KPMG

AliResearch 阿里研究院

数据大治理

2020年7月

毕马威中国

行政摘要

作为数字经济的核心生产要素，数据正成为经济转型和发展的新引擎，以及社会治理的有效工具。例如，在此次新冠肺炎疫情的防控工作中，包括大数据分析和人工智能在内的高科技手段被广泛应用在疫情监测分析、病毒溯源、防控救治、资源调配等环节，效果显著，体现了大数据在公共卫生事件及社会治理中的重要性。因此，进一步鼓励数据的有效利用是新经济发展不可或缺的必要条件；但与此同时，由于大量数据中包含有个人隐私及商业机密等敏感信息，一旦泄露将对个人或企业带来难以估量的伤害和损失，保护数据安全，降低数据风险也迫在眉睫。如何在两者之间找到平衡，构建合理、有效的数据治理体系是一个重要的问题。

数字经济是新的经济形态，对原有生产方式和社会分工方式进行了重新定义，因此目前各国对于数据治理和数据安全领域的立法都还处于摸索状态。例如，欧盟通过了目前最严格的个人信息安全立法《通用数据保护条例》（General Data Protection Regulation，简称GDPR），实施两年以来尽管在个人信息保护及提升民众对个人数据保护权的认识方面颇有建树，但有研究显示它同时也提高了企业的合规成本，对于创新型初创公司的发展可能形成阻碍。美国、韩国、日本等国家也都出台了相关法规体系，致力于构建出多元化、多层次的数据治理规范体系。中国目前也正在抓紧制定个人信息保护法和数据安全法。

本报告首次提出了“数据大治理生态体系”的概念，它扩充了传统意义上的数据治理的内涵，从企业层面上升到社会层面，从顶层设计上明确各相关主体的权利和义务，既注重保护个人隐私和数据安全，又注重更好地挖掘数据价值、促进数字经济发展，从而实现全社会效益的最大化和可持续发展。该体系具有多物种、多角色、流动性等几大特征：

- 多物种是指这一体系中的参与者众多，既有企业、个人、政府等主体，也包含行业协会、产业联盟、消费者保护协会、媒体、智库、国际组织等机构在内的众多利益相关体。
- 多角色是指这一体系中的参与体可能同时担任着不同的角色，既是数据的生产者也是数据的使用者，各司其职同时又相互关联和支撑。
- 流动性是由数据的虚拟性和流动性等特点决定的。数据主权、数字经济已经成为各国高度关注的全球性问题。一个国家或地区的数据治理立法和实施会对其他地区产生“规范溢出”的影响，数据倾向于流向适应数据产业发展需求的地区。

在该生态体系中，企业、个人和政府是其中最主要的三大参与主体：

企业：企业是数字经济的核心推动者。企业的数据治理指的是企业对所拥有的数据资产的治理，这些数据资产也是企业资产的重要组成部分。因此，企业对数据资产的治理也可以被看作是公司治理的一部分。与公司治理相似，数据治理也需要在企业战略层面从上至下进行推动，通过建立组织架构，明确董事会、监事会、高级管理层及内设部门等职责要求，制定和实施系统化的制度、流程和方法，确保数据统一管理、高效运行，并在经营管理中充分发挥价值。

企业端数据治理整体框架通常包括四大关键环节：
- 数据战略：企业对数据治理的整体策略和方向；
- 数据资产盘点：明确企业数据的范围和分布；
- 数据规范：打破数据壁垒，实现数据互通和共享；
- 企业数据治理对三道防线：实现数据质量闭环管控。

公众：公众是数字经济的主要参与者。随着全球互联网渗透率的提高，商业世界中用户所产生的包含个人信息的数据也实现了几何级数的增长。同时，物联网环境下“无目的”的数据收集（如摄像头）也将远远超过“有目的”的数据收集。在一定意义上，数据自动化记录正在成为人类社会各类设施设备的基本属性之一，高度数据化正在成为个体生活环境的基本特征。在这一必然趋势下，对个人信息的判断及其保护机制，以及对时代发展与技术创新的影响，也有必要重新思考和认知。一方面，企业通过挖掘用户数据实现有效的用户画像，不断优化客户的购物和服务体验；但另一方面，个人信息在不断的被获取、存储、交易、利用，与之相关的数据泄露事件也可能发生，用户数据的产生和使用正在成为一种社会挑战。在健全个人信息保护相关法律的同时，加强对公众的信息保护教育和提高其自我保护意识、完善消费者数据维权渠道也十分重要。

政府：政府是数字经济的参与者、推动者，同时也是监管者。政府在数据大治理中可以发挥三个关键作用：第一，搭建共享平台，实现政府部门内部政务服务数据的互联互通和共享，提高政务服务效率和质量；第二，通过信息公开，合理、可控地将相关政府数据开放给社会公众，更好地挖掘数据的潜在价值，推动科技创新和数字经济发展；第三，完善重构政府数据治理制度体系，实现数据隐私保护和社会效益最大化之间的平衡。同时，数字经济时代的立法也应实现从监管到治理的转变。传统的互联网监管政策更多的是政府单方面的管理，而数据大治理强调多元化参与，不仅包括政府数据治理，也包括企业自律和消费者个人信息保护意识提高等等，政府、企业、公众三方协同配合，共同挖掘数据的价值。我们建议制定数据治理政策时可以参考如下四个原则：鼓励创新、开放包容、多方参与、协同治理。

最后，本文也探讨了衡量数据治理体系的一个指标体系框架。这个框架可以包含三大类指标：数据产业发展指标、个人信息保护指标、数据安全指标。我们将目前较为重要的考察指标分类列出，作为建立指标体系的初步探索，也希望能够为日后构建成熟指标体系提供一个初步的基础。

致辞

数字经济正在改变我们生活和工作的方方面面。数字经济的崛起推动了社会发展，不仅为消费者提供了更多的选择和便利，也促进了新的业态和经济模式的诞生。

蔓延全球的新冠肺炎疫情使全球经济面临重大挑战，生产、消费、贸易等活动受到显著影响，但疫情也为数字经济的发展提供了新的机遇。例如，大数据技术在疫情监测分析、病毒溯源、防控救治、资源调配等各个不同的场景中得到了充分的应用；智能手机上的“健康码”成为了帮助疫情防控的个人电子通行证，为推动企业健康合理的复工复产提供了便利；生鲜电商、在线教育、网络视频会议、线上医疗咨询、直播电商等数字经济新业态也正在改变传统的生产和消费习惯。

数据是数字经济的核心。对于企业而言，数据是企业重要的资产，拥有大量数据并能有效利用的企业将在竞争中获得优势。但随之而来的数据安全、隐私保护、数据真实性等诸多问题也不容忽视。因此，有效的数据治理不仅仅是企业必须高度重视的问题，数据治理的外部性也使其对社会和个人都有着深远的影响。

在此背景下，毕马威与阿里研究院结合各自的行业经验，在和相关专家和学者进行了深入研究的基础上，提出了“数据大治理生态体系”这一全新概念，将传统意义上企业端的数据治理上升到了社会层面，强调从顶层设计上明确各相关主体的权利和义务，在保护个人隐私和数据安全、挖掘数据价值、促进数字经济发展的多重目标之间达到平衡，从而实现社会效益的最大化和可持续发展。

数字经济的发展离不开有效的数据治理，如何治理日趋复杂的数据生态系统，确保在发挥数据潜力的基础上恰当地管理其风险，已经成为全球范围内政策制定者所面临的一大挑战。数字经济是新的经济模式，数据大治理也是需要不断深入研究的重要问题。我们希望和社会各界共同努力，共同探讨如何使数据这一重要的生产资料可以发挥出最大的价值，推动数字经济蓬勃发展。

陶匡淳
毕马威亚太区
及中国主席

致辞二

近年来，我国数据生产力继续保持高速发展，在技术突破、产业创新、引领传统产业转型等多个层面，都取得了显著进展。国家政策对此也给予了鼓励和支持：2019年，十九届四中全会首次将数据与劳动、资本、土地、知识、技术、管理等生产要素并列；2020年进一步提出要“加快培育数据要素市场。”

数据生产力的发展呼唤相应生产关系，也即数据治理的不断创新。当前的突出问题是：在相关研究和政策视野中，数据应用创新与数据治理创新未能实现平衡并重，而是存在割裂和偏颇。我认为，脱离数据应用创新的数据治理，将会缺乏活力和生命力。为有效讨论这一问题，我们需要回到周其仁先生所主张的“真实世界的经济学”，看看作为应用创新和治理创新标杆的互联网平台，已经取得了哪些进展。

面对千万级商家、近10亿消费者、数十亿同时在线商品动态变化的复杂商业生态系统，阿里巴巴运用大数据技术开展商业创新和协同治理成效显著。2019年，阿里平台上96%的疑似侵权链接一上线即被封杀，96%的知识产权投诉在24小时内被处理。每万笔交易疑似侵权商品量仅1.03笔，5年内下降67%。阿里巴巴的ET城市大脑，也在有效帮助政府用数据治理城市，“让城市会思考。”在杭州萧山区，信号灯自动配时路段的平均道路通行速度提升了15%；平均通行时间缩短3分钟；应急车辆到达时间节省50%，救援时间缩短7分钟以上。

阿里巴巴的数据应用及治理模式也已经在向社会开放，有效支持和赋能了多个领域治理效率的提高。2019年，阿里向全社会开放以“知识产权保护科技大脑”为代表的核心技术，与阿里联手围剿假货源头的区县执法机关达439个，协助抓获的制售假犯罪嫌疑人超过4000人。国家知识产权局发布的《中国电子商务知识产权发展研究报告（2019）》，第一次将“技术赋能+多元共治”的假货治理阿里模式作为中国经验、中国样本在全社会推广。阿里巴巴的“数据应用创新+数据治理创新”，是这个时代的先行样本之一。当前一项最迫切的工作，就是要深入研究更多的成功案例，系统总结、推广此类有效的模式和机制。

从更大范围来看，当前数据治理领域还存在着诸多值得重视的问题，如：在思维上试图为新技术“超前立法”，在领域上对个人信息和国家安全之外的企业创新关注不够，在制度设计上可能走向零和博弈、忽视了激励相容的可能性，在政策流程上对数据政策的经济社会后果评估不充分，在路径上看重国外法律、忽视我国国情等。

数字经济才刚刚开始，数据治理也必然要经过一个长时段的探索。面对这一领域很多“两难甚至是多难”的选择，我认为，秉承和践行“开放、分享、透明、责任”的新商业文明，应是一个基本共识，也是一把最为可行的标尺。

高红冰
阿里巴巴集团副总裁
阿里研究院院长

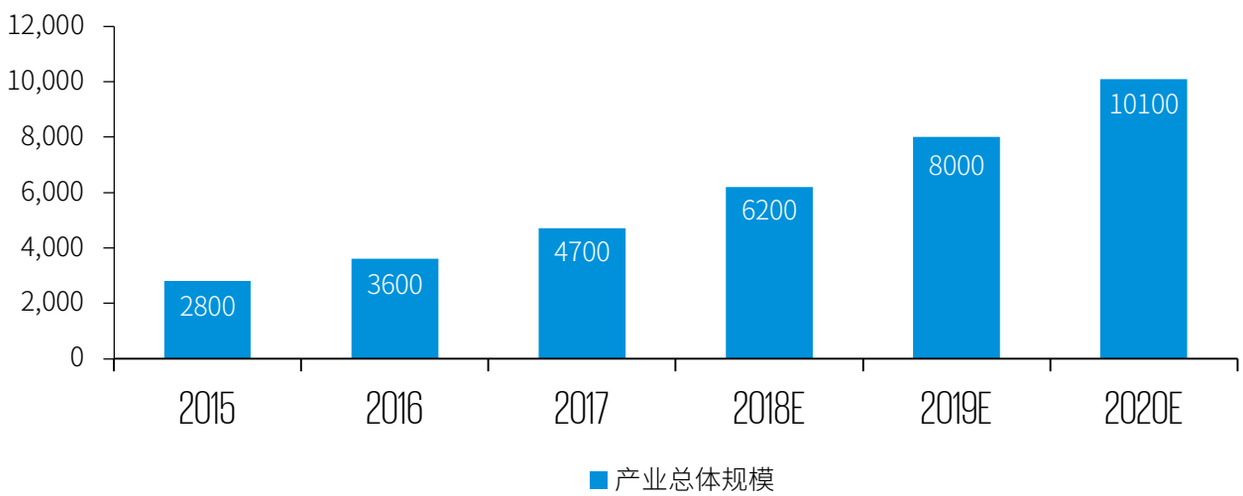
目录

1

构建“数据大治理”生态体系

当前，全球正处于大数据变革的新时代，移动互联网、智能终端、新型传感器快速渗透到地球的每一个角落。英特尔公司预计[1]，到2020年全球数据使用量将达到约44ZB（1ZB≈10万亿亿字节），涵盖经济社会发展的各个领域，仅中国产生的数据量就将达到8ZB，大约占据全球总数据量的五分之一。由此产生的革命性影响将重塑生产力发展模式，重构生产关系和组织方式，提升产业效率和管理水平，提高政府治理的精准性、高效性和预见性。

图1 中国大数据产业总体规模 （单位：亿元）



资料来源：中国信息通信研究院，毕马威

作为数字经济的核心生产要素，数据正成为经济转型和发展的新引擎，以及社会治理的有效工具。正是建立海量数据之上，大数据、云计算、人工智能等新技术、新产业才有可能实现颠覆性创新。此次新冠肺炎疫情的防控工作中，包括大数据分析和人工智能在内的高科技手段被广泛应用在疫情监测分析、病毒溯源、防控救治、资源调配等环节，效果显著，体现了大数据在公共卫生事件及社会治理中的重要性。

2017年工业和信息化部正式印发的《大数据产业发展规划（2016－2020年）》（以下简称《规划》），就提出要以“推动促进数据开放与共享、加强技术产品研发、深化应用创新为重点”；而同年开始正式实施的《网络安全法》也专设“网络安全支持和促进”一章，特别指出鼓励数据开放和利用，其第42条第1款还赋予了利用匿名化数据的自由，这一被称为“大数据条款”的规定为企业创新打开了大门。

1. “Increasing Data Needs Call for Innovative Storage Solutions”, Intel, https://www.intel.sg/content/www/xa/en/technology-provider/sales/storage/overview.html

数据大治理扩充了传统意义上的数据治理的内涵，从企业层面上升到社会层面，强调从顶层设计上明确各相关主体的权利和义务，既注重保护个人隐私和数据安全，又注重更好的挖掘数据价值、促进数字经济发展，从而实现社会效益的最大化和可持续发展。

我国现在正处于从传统产业型经济向以数字经济为代表的创新型经济转变的过程中，进一步鼓励数据的开放和利用是新经济发展不可或缺的必要条件；但与此同时，由于大量数据中包含有个人隐私及商业机密等敏感信息，一旦泄露将对个人或企业带来难以估量的伤害和损失，因此保护数据安全，降低数据风险也迫在眉睫。如何在两者间找到平衡，从而形成数据大治理这一可持续发展生态，则需要数字经济中最重要的三个参与主体，即作为消费者的个人、企业和政府在各司其职的基础上通力协作。

数据治理这一概念来源于企业端，主要以企业为对象，仅从一个组织的角度考虑大数据治理的相关问题，强调的是从企业的高级管理层及组织架构和职责入手，建立企业级的数据治理体系，自上而下推动数据相关工作在全企业范围的开展。但随着数据开放和流通技术及渠道的逐步完善，数据的跨组织乃至跨境流动和应用已经发生，并呈现出日益普及的趋势。我们需要意识到数据治理是涉及个人、企业、政府，行业内和跨行业，区域内和跨区域，全国乃至全球多个层次的问题，通过多层次的协同才能实现。

本报告中提出的数据大治理扩充了传统意义上的数据治理的内涵，从企业层面上升到社会层面，强调从顶层设计上明确各相关主体的权利和义务，既注重保护个人隐私和数据安全，又注重更好地挖掘数据价值、促进数字经济发展，从而实现社会效益的最大化和可持续发展。

由于参与主体众多且跨区域跨国，实现数据大治理可持续发展的生态体系具有**多物种、多角色、流动性**等几大特征。其中：

- 多物种是指这一体系中的参与者众多，既有企业、个人、政府等主体，也包含行业协会、产业联盟、消费者保护协会、媒体、智库、国际组织等机构在内的众多利益相关体。
- 多角色是指这一体系中的所有参与体都担任着不同的角色，各司其职同时又相互关联和支撑。
- 流动性是由数据的无形和流动性强等特点决定的。数据主权、数字经济已经成为包括欧盟以及美国在内的国际各方高度关注的全球性问题，各方立足自身实际情况和政策基准制定这一领域的数据治理规范，会对他国产生“规范溢出”的影响，同时数据也会自然流向合乎数据产业发展需求的国家和地区。

图2 数据大治理生态体系的主要参与者

资料来源：毕马威，阿里研究院

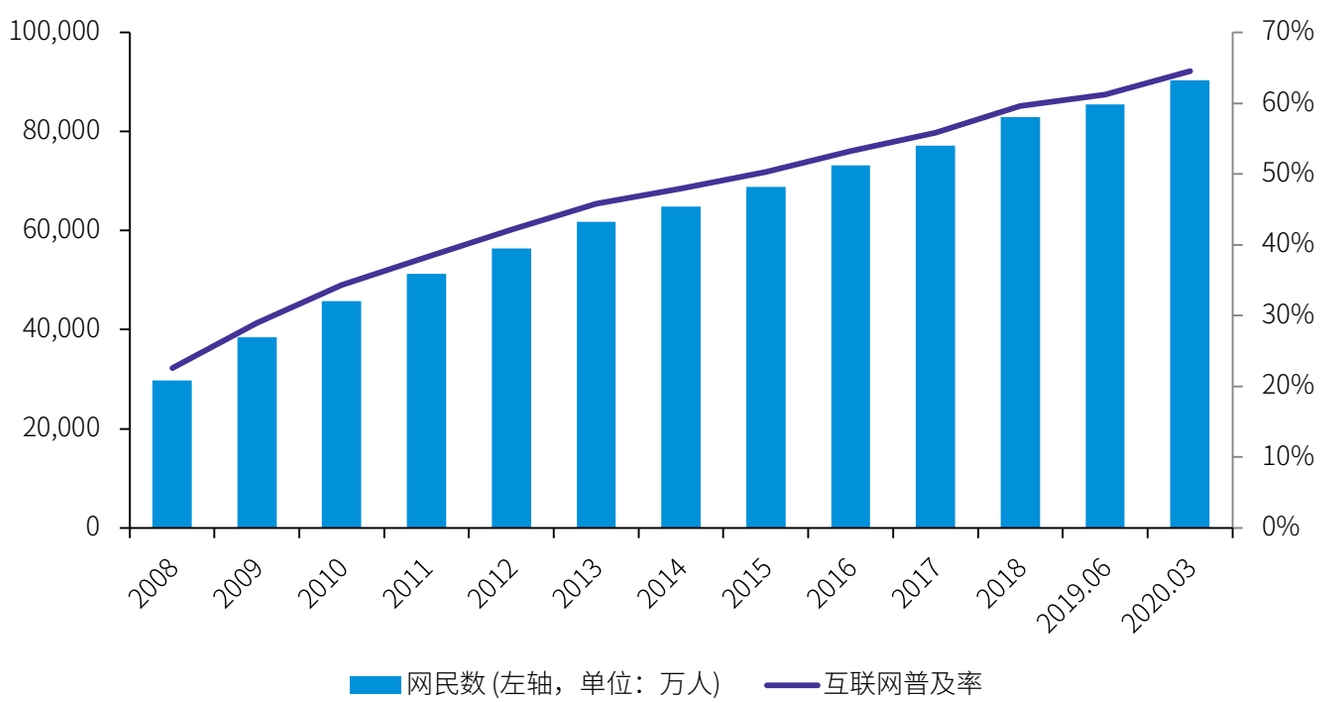
这一生态体系中企业、公众和政府是其中最主要的三大参与主体，其中：

企业是数字经济的核心推动者。目前世界范围内的几乎所有的行业都正在经历由大数据、人工智能（AI）等新兴技术推动所带来的产业升级，而科技企业更是这股产业升级浪潮中的佼佼者。据Wind数据显示，截至2020年5月，全球市值最大的十家公司中，苹果、微软、亚马逊、谷歌、阿里巴巴以及Facebook等互联网公司均名列前茅。

中国科技企业的快速壮大不仅引领了创新型数字经济的发展，同时也为整体经济注入了新的活力。据美国科技网站Techcruch的统计[2]，截至2019年11月7日，中国的独角兽企业数量已达180家，比2018年底增加了31家。科技企业的不断壮大也带动了数字经济在国家GDP总量中的比重。由中国信通院发布的2018年《G20国家数字经济发展研究报告》中显示，与2016年相比，G20国家数字经济总量持续扩大，由2.09万亿美元增加到26.17万亿美元，增长率高达8.64%，高于GDP增速约2.12个百分点。其中美国位于首位，总量达11.5万亿美元。中国位于第二，总量为4.02万亿美元。中国的数字经济GDP占比超过20%，同比增长幅度为G20国家之首，达2.51个百分点[3]。

公众是数字经济的主要参与者。根据中国互联网络信息中心在今年4月所发布的第45次《中国互联网络发展状况统计报告》显示，截至2020年3月，中国网民规模已达9.04亿，互联网普及率高达64.5%，其中手机网民规模达8.97亿， 移动上网率达到99.3%。

图3 中国网民规模和互联网普及率



数据来源：中国互联网络信息中心（CNNIC）,毕马威分析

2. Techcruch Unicorn Leaderboard, updated on November 7, https://techcrunch.com/unicorn-leaderboard/?renderMode=ie113.
3. 中国信息通信研究院，《G20国家数字经济发展研究报告》（2018年），2018年12月

蓬勃发展的数字经济一方面使得作为数据主体的个人用户享受到了无以伦比的便捷服务，生活质量得到了大幅度的改善；但另一方面，个人信息不断的被获取、存储、使用、交换，与之相关的数据泄露事件时有发生，用户数据和隐私的合理保护正在成为一种社会挑战。

由于我国目前在个人信息保护方面的立法还不完善，因此加强对个人用户的信息保护教育和提高其自我保护意识就显得尤为重要。个人用户只有在感觉到自己的隐私信息和人身财产是安全的情况下才能激发其作为数字经济主体的主观能动性，促进消费的增长。

政府是数字经济的参与者、推动者，同时也是监管者。数字经济时代的大数据、云计算、区块链、人工智能等新兴技术的蓬勃发展，为数字政府的构建奠定了坚实的技术基础，使得数字政府的内涵正在以“网上政务”为核心的1.0时代，迈向以“数据化运营”为核心的2.0时代，通过业务中台和数据中台的建设，实现政府内部系统的打通和数据协同，极大提高了政务服务的效率和质量。

数字经济时代，数据已成为驱动经济发展和技术创新的国家基础性战略资源，成为衡量一个国家竞争力的重要标志。因此，政府数据开放成为全球普遍趋势，很多国家开始制定专门的数据开放法。李克强总理曾指出“中国超过80%的信息数据资源掌握在各级政府手中[4]”，对这部分政府数据的开放和利用，可以极大地释放数据能量，创造公共价值。近年来，中国出台了一系列政府数据开放相关的政策措施，例如，2015年国务院印发《促进大数据发展行动纲要》，对推进政府数据开放起到积极作用。但是，我国仍然缺乏开放政府数据的专门立法。未来，我们建议可借鉴美国等国际经验，建立统一的国家级政府数据开放平台，助推我国数字经济高质量发展。

行业协会和产业联盟等主要作为政府和企业之间的桥梁，在国家法规和政策的指导下，制定并执行行规行约和各类标准，监督企业的行为，并向政府传递共同需求。

4.《李克强：信息数据“深藏闺中”是极大浪费》，北京日报，2016年5月

由于数字经济属于全新的经济形态，是对生产方式和社会分工方式的重新定义，因此目前各国对于数据治理和数据安全领域的立法都还处于摸索状态。以目前对于个人信息安全立法最严格的欧盟GDPR为例，其实施以来尽管在个人信息保护及提升民众对个人数据保护权的认识方面颇有建树，但是也显著的提高了企业的合规成本，对于创新型初创公司的发展有所阻碍[5]。中国目前正在制定个人信息保护法和数据安全法。其中个人信息保护法是关于个人信息保护的基本法，数据安全法是按照总体国家安全观要求，在数据安全领域的基础性规定，侧重于国家安全。在立法过程中所面临的最大挑战莫过于如何重新定位和统一定位个人信息属性和保护的模式，既保护个人的权利，又促进整个数字经济的发展。

综上所述，要建立数据大治理这一可持续发展的数字经济生态需要政府在立法和规则方面形成统一的顶层设计体系，这一体系一方面需要在正确引导企业进行数据合规的同时不断激发其在创新方面的积极性，另一方面需要通过加强个人信息的安全保护从而加强作为个人用户的公众对数字经济的参与体验。

5. “The Short-Run Effects of GDPR on Technology Venture Investment”，Jian Jia, Ginger Zhe Jin, Liad Wagman, November 2018, https://www.nber.org/papers/w25248

2

主要国家数据安全立法比较

受2018年开始实施的欧盟《通用数据保护条例》的影响，个人隐私的保护已引起了各国政府和民众的高度重视，不少国家和地区都逐步加强了数据保护的法律监管措施。截至2018年底，全球已有近120个国家和独立的司法管辖区采用了全面的数据保护或隐私法律来保护个人数据，另有近40个国家和司法管辖区存在有待批准的此类法案或倡议。通过对包括欧盟、美国、韩国、日本及中国等主要国家的数据安全和治理立法实践的比较，我们不难看出如何保护个人信息和平衡数据治理中的各方利益已成为现代社会所面临的挑战，成为了全球性的法律问题。了解全球范围内的立法趋势对于引导中国公民权利意识，规范政府和社会行为，平衡各方利益都具有重要意义和作用。

2.1 欧盟

> 了解全球范围内的立法趋势对于引导中国公民权利意识，规范政府和社会行为，平衡各方利益都具有重要意义和作用。

GDPR实施基本情况

欧盟的《通用数据保护条例》（General Data Protection Regulation，简称GDPR）自2018年5月25日起在欧盟成员国内正式生效实施，如今法规实施已两年有余。

2020年6月22日，欧盟数据保护委员会发布了关于GDPR实施两周年以来的评估报告[6]，特别对于GDPR在跨境数据转移、合作和一致性机制的执行和实施情况做了阶段性的总结与回顾。 报告提出，GDPR实施两周年后，成功实现了加强保护个人数据保护权和保障个人数据在欧盟内部自由流动的目标，但也发现了一些未来需要进一步改进的领域。这些需要进一步改进的领域包括：

- 各成员国在数据保护领域所投入资源的不平衡导致相互合作和一站式执法机制的推行还存在不理想的情况；
- 中小企业实施GDPR仍面临挑战，需要相关机构的进一步协助；
- 进一步鼓励创新，同时监测GDPR的实施对新技术的应用是否有任何阻碍作用；
- 促进和支持欧洲和国际监管机构间的交流与合作。

6. Communication from the commission to the European Parliament and the Council – Data protection as the pillar of citizen’ s empowerment and the EU’ s approach to digital transition – two years of application of GDPR, June 22, 2020.

影响

GDPR在根本上改变了欧盟，甚至欧盟以外的个人信息保护和数字经济发展的面貌，这一具有里程碑意义的隐私和数据安全监管法规对个人、企业、产业等均产生了不同程度的影响。

表1 GDPR实施后在个人用户、企业和产业层面产生的影响

层级	正面影响	数据或实例	负面影响	数据或实例
用户	1、增强了公民对个人数据保护权的认识。[7]	调查显示欧盟公民中有67%表示他们已经听说过GDPR，其中36%的人表示他们非常了解GDPR的含义。此外，接受调查的57%的欧盟公民表示，他们知道该国存在负责保护其数据权利的公共机构。该结果表明，与2015年的欧盟民调（Eurobarometer）相比，增长了20个百分点。	1、GDPR未能增加用户的信任。	据欧盟委员会的调查，GDPR生效六个月后，消费者对互联网的信任度达到十年来的最低点。
			2、GDPR对用户的在线访问产生负面影响。	GDPR出台后，美国主流新闻网站，包括《洛杉矶时报》和《纽约日报》等，都处于被封锁状态，无法被欧洲读者看到，一些网站开始要求欧盟用户同意新的使用条款。
	2、消费者能够享受更快捷的服务。	例如，《今日美国报》为欧洲用户提供了一个完全没有广告，没有Cookies跟踪，甚至不含有任何JavaScript代码的极简版面，加载速度十分迅速。	3、GDPR过于复杂，消费者无法理解。	调查显示，在数字文化普及度较高的爱沙尼亚，有71%的人口从未听说过GDPR或不知道它到底是什么。
	3、用户对数据有了更大的控制权。	根据GDPR的规定，用户享有数据访问权、被遗忘权、限制处理权、数据携带权等权利。	4、GDPR对用户数据权益保障程度有限。[8]	调查显示，仅有5%的用户阅读了巨头企业近期更新的隐私政策。

7. “1 year GDPR – taking stock”， European Data Protection Board， May 2019，https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en
8. “What the Evidence Shows About the Impact of the GDPR After One Year”，Center for Data Innovation，June 2019，https://www.datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/

层级	正面影响	数据或实例	负面影响	数据或实例
企业	1、合规企业遭遇隐私泄露的概率更低、损失更小。[9]	数据泄露频率更低（74%对比 89%），发生泄露时，其受影响的数据记录数量更少（79，000 条记录对比212，000 条记录），系统停机时间更短（6.4 小时对比 9.4 小时）	1、GDPR对欧洲新兴科创企业有很大负面影响[11]。	• GDPR使新企业每周减少90万美元投资。 • GDPR使新兴、年轻和成长阶段企业每笔交易融资额分别缩水27.1%、31.4%和77.3%。
	2、促进企业销售收入增长。	相比那些尚未实现 GDPR 合规的组织，合规企业因客户的数据隐私顾虑而导致的销售周期延迟更短（3.4 周对比 5.4 周 ）	2、GDPR过于复杂，企业无法实施。	根据2018年10月对数据保护专业人员进行的一项调查，约五分之一(19%)的受访者表示，完全遵守GDPR是不可能的。
	3、增强员工忠诚度。[10]	当员工相信自己的雇主在保护他们的个人数据时，他们能以更高的忠诚度和良好的口碑回报他们的雇主。	3、GDPR的实施将显著提高企业的合规成本。	为适应新规的要求，欧盟相关企业的运营成本共将提升2000亿欧元，而美国企业则需要多投入约417亿欧元。[12]
产业	1、GDPR带动了隐私合规产业链的发展。	一些云服务公司正在帮助企业级用户和伙伴满足GDPR的合规要求，提高防范黑客攻击的能力等。	1、GDPR削弱了欧洲数字广告行业的竞争力。	数字广告供应商在欧盟的市场份额遭受损失，尤其是规模较小的广告商，其在2018年4月至7月之间失去了18%~31%的市场份额。[13]
	2、推动全球数据安全和个人信息保护立法。	随着GDPR的生效，巴西、日本等国家都通过并颁布了与之类似的隐私法律，印度正在积极地制定有关法律。在GDPR的影响下，美国加利福尼亚州新的隐私法律也已在2020年生效。	2、GDPR的实施阻碍云计算、人工智能、区块链等新兴产业的发展。	• GDPR所要求的算法透明和负责及其导致的数据类型和数量的下降，为人工智能的准确度和创新带来挑战。 • 区块链方面也同样面临着挑战。分布式、去中心化的区块链系统，尤其是公有链体系，其具有数据透明且不可篡改的特性，同GDPR中心化的规范方式存在冲突。

资料来源：网络公开信息收集，毕马威，阿里研究院

9. “Cisco 2019 Data Privacy Benchmark Study”，Cisco，January 2019, https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1963564
10. “Seizing the GDPR Advantage From mandate to high-value opportunity”，Capgemini Digital Transformation Institute，May 2018, https://www.capgemini.com/wp-content/uploads/2018/05/seizing-the-gdpr-advantage4.pdf
11. 《GDPR对科技创业投资的短期影响》，美国国家经济研究局（NBER），2018年12月。
12. 《“最严”条例“严”在哪里》，人民日报，2018年6月

GDPR对欧盟境外的企业也产生了深远的影响。GDPR采用了类似于此前美国长臂管辖的法律模式，将执法边界延伸到了所有收集欧盟公民信息的企业，对互联网产业相对发达的中美两国企业影响尤甚[14]。自2016年4月GDPR被通过以后，欧盟给了各方两年的缓冲期。欧盟内企业关于GDPR合规的意识普遍较强，甚至有不少企业已经为GDPR付出了较大的财务、管理成本，相比之下，欧洲之外的企业行动相对迟缓。例如Spiceworks在GDPR实施前两周针对企业合规情况进行了调查，结果显示，61%的英国公司表示他们在截止日期前已经或即将完全符合GDPR的合规要求，欧盟其他国家该比率为46%。与此同时，受新法规影响的美国公司中，只有25%的机构表示会在GDPR生效前做好合规的准备[15]。

如今，GDPR正在推动全球隐私保护立法进程，且已经成为全球很多国家和地区进行个人数据保护立法时所参考的对象。在数据政策制定方面，外界关注的焦点普遍集中在如何在加强数据监管与促进数字经济发展之间取得平衡，这也是众多互联网企业，特别是中小科技企业的诉求。在加强数据隐私保护监管的同时，如何增强客户体验、改善中小企业生存环境、为数字产业的发展提供松紧适度的政策条件，是值得全球各国数字政策制定者思考的问题。

除了GDPR之外，关于数据治理，欧盟也通过了《非个人数据自由流动条例》，致力于促进非个人数据在欧盟境内的自由流动，欧盟各国在国内亦都建立了针对政府、企业、个人等多元主体数据治理的相应法规体系，构建出多元化、多层次的数据治理规范体系。

13. “What the Evidence Shows About the Impact of the GDPR After One Year", Center for Data Innovation, June 2019, https://www.datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/
14. 《史上最严数据保护法案GDPR正式生效“长臂管辖”颠覆既有商业模式》，中国经营网，2018年6月， http://www.cb.com.cn/zjssb/2018_0601/1238511.html
15. 《GDPR实施百天后，英国数据官员如何评价？》，APUS研究院， 2018年9月

2.2 美国

与欧盟统一立法模式不同，美国并未在联邦层面制定统一的数据隐私保护基本法，而是采取了分行业式的分散立法模式，形成了针对金融、征信、医疗、电信、教育以及儿童在线隐私等若干领域的个人隐私保护立法体系[16]。

在州层面，美国各州亦形成了各自的数据保护法律框架。目前，各州均已制定了应对数据泄露的立法，一些州也出台了不同类型的消费者保护立法。其中，2018年6月加利福尼亚州通过的《2018加州消费者隐私保护法》（California Consumer Privacy Act，简称CCPA）备受关注，这项法案被称为全美最严厉、最全面的个人隐私保护法案，已于2020年1月1日生效，其在数据主体权利、数据泄露的预防和问责机制等方面受到GDPR的影响。根据法案，从2020年开始，用户有权查阅自己被收集的数据，要求删除数据，以及选择不将数据出售给第三方。CCPA对中小微企业更加友好，只有满足年度总收入超过2500万美元或者出售个人信息的收入超过年度总收入50%等一系列条件的企业才需遵守该法案。另外，CCPA中没有数据跨境方面的限制，相较于欧盟的GDPR，其更鼓励个人信息的商业流通。美国鼓励数据流动的背后，是源于其高度发达的数字产业，加州是硅谷所在地，是全球科技、互联网及相关新兴产业发展的开创者和引领者，聚集了众多高新技术中小公司，同时又拥有谷歌、Facebook、惠普、英特尔、苹果公司等大科技公司，是全球数据流向地。许多企业都从加州消费者中收集大量的个人信息，消费者向企业分享的个人信息也在不断增加，数据对产业的发展至关重要。

针对数据跨境问题，2018年3月23日，美国参议院通过《澄清境外数据合法使用法案》（Clarifying Lawful Overseas Use of Data Act，简称CLOUD），并于当日生效，该法案旨在解决云计算时代跨境执法请求引发的数据争端问题，其一改之前的“数据存储地标准”，转而采用“数据控制者标准”，规定无论通信、记录或其他信息是否存储在美国境内，数据控制者均有义务遵循美国的强制性命令向其提供。

16. “Data Protection Law: An Overview”， The Congressional Research Service， March 2019，https://crsreports.congress.gov/product/pdf/R/R45631

2.3 日本

日本《个人信息保护法》（The Act on the Protection of Personal Information（57/2003））于2005年4月1日起施行。随着信息技术的急速发展和个人信息不断外延拓展，该法于2015年进行了大幅修正，最新修订法案于2017年5月30日起施行。修正案在立法目的中增加了“在对个人权利利益加以保护的同时，还考虑到个人信息正确且有效的使用有助于增加经济产出、创造有活力的经济社会、丰富国民生活及其他有用之处”，对个人信息的社会价值予以肯定。

法案还增设日本个人信息保护委员会（Personal Information Protection Commission，简称PPC）作为日本个人信息处理从业者的专门监管机构，PPC以《个人信息保护法》为法律依据，确立了“保护个人权益利益，兼顾个人信息有用性”的指导原则，行业自治同国家统一立法并行不悖。此外，就境外个人信息的处理，修正案引入了相关限制措施[17]。《个人信息保护法》在日本隐私权行政法规保护方面居于绝对的核心地位，对日本国民隐私起到重要的保护作用。除顶层的《个人信息保护法》外，日本的个人信息保护制度规定根据团体、组织的性质，分别适用不同的法律关系，并且在信用、医疗、电信、教育等领域制定专门法。

2019年4月25日，日本个人信息保护委员会发布了《个人信息保护法》修正案中期汇总。此次中期汇总新增企业停发广告义务，即在个人要求企业停止将收集的地址和姓名等个人信息用于广告时，企业有义务同意。

17. 根据现行法第24条的规定，原则上，未经本人同意，个人信息处理业者不可以向在海外的第三人提供个人数据，但在“该第三人所在国家是个人信息保护委员会规则承认的，作为在保护个人权益方面设立有与日本水平线相当的个人信息保护制度”的情形中，以及该第三人完善体制符合个人信息保护委员会规定的标准或符合现行法第23条中的具体情形下，可以向海外的第三人提供该个人数据。

2.4 韩国

在个人信息及数据保护法律领域，韩国形成了《个人信息保护法》，《信息通信网利用促进及信息保护法》及《信用信息的利用及保护法》三法分立的局面，相关职能分别归属于个人信息保护委员会、广播通信委员会与韩国网络振兴院。在信息技术产业保护立法方面，韩国拥有包括《信息保护产业振兴法》，《云计算发展及用户保护法》及《大数据利用及产业振兴法(议案)》等一系列法律规定。

2018年9月18日，韩国对《信息通信网络的利用促进和信息保护等相关法》进行了部分修订，建立国际企业的个人信息保护和跨境传输相关新规则。修正案设置国内代理人制度，规定在韩国内没有地址或营业场所的信息通信服务提供者，在符合相关规定后，应当指定在韩国国内有地址或营业场所的人作为其代理人代理进行相关事项。对于国际公司个人数据跨境传输问题，修订要求信息通信服务提供者事先告知用户个人信息转移接受者相关事项、获得用户同意、并采取保护措施等。

2.5 中国

作为数字经济大国，我国也正在积极建立和完善个人信息保护立法。目前，我国有《刑法》、《民法典》、《民法总则》、《消费者权益保护法》、《网络安全法》、《电子商务法》等多部法律、法规和规章涉及个人信息保护，不过，不同于世界上的大多数国家，我国并未制定统一的个人信息保护专门法。在个人信息保护领域，我国采用分散立法的模式，立法体系由法律、法规、规章以及各类规范性文件等共同组成，形成多层次、多领域、内容分散、结构复杂的个人信息保护法律体系。

表2 中国个人信息保护的基本法律规范框架

时间	法律法规	相关内容
2012年12月	《全国人民代表大会常务委员会关于加强网络信息保护的决定》	首次以法律文件的形式对个人电子信息保护的要求做了明确规定。
2013年7月	《电信和互联网用户个人信息保护规定》	具体规定了电信业务经营者、互联网信息服务提供者收集、使用用户个人信息的规则和信息安全保障措施等要求。
2016年11月	《网络安全法》	将个人信息保护纳入网络安全保护的范畴，其第四章“网络信息安全”对个人信息保护作了专章规定。
2017年3月	《民法总则》	在民事基本法的层面确立了个人信息保护条款。
2017年5月	《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》	对侵犯公民个人信息犯罪的定罪量刑标准和有关法律适用问题作了全面、系统的规定。
2017年12月	《信息安全技术个人信息安全规范》	以国家标准的形式，明确了个人信息的收集、保存、使用、共享的合规要求。
2018年8月	《电子商务法》	中国第一部全面针对电子商务的成文条款。
2019年1月	《关于开展App违法违规收集使用个人信息专项治理的公告》	由中央网信办、工信部、公安部、市场监管总局等四部门联合，将重点开展个人信息收集和使用情况评估、监管和处罚、打击违法犯罪、APP安全认证四个方面的工作。
2019年8月	《儿童个人信息网络保护规定》	这是我国第一部专门针对儿童网络保护的立法，具有里程碑意义。《规定》对儿童个人信息进行全生命周期保护，包括收集、存储、使用、转移、披露、删除等环节。
2019年11月	《App违法违规收集使用个人信息行为认定方法》	四部委联合发布，旨在规范监管部门对App违法收集使用个人信息行为的认定，也为企业合法收集使用个人信息提供参考。
2020年5月	《民法典》《民法典人格权编》	专章规定了隐私权和个人信息。明确强调自然人享有隐私权，自然人的个人信息受法律保护，处理个人信息的应当遵循合法、正当、必要原则。
2020年6月	《数据安全法》	全国人大进行一审

资料来源：网络公开信息收集，毕马威，阿里研究院

中国有近40部法律、30余部法规涉及个人信息保护[18]，其中最具有代表性同时最受关注的是自2017年6月1日起施行的《中华人民共和国网络安全法》（People’s Republic of China Network Security Law，以下简称《网络安全法》），自2019年1月1日起施行的《电子商务法》（Electronic Commerce Law），以及将于2021年1月1日开始实施的《中华人民共和国民法典》。

《网络安全法》是我国第一部全面规范网络空间管辖的基础性法律，也是国家网络空间安全保障工作的总纲领，在我国网络安全立法领域具有里程碑意义。该法开创性地新设了相关制度，如针对网络产品服务提供者信息泄露、毁损、丢失时的告知和报告制度，针对关键信息基础设施运营者，明确了信息境内留存原则及安全评估原则。

《民法典人格权编》专章规定了隐私权和个人信息，明确强调自然人享有隐私权，自然人的个人信息受法律保护，处理个人信息的应当遵循合法、正当、必要原则。同时，明确了行为人合理利用自然人个人信息的范畴，包括在自然人或者其监护人同意的范围内合理实施的行为，合理处理该自然人自行公开的或者其他已经合法公开的信息，为维护公共利益或者该自然人合法权益，合理实施的行为等。

我国也正在积极制定针对个人信息保护、数据安全的专项法律。2019年1月25日，中央网信办、工信部、公安部、市场监管总局等四部门联合发布《关于开展App违法违规收集使用个人信息专项治理的公告》。该专项治理将重点开展以下工作：一是组织相关专业机构，对用户数量大、与民众生活密切相关的App隐私政策和个人信息收集使用情况进行评估。二是加强对违法违规收集使用个人信息行为的监管和处罚，包括责令有关App运营者限期整改；逾期不改的，公开曝光；情节严重的，依法暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。三是公安机关开展打击整治网络侵犯公民个人信息违法犯罪专项工作，依法严厉打击针对和利用个人信息的违法犯罪行为。四是开展自愿性App个人信息安全认证，鼓励搜索引擎、应用商店等明确标识并优先推荐通过认证的App。

18. 《拧紧个人信息保护阀》，新华社，2019年1月18日，http://www.xinhuanet.com/politics/2019-01/18/c_1124006435.htm

2019年11月，国家互联网信息办公室、工业和信息化部、公安部、市场监管总局等四部委联合制定了《App违法违规收集使用个人信息行为认定方法》。该办法对于“未公开收集使用规则”、“未明示收集使用个人信息的目的、方式和范围”、“未经用户同意收集使用个人信息”、“违反必要原则，收集与其提供的服务无关的个人信息”、“未经同意向他人提供个人信息”、“未按法律规定提供删除或更正个人信息功能”或“未公布投诉、举报方式等信息”等六大类违规收集行为划定了具体的范畴，为监督管理部门认定App违法违规收集使用个人信息行为提供了参考，为App运营者自查自纠和网民社会监督提供了指引。

而备受各方关注的《个人信息保护法》在2018年就被列入十三届全国人大常委会立法规划，目前法工委正在会同有关部门研究论证，加紧推进《个人信息保护法》的起草工作，将按照立法工作计划，适时提请常委会审议。

3

企业端的数据治理

数据已成为企业的核心资产和重要战略资源，是重要的生产因素。在数据驱动的数字时代，企业只有将核心业务数据更好地掌握在手中，才能从中萃取更大的业务价值，进而优化产品管理，拓展市场新渠道，打造企业核心竞争力，而数据治理就是挖掘这些价值的重要手段和工具。

3.1 数据治理是企业公司治理的组成部分

企业的数据治理指的是企业对所拥有的数据资产的治理。但是，并非企业所拥有的所有数据都能被称为数据资产，只有其中关乎重大商业利益的数据资源才是数据治理的对象。重要的数据资源可以为企业带来显著的商业利润，因此这些数据资产也是企业公司资产的重要组成部分。因此，企业对数据资产的治理也可以被看作是公司治理的一部分，公司治理中出现的典型问题，在数据治理中也通常会出现。例如，在公司治理中常常会出现的资产所有者和实际经营者相分离的问题在数据治理中也很普遍。数据资产的所有者和实际使用经营者通常不是同一个主体，而且其权属问题也一直存在争议。

表3 公司治理与数据治理的比较

	公司治理	数据治理
目的	保护和协调公司与各个利益相关体之间的利益关系	属于公司治理的范畴，实现数据相关利益主体的价值与风险平衡
职能	通过一整套程序、体系、制度，规范权利和责任，监督、制衡公司经营者，维护股东利益	规范数据权利和责任体系，指导与监督数据管理与运营处于正确轨道
组织	股东会、董事会、监事会、各专业委员会	股东会、董事会、监事会、各专业委员会、数据治理委员会
实施依据	公司法、公司章程	数据治理原则及数据战略
政府职能	制定法律法规，通过直接或间接手段指导和监督	制定法律法规，监督个人隐私与数据安全得到合理的保护
直接实施者	董事会	董事会和数据治理委员会

资料来源：网络公开资料整理，毕马威分析

与公司治理相似，数据治理也需要在企业战略层面从上至下进行推动，通过建立组织架构，明确董事会、监事会、高级管理层及内设部门等职责要求，制定和实施系统化的制度、流程和方法，确保数据统一管理、高效运行，并在经营管理中充分发挥价值的动态过程。例如，2018年5月21日中国银行保险监督管理委员会正式发布了《银行业金融机构数据治理指引》，要求银行业金融机构应当将数据治理纳入公司治理范畴，建立自上而下、协调一致的数据治理体系；并根据数据治理情况评价公司治理水平，甚至与监管评级挂钩。

3.2 企业数据治理的关键环节

《银行业金融机构数据治理指引》的颁布实施使商业银行的数据治理工作有了明确的规范和依据。对于没有监管机构的行业，大部分企业会参考行业通用实践框架，如《数据管理能力成熟度评估模型》（Data Management Capability Maturity Assessment Model, 简称DCMM），构建企业端数据治理整体框架。这个框架通常包括以下关键环节：

- **数据战略：**企业端数据治理的整体策略和方向
- **数据资产盘点：**数据治理工作的先行任务，明确企业数据的范围和分布
- **数据规范：**打破数据壁垒，实现数据互通和共享
- **企业数据治理三道防线：**实现数据质量闭环管控

3.2.1 数据战略——引领企业数据治理方向

在全球信息化快速发展的大背景下，数字化转型已经各家企业面临的最为迫切的任务之一，而数据战略的制定是数字化转型工作开展的首要工作，也是最为重要的工作，数据战略是组织开展数据工作的愿景、目的、目标和原则，是组织开展各项数据相关工作的宗旨和指引，同时也引领了企业数据治理的方向。通常企业在制定数据战略时会首要明确数据战略规划，即明确企业数据管理的愿景和目标，为了保证数据战略目标的可执行可落地，会结合现状与愿景之间的差距分析制定战略任务，并明确实施路径。同时在后续要进行定量和定性的衡量，回顾和考核数据战略任务的完成情况。

以银行业为例，现如今全球银行业已经全面步入数字化时代，领先银行纷纷实施数据化创新战略，在过去的五年中，围绕着数字化、大数据、金融科技、敏捷银行、开放银行和生态圈六个领域，国内外银行纷纷开启探索之旅。例如，国内某大型国有商业银行着眼于集团跨境、跨业、跨界转型发展，在高起点上推进智慧银行建设，制定了“智慧银行ECOS工程”战略。其中，E是Enterprise-level，代表“企业级”，寓意银行立足全集团视角，构建产品整合、信息共享、流程联动、渠道协同的新体系，给客户带来更好的一站式体验。C是Customer-centred，代表“以客户为中心”，体现出银行“客户至上”的服务理念，不仅是“客户身边的银行”，而且是“客户心中的银行”。O是Open，代表“开放融合”，银行适应金融生活化、场景化趋势，以自有融e行、融e联、融e购“三融”平台为基石，以API开放平台和金融生态云平台为跨界合作抓手，积极打造开放、合作、共赢的金融生态圈。S是Smart，代表“智慧智能”，布局人工智能、区块链、云计算、大数据、物联网等前沿技术领域，为客户服务、精准营销、风险控制、决策管理等提供“最强大脑”，为银行转型创新带来强大动力。

3.2.2 数据资产盘点——数据治理先行任务

数据资产盘点工作是数据治理的先行任务，数据资产盘点旨在解决“有什么”（数据资产）的问题，为后续“用什么”（数据资产）、“如何用”（数据资产）奠定基础。数据资产盘点工作的工作目标主要有四点，一是通过对关键系统关键数据资源的梳理，形成企业数据资产目录；二是通过数据资产盘点，推进企业数据整合共享以及相关标准化工作；三是分析总结企业数据资产现状及问题，开展治理工作，提升数据质量；四是以体现数据价值为目标，推进数据资产使用，实现数据价值最大化。经过众多项目的实践总结，毕马威认为数据资产盘点工作可以遵循“盘”、“规”、“治”、“用”的工作思路开展。

表4 数据资产盘点工作的具体步骤

“盘”	从企业现有业务系统和数据出发，盘点数据资产，在该项工作中主要解决“要什么”、“有什么”和“在哪里”这三个问题，形成企业数据资产框架和数据资产目录，支持建立全面覆盖的企业级数据资产地图。
“规”	基于公司数据规范，明确数据管理目标，以目标为导向，识别“规范性差距”。 “规范性差距”从四方面进行识别， • 范围差距：从业务价值、同业输入的角度，识别企业数据资产的“缺口”； • 标准化差距：数据资产是否存在不满足行业数据标准的情况； • 质量差距：数据资产是否满足质量管控要求； • 自动化差距：是否存在手工数据。
“治”	基于“规范性差距”，结合数据管理的现状，建立数据质量提升规划，开展数据质量提升。
“用”	规划设计应用模式，应用场景，解决数据“价值实现”的目的。

资料来源：毕马威分析

3.2.3 数据规范——打通数据壁垒，加强数据共享

数据规范是指针对企业所拥有的不同的数据类别，制定相应需要遵守的标准要求。如同字典，数据规范有数据的明确解释与定义，它可以使不同行业、不同背景的人对一个事物有相同的认识，是有效沟通交流的基础；如同交通规则，为了使数据的交互、整合、使用更加流畅，数据间的问题和冲突大大减少，所有数据都应遵循一个统一的标准体系，数据规范是数据共享和使用基石。

目前大多数企业的系统建设为“烟囱式”，各个系统如同烟筒一样独立支持业务应用，仅在功能层面有少许交互，而企业未建立统一的数据汇总、整合平台，导致各个系统之间的数据壁垒严重，数据无法释放价值。以银行业为例，在受理信用卡业务时使用的信用卡系统与银行常规存款贷款业务使用的核心系统相对独立。某银行核心系统在新建客户时，需录入客户的“学历”信息，根据国家标准，学历为“代码类”，有研究生教育、博士研究生毕业、博士研究生结业、博士研究生肄业等40个码值；而客户申请信用卡时，信用卡系统也需采集客户的“学历”信息，信用卡系统的学历也为“代码类”，但仅有初中以下、高中/职高、大学专科/高职学院、大学本科、研究生及以上5个码值。核心系统与银行卡系统对于学历的定义不同，对应的码值不同，造成在整合过程中，由于无统一的数据规范，“学历”数据的信息缺失严重。

为避免因未开展数据规范造成的不良影响，可从以下两点入手：

第一，企业应建立统一的、权威的数据规范——数据标准。数据标准从业务属性、技术属性和管理属性三方面定义了数据分类、数据标准名称、业务定义、取值范围、数据类型、数据长度、数据定义部门等内容，阐明了数据“应该是什么”的问题。

第二，企业应将数据标准落实系统开发中，保证新系统中产生的数据都满足数据规范要求，具体的流程包括：在需求提出阶段审查数据需求是否符合数据标准要求；在需求设计及系统开发阶段严格遵守数据标准进行系统设计及开发；在测试阶段纳入数据规范测试，检查数据规范的落实情况；通过以上机制，从技术流程控制角度，保证了新建系统中的数据满足规范要求。针对已有系统中不满足数据标准的情况，应适时开展系统改造，在系统层面落地数据标准，保证已有系统增量数据的规范性；对于存量数据，可根据需要进行存量数据的专项整改。

例如，对于前文“学历”数据标准不一致现象，应建立对应的数据标准，明确学历的业务定义，即“受教育者在教育机构接受科学、文化知识训练并获得国家教育行政部门认可的学历证书的经历”；结合国家标准、行业标准、业务要求等方面内容，确定“学历”的取值范围；根据开发阶段的技术需要，定义“学历”的数据类型和数据长度内容等。若定义“学历”遵循国家标准，那么银行卡系统的“学历”就不符合标准，为“问题数据”，企业应及时推动银行卡系统开展落标的系统整改工作，最终实现核心系统与银行卡系统都遵循“学历”的数据标准要求，有相同的40个码值，从而打破了数据整合交互过程中障碍。

3.2.4 构建数据治理三道防线，实现数据闭环管控

“数据治理三道防线”是数据管理的组织架构，是数据管理全面化、体系化的具体体现。越来越多的领先企业认可“三道防线”是数据治理架构的最佳实践。

“三道防线”中的第一道防线为业务管理条线，主要负责本业务管理条线的数据治理，实施数据源头管控，负责相关业务制度的制订、执行、日常检查和持续改进，管理业务领域数据源，落实数据质量控制机制，执行数据治理相关工作要求，及时收集业务管理条线的数据问题和数据需求，动态调整制度、流程、数据控制措施，提出数据治理体系和数据管理工作提升建议。

第二道防线为数据治理管理条线，主要负责实施数据治理体系建设，协调落实数据管理运行机制，制定和实施系统化的制度、流程和方法，发挥其对一线部门的设计、管理、控制、指导和监督作用，实现数据统一管理和有效运营，组织推动数据在企业经营管理流程中发挥作用；并对条线的风险进行识别、计量、监测和控制，将数据治理融入到业务流程、产品创新和日常管理当中，提升第二道防线穿透式数据风险管控效果。

第三道防线为审计监督条线，应以促进企业经营目标和数据战略的实现为出发点，强化以数据问题为导向的内部审计和检查，对重点业务和管理领域开展检查，揭示重大违法违规数据问题和重大数据风险，对企业数据治理状况进行再评估；对第一、二道防线的管理措施和效果进行再评估、再监督；对数据治理的整体有效性进行再评估；向董事会和高级管理层提出独立的建议和报告，并建立常态化整改持续跟踪机制，强化审计成果利用。

“数据治理三道防线”融合了企业前、中、后台的部门和人员，只有各负其责，加强“三道防线”的沟通联系，形成合力，实现信息共享、联动互动、合理覆盖，才能建成有效的全面数据治理体系，切实提升数据管理水平，充分释放数据价值。

图4 数据治理的三道防线 —— 按工作职能划分

资料来源：毕马威分析

在“三道防线”的架构中还需要明确董事会、监事会、高级管理层和相关部门的职责分工，建立多层次、相互衔接的运行机制。其中董事会作为数据治理的最高决策机构，对数据治理承担最终责任；第二，由高级管理层负责建立数据治理体系，制定和实施问责和激励机制，组织评估数据治理的有效性和执行情况，保障数据治理资源配置，并定期向董事会报告；第三，在董事会或高级管理层下设立数据治理委员会和首席数据官，审批数据战略及与数据治理相关的重大事项；第四，由业务部门、数据治理牵头部门、内部审计等部门组成“三道防线”，形成完整的数据治理架构体系，各司其职、分工合作并有效发挥作用。

3.3 企业间的数据共享

数据的价值在于流动。除了企业内部数据治理以及企业与消费者之间的连接，企业间的数据流动同样值得重视。欧洲委员会于2018年4月对外发布的《欧洲企业间数据共享研究报告》（Study on data sharing between companies in Europe）选取欧洲经济区（EEA）24个国家129家大中小微企业作为调研对象，对智能交通、智能农业、智能制造、电信运营商、智能家居、智能电网和仪表六大特定商业领域的企业间数据共享和再利用情况进行了调查分析。报告建议政府部门进一步提高对企业间数据共享和再利用重要性的认识，并大力促进其发展。此外，在严格的数据保护法律法规之外，政府应采取鼓励数据共享的柔性措施，并为有意愿发展数据共享和再利用的企业提供必要的指引和资金支持。

报告同时指出，尽管欧盟先后发布《数据单一市场战略议程》、《关于促进蓬勃发展的数据驱动型经济的通告》、《数字单一市场（DSM）战略》、《关于建立欧洲数据经济的通告》等企业数据共享相关的法律法规，但无论是数据供给方还是需求方，仍然在数据共享方面存在诸多障碍。就数据提供方而言，技术障碍及相关成本投入、法律法规的不确定性是影响数据共享的主要因素；数据需求方主要面临数据获取难和标准化不足所带来的数据再利用成本高企、自身数据管理技能不足等障碍。

就我国而言，企业间数据共享的典型应用是数据交易所模式。但限于价值评估方式不明确、相关法规标准缺失、权属界定存在困难、交易技术链条有待完善等问题，数据交易所在我国面临诸多难题。整体来看，企业间的数据流动有待进一步“破题”。

4

公众端的数据治理

4.1 个人信息的界定

> “个人数据”指的是任何已识别或可识别的自然人（‘数据主体’）相关的信息；可识别的自然人是能够被直接或间接识别的个体，特别是通过诸如姓名、ID号、位置数据、网上标识，或者与该自然人的身体、生理、遗传、心理、经济、文化或社会身份有关的一个或多个因素。

随着全球互联网渗透率的提高，商业世界中用户所产生的包含个人信息的数据也实现了几何倍的增长。一方面，企业可以通过挖掘用户数据实现有效的用户画像，从而进一步优化客户的购物和服务体验；但另一方面，个人信息在不断的被获取、存储、交易、利用，与之相关的数据泄露事件时有发生，用户数据的产生和使用正在成为一种社会挑战。

仅仅在2018年，就至少有Facebook、Under Armour、My Heritage、圆通、顺丰、华住等用户数据泄露事件发生[19]。其中最引人注目的是某大型国际酒店集团受黑客入侵的5亿用户信息中，用户的姓名、住址、电话号码、电子邮件地址、护照号码、信用卡等所有核心的信息都遭到了泄露。在中国个人数据泄露事件也屡屡发生。中国消费者协会2018年8月发布的《APP个人信息泄露情况调查报告》[20]显示，当前我国遭遇过个人信息泄露情况的人数占比为85.2%。当消费者个人信息泄露后，约86.5%的受访者曾收到推销电话或短信的骚扰，约75%的受访者接到诈骗电话，约63.4%的受访者收到垃圾邮件。

要加强个人用户的数据治理就需要首先了解个人数据的定义以及类别。对于以数据形式而存在的个人信息，欧盟GDPR第四条的定义是：“个人数据”指的是任何已识别或可识别的自然人（“数据主体”）相关的信息；可识别的自然人是能够被直接或间接识别的个体，特别是通过诸如姓名、ID号、位置数据、网上标识，或者与该自然人的身体、生理、遗传、心理、经济、文化或社会身份有关的一个或多个因素。”数据化的个人信息可以被分为以下几大类别：

- 基本信息：为了完成大部分网络行为，消费者会根据服务商要求提交包括姓名、性别、年龄、身份证号码、电话号码、Email地址及家庭住址等在内的个人基本信息，有时甚至会包括婚姻、信仰、职业、工作单位、收入等相对隐私的个人基本信息。
- 设备信息：主要是指消费者所使用的各种计算机终端设备（包括移动和固定终端）的基本信息，如位置信息、Wifi列表信息、Mac地址、CPU信息、内存信息、SD卡信息、操作系统版本等。
- 账户信息：主要包括网银帐号、第三方支付帐号，社交帐号和重要邮箱帐号等。
- 隐私信息：通讯录、通话记录、短信记录、聊天记录、个人视频、个人照片、精确位置等信息

19. 《2018年全球互联网十大数据泄露事件盘点》，新浪新闻，2018年9月3日，https://tech.sina.com.cn/i/2018-09-03/doc-ihiqtcan1036279.shtml
20. 《APP个人信息泄露情况调查报告》，中国消费者协会，2018年8月29日，http://www.cca.org.cn/jmxf/detail/28180.html

- 社会关系信息：好友、家庭成员、单位等信息
- 网络行为信息：上网时间、上网地点、搜寻记录、聊天交友、购物等行为信息

中国并未在法律上对网络空间中的隐私进行明确的界定，使用更多的概念是“个人信息”这个词。对于个人信息的界定，中国不同的法律法规也给出了相应的解释。“可识别性”是认定个人信息的重要标准，只有能够识别某一特定自然人的信息，才能被认定为个人信息。2017年12月29日发布的《个人信息安全规范》作为个人信息保护的国家标准，明确判定某项信息是否属于个人信息，应考虑以下两条路径：一是识别，即从信息到个人，由信息本身的特殊性识别出特定自然人，个人信息应有助于识别出特定个人；二是关联，即从个人到信息，如已知特定自然人，则由该特定自然人在其活动中产生的信息（如个人位置信息、个人通话记录、个人浏览记录等）即为个人信息。符合上述两种情形之一的信息，均应判定为个人信息。

《中华人民共和国网络安全法》第七十六条第（五）项规定：个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第一条规定，个人信息还包括通讯联系方式、账号密码、财产状况、行踪轨迹（比如在互联网上的位置数据和日志信息）等。此外，种族、宗教信仰、个人健康和医疗信息等敏感信息也属于个人信息范畴。

进入信息化时代中国在个人信息保护领域面临着两个突出问题。第一是电信诈骗，中国个人信息保护起步于欺诈交易，因为犯罪份子能够利用个人信息精准地实施诈骗、绑架等各种犯罪，例如2016年轰动全国的徐玉玉案当事人就是电信诈骗的受害者。第二个问题是个人信息的黑灰色产业非常猖獗，也就是个人信息的买卖。企业对于个人信息的需求旺盛，因为企业要开拓市场，就是必须先获得个人信息，如果没有合法获得渠道的话，就只能通过黑市买卖，从而形成了被称为“灰黑”产业的供应链，黑的是犯罪，灰色的产业是满足商业需求。据《中国网民权益保护调查报告2017》披露，当前我国网络非法从业人员已超150万人，黑灰产市场规模已达到千亿元级别。在被破获的个人信息贩卖案中，数据级别高达数亿甚至数十亿条的不鲜见。数目最大的“9·27特大窃取贩卖公民个人信息专案”中，被盗公民个人信息超过50亿条。

我国已经陆续颁布、实施了一系列个人信息保护的法律法规，但是由于分散立法，未能形成完整的体系。针对这一现状，公众端的数据治理就显得至关重要，尤其是加强个人用户的自我防范意识，以及在个人信息遭到泄露时，合法合理的利用相关法律法规进行维权这两个方面。

4.2 加强个人用户的自我防范意识

自我防范意识的提升是个人信息保护的首要一环。用户个人信息的泄露在很大程度上与其缺乏个人信息保护意识及不良的网络习惯有关。网络消费者尤其应当谨慎透露个人信息，因为他们往往更倾向于通过分享披露个人数据信息换取即时的便利性，而对长期的风险隐患意识不足。有调查发现，消费者在选择数字支付工具时，59.6%的受访者将“便捷”作为首选的考察因素；而只有8.4%、10.4%的受访者会从“安全防范机制”、“健全的个人隐私及信息保护政策”的角度来考虑[21]。用户自我防范意识的提高能在源头上有效避免个人信息泄露，进而减少个人信息的非法利用空间。因此，国家网络监管部门、消费者协会等组织可以加大宣传、教育和引导力度，提升消费者尤其是未成年消费者的自我防范意识。例如，鼓励个人建立基本的网络防范意识[22]：

- 尽量不使用公共场所的WIFI。对于黑客来说，公共场合的WIFI极容易侵入，这也意味着个人信息将暴露在黑客的视线下。
- 尽量访问具备安全协议的网址。尽量登录网址前缀中带有“https:”字样的网站，具备这种安全协议的网址的安全性较高。
- 不同软件尽量不要使用同一组账号密码。黑客常常会购买带有大量个人信息的数据库进行“撞库”，设置多组账号和密码可以防止黑客侵入下一个账户，可以及时止损。
- 妥善处置快递单等包含个人信息的单据。对于含有姓名、电话、住址等信息的单据凭证要及时销毁，不经意扔掉也可能导致个人信息泄露。

21. 《数字支付安全与隐私保护|中国大陆消费者态度调查报告》，新华社《经济参考报》与全球领先的数字支付技术公司Visa联合发布，2018年8月。
22. 《网络时代如何保护个人信息安全 专家提四方法建议》，新华网，2018年8月22日，http://www.xinhuanet.com/2018-08/22/c_1123308998.htm

4.3 完善消费者数据维权渠道

中国消费者协会自2017年开始发布“十大消费维权舆情热点”，自2017年起“互联网+”领域就开始成为用户维权的主要阵地，2017年有8个热点都与互联网有关；而2018年的热点中个人信息保护缺失和大数据杀熟这两个与数据安全息息相关的消费者权益损害问题已经上升到了十大热点中的第二和第三位；2019年AI换脸软件涉嫌侵犯用户隐私的讨论也受到舆论高度关注。由此可见，在加强用户自我防范意识的同时，为个人提供更有效、更易用的维权渠道也十分重要。

目前，我国个人信息遭泄漏后，消费者一般可通过以下三种方式维权[23]：

- 按照全国人大常委会《关于加强网络信息保护的决定》，遭遇信息泄漏的个人有权立即要求网络服务提供者删除有关信息或者采取其他必要措施予以制止。
- 个人还可向公安部门、互联网管理部门、工商部门、消协、行业管理部门和相关机构进行投诉举报。国家网信办所属的中国互联网违法和不良信息举报中心（举报专线12377）专职接受和处置社会公众对互联网违法和不良信息的举报。
- 消费者还可依据《侵权责任法》、《消费者权益保护法》等，通过法律手段进一步维护自己的合法权益，如要求侵权人赔礼道歉、消除影响、恢复名誉、赔偿损失等。

23.《国家网信办：个人信息被泄露有三种途径维权》，上海市政府

平台企业也积极通过技术手段开展治理创新。据《2019阿里巴巴知识产权保护年度报告》，2019年，阿里向全社会开放以知识产权保护科技大脑为代表的核心技术，和阿里联手围剿假货源头的区县执法机关从2018年的227个增至439个，一年新增93%，协助抓获的制售假犯罪嫌疑人从2018年的1953人增至4125人，一年上涨111%。国家知识产权局发布的《中国电子商务知识产权发展研究报告（2019）》，第一次将“技术赋能+多元共治”的假货治理阿里模式作为中国经验、中国样本在全社会推广。2019年阿里平台，96%疑似侵权链接一上线即被封杀，消费者举报删除的疑似侵权链接量再降57%，截至2019年9月底的一年内，平台新增活跃用户9000万；96%的知产投诉在24小时内被处理，阿里知产保护平台的品牌权利人入驻量再增20%；每万笔交易疑似侵权商品量仅1.03笔，5年内下降67%。

但也需要看到，由于数据隐私泄露取证难、诉讼成本高等原因，用户维权过程一直异常艰难。由中国青年政治学院互联网法治研究中心和封面智库联合发布的《中国个人信息安全和隐私保护报告》[24]在对全国100多万份调查问卷进行系统分析研究后发现：

- 在被问到发现个人信息泄露会采取什么行动的问题时，71%的参与调研者选择了掐断电话或不予理睬，选择拉黑及拒接的比例为63%；仅有20%左右的参与调研者选择了举报、投诉、报警等积极应对措施。
- 在解释未能维权的原因时，半数以上的参与调研者因不知如何维权（占60%）和没有发现经济损失（占56%）而选择了沉默。
- 值得关注的是，参与调研者中有高达44%的比例选择了因维权程序太复杂、成本太高而放弃维权，另有34%的人是因缺少维权证据而无奈放弃。

24. http://www.sohu.com/a/128010313_481893

案例:

2018年11月，微博网友“花总丢了金箍棒”曝光酒店卫生乱象，引爆舆论。仅仅几个小时之后，花总的个人信息被一家酒店的员工曝光在网上。之后还有人威胁他的生命，导致他就算戴着口罩也无法“正常”入住酒店，人身安全和工作生活均受到严重影响。从此，花总走上艰难的维权之路。可是奔波了近两个月，花费十多万元，却仍然未能找到信息泄露源头在哪。[25]

在数字经济时代，作为数据主体的个人用户一方面依赖于数据控制者提供的各种便捷服务；另一方面，在服务过程中采集、生成的海量个人数据也成为企业商业模式创新和商业利益的主要来源。也就是说，没有网络服务商提供的技术、平台和服务，个人数据很难发挥出最大的价值；没有数据主体的参与，网络服务商的商业模式也将成为无源之水。

作为个人用户和网络消费者，一方面需要做到不随便泄露个人隐私信息，在个人隐私泄露、受到骚扰时要主动维权；同时也没有必要因为畏惧大数据技术而拒绝接受新事物，拒绝享受便捷的服务和福利，毕竟数据经济时代已经到来而且必将继续渗透进入社会和个人生活的方方面面。

随着物联网（IoT）的发展，2020年全球将有200亿以上的联网设备。与此同时，IoT环境下无目的的数据收集（如摄像头）也将远远超过有目的的数据收集。换句话说，数据自动化记录正在成为人类社会各类设施设备的基本属性，高度数据化正在成为个体生活环境的基本特征。在这一必然趋势下，对个人信息的判断及其保护机制，以及对时代发展与技术创新的影响，也有必要重新思考和认知。

25. 《花总奔波维权两月仍不知信息泄露源头，“非常难受只能死磕”》，澎湃新闻，2019年1月22日，https://www.thepaper.cn/newsDetail_forward_2885679

5

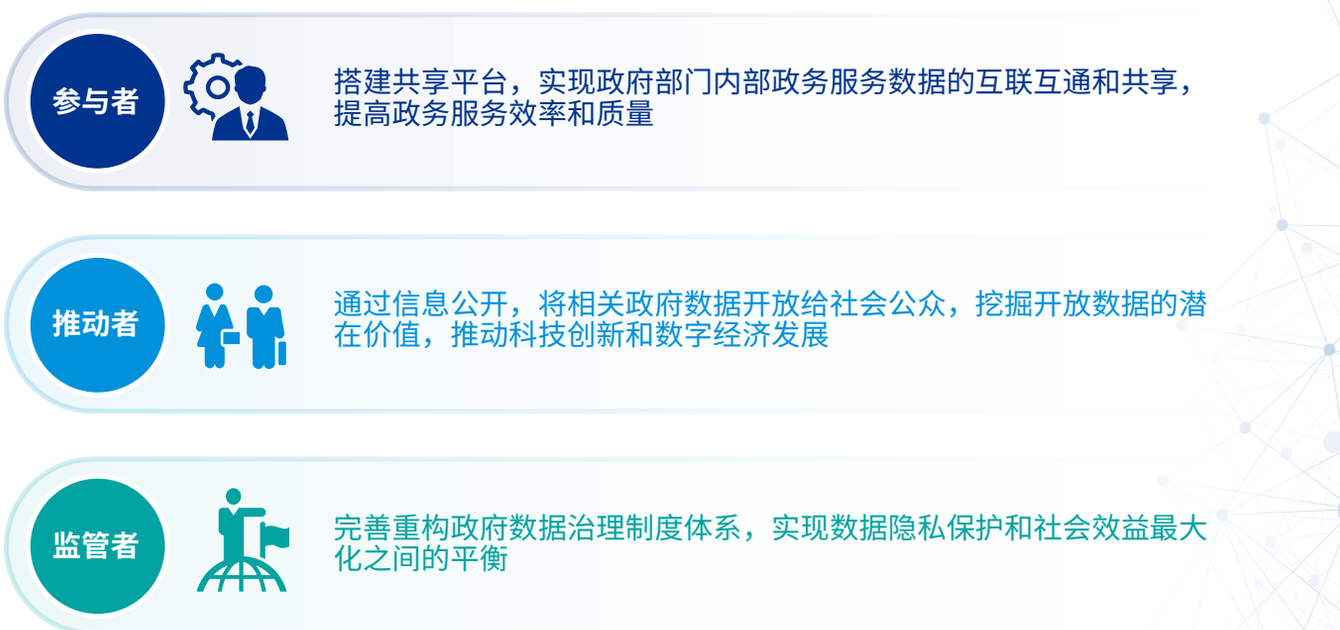
政府端的数据治理

近年来，大数据、云计算、区块链、人工智能等技术的蓬勃发展，为数字政府的构建奠定了坚实的技术基础，极大地推动了“互联网+政务服务”概念的提出及其实施和推广，使得政府端数据治理备受社会关注。

一般而言，政府数据治理主要涉及四大议题：1.政府对于政务数据的自我治理和使用；2.政府部分数据开放的程度和标准；3.政府对于企业和个人数据的获取；4.政府对数据的国际管辖权问题。

本文按照政府担任的角色，将政府端的数据治理提炼为三层含义：第一，搭建共享平台，实现政府部门内部政务服务数据的互联互通和共享，提高政务服务效率和质量；第二，通过信息公开，合理、可控地将相关政府数据开放给社会公众，更好地挖掘数据的潜在价值，推动科技创新和数字经济发展；第三，完善重构政府数据治理制度体系，实现数据隐私保护和社会效益最大化之间的平衡。由此可见，政府在数据治理工作中担任多重角色，既是数据治理的参与者，又是推动者和监管者。

图5 政府在数据治理工作中担任的角色



资料来源：毕马威

5.1 打破信息孤岛，实现政府数据的互联互通和共享

> 数字政府的内涵正在随着大数据、云计算等新技术的引入发生变化，其正在从以‘网上政务’为核心的“数字政府1.0”时代，走向以“数据化运营”为核心的“数字政府2.0”时代。

经过约30年的信息化建设，政府各职能部门围绕着业务需求搭建了众多的业务系统，建立了越来越多的业务数据。但由于政府部门间的信息隔离与壁垒，再加上部门间协作不够深入等原因，这些业务数据缺乏相互之间的互联互通，难以通过数据关联释放数据活力，呈现出有价值的信息，导致虽然拥有大量的数据，却持有较少信息的矛盾状态。

政府数据共享的宗旨是提高政务服务的效率和质量，提升政务服务供给能力，加快推进“数字政府”的构建。将政府数据按需共享给相关职能部门，可以有效提升其他相关事项办理过程中申请主体的申办效率及受理、审批人员的服务效率，促进跨部门政务服务与管理流程的优化及相关业务的重组，提升服务质量。特别是在大型项目的审批工程中，由于涉及的材料多、部门多、流程多等，如果各相关职能部门间业务数据不流通、不共享，申请主体就需要在各个环节都要提供其前置环节办理结果的证明，并需要重复提交各种申请材料，受理窗口也需要不断的核验这些材料，既浪费资源又存在隐患，难以发挥出电子政务的系统性优势。若相关政府数据可以实现按需流通共享，前后环节便可以自动触发、无缝对接，从申办及提交初始材料开始，让数据自动流通，沿着业务流程形成一条政务服务链，可以节约申办成本及受理成本，极大提高政务服务质量。

数字政府的内涵正在随着大数据、云计算等新技术的引入发生变化，其正在从以“网上政务”为核心的“数字政府1.0”时代，走向以“数据化运营”为核心的“数字政府2.0”时代。数字政府1.0是把线下的政务办事窗口搬到网站和手机上，是互联网和政务在物理层面的连接；而以数据化运营为核心的数字政府2.0则是通过系统打通和数据协同，形成整个政务流程的再造。一个形象的例子，电子政务之前，百姓想要办一件事，需要跑5个政府部门窗口；数字政府1.0之后，百姓不用跑很多政府窗口了，可以通过网站和手机线上办理；而数字政府2.0则可以实现底层部门数据共享，只需要在线上点一个窗口就可以办理多种便民服务，大大提高了政务服务的效率和质量。

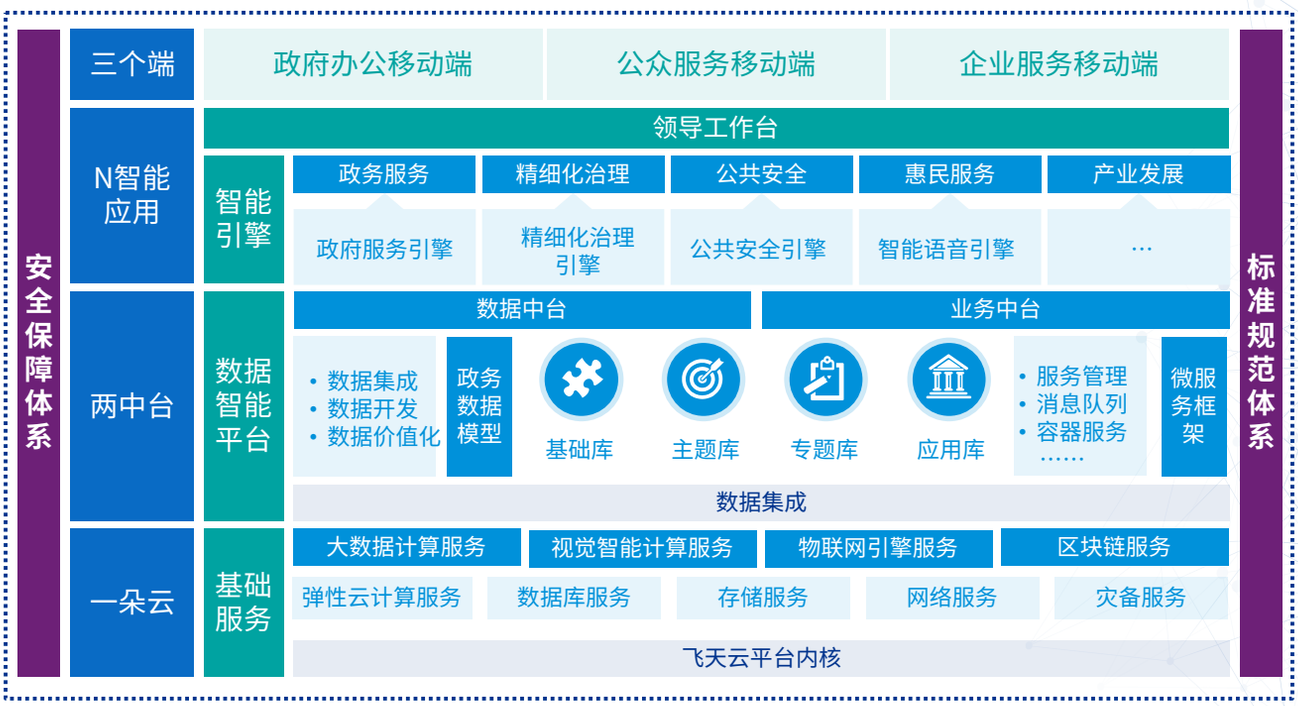
在此次新冠肺炎疫情中，也体现了政府数据共享的重要性，政府部门利用数据共享平台协同统计并核验确诊病历人数、疑似病例人数和死亡人数等相关数据，这里面有海量数据查询和校验技术的运用，实现了收集疫情相关数据和发布疫情统计数据的实时性和准确性。

图6 数字政府即将迈入2.0时代

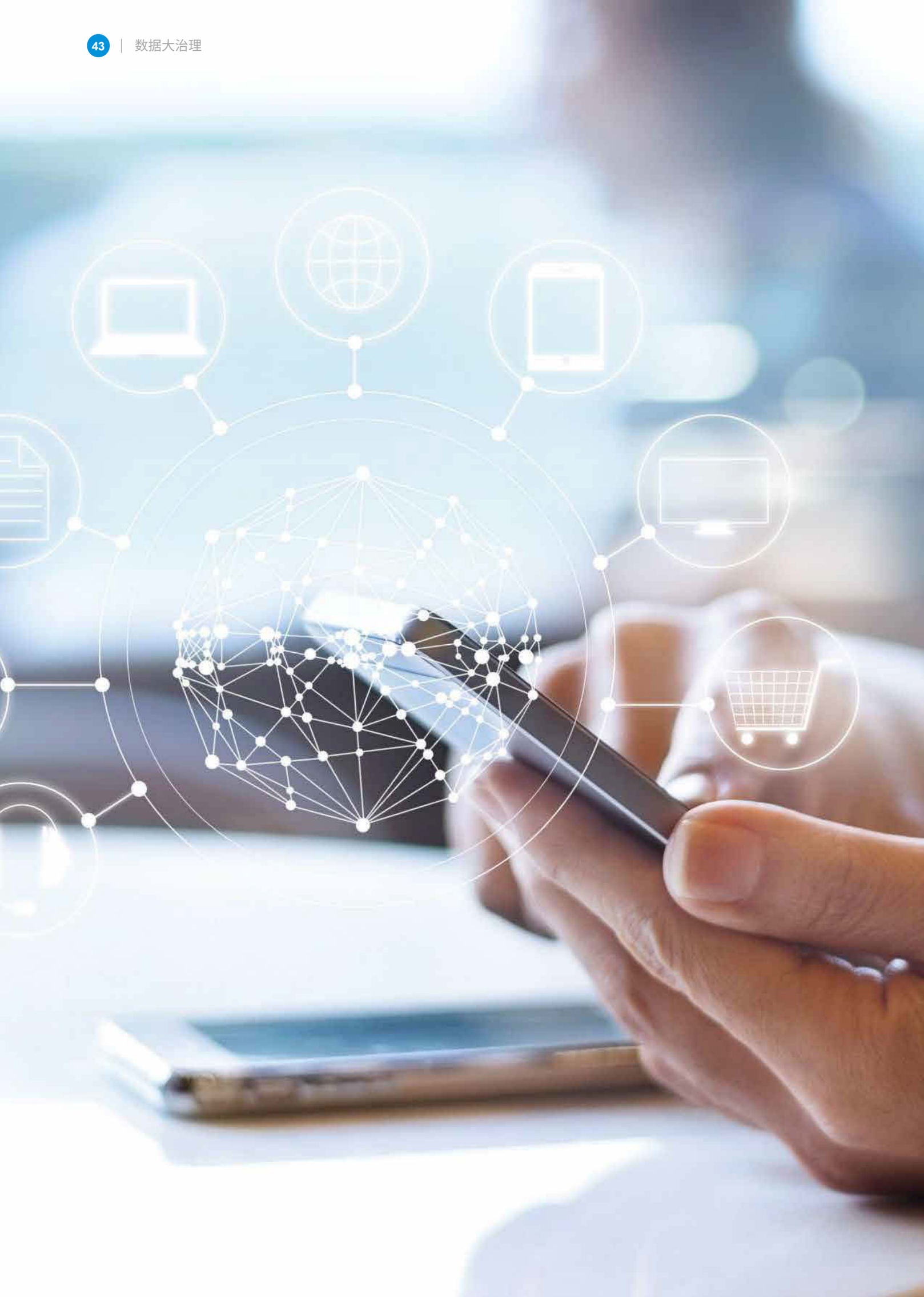
资料来源：毕马威，阿里研究院

数据化运营的前提是数据治理，需要通过业务中台和数据中台的建设，才能由表及里进入到政务流程再造阶段。针对数字政府的数据化运营，2020年，阿里巴巴全面升级服务数字政府战略，形成数字政府1+2+3+N能力大图，即统一的云平台底座，数据中台和业务中台，以及政府办公移动端、公众服务移动端、企业服务移动端，以此为基础整合生态力量，构建N个应用创新体系。

图7 阿里巴巴1+2+3+N的数字政府技术架构



资料来源：阿里云智能



目前，支付宝已成为全国最大的网上办事平台，可一站式办理的政务服务类别多达1064项，涵盖从办理社保、公积金、水电燃气等生活缴费，到高考成绩查询、办理国际驾照等服务内容。有调查显示，平均每4个中国人，就有1个利用支付宝办事。钉钉用户数也已突破3亿，企业组织数突破1500万家。2019年国税总局浙江省税务局基于“钉钉+丁税宝”打造的浙江税务征纳沟通平台，让企业办税“一次都不用跑”，已经服务超过150万家企业。在数字政府领域，阿里巴巴已与全国30个省市区达成合作，覆盖了442个城市，包括1000多项服务类型，服务了9亿用户。[26]

26. 《阿里巴巴升级服务数字政府战略:覆盖442城 服务9亿人》，新浪财经，2019年7月。
https://finance.sina.com.cn/stock/usstock/c/2019-07-25/doc-ihytcitm4511762.shtml

5.2 开放政府数据，推动数字经济产业发展与创新

> 在保障国家秘密、商业秘密和个人隐私的前提下，如果将政府数据最大限度地开放出来，让社会进行充分融合和利用，有利于释放数据能量，驱动经济发展和技术创新

各国政府在履行行政职能、管理社会公共事务等的过程中掌握了大量数据，这些数据是社会的公共资源，在保障国家秘密、商业秘密和个人隐私的前提下，如果将政府数据最大限度地开放出来，让社会进行充分融合和利用，有利于释放数据能量，驱动经济发展和技术创新。

政府数据开放起源于科学数据的共享。随着现代科学技术的迅猛发展，学科交叉融合加快，海量科学数据呈现井喷式的增长。有效地收集、管理、开放和共享科学数据，能够避免重复研究、降低科研成本、提高国内及国际研究人员的参与度，从而提升研究效率，推动创新创业和经济发展。

美国是开放政府数据的先行者。早在20世纪80年代，里根政府就曾提出收集国家科学基金会支持的研究项目所产生的所有数据并将其商业化，但该举措当时仅涉及一个部门，成效有限。奥巴马政府认为开放数据不仅有助于确保政府的公开、透明和负责，且有助于促进创新创业、科学发展并带来其他公共利益。2009年1月，奥巴马签署首份总统备忘录《透明和开放的政府》，随后，美国政府开放数据的门户Data.gov网站正式上线发布。Data.gov分为教育、能源、金融、健康等各个板块，用户只需要进入各个板块，就可以搜索到联邦政府所有公开数据。Data.gov还提供了自动统计和分析功能，不仅可以对联邦政府部门活动数据进行统计分析，还会针对用户数据需求进行处理。

数据开放是美国政府长期执行的重要战略，多年来美国建立了国会立法、联邦政策和部门规章三层面的制度框架，将数据开放的理念贯穿整个科研项目管理周期，并与时俱进、不断更新，保证了联邦资金效率和影响的最大化，对我国政府数据开放方面的未来制度设计具有一定的借鉴意义。综合来看，美国政府数据开放有五大原则：公共性、易获取性、充分说明性、完整性和及时性等。

图8 美国政府数据开放的五大原则

资料来源：美国联邦政府数据开放政策整理，毕马威

此外，美国于2019年1月通过的《开放政府数据法》还提出设立首席数据官及其委员会制度，以及建立开放政府数据的报告及评估制度，对政府开放数据进行反馈评估和改进。

近年来，中国也出台了关于推进政府数据开放的系列政策措施。2015年我国印发《促进大数据发展行动纲要》，将政府数据开放共享上升为国家战略，要求在未来5-10年“形成公共数据资源合理开放共享的法规制度和政策体系”。之后，贵阳、上海等多个地方政府先行先试，在积极开展政府数据开放工作的实践基础上制定了相关的地方性法规，对推进我国政府数据开放起到积极作用。在2019年全国两会上，也有多位代表委员聚焦于政府数据资源的开发利用、公共数据开放力度、政府数据共享开放法律健全等，为政府数据开放建言献策。

自2012年上半年上海市推出全国第一个政府数据开放平台起，截至2020年2月，我国已陆续上线90多个符合政府数据开放基本特征的中央部委、地级市及以上平台。其中，中央部门已有交通部、国家统计局、国家气象局、国家林业局4家单位建设数据开放平台。地方上也有上海、北京、湛江、无锡、武汉、东莞、肇庆、青岛等50多个城市建设数据开放平台。已建成的数据开放平台涉及的数据领域也非常多，包括教育科技、民生服务、道路交通、健康卫生、资源环境、文化休闲、机构团体、公共安全、经济发展等约15种[27]。

但我国目前仍在国家层面缺乏对政府数据开放的明确规则指引和立法，专门立法相对滞后，亟待进一步建立健全相关政策法规体系。我们可以借鉴美国等国际立法以及各地区先行先试的经验，制定开放政府数据的专门立法，建设统一的国家级政府数据开放平台，有效提升政府数据开放的力度，助推我国数字经济的高质量发展。

27. 政府数据开放与创新发展实践，张峰，http://www.sic.gov.cn/News/612/10423.htm

5.3 完善重构政府数据治理制度体系

为了真正解决好政府数据的共享和开放问题，实现数据资产价值最大化，我们应该发挥制度优势与政策红利，通过“数字政府”顶层设计对数据背后的机制进行调整，通过法制建设，完善政府数据治理规范，保护公民个人及社会组织隐私，建立满足数据安全标准的工作机制。

个人信息保护是一个重要法律命题。各个国家都在持续地制定和修改相关立法，完善个人信息保护的规则，维护个人信息主体的权利，并对数据的权属、数据的利用规则以及数据各方主体之间的权利配置问题持续探讨。截至目前，全球共有100多个国家和地区制定了专门的个人信息保护法，确立了包括个人信息收集和使用、跨境传输、登记注册以及泄露通知等基本制度[28]。

随着互联网的迅猛发展，个人信息收集以及利用的场景和方式都发生了巨大的变化，传统的个人信息保护的相关规则正在面临着挑战和变革。数字经济时代的分享经济等新型商业模式、经营方式等也与传统产业有很大不同，传统的治理模式已不再适应新兴经济态势的发展。法律法规政策的制定不能削足适履，硬性要求新事物符合旧事物的政策框架，而是需要因时制宜地调整或者制定新的监管政策。既要做到数据安全保护，又要促进数字经济发展，为数字经济营造开放包容的发展环境。

> “一方面，制度设计要兼顾个人信息保护、创新与效率等价值目标；另一方面，也要充分认识到我国与发达国家在制度环境、产业发展状况等方面的差异，可部分借鉴，但不能照搬”

因此，当前制定个人信息保护法要结合数字经济的发展特点，一方面，制度设计要兼顾个人信息保护、创新与效率等价值目标；另一方面，也要充分认识到我国与发达国家在制度环境、产业发展状况等方面的差异，可部分借鉴，但不能照搬；**设计制度时，要珍惜我国数字产业多年来快速发展所创造的成果，稳住节奏推进数字产业规范发展。**

28.《大数据时代,个人隐私何处藏?》，周叠瑶，《小康》2019年24期

图9 数字经济时代，个人信息保护法律法规制定应考虑的问题

制度设计要兼顾个人信息保护、创新与效率等价值目标

认识到我国与国外在制度环境、产业发展状况等方面的差异，可借鉴但不能照搬

珍惜我国数字经济快速发展所取得的成果，推进数字经济长期可持续发展

资料来源：毕马威分析

此外，数字经济时代的立法还应实现从监管到治理的转变。数字经济数据治理更多强调的是多元化参与，不仅包括政府数据治理，也包括企业自律和消费者个人信息保护意识提高等等，政府、企业、消费者三方要协同配合，共同挖掘数据的价值。

总之，政府端数据治理的主要目的是对数据进行利用，发挥大数据的价值，实现社会效益最大化。数字经济时代，数据可以看作是一种社会资源，在制度设计时，应该尽量使数据资源的流动和分配更方便、更容易，从而提高各项经济资源的使用效率，最大化地发挥出数据的价值。我们建议制定数据治理政策时可以参考如下四个原则：**鼓励创新、开放包容、多方参与、协同治理**。

6

如何实现“数据大治理”生态体系的持续发展

> 评估数据大治理的效果，需要同时考虑产业发展、个人信息保护和数据安全，亦即在发展和安全这两个最基本的价值之间，通过多主体的努力，寻求最佳的动态平衡点。

近几十年来，数字经济的崛起推动了全球经济前所未有的创新和发展，数据的自由流动也为社会创造了新的产业和就业机会，改善并提高了人民的生活水平。与此同时，对数据的恶意利用对个人和社会也造成了意想不到的伤害。如何治理数字经济下复杂的数据生态系统，确保在发挥数据潜力的基础上恰当地管理其风险，已经成为全球范围内政策制定者所面临的一大挑战。

数据大治理需要多方主体共同参与，各司其职，协调配合，形成数据治理的动态生态系统。而对数据大治理效果的评估，也需要构建多层次、多维度、多角度的立体指标体系。成熟指标体系的构建，还需要全方位实证调研数据和顶层设计的通盘考虑。本报告在此提供“数据大治理评估指标框架”的示例，将目前较为重要的考察指标分类列出，作为建立指标体系的初步探索，也希望能够为日后构建成熟指标体系提供一个初步的基础。

评估数据大治理的效果，需要同时考虑产业发展、个人信息保护和数据安全，亦即在发展和安全这两个最基本的价值之间，通过多主体的努力，寻求最佳的动态平衡点。因此，在指标框架的示例中，可将指标体系分为三个类别，分别为：数据产业发展指标、个人信息保护指标、数据安全指标。

图10 数据大治理评估指标框架

数据产业发展指标

- 数据产业发展情况
- 数据驱动GDP情况
- 政府数据开放度
- 数据共享和流动情况
- 政府数据获取便利程度

个人信息保护指标

- 个人信息保护立法体系完善程度
- 政府执法机制与效能
- 司法保护实践与规则建构
- 标准和行业规则完善程度
- 企业合规情况
- 公众隐私和个人信息保护意识

数据安全指标

- 数据安全领域立法立规完善程度
- 行政监管和执法效能
- 标准和行业规则完善程度
- 企业战略和合规实践
- 数据安全产业发展情况
- 数据安全国际合作情况

资料来源：中国社会科学院大学互联网法治研究中心

在“数据产业发展指标”中，主要考察数据产业本身发展情况以及数据对整体经济社会发展的贡献程度。一方面，需要考察数据产业的发展情况，另一方面，数据作为生产要素对于经济社会发展的贡献程度，可以通过考察数据对于驱动GDP的贡献程度来评估。数据共享、开放和流动状况，也是评估数据对于产业发展驱动的重要指标。其中，政府数据的开放程度以及获取的便利程度，可以作为观察整体数据开放程度的重要指标，这也回应了报告中对于政府在数据大治理中角色的研究，政府不仅要承担起监管的角色，本身的数据开放和共享，也是评估数据大治理效果的重要依据。

“个人信息保护指标”主要着眼于对于个人基本权益的保护，这一领域的治理效果，也是通过考察制度和实践的各个层面指标来展开。首先应当考察个人信息保护立法体系的完善程度，作为个人信息保护指标的重要前提和基础。在执法层面，应当考察政府行政执法的机制与效能，以及法院在司法保护中的实践与规则建构情况。除此之外，从多主体治理的角度考察，还应当注重标准制定组织和行业协会在规则建构和个人信息保护中的参与和成熟程度。从企业层面，对其个人信息保护合规情况的评估目前已有较为丰富的实践，这也是落实个人信息保护最基本层面。最后，从个人角度，公众隐私和个人信息保护的意识，亦是治理效果的重要维度和基础。

“数据安全指标”主要从数据引发的公共安全、国家安全、产业安全维度出发进行构建，考察立法框架、执法效能、配套规则、安全产业、企业合规以及国际合作等多主体、多层次的指标评估，主要包括作为制度基础的立法立规完善程度、数据安全领域行政监管和执法效能、标准和行业规则完善程度、企业的数据安全战略和合规实践，以及数据安全产业作为独立产业的发展情况。最后，由于数据安全越来越成为国际性的问题，跨境数据安全问题凸显重要性，因此数据安全国际合作情况也应当成为评估指标的组成部分。

指导委员会、作者及致谢

指导委员会：

陶匡淳　毕马威中国及亚太区主席

刘逸明　毕马威阿里巴巴全球业务主管合伙人

陈竹青　毕马威阿里巴巴全球业务主管合伙人

高红冰　阿里巴巴集团副总裁、阿里研究院院长

作者：

康 勇　毕马威中国首席经济学家

陈立节　毕马威中国数据治理主管合伙人

杨晗　毕马威中国管理咨询总监

王 薇　毕马威中国研究经理

张杭川　毕马威中国管理咨询经理

郑亚男　毕马威中国研究员

刘晓春　中国社科院大学互联网法治研究中心执行主任

顾伟　阿里巴巴集团法律研究中心副主任

宋 斐　阿里研究院资深专家

致谢：

安筱鹏　阿里研究院副院长

李倩　阿里巴巴集团政策法规研究室总监

刘明　阿里巴巴集团政策法规研究室专家

许可　对外经济贸易大学数字经济与法律创新研究中心执行主任

王淇　国家知识产权局知识产权发展研究中心发展处副处长

王莹　阿里巴巴集团法律研究中心主任

康敬奎　苏州大学学报编辑部主任

关于毕马威中国

毕马威在中国内地、香港和澳门运营的成员所及关联机构统称为“毕马威中国”。

毕马威中国在二十四个城市设有二十六家办事机构，合伙人及员工约12,000名，分布在北京、长沙、成都、重庆、佛山、福州、广州、海口、杭州、济南、南京、宁波、青岛、上海、沈阳、深圳、苏州、天津、武汉、厦门、西安、郑州、香港特别行政区和澳门特别行政区。在这些办事机构紧密合作下，毕马威中国能够高效和迅速地调动各方面的资源，为客户提供高质量的服务。

毕马威是一个由专业服务成员所组成的全球网络。成员所遍布全球147个国家和地区，拥有专业人员超过219,000名，提供审计、税务和咨询等专业服务。毕马威独立成员所网络中的成员与瑞士实体 — 毕马威国际合作组织（“毕马威国际”）相关联。毕马威各成员所在法律上均属独立及分设的法人。

1992年，毕马威在中国内地成为首家获准中外合作开业的国际会计师事务所。2012年8月1日，毕马威成为四大会计师事务所之中首家从中外合作制转为特殊普通合伙的事务所。毕马威香港的成立更早在1945年。率先打入市场的先机以及对质量的不懈追求，使我们积累了丰富的行业经验，中国多家知名企业长期聘请毕马威提供广泛领域的专业服务（包括审计、税务和咨询），也反映了毕马威的领导地位。

关于阿里研究院

研究院成立于 2007 年 4月，依托并深深扎根于全球最大、最具活力的商业生态系统—由电子商务、电商物流、云计算与大数据、大文娱等构成的阿里巴巴商业生态圈。秉承开放、分享的互联网精神，面向研究者和智库机构，通过数据、技术、案例、理念的分享，成为新商业、新经济与新治理领域的智库平台。

研究范围包括：微观层面的消费者洞察、企业数字化转型、模式创新（如 C2B 模式、未来组织模式） 研究等，中观层面的产业互联网化研究（如供应链、电商物流、农村电商等），宏观层面的新经济与传统经济的互动研究（如互联网与就业、消费、进出口等）、互联网治理研究（如网规、数字治理）和未来研究等。

kpmg.com/cn/socialmedia

如需获取毕马威中国各办公室信息，请扫描二维码或登陆我们的网站：
https://home.kpmg.com/cn/en/home/about/offices.html

刊物编号：CN-MKT-0001

二零二零年七月