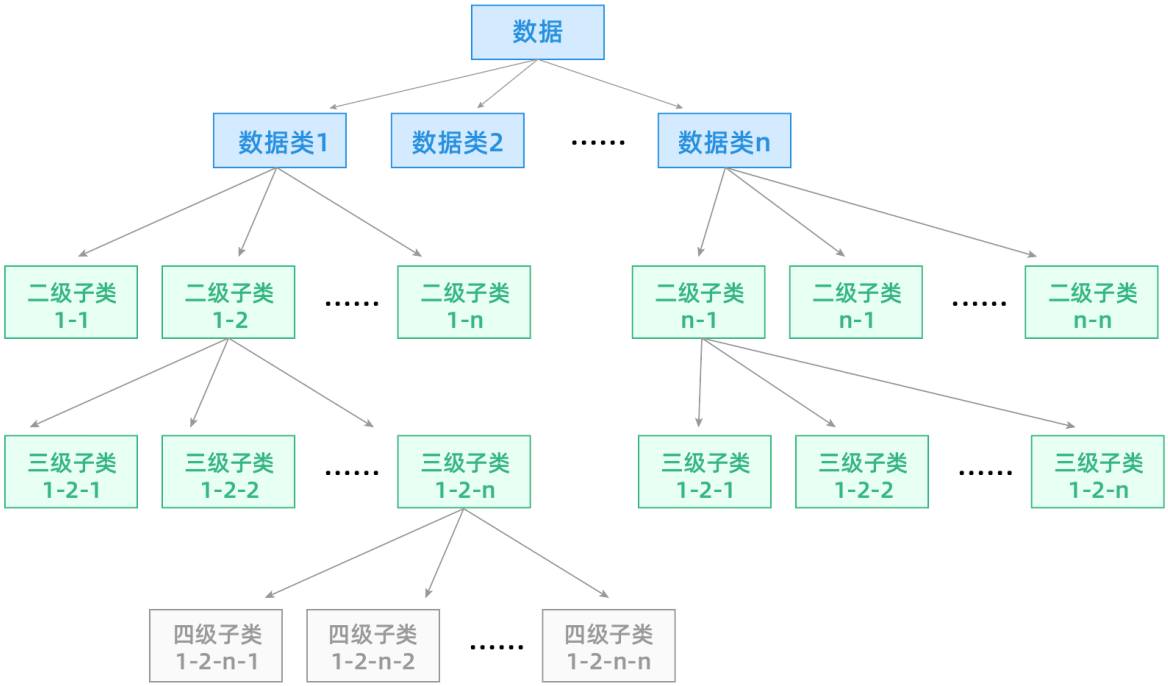

图 28　基础电信企业数据分级方法

在数据分类基础上，根据数据重要程度以及泄露后造成的影响和危害程度对基础电信企业数据进行分级。

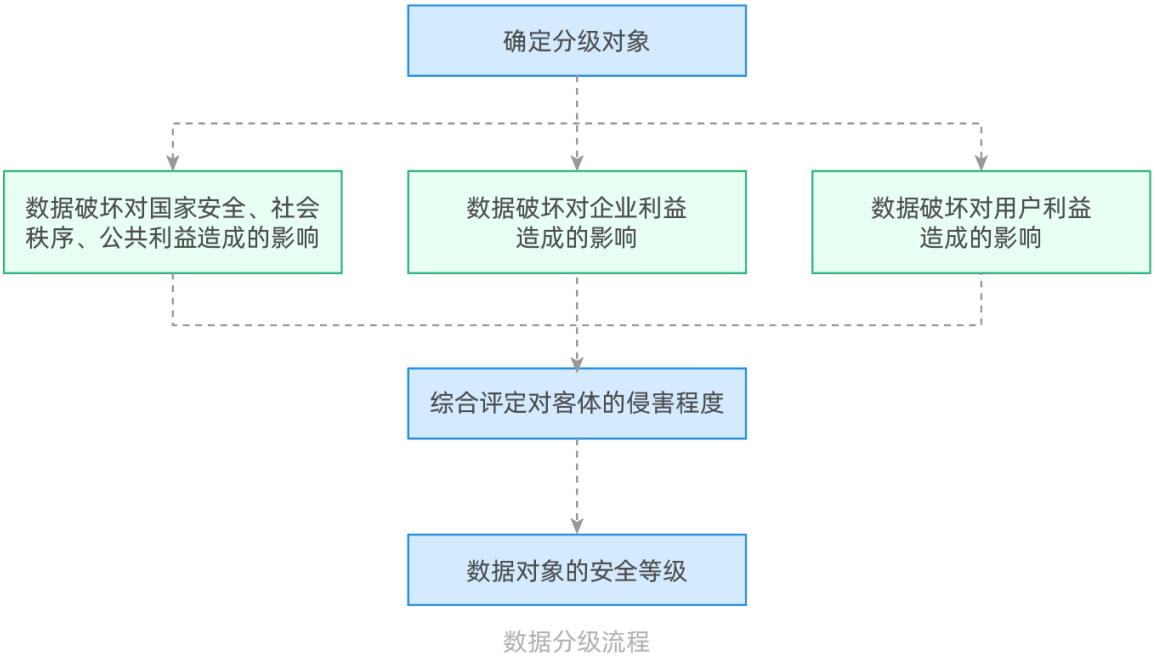

图 29 数据分级流程

确定数据分级对象、确定数据安全受到破坏时造成影响的客体、评定对影响客体的影响程度、确定数据分级对象的安全等级，以此为依据实施安全防护策略。

- **增强数据安全管理**

大数据背景下，电信运营商客户信息常常受到数据安全的威胁，想要增强客户信息的安全性，必须要增强数据安全治理体系的建设。

首先，需要继续加强传统网络安全手段的建设，通过数据梳理、数据库安全网关、数据库审计、数据脱敏、数据加密、DLP 防泄密等基础数据安全设备构筑防护能力。其次，针对大数据的特殊环境进行研究，解决虚拟化、大数据共享、非关系型数据库安全等新型问题，作为传统网络防御手段的有效补充。最后，需要遵循国家针对大数据下安全标准，制定适合本行业科学、合理的标准，为电信和互联网数据安全打下良好基础。

4.3 典型案例 2：基于联邦学习的分布式可信医疗精确营销

聚焦医疗行业，某省健康导航平台是运营商省公司联合省卫健委共同打造的省级统一医疗健康服务平台，平台汇集全省 800 多家医院的优质资源，提供预约挂号、排队叫号、报告查询、体检预约、在线药房等服务。目前累计注册用户超 1500 万，累计服务人次超 6000 万，在省内医疗行业形成巨大规模和影响力。面向如此庞大的用户，平台运营方一直在探索互联网运营方式，但传统的推荐营销手段因受数据量限制，效果欠佳。运营商省公司拥有海量用户的属性和行为数据，平台运营方却无法获取运营商数据，从而影响推荐算法的预测效果。因此，急需通过技术手段在保障双方数据隐私的情况下，进行联合模型构建，提升推荐模型的准确性。

（1）场景概述

通过引入联邦学习技术，基于联邦学习模型架构，在保证数据隐私安全的前提下构建跨域建模能力，赋能健康导航业务场景下的精准推荐。联邦学习在多方本地化部署的基础上，服务端、客户端及协调方通过网络互联进行联合建模，实现数据不出库、不共享数据，有效解决数据孤岛问题。联合模型充分利用运营商省公司大数据优势和健康导航平台行业经验，建设健康导航平台 APP 用户弹窗问诊功能推荐，以提高 App 推荐的精准性。

图 30　模型

（2）技术框架

联邦学习在多方本地化部署的基础上，服务端、客户端及协调方通过网络互联进行联合建模，实现数据不出库、不共享数据，有效解决数据孤岛问题，主要包括：数据准备、特征工程、加密对齐、模型训练、模型推理五个模块。

图 31 技术框架

（3）模型具体方案

模型具体方案如下：

训练逻辑：健康导航平台根据业务需求发起训练，然后经协调方和运营商做数据对齐，完成后开始与运营商交换参数并训练模型。具体步骤如下：

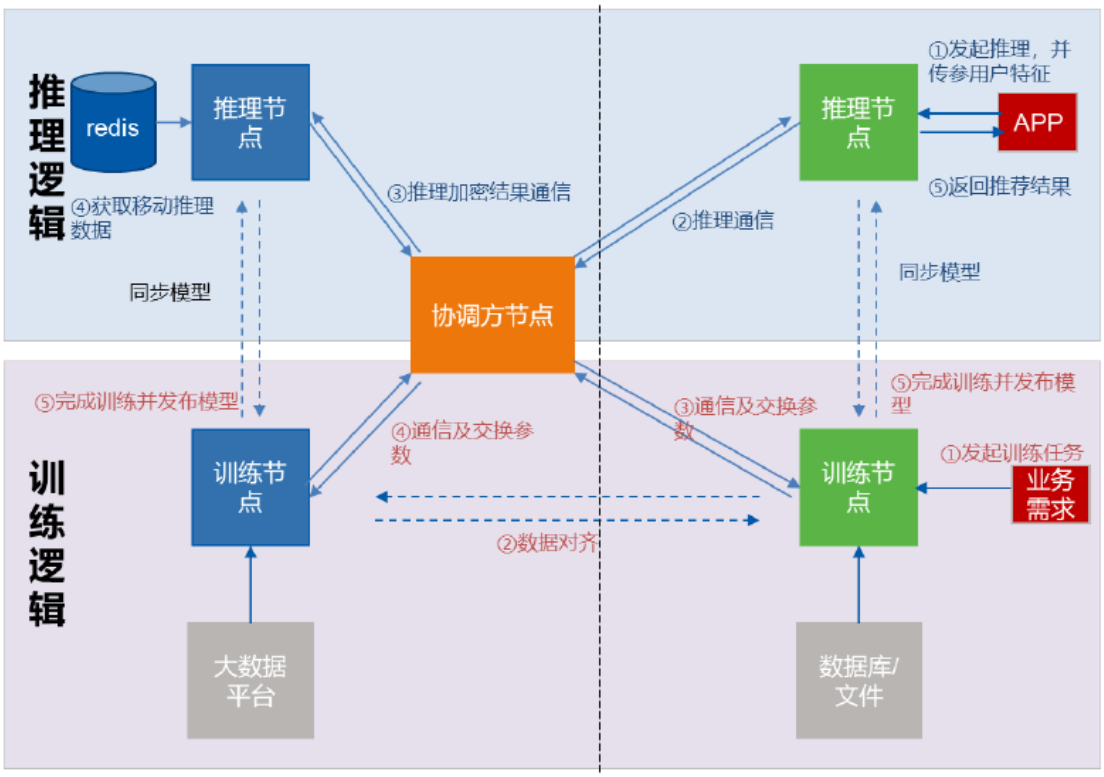

图 32 具体方案

（4）隐私科技价值

该应用创新性地利用联邦学习分布式架构进行部署和建模，安全匹配、安全统计、安全模型等功能助力参与联合营销的各机构原始和明细数据不出库的前提下进行跨域数据驱动精准营销，同时保障机构数据安全与个人隐私，确保数据应用安全合规。

数据经授权后方可进行安全计算，最小化利用，数据调用可追溯审计。基于多方安全计算等隐私保护技术，实现数据可用不可见，解决不同机构之间的数据协同计算过程中的数据安全和隐私保护问题，助力机构安全高效地完成联合营销等跨机构数据合作任务，驱动业务增长。

基于联邦学习和数据加密，该应用实现了运营商及健康导航平台双方数据的“虚拟融合”，大幅提升了推荐模型的准确率，联邦学习模型效果相对自有数据模型效果提升 111% 以上，实现问诊、体检等场景的精准推荐。同时打造“场景冷启动模块”“用户冷启动模块”解决对新增场景的用户群推荐，和新增用户的业务场景推荐等问题，有效提升就医用户满意度。

P-A-R-T 05

未来展望

PART 5

未来展望

隐私科技的产业发展是一个从理念构建到规模化应用的过程。由于这一概念少有研究且尚未形成公认定理，产业发展缺乏规范性引导，至今未形成集聚。然而，在个人信息权益保护、数据流通与共享、个人信息合理利用的全球性需求下，隐私科技产业正在步入快车道。隐私科技产业发展将以愈发成熟的隐私设计理念为基础，依托快速迭代的技术、产品及服务占据市场份额，通过开源形成广泛协作的生态圈，从而完成规模化行业应用，构建未来的数据智能网络。

《全球数据合规与隐私科技发展报告（2022）》重点关注隐私科技产业的发展，根据近一年的洞察，对产业未来提出几点展望，对 2021 年的洞察结论予以补充。

5.1 市场：数据合规即服务衍生新的商业机会

继网络即服务、网络安全即服务等商业市场蓬勃发展，数据合规即服务（Data compliance as a service）将成为未来重要商业模型之一，挖掘数字时代的新“蓝海”。伴随强监管下的安全检查、风险评估要求，由第三方机构提供的以个人信息保护影响评估（PIA）工具及相关服务逐步被市场认可与接受，成为数据合规即服务的突破口。**未来，数据合规即服务应是覆盖企业数据处理全生命周期，判断企业数据处理活动的合法合规程度及其对个人信息主体合法权益可能造成的风险，并提供解决方案。**隐私计算作为数据合规即服务的技术支撑能力之一，在数据流通和融合场景中，促进数据的‘可用不可见”，进一步帮助企业挖掘数据价值。与此同时，隐私计算不是数据合规的“万全之策”，无法一揽子解决数据合规与隐私保护问题，因此，更广泛意义的数据合规即服务将引领数据合规市场的百花齐放。

5.2 应用：隐私设计原则从理论转为企业实践

隐私设计原则是综合多种技术、运行系统、工作流程、组织架构、基础设施的一种保护理念，包括将隐私内嵌到企业管理架构和业务场景，化被动合规为主动防御，将个人信息保护视为组织运行的默认前提等。鉴于所有的数据安全合规都并非简单的技术问题，其中不仅涉及数据与业务之间的场景关系、数据与人之间的处理关系，而且涉及法律法规、标准流程等合规合法问题。随着科技发展、企业隐私保护理念逐步拓展，将安全前置，将数据合规贯穿于数据安全生命周期成为数据合规与治理的重要

思路。由此，隐私设计原则应运而生。

目前部分企业及机构已经积极地推动隐私设计实践，与此同时，聚焦个人信息安全问题的隐私科技也融合了隐私设计理念。一方面，将个人信息保护理念嵌入 IT 系统，通过技术手段优化隐私计算、完善个人信息安全能力框架。另一方面，将个人信息安全与业务流程设计相结合，基于企业内部业务场景、业务流程，从技术能力、合规能力、运营能力、管理能力、流程制度等维度快速搭建内部个人信息安全壁垒，实现机器 + 人工的全流程隐私科技综合管理与运营方案。

5.3 人才：数据合规及隐私保护人才缺口增长

事件和合规驱动企业调整人才需求，根据 Gartner 的数据，到 2025 年，50% 在中国开展业务的大型跨国公司将设置专职的数据安全负责人，具备本地法律专业知识和语言技能，以满足中国市场相关的数据保护需求。人才市场的供需明显不对称将激发培训服务的增长，再加上《个人信息保护法》规定，需"定期对从业人员进行安全教育和培训"；《数据安全法》规定，开展数据处理活动应当依照法律、法规的规定，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。积极开展外部人才引进和内部人员定期隐私保护相关培训成为企业完善数据安全能力、推动合规实践的必然举措。越来越多的中小型企业将在数据安全合规人才引育方面增加支出，依托专业的培训服务，定期开展人才培训、意识教育以及相关资质认证。

5.4 标准：技术成熟度和通用性标准亟待制定

大众对于数据安全的关注聚焦于安全性、技术成熟度、通用性和落地可实施性四个方面。诸如零信任、隐私计算等新型理念与技术将被引入数据合规领域，从技术落地为切实可行的解决方案，为传统的数据安全解决思路增加创新力和完善性。未来，超大规模云提供商将进一步提供可信的执行环境，帮助越来越多上云企业在云环境获得安全性和隐私性的保障，隐私计算等新型理念与技术进一步从学术研究项目过渡到商业解决方案，被积极应用于金融、电子政务和医疗保健领域。

与此同时，聚焦隐私科技中的关键技术，利益相关方需要合力制定多方安全计算、联邦学习、同态加密、差分隐私等技术应用标准，建立技术成熟度模型，进一步推动技术快速成熟与市场化。目前，已有相关隐私计算系列标准制定完成，如《基于多方安全计算的数据流通产品技术要求与测试方法》《基于联邦学习的数据流通产品 技术要求与测试方法》《基于可信执行环境的数据计算平台技术要求与测试方法》《区块链辅助的隐私计算技术工具技术要求与测试方法》，后续技术安全性的标准还将进一步统一和规范；技术成熟度需要加强计算效率和性能的重视；通用性则涉及不同行业、不同企业、

不同业务场景之间，相关技术是否通用。这些都是隐私科技发展必须思考的问题，只有持续性推动隐私计算技术成熟度和通用性的标准化，才为数据合规流通夯实技术基础，加快隐私科技产品市场化阶段的可复制性。

5.5 技术：开源驱动行业创新发展与生态建设

开源是驱动协同创新、推动产业链发展及生态建设的重要模式，而在隐私科技的“商业化蓝图”中，开源生态也是“标配项”之一。目前，基础软件市场的开源模式已经基本成熟，新兴技术在技术萌芽期、发展期及市场完全成熟后这三个阶段往往也会迎来一波开源项目的数量增长。尤其在技术发展期，开源不仅降低研发成本，而且社区协作的框架可以对现有技术进行优化和“打补丁”。

基于此，隐私计算的发展路径将与技术开源休戚与共。2022 年，国内首个国际化自主可控隐私计算开源社区——开放群岛（Open Islands）开源社区成立，开源隐私计算框架“隐语”、因果学习开源项目 YLearn、隐私计算开源平台 Primihub 等项目频出，开源之风盛起。除了头部互联网企业拥抱开源，中小型科技公司等新锐力量也在席卷隐私科技，通过开源吸引更多国内外企业和研究人员加入资源共建，推动隐私计算性能提升、场景适配，为隐私科技的商业蓝图构建技术生态。

5.6 产业：规模化应用构建数据智能网络生态

随着个人信息安全的市场需求进一步增长，大型企业面临业务场景复杂、数据类型多样、数据流通频繁跨域 / 跨境企业自身安全能力有限等挑战，无法独立完成全覆盖的个人信息安全及合规工作。因此，企业将寻求第三方的安全能力支撑。隐私合规服务供应商或成企业重要解决方案。

未来，随着隐私科技的应用真正成熟化，安全产品与服务供应商将考虑到市场接受程度、技术市场化、产品可复制等问题。相关供应商将以软件销售和服务为主，基于行业与用户场景的特定，提供个性化与定制化的解决方案，并且注重低代码 / 零代码开发、轻量化部署，从而快速拓展隐私科技市场。同时，隐私计算并不会局限于一个技术模块或 IT 系统，更多安全服务提供商将选择把隐私计算能力平台化，融合多个功能，形成个人信息管理或运营平台，为企业提供工具化、整体性的个人信息安全能力。而当隐私科技的行业应用达到一定规模之后，将构建一个庞大的数据智能网络生态，降低个人信息合规成本，创造更多的业务发展可能性。

附录
APPENDIX

常见隐私科技解决方案类型

注：相关定义参考 GB/T 35273–2020《信息安全技术 个人信息安全规范》、IAPP

1）数据发现、分级分类与标识

定义：通过自动化的数据扫描和策略识别的方式定位数据、分级分类数据，以进一步实现分级保护。在数据发现过程中基于正则表达式、关键字、UDF等模式或者机器智能学习模式，自动将库、表中的数据进行识别和分级分类，并可视化分级分类结果。基于分级分类结果对字段或表级别打标签。

2）数据去标识化、匿名化工具

数据去标识化工具在个体基础上，采用技术手段如假名、哈希、加密等替代对个人信息的标识，保留了个体的颗粒度，使其在不借助额外信息的情况下，无法识别或者关联个人信息主体。数据匿名化工具通过对数据进行随机映射、统一泛化等操作，使其发布的数据无法关联到任何具体个体。

3）数据映射

采用手动或自动的方式帮助企业确定整体数据流，识别企业处理的个人信息，个人信息的来源和去向，存储、传输或处理数据的系统或流程。

4）个人信息授权管理

帮助企业收集、跟踪、展示和管理用户的个人信息授权同意，保证数据在不同阶段的处理活动均给予“告知 – 同意”的原则。

5）数据主体权利管理

帮助企业为个人行使数据权利提供更便捷的方式，包括响应个人关于行使访问权、更正权、可移植权和删除权等权利的请求。

6）数据流动监控

通过技术来实现对数据真实流转情况的可视以保证数据资产分布及访问行为态势的清晰度、透明度和可控性，并通过对数据流转路径和敏感数据访问行为的分析，预测数据资产可能面临的泄露风险、丢失和滥用。

7）隐私事件响应

提供符合法律要求的合规应急事件自动化处理，包括向相关方提供隐私事情详情和需履行的事件通知义务，帮助企业应对法律风险。

8）隐私风险与合规评估平台

帮助企业基于线上流程和评估模板开展隐私影响评估、数据出境安全评估、第三方合规评估、风险隐患定位等评估工作，高效规模化完成需要电子

表格、数据输入和报告的任务，为企业提供合规性证明的平台。

9）数据和隐私合规检测工具

针对网页、安卓 App、iOS App、小程序、IoT 设备等进行自动化隐私合规检测的工具，以确保企业的网页 cookie、APP、小程序等遵守相关法律法规和政策。

10）隐私计算平台

基于一种或多种隐私计算技术，如联邦学习、多方安全计算、隐私求交、可信执行环境、差分隐私等技术，在保证数据提供方不泄露原始数据的前提下，对数据进行分析计算，实现数据在流通与融合过程中“可用不可见”的数据处理平台。

主流隐私计算技术

1）差分隐私

差分隐私是密码学中的一种手段，当从统计数据库进行查询时，提供了一种最大化数据查询的准确性，同时最大限度减少识别其记录的机会。它可以通过对数据引入随机性，添加噪声，从而防止数据被推测。差分隐私能够做到在利用数据来满足业务需求的同时，抵抗外部攻击和实现隐私保护。在差分隐私技术的实践中，实现差分隐私保护的机制通常包括拉普拉斯机制和指数机制。拉普拉斯机制实现了对数值型结果的保护，指数机制则是实现对离散型结果的保护。如今，差分隐私已经应用到各行各业的业务场景中，比如医疗行业用于患者电子健康档案的保护、医疗传感器如可穿戴设备的地理位置信息的保护等。

2）同态加密

同态加密是一种特殊的密码学技术，它可以通过对加密的数据进行计算得到密文计算结果，后对其 进行解密得到与原数据计算结果相同的结果。同态加密能够真正做到数据的“可算不可见”，在得到正确 结果的同时保证了数据安全和隐私保护。在实践中，同态加密根据加密方式可以分为部分同态加密和全同态加密。部分同态加密是指仅支持对密文进行部分的计算，全同态加密是指对密文进行任意的计算。

近几年，同态加密的应用场景较广泛，在云计算、区块链和物联网中都存在同态加密的运用。如在云计算场景下，通过同态加密实现数据的流通，保证数据在流通的全过程中是密文的形式，确保数据安全。又如在区块链场景下，同态加密帮助实现了链上数据的保密性。同态加密的运用为数据的流通提供了安全保障，因此它已逐渐渗透到了医疗、金融、法律业等高度监管的行业。

3）联邦学习

联邦学习是隐私计算中最常见的一项技术，它本质上是一种分布式机器学习技术，通过中央服务器来实现对加密数据的流通与处理，最后完成多方

分布的机器学习框架。联邦学习能够在确保数据合规与隐私保护的前提下，多方共同参与完成联合建模。在整个过程中，既保证了数据安全，又实现共同学习的目标，协助企业解决数据孤岛、数据不可用、数据泄露等问题。实践中主要运用在企业风控评定、安全防控检测、医疗诊断等方面。

联邦学习在使用过程中，根据参与方之间的样本分布，分为横向联邦学习、纵向联邦学习和联邦迁移学习，不同的分类在实践中对应解决了不同类型的问题。

- 横向联邦学习适用于参与方特征相同，但是样本重叠较少的情景。横向联邦学习主要通过增加样本数量，达到了提升模型的准确性和泛化能力的目的。
- 纵向联邦学习则适用于参与方样本相同，但是特征重叠较少的情景。纵向联邦学习主要通过丰富样本来优化学习模型。
- 联邦迁移学习适用于参与方特征和样本重叠度都较低的情景，是对横向联邦学习和纵向联邦学习的补充。

4）隐私集合求交

隐私集合求交指的是，在保证互相之间不透露原始数据集的情况下，求得多方数据集之间的交集。隐私集合求交的用途十分广泛，如广告效果追踪、多方安全计算等。在前面联邦学习的介绍中，纵向联邦学习需要较高的参与方样本重合度，那么如何才能在不向其他联邦学习参与方透露自己有哪些数据的情况下仍能找出重合的数据样本呢？答案便是隐私集合求交。隐私集合求交有多种实现手段，如将数据进行哈希处理后进行求交，便可以迅速找到交集，并使得对方无法获得原始数据；当然，哈希仅仅是比较简单的手段，且安全性不佳。目前，常见的隐私集合求交方法包括不经意传输、基于密钥的方案、基于混淆电路的方案等，不同方案在安全性、计算成本、通信成本等方面有着不同的优劣势。

5）多方安全计算

多方安全计算是指，各参与方在互不信任的场景下，共同计算一个联合函数，并保证参与方仅能获得自己的计算结果，不泄露其他任何信息。它既能够确保数据的保密性，还能够确保各参与方都收到原有计算函数的正确结果。多方安全计算主要可以分为混淆电路和秘密分享。混淆电路能够在保证不泄露参与方数据的情况下进行计算，并且指定计算结果的所属者。秘密分享是通过拆分秘密信息，来实现数据安全，防止信息被丢失、破坏和篡改。近几年，多方安全计算陆续开始也应用到各类行业，其中混淆电路通常用于各类计算，而秘密分享在身份认证、密钥管理等方面有重要的作用。

6）零知识证明

零知识证明同样是一种特殊的密码学技术。一般来说，若需证明一个事实，如自己的身份、对某权益的所有权，验证者需与证明者掌握同样的信息才可进行验证，如口令、证书；但利用零知识证明技术，证明者能够在让验证者掌握任何被验证的具体信息的情况下，验证者仍可以进行有效的验证。“色盲游戏”是一个经典的零知识证明的例子：假设你有红绿两个小球，两个小球除了颜色之外完全相同，但你的朋友是红绿色盲，无法区分两个小球，那么为了证明这两个小球颜色的确是不同的，你的朋友双手各持一个小球并将手藏在身后，然后随机交换双手的球并询问你双手的球是否交换过，那么由于你每次都能答对，你的朋友最终相信了这两个球的

颜色的确是不同的，尽管他最终也无法知道两个球分别是什么颜色。

目前，零知识证明被较多用于加密货币中，用于保护交易中的隐私，确保匿名支付的情况下仍然能够在区块链上验证交易。主流协议包括 zk–SNARK, zk–STARK 等。但除了加密货币中的匿名支付之外，零知识证明的特性使其能够用于更加广泛的场景，包括：

- 资产管理：如在 NFT、元宇宙的应用中，同过零知识证明在不泄露具体资产信息的情况下证明自己对资产的所有权；
- 身份认证与访问控制：在不泄露申请人的具体身份信息、口令的情况下，进行身份认证、权限管理；
- 合规证明：在不泄露合规详情的情况下，如纳税记录，证明自己对法律法规的遵从情况。

7）合成数据

顾名思义，合成数据即通过计算机来生成的“假”数据，而不是从客观世界收集到的可以反应真实事件、环境、人物的数据。在很多数据使用场景中，受限于数据获取的困难、成本的限制以及隐私合规的要求，真实数据无法满足使用要求，如在模拟自动驾驶路况时，通过合成数据模拟出大量现实中较难出现的极端工况数据；训练机器学习模型时，通过合成数据模拟出样本不足的数据集；在涉及个人信息相关的研发、测试中，通过合成数据模拟出符合业务需求的个人信息，从而避免使用真实的个人信息；

8）可信执行环境

可信执行环境，即在中央处理器内预制特定、隔离的安全区域，有着独立的硬件资源和软件程序，在该区域内加载的程序和指令均以既定的形式运行，除授权信道外，可信执行环境中的信息无法被外部访问，且在可信执行环境内部中的可信应用也是相互隔离的。通过这种机制，有效地保护了可信执行环境中数据及可信应用的机密性和完整性。

除了保护交易、内容保护等安全使用场景外，可信执行环境在联邦学习中也有其用武之地。在联邦学习中，为了保护聚合各方模型数据的参数服务器的数据安全，通常会采用同态加密等密码学手段进行保护，但同时也带来了极高的运算成本，降低了联邦学习的效率，而在可信执行环境中进行参数聚合，则可以较好地平衡安全与效率。

文末引用

[1] TrustArc, 2022 Global Privacy Benchmarks Report

[2] IBV,Prosper in Cyber Economy

[3] 欧盟委员会 ,Working Programme 2023, COM(2022)

[4] 工业和信息化部人才交流中心，《网络安全产业人才发展报告（2022 年版）》

EY安永
Building a better working world

建设更美好的商业世界

安永的宗旨是建设更美好的商业世界。我们致力帮助客户、员工及社会各界创造长期价值，同时在资本市场建立信任。

在数据及科技赋能下，安永的多元化团队通过鉴证服务，于 150 多个国家及地区构建信任，并协助企业成长、转型和运营。

在审计、咨询、法律、战略、税务与交易的专业服务领域，安永团队对当前最复杂迫切的挑战，提出更好的问题，从而发掘创新的解决方案。

APAC no. 03016273
ED None

关注安永微信公众号，
扫描二维码，获取最新资讯。

ey.com/china

SICSI
CYBER RESEARCH INSTITUTE
赛 博 研 究 院
Shanghai Institute of Cyberspace Security Industry

上海赛博网络安全产业创新研究院（以下简称赛博研究院）是在上海市经信委和上海市社团局共同指导下的民办非企业，是国内从事数字经济、网络安全、数据合规的专业智库。

赛博研究院秉持专业、诚信、创新、合作的精神，已经为各级党政部门和各类企事业单位提供了包括战略规划、合规咨询、人员培训、技术平台等综合服务，并是上海市通信管理局、国家计算机网络应急技术处理协调中心上海分中心等监管部门的专业支撑单位，积极推动我国数字经济发展和网络强国建设。

成立至今，赛博研究院已发布《全球数据跨境流动政策与中国战略》《人工智能赋能网络空间安全：模式与实践》《数据安全治理白皮书》《云平台安全责任与治理》《智能网联汽车产业趋势与安全挑战》《人工智能数据安全风险与治理》《人工智能时代数字内容治理的机遇与挑战》等数十份具有较高影响力的专业报告。

关注赛博研究院微信公众号，
扫描二维码，获取最新资讯。

www.sicsi.org.cn

EY安永
Building a better working world

SICSI
CYBER RESEARCH INSTITUTE
赛博研究院