金杜观察
KWM INSIGHTS

金杜律师事务所
KING&WOOD
MALLESONS

2020年11月 总第06期
November 2020 Issue 06

数字社会网络安全、数据合规及治理

金杜律师事务所　金杜数字经济国际法律服务中心　金杜法律研究院　联合出版

数字社会网络安全、数据合规及治理

本出版物汇集了金杜律师事务所网络安全、数据合规及治理团队于2016年至2020年期间，发布的以人工智能、数据合规和网络安全为主题的54篇文章，其中少部分表述具有时效性，仅将不同时间、不同阶段的立法和执法发展情况呈现出来，以期对法律本身、立法执法、法律问题等作出进一步延展和思考。

有关本书的咨询及意见和建议，请联系：
publication@cn.kwm.com

开篇寄语

2020年4月以来，中共中央、国务院连续颁布《中共中央、国务院关于构建更加完善的要素市场化配置体制机制的意见》等多项宏观政策法规，将数据作为与土地、劳动力、资本、技术并列的生产要素，要求推进政府数据开放共享、提升社会数据资源价值、并加强数据资源的整合和安全保护。实践中，各地不断尝试利用数据要素打造新型经济形态，贵阳、上海等地的大数据交易中心已经陆续成立。立法与实践层面对数据要素市场培育的强烈呼吁，吹响了数字经济时代来临的号角，数据要素引动的产业经济模式正在发生深刻的转变。

数字经济时代，数据安全及合规问题是企业面临的首要问题。企业如果不能保证基本的数据安全性、数据处理活动的合规性，将会面临数据泄露、数据丢失等多发安全事件，数据资源的开发利用亦将因缺乏数据资产的固定而无从谈起。做好数据安全及合规工作是基石，在此基础上，企业还应当积极探索数据资产的固定及其商业价值的开发，通过发挥数据价值为企业提升综合竞争力助力。可以预见，开发数据利用价值，提升数据使用效率，将能极大地提升企业在提供产品或服务时的综合竞争优势，而这也是一直以来中央号召整合数据资源、通过数据要素推动新型产业发展的直接体现。

与此同时，伴随着“数据主权”的浪潮在全球范围内兴起，我们注意到数据价值、数据作为重要生产要素的理念也在全球范围内得到承认。不同国家/地区对于数据安全和数据价值的高度重视不约而同地将以上理念具化为对数据本地化提出要求、对跨境数据传输作出限制等多个方面。例如美国在《澄清境外合法使用数据法案》（CLOUD Act）中肯定美国执法机关对美国企业“控制”的境内外数据享有“主权”；欧盟在《通用数据保护条例》（GDPR）也以普遍适用（即包含所有针对欧盟用户提供产品和服务的企业）的同等保护水平要求从安全角度建立了个人数据向境外传输的管控体系；此外，俄罗斯、印度等国家/地区也纷纷通过本地化等规则，以期确立对数据传输的控制。

面对这一全球化浪潮的兴起，企业需要积极对自身数据资产管理进行顶层设计，在全球范围内合理布局数据资产体系进行应对。长期来看，企业为适应这一全球化浪潮，可能需要构建多样化、多层级的全球数据资产管理体系，进而实现业务发展与合规义务的平衡。这将有利于企业充分发挥主观能动性，在寻找对契合自身利益的资产管理体系的同时，避免不同司法辖区行使数据主权带来所适用法律规范的冲突，及潜在的企业之间可能的跨境争议纠纷，以减少争讼成本。

金杜律师事务所（“金杜”）作为中国最早开展数据安全及合规业务的律师事务所之一，深知数据安全、数据合规、数据价值开发等在提升企业竞争力过程中举足轻重的作用。我们始终将协助企业保证数据在全生命周期的处理活动中得到安全有序、合法合规的开发利用作为工作的核心。与此同时，我们紧跟党中央、国务院推动数字经济发展的步伐，关注数据要素市场及相关行业发展的新动向，及时借鉴数据产业发展的成果，积极从数据资产化、商业化、智能化建设等多个角度为企业的数据利用提出建议，以期协助企业实现商业价值的赋能。

金杜是一家总部位于亚洲的全球性律师事务所。多年来，金杜积累并搭建了广阔的全球法律服务网络，一方面在新加坡、日本、美国、澳大利亚、英国、德国、西班牙、意大利等欧洲主要城市和中东均设有各行业领先的办公室，对数字经济带动的国际业务发展保持高度敏感且密切关注，在跨司法辖区业务方面具有先进经验和领先地位；另一方面，由各司法领域的国际化法律人才组成的先进业务团队也为金杜提供了巨大且广泛的知识储备与交流平台。上述全球化、多元化的国际法律服务网络为金杜应对数字经济改革提供了保障，这有利于我们在协助企业应对全球“数据主权”浪潮的过程中，整合全球资源，为企业搭建符合当地监管要求及其自身利益的全球数据资产管理体系。

2020年11月20日，金杜数字经济国际法律服务中心（“服务中心”）正式成立。金杜数字经济国际法律服务中心的设立致力于为企业在数字经济时代日益多样化的法律需求提供全方位的解决方案。服务中心将充分调动金杜在各领域长期理论与实践经验的积累，向客户提供多样化的数字经济国际法律服务；同时，还将纵向深耕细分行业，深入挖掘数据领域的前沿热点问题，以期在未来能够为企业提供一站式多样化法律服务的同时，助力企业在数字经济时代更长远的商业发展。

王 玲
2020年11月

金杜数字经济国际法律服务中心简介

2020年4月9日，中共中央、国务院发布《中共中央、 国务院关于构建更加完善的要素市场化配置体制机制的意见》，明确将数据作为新型生产要素，在国家层面正式确认数据的基础资源地位，正式开启数字经济社会新阶段。为响应习总书记、中央政府的号召，金杜律师事务所于2020年11月20日正式成立金杜数字经济国际法律服务中心（“本中心”）并于同日举办首届“海南自由贸易港数字经济投资法律研讨会”。

基于数字经济在当今中国多领域、跨产业的发展态势，一方面响应中央部署海南全岛建设自由贸易港，另一方面也承接金杜律师事务所“智造”粤港澳大湾区的整体规划，在组织架构方面，本中心已在海南省三亚市设立常设机构，聚集金杜内部各个业务部门对数字经济有意向、业务上有联系的合伙人和律师，共同打造数字经济法律研究和对外数据法律服务综合性平台。同时，本中心还将积极研究参与数据交易的试点，挖掘新型法律服务模式，搭建国际化数据交易的法律服务与信息平台。

本中心将以建设跨部门、多学科的国际化创新型综合法律服务平台为目标，旨在聚焦数字经济时代的客户需求和价值导向。通过对内整合和优化金杜律师事务所生态圈资源，突出针对数字经济时代的法律服务，在内容创新和产品创新的基础之上，积极跟踪市场变化与发展、参与规则制定、引领数字经济时代法律服务，致力于打造权威、独立、专业、创新的国际品牌。同时，本中心还将整合线上平台和线下赋能，通过金杜云办公室，汇聚金杜全球法律服务网络及其专业人员，持续探索、革新数字经济领域全方位、国际化的综合服务新形态，应对数字经济时代日趋多样化、去本地化的市场需求。借助本中心的平台与品牌，我们将与各界领军人物和机构开展深度合作，共同推动数字经济产业的互惠共赢、蓬勃发展。

金杜长期致力于通过前沿技术助力业务创新，特别是金杜自2020年以来依托云中子线上法律服务平台设立了国内外多个城市的云办公室。本中心的成立将发挥金杜在数字经济服务转型需求上所具备的得天独厚的平台优势，帮助企业客户应对新数字经济浪潮所带来的挑战。

目录

第一部分：人工智能

第二部分：数据合规

第三部分：网络安全

第一部分：
人工智能

人工智能系列开篇：伦理准则与现行规制

从娱乐、出行到日常消费，人工智能正在悄然改变着我们的生活。大家可能已经习惯智能“美颜”后的自己，享受“刷脸支付”的便捷，甚至和Siri聊起了家常。而当AlphaGo击败人类围棋大师，人工智能利用深度学习能力挑战人类记忆高手，人们又不得不对这一由人类创造的“智能”产生莫名恐惧：我们一手创造了“它”，但当“它”超过了人类的一般认知，我们还能否有效地控制“它”？当某型号飞机自动驾驶系统在错误的信号下撞向地面后，人们开始严肃的讨论人工智能的边界以及监管路径。

从人工智能的研发、应用和监管多个环节出发，类似的讨论集中在人工智能的伦理原则、安全管控、决策机制、数据合规等不同方面。本文将作为“智创未来：人工智能的伦理与合规”系列的开篇介绍目前人工智能的发展现状和主要应用场景、主要国家对于人工智能的伦理关注以及现有法律法规对人工智能的监管“抓手”。

一、 人工智能的发展现状

（一）人工智能的技术体系架构和重要要素

发展人工智能，离不开计算算力、算法、数据三大要素[1]。其中，计算算力是人工智能发展的主要助推力，人工智能的核心技术算法为人工智能应用落地提供了保障，而海量数据为算法模型提供基础，是人工智能前沿技术发展的重要资源。当前，人工智能基础算法较为成熟，深度学习的人工智能算法快速发展；而数据的价值在人工智能时代也日益凸显，成为企业的重要资产，并为更高级的算法提供素材[2]。

（二）人工智能进入产业化应用阶段

总的来说，人工智能产业链可分为基础层，技术层和应用层。其中基础层提供计算力，由数据中心及运算平台构成，技术层解决技术开发与输出，开发面向不同领域的技术，应用层主要为行业提供服务、产品，其核心在于提供商业化解决方案。目前人工智能技术在很多产业和领域已经得到广泛应用，人工智能应用层面的创业者利用海量数据和市场优势，将人工智能技术直接用于终端产品层面的研发，助力人工智能进入产业化应用阶段[3]。

技术层面上，智能语音、自然语言处理和计算机视觉等基础应用技术日臻成熟，逐渐形成了商业和产业化模式，多个科技巨头都在该层面深度布局。而应用层的企业则利用人工智能技术针对不同场景或行业领域研发产品或提供服务，其中，与技术相关的应用领域和应用场景包括：

第一，智能语音技术被广泛应用于智能家居、智能车载、智能客服等领域，例如，个人智能语音助手，特别是智能手机的语音助手，极大地提高了手机的易用性；智能音响在播放音乐之外，还可以连接和控制智能家居终端设备的各类产品，为家庭日常交互提供便利。除智能语音技术之外，其他的人机交互技术还处于初期发展阶段，例如近年来体感交互游戏推陈出新，但多数游戏的体验感欠佳[4]。

[1] https://tech.huanqiu.com/article/9CaKrnK59Wb

[2] http://www.caict.ac.cn/kxyj/qwfb/bps/201809/P020180906443463663989.pdf

[3] https://www2.deloitte.com/content/dam/Deloitte/cn/Documents/innovation/deloitte-cn-innovation-ai-whitepaper-zh-181126.pdf

[4] http://www.caict.ac.cn/kxyj/qwfb/bps/201812/P020181227308307634492.pdf

第二，自然语言处理技术的应用方向主要包括文义解析、机器翻译以及信息的过滤与检索，其中机器翻译是近来的热门应用方向，但受制于语义理解及分析的复杂性，机器翻译的质量还有待提高。

第三，计算机视觉的应用较为宽泛，应用领域包括安防、交通、医疗、互联网消费等，例如，我国火车站通过摄像头采集旅客人脸信息，与身份证人脸信息进行验证；用户通过在电商平台上传意向产品或类似产品的照片进行搜图购物；游戏玩家通过AR、VR游戏享受沉浸式游戏体验等。

第四，知识图谱被广泛应用于智能搜索，知识问答、个性化推荐领域，并可辅助行业进行大数据的分析与决策，如各大视频平台利用其注册用户的观看行为建立知识图谱，分析用户喜好并进行相关内容的推送[5]。

除此之外，多个行业利用复合型的人工智能技术实现产品的更新迭代，例如智能机器人、自动驾驶等。

二、 人工智能技术引发的伦理关注

站在普通公众的视角，我们一边感叹于人工智能的强大能力，另一边也不由得对其模拟人类心智思维的“黑科技”充满敬畏。人们谈人工智能越多，似乎越容易陷入“人机对立”的焦虑：当人工智能未来能够发展出具有自我意识的产品，是否应当被赋予人类同等的权利？人工智能的产物未来是否可能会与人类形成对立？当具有自我意识的人工智能产品作出侵害他人权益的行为，谁应该承担起这份责任？当下，人工智能技术进入新的发展阶段，并快速渗透各行各业，融入人们日常生活，这些“终极拷问”已不仅仅出现在影视作品创造的“高科技幻影”中。一方面，公众对于人工智能技术的认知有限，迅速发展的人工智能技术使得公众产生了恐慌心理，导致人们认为人工智能技术成果的难以预测、量化和评估；而另一方面，人类的认知能力本身具有社会局限性，每一个特定的历史阶段所取得的知识成果都受到时代条件的局限，因此，我们客观上也难以准确评估和完整预测人工智能的发展可能存在的风险。

正是意识到人工智能发展的不确定性，多数国家在鼓励人工智能技术开发应用的同时，也从国家政策、法律法规层面对于人工智能的发展方向给予指引。国务院于2017年7月发布的《新一代人工智能发展规划》已认识到人工智能发展可能引发方方面面的社会问题，例如可能改变就业结构、冲击法律与社会伦理、侵犯个人隐私、挑战国际关系准则等，将对政府管理、经济安全和社会稳定乃至全球治理产生深远影响。因此，国务院要求在大力发展人工智能的同时，必须高度重视可能带来的安全风险挑战，确保人工智能安全、可靠、可控发展，提出要重视人工智能法律伦理的基础理论问题研究，并且要有步骤地建立起人工智能伦理规范和政策法规体系，加大对数据滥用、侵犯个人隐私、违背道德伦理等行为的惩戒力度。[6]2019年6月17日，国家新一代人工智能治理专业委员会发布《新一代人工智能治理原则——发展负责任的人工智能》，提出了人工智能治理的框架和行动指南，强调了**和谐友好、公平公正、包容共享、尊重隐私、安全可控、共担责任、开放协作、敏捷治理**等八项原则[7]。

国际社会对于人工智能的伦理探讨也由来已久。2016年8月，联合国教科文组织（UNESCO）和世界科学知识与技术伦理委员会（COMEST）联合发布了《机器人伦理报告初步草案》（Preliminary Draft Report of COMEST on Robotics Ethics），讨论了机器人的制造和使用促进了人工智能的进步，并审视了机器人的应用以及人类与机器人互动所可能产生的伦理问题。[8]美国电气和电子工程师学会（IEEE）也从2016年开始致力于人工智能在技术和伦理考虑方面的标准制定工作，并于2016年12月发布的《合伦理设计：利用人工智能和自主系统最大化人类福祉的愿景》（Ethically Aligned Design, A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems）第一版，旨在鼓励科技人员在人工智能研发过程中优先考虑伦理问题，并就人工智能及自主系统涉及的伦理问题进行专题性阐述。[9]目前该文件的第二版已于2017年12月发布[10]。 随着理论研究的不断深入，近年来，不少国家和地区基于对人工智能伦理规范的长期研究，在形成人工智能未来发展的伦理性准则或要求方面有了最新

[5] http://www.cesi.ac.cn/images/editor/20180124/20180124135528742.pdf

[6] http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm

[7] http://www.most.gov.cn/kjbgz/201906/t20190617_147107.htm

[8] https://unesdoc.unesco.org/ark:/48223/pf0000245532

[9] https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead1e.pdf

[10] https://standards.ieee.org/news/2017/ead_v2.html

进展。下表对于2019年以来部分国家和地区在人工智能伦理准则方面的最新文件进行了总结和梳理。

• 欧盟

- 欧盟于2019年4月8日公开发布了《可信赖人工智能伦理准则》（（Ethics Guidelines for Trustworthy AI） “《欧盟准则》”）[11]，指出人工智能的发展方向应为“可信赖AI”，并据此确立了人工智能发展的三项基本要素，即（1）人工智能技术须符合法律规定，（2）人工智能技术须满足伦理道德原则及价值，以及（3）人工智能在技术和社会层面应具有可靠性。
- 《欧盟准则》对于伦理原则的内涵做了进一步阐释，包括尊重人类自主性、防止侵害，以及公平性和明确性。在伦理原则要求下，《欧盟准则》也提示人工智能技术应用过程中应重点关注和保护弱势群体的利益，包括儿童、残障人士以及其他因信息不对称而存在相对弱势地位的场景，包括在雇主与雇员以及企业与消费者关系场景等。
- 此外，《欧盟准则》还提出了“可信赖AI”应当满足七项要求，即通过技术或非技术方式保障人工智能技术保障人的能动性和监督能力、安全性、隐私数据管理、透明度、包容性、社会福祉、问责机制，以确保人工智能足够安全可靠。

• 美国

- 美国国家标准与技术研究院（NIST）于2019年8月发布了《美国如何领导人工智能：联邦参与制定技术标准及相关工具的计划》（US Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools）（“《计划》”）。《计划》根据2019年2月美国总统特朗普发布的第13859号启动“美国人工智能行动倡议”的行政令所颁布，旨在确保使用人工智能技术的系统可靠、稳健和值得信赖。
- 《计划》提出了有助于美政府推动负责任地应用人工智能的多项举措，建议美国政府更加深入并长期地参与人工智能标准的制定工作。在人工智能的伦理考量角度，《计划》强调，参与人工智能标准制定的人必须了解并遵守美国政府的政策和原则，包括涉及社会和道德问题，治理和隐私的政策和原则。
- 为促进人工智能标准的开发和使用，《计划》进一步建议美国政府促进跨科学科的研究和协作，以增加对社会和伦理考虑在人工智能领域相关性的理解。同时，在制定有关社会与伦理考虑的标准过程中，应当区分技术与非技术标准。

• 日本

- 日本“增强和促进创新的人工智能战略专家会议”于2019年2月15日决定成立“以人为本的人工智能社会原则委员会”，委员会会议的一般事务将由内阁办公室与有关行政机构合作处理。在此基础上，委员会会议形成了《以人为本的人工智能社会原则》（Social Principles of Human-Centric AI）[12]。
- 该文件强调了人工智能的应用应服务于全人类和社会公众利益，并指出人工智能发展须以实现尊重人类尊严、多样化和包容性、可持续发展等基本的社会发展理念为目标，强调了人工智能的使用不应侵犯宪法和国际法上所保障的基本人权，避免过度依赖人工智能导致其操纵人类决策等。
- 该文件第四部分明确了人工智能应当满足的社会原则：（1）以人为本；（2）教育/扫盲原则；（3）隐私保护原则；（4）确保安全原则；（5）公平竞争原则；（6）公平、问责制和透明度原则；（7）创新原则。

• 新加坡

- 2019年1月，新加坡个人数据保护委员会（PDPC）与信息媒体发展局（IMDA）正式提出《人工智能治理框架建议模型》（A Proposed Model Artificial Intelligence Governance Framework），以帮助企业解决因跨行业使用人工智能技术带来的道德以及管理方面的问题。该文件所述人工智能模型框架主要侧重于四个领域：内部治理，决策模型，运营管理和客户关系管理。[13]

[11] https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai

[12] https://www8.cao.go.jp/cstp/english/humancentricai.pdf

[13] https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Resource-for-Organisation/AI/A-Proposed-Model-AI-Governance-Framework-January-2019.pdf

- 该文件明确其提出的模型框架基于两项基本指导原则，即（1）人工智能制定或协助的决策应该是可解释的，透明的，对消费者是公平的；以及（2）人工智能实施应该以人为本。

• 澳大利亚

- 2019年4月，澳大利亚工业创新和科技部发布了澳大利亚政府资助英联邦科学与工业研究组织CSIRO的Data61起草的《人工智能：澳大利亚的伦理框架》（Artificial Intelligence: Australia's Ethics Framework）讨论稿，旨在明确人工智能技术不同应用场景下所应当关注的伦理性问题，应用场景涵盖数据治理、自动化决策、人类行为预测，并探讨了人工智能应用的两个现有的典型场景——自动驾驶和安防技术应用下所应当关注的问题。
- 该文件基于此前各界对于人工智能伦理研究的基础上，明确提及人工智能须关注的八个核心原则：（1）产生福利原则；（2）不侵害原则；（3）合法合规原则；（4）保护隐私原则；（5）公平原则；（6）透明和可解释原则；（7）可争议原则；（8）问责原则。[14]
- 该文件也进一步指出，数据是人工智能的核心，因此人工智能的应用也不可避免与隐私和数据相关的问题密切关联，据此，应当对人工智能使用不适当或不准确的数据集所可能导致的歧视性问题予以关注。

三、 规范人工智能技术应用的法律规则和难题

可以看出，各国、各地区已经从国家政策和原则导向的高度，尝试对人工智能的未来发展划出一条“伦理”界限。在基本原则的设定上，各国一致强调人工智能发展应当“以人为本”、“合法合规”，寻求人工智能的公平、透明和安全的成长环境，一方面为人工智能向健康、可信赖的方向发展提供引导，另一方面则有助于帮助公众深化对人工智能技术的认知，消除因技术的未知而带来的社会焦虑与群体恐慌。这些基本的伦理准则并不是“纸上谈兵”，实际上基本的精神已经贯穿在规范人工智能技术发展与应用的行为要求和法律文件中，并随着社会对人工智能技术认知的不断加深而更加具象和细化。当然，规则的落地也往往遇到诸多实践难题，如何确保在多方利益主体诉求中寻求各方利益的平衡，仍旧值得我们深思与探讨。

立足于人工智能技术应用的不同场景，各国及行业立法和监管层面均以“以人为本”原则为起点，保障人的主体权益保护的具体落实。例如：

• 机器学习：数据保护与行业发展的平衡

人工智能技术的发展离不开数据。前述《人工智能：澳大利亚的伦理框架》也强调了数据在人工智能技术发展进步中的核心地位。基于深度学习的人工智能技术，需要基于大量的数据基础，通过计算找寻数据中的规律，运用该规律对具体任务进行预测和决断。这一学习过程则不可避免要求企业充分挖掘、采集和处理数据，以为机器的深度学习提供“养分”。此时，则需要站在人工智能技术发展“合法合规”的原则角度，充分审视企业在为人工智能的学习训练收集数据的过程中，其手段、方式等是否符合法律要求。例如，当企业以爬虫方式从公开网站获取数据时，如果采取了不当措施导致被采集的网站经营者权益遭受侵害的，则应当承担相应的法律责任。结合我国司法实践，针对不当采取爬虫技术抓取数据而损害他人权益的行为，既可从反不正当竞争的角度，对于该种行为予以民事侵权上的苛责；在情节严重的情况下，例如使用技术手段规避或突破他人网站设置的技术保护措施的手段抓取数据的，甚至可能构成侵入计算机信息系统等犯罪行为；而在抓取的数据属于他人采取技术措施保护的个人信息的情况下，也将可能落入侵犯公民个人信息罪的范畴，从而需要承担相应的刑事责任。正是注意到爬虫等自动化数据采集手段对于多方利益带来的困扰，我国在最近颁布的《数据安全管理办法（征求意见稿）》中为自动化采集划出“红线”，[15]在刑事责任之外，以行政性规范要求的方式力求实现自动化数据采集的规范运作。

[14] https://consult.industry.gov.au/strategic-policy/artificial-intelligence-ethics-framework/supporting_documents/ArtificialIntelligenceethicsframeworkdiscussionpaper.pdf

[15]《数据安全管理办法（征求意见稿）》第十六条规定，网络运营者采取自动化手段访问收集网站数据，不得妨碍网站正常运行；此类行为严重影响网站运行，如自动化访问收集流量超过网站日均流量三分之一，网站要求停止自动化访问收集时，应当停止。

• 人脸识别：个人数据权益与公共安全监控的冲突

如前所述，计算机视觉技术已经开始广泛应用。在金融、移动、安防等产业，人脸识别是当前商业成熟度较高的计算机视觉产品，广泛应用于账号身份认证、手机刷脸解锁、人流自动统计和特定人物甄别等诸多场景。[16]然而，人脸识别技术由于涉及人们面部生物特征的采集与识别，具有极高的隐私敏感性；如稍被滥用，则可能对公民隐私保护产生极大威胁。正是考虑到技术不成熟和技术滥用可能导致的隐私威胁，部分国家、地区开始对公权力机关使用人脸识别技术进行执法活动予以限制和禁止。2019年7月17日，美国的奥克兰市通过一项法案，包括警察在内的市政机构人员将被禁止获得或使用人脸识别技术，成为继今年五月份旧金山和六月份萨默维尔后，美国第三个禁用人脸识别技术的城市。[17]奥克兰市议会主席在其报告中表示，人脸识别技术通常并不准确，可能具有入侵性，且缺乏统一标准。报告进一步指出，错误的人脸识别可能导致滥用武力、错误监禁，且可能加剧种族偏见问题。[18]从公权力的角度，人脸识别技术确乎为公共安全监控提供了更加高效、便利的途径，在我国已被使用于诸多安监及犯罪侦查场景，例如火车站进站验证、酒店入住验证、犯罪嫌疑人面部匹配等。而另一方面，人脸识别涉及较高敏感度的个人隐私信息，以实现公共安全防控目的而过多采集和处理公民隐私信息，是否合乎必要原则仍有待商榷；而当技术由于本身局限性而做出错误决策，导致公民主体权益受损时如何弥补，也为人脸识别技术的应用提出了难题。

• 自动化决策：机器决策下的个人主体权益保障

在人工智能算法应用于自动化决策的场景下，相关法律法规从保障主体权益的角度，立足于公平原则，对企业应用自动化决策技术提出了具体要求。我国《电子商务法》第十八条要求电子商务经营者在根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务的搜索结果时，应当同时向该消费者提供不针对其个人特征的选项。当前，电子商务经营者积累了大量用户个人信息、交易记录等，并利用大数据对消费者进行个人画像，通过自动化决策技术，能够实现为消费者呈现个性化的搜索展示，实现精准营销。这种“区别化”对待的方式，极易因自动化决策程序的算法设置而缩减甚至抹杀用户全面了解商品价格、商品信息的机会，从而对其知情权和公平交易的权利造成侵害。据此，法律要求电子商务经营者应同时为消费提供非基于自动化决策的商品搜索结果，以实现尊重和平等保护消费者合法权益。类似的，在《信息安全技术 个人信息安全规范》中，明确提及如果当仅依据信息系统的自动决策而做出显著影响个人信息主体权益的决定时（例如基于用户画像决定个人信用及贷款额度，或将用户画像用于面试筛选），个人信息控制者应向个人信息主体提供申诉方法。这一要求旨在确保当主体权益因自动化决策结果而受到影响时，保障受影响的主体质疑自动化决策所做结论的权利。

当然，对于人工智能引发的问题思考不止步于此。当下，随着人工智能产品越来越趋于复杂化，各类技术的交叉使用、技术的更新迭代必将引发更多的社会问题。而不同学科也在基于不同角度去审视，去一遍又一遍地给予人工智能未来征途以“灵魂敲打”。站在法学领域的高度，上至人工智能是否能够具备法律意义上的“人”的资格这一总括性问题，下至人工智能的“创作”可否受到保护、人工智能侵害他人权益如何进行责任分配等这些具象化问题，均会随着技术的脚步迈向更高层次、更广领域的思考与讨论。这些问题均离不开对人工智能技术的透彻理解。从上述各国人工智能伦理性问题研究的最新进展也可以看出，**多数国家对于算法的透明性和可解释性提出了明确要求，这也是解决因算法引发歧视性问题的一个有效路径**。我们将在未来的系列文章中与大家做深入的分享和探讨。

（本文发布于2019年09月21日。）

[16] 参见信通院《人工智能发展白皮书产业 应用篇》。

[17] Oakland bans the use of facial recognition, becoming third US city to do so, see at https://www.foxnews.com/tech/oakland-bans-facial-recognition-third-us-city

[18] Oakland bans use of facial recognition technology, citing bias concerns, see at https://www.sfchronicle.com/bayarea/article/Oakland-bans-use-of-facial-recognition-14101253.php

AI与大数据的“理想城”：智慧城市合规的基础要点

一、背景

庚子鼠年之初，突如其来的新冠肺炎疫情让各地纷纷启动重大突发公共卫生事件一级响应，举国上下竭尽所能加入到疫情防控保卫战之中，城市综合治理面临前所未有的挑战。正如我们在前面三篇文章中的探讨，在疫情防控背景之下，健康医疗数据的共享[1]、与疫情相关的政务数据资源共享与合理公开[2]以及联防联控工作中对个人信息的保护[3]，都成为了这个特殊时期数据合法合规利用应当关注的重点内容。而在此之上，从城市整体规划的角度出发，充分发挥高新技术的赋能助力效用，加快建设全面统筹、服务全局的智慧城市则为未来数据的有效综合治理提供了进阶方案，响应了城市治理的现代化要求，成为了当下及未来城市规划的题中之义。

如今，在城市治理亟需升级增智的情势之下，2月10日，上海市发布《关于进一步加快智慧城市建设的若干意见》，提出了“到2020年，将上海建设成为全球新型智慧城市的排头兵，国际数字经济网络的重要枢纽”的建设目标，要求统筹完善“城市大脑”架构，全面推进政务服务“一网通办”，全面赋能数字经济蓬勃发展，切实保障网络空间安全，全面增强智慧城市工作合力。[4]

建设智慧城市不仅是应对公共事件的良药，也是适应新时代社会经济发展和技术革新的必然要求。21世纪以来，新型工业化国家城市化进程加速，据预测，到2050年，近68%的世界人口将生活在城市。[5]大量涌入城市的人口将给城市管理者带来包括资源分配、交通堵塞、环境卫生等方面的巨大挑战，促使城市顺应信息化建设的潮流，借助先进信息技术发展力量，寻求城市规划和城市治理的新方法，提供交互式和包容性的创新城市系统，破解城市发展困局，保障居民需求，不断优化和提升，最终实现城市的可持续发展。[6]当下，我国的智慧城市建设以雄安新区为代表，其规划以集中承接疏散北京非首都功能为出发点，[7]以人工智能、大数据、物联网等前沿技术为依托，旨在实现城市的智慧化管理，拓展地下空间利用率，建设智能高效宜居新型城市，打造全球领先的数字城市，为我国城市化的变革提供一个以创新技术驱动的未来城市样本。[8]

---

[1]《疫情防控丨同舟共济——不同场景下健康医疗数据流转的合规路径》，https://mp.weixin.qq.com/s/_NXx6lZUrZc4WtADDnqoug.

[2]《疫情防控 | 数据资源流转与公开》，https://mp.weixin.qq.com/s/tGfEjt9qbEZUy1JW-jRq2Q.

[3]《疫情防控 | “风口”的安全降落伞——解读APP收集个人信息的最新规范》，https://mp.weixin.qq.com/s/zz8ZDuQC1uLVxmaQBCld9w.

[4]上海市关于进一步加快智慧城市建设的若干意见.

[5]United Nations, Department of Economics and Social Affairs, 2018 Revision of World Urbanization Prospects, see at https://www.un.org/development/desa/publications/2018-revision-of-world-urbanization-prospects.html.

[6]许晶华. 我国智慧城市建设的现状和类型比较研究[J]. 城市观察: 2012(4). 2012.

[7]国务院关于河北雄安新区总体规划（2018—2035年）的批复.

[8]详见雄安新区建设规划代表了智慧城市最新思维[EB/OL]. http://www.xinhuanet.com//fortune/2018-04/23/c_129856636.htm. 2018-04-23.

二、智慧城市发展现状

（一）智慧城市的概念和内涵

“智慧城市”一词诞生于20世纪90年代，其定义和内涵持续演变，各界由于出发点和侧重点不同，目前暂无统一和明确的权威性定义。[9]但总的来说，智慧城市是充分利用新科技和新思想，让城市系统、运作和服务得以改造和升级，更具智慧的城市。[10]具体而言，智慧城市的建设以数字化、智能化的城市基础设施为基础，运用物联网、云计算、大数据、移动互联网等新一代信息通信技术手段，整合城市运行核心系统关键信息，[11]强调城市信息的全面感知，城市生活的智能决策与处理，实现城市经济和社会组织的高效化和协作化，城市社会服务的普惠化与人性化。[12]

（二）域外发展

智慧城市作为未来城市的发展方向，许多国家都将智慧城市建设纳入国家战略，成为各国提升全球信息化竞争力的重点关注内容。德勤研究报告显示，目前全球在建智慧城市数量超过1000，无论是发达国家还是发展中国家，都积极参与到智慧城市的建设之中，推动新一轮的城市变革，现已形成了多个智慧城市群。[13]下表请见选取的三个智慧城市建设先驱国家的发展概况及典型案例列举。

区域	近期国家战略/规划	典型案例
美国	*2015年联邦政府发布《白宫智慧城市行动倡议》，宣布将投入至少1.6亿美元用于包括智慧城市建设在内的物联网运用研究项目，一方面通过国家科学基金会（NSF）和国家标准和技术研究所（NIST）向学术机构分别提供3500万美元和1000万美元，以加强智慧城市基础技术研发；另一方面通过国土安全部、交通部、能源部、商务部等政府相关部门投入4500万元，推动安全、能源、气候应对、交通等领域应用技术研发。[14] *2017年1月，美国网络与信息技术研发计划（NITRD）智慧城市与社区任务组发布《智慧城市与社区联邦战略计划：共同探索创新》草案报告，指导和协调智能城市/相关社区的联邦活动，促进当地政府与利益相关方的参与。[15] *2019年联邦政府发布《美国人工智能倡议》，要求联邦政府将人工智能的发展与研发放在首要位置，并且将更多的资源与经费用于人工智能技术的开发与推广，其中包括对利用人工智能进行的智慧城市的开发。[16]	**圣地亚哥——“世界上最大的城市路灯物联网传感器网络”** 与通用电气合作，在14000盏LED路灯上安装4200个智慧节点，嵌入多个感应器，以灯柱为基础打造一个开放、安全的数位基础设施，并在此之上安装智能城市设备，同时大量开发数据API端口和应用，连接市内警察局、交通管理局等多个部门，实现对城市主要街道活动的监测，进而优化公共交通、强化应急管理、改善公共安全。[17]
日本	*2010年日本经济产业省制定“环境未来都市”国家战略项目，制定智能城市五年计划。 *2011年东部大地震后，经济产业省制定智能电网发展计划。 *2012年，总务省实行日本震后以防灾为重点的“ICT智慧城综合战略”。[18]	**福冈——“从人为本到落实参与”** 与LINE合作，以LINE账号好友为基础，协助市政解决市民在日常生活中最棘手的问题，如解决回收大型垃圾的时间的限制、加速公共设施毁损保修、提供避难行动支援，实现从防灾准备到复原的多功能服务。[19]

[9] 亿欧智库. 道阻且长，行则将至：2019年中国智慧城市发展研究报告[R]. 2019.

[10] IBM Institute for Business Value, Smarter Cities for smart growth, 2010.

[11] 许晶华. 我国智慧城市建设的现状和类型比较研究[J]. 城市观察: 2012(4). 2012.

[12] 中国电子技术标准化研究院. 中国智慧城市标准化白皮书[R]. 2013.

[13] 德勤. 超级智能城市2.0：人工智能引领新风向-全球城市在进阶[R]. 2019.

[14] 海外如何推进智慧城市政策[EB/OL]. https://bbs.pinggu.org/thread-5916513-1-1.html. 2017-08-12.

[15] 美NITRD发布“智慧城市与社区联邦战略计划”[J]. 网络安全和信息化动态: 2017(3). 2017.

[16] American AI Initiative, see at https://www.whitehouse.gov/ai/executive-order-ai/.

[17] Robert Moss, Building a Smart City? Start with Street Data, see at https://www.insight.tech/cities/building-a-smart-city-start-with-street-data.

[18] “日本智慧城市建设案例与经验”[EB/OL]. https://mp.weixin.qq.com/s/D7HzzAqrs5VQVKMucWznDg. 2017-07-15.

[19] Susan Hong. 打造市民参与的智慧城市[EB/OL]. EE Taiwan. https://www.eettaiwan.com/news/article/20191118NT01-building-citizen-centric-smart-cities. 2019-11-18.

区域	近期国家战略/规划	典型案例
新加坡	*2015年，信息通信部发布“智慧国家2025”计划，明确数据泛在采集、智能分析与处理等建设重点。 *2017年， 新加坡推出包括国家身份系统、电子支付平台、生命时刻计划、智能城市交通、智能国家传感器平台、以及统一数码平台（CODEX）在内的五项国家计划。[20]	新加坡——“整体政府框架下的智慧国” 建立完善的信息化基础设施，实现WIFI全覆盖，实现公共服务网络化，利用ICT技术建立跨行业的信息交换系统和综合医疗信息平台，积极推进远程医疗。[21]

（三）国内现状

我国国家层面的智慧城市建设始于2012年，住建部发布《关于开展国家智慧城市试点工作的通知》，启动了中国智慧城市的试点申报和实施管理。2014年，国务院发布《国家新型城镇化规划（2014-2020）》，将智慧城市建设与绿色、人文城市并列作为推进新型城市建设的范式，[22]首次将智慧城市建设引入国家战略，并提出到2020年，建设一批特色鲜明的智慧城市。[23]2016年，国家发布的“第十三个五年计划”中，智慧城市被列为新型城镇化重大工程。此后，国家出台了一系列关注智慧城市基础设施建设和细分场景的指导意见，并由全国信息技术标准化委员会、全国通信标准化委员会领头，制定了多项有关智慧城市建设的国家标准体系，内容涵盖智慧城市的顶层设计、总体框架、评价模型及基础评价指标体系等多个方面，为智慧城市建设提供技术指引。[24]2019年年末，住建部决定成立智慧城市专业委员会，旨在进一步组织展开智慧城市领域的基础性研究，加强对地方智慧城市建设工作的指导。

与国家层面的智慧城市建设并行，各地智慧城市也积极加入到智慧城市建设的浪潮之中，结合各区域的发展需求，纷纷提出智慧城市发展规划。截至目前，全国智慧城市试点已基本覆盖全国各个省、市和自治区。[25]

三、智慧城市的技术框架与数据

作为“互联网与城市建设结合的样本”，智慧城市的搭建遵循了互联网大脑架构的基本原理，通过城市中枢神经系统（即“城市大脑”）[26]作为沟通智慧城市物联网系统、基础设施建设和人工智能建设的纽带，完成大数据在智慧城市技术框架下的汇聚、流转与应用，并由此产生城市智慧。

（一）智慧城市技术框架介绍

智慧城市技术框架的研究既有助于明确相关技术的研究和发展方向，同时也对智慧城市标准化工作和智慧城市运行中的合规监管提供了重要的借鉴。关于智慧城市的技术体系研究众多，包括但不限于微软亚洲研究院提出的“城市感知与数据捕获”、“城市数管理”、“城市数据分析”、“服务提供”的四层反馈结构，[27]科技部863计划在2012年《智慧城市技术白皮书》中总结的“城市感知层”、“数据传输层”、“数据活化层”、“支撑服务层”、“应用服务层”及“行业服务层”和“标准与评估体系”、“安全保障体系”的“六横两纵框架”[28]等。而在2013年发布的《中国智慧城市标准化白皮书》中，智慧城市的技术体系被界定为“四个层次要素和三个支撑体系”，即物联感知层、网络通信层、数据及服务支撑层、智慧应用层和标准规范体系、安全保障体系和建设管理体系。[29]

[20] 党倩娜. 新加坡智慧城市主要战略计划及具体举措[EB/OL]. 第一情报- ISTIS视点. http://www.istis.sh.cn/list/list.aspx?id=12363. 2019-12-02.

[21] 探讨新加坡如何构建智慧城市范本[EB/OL]. https://tech.hqew.com/fangan_1875990.2017-05-23.

[22] 徐振强, 刘禹圻. 基于“城市大脑”思维的智慧城市发展研究[J]. 区域经济评论, 2017(1).

[23] IBM Institute for Business Value, "Smarter Cities for smart growth", 2010.

[24] 国务院关于河北雄安新区总体规划（2018—2035年）的批复.

[25] 国务院关于河北雄安新区总体规划（2018—2035年）的批复.

[26] 智慧城市的互联网大脑架构图，大社交网络与智慧城市结合是关键[EB/OL]. https://mp.weixin.qq.com/s/3lZ3JfYaNQpJZOyOKXe7HA. 2016-11-03.

[27] 郑宇. 城市计算与大数据[J]. 中国计算机学会通讯. 2013, 9(8): 8-18. 转引自：王静远, 李超, 熊璋, 单志广. 以数据为中心的智慧城市研究综述[J]. 计算机研究与发展, 2014, 51(02):239-259.

[28] 863计划“智慧城市（一期）”项目组. 智慧城市技术白皮书[R]. 2012.

[29] 中国电子技术标准化研究院, 全国信息技术标准化技术委员会SOA分技术委员会. 中国智慧城市标准化白皮书[R]. 2013.

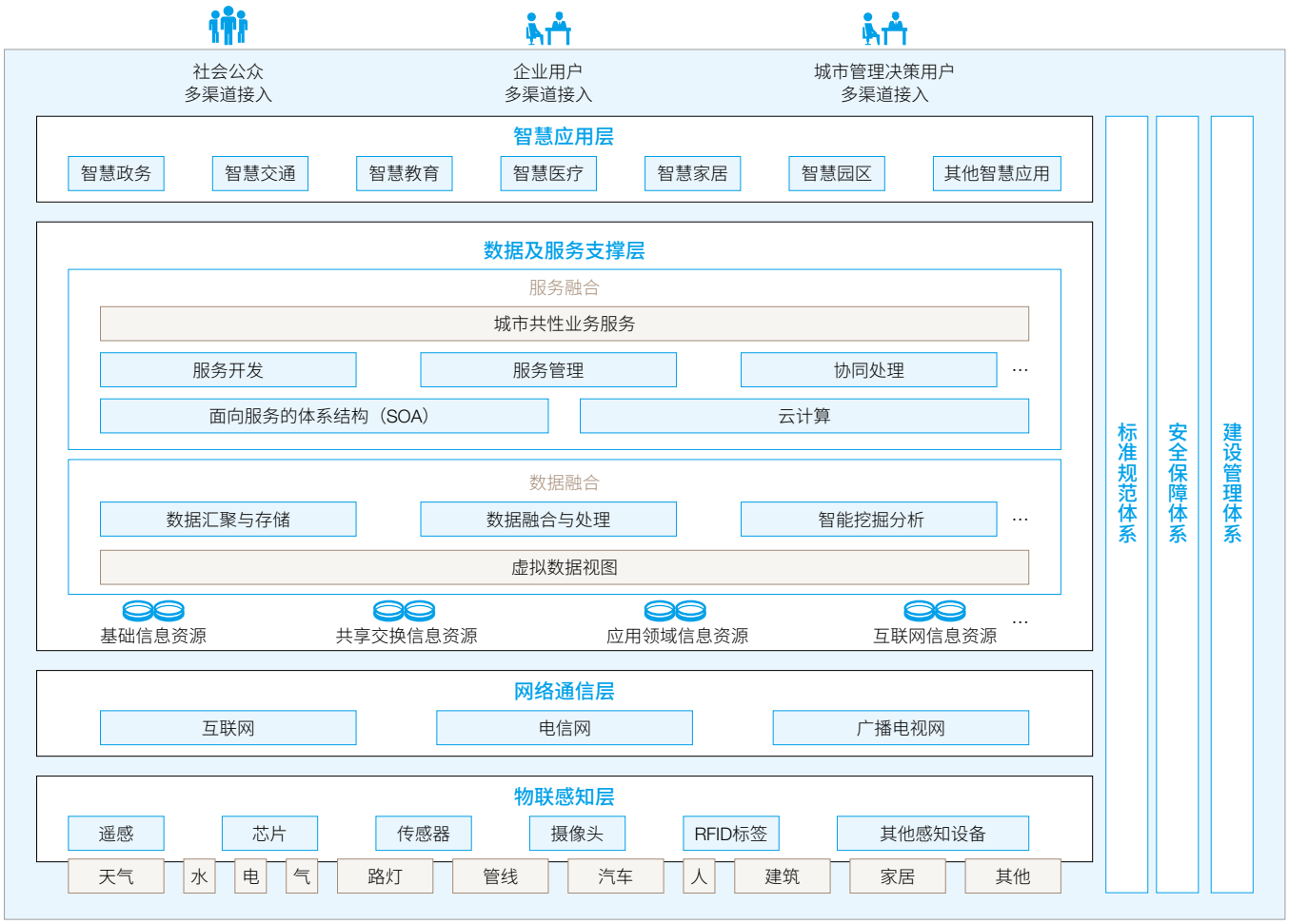


图1 《智慧城市标准化白皮书》智慧城市技术体系框架

其中，数据与服务支撑层可以被进一步划分为数据支撑层和服务支撑层；同时在整个技术框架中，在物联网感知层之外还有更底层的“社会基础设施”，即与智慧城市建设相关的配套硬件设施，[30]因此，我们理解智慧城市的技术框架可以分为六个层次，即：

- **基础设施层：**基础设施层是指与智慧城市建设相关的配套硬件设施，除了传统的信息中心机房、信息亭[31]外，智慧城市中的基础设施还包括5G商用网络的基础设施、云计算数据中心等。[32]
- **信息感知层：**信息感知层是指通过物联网络射频识别、传感和智能嵌入等技术及设备，捕捉、识别和采集城市系统信息数据的技术环节，其所涉及的场景极为丰富，举例而言，上海市在2018年发布的《新型城域物联专网建设导则》中，例举了公共安全、公共管理、公共服务中共计33类场景的物联感知要求。[33]
- **网络通信层：**网络通信层通过“普适、共享、便捷、高效的网络通信基础设施，为城市级信息的流动、共享和公用提供基础”，[34]其中5G商用网络的建设提速为新型智慧城市建设发展赋能，“低时延、高带宽”的5G网络为对实时性要求较高的高清直播、无人

[30] 臧维明, 李月芳, 魏光明. 新型智慧城市标准体系框架及评估指标初探[J]. 中国电子科学研究院学报, 2018, 13(01):1-7.

[31] 臧维明, 李月芳, 魏光明. 新型智慧城市标准体系框架及评估指标初探[J]. 中国电子科学研究院学报, 2018, 13(01):1-7.

[32] 参见中国信息通信研究院. 新型智慧城市发展研究报告[R]. 2019.

[33] 上海市经济和信息化委员会. 新型城域物联专网建设导则[S]. 2018.

[34] 中国电子技术标准化研究院, 全国信息技术标准化技术委员会SOA分技术委员会. 中国智慧城市标准化白皮书[R]. 2013.

驾驶、车联网和远程手术等智慧应用的发展提供了动力和支持，[35]更增强了智慧城市通过全面实时数据进行事件预测和解决、需求分析和相应的能力。[36]

- **数据支撑层：**数据支撑层是指通过数据的资源交互共享和融合为智慧城市提供数据支撑，包括但不限于多源数据的标准化与汇聚融合、数据的安全存储与开放、数据融合与处理等，其中SOA（Service Oriented Architecture，面向服务的体系结构）、云计算和大数据等技术在这一层次中起到了“关键的技术支撑作用”。[37]
- **服务支撑层：**服务支撑层是指将前述层次的“数据资源和应用系统资源进行统一的服务化封装、处理及管理”以提供统一的“城市级的公共、共性信息类服务”，这些服务可能包括“位置服务、饰品店宝服务、社交网络服务、虚拟现实服务等”。[38]
- **智慧应用层：**智慧应用层则是将智慧城市的资源与能力与行业产业结合，为政府、企业、公众提供实际的智能化应用和服务。随着硬件设施的完善、底层数据资源的扩充和智慧城市技术的发展，智慧应用层的外延也在不断拓展，从智慧治理、智慧政务、智慧交通到智慧医疗、智慧养老、智慧生态……，智慧城市不仅仅在社会治理方面发挥着重要作用，也提升了社会服务的质量和效率；不仅仅涉及城市内部的生产生活关系，也有助于正确认知和处理城市与自然之间的关系。

（二）智慧城市中的数据

智慧城市同时还是大数据和数字技术的产物。中国信息通信研究院（“信通院”）在《新型智慧城市发展研究报告》中指出，“在数据驱动理念下，城市大数据平台日益成为新型智慧城市的核心组成平台”。[39]麦肯锡全球研究院在回答“城市的‘智慧’源自何处”时，也指出“机构获得的数据越全面、越实时，它们就越有能力观测事件发生的详情、分析需求模式的变化，从而采用响应更及时、成本更低的解决方案”。[40]

智慧城市中的数据类型体量庞大，具有“时空多维性、多尺度与多粒度、多元异构”等特征。 以智慧交通为例，其中所涉及的信息感知终端包括但不限于摄像头、车载终端、微波监测、超声波监测等，所采集的车辆及交通信息包括但不限于车辆属性、车辆速度、车辆行驶路径、行驶方向、排队时间等[41]，除采集的数据体量庞大外，不同的信息感知终端采集的数据结构也可能有所差异。此外，智慧城市在进行数据采集和分析应用时，还需要充分考虑数据在时间和空间维度的演化（即时空多维特性），和在不同的时间尺度和空间颗粒度时所采集数据的差异性和关联性（即多尺度与多粒度）。这些特性都对数据的安全存储及后续的融合利用带来了挑战。

四、智慧城市建设中的合规要点初探

人工智能、大数据等技术的飞速发展和应用于智慧城市的实践有助于构建一个更加宜居的城市家园。但另一方面，为智慧城市建立规范标准体系、安全保障体系和建设管理体系，平衡公共利益与个体权利的保护，与智慧城市的技术发展和实践同等重要，这也是各国智慧城市实践中正在关注的内容。以人工智能技术运用及数据融合为例，如何在运用技术过程中识别并防范风险、平衡不同主体的利益，是发展智慧城市的必答题。

（一）人工智能技术在新型智慧城市建设中的伦理风险与使用边界

从城市大脑、自动驾驶到人脸识别，人工智能技术已经融入到智慧城市的“数据管理、智慧交通、惠民服务、智慧安防、智能制造等各类领域”。[42]人工智能的运用在为新型智慧城市赋

[35] 中国信息通信研究院. 新型智慧城市发展研究报告[R]. 2019.

[36] 参见麦肯锡全球研究院. 智慧城市：数字技术打造宜居家园[R]. 2018.

[37] 中国电子技术标准化研究院, 全国信息技术标准化技术委员会SOA分技术委员会. 中国智慧城市标准化白皮书[R]. 2013.

[38] 中国电子技术标准化研究院, 全国信息技术标准化技术委员会SOA分技术委员会. 中国智慧城市标准化白皮书[R]. 2013.

[39] 中国信息通信研究院. 新型智慧城市发展研究报告[R]. 2019.

[40] 参见麦肯锡全球研究院. 智慧城市：数字技术打造宜居家园[R]. 2018.

[41] 王静远, 李超, 熊璋, 单志广. 以数据为中心的智慧城市研究综述[J]. 计算机研究与发展, 2014, 51(02):239-259.

[42] 中国信息通信研究院. 新型智慧城市发展研究报告[R]. 2019.

能，引领并开拓智慧城市的新型应用场景的同时，也相应地在一定程度上为智慧城市下的社会治理和社会服务嵌入了伦理风险。在智慧城市的语境下，平衡人工智能技术所带来的生产效率提升和可能的歧视风险，需要城市管理者在关注人工智能技术自身伦理道德体系的构建，评估人工智能在智慧城市中的利用带来的伦理风险的基础之上，合理界定人工智能技术在智慧城市中的使用边界。

• 智慧城市建设中的人工智能伦理之算法相关风险点

智慧大脑作为智慧城市系统的关键，其决策将现实影响整个城市的资源调配。置身智慧大脑操控运作的城市之中，大家需要对人工智能决策的可靠性进行严密的论证。鉴于算法伦理在人工智能伦理的基础地位，[43]问题的症结则在于与机器算法相关的伦理风险，具体包括：算法公正性（算法歧视）、算法透明度及结果可解释性等。

首先，算法歧视，通常是指由于算法的设计者或开发人员对事物的认知存在主观上的某种偏见，或不经意使用了带有偏差的训练数据集等原因，造成模型准确性的偏差甚至产生歧视性的结果。[44]具体而言，其原因有三：

一是数据中预先存在的偏见所导致的算法歧视；

二是使用算法本身可能是一种歧视；

三是算法决策中数据的抽样偏差及其所设置权重的不同也有可能导致算法歧视。[45]

在现实生活中，算法歧视并不罕见，无论是亚马逊人工智能招聘系统涉嫌性别歧视[46]、还是美司法部门利用COMPAS系统预测再犯罪率导致种族歧视的争议，[47]人工智能算法在决策时可能产生偏见和歧视已经在某种程度上成为共识，在公共领域审慎使用人工智能技术的呼声也时常出现。因此，在智慧城市建设过程中，城市管理者理应对人工智能技术，特别是算法模型的初始设计和后续运用的全流程进行全面审慎评估，以确保算法的公正性。

其次，人类对算法的安全感、信赖感、认同度可能取决于算法的透明度和结果的可解释性。[48]算法的透明度旨在通过向用户公开算法细节，保障用户对算法的知情权，而结果的可解释性则需要确保算法、输入数据与输出结果之间的紧密联系。[49]就人工智能技术的运用而言，人们质疑智慧大脑的自主决策，主要是因为系统输出决策之时，往往并不提供做出具体决策所依据的材料、理由并证明结果与输入数据的紧密关系。[50]因此，在技术层面，智慧城市的人工智能开发，应当以强调用户与自动化决策系统的交互为核心，在已评估解释具体应用模式的难易程度的基础之上，考虑设置机制向用户解释系统产生的结果与参考标准，[51]增强人工智能决策的可信度。

• 智慧城市建设中的人工智能伦理之数据相关风险点

界定人工智能技术在智慧城市中的使用边界另一个动力，可能源于人工智能技术对海量数据的需求所带来的数据质量、隐私保护等多方面的风险。

首先，以数据安全与隐私保护为例，人脸识别技术作为人工智能技术的典型拓展，人脸识别在现代社会中的运用越来越广泛，就智慧城市而言，截至2019年，“全国已有40余个城市启动了‘刷脸政务’，覆盖范围囊括商事登记、交通罚单缴纳、公积金查询、个税申报、社会保障等”，[52]人脸识别技术的运用能够通过对面部识别特征的采集和比对实现更精准高效的个人身份认证，为民众在办理政务服务过程中的身份认证提供更多的选择。但另一方面，面部识别特征属于个人敏感信息，具有高度的人身属性。而随着在银行、非金融支付机构等对人脸识别技术的运用，面部识别特征还与个人财产安全产生了密切的联系。在该情况下，如果对人脸数据的安全保障措施不能与采集人脸数据的实践范围相匹配，隐私泄露的风险可能大大增加，因此综合考虑人

[43] 孙保学. 人工智能算法伦理及其风险[EB/OL]. https://mp.weixin.qq.com/s?src=11&timestamp=1579588170&ver=2109&signature=0v59Q8kFXMuLiH9VDlP057j00NeCJHnSzDOzRQ*Fdk3ppAe5MVEqo0a65SWg1fvEM0iMmlSN-ggNAo9UJ2mVaB0JZh5L8k6mdP-zvjazoplQR0vFbUVzZolHt*iuOKMK&new=1. 2019-12-20

[44] 全国信息安全标准化技术委员会大数据安全标准特别工作组人工智能安全标准化白皮书（2019版）[R]. 2019.

[45] 刘培, 池忠军. 算法歧视的伦理反思[J]. 自然辩证法通讯, 2019(10).

[46] AI时刻. 亚马逊AI招聘工具被爆性别歧视，不喜欢女的?[EB/OL]. http://www.sohu.com/a/259640276_100183993. 2018-10-15.

[47] 张俊贤. 违规、歧视、安全问题，如何应对AI时代的风险[EB/OL]. https://www.yicai.com/news/100318593.html. 2019-09-23.

[48] 全国信息安全标准化技术委员会大数据安全标准特别工作组人工智能安全标准化白皮书（2019版）[R]. 2019.

[49] EC High-Level Expert Group AI Ethics Guidelines for Trustworthy AI, 2019.

[50] 曹建峰 算法歧视：看不见的不正义[EB/OL] https://zhuanlan.zhihu.com/p/31078631?from=timeline, 2017-11

[51] 中国电子技术标准化研究院人工智能标准化白皮书（2018版）[R]. 2018

[52] 中国信息通信研究院. 新型智慧城市发展研究报告[R]. 2019.

脸识别技术在智慧城市中的应用边界，适度在公共领域应用人脸识别技术，可能是平衡社会利益（社会治理及服务的效率）与个人利益（个人数据安全、隐私保护和财产安全）的手段之一。

其次，数据作为人工智能的基础资源，人工智能模型的精度受限于训练数据和影像数据的质量。[53]与前述算法的公正性紧密相关，若在算法模型中引入偏见数据或虚假数据，鉴于人工智能算法的“涌现性”和“自主性”，[54]系统将在学习过程中不断吸收偏见和错误知识，最终导致错误的预测结果。因此，将人工智能技术运用到智慧城市之中，结合系统机器学习对数据的依赖度，则需要追溯数据来源、分析考察数据的完整性和关联性，以验证数据的准确性，保证数据质量，进而避免人工智能系统决策的误导和误差性。[55]实**践中，也不妨采用“沙盒”等监管方式，利用封闭试点的试验方法，从实证角度来核查决策的准确性，从而反向验证基础数据样本的完整性和关联性。**

随着人工智能技术的飞速发展和广泛利用，其在智慧城市中的运用所带来的伦理风险可能不止于此。当人工智能所带来的新风险被许多人感知到的时候，人们自然希望法律能够因应这种风险提供新的保障。[56]因此，**对于人工智能技术开发者和智慧城市建设者、管理者而言，积极识别人工智能技术运用可能产生的伦理风险，遵循法律要求，维护道德底线，并界定使用边界，是智慧城市建设中应当承担的社会责任。**

（二）智慧城市中的数据融合与开放利用

海量数据的融合与开放利用是新型智慧城市的又一鲜明特征。不同于传统智慧城市中强调政务数据的共享交换，新型智慧城市模式下数据范围进一步扩大为城市大数据，[57]所涉及的不再仅仅是政务数据，还可能包括企业数据和个人信息。如何在现有法律法规的规制下，实现数据的汇聚与融合？如何从法律层面明确智慧城市系统中的数据安全责任？如何界定智慧城市中数据的开放共享范围等等，都是智慧城市发展亟需回答的问题。

• 在尊重数据资产价值、保障个人信息的基础上开展数据汇聚融合，打破数据孤岛

新型智慧城市模式中的数据不仅仅包括传统政务数据，还可能包括大量的企业数据和个人信息。

而无论是前者还是后者，都可能面临着数据控制者不愿、不敢、不能对外共享数据，进而形成数据孤岛，阻碍数据汇聚融合的情形。**其一**，对企业而言，随着数字经济时代数据作为资产的价值得到日益广泛的认可，并成为企业核心竞争力的一部分，对某些数据的独占可能会巩固和强化企业的竞争优势，企业对外共享数据的动力也因此受到抑制。**其二**，目前国内的法律法规对于政务数据的公开共享、不同行业数据的公开共享和个人信息的公开共享都有所规定和限制，如国务院在《政务信息资源共享管理暂行办法》中规定“不宜提供给其他政务部门共享使用的政务信息资源属于不予共享类”；[58]《中华人民共和国人类遗传资源管理条例》中要求组织、个人在采集、保藏、利用、对外提供我国人类遗传资源（利用含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料产生的数据等信息资料）时，不得危害我国公众健康、国家安全和社会公共利益；[59]而中国人民银行在新近制定的《个人金融信息（数据）保护试行办法（草案）》中，对金融机构对外共享个人金融信息进行了严格的限制，这些规定和限制可能导致政府部门、企业等因为存在法律风险而不敢对外共享数据。**其三**，数据在采集标准、统计口径和传输接口方面可能存在的较大差异，也使得数据拥有者不能对外共享数据。

面对数据孤岛，**智慧城市的发展需要遵守现行法律法规对数据融合的禁止性、限制规定，在合法合规的基础上完成数据汇聚融合，同时也应当通过智慧城市运作模式优化，为不同主体和不同来源的数据参与数据汇聚融合提供激励；通过法律法规确定智慧城市中数据融合的范围，并适度协调智慧城市建设中数据融合需求与其他数据保护规则之间的张力；通过统一的数据采集、传输标准确保数据融合的技术可行性。**

• 明确数据安全责任、建立数据安全事件应急联动机制是保障智慧城市数据安全的重要途径

新型智慧城市模型中海量数据的融合还会对系统的数据存储处理和安全保障能力产生考验。智慧城市下的海量数据及其背后的数据价值可能引发针对性的数据攻击，造成个人信息、重要数据的泄露和智慧城市运营系统的崩溃。具体而言，从数据属性角

[53] 全国信息安全标准化技术委员会大数据安全标准特别工作组人工智能安全标准化白皮书（2019版）[R]. 2019.

[54] 全国信息安全标准化技术委员会大数据安全标准特别工作组人工智能安全标准化白皮书（2019版）[R]. 2019.

[55] Personal Data Protection Commission, A proposed Model Artificial Intelligence Governance, 2019.

[56] 郑戈. 人工智能与法律的未来探索与争鸣[J]. 2017

[57] 中国信息通信研究院. 新型智慧城市发展研究报告[R]. 2019.

[58]《政务信息资源共享管理暂行办法》第九条第四款。

[59]《中华人民共和国人类遗传资源管理条例》第二条、第八条。

度来看，智慧城市中可能包含大量的政务数据、企业数据和个人信息，其中不乏涉及国家安全、商业秘密和个人隐私，因而数据安全是智慧城市建设中的重中之重。同时，从网络系统安全角度来看，智慧城市的大数据平台可能与多个网络安全保护等级较高的系统，如金融行业、医疗行业系统等进行对接，因此从网络安全等级保护的相关要求出发，同样需要对智慧城市的系统安全性加以重视。

就数据安全和系统安全而言，考虑到智慧城市技术框架下涉及数据的产生、收集、存储与处理、融合、应用和对外提供等多个环节，包括数据原始所有者、数据传输系统运营者、数据能力提供者、数据服务使用者等多个主体，智慧城市的运行有必要在建立数据存储和安全保障技术标准的同时，明确数据流转的不同环节中相关主体的数据安全责任，鼓励各主体积极采取适当的数据安全措施，建立合适的数据安全管理制度，并在发生数据安全事件，对社会、企业或个人造成损害时承担相应的责任；同时还可以考虑制定适用于智慧城市框架的数据安全事件应急联动机制，以便在发生数据安全事件时及时发现并采取响应措施，降低数据安全事件的损害后果，保障数据安全。

- **分级分类界定智慧城市中数据的开放利用范围，在保障信息安全和数据主体利益的同时实现数据价值的最大化**

数据的开放与共享是智慧城市发挥作用、展现能力的重要前提。智慧城市顶层设计下的数据支撑层、服务支撑层和智慧应用层均不同程度涉及数据的开放和共享。以上海为例，2019年11月，上海市公共数据平台正式开通运行，开放的2100项公共数据“基本覆盖各市级部门的主要业务领域”并重点聚焦“金融、医疗、旅游、交通、能源、城市管理和开放数据等7个领域”。[60]但无论是政务数据、企业数据还是个人信息，从信息自身价值、信息开放的制度成本和基础设施成本、信息开放产生的社会价值、不当或非法利用信息可能造成的后果等角度来考量，智慧城市中的数据不能也不应无限制地向社会公众开放。

在这种情况下，数据的分级分类开放将成为数据共享与利用的必然选择，即依据相关法律法规的要求，参考数据开放对象的安全保护能力、获取数据的主体对开放数据的使用目的和方式等情况对数据进行分级分类开放。例如，电子病历、医疗影像图片等数据的开放将有助于智慧医疗下AI诊疗算法的训练与优化；但另一方面电子病历、医疗影像图片等数据的开放又会受到行业监管及个人信息保护等方面法律法规的制约，在这种情形下，数据的开放一方面需要保障承接主体具有适当的数据安全保护能力，针对特定群体开放；另一方面，鉴于AI诊疗算法的优化这一用途并不以识别电子病历、医疗影像图片中的个人信息为前提，政府或有关机构在开放该部分数据时，可以考虑在技术可行的范围内对数据进行脱敏、去标识化等处理，以尽可能降低数据开放利用的风险，同时最大限度促进对数据的利用。

五、小结

智慧城市是现代化治理的重要体现，也是社会经济和技术发展到一定高度后的必然选择。但如何在提高治理能力，维护公共利益的同时，平衡社会与个体的权利关系，是从技术、法律、道德伦理多个角度的重大考验。结合上文的初步分析，我们建议智慧城市的建设过程中应当注重以下方面：

1、注重人工智能道德伦理的论证，成立人工智能道德伦理委员会，建立人工智能道德伦理风险评估机制。

2、对于核心算法的透明性、公正性和准确性等建立事前、事中和事后的监管机制，建议通过“沙盒”等方式验证算法的公正性等。

3、确认人工智能技术在不同场景下，尤其是公共领域的使用边界，加强算法透明性。

4、论证数据融合的合理性和合法性，针对不同行业、不同主体数据的数据融合建立合规制度和标准。在不违反现行法律法规的前提下，有限度的实施数据融合。

5、加强数据基于安全、价值等不同维度的分级分类，平衡数据融合后关于网络及数据安全的责任以及数据开放共享的价值分配，建立合法合规的责任体系和数据共享使用标准。

当然，给智慧城市的答卷远不止于此，我们也会在今后的文章里和大家一起分析和探讨我们新的思考。随着人们不断加深的对智慧城市的认识和对智慧城市边界的探索，智慧城市所面临的更多具体的风险也可能会相应地显现。如何正确处理这些问题，可能需要技术、法律、道德伦理等多个方面协作分析。从六千年前乌鲁克城诞生、到近代工业化城市的兴起，城市与人类之间的关系始终在社会文明进程中占据一席之地，城市模式的发展与创新，体现了人类对更美好生活的追求，而对城市模式中技术及伦理风险的认知和探讨也最终将帮助人们寻得更宜居的家园并推动社会文明的进步。我们坚信智慧城市的发展，最终将再次印证这一事实，并期待包括法律在内的人文科学在技术和社会变革中发挥应有的作用。

（本文发布于2020年02月19日。）

[60] 上海市公共数据开放平台开通[EB/OL]. http://www.gov.cn/xinwen/2019-11/20/content_5453799.htm. 2019-11-20.

“AI”的伦理风险与建议

引言

1956年的暑期，计算机学家John McCarthy首次提出Artificial Intelligence（人工智能，简称“AI”）的概念。此后，AI又根据发展程度被进一步划分为：弱人工智能ANI[1]、强人工智能AGI[2]和超级人工智能ASI[3]三个阶段。60多年后的今天，ANI已经在不知不觉中成为我们生活的一部分，从汽车自动驾驶、手机语音助手、邮箱垃圾邮件识别过滤、购物网站个性化推荐、输入法和翻译软件的智能语音识别、再到AI医疗辅助识别…… “我们已经生活在一个被弱人工智能包围的世界”[4]。

AI的发展有助于一个“智能的、精细化的和人性化的‘最好时代’”[5]的诞生，这也是我们无限憧憬着的更好的未来。但如同每项新技术一样，AI必须直面技术所带来的道德伦理风险质疑，特别是考虑到AI对于传统工具甚至人工劳动力的替代，其道德伦理风险一直以来都是争议的焦点。一方面，“社会必须信任人工智能技术能够给人带来的利益大于伤害，才有可能支持继续发展人工智能”，[6]因此如果无法对伦理风险作出回应，AI技术的发展和应用将会面临巨大挑战。另一方面，对伦理规范的研究“对于人工智能社会关系的调整……具有……先导性的作用”，能够先于法律为AI技术的发展提供规范和道德标准，并“为后续法制建设提供重要法源”，甚至“在一定时候，……转化为法律规范”[7]。

据此，本文将根据各国在AI伦理风险管理层面的指南及准则内容，从算法、数据和社会治理三方面对AI伦理风险的评估指标进行简要总结和例举分析，并就AI伦理风险和负责任的AI实践等问题进行探讨和分享。

一、各国AI伦理风险研究现状

尽管2019年3月初，联合国教科文组织总干事阿祖莱在“推动人性化人工智能全球会议”上表示，“目前还没有适用于所有人工智能开发和应用的国际伦理规范框架”。[8]但不可否认的是，在过去几年中，AI的伦理风险已经成为世界多国在该领域的重点关注问题。

2019年1月，新加坡个人数据保护委员会（PDPC）发布了《人工智能治理建议框架（征求意见稿）》，旨在帮助企业解决其使用人工智能可能面临的伦理道德及运行管理问题。[9]2019年4

[1] Artificial Narrow Intelligence.

[2] Artificial General Intelligence.

[3] Artificial Superintelligence.

[4] "Our world is full of these limited AI programs which we classify as 'weak' or 'narrow' or 'applied'… All these narrow AIs are like the amino acids in the primordial ooze of the Earth. The ingredients for true human-like artificial intelligence are being built every day, and it may not take long before we see the results." Saena, A. We Live in a Jungle of Artificial Intelligence that will Spawn Sentience, https://singularityhub.com/2010/08/10/we-live-in-a-jungle-of-artificial-intelligence-that-will-spawn-sentience/, Aug 10, 2010, cited on Jan 20, 2020.

[5] 吴汉东：《人工智能时代的制度安排与法律规制》，《社会科学文摘》2017年12期。

[6] 郭锐：《人工智能的伦理问题与治理原则》，载https://mp.weixin.qq.com/s?src=11&timestamp=1599035808&ver=2559&signature=zHkyW*aJCD8mzefWpz6roaRyM1v78co8HAG0rtYoWbUD-3FJJqvdltd0lEfbi8MjWYFq7YIT7NVmsHqLqxzBHVwdlq3gwwi7KiCitzDiftWcx7n8A82X2CpdJo6Wip1W&new=1，2019年8月30日。

[7] 吴汉东：《人工智能时代的制度安排与法律规制》，《社会科学文摘》2017年12期。

[8] 杨峻：《超越“机器人三定律”，人工智能期待新伦理》，载http://www.xinhuanet.com/2019-03/18/c_1124249611.htm，2019年3月18日。

[9] Personal Data Protection Commission, A proposed Model Artificial Intelligence Governance, 2019.

月8日，欧盟发布了《可信赖人工智能伦理准则》，指明人工智能的发展方向应为“可信赖人工智能”（“Trustworthy AI”），并提出了七项要求：保障人类能动性及监督能力、安全性、隐私数据管理、透明度、包容性、社会福祉和问责机制；[10]同时欧洲议会研究机构（EPRS）还发布了《算法责任与透明度治理框架》[11]，提出“将算法透明和责任治理作为解决算法公平问题的工具”[12]。2019年4月，澳大利亚英联邦科学与工业研究组织CSRIO的DATA 61起草了《人工智能伦理框架）讨论稿）》，明确了人工智能的八大核心原则：产生福利、不侵害、合法合规、保护隐私、透明度和可解释性、可争议及问责制原则。[13]2019年11月，美国人工智能国家安全委员会发布中期报告[14]，指出就国家安全层面而言，AI道德及可信赖性主要包括三部分：1）可信赖AI系统的设计和开发的伦理性；2）可信赖AI系统使用的伦理性；和3）使用AI时保留的权利与自由问题。

在中国，AI伦理风险同样是不可忽视的问题。自国务院2017年7月发布《新一代人工智能发展规划》，将人工智能的发展上升为国家战略；2019年4月，国家人工智能标准化总体组发布《人工智能伦理风险分析报告》，将AI的伦理风险划分为算法相关的伦理风险、数据相关的伦理风险、应用相关的伦理风险以及长期和间接的伦理风险，并从算法、数据和社会影响三个方面阐述了人工智能伦理风险评估指标。2019年5月，北京智源人工智能研究院发布《人工智能北京共识》，从研发、使用和治理三个方面提出了人工智能发展应当遵循的多项原则，包括（1）研究与开发中的“造福、服务于人、负责、控制风险、合乎伦理、多样与包容、开放共享”；（2）使用时的“善用与慎用、知情与同意、教育与培训”以及（3）治理中的“优化就业、和谐与合作、适应与适度、细化与落实、长远规划”原则。

二、AI伦理风险的基本评估要素

识别可能存在的风险并构建伦理风险评估框架，是控制AI伦理风险的重要途径。结合前述各国对AI伦理风险的研究及已经构建的可信赖AI标准，我们总结AI伦理风险的评估要素如下：

风险类别	评估指标	指标含义
算法相关	透明度	算法透明度是指研发者和应用者有义务保障用户对算法的知情权。
	准确性	算法准确性是指以统计结果为基础，衡量并提升AI系统的准确性程度。
	可靠性	算法可靠性是指AI系统应当具备一定程度的抗击打能力，建立应对攻击的必要防御机制。
	可解释性	算法可解释性需要确保算法、输入数据与输出结果之间的紧密联系。
	可验证性	算法可验证性是指算法能在不同情况下重复计算得出相同的结果，以验证和判断结果的正常与否。
	可追溯性	算法可追溯性包括对输入数据、算法或模型编程、应用或测试场景、算法结果的追溯。
	问责制	算法问责制是指运营者有能力根据其意图验证行为、并识别和纠正有害结果，同时该能力将作为运营者对算法结果负责的正当性基础。
数据相关	隐私保护	隐私保护关注AI开发者、运营者是否在数据收集和应用于AI技术的各环节实现对个人主体隐私权益的充分保障。
	数据质量	数据质量是指保证数据的可靠性、准确性、关联性和完整性，避免数据的错误、偏差传导至AI系统。
	人员管控	人员管控是指避免因企业内部数据治理人员的访问行为引发伦理风险。
社会治理	向善性	向善性要求AI发展应当以人类福祉为最终目的、服务人类整体的价值目标与伦理准则。
	公正性	公正性要求AI发展应当以利于社会公平公正为目标，避免AI歧视。
	人类主体性	人类主体性强调人类不应过分依赖和信任AI，应当保障自主学习能力和对决策权的控制能力。

[10] EC High-Level Expert Group AI, Ethics Guidelines for Trustworthy AI, 2019.

[11] European Parliament Research Service, A Governance Framework for Algorithmic Accountability and Transparency, April 2019.

[12] 腾讯研究院：《欧盟人工智能伦理与治理的路径及启示》，载https://www.chainnews.com/zh-hant/articles/831032315738.htm，2019年9月25日。

[13] Dawson D and Schleiger E, Horton J, McLaughlin J, Robinson C, Quezada G, Scowcroft J, and Hajkowicz S Data 61 CSIRO Artificial Intelligence: Australia's Ethics Framework, 2019.

[14] National Security Commission on Artificial Intelligence, Interim Report, November 2019.

以下将从算法、数据以及社会治理三方面以相关的AI伦理风险评估要素为例，探讨如何将评估要素细化，以期认知、控制和降低人工智能伦理风险，并为企业AI实践提供参考建议。

（一）与算法相关的AI伦理风险

作为人工智能的核心，“算法伦理”在“人工智能所涉及的伦理问题中……居于基础地位”。[15]与算法相关的AI伦理风险可能包括透明度、准确性、可解释性等多项内容。

以算法透明度为例，黑箱问题无疑是人类对AI技术的关注重点之一，如果无法了解或解释AI决策的过程，人类是否或能在多大程度上接收AI的决策结果？答案并不乐观。MIT科技评论曾警示“没有人真正知道现今的机器学习算法是如何决策的，而这恐将成为一大隐忧”。[16]同样是由于透明度问题，AI Now Institute[17]曾呼吁应停止在刑事司法、医疗健康、社会福利和教育等核心公共领域（“高风险领域”）使用“黑箱”AI和算法。[18]因此，保障透明度对控制和降低AI伦理风险至关重要。

尽管如此，透明度的概念和含义仍然需要进一步澄清。EPRS在《算法责任与透明度治理框架》[19]中指出，算法的透明度并非是“一刀切”的概念，相反，根据算法决策系统的类型和用途，算法透明度可能包含以下一项或多项内容：代码、逻辑、模型、目标（如优化目标）、决策变量或其他与算法执行有关的要素；同时，算法透明度既可能是整体透明度[20]也可能是局部透明度[21]。而就AI透明度而言，欧盟在《可信赖人工智能伦理准则》中，还进一步强调了AI实践时不应使用户将AI系统混淆为人类；且用户应当有权利拒绝与AI系统交互；同时AI系统的终端用户应当能够通过适当方式了解该系统的能力及其局限性……[22]

总体而言，我们建议，至少可以考虑根据以下内容来评估AI的透明度风险。

---

[15] 参见孙保学：《人工智能算法伦理及其风险》，载https://mp.weixin.qq.com/s/_NxdAwvPg7clWviLh5pMjg，2019年12月20日。

[16] "No one really knows how the most advanced algorithms do what they do. That could be a problem." Knight, W. (2017, April 11). The Dark Secret at the Heart of AI, MIT Technology Review. Retrieved December 12, 2019, from https://wenku.baidu.com/view/a2fc8229cfc789eb172dc8fa.html.

[17] 纽约大学AI研究中心。

[18] "Core public agencies, such as those responsible for criminal justice, healthcare, welfare, and education (e.g "high stakes" domains) should no longer use 'black box' AI and algorithmic systems." Quoted from Ten Recommendations to Make AI Safe for Humanity, (2017, Nov.1). Retrieved on December 12, 2019, from https://boingboing.net/2017/11/01/no-black-boxes.html.

[19] "Transparency - Depending on the type and use of an algorithmic decision system, the desire for algorithmic transparency may refer to one, or more of the following aspects: code, logic, model, goals (e.g. optimisation targets), decision variables, or some other aspect that is considered to provide insight into the way the algorithm performs. Algorithmic system transparency can be global, seeking insight into the system behaviour for any kind of input, or local, seeking to explain a specific input - output relationship." European Parliament Research Service, A Governance Framework for Algorithmic Accountability and Transparency, April 2019.

[20] 即试图解释任何输入下的系统行为。

[21] 即解释某一特定的输入-输出之间的对应关系。

[22] "AI systems should not represent themselves as humans to users; ... In addition, the option to decide against this interaction in favour of human interaction should be provided where needed to ensure compliance with fundamental rights. Beyond this, the AI system's capabilities and limitation should be communicated to AI practitioners or end-users in a manner appropriate to the use case at hand."

透明度

（1）是否与用户进行沟通，告知其是在与AI系统交互，而不是与人交互？是否有给AI系统贴上这样的标签？
- ☐ 是否向用户披露产品中存在AI的应用？
- ☐ 是否向用户披露产品中AI的应用涉及自动化决策？
- ☐ 是否向用户披露AI在针对用户自动化决策过程的具体作用？

（2）是否设置机制向用户解释AI系统产生的结果，包括原因及标准？
- ☐ 是否已经考虑用户反馈意见并利用反馈意见来调试系统？
- ☐ 是否就潜在或已感知的风险与用户进行沟通？
- ☐ 根据具体用例，是否考虑过与其他受众、第三方或一般公众的沟通和透明性？

（3）是否向用户阐明AI系统的目的及受益主体？
- ☐ 是否已指定产品使用场景并向用户告知？
- ☐ 是否考虑过不同用例下人类心理学和潜在限制的风险，例如：混淆、确认偏差或认知疲劳等？
- ☐ 是否有向用户进一步说明AI系统对用户的影响，以及这些影响是否可逆？

（4）是否向用户告知AI系统的特点、局限性和潜在缺陷？

（5）是否周期性地对AI系统输出结果进行外部审核？

（二）与数据相关的AI伦理风险

考虑到数据对于机器学习的重要性，与数据相关的AI伦理风险同样不容忽视。数据伦理风险的评估应参考数据质量、隐私保护、人员管控等多个方面进行综合评价。

以数据质量为例，数据作为AI学习的基本要素，其质量优劣将直接决定AI学习后的成果。数据质量优劣的评判可基于两种维度，数据样本的数量与数据自身质量。[23]具体言之，当数据数量不足，用于训练系统的数据不能准确地表现系统将运行的环境时，就会产生数据样本偏差，最终的结果往往导致AI系统的执行或者结论以偏概全。比如将AI引入股票投资领域时，若所学数据只包括每天公司变动的情况以及公司股价变化情况，而没有考虑到国家政策时事的变化等全方位因素，则会导致AI的预测结果产生偏差。当数据本身质量不佳，如包含了虚假数据、失效数据或由于刻板印象产生的偏见数据时，会导致系统在学习的过程中不断吸收错误或偏见的知识与观念，也会导致最后的错误与偏见，如亚马逊的人工智能招聘系统曾被爆出涉嫌性别歧视，[24]报道中认为因为人工智能招聘系统学习的数据是过去十年应聘者的简历与最后的录取结果等信息，而过去十年的招聘中男性录取概率更高，系统便记住了这一特征，形成性别偏见，降低了对女性应聘者的录取率。

基于通常对于数据质量的理解，结合AI系统中机器学习对于数据的依赖程度，就数据质量的具体评估，可能需要回答以下问题：

[23]《推荐：一文了解AI时代的数据风险（后真相时代、算法囚徒和权利让渡）》，载https://blog.csdn.net/Tw6cy6uKyDea86Z/article/details/84001518，2018年11月12日。

[24]《亚马逊AI招聘工具被爆性别歧视，不喜欢女的？》，载http://www.sohu.com/a/259640276_100183993，2018年10月15日。

数据质量

（1）数据的可靠性

☐ 是否清楚了解数据的谱系（来源）？

☐ 是否对数据自产生至最终应用的各个流转环节进行记录？

☐ 是否设置了数据来源的可靠性评估机制？

（2）数据关联性

☐ 在选取用于AI系统训练的数据前，是否预先将所选取数据的属性与AI训练的目的进行对应和匹配

（3）数据准确性验证

☐ 是否在数据流转中设置了专门环节，确保数据在流转过程中持续的准确性和不被篡改，例如对数据流转谱系进行记录，在终端数据存在误差时可以及时查询各流转环节，找出出现错误的环节并予以纠正

☐ 在以人工对数据进行标签标记的设置时，是否采取验证措施，以确保标签属性的准确性

☐ 当数据具有较强的时效性时，是否定期对数据池进行审查与更新

（4）数据的完整性验证：需考虑数据提取和数据变换的情况

☐ 在提取用于AI系统训练的相关数据时，是否对数据的取舍进行合理性和必要性评估？

☐ 在删除相关数据时，是否充分考察其对数据完整属性的影响？

☐ 是否采取措施确保数据池不被破坏或侵入？

（三）与社会治理相关的AI伦理风险

人工智能高速发展的同时，也会破坏人类旧有的生活秩序，对社会治理带来更大的挑战。霍金曾表示过对人工智能的担忧：“人工智能的成功有可能是人类文明史上最大的事件。但是人工智能也有可能是人类文明史的终结，除非我们学会如何避免危险。”因此与社会治理相关的AI伦理风险应受到格外关注，在AI开发的过程中应当重点关注其向善性、公正性与人类主体性。

以人类主体性为例，随着AI技术日趋发达，它将在社会的多个领域占据一席之地，在给人们生活带来便利的同时，也可能会在一定程度上弱化人类主体的能力，包括但不限于创造力、记忆力、判断力。此时如何处理好人与人工智能间的关系变得格外关键。数十年前，阿西莫夫就曾提出著名的“机器人三定律+零定律”[25]警示人类，在如今这个技术更为纯熟的年代，为避免科幻作品中人类沦为机器附庸情景的发生，人类更应保持警惕并明确人类作为AI生产者的主体地位。无论技术多么高效准确，仍不能放弃自主学习和对决策权的控制能力，避免过于依赖与信任人工智能。

对于人类主体性的保障，可能需要考虑以下问题：

[25] 阿西莫夫的机器人定律即：第零定律：机器人必须保护人类的整体利益不受伤害。第一定律：机器人不得伤害人类个体，或者目睹人类个体将遭受危险而袖手不管，除非这违反了机器人学第零定律。第二定律：机器人必须服从人给予它的命令，当该命令与第零定律或者第一定律冲突时例外。第三定律：机器人在不违反第零、第一、第二定律的情况下要尽可能保护自己的生存。

人类主体性

（1）是否进行AI损害及人类参与度评估，考虑决策造成的损害严重程度、产生损害的可能性？
□ 是否以非有意的方式影响（终端）用户的决策过程？

（2）能否确保不过分依赖AI决策，保证公民自主学习的权利？

（3）是否采取了防范措施以避免对AI系统的过分自信或对AI系统的过分依赖？

（4）是否考虑人类对特定AI系统的利用和控制？
□ 是否考虑人类对于具有情感依赖AI系统的利用进行限制
□ 是否考虑对于情感依赖AI系统的学习能力进行限制
□ 是否考虑对于情感依赖AI系统情绪性表达进行非人类化

（5）AI系统是否接受外部审核？是否有与管理AI自治相关事件的补救措施？

（6）是否建立了检测和响应机制，以评估可能出现的问题？

（7）在需要的情况下，是否可能会出现停止按钮或其他停止运行的程序？相关程序是完全或部分停止AI服务还是将控制权转交给人类？

二、企业AI实践建议

AI技术的飞速发展在为生活带来便捷的同时，也对伦理道德以及传统的社会治理体系造成了挑战，对于从事研发、应用AI的企业而言，负责任的AI实践既是规避技术和法律风险的必然要求，也是企业社会责任感的重要体现。面对AI实践，我们建议企业考虑：

（一）建立AI伦理道德委员会

2019年7月24日，中央全面深化改革委员会（**“中央深改委”**）审议通过了《国家科技伦理委员会组建方案》。与国家科技伦理委员会的组建相呼应，基于AI伦理风险的专业性与复杂性，我们建议从事人工智能的相关企业可以结合业务实际情况，考虑建立内部AI伦理道德委员会，以强调AI伦理风险的重要性，强化企业开发人员的风险意识与社会责任，为企业AI伦理风险合规提供保障，应对人工智能高速发展带来的挑战。具体而言，伦理道德委员会由具有不同专业背景的开发人员、法务人员、合规人员以及其他行政人员组成。委员会主要职能包括但不限于：建立企业人工智能伦理道德准则及指引、对企业开发过程中面对的伦理道德风险问题做出决策、开展算法审计及质量审查、组织协调企业内部各部门的伦理风险应对工作。[26]

[26] 郭锐、李依、刘雅洁：《人工智能企业要组建道德委员会，该怎么做》，载http://www.bjnews.com.cn/feature/2019/07/26/608130.html，2019年7月26日。

（二）增强算法透明性

为保障用户对算法的知情权，同时也考虑到未来可能建立的人工智能相关法规，我们建议企业在不侵害公司商业秘密的前提下，向用户适度公开AI系统及算法的细节。具体而言，透明度要求向用户披露AI的使用情况、AI系统的目的、特点、缺陷、服务对象及可能对用户的影响，同时，也要求向用户解释AI系统产生的结果并对AI系统进行周期性地外部审核。[27]

（三）建立数据溯源机制

为符合《网络安全法》、《个人信息安全规范》等相关法律法规对于个人信息保护以及个人信息主体权利的要求，我们建议企业建立数据溯源机制。具体而言，溯源机制要求算法能够捕获所有输入数据，适当存储与监督、维护目的有关的数据，并建立机制记录算法或模型编程、应用或测试场景以及算法结果。[28]

（四）合规与技术结合的数据融合和数据共享

数据，是人工智能技术开发和应用的重要基础。挖掘数据的价值需要促进数据在企业内部的融合以及外部的共享。 但数据的融合与共享应当在合规的前提下进行，搭建数据融合和共享的合规框架是发展AI技术的前提。同时目前也有一些新型的技术比如联邦学习法等旨在协助参与企业在保持数据独立性的情况下，完成信息数据的加密交换。通过合规框架与新技术的利用，充分确保数据的合规融合和流动是AI进一步发展，摆脱数据“原罪”的重要共识。

（五）建立内部AI监督问责机制

为尽可能消除人工智能偏见与歧视的问题，同时满足对AI算法的预防性监管的要求，我们建议企业建立内部AI监督问责机制。具体而言，企业在开发算法时应采用各种控制措施以确保AI算法能够根据其意图运行，并建立定期的运行评估机制，对行为进行验证，包括但不限于内部审核机制，进行风险影响评估并形成报告，定期开展内部教育培训，开通用户投诉监督通道等。

三、结语及后记——应有大爱

AI技术的发展预示着又一场人类的超级革命，在ANI已然渗透进社会生活方方面面的同时，对AGI和ASI的不懈追求仍在继续。但或许必须承认的是，如果无法正确认识并控制ANI所带来的伦理风险，对AGI和ASI的探索将面临重重阻碍，人类对于AI未知的恐惧将长久的影响社会的进步和发展。但如同人类经历的种种重大变革一般，历史的车轮终将飞速向前奔驰。对于AI的新革命，我们希望大家尽可能摆脱个体认知和价值取向的局限，以人类整个群体的福祉为出发点，以“大爱”来看待AI道德伦理的风险，把缰绳攥在自己手中，有控制的迎接未知的未来。

这篇文章成稿于2020年1月23日，正值新型冠状病毒肆虐的非常时期。作为疫情重灾区的武汉在今天宣布“封城”，以近乎壮士断腕的决绝姿态来应对一场未知的疫情风险。不得不说，我们对于未知难免恐惧，但人性的光辉在关键时刻总是格外的闪耀。我们对在武汉和各地坚守的你们致敬，也对人类的“大爱”充满信心。让我们心存敬畏，用“大爱”来冲淡未知的恐惧，一起度过每一个难关。

（本文发布于2020年1月23日。）

[27] EC High-Level Expert Group AI, Ethics Guidelines for Trustworthy AI, 2019.

[28] Personal Data Protection Commission, A proposed Model Artificial Intelligence Governance, 2019.

人工智能系列之
人脸识别信息的内涵与合规难题

一、背景

计算机视觉技术作为人工智能（AI）技术发展的重要应用之一已经在我们的日常生活中屡见不鲜。在金融、移动、安防等产业，作为主流技术之一的人脸识别被广泛应用于账号身份认证、手机刷脸解锁、人流自动统计和特定人物甄别等诸多场景[1]。在人脸识别技术为生活创造更加便捷和安全环境的同时，考虑到人脸的特殊敏感性，社会各界也愈发关注人脸识别技术潜在的技术缺陷、歧视性及不可预见性对自然人隐私和平等保护带来的威胁和挑战。

仅就2019年而言，全球范围内人脸识别技术使用相关的案件便层出不穷：瑞典数据保护机构（DPA）因当地一所高中使用人脸识别技术来记录学生出席情况开出金额20万瑞典克朗（约人民币14.6万元）的罚单[2]；美国四个城市相继禁止政府部门使用人脸识别技术[3]；微软公司疑似因隐私保护和授权瑕疵方面的原因删除了曾为全球最大的人脸识别数据库MS Celeb[4]；Facebook因人脸识别功能或面临着可高达350亿美元的集体索赔[5]；我国AI换脸软件ZAO因涉嫌侵犯隐私被工信部约谈整改[6]等等。

本文将从人脸的特殊属性出发，旨在探讨人脸信息的多层次内涵，分析人脸识别技术可能引发的隐私相关问题，同时比较研究不同司法辖区对于人脸识别信息被利用前的知情权、信息采集范围和使用边界等问题的规制思路，以期为企业合规应用人脸识别技术提供参考。

二、人脸的多重属性

在全球范围内，当技术不断将人脸识别先进性推向新的高度时，对其秉持保留或反对意见的声音却愈演愈烈。而这与“人脸”所具有的多重特殊属性紧密关联，具体而言：

- **人脸具有更强的人格属性**。相比于其他个人信息，人脸图像与自然人就其人格所享有的精神性权利密切相关。肖像权作为一项重要的人格权，是指自然人对其肖像拥有的包括允许他人使用在内的绝对支配权并有权禁止他人非法使用。[7]而以侮辱或恶意筹划的形式使用他人肖像，将进一步构成侵犯名誉权的行为。因此，相比于其他个人信息，面部图像带有的更强的人格属性，体现着人格利益与精神价

[1] 参见信通院《人工智能发展白皮书产业 应用篇》。

[2] 简要新闻公告（英文）参见欧盟数据保护委员会官网：https://edpb.europa.eu/news/national-news/2019/facial-recognition-school-renders-swedens-first-gdpr-fine_en。完整版新闻公告（瑞典语）参见瑞典数据保护机构官网：https://www.datainspektionen.se/nyheter/sanktionsavgift-for-ansiktsigenkanning-i-skola/?utm_source=POLITICO.EU&utm_campaign=360ade166e-EMAIL_CAMPAIGN_2019_08_22_04_59&utm_medium=email&utm_term=0_10959edeb5-360ade166e-190359285

[3] 参见“Berkeley Bans Government Face Recognition Use, Joining Other Cities”, https://news.bloomberglaw.com/privacy-and-data-security/hold-berkeley-bans-government-face-recognition-use-joining-other-cities

[4] 参见“Microsoft quietly deletes largest public face recognition data set”, https://www.ft.com/content/7d3e0d6a-87a0-11e9-a028-86cea8523dc2

[5] 参见Patel v. Facebook一案有关裁决。

[6] 参见http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057724/n3057728/c7392754/content.html

[7] 参见秦某某诉视觉（中国）文化发展股份有限公司、汉华易美（天津）图像技术有限公司侵害肖像权纠纷案，（2019）京0491民初12225号。

值，从而相关使用行为更易引发侵犯自然人人格权益的顾虑。然而，对于那些不会牵涉任何自然人人格属性的使用行为而言，如仅将人脸信息用于机器算法演练的行为，从人格权所衍生出的法益保护主张可能难以适用。

- **人脸信息在当前经济下不同的财产价值**。在人格层面上的精神性权利之外，人脸中体现出的财产利益最早起源于名人肖像的商业化利用活动，随着人脸所蕴含的财产价值渐渐被认可，在不同司法辖区就是否承认独立的肖像财产权形成一元保护和二元保护的不同模式。然而，在传统法学研究中，能够就人脸主张包含财产利益的权利主体一般只限于名人，而普通人的肖像仅具有潜在的财产价值。进而当肖像被非法商业化利用时，名人能够主张财产损害赔偿，而普通人原则上仅限于精神损害赔偿。[8]然而，在人脸识别技术得以普及的当下，人脸信息不仅仅是自然人的肖像、名誉等人格利益的体现，更是代表着门禁的钥匙、银行卡支付的密码，当人脸信息所蕴含的财产价值得以极大地挖掘时，传统肖像权保护领域中针对财产价值名人/普通人的划分边界也被突破。
- **人脸背后具有更广泛的信息内涵**。技术的发展不单单将人脸的可识别性进行最大化发挥，更是不断深入地挖掘人脸背后的价值。通过人脸识别技术，人脸信息不仅可以用来准确地识别“我是谁”（**身份识别场景**），同时可以用来比对“我是否是我”（**身份验证场景**）；甚至，通过结合大数据技术能够获知、预测“我是一个什么样的人”，而根本无需知道“我是谁”（**标签画像场景**）。相比于其拟用于的处理目的及所携带的更高的安全风险而言，处理人脸数据更可能构成对数据隐私保护制度中收集个人信息“必要性”原则的违反。

除上述人脸信息的特殊属性外，从技术层面而言，人脸识别信息的使用可能带来更高的安全风险。相较于其他个人信息类型，人脸识别可以通过远距离与较为隐蔽的操作实现，人脸图像的收集更可能以被收集人无感知的方式进行，存在更大的技术滥用的潜在隐患。

在尚缺乏具体法律规则加以规范的情形下，如何更好地平衡利益冲突从而识别出更为优先保护的法益，我们理解就场景不同可能遵循着以下基本原则：

- **商业化场景**：在满足个人信息主体“知情同意”情形下，鉴于人脸信息蕴含着更高的信息安全风险以及潜在的更广泛的信息内涵，企业应当谨慎评估使用行为是否遵循“合法、正当、必要”原则，避免被质疑“杀鸡焉用宰牛刀”。
- **基于公共利益的应用场景**：与传统法学上对于肖像权的限制观点相类似，基于社会公共利益所需的情形下，自然人就其人脸信息所享有的权利也得以在一定程度内被限制。然而考虑到过度使用人脸识别技术可能对种族平等、言论自由可能带来的威胁，一般认为在公共场所使用这一技术时，建议注意遵守授权原则、法律保留原则、比例原则等。

三、人脸识别技术应用的合规问题

下文中，我们将围绕几个典型的人脸识别应用场景中涉及的问题展开讨论，以期一同探索可能的合规路径。

（一）含人脸图像的照片的性质认定

场景1

为了统计火车站检票口在特定时间点的客运流量情况，某国当地工作人员从监控录像中捕捉到一些清晰度有限的监控图像。虽然这些截图中可能包含有人脸图像，但由于拍摄距离较远且像素较低，在缺乏进一步技术处理的情形下，并不具有能够识别或确认特定自然人的属性。

讨论

对于包含人脸图像的截图能否被认定是人脸识别信息，进而构成个人敏感信息？

分析

《信息安全技术 个人信息安全规范》（“《个人信息安全规范》”）中，面部识别特征与个人基因、指纹、声纹、掌纹、耳廓、虹膜等一并构成个人敏感信息下的“个人生物识别信息”，保护程度和相关的合规要求均较一般个人信息更高。今年6月，全国信息安全标准化技术委员会发布了《信息技术 安全技术 生物特征识别信息的保护要求（征求意见稿）》，其中对于生物特征识别数据（biometric data）的定义为“生物特征样本、生物特征、生物特征模型、生物性质、原始描述数据的生物识别特征，或上述数据的聚合”，而“人脸”被列为可据以对个体进行识别的生理特征之一。然而，对于承载人脸图像的照片是否会被认定为个人敏感信息，我国目前尚未予以明确。

根据欧盟地区的数据保护法《通用数据保护条例》（“GDPR”）的规定，面部图像（facial image）构成特殊类型个人数据下的“生物识别数据”，进而相较于一般个人数据受制于更高的保护要求。根据其定义，“生物识别数据”是指经由特定技术处理，获取的有关自然人身体、生理或行为特征的个人数据，并且该个人数据能够识别或确认特定自然人。[9]GDPR进一步指出，处理照片并不当然地被认为是处理生物识别数据，而仅在当通过特定技术方法对照片进行处理，使其能够识别或确认特定自然人时，才被视为构成生物识别数据。[10]

[8] 冉克平，《肖像权的财产利益及其救济》，载于《清华法学》2015年第4期。

[9] 参见GDPR第4（14）条。

因而一般而言，包含人脸图像的照片在性质上并非当然构成受到更高保护程度的生物识别信息/个人敏感信息，而是当经由特定技术处理后能够使其具有可识别个人身份的属性时，才会受制于更高的合规要求。

（二）人脸识别信息采集的必要性探讨

场景2

瑞典一间学校对其某班级试点使用人脸技术识别技术进行学生课堂考勤。该学校声称学生已同意参与该试点应用，但并未就采用人脸识别技术进行影响评估或向瑞典DPA进行事前咨询。2019年8月，瑞典DPA针对这一行为处以自GDPR实施以来的瑞典首例处罚。

讨论

在存在其他可行的且对个人信息主体影响较小的替代性方案情况下，人脸识别信息采集用于考勤、计数等用途是否具有必要性?

分析

《网络安全法》（“《网安法》”）规定了网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则。《个人信息安全规范》中对于个人信息收集进一步提出了最小化要求。

对于人脸识别信息的采集，由于其相比其他的个人信息具有更为特殊的性质，企业在采集之前需要谨慎考虑是否有其他可替代的方案，通过收集敏感度相对较低的信息，是否能够实现同样的目的。

在上述案件中，瑞典DPA即认为，因人脸识别技术可能构成对个人隐私的严重侵犯，且存在其他可行、高效的考勤记录方式，该学校对于这一技术的应用超出了实现目的之必要限度，违背了数据处理的最小化原则。然而，随着科技和企业商业模式的日新月异，对于不同企业实现某一功能产品或服务数据采集的必要性可能越来越难以用同一标准予以衡量而需要做个案的分析。

（三）人脸识别技术的商业化使用

场景3

在新零售场景中，超市运营商通过监控影像中的人脸信息识别出存量用户之后，将继续跟踪其在货架或区域的停留时间等，进一步分析其关注点和兴趣，并向销售人员推送此用户此前的喜好和购物习惯等，以对用户进行进一步的精准广告营销。

讨论

基于监控、安保目的安装的安监设备所收集的人脸图像、影像信息，能否进一步用于商业化精准广告营销?

分析

《网安法》要求网络运营者收集、使用个人信息，应明示收集、使用信息的目的、方式和范围，并经被收集者同意。将监控设备基于安监目的所收集的人脸图像、影像信息进一步应用于商业化的精准广告营销，超出了消费者对于其个人信息使用的正常预期。因而，超市运营者需要对于该述信息被用于精准广告营销的目的、方式和相关个人信息范围等予以全面的披露，并获得用户的授权同意。在消费者拒绝该精准广告营销的行为以后，超市运营商不得再向其进行定向推送。

类似地，以美国华盛顿州于2017年5月发布的众议院1493号法案（“H.B. 1493”）为例，其对于出于商业目的获取个人生物识别数据的行为确立了通知和同意规则[11]。原则上，法案要求收集生物识别数据并可将其与特定身份个人进行匹配的企业，应当披露其如何使用该生物识别数据，并在获取处理[12]或更改个人生物识别符之前向个人进行告知并征得其同意 。[13]

因此，企业因安全监控等目的所获知的人脸图像、影像，如后续被用于其他商业目的，则需保障个人信息主体的知情、同意要求。此外，企业还需采取合理措施防止对该述信息的未经授权访问或获取，并遵循保存时限合理必要的最小化要求。

（四）公共场所使用人脸识别技术的限制

场景4

某国在道路两侧安装了人脸识别系统，主要用于抓拍闯红灯的行人和非机动车驾驶者，在晚上也能清晰成像。行人被“抓了现行”，闯红灯的短视频和放大后的头像将直接曝光在路口的显示屏上，呈现在公众面前。此外，这套设备还与居民身份信息系统相连，通过人脸识别出的违法者姓名、身份证号码等个人信息，也将显示在电子屏上。

讨论

对于基于公共安全等目的在公共场所安装视频监控是否需要满足一定的限制要求，从而与个人隐私保护相平衡?

---

[10] GDPR引言第51条：“The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person.”

[11] “商业目的”是指在与个人进行的初始交易无关的情况下，基于向第三方出售或披露生物识别符以进行商品或服务推销之目的首次获得个人的生物识别符。“商业目的”不包括安全或执法目的。H.B. 1493，第3（4）条。

[12] “获取处理”是指获取个体的生物识别符，将其转换为无法逆向重建为原始图像的引用模板，并将其存储数据库中，该数据库可将生物识别符与特定个体进行匹配。H.B. 1493，第3（5）条。

[13] “生物识别符”是指通过自动测算个体的生物学特征（例如指纹，声纹，眼视网膜，虹膜或其他用于识别特定个体的独特生物学特征或特征）而生成的数据。“生物特征识别符”不包括根据1996年联邦健康保险可移植性和责任法案所拍摄的物理或数字照片，视频或音频记录或由此产生的数据，也不包括用于医疗保健、付款或操作目的收集，使用或存储的信息。

分析

一方面，政府基于建设智慧城市如在地铁等公共交通枢纽场地安装人脸识别装置或基于行政执法目的收集、使用人脸信息，是对公共安全的保障甚至能够推动公共出行的便捷。另一方面，在日益增多的公共场所监控场景中，个人无法拒绝对于人脸识别信息的获取，也同时增加了个人信息被滥用的风险。

2019年9月4日，作为首例肯定警方使用人脸识别技术合法性的法院判决，在Edward Bridges诉南威尔士警察局局长与英国内政大臣一案[14]中，英格兰和威尔士高等法院行政庭判决支持了被告南威尔士警方使用部署了人脸识别技术的街道闭路电视获取原告的实时位置信息并将其逮捕的行为。法院认为（1）该案中人脸识别技术的应用均符合英国《数据保护法》、各级相关法律法规与南威尔士警方完备的系列执法政策与敏感信息处理政策，（2）南威尔士警方将部署该技术的措施均告知公众，限定使用时间与范围，且没有对外披露原告个人信息，且（3）该技术的应用具有维护公共治安和保护重大公共利益的必要性。综上，该法院认为该人脸识别技术的应用实现了个人隐私权利与公共利益的平衡，没有违反《欧洲人权公约》第8条与英国《数据保护法》第35条对执法机关的限制。

虽然上述为公权力使用场景，但其中所体现出的利益权衡对于在公共场所部署监控设备的企业而言依然有一定的借鉴意义。企业在处理人脸识别信息时应当考虑行为的正当性和必要性，应积极制定并遵从敏感信息处理政策，以明示告知信息主体并取得信息主体的妥当授权，确保收集和处理该信息仅应以其业务目的之必要为限度，并在上线监控技术之前对其可能对个人隐私造成的影响予以评估。

（五）人脸识别技术下的歧视问题

场景5

人脸识别的迅速发展使其能够运用于求职、交友、教育等多个领域。在求职领域，通过对应聘者的人脸图像的实时分析，AI能够基于其强大丰富的数据分析处理能力，评价应聘者的性格、情绪、心理状态、能力，从而协助雇主决策他或她是否是最合适招聘岗位的人员。

讨论

在缺乏监管、有效保障措施、透明度和问责机制的情形下，如何避免人脸识别算法所导致的歧视现象？

分析

受限于技术发展现状、原始数据的偏差、算法设计者自身的偏见，使用人脸识别算法通过标签化的判断方式增加了作出歧视性决策的风险，而这些风险绝大程度上将由本身已处于相对劣势地位的人群承担。在缺乏监管、有效保障措施、透明度和问责机制的情形下，人脸识别算法的运用将加速现有的不平等现象。而令人担忧的是，通过借助复杂晦涩的算法，歧视往往以一种不易察觉的方式进行。

作为第一个规范在视频面试中对AI使用行为的州法，美国伊利诺伊州通过了人工智能视频面试法案（Artificial Intelligence Video Interview Act），其将于2020年1月1日生效。在法案下，雇主仅有当满足下列条件时才可对面试视频进行AI处理以决定其是否合适相关岗位：（1）已告知应聘者应聘视频会被AI处理以判断其是否适格；（2）向应聘者告知AI的工作原理以及AI将使用何种特征来评估应聘者；（3）就拍摄视频行为以及后续的AI处理行为获取应聘者的同意。同时，该法案还禁止雇主对应聘者视频的进一步分享行为，除非被分享方具有分析应聘者适格与否的必要专业知识或技能。尽管该法在算法使用透明度上具有很大的推动意义，但考虑到一般算法仅作为雇主决策的辅助性手段，法案本身并未明确提及应对算法歧视性潜在的救济渠道。

随着我国对于个人信息处理的合法性、透明性要求日渐增强，企业在完全依靠自动化算法处理人脸识别信息并作出显著影响个人信息主体权益的决定时（例如基于用户画像决定个人信用及贷款额度，或将用户画像用于面试筛选），为了避免可能的算法歧视对自然人造成的影响，建议应：（1）全面告知人脸识别信息的使用用途；（2）AI自动算法的工作原理以及AI将使用何种特征来评估数据主体；（3）就收集人脸识别信息以及后续的AI处理行为获取数据主体同意；以及（4）向个人信息主体提供申诉方法，以保障受影响的主体质疑自动化决策所做结论的权利。

四、建议和我们的思考

人脸识别技术已经在多个场景被广泛应用，尽管目前全球对于人脸识别中的法律规制边界和更深层次的道德伦理问题仍未达成明确的共识，但考虑到目前已经生效的法律要求，当前企业在部署或使用包括人脸在内的生物识别技术时应当关注以下问题：

（一）审慎考量，遵守合法、正当、必要原则

可以预见，随着车联网、物联网的建设，人脸识别等生物识别技术的应用广度和深度也将逐步拓展和加强。然而，瑞典GDPR处罚案件的核心问题围绕于该技术在特定应用场景中是否具备合法性基础且符合必要的限度。考虑到人脸识别信息的高度敏感性，监督态势将可能呈现趋严态势。因此，企业在对相关技术进行部署和应用时，应持续遵守合法、正当与必要的原则，在部署前开展必要的个人信息安全影响评估，以确保生物识别信息的处理严格遵从法律法规和监管要求。

（二）有渠道让被采集人知情并获得同意

在我国《网安法》第四十一条的要求下，对于人脸图像的获取和后续可能的

[14] 参见R (Bridges) v CCSWP and SSHD。

处理活动，建议企业应确保被采集人对拟开展的处理活动的充分知悉，并征得其同意。在运用人脸识别技术进行自动化决策时，应谨慎评估该决策对个人主体权益的影响，以及是否需要为相关个人提供通畅的申诉渠道。

（三）承担更高的数据安全保护义务，确保数据安全

人脸识别系统捕获的面部特征信息可能属于个人敏感信息。根据我国的个人信息保护制度，企业对此类信息需要承担较为严格的安全保护义务。因此，企业应注意持续提升对人脸识别信息等生物识别信息的安全防护，按实际情况的需要采取加密保护、隔离存储、脱敏使用等技术措施，并在确认不具备处理的必要性后进行及时、彻底的销毁。

（四）密切关注行业立法与监管态势，积极应对相关主管部门对人脸识别技术应用有关的规范出台情况

除2019年6月发布的《信息技术 安全技术 生物特征识别信息的保护要求（征求意见稿）》外，我们了解到多达二十余个与生物特征识别技术相关的标准规范也正在制定过程中。

众多的技术应用规范，既能为处于不同行业的企业在业务经营与企业管理过程中应用人脸识别等生物识别技术提供明确指导，同时也或将带来更高的合规要求。相应地，企业应当继续保持高度的合规意识，确保在规章制度与技术规范上能够及时、积极地响应生物识别技术的应用规范。

除要求企业遵守现行的法律法规要求，合规使用包括人脸识别在内的生物识别技术以外，从行业发展和法律规制两个不同的角度，**社会各界可能都需要进一步讨论生物识别技术所触及到的技术、法律及道德难题：**

（1）通常大家理解的生物识别技术以“识别”特定个人为主要目的，但实际运用中仍存在其他多样化场景，例如有些未来自动驾驶技术中采取的生物识别技术是以识别“人类”与“其他物体”为诉求（比如路测阶段），并不一定会涉及特定个人的人格或财产权益。对此类不以“识别”特定个人为目的的生物识别技术是否有必要严格的受制于个人信息保护的规制？或者生物识别设备的本地匿名化处理能否降低告知同意的标准？

（2）随着技术的发展，生物识别的物理或环境要求可能会大幅度降低。除支付、身份验证等私密场景以外，生物识别技术会更为广泛的应用在公共场合，比如小区安防 、“智慧城市”等。未来个人信息主体可能会更为隐蔽地被“识别”，而企业在应用生物识别技术时也愈发缺乏与个人信息主体的交互界面来主动告知个人信息主体，并获得其同意。如何解决技术进步与个人信息保护的平衡会是将来长时间困扰社会公众和企业的难题，是通过加强公共场合的告知或者对于新型技术应用的社会媒体宣传，还是建立沟通渠道加强事后的救济来维系这种平衡？

（3）基于公共场所安全监管要求被收集的生物识别信息（比如机场安检等），其收集的合法性可能基于特定的交互场景（比如飞机上视频和音频采集的告知），也基于公众对于法律法规的合理预期（法律法规的公示效果）。然而，对于新商业场景下收集的生物识别信息是否可以通过合理预期来降低告知同意的标准？比如无人超市等新零售场景，在媒体宣传以及公众告知的前提下，在满足提醒义务后，是否可以认为主动步入无人超市的个人已经被对生物识别信息收集有了合理预期？对于类似的新型业务生态，是否有必要通过立法立规的方式来加强公示作用？

（4）生物识别信息（比如人脸识别信息）已在一定程度上突破了肖像权等法律权利保护和适用的范围。这类信息在大数据经济背景下的法益可能已经超出了现有法律制定时的社会及经济基础。我们理解这类生物识别信息具有多层次的内涵：

- **识别内涵**：这类信息的最大商业价值是作为唯一并相对方便和准确的身份标识符（不同于DNA或者设备识别码等），基于唯一性的人格属性而衍生出商业价值，比如生物识别信息与应用场景之间的强关联关系（比如刷脸支付、门禁）。
- **关联内涵**：人脸等生物识别信息除了识别以外，还能根据识别特征来通过大数据分析等技术以关联特定主体的其他信息，比如性别、年龄、皮肤状况、种族、性取向、婚姻状况、儿女长相、甚至五十年后长相预测等。
- **验证内涵**：生物识别信息除识别或关联特定主体，在很大程度上能验证统计场景下的结果。比如智慧城市的应用中，通过验证真实的个体流动，来测试交通热力图的真实性和有效性。

在上述不同内涵中，无论是信息可能存在的人格属性还是附属的财产价值程度可能不尽相同，涉及的主体多样，因而以个人信息附属的“权益”而不是绝对的“权属”来区分保护的对象和边界可能更具可行性。

（5）对于生物识别信息的关联内涵而言，尽管其用途广泛，但容易引发比如判断错误、歧视等道德伦理问题，比如通过人脸识别信息来实现判断个人的性取向、种族、宗教信仰等非识别性目的。由于生物识别技术的自动化特征，类似的关联信息可能通过自动化处理或决策，缺乏透明性也不易于监管，即使实际上发生了失误或歧视等问题也很难追溯。如何加强算法可解释性，避免算法歧视或者信息不完整而导致决策误差？

随着科技的日新月异，人脸的价值将得到更多的开发、应用场景也会更加丰富多样，现有法律法规对于肖像权或者个人信息主体权益的保护形式和边界可能都将受到挑战。如何在确保公共安全、个人权益的同时，促进人脸应用相关新科技的发展仍然有待各界的深入讨论。

（本文发布于2019年11月12日。）

第二部分：数据合规

“明者因时而变，知者随事而制”
——《个人信息安全规范》实务探讨

回首2017年，全球个人信息保护立法快速发展。比如在亚太地区，《中华人民共和国网络安全法》（以下简称“**《网安法》**”）于2017年6月1日实施，2017年2月澳大利亚通过强制性数据泄露通知法案。此外日本的《个人信息保护法》（Personal Information Protection Act）修订版也于2017年5月30日起全面生效。

展望2018年，个人信息保护的发展更值得大家期待。欧盟委员会颁布的《一般数据保护条例》（General Data Protection Rules，下称“**GDPR**”）将在2018年5月25日正式生效实施，其管辖范围的规定不论是否在欧盟成员国有无实体，有无在成员国内处理个人信息，使得任何向欧盟境内提供商品或者服务，或者监控在欧盟内欧盟居民的行为的组织，都受GDPR的管辖。考虑到全球经济一体化趋势，GDPR管辖范围的扩大很大程度上将影响全球个人信息保护的实践。随着该立法趋势，各国个人信息保护立法将不可避免的冲击本土及跨国企业的实践，各企业需要在各国个人信息保护规则中寻求共性、建立普遍适用的合规体系。

在这个大背景下，国家标准化委员会参考国内法律法规、国际规则和实践制定的《信息安全技术 个人信息安全规范》（GB/T 35273-2017）（以下简称“**《个人信息安全规范》**”）在2018年1月24日正式公布，并将于2018年5月1日正式实施。

本文将结合其他国家的立法实践，讨论《个人信息安全规范》适用中的实务问题。

一、《个人信息安全规范》的基本框架

全国人大常委会2012年12月审议通过《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》，2016年11月审议通过《网安法》（以下简称“**一法一决定**”）。“一法一决定”的颁布和实施，对企业处理个人信息提出了基本法律要求，比如、《网安法》就在第四章“网络信息安全”中对个人信息保护的基本原则、网络运营者的行为义务等进行了总括性规定。在现有原则性、概括性的法律条文下，企业有关个人信息保护的具体合规工作仍旧缺乏具体指引。《个人信息安全规范》的颁布，从国家标准层面对企业收集、保存、使用、共享、转让、公开披露信息等信息处理环节的各项行为提供了具体的合规指引。

<table>
<tr><td>术语和定义</td><td colspan="2">在《网安法》的基础之上，新增界定了若干核心的标准术语和定义，如个人信息、个人敏感信息、个人信息控制者、明示同意、用户画像、个人信息安全影响评估、匿名化与去标识化</td></tr>
<tr><td>个人信息安全基本原则</td><td colspan="2">权责一致、目的明确、选择同意、最少够用、公开透明、确保安全、主体参与</td></tr>
<tr><td rowspan="6">个人信息处理流程</td><td>个人信息的收集</td><td rowspan="6">按照个人信息的处理流程，针对各个环节中对个人信息控制者的要求、个人信息主体所享有的权利进行具体、详尽的阐述</td></tr>
<tr><td>个人信息的保存</td></tr>
<tr><td>个人信息的使用</td></tr>
<tr><td>个人信息的委托处理、共享、转让、公开披露</td></tr>
<tr><td>个人信息安全事件处置</td></tr>
<tr><td>组织的管理要求</td></tr>
</table>

附件	个人信息示例	以定性描述+非穷尽列举的方式，介绍个人信息与个人敏感信息的判定标准与示例
	个人敏感信息判定	
	保障个人信息主体选择同意权的方法	结合《个人信息安全规范》的要求，以提供实践模板的方式，阐释企业的产品与服务在需要收集个人敏感信息与拟定隐私政策时需要关注的内容与要求
	隐私政策模板	
参考文献	从参考文献目录可见，在《个人信息安全规范》指定的过程中，起草者不仅仅参考了我国个人信息保护领域方面的主要法律法规和既存的国家标准，更进一步地参考了多部与个人信息保护相关的外国法律法规与标准等，如欧盟的《一般数据保护条例》、欧美隐私盾、欧洲标准委员会的《个人数据保护实践（good practices）》OECD隐私框架、APEC隐私框架，以及美国国家标准与技术研究院（NIST）的相关文献。	

二、《个人信息安全规范》的效力

根据2017年11月4日修订通过，2018年1月1日施行的《中华人民共和国标准化法》，“标准包括国家标准、行业标准、地方标准和团体标准、企业标准。国家标准分为强制性标准、推荐性标准，行业标准、地方标准是推荐性标准”[1]。《个人信息安全规范》是一项推荐性国家标准，并不要求企业强制执行。 换句话说，企业个人信息安全保护工作一旦与《个人信息安全规范》中的要求不一致，并不一定意味着企业必然违反相关的法律法规。

但根据《国务院办公厅关于印发国家标准化体系建设发展规划（2016-2020年）的通知》，国家标准体系建设一贯遵循“强制性标准守底线、推荐性标准保基本、企业标准强质量”的原则。作为推荐性标准，一般需满足“基本通用”的要求，《个人信息安全规范》应该被视为企业“基本通用”的实践指南，具有普遍适用性。

此外，值得企业注意的是，推荐性国家标准尽管没有强制力，但除了为各类组织提供实践指引以外，其作用还包括为监管机构执法提供参考。《个人信息安全规范》中就明确指出，其“适用于规范各类组织个人信息处理活动”，也适用于“主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估”。

考虑到“一法一决定”的配套措施体系仍处于基础建设阶段，尽管我们理解《个人信息安全规范》是一项不具有强制力的国家标准，但由于其普遍适用性，以及可能作为监管部门执法的参考材料，一旦企业的实践背离《个人信息安全规范》中的要求，实践中企业可能需要承担更大的证明成本以说明企业行为的合规性，因此我们仍然建议在实践中，企业应把《个人信息安全规范》的要求落实到位，以求在个人信息安全保护体系建设中，做到合规、安全和高效。

三、国内企业适用《个人信息安全规范》的注意要点

随着《网安法》的颁布和实施，大多数国内企业都根据《网安法》的基本原则以及行业惯例形成了基本的个人信息安全保护制度。但《个人信息安全规范》以《网安法》为基础，结合其他司法辖区的立法和实践，为企业提出了更为具体，更为细致的要求。企业需要根据《个人信息安全规范》的要求，打破与之冲突的行业惯例，重新审视内部个人信息安全保护制度。

（一）怎么同意才作数?

实践中，企业收集信息征得个人信息主体同意的方式往往比较简单，通常采用的是不拒绝视为同意的原则，个人信息主体的知情同意往往流于形式。《个人信息安全规范》中不仅明确定义了 “明示同意”的概念，直接提出了“个人敏感信息的收集和使用需获得用户明示同意”的新要求，还以实践模板的方式演示了“明示同意”的方式。为了适应《个人信息安全规范》的要求，企业需要结合具体的数据类型、收集和使用场景，制定最合适的获取个人信息主体授权同意的方式，做到用户体感和个人信息保护的平衡。

（二）用户同意万事大吉?

目前行业实践中，大部分企业都将用户的知情同意作为个人信息收集的充分合规条件，忽略了必要性原则的门槛。对于《网全法》第四十一条规定的收集、使用个人信息的必要性原则，《个人信息安全规范》第5.2条进一步给出了三项衡量标准，即

[1] 见《中华人民共和国标准化法》，第二条。

收集个人信息与实现产品或服务的业务功能之间的直接关联、最低频率和最少数量关系标准。相比于欧盟GDPR中对于目的受限（Purpose Limitation）和数据最小化（Data Minimisation） 原则，《网安法》并未对必要性原则展开说明，《个人信息安全规范》的细化要求有利于保护个人信息主体的合法权益。

对于企业而言，有必要厘清自身产品和服务的具体业务功能以及实现该功能所必要的个人信息类型、收集频率和数量。否则在无法建立企业收集、使用个人信息必要性的情况下，企业很可能遭到用户和监管机构的质疑和挑战。侵犯个人信息相关主体的合法权益，可能会引发公益性集体诉讼，公司不仅要承担财产和名誉受损的风险，企业短时间所需更正的数据收集方式和类型，可能对公司的业务形态造成重大影响。

（三）不同信息要不同对待！

对于个人信息的收集，企业通常“一网打尽”，在收集、存储和使用各个环节“一视同仁”。但《个人信息安全规范》区分了个人一般信息和个人敏感信息。《个人信息安全规范》附录B还列举了个人敏感信息的判定因素和具体类型，包括个人财产信息、个人健康生理信息、个人生物识别信息、个人身份信息、网络身份识别信息等。

根据《个人信息安全规范》，企业首先需要了解自身收集的数据类型和数量，并将其进行相应的分类。对于个人敏感信息，建议按照《个人信息安全规范》的要求进行收集、存储和使用：

- 收集个人敏感信息时，应取得个人信息主体的明示同意；
- 收集个人敏感信息时，应区分产品核心功能和附加功能；
- 存储个人敏感信息时，应采用加密等安全措施；
- 对个人敏感信息的访问、修改等行为，宜在对角色的权限控制的基础上，根据业务流程的需求触发操作授权。

（四）用户权利不能不理！

对于个人信息的主体而言，除《网安法》中规定的删除权与请求更正权利以外，《个人信息安全规范》还对个人信息主体的权利进行了细化要求，以增强个人信息主体对其个人信息的控制。例如个人信息主体撤回同意权利、注销账户权利、获取个人信息副本权利、对于自动决策的申诉权利等。[2]此外，个人信息主体的上述权利实现机制也须在个人信息控制者制定的隐私政策中予以明示。

[2]《网安法》第四十三条规定，个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

此外，对于尚未建立对个人信息主体各项请求进行响应的企业而言，应当针对企业的商业实践和数据处理的目的尽早建立相应的响应机制。例如，企业可以在隐私政策中告知用户联系热线或者在服务平台上建立查询、修改个人信息或注销账户的方式，以满足个人信息访问、更正个人信息或注销账户的请求权。

（五）安全事件如何应对？

《网安法》第二十五条和第四十二条，分别提出了网络运营者应当制定并在发生危害网络安全的事件时及时启动网络安全事件应急预案，以及个人信息安全受到严重侵害时及时通报用户和有关主管部门的要求。《个人信息安全规范》第9部分对网络安全事件应急预案和个人信息安全事件处置予以了进一步的详细规定，包括安全事件应急处置和报告、安全事件告知两方面的内容。

在安全事件应急响应方面，建议企业制定个人信息安全事件应急预案，其中包括个人信息安全事件的分类、事件分级、组织体系与职责、预防预警、应急响应、保障措施等；定期组织内部相关人员进行应急响应培训和应急演练；在发生个人信息安全事件时，应及时将事件相关情况告知受影响的个人信息主体及有关主管部门。

（六）制度建设很重要

事前的预防效果一般而言优于事后的补救，对于安全事件的处理问题，配备完善的技术队伍，明确各方负责人的领导责任，以此形成良好的管理系统和个人信息保护工作机构，为个人信息安全事件建立坚实的防火墙是比较有效的预防措施。《个人信息安全规范》就组织的管理要求制定了一系列相关规范，尤其是对于个人信息处理从业人员较多或者处理大量个人信息的企业，还需设立专职的个人信息保护负责人和个人信息保护机构。

对于企业而言，较为主要的个人信息组织管理措施包括定期对个人信息安全影响进行评估，建立自身的评估机制，除此以外，还应建设适当的数据安全能力，定期对相关人员进行管理培训，并对自身建立的相关隐私政策以及安全措施的有效性进行审计，完善具体的审计系统，落实必要的管理和技术措施，最大程度地防范个人信息的泄露、损毁和丢失等情况发生。

四、跨国企业适用《个人信息安全规范》的注意要点

对于国内企业，跨国企业所面临的个人信息保护问题更为复杂。由于跨国公司数据流转的多个环节可能涉及多个司法辖区，企业内部个人信息安全合规体系往往需要协调多国个人信息保护的法律和要求。

此次公布的《个人信息安全规范》已经参考了OECD隐私框架、APEC隐私框架等国际规则，GDPR、欧美《隐私盾框架》（EU-U.S. Privacy Shield Framework）、美国《消费者隐私权法案》（Consumer Privacy Bill of Rights）等欧美个人信息保护

方面的立法，并与这些国家上通行的个人信息保护规则具有很多相似之处。比如围绕个人权益为中心的目标，《个人信息安全规范》和GDPR都借鉴了OECD（Organization for Economic Co-operationand Development）《保护个人信息跨国传送及隐私权指导纲领（1980）》和APEC（Asia-Pacific Economic Cooperation）《隐私保护框架（2004）》等国际准则和地区立法的规定，针对个人信息控制者开展个人信息处理活动提出了个人信息安全的基本原则。

但跨国公司需要注意其中的差异，以免造成实践中的混乱：

（一）GDPR与《个人信息安全规范》差异举例

对于网络运营者需满足的个人信息主体相关权利而言，《个人信息安全规范》与GDPR的规定具有很多相似之处，值得注意的是其中的差异。以数据可携权为例：

“用户要求微信把个人数据给钉钉？！”

数据可携权是一项比较有争议的权利。在数据成为企业竞争资源的情况下，即使用户提出要求，很少企业愿意将用户个人信息的副本传输给别的企业。

但GDPR的第20条规定了，数据主体有权以有序的、常用的、机器可读的方式获取其个人数据，并且有权将这些数据转移到另一个控制者，原始收集、存储这些数据的控制者不得干扰数据主体的转移。在技术可行的情况下，数据主体有权要求原始收集、存储其个人数据的控制者直接将这些数据转移到另一个控制者。数据可携权不得不利地损害他人的权利和自由。根据该项规定，如果数据主体有要求，就会出现微信不得不将用户个人信息副本提供给钉钉的情况。

让中国大多数企业松了口气的是，尽管《个人信息安全规范》第7.9条也规定了个人信息可携权。但与GDPR不同的是，《个人信息安全规范》将数据可携权的行使对象限定在了四种特定的个人信息类型：（a）个人基本资料、个人身份信息；（b）个人健康生理信息、个人教育工作信息。因此只有涉及到用户基本信息，以及用户和社会公共利益的情况下，微信才有可能需要将信息提交给钉钉。

（二）《个人信息安全规范》相比GDPR更为具体的要求

值得注意的是，《个人信息安全规范》并未是对国外规则的照搬和套用，其根据中国个人信息保护实践提出了一些更为具体的要求，大部分已经根据GDPR进行内部调整的企业需要尤其注意：

	欧盟GDPR	《网安法》及《个人信息安全规范》
处理要及时	并未就数据控制者在数据处理各个环节中需采取的措施予以明确说明	收集个人信息后，**个人信息控制者宜立即进行去标识化处理，并采取技术和管理方面的措施，将去标识化后的数据与可用于恢复识别个人的信息分开存储**，并确保在后续的个人信息处理中不重新识别个人
存储有要求	并未就数据控制者在数据处理各个环节中需采取的措施予以明确说明	个人信息控制者**在存储个人敏感信息时，应采用加密等安全措施；存储个人生物识别信息时，应采用技术措施处理后再进行存储**，例如仅存储个人生物识别信息的摘要
通知要到位	仅对于**被公开**的数据，数据控制者在获悉数据主体请求后要求采取**“合理措施”**告知（第三方）删除数据。（因此，并不是绝对的义务）	个人信息控制者违反法律法规规定或违反与个人信息主体的约定向第三方共享、转让个人信息，且个人信息主体要求删除的，**个人信息控制者应立即停止共享、转让的行为，并通知第三方及时删除**
答复时间短	**考虑到响应请求的复杂性和请求的数量众多，响应实现可推迟两个月**	**个人信息控制者对于数据主体的请求，应在三十天内或法律法规规定的期限内做出答复及合理解释（无推迟响应的规定）**
特殊信息存本地	无此要求	关键信息基础设施运营者在中国境内运营中收集和产生的个人信息和重要数据需在境内存储
父母管得宽	仅处理16岁以下未成年人**社会服务信息**需获得监护人同意	收集未满14周岁未成年人的**所有个人信息**都需获得监护人的明示同意
来源不明查得严	数据控制者需向数据主体提供有关间接获取其数据的信息	间接获取个人信息时应要求个人信息提供方**说明个人信息来源，并对其个人信息来源的合法性进行确认**

	欧盟GDPR	《网安法》及《个人信息安全规范》
画像要谨慎	无用户画像的区分	**区分直接和间接用户画像**。为准确评价个人信用状况，可使用直接用户画像，而仅用于推送商业广告目的时，则宜使用间接用户画像
隐私政策写得细	隐私政策需包含处理个人数据的目的以及法律依据	隐私政策需包含收集、使用个人信息的目的，以及**目的所涵盖的各个业务功能**，例如将个人信息用于推送商业广告，将个人信息用于形成直接用户画像及其用途等

总结

“明者因时而变”

在数据经济全球化发展的趋势下，各国对于个人信息保护的立法不仅影响个人信息相关主体的合法权益，也间接关系到本国数据经济发展的速度。 如何在数据经济发展和个人信息保护中间找到平衡点的关键之一是要解决高速发展的数据经济形式和个人信息保护法律法规稳定性的矛盾。 《个人信息安全规范》作为一项国家推荐性标准，兼具技术性和灵活性的特点，参考国际规则，及时地填补了中间的空缺。在当前数据经济的发力阶段，顺应发展潮流，应时而变，是企业合规工作和监管机关执法的重要参考。

企业也应该“应时而变”，摈弃不合时宜的个人信息收集使用的行业惯例，冲破惯性思维，按照《个人信息安全规范》中要求重新审视商业行为，梳理内部个人信息安全保护制度，降低合规风险的同时也提高企业数据资产的竞争力。

“知者随事而制”

尽管《个人信息安全规范》为企业的合规工作提供了重要的参考，但不同主体、不同的行业甚至不同的商业模式都对个人信息有不同的需求，采用不同的收集、使用、存储和传输方式。因此生搬硬套《个人信息安全规范》即无法满足个性化的商业发展需求，也无法实现充分开发数据价值的目的。《个人信息安全规范》确实为符合《网安法》相关条文提供了一套合规体系建议，但是企业仍然需要在确保自己符合《网安法》相关规定的同时，根据自身发展的需要和行业特点个性化建设自身的合规制度。

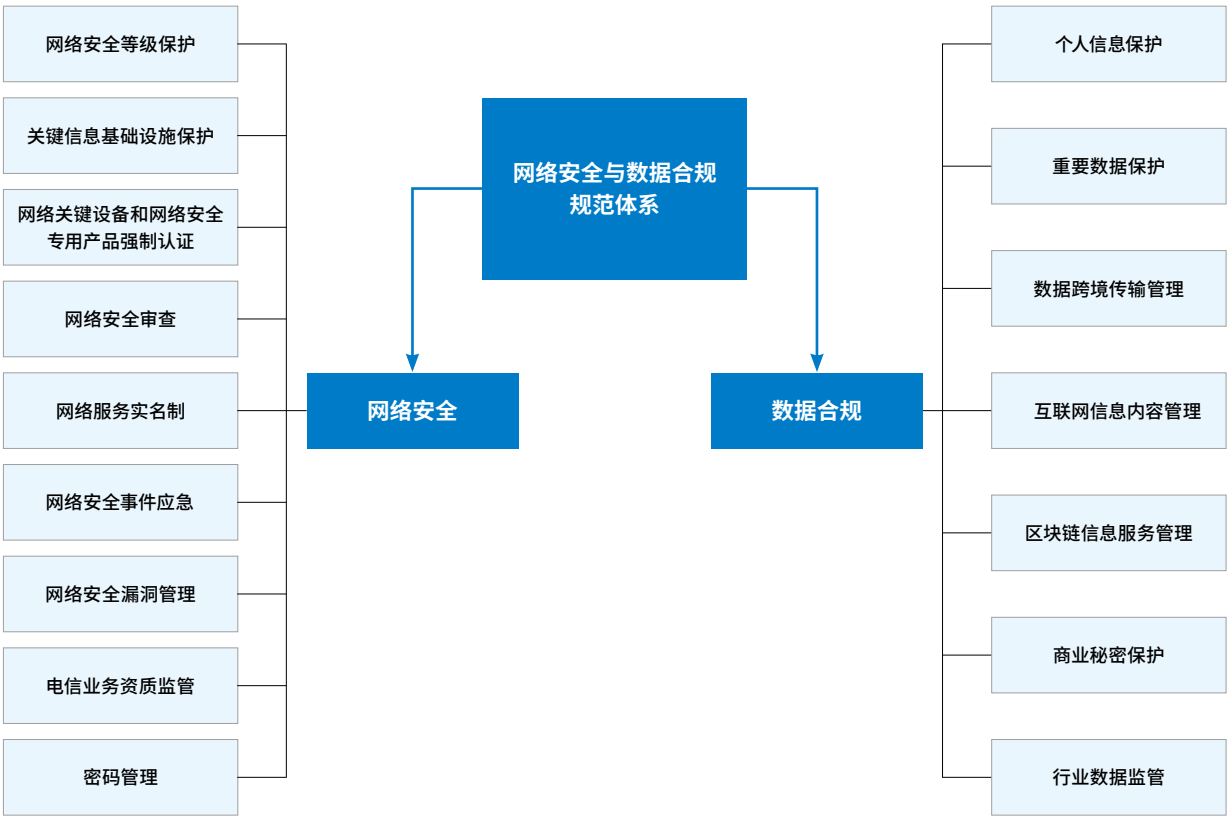
总而言之，“明者因时而变，知者随事而制”。企业应打破不合时宜的行业惯例，积极关注个人信息保护的立法和执法动向，创新性发展个人信息保护方式，参考《个人信息安全规范》搭建符合自身需求的新架构，努力走出一条数据安全合规和商业化应用的双赢之路。

（本文发布于2018年02月07日。）

2020年网络安全与数据合规：合规创造价值

引言

距离我们将“网络安全与数据合规”（Cybersecurity & Data Compliance）作为合规工作的单独门类已经近四年时间，网络安全与数据合规工作的内涵和外延不断地发生变化，逐步形成了以《网络安全法》（以下简称“《网安法》”）以及《全国人大常委会关于加强网络信息保护的决定》（统称“一法一决定”）为基础，配套法律法规以及国家标准为框架的合规体系。



企业对网络安全与数据合规工作的认识也日益加深，大多数企业已经任命专门的网络安全负责人以及个人信息保护负责人，加强内部网络安全与数据合规制度建设与培训。企业内部合规意识的增强得益于网络安全与数据合规相关规则高频率的出台和广泛的宣传，同时近年来相关执法活动的逐步开展也推动了企业内部合规工作的落地。

从2019年的立法执法活动来看，我国网络安全与数据合规工作即将迈入2.0时代。**企业2020年合规工作即将步入“深水区”，不仅以“技术+合规”为基础，兼顾企业的商业发展，同时以网络及数据合规资产为导向的合规工作还将直接影响企业的商业价值。“合规创造价值”将成为2020年网络安全与数据合规的工作重点。**

本文将回顾**2019年的重要立法、执法和相关活动（请见文后附表）**并以此展望2020年网络安全与数据合规工作。

一、2019年网络安全与数据合规回顾与述评

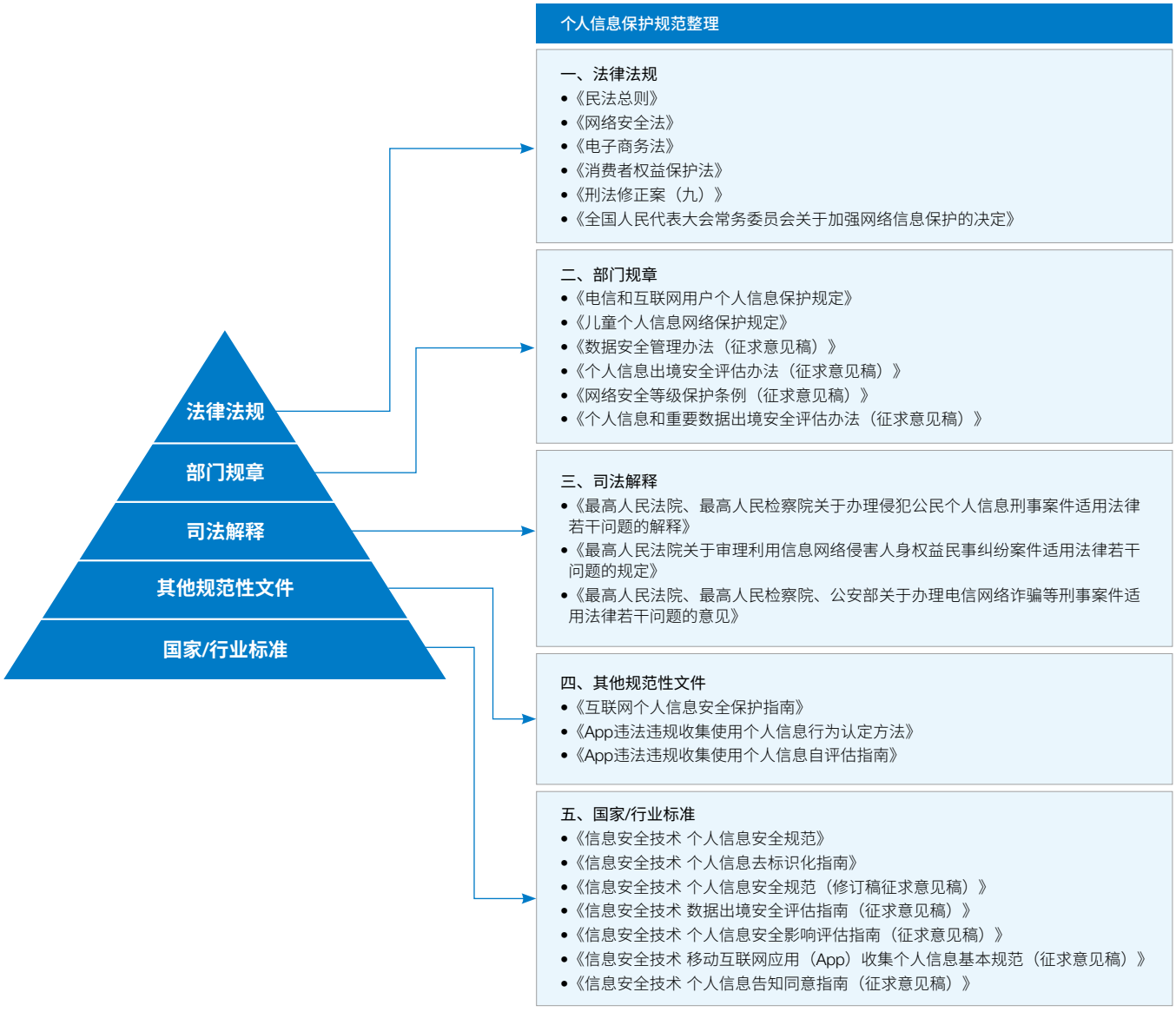
个人信息保护是2019年网络安全与数据合规工作的重点领域，网络安全等级保护、关键信息基础设施（以下简称“CII”）保护、数据跨境传输与互联网信息内容服务管理等领域也有重要的发展。同时主管部门在多项重点问题上已经形成较为成熟的监管思路，正逐步推进执法和监管的落地，我国网络安全与数据合规的治理格局也日益稳定。

（一）个人信息保护进入深水区，数据管理与利用双管齐下

- 立法工作相互衔接，“层层”递进

1. 以法律为核心，法规与国家及行业标准配套的立法体系
2. 强化特定类型比如儿童个人信息的保护
3. 细化个人信息同意、收集必要性等具体规范

作为个人信息保护的基础性法律之一，《网安法》从其颁行伊始，其体系规则通过“战略-法律-法规-国家及行业标准”的次序和层次做到“层层递进，逐步落实”。这一“多层次”的规则构建思路在2019年个人信息保护领域中得到了显著的体现。



从基本法律层面看，个人信息保护的原则在多项法律中相互衔接，逐步发展。《民法总则》第111条对“个人信息权利”作出规定，与《网安法》中关于“个人信息保护”的基本规则进行呼应。《民法典分编》草案中也将可能纳入“隐私权和个人信息保护”的专章专节，正式在民事法律关系领域的基本大法中确立了个人信息基本民事权益的法律地位。此外，《个人信息保护法》也被列入了全国人大常委会的立法计划，有望成为我国关于集个人信息属性、民事权益和保护规则于一体的基础性法律。

从具体规范层面看，《儿童个人信息网络保护规定》是我国第一部针对儿童的个人信息保护的专门立法，不仅具有立法领域上的综合性，更具有保护主体上的针对性，弥补了我国关于儿童个人信息保护具体规则的空白，也让我国儿童个人信息保护的水平与国际要求逐渐接轨（详情请见文章**《儿童个人信息保护的亮点和启示》**）。除此以外《数据安全管理办法（征求意见稿）》等规章文本也陆续出台，还有《个人信息去标识化指南》《个人信息安全规范（修订稿征求意见稿）》和《个人信息安全影响评估指南（征求意见稿）》等国家标准的编制。从构建规则的角度看来，我们理解，主管部门已从个人信息保护的基础规则，逐渐开始关注具体的操作环节和特定类型的个人信息，例如去标识化、安全影响评估和儿童个人信息等，注重在现有成型的规则框架中进一步丰富个人信息保护工作的内涵，以期为执法实践和企业合规提供更全面、具体的参照。

相类似地，2020年初出台的另外两份国家标准（《移动互联网应用（App）收集个人信息基本规范》和《个人信息告知同意指南》）征求意见稿也在一定程度上延续了这一趋势：从微观与实质入手，要求企业全面检视“App采集的个人信息是否最少必要”以及“同意是否充分有效”，并通过必要的技术和组织措施进行完善。

- **App治理由表及里、多方共治**

1. 多部门联合执法与单独执法相结合
2. 执法内容从文本优化深入到产品设计和技术实现
3. 加强实质性合规，考虑开展APP认证

贯穿2019年的App个人信息保护专项治理与执法活动也体现出个人信息保护工作正逐步进入“深水区”（详情请见文章**《图示移动App个人信息保护的重点》**”）。

承接2018年的执法治理活动，2019年初，中央网信办、工信部、公安部、市场监管总局等四部门决定全年在全国范围内组织开展App违法违规收集使用个人信息专项治理，而治理工作的关注点也从前期的App隐私政策制定与起草、App产品功能的整体设置，逐步深入至用户账户的注销管理、用户权利的响应机制、App处理个人信息所使用的技术模块（如SDK、API、Cookie等）与重要系统权限（如摄像头、存储读写、麦克风、位置、系统日志等）的调用是否合规等问题。同时，从App监管向外延伸的工作中可见，主管部门也高度关注由新兴技术利用引发的个人

信息保护问题，如“3·15晚会”曝光的Wi-Fi探针、使用场景日渐增多的人脸识别技术、多见于大数据采集与分析行业的爬虫技术等等。

由此可见，个人信息保护监管的“形式合规”阶段（如优化用户协议与隐私政策）即将成为过去式，强调精细化、定制化、微观化的“实质合规”将成为主管部门未来工作的关注重点。**因此，这将既要求合规部门对产品所使用的技术具有全面、透彻的认识，也需要商务、技术部门在产品生命周期内始终保持高度的合规意识，才能确保企业在“形式合规”的基础上，在实质层面真正落实App个人信息保护的合规工作。**

此外，App治理工作在监管手段上还呈现出两大特点。一方面，四部门虽有联合行动，不同部门也会在自身职权范围内开展相应的执法，例如公安部的“净网行动”、工信部的信息通信领域App专项整治等，且不同部门的执法要求与关注点还可能存在差异。因此，**为了更好地应对不同部门的专项执法要求，企业在设计产品合规方案时就应该充分考虑执法的趋势与程度，在可行的范围内以更为严格的标准落实合规，以避免周旋于不同治理要求之中而应接不暇。**

另一方面，除了专项整治外，App安全认证更是主管部门在监管形势上的又一创新。App运营者参与申请App安全认证，既能发挥第三方独立检测机构的技术优势，也能发挥以各大搜索引擎、应用市场在辅助监督层面的价值，一定程度上减轻主管部门的执法负担，更能调动App运营者的合规积极性，可谓一举多得。考虑到未来的App治理工作将进一步深入，App安全认证的范围亦即将放开，有条件的企业确实可以考虑通过取得安全认证的方式，推进App产品的实质合规，以便更为游刃有余地配合执法工作。

- **重点行业严格执法 数据全链条合规**

1. 金融、征信、医疗、交通、电信、互联网等行业是重点监管行业
2. 公安个人信息保护执法中注重数据全链条的合规性
3. 资本市场也注重数据合规性，以合规为出发点考虑企业持久盈利能力
4. 建议企业从自身合规为起点，流程合规性证据，同时加强第三方数据合规性管控
5. 企业的数据合规工作宜早不宜迟

考虑到不同的行业所涉个人信息的敏感程度、规模有所区别，主管部门在执法中也有区分轻重缓急。**金融、征信、医疗、交通、电信、互联网等行业因在经营过程中能够接触到海量的个人（敏感）信息，且行业覆盖范围极其广泛，始终是主管部门高度关注的“严监管”行业。**

2017至2018年间，以“数据堂案”为典型的电信行业侵犯公民个人信息等相关案件轰动一时。2019年，围绕“个人金融信息”“（类）征信业务”“爬虫技术”等关键词、以“套路

贷”“砍头贷”“714高炮”等经济活动犯罪为导火索引发的金融风控行业全链条彻查，出现引发广泛社会关注的系列案件。值得注意的是，在刑事侦查领域，**公安部门对“严监管”行业的关注通常不会停留在某一业务节点，而通常会延伸至切入点的上游或下游业务，并从宏观层面考察上下游业务之间可能存在的关联性，以及其中可能涉及的个人信息处理活动。**

同时，相关的执法也引发行业主管部门对行业格局、业务逻辑、业内规范的反思，比如在金融行业，《个人金融信息（数据）保护试行办法（初稿）》和《金融消费者权益保护实施办法（征求意见稿）》陆续出台，旨在新经济条件下规范个人金融信息收集和使用。

此外，包括个人信息保护在内的数据合规问题也引发了资本市场的关注。比如2019年下半年各大证券交易所也在IPO（尤其是科创板）中加大对拟上市企业数据合规情况的问询，除了发函要求保荐机构与律师事务所针对具体个人信息处理问题发表正式意见以外，个别项目中证券交易所甚至组成督查组进场驻扎，对重点关注问题进行现场勘验（详情请见文章**《企业上市关注的重点数据合规问题》**）。而其中，主营业务中实质性涉及个人信息采集、分析和共享等处理活动的拟上市企业备受关注，存量数据的合规性问题、企业内部数据合规制度的完备性问题以及企业与外部第三方间数据交互的合规性问题则是证券交易所密切关注的重点。

换言之，我们理解，企业（尤其是处于“严监管”行业的企业）日后在开展个人信息保护工作时，首先要“独善其身”，进行数据全面梳理、文本优化与内部制度构建，并保留合规性证明文件为日后应对检查准备，同时为融资等后续资本运作保存材料。并且，还应当注重与自身存在数据交互的第三方，以最大限度地避免数据合规瑕疵在业务流程中得以传导和流入。此外，企业开展数据合规的时点宜早不宜迟，不能在业务和产品上市、商业模式基本成型后再行考虑和开展数据合规评估，而应当在产品的设计之始就纳入数据合规理念，并使之贯穿于产品的全生命周期。

• 数据“合规”与“价值”并举

1. 数据合规不是为了应对执法，应该创造价值
2. 数据溯源与确权的最终目的是为了固定数据相关权益
3. 数据资产、数据治理是数据价值合法合规实现的基础

纵使如此，执法与监管本身并不是目标，正如“合规创造价值”的观点一般，“合规”并非终极目的，而是创造“价值”的必备要件。因此，从充分调动数据利用积极性的角度而言，我们注意到，《数据安全管理办法（征求意见稿）》中除了凸显“个人信息与重要数据的跨境传输实施分轨管理”以外，其最大的特点则是立法的出发点与落脚点在于“数据”，而并未限定特定的类型（详情请见文章**《短评〈数据安全管理办法（征求意见稿）〉》**）。随着《数据安全法》亦被列入了立法规划之中，我们理解，国家对数据治理的布局思路也逐步体现，既要强调安全管理，开展经营与运行时做到实质合规，也要强调合理利用，在合规的基础上充分挖掘数据对经济活动的价值。

因此，国家领导层所大力倡导的、《区块链信息服务管理规定》所指向的区块链技术或许正是体现这一思路的典型代表：在监管数据合规的同时，需要逐步利用技术手段实现数据的安全可信共享，在维护数据隐私和安全的前提下促进数据的共享和流动，打破数据孤岛，让数据产生价值。由此可见，数据价值的合理开发和利用，也将成为未来数据管理工作的又一重点。对数据驱动型企业而言，如何将数据从纯粹的业务材料提升为数据资产，使其得以固定、并能够为企业创造和实现价值，将是难以绕开的核心问题（详情请见文章**《“数据资产”的误区与合规条件》**）。相应地，如何在企业内构筑“数据资产管理体系”以更高效的形式运营数据，亦将成为企业未来在合规前提下谋求可持续发展的核心任务。

（二）网络运行安全防护更上层楼

• 等保2.0为核心的网络安全保护体系

1. 网络安全等级保护是企业需要履行的法定义务
2. 对等保2.0的实施落地将是执法长期关注的指标
3. 等保2.0的实施落地是企业网络安全的基础，但不是终点

以GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》为代表的三项网络安全等级保护核心国家标准正式生效，意味着“等保2.0”时代的新里程正式启航。

与“等保1.0”有所不同，“等保2.0”源自于《网安法》第二十一条对“网络安全等级保护制度”的框架性规定，因而其法律依据的位阶更高，在企业合规工作中具有更强的必要性与引导作用。此外，为体现更好的政策与产业兼容性，等保2.0体系也将云计算、移动互联、物联网、工业控制系统和大数据等应用纳入防护体系中，并在安全通用要求的基础上拟制了拓展要求，以便相关企业能够最大限度地定制等保合规策略（详情请见文章**《国际新形势下的等保2.0》**）；同时，新《密码法》也为等级保护中的“密码”使用提供了必要的指引与启示。（详情请见文章**《〈密码法〉要点评析及企业合规路径》**）

随着基本要求、测评要求、安全设计技术要求和实施指南的正式落地，等保2.0的标准体系已基本完善；虽然2019年主管部门并未专门针对等保2.0开展专项治理活动，考虑到等级保护备案/认证属于标准化合规事项，“是否落实等级保护制度”一直是公安机关在日常网络安全检查和临时突袭检查中的必检科目。因未能及时落实等保义务，继而引发其他安全或违规事件而导致行政处罚的案例也并不鲜见。由此可见，作为网络安全常态合规中必不可少的部分，等保2.0是承载网络安全与数据价值的基本所在，缺乏对网络与信息系统合适、对等的防护，安全与价值犹如无源之水、无本之木。因此企业在日常合规中也应将网络安全等级保

护工作置于显要位置，并应将其作为企业进一步增加网络安全能力的重要基础。

- **CII保护箭在弦上、稳步推进**

1. CII保护的前提是CII识别，CII识别工作已经逐步推进
2. CII保护应当从等保、数据出境义务、网络产品及服务采购等多环节把控

事实上，与等保2.0密切相关、国家网络安全工作核心的CII保护也在稳步进行。不少行业已逐步进行内部评定，并初步筛选和识别该行业内的CII。与此同时，2019年12月，全国信安标委秘书处就在北京组织召开了国家标准《信息安全技术 关键信息基础设施网络安全保护基本要求（报批稿）》的试点工作启动会，并在电信、广电、能源、交通、金融、卫生健康等重点行业和领域选取了12家单位作为标准应用试点单位。由此，从内部合规的角度，企业应当密切关注自身行业内对CII识别与试点合规的情况。

就CII规则体系构建的层面而言，除了等保2.0能够为不同等级的CII（原则上不低于三级）提供网络安全合规参照外，《云计算服务安全评估办法》与《网络安全审查办法（征求意见稿）》的出台，也进一步夯实了CII在开展网络产品与服务（如云计算服务）采购活动中的安全可控，从国家层面为CII保护提供必要的规则支撑（详情请见文章**《〈网络安全审查办法（征求意见稿）〉简析》**）。我们理解，鉴于二者均以“是否关切或影响国家安全、经济安全、社会稳定、公共利益”等指标作为衡量与判别因素，随着CII保护工作条件的日臻成熟，CII的范围与对象将逐渐明朗，“重要数据”的界定思路和范围也可能得以进一步明晰，相应的合规工作也将能够正式启动。可以预见的是，如《关键信息基础设施安全保护条例》能够早日出台，主管部门与各行业企业将会在更大范围内，更有力地推动CII保护工作的开展。

（三）互联网信息内容服务管理是网络生态治理的核心

互联网信息内容管理一直以来都是监管和执法的重点领域。2019年内出台的《网络生态治理规定》与《互联网信息服务严重失信主体信用信息管理办法（征求意见稿）》不仅说明互联网信息内容服务管理是网络安全治理中不可或缺的重要组成部分，也证明了其在网络生态治理中的核心地位。

一方面，《网络生态治理规定》通过对“网络信息内容生产者”、“网络信息内容服务使用者”和“网络信息内容服务平台”进行责任划分，要求其各自规范自身任内行为，将显著有利于建立健全网络综合治理体系，落实互联网企业信息管理主体责任，并能够以法律的武器遏制网络暴力、人肉搜索、深度伪造、流量造假、操纵账号等污染网络生态的行为，构筑严厉的“事后追究机制”。

另一方面，《互联网信息服务严重失信主体信用信息管理办法（征求意见稿）》则是响应2019年7月颁行的《国务院办公厅关于加快推进社会信用体系建设构建以信用为基础的新型监管机制的指导意见》的号召（详情请见文章**《新型信用监管机制问答》**），从互联网信息服务领域促进信用建设，并计划启动信用黑名单管理和失信联合惩戒，有意向严重失信主体呈现“前置性威慑”，以抑制违法违规行为的出现。

两份规范性文件虽然规制切入点和工作机制有所不同，但二者都是从责任追究的角度出发，拟进一步加强对我国互联网空间信息内容服务的监管。考虑到“网络信息（内容）服务”的范围较为宽泛，除了提供相关服务的平台企业需要着重关注以外，普通企业在管理内部网络信息内容服务时也需谨慎行事，避免因轻视的心态而引发不利的合规后果。

二、2020年网络安全与数据合规工作的展望与启示

（一）展望

结合2019年工作的回顾，在2020年我们重点提示如下：

- 个人信息保护的监管态势与多方共治的态势将得以保持。主管部门的“微观”监管视角也将可能延续和进一步推进，持续关注App和移动智能设备中用于采集用户个人信息的技术手段，而国家与行业标准也将仍然是执法实践与企业合规工作参考的重要材料。
- 随着人工智能、物联网、云计算、生物识别等技术的进一步发展和普及，利用前述技术开展个人信息处理的产品和应用也将成为主管部门的关注重点；而监管的切入点将不限于App专项治理与安全认证、企业拟议IPO、专项刑事案件调查等，而可能是在更多既存的日常检查与执法活动中嵌入数据合规方面的考察内容，使数据合规进一步成为常态化监管要求。
- 随着等保2.0体系的完备与成熟，以及CII保护工作的试点完成，《关键信息基础设施安全保护条例》将可能得以正式出台，CII保护工作也可能将实质性地铺开。相应地，不排除与CII存在一定关联的“重要数据”识别和划定工作也将在不同行业中展开。
- 历经2017年与2019年两次的规制路径优化，数据跨境传输的监管思路也逐渐成熟，在一定程度上具备了正式出台监管规范的条件。考虑到《数据安全管理办法（征求意见稿）》初步体现了“分轨管理”的机制，《个人信息出境安全评估办法（征求意见稿）》已经呈现借鉴欧盟GDPR标准合同条款思路的趋势，因而不排除主管部门将可能分别针对个人信息与重要数据的跨境传输更新和修订安全评估指南，以进一步完善跨境传输的工作机制。
- 电信与金融行业中主要涉及的个人信息处理活动在既往的专项执法中已进行了必要的梳理，而目前金融行业的个人信息处理与利用规则仍然处于破局攻坚阶段，业内产业链与格局也在主管部门的指引下相应调整。由此可见，“严监管”行业将仍然是执法监管的关注重点，而伴随执法监

管而来的还将是行业规则与业务逻辑的革新。

- 在严厉打击“严监管”行业中侵犯公民个人信息与其他数据权益案件的同时，“数据资产”的概念也逐渐浮出水面。在强调数据安全治理的同时，如何在合规的基础上盘活数据并使之成为资产，得以为企业创造更大的价值，既是主管部门需要提供指引与支撑的领域，也是企业需要深入思考与创新的问题。

（二）启示

关键词：技术+合规+产品；数据合规体系；数据融合；数据资产；数据治理

综上所述，针对企业2020年的网络安全与数据合规工作，我们建议：

- 企业的数据合规工作应该从关注隐私政策文本与产品界面优化，转而更多地关注产品功能的设计逻辑与底层技术；在设计、研发、运营等环节中嵌入数据合规元素，确保产品全流程合规和常态化合规；同时，企业可以考虑通过App安全认证等方式提升产品合规知名度。
- 企业内部数据合规体系的构建已成必要，因而需要召集产品、商务、技术与合规部门，共同了解企业当前的数据安全与合规现状，从企业的业务战略与目标出发，整理明确出数据合规的关键需求；在整体的信息化规划下进行数据合规体系、架构等的设计规划工作，并在落实数据合规的相关制度时，注重实施情况的反馈与制度的持续性改进。
- 企业应该密切关注主管部门的监管动态，尤其是位于“严监管”行业的企业，一方面需要留心行业主管部门结合本行业实际，对网络安全与数据合规提出的定制化要求；另一方面，也需要跟进《网安法》体系监管机构对数据跨境传输、重要数据保护等“待定领域”的最新动态，并在可行的范围内参考征求意见稿开展内部自查合规，以备应对专项执法活动的不时之需。
- 企业数据资产管理体系的构建是大势所趋。企业需要明确自身数据集合的类别与对应可主张的权利来源，完善数据融合体系为固定形成数据资产提供必要的基础（详情请见文章《**万字长文说“数据融合”**》）；通过数据资产模型规划和数据资产分级与分类，将数据集合进行“资产化”为后续的管理和使用提供便利；切实建立一套常态化、体系化、标准化的管理措施，针对特定数据资产拟定相应的管控措施与流程，以便数据资产的可持续运营。

2019年《网络安全法》体系重要立法、执法和相关活动整理

	规范制定	执法工作	其他
个人信息保护	法律、法规和规范性文件 •《民法总则》第111条 •《儿童个人信息网络保护规定》 •《数据安全管理办法（征求意见稿）》 •《民法典分编》草案进一步拓展个人信息保护的内容 •《个人信息保护法》《数据安全法》列入立法计划 国家标准 •《信息安全技术 个人信息去标识化指南》 •《信息安全技术 个人信息安全规范（修订稿）》（征求意见稿） •《信息安全技术 个人信息安全影响评估指南》（征求意见稿）	1月份：中央网信办、公安部、工信部、市场监管总局（以下统称“四部门”）宣布开展App违法违规收集使用个人信息专项治理 1月份（覆盖全年）：公安部组织部署全国公安机关开展“净网 2019”专项行动，依法严厉打击侵犯公民个人信息、黑客攻击破坏等网络违法犯罪活动，着力围绕金融行业“套路贷”行为进行全产业链条查处与打击 11月份：工业和信息化部开展为期三个月的信息通信领域App侵害用户权益专项整治行动 11月份：公安部加大打击整治侵犯公民个人信息违法犯罪力度，组织开展App违法违规采集个人信息集中整治，集中发现、集中侦办、集中查处整改了100款违法违规App及其运营的互联网企业	3月份：四部门联合发布《App违法违规收集使用个人信息自评估指南》 3月份：市场监管总局与中央网信办发布《关于开展App安全认证工作的公告》 4月份：公安部牵头北京网络行业协会、公安部第三研究所发布《互联网个人信息安全保护指南》 12月份：四部门联合发布《App违法违规收集使用个人信息行为认定方法》

	规范制定	执法工作	其他
个人信息保护	**行业相关** • 金融/征信 10月份：央行出台《个人金融信息（数据）保护试行办法（初稿）》 12月份：央行出台《金融消费者权益保护实施办法（征求意见稿）》 • 医疗 7月份：国务院颁布的《人类遗传资源管理条例》正式生效 • 证券 交易所针对拟上市公司（尤其是科创板IPO）的数据合规情况进行发函问询和进场督查		
网络安全等级保护	**立法工作** •《密码法》 •《信息安全技术 网络安全等级保护基本要求》 •《信息安全技术 网络安全等级保护安全设计技术要求》 •《信息安全技术 网络安全等级保护测评要求》 •《信息安全技术 网络安全等级保护实施指南》 •《网络安全威胁信息发布管理办法（征求意见稿）》 **执法工作** • 四部门于2019年5月至2019年12月，联合开展全国范围的互联网网站安全专项整治工作		
关键信息基础设施保护	**立法工作** •《云计算服务安全评估办法》 •《网络安全审查办法（征求意见稿）》 **其他** •12月份：《信息安全技术 关键信息基础设施网络安全保护基本要求》（报批稿）试点工作启动，在电信、广电、能源、交通、金融、卫生健康等重点行业和领域选取了12家单位作为标准应用试点单位		
数据跨境传输	**立法工作** •《数据安全管理办法（征求意见稿）》（第二十八条） •《个人信息出境安全评估办法（征求意见稿）》		
互联网信息内容服务管理	**立法工作** •《网络信息内容生态治理规定》 •《区块链信息服务管理规定》 •《网络音视频信息服务管理规定》 •《互联网信息服务严重失信主体信用信息管理办法（征求意见稿）》		

（本文发布于2020年02月10日。）

变化纵横出新意
——民法典中个人信息的定位及影响

《中华人民共和国民法典》（下称“**《民法典》**”）将于2021年1月1日正式生效。作为中国第一部以“法典”命名的法律，《民法典》集我国民事领域立法之大成，是我国民事立法领域具有划时代意义的重大立法成果。相较于此前的分散立法，本次《民法典》的一大亮点是将有关人格权的规定独立成编。这一编排体例的创新体现了当下民事法律体系对人身自由、人格尊严的重视与保障。

一方面，《民法典》在人格权编下对自然人“隐私权”和“个人信息”的新增规定和具体要求，反映了我国民事立法对互联网、信息数字化时代下个人隐私、个人信息等权益保障迫切需求的法律回应，为民事主体寻求个人隐私、个人信息方面的法律救济提供上位法依据。另一方面，个人信息等数据作为数字经济时代产业发展的关键要素之一，在我国产业发展促进的政策中同样有着举足轻重的地位。[1]在《民法典》施行之际，对个人信息及其有关权益的准确定位，将有助于企业正确认识个人信息商业化应用背后的权益逻辑，为日后的个人信息合规以及企业数据资产化工作提供理论支持。

一、个人信息性质的确立

（一）“民事权利”章节下的个人信息

相较于欧洲、美国等国家地区将个人数据保护作为基本人权的内容，或通过隐私体制对个人信息主体的权益予以保障，中国将如何定位个人信息保护一直是国际社会关注的焦点。

实际上，早在2017年颁布施行的《民法总则》中，就已明确将个人信息保护纳入民法视野。此次《民法典》吸纳了总则部分的全编规定，重申了个人信息保护的定位，强调获取个人信息应“依法取得”并“确保信息安全”，不得“非法收集、使用、加工、传输他人个人信息”，不得“非法买卖、提供或者公开他人个人信息”。[2]

虽然个人信息保护条款本身并未对“个人信息”是否构成法律意义下的民事权利进行明确，但从条款编排来看，无论是此前的《民法总则》还是当下的《民法典》，均将其置于“民事权利”章节之下，这一编排一定程度上反映了立法者从民事权利视角对个人信息保护进行法律定位的意图。

（二）个人信息的“人格权”的属性

此次《民法典》对于个人信息保护新增条款的编排进一步确认了个人信息的人格权属性。如前所述，人格权的独立成编构成了本次《民法典》在体例编排上的创新亮点，而将个人信息保护纳入《民法典》人格权编，则是对产业释放了又一大信号，即个人信息的人格权属性得到立法肯定。《民法典》第九百九十条对人格权的定义和范畴进行了明确，包括民事主体享有的生命权、身体权、健康权、姓名权、名称权、肖像权、名誉权、荣誉权、隐私权等权利。虽然其并未对个人信息的权利定位予以明确，但该条第二款强调了自然人同时享有“基于人身自由、人格尊严产生的其他人格权益”。个人信息作为识别、表明个人身份的标记信息，其存在本身就天然与个人在信息社会环境中的人格尊严存在密切联系。据此，个人信息将可能作为一种尚未具化为独立权利的“人格权益”受到保护。

[1] 2020年4月9日颁布的《中共中央 国务院关于构建更加完善的要素市场化配置体制机制的意见》明确提及要加快培育数据要素市场，提升社会数据资源价值，同时须加强数据资源整合和安全保护。

[2] 见《民法典》第一百一十一条。

诚然，当下有关个人信息乃至数据的法律属性仍旧存在较大争议。产业领域的个人信息处理涉及多方主体，各方对于个人信息是否应当享有某种权益、权益边界为何仍亟待讨论。但本次《民法典》对个人信息的人格权定位，至少确认了个人信息主体一侧对个人信息享有的权益属性，有助于未来进一步厘清个人信息相关的权益边界。

二、个人信息保护具体规则的创新与突破

如前所述，《民法典》中对个人信息保护的相关规定，意味着“自然人对个人信息享有受保护的民事权益”[3]的认可，而将其放置于“人格权编”的编纂体例，则强调了这种受保护的民事权益与“人作为目的性的存在”[4]、“人格尊严和人格自由”[5]之间的紧密联系。以下，我们尝试结合个人信息保护的相关条款及民法典的编撰体例，探讨个人信息保护具体规则的内涵。

《民法典》“总则”部分沿袭了2017年《民法总则》中对个人信息保护的原则性规定，重点强调并规制了第三人对公民个人信息的收集、使用、加工、传输、提供、公开等行为。同时，《民法典》“人格权编”第五章对个人信息的定义、[6]处理个人信息的原则和条件、[7]自然人针对个人信息的查阅、复制、请求更正、请求删除的权利、[8]信息处理者不得泄露、篡改、向他人非法提供个人信息及保障信息安全义务、[9]法定机构及其工作人员对个人信息的保密义务[10]等内容作出了特别规定。

（一）个人信息处理的合法基础：“个人信息主体的同意为原则”及有限例外

与2017年生效的《中华人民共和国网络安全法》（下称“《网安法》”）体系[11]相协调，《民法典》在第一千零三十五条第一款中重申了“个人信息主体或其监护人的同意”作为全生命周期的个人信息处理（包括收集、存储、使用、加工、传输、提供、公开等环节）的合法性基础，体现了对个人信息主体在个人信息处理全流程中主体性的认可与尊重，充分保障了个人信息主体的同意权。第一千零三十五条的规定同时与第一千零三十七条、第一千零三十八条共同构成了对个人信息处理事前同意、事中知情、[12]事后救济[13]框架，为个人信息主体提供了周延的保护。

第一千零三十五条同时首次从法律层面肯定了除“征得该自然人或者其监护人同意”外，“法律、行政法规另有规定”也可以作为处理个人信息的合法基础，既有助于明确《民法典》、《网安法》下关于授权同意与其他法律法规衔接的处理方式；同时也能够帮助信息处理者更加准确地理解个人信息处理行为的合规边界，选择合适的信息处理方式和商业模式，对个人信息处理的实践将产生巨大的影响。如果企业或其他信息处理者能够确认相关的信息处理行为是根据法律、行政法规的规定而开展，则可能无需另行征得自然人或者其监护人的同意。

我们期待着以《民法典》为开端的对个人信息处理合法性基础体系的进一步明确与构筑，能够更好地为平衡个人信息保护与利用、充分保障个人信息的“人格尊严和自由价值”同时发挥其“商业机制”和“公共管理价值”[14]提供指引。

（二）个人信息处理主体的概念创新：“信息处理者”

欧盟《通用数据保护条例》（General Data Protection Regulation, 下称“GDPR”）对于个人数据的处理主体基于责任和义务区分“个人数据的控制者”、“个人数据的处理者”以及“个人数据的共同控制者”等不同主体，其目的之一是明确个人数据处理中不同主体的责任边界。我国推荐性国家标准GB/T 35273《信息安全技术 个人信息安全规范》也曾参考其他司法辖区的做法将“个人信息控制者”[15]作为主要的规制对象和义务主体。

《网络安全法》考虑到适用的范围，以个人信息常见载体“网络”为切入点，通过定义“网络运营者”（即网络的所有者、管理者和网络服务提供者），来对个人信息的“收集、使用”“存储”等个人信息全生命周期处理环节进行规制，并强调网络运营者对于个人信息主体权利的响应要求。

区别于《网安法》以及其他司法辖区的做法，《民法典》第一千零三十五条中将“个人信息的处理”界定为“包括个人信息的收集、存储、使用、加工、传输、提供、公开等”各个环节，并肯定了自然人向“信息处理者”请求行使针对个人信息的权利、以及“信息处理者”需承担的信息安全义务等内容。[16]结合相关条款，我们理解民法典中“信息处理者”应当包括参与个人

---

[3] 程啸. 民法典编纂视野下的个人信息保护[J]. 社会科学文摘, 2019(11):71-73.

[4] 张新宝. 从隐私到个人信息:利益再衡量的理论与制度安排[J]. 中国法学, 2015(03):38-59.

[5] 程啸.民法典编纂视野下的个人信息保护[J]. 社会科学文摘, 2019(11):71-73.

[6] 《民法典》第一千零三十四条。

[7] 《民法典》第一千零三十五条。

[8] 《民法典》第一千零三十七条。

[9] 《民法典》第一千零三十八条。

[10] 《民法典》第一千零三十九条。

[11] 《网安法》第四十一条第一款“网络运营者收集、使用个人信息，应当……经被收集者同意”。

[12] 《民法典》第一千零三十七条第一款，“自然人可以依法向信息处理者查阅或者复制其个人信息”。

[13] 《民法典》第一千零三十七条第一款，“发现信息有错误的，有权提出异议并请求及时采取更正等必要措施”；第二款，“自然人发现信息处理者违反法律、行政法规的规定或者双方的约定处理其个人信息的，有权请求信息处理者及时删除”。《民法典》第一千零三十八条第二款“发生或者可能发生个人信息泄露、篡改、丢失的，应及时采取补救措施，按照规定告知自然人并向有关主管部门报告”。

[14] 张新宝. 从隐私到个人信息:利益再衡量的理论与制度安排[J]. 中国法学, 2015(03):38-59.

[15] 如GB/T 35273-2020《信息安全技术 个人信息安全规范》第3.4条将“个人信息控制者”界定为“有能力决定个人信息处理目的、方式等的组织或个人”。

[16] 《民法典》第一千零三十七条、第一千零三十八条。

信息全流程处理的各方主体，而不仅局限于“有能力决定个人信息处理目的、方式”的“控制者”。

我们理解，《民法典》中“信息处理者”概念的引入和基于“信息处理者”的义务责任构筑方式，在一定程度上反映了从“个人信息主体权益”出发的立法思路。从比较法来看，尽管“个人信息控制者”与“个人信息处理者”[17]两者之间的相对权利义务关系上可能存在差异，但“个人信息控制者”相对于“个人信息主体”而需承担的责任和义务水平应当并已经实质性地通过法律法规、协议（如实践中通常采用的数据保护协议）约定施加于“个人信息处理者”，因此就“个人信息控制者”“个人信息处理者”分别相对于“个人信息主体”应当承担的责任和义务可能并不存在实质且显著的差异，将相关的责任义务概括性地及于参与个人处理的各方主体，可能有助于个人信息主体依据实际情况选择主张权益的具体对象和方式，实践中可能有利于个人信息主体主张权益。

（三）隐私权与个人信息保护的关系

除了前述的一般性规则外，本次《民法典》个人信息保护规则中另一项值得关注的内容则是“关于隐私权和个人信息保护的关系”[18]。有关隐私权和个人信息保护的关系是《民法典》编撰过程中的争论焦点问题之一，比较法上广泛采取的隐私与个人信息“一元制”保护模式[19]曾一度影响我国在个人信息保护与隐私权的立法模式探讨以及司法实践，即认为无须单独规范个人信息条款，而是可以通过隐私权等既存具体人格权实现对个人信息的保护。在这种情况下，司法实践中对于某些不当利用个人信息并因此造成人格权益损害的行为，往往需要通过具体的人格权利，如隐私权、名誉权等方式进行规制和救济。

例如，在此前引发广泛关注的某知名旅游中介网站及航空公司泄露客户隐私信息案[20]中，二审法院认为“单独的……姓名和手机号不构成隐私信息，但当姓名、手机号和……行程信息（隐私信息）结合在一起时，……整体上成为隐私信息”，在另一案件中，被公开披露“姓名、照片、住址、工作单位等身份信息”的原告以侵犯名誉权和隐私权为由起诉被告并得到法院支持。[21]但是，由于中国法律体系下“隐私”概念的内涵相对较为固定，在运用隐私权乃至于肖像权、姓名权、名誉权等具体人格权保护“个人信息”权益时仍然可能存在力有不逮的情形。例如，有学者[22]在分析隐私与个人信息时认为，“隐私权制度设计”所保护的隐私利益属于“人格自由与人格尊严方面的人格利益”；但个人信息除了“人格尊严和自由价值”，还具备“商业价值”[23]和“公共管理价值”[24]，而后两者也是个人信息被“不当收集、处理、利用和传输”的重要诱因，但却较难通过隐私权体系进行保护。举例而言，如果自然人已经主动披露“隐私信息”，由于信息私密性已经被自然人的行为主动放弃，则很难在之后再主张隐私权遭到侵犯；但此时对于已经公开的个人信息的不当利用，仍然可能损害相应自然人的权益。

因此，随着司法实践经验的不断累积和学术讨论的不断深入，区分个人信息与隐私权的边界逐渐成为中国学术界和立法者们的共识。[25]2017年颁布生效的《民法总则》在第一百一十条“隐私”等人格权之外明确提出了“个人信息”保护，[26]从立法层面确定了个人信息保护与隐私权的二分体制。而从本次《民法典》的体系结构中不难看出，关于隐私权和个人信息保护的具体内容虽然共同规定在“人格权编”的第六章，两者在条款文本上仍然相对独立，[27]例如第一千零三十三条中规定“除法律另有规定或者权利人明确同意外”，任何组织或个人不得以列明的或其他方式侵害他人的隐私权；而第一千零三十五条中处理个人信息的条件之一则为“征得该自然人或者其监护人同意”。尽管“明确同意”的内涵与外延尚未完全明确，但从文义表述来看其与“同意”应有不同，该“明确同意”是否更接近于个人信息的“明示同意”[28]的标准则可能还有待进一步探讨。

---

[17] 与“个人信息控制者”的概念相对，此处“个人信息处理者”是指开展个人信息处理行为，但可能无权决定个人信息处理的目的和方式的组织或个人。

[18] 李慧琪. 民法典编纂专家：建议设立独立的个人信息保护机构[EB/OL]. https://mp.weixin.qq.com/s/1Z3R91ZWlPuniMbJ3qBg0Q. 转引自：微信公众号“网络法实物圈”. 发布日期：2020年5月19日，最后访问日期：2020年6月4日.

[19] 李永军. 论《民法总则》中个人隐私与信息的“二元制”保护及请求权基础[J].浙江工商大学学报, 2017(03):10-21.

[20] 庞理鹏与北京趣拿信息技术有限公司等隐私权纠纷案，[2017]京01民终字509号。

[21] 王某与张某、北京凌云互动信息技术有限公司、海南天涯在线网络科技有限公司侵犯名誉权纠纷系列案，[2008]朝民初字第29276号。

[22] 张新宝. 从隐私到个人信息：利益再衡量的理论与制度安排[J].中国法学, 2015(03):38-59.

[23] 即个人信息在定向营销、数据库营销、信用经济等商业模式中有着重要意义，已经成为“重要生产要素、无形资产和社会财富”。引自：张新宝. 从隐私到个人信息：利益再衡量的理论与制度安排[J]. 中国法学, 2015(03):38-59.

[24] 即收集和利用个人信息同时也是“实施社会管理和提供公共服务”的普遍做法。引自：张新宝. 从隐私到个人信息:利益再衡量的理论与制度安排[J]. 中国法学, 2015(03):38-59.

[25] 参见王利明. 论个人信息权的法律保护：以个人信息权与隐私权的界分为中心[J]. 现代法学, 2013(04):62-72. 张新宝. 从隐私到个人信息：利益再衡量的理论与制度安排[J]. 中国法学, 2015(3): 38-59.

[26]《民法总则》第一百一十一条。

[27] 即第一千零三十二条和第一千零三十三条规定了隐私权的范围及隐私权侵权行为；第一千零三十四条至第一千零三十九条则包含了个人信息的定义、个人信息主体的受保护权益及信息处理者的义务与责任等内容。

[28] 即“个人信息主体通过书面、口头等方式主动做出纸质或电子形式的声明，或者自主做出肯定性动作，对其个人信息进行特定处理作出明确授权的行为”。

从侵权的责任承担角度来看，《民法典》第一千零三十三条中规定的“处理他人的私密信息”构成侵犯他人隐私权和第一千零三十四条第三款中的规定“个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定”一方面是立法者面对隐私权与个人信息保护之间体系衔接的处理方式之一，体现了对隐私权与个人信息“客体交错性”和“侵害后果竞合性”的肯定和立法回应。即从客体而言，“自然人……不愿为他人知晓的私密信息”既应当属于隐私，[29]也可能属于个人信息。[30]而从侵害后果而言，“行为人实施某一行为可能同时造成对多种权利的侵害，从而形成多种权利受侵害、产生责任竞合的现象”[31]。从这个角度来看，“个人信息中的私密信息，适用有关隐私权的规定”所规范的含义可以理解为行为人实施以私密信息为客体的行为造成侵权时，如出现竞合应当以隐私侵权责任为先。另一方面也可以被视为从个人信息权益角度对于不适用于隐私权的个人信息侵害行为提供补充的救济措施，为个人信息主体提供了更为全面的保护和救济。

（四）侵犯个人信息的民事救济

1. 侵权责任

通常如果未能为保护的权益提供充分的救济措施，“权利”容易变成“一纸空文”。《民法典》中关于个人信息保护的另一个重点即是个人信息权益侵害的救济措施和责任承担问题。《民法典》中“人格权编规定的人格权请求权和侵权责任编中的侵权赔偿责任等救济方式”[32]均能够适用于个人信息保护。《民法典》“总则”第一百二十条中规定，“民事权益受到侵害的，被侵权人有权请求侵权人承担侵权责任”。

同时“人格权编”第九百九十五条中进一步规定了，“人格权受到侵害的，受害人有权依照本法和其他法律的规定请求行为人承担民事责任。受害人的停止侵害、排除妨碍、消除危险、消除影响、恢复名誉、赔礼道歉请求权，不适用诉讼时效的规定”，个人信息保护是否适用于人格权完整的救济措施还有待确认。但《民法典》中对于涉及个人信息权益保护方面，则体现为：

（1）请求信息处理者采取更正等必要措施或及时删除个人信息（比如备受争议的信用评价）；[33]

（2）信息处理者发生个人信息安全事件时应及时采取补救措施；[34]

（3）医疗机构泄露患者隐私、个人信息或未经同意公开病历资料的侵权责任[35]等内容。

这些将在实质上为个人信息主体提供充分的保障，让权益得到真正的落实与践行。

2. 免责事由

在请求权基础和侵权责任之外，对“免责事由”的探讨则有助于我们更全面地理解个人信息的责任体系。其中，《民法典》“人格权编”第九百九十九条中规定，“为公共利益实施新闻报道、舆论监督等行为的，可以合理使用民事主体的姓名、名称、肖像、个人信息等”；而第一千零三十六条中规定了处理个人信息的行为人无需承担民事责任的三种情形，即“（一）在该自然人或者其监护人同意的范围内合理实施的行为；（二）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，但是该自然人明确拒绝或者处理该信息侵害其重大利益的除外；（三）为维护公共利益或者该自然人合法权益，合理实施的其他行为”。从文义表述来看，不难发现二者可能稍有不同，其中第九百九十九条所规定的为“可以合理使用……个人信息”；而第一千零三十六条的表述则是“无需承担民事责任”。

鉴于《民法典》中所规定的一般原则为民事权益受到侵害，被侵权人有权请求侵权人承担侵权责任，我们理解行为人无需承担侵权责任的可能性有两种：

（1）其一是行为人的行为并未侵害权利人的民事权益，因此自然没有请求承担侵权责任的基础；

（2）其二则是行为人的行为可能导致权利人的民事权益受损，但出于利益平衡以及其他考虑构成了免责事由，即行为人无需承担民事责任。

对于第九百九十九条中和第一千零三十六条中所规定的“可以合理使用……个人信息”和“无需承担民事责任”具体应当属于何种情形，可能会影响未来司法实践中的举证责任分配和实践中判定标准的高低，因此可能有待于进一步明确。

3. 其他责任

除侵权责任外，《民法典》第一百七十六条中还规定了“民

[29]《民法典》第一千零三十二条第二款：隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。

[30]《民法典》第一千零三十四条：个人信息是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特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等（第一款）。个人信息中的私密信息……（第二款）。

[31] 王利明. 论个人信息权的法律保护：以个人信息权与隐私权的界分为中心[J]. 现代法学, 2013(04):62-72.

[32] 李慧琪. 民法典编纂专家：建议设立独立的个人信息保护机构[EB/OL]. https://mp.weixin.qq.com/s/1Z3R91ZWlPuniMbJ3qBg0Q. 转引自：微信公众号“网络法实物圈”. 发布日期：2020年5月19日，最后访问日期：2020年6月4日.

[33]《民法典》第一千零三十七条；《民法典》第一千零二十九条。

[34]《民法典》第一千零三十八条。

[35]《民法典》第一千二百二十六条。

事主体依照法律规定或者按照当事人约定，履行民事义务，承担民事责任”。第五百七十七条中进一步规定，“当事人一方不履行合同义务或者履行合同义务不符合约定的，应当承担继续履行、采取补救措施或者赔偿损失等违约责任”。就个人信息的保护而言，行为人的行为除了因侵害合法人格权益而可能需要承担侵权责任外，是否可能因违反了《隐私政策》或其他告知文本中的个人信息处理方式而构成未履行与个人信息主体的约定，并相应需要承担违约责任，可能也是未来值得关注的议题。

三、《民法典》的深远影响：个人信息保护的新时代

（一）数据的“蛮荒时代”成为历史

《民法典》的颁布，对个人信息的人格属性及其保护规则进行了私法层面的确认和重申。虽然在具体规则上，《民法典》基本上沿袭和承继了现行规范下对信息处理者的行为规制，但无论是个人信息的民事权益和人格属性定位，还是将其与隐私权的内容进行界分，均很大程度上表明立法者从私法视角为个人信息的保护再次“正名”的意图。自此，对于个人信息的保护，将不再仅局限于《网安法》以及《刑法》等公法层面的处罚和制裁，个人信息主体为保障自身个人信息权益而直接向违约或侵权行为人主张私法上的救济已不存在法律依据上的障碍。这进一步向产业发出了信号：数据“原始积累”的“蛮荒时代”将成为历史，个人信息的全方位法律保护时代已经来临。对于企业而言，以合法、合规的姿态迎接个人信息保护的新时代，才能够为自身业务的拓展、促进产业可持续发展构建坚固的堡垒。

（二）个人信息保护民事诉讼将成趋势

随着人们的个人信息保护意识不断增强，在可预见的未来，个人通过提起侵犯个人信息的民事诉讼实现个人信息权益救济将成为一大趋势。同时，侵犯公民个人信息的行为往往涉及较大规模的自然人群体，个人信息保护的公益诉讼将可能成为未来我国民事公益诉讼领域的又一大亮点。事实上，司法实践已开始个人信息保护公益诉讼的尝试。例如2019年底山东菏泽市牡丹区检察院针对侵犯公民个人信息的行为提起了全省首例刑事附带民事公益诉讼，在公民个人信息保护领域对公益诉讼的适用情形进行了有益探索；[36]今年3月，安徽利辛县检察院提起的刑事附带民事公益诉讼也进入了实体审理的阶段。[37]在美国、欧洲等地，提起或参与个人信息和隐私保护的集体诉讼已成为公民实现权利救济的常规途径。随着我国公益诉讼制度的不断健全，公民个人通过公益诉讼方式参与到个人信息权益保障的救济程序中将不再是难题。这也进一步预示着未来侵犯个人信息的行为将面临越来越高的违法成本，事前的合规调查工作对于企业有效控制业务风险而言显得愈发重要。

（三）数据精细化、资产化管理的时代已经到来

如前所述，《民法典》从私法角度进一步提升了个人信息保护的高度，对于企业而言，对个人信息主体权益的尊重与保障不仅是个人信息收集利用阶段必须履行的法定义务，也将成为未来内部数据管理和商业模式创新的必要前提。一方面，企业收集或处理的数据往往种类繁多，来源不一，不同类型和来源的数据必然存在安全保障上的不同层次的需求。为此，从数据自身属性出发，探求不同性质数据在法律上的不同保护定位，以数据分类、分级等方式对不同类型的数据风险级别进行识别，实现数据的精细化管理，将成为企业有效控制合规风险、构建整体数据资产管理框架的前提基础和必备工作，另一方面，这也能够为通过数据打通融合等模式挖掘企业内部数据价值的工作提供必要的合规前提，进一步帮助企业实现数据作为生产要素的最大价值，构建有效的数据资产化管理体系。

四、未来已来：个人信息保护的思考与展望

从《民法典》对于个人信息的性质和定位来看，其尝试建立的个人信息保护制度以个人主体权益保障为导向和基本逻辑。随着数据产业的发展，企业的数据资产化战略日益深入，我们不得不进一步思考：除了个人信息主体的人格利益应当受到保护以外，个人信息之上是否还存在其他值得保护的利益？对于这些利益的保护应当如何兼顾?

当下理论及实务界已有不少针对个人信息特点和属性的深入讨论。除了强调以私权为核心实现和保障自然人对于个人信息的自我管理和自由支配外，[38]也有不少论者注意到了个人信息具备的经济价值，从而产生了诸多对于个人信息“财产性利益”及其归属的讨论。有观点认为，如从个人信息主体角度探讨其对于个

[36] 全省首例！侵犯公民个人信息，牡丹区检察院提起刑事附带民事公益诉讼，https://k.sina.com.cn/article_2620088113_9c2b5f3102000qpbx.html?from=news&subch=onews

[37] 亳州首例！侵犯公民个人信息，利辛县检察院提起刑事附带民事公益诉讼，http://www.ahlixin.jcy.gov.cn/jcyw/202003/t20200313_2791495.shtml

[38] 参见王利明. 论个人信息权的法律保护：以个人信息权与隐私权的界分为中心[J]. 现代法学, 2013(04):62-72.

人信息享有的权利，保护的并非是自然人对于其个人信息享有某种经济利益，而是自然人对其个人信息被他人收集、存储、转让和使用的过程中的自主决定的利益。[39]这一观点与现行法律法规下个人信息保护制度相衔接，包括《民法典》、《网安法》在内的个人信息保护规范均从个人信息主体知情、同意的角度建立他人收集、使用、处理个人信息的合法性基础。然而，站在产业发展的视角反观现有规则，我们发现，仅仅通过行为规制的手段对个人信息的收集、处理行为进行合规性限制似乎并不足够——对于个人信息保护的合规要求似乎无法完全解决产业实践在个人信息乃至数据利用的现实需求。

在大数据产业蓬勃发展的今天，我们无法忽视个人信息所蕴含的巨大经济价值。当个人的上网行为被完整地留存和记录，这些在虚拟空间留下的个人痕迹蕴含了大量丰富的信息内容。运用数据分析技术，这些网上的记录将很容易地展现个人的兴趣爱好、浏览习惯、消费偏好，甚至能够反映个人的性别、年龄、职业、身份等。这种具有丰富信息含量和指示意义的数据信息，大大便利了企业的商业变现能力。例如，企业可以通过对个人信息进行统计分析，实现不同人群的消费偏好和习惯的标签化，从而进行精准营销、产品设计或提升服务，为企业创造实际的收益。数据规模的不断积累和数据类型的不断丰富，还进一步促进了数据产业的兴起和发展。在基于数据分析的各类服务场景中，例如程序化广告、舆情分析等等，数据正在进一步发挥其现实的经济价值。从这一角度看，企业在提供产品、服务的过程中收集、处理个人信息，其动机很难摆脱对个人信息所蕴含经济价值的重视。

而另一方面，当数据发展成为推动经济发展的生产要素，法律如果仅从个人信息的人格权属性角度展开个人信息收集、使用的行为规制，似乎略显单薄。因为在该阶段，谁掌握了数据要素，谁就可能在产业发展中占据优势。当市场主体前赴后继地涌向数据高地，争相占有数据资源，彼此之间难免会产生诸多数据资源归属的纠纷争议。而如果数据要素的权属规则仍旧缺位的话，将可能导致企业之间有关数据获取与使用权益的边界划定缺乏明确的规则指引，企业付出大量人力、物力、财力形成的数据资产也难以得到有效保障。

实际上，这些纠纷争议在过往的司法案例中屡见不鲜。无论是此前的“新浪v脉脉”案，[40]“谷米科技vs元光科技”纠纷案，[41]还是近期因“微信数据”引发的数据权益纠纷[42]等，均或多或少地涉及包括个人信息在内各类数据的权益归属问题，而法院从反不正当竞争角度出发，对企业就数据资源享有的竞争性利益做出明确表态，甚至认为数据资源构成一种无形财产权益受到保护。囿于对数据权属无明确法律规定，这一保护目前尚停留在司法这一最后防线，也仅局限于反不正当竞争法层面的兜底性保护，这一定程度上反映了现有的个人信息及数据保护规则在解决数据权益纠纷方面发挥作用的有限性。未来随着大数据产业的发展，有关数据权益的争议与纠纷必将愈演愈烈，如何通过法律规则的设计对数据的权益归属进行合理的分配，实现民法“定分止争”的具体要义，同时又能在数字经济产业政策背景下促进大数据行业的有序、健康发展，将成为未来数据领域立法不得不考虑的重要议题。

总之，《民法典》强调个人信息包含的人格利益，有助于大数据时代个人信息主体的权益保障，**但我们希望指出的是，人格利益保障不应是个人信息保护的全部。未来的个人信息保护立法应考虑为个人信息经济利益和价值实现留出空间。**一方面，这至少与其他人格权，如姓名权、肖像权的保护逻辑相一致，也与《民法典》人格权的一般规定相协调。虽然《民法典》九百九十二条明确规定人格权不得放弃、转让或继承，但恰如《民法典》第九百九十三条规定所规定的，民事主体可以将自己的姓名、名称、肖像等许可他人使用。这恰恰是出于对个人姓名、肖像所包含的经济利益和其商业变现能力的肯定。

而另一方面，《民法典》对于个人信息保护在人格权视角上的侧重，也并不意味着对于企业数据权益的否定。既往的司法实践已经对企业就数据享有财产性权益进行了积极的回应，未来随着数据产业发展日趋成熟，企业对于个人信息及数据资源的权属要求也将越来越强烈。我们同样也看到，《民法典》第一百二十七条也为数据、网络虚拟财产的保护留出了空间。立足于产业政策视角，我们期待着未来立法从个人信息和数据的经济价值出发，对这些“无形资产”的定位和权属进行一定的界分，从而更好地促进数据产业的良性、健康发展。

（本文发布于2020年06月10日。）

[39] 见程啸：论大数据时代的个人数据权利[J]，中国社会科学，2018(3):102-122。

[40] 见北京知识产权法院（2016）京73民终588号民事判决书。

[41] 见广东省深圳市中级人民法院（2017）粤03民初822号民事判决书。

[42] “微信数据”引发数据权益之争 群控软件被判赔260万元，杭州互联网法院宣判首例涉微信数据权益认定不正当竞争案，见浙江法院网：http://ssfw.zjsfgkw.cn/art/2020/6/4/art_56_20847.html

“欲穷千里目，更上一层楼”
——《个人信息安全规范》最新修订要点评述

引言

自2019年2月，全国信息安全标准化技术委员会（**“信安标委”**）首次发布《信息安全技术 个人信息安全规范（草案）》，历时逾1年，历经6月及10月两版《信息安全技术 个人信息安全规范》（征求意见稿）（分别称为**“6月征求意见稿”**、**“10月征求意见稿”**），推荐性国家标准GB/T 35273-2017《信息安全技术 个人信息安全规范》（**“现行《规范》”**）修订工作于2020年3月6日完成。新版标准GB/T 35273-2020《信息安全技术 个人信息安全规范》（**“新版《规范》”**）于当日正式发布，并将自2020年10月1日起正式生效，以代替现行《规范》。

相比于现行《规范》，新版《规范》在内容上有较大变化，除了授权同意例外[1]、账户注销[2]、责任部门与人员[3]、个人信息处理活动记录[4]、实现个人信息主体自主意愿的方法[5]等内容的修改外，还新增了多项业务功能的自主选择[6]、用户画像[7]、个性化展示[8]、基于不同业务目的的信息汇聚融合[9]、第三方接入管理[10]、个人信息安全工程[11]等相关要求。新版《规范》在总结国内外执法监管实践经验的基础之上，体现了对技术发展、商业模式创新下个人信息保护新型问题的关注，为个人信息主体的权利保障与企业个人信息保护的合规实践提供参考。

有鉴于此，我们对现行《规范》、10月征求意见稿及新版《规范》进行文本比对，并从中选取几项重要变化，就其内容及所反映的个人信息保护与利用的新趋势与大家共同探讨。

一、部分重点修改内容评析与新趋势探讨

本章节以文本对比的方式呈现本次新发布的《个人信息安全规范》的三大重点修改内容，并由此总结个人信息保护领域的变化与趋势，进而为企业的个人信息保护合规工作提供方向性建议。

---

[1] 参见新版《规范》5.6。

[2] 参见新版《规范》8.5。

[3] 参见新版《规范》10.1。

[4] 参见新版《规范》11.3。

[5] 参见新版《规范》附录C。

[6] 参见新版《规范》5.3。

[7] 参见新版《规范》7.4。

[8] 参见新版《规范》7.5。

[9] 参见新版《规范》7.6。

[10] 参见新版《规范》9.7。

[11] 参见新版《规范》11.2。

（一）对个人生物识别信息保护提出优化要求

现行《规范》	10月征求意见稿	新版《规范》
（一）个人生物识别信息的收集		
无	无	**5.4 收集个人信息时的授权同意** c）收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意； 注：个人生物识别信息包括个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等。
（二）个人生物识别信息的存储		
6.3 个人敏感信息的传输和存储 对个人信息控制者的要求包括： b）存储个人生物识别信息时，应采用技术措施处理后再进行存储，例如**仅存储个人生物识别信息的摘要。**	**6.3 个人敏感信息的传输和存储** 对个人信息控制者的要求包括： b）存储个人生物识别信息时，应采用技术措施确保信息安全后再进行存储，例如将个人生物识别信息的原始信息和摘要**分开存储，或仅收集、存储、使用摘要信息。**	**6.3 个人敏感信息的传输和存储** 对个人信息控制者的要求包括： b）个人生物识别信息应与个人身份信息**分开存储；** c）**原则上不应存储原始个人生物识别信息**（如样本、图像等），可采取的措施包括但不限于： 1）**仅存储个人生物识别信息的摘要信息；** 2）在**采集终端中直接使用**个人生物识别信息实现身份识别、认证等功能； 3）在使用面部识别特征、指纹、掌纹、虹膜等**实现识别身份、认证等功能后删除**可提取个人生物识别信息的**原始图像。** 注1：**摘要信息**通常具有**不可逆**特点，无法回溯到原始信息。 注2：个人信息控制者履行法律法规规定的义务相关的情形除外。
（三）个人生物识别信息的共享		
无	无	**9.2 个人信息共享、转让** i）个人生物识别信息**原则上不应共享、转让。因业务需要，确需共享、转让的，**应**单独**向个人信息主体告知目的、涉及的个人生物识别信息类型、数据接收方的具体身份和数据安全能力等，并征得个人信息主体的明示同意。

新版《规范》在现行区分个人信息和个人敏感信息的保护框架之内，新增并强调对个人生物识别信息在收集、存储、共享三大环节的保护要求，对近年来各行业日益频繁及普遍的对个人生物识别信息利用进行更全面的监督与管理，从而响应大数据发展潮流下日益突出的新型个人信息保护问题，进一步提升对个人信息主体的信息保护水平。

基于以上表格总结，在内容修改方面，我们可以看出：

- **个人生物识别信息收集方面：**新版《规范》对个人信息控制者提出了“单独告知”及“取得明示同意”的双重要求，相较于现行《规范》及10月征求意见稿中已有的对收集个人敏感信息时应当确保获得个人信息主体的明示同意的要求更为严格。
- **个人生物识别信息存储方面：**不难看出，在《个人信息安全规范》沿革过程中，对个人生物识别信息的保护要求始于信息存储环节。现行《规范》已在“个人敏感信息的传输和存储”章节提出了对个人生物识别信息存储的特殊技术处理要求，并建议个人

信息控制者仅存储“个人生物识别信息的摘要”；10月征求意见稿在个人生物识别信息存储之前的技术处理要求方面，新增了“将原始信息和摘要信息分开存储”的建议，为企业提供了多项技术参考，而新版《规范》则将前述规范版本中的“分开存储”建议上升为具体要求，明确提出了“不应存储原始生物识别信息”的原则，并列举了包括仅存储摘要信息、在采集终端直接使用、识别认证身份后删除原始图像在内的具体实现方式以供企业参考。

具体而言，“在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能”及“识别认证身份后删除原始图像”的两条可选路径可能意味着企业可以将原始个人生物信息存储于采集终端，但限制其将原始个人生物识别信息上传至企业服务器进行身份认证以外的后续使用，这可能会对部分企业运营及产品模式产生重大影响。其次，就实践中企业进行身份识别与验证的一般情况来看，很多企业可能会将认证成功的证件照片长期存储，并用于后续相同客户的身份验证。但在新版《规范》的要求之下，该验证后的证件照片是否属于可提取个人生物识别信息的原始图像，企业能否于服务器中留存并调取使用等问题值得进一步探讨。同时，该等原则仅以“履行法律法规规定的义务”为例外，足可见标准制定者对个人生物识别信息存储的强监管态度。

我们理解，标准制定者对个人生物识别信息存储的严苛要求可能出于对个人生物识别信息本身的唯一性考虑。12原始个人生物识别信息作为自然人从出生以来即无条件拥有的信息素，具有天然的强人身附属性及私密性；相较于其他结合社会性特征的个人信息，其泄露可能会带来的对个人信息主体人身权，特别是人格权的侵犯与影响更为严重。13此外考虑到目前面部识别特征、虹膜、指纹等个人生物识别信息广泛用于个体身份验证以及财产支付等场景，个人生物识别信息与个人信息主体财产权的关联也愈发紧密。因此，从对个人生物识别信息的保护和使用程度的把控来看，新版《规范》意图将原始个人生物识别信息的使用范围与使用时段限于采集端，综合考虑了现实商业场景中身份验证等对原始个人生物识别信息的利用需求以及对个人信息主体人身权的保护，同时也为企业提供了储存摘要信息的路径，促使企业思考如何提高技术水平，转变商业模式，以便形成对个人生物识别信息合规利用的最佳路径。

- **个人生物识别信息共享方面：**个人生物识别信息以不共享、不转让为原则，确需共享、转让的，首先需要符合“业务需要”的必要性要求，其次，与上述个人生物识别信息收集的要求类似，新版《规范》针对个人生物识别信息的共享在原来个人敏感信息共享的“明示同意”及“额外告知内容”要求的基础之上额外提出了向个人信息主体“单独告知”的要求，同样体现了标准制定者对个人生物识别信息保护的重视。

同时，我们也注意到，针对个人生物识别信息在存储和共享方面体现“原则+例外”的标准制定理念，与欧盟《一般数据保护条例》第九条有关包括生物性识别数据在内特殊类型个人数据处理[14]及中国人民银行于2月13日发布的《个人金融信息保护技术规范》要求的“受理终端、个人终端及客户端应用软件均不应存储个人生物识别信息的样本数据、模板，仅可保存完成当前交易所必须的基本信息要素，并在完成交易后予以清除”[15]的思路保持一致。

随着人工智能技术的发展及社会信息变革，对个人生物识别信息的利用将会越发广泛，而随着应用场景的多样化，对个人信息主体保护的挑战也将逐渐升级。我们可以预见，标准制定者将在不断深化对个人生物识别信息的保护的同时，进一步探索如何在商业应用强需求和个人权益保护之间实现基本平衡并推进企业在个人生物识别信息利用方面的合规良性发展。

基于上述对新版《规范》中个人生物识别信息优化要求的解析，我们建议企业：

- 梳理现有业务中涉及个人生物识别信息收集与共享的场景，在正式开启个人生物识别信息采集功能或进行个人生物识别信息共享之前，设置单独的个人生物识别信息采集或共享声明呈现界面或跳转链接；
- 相关声明应依据不同功能场景下的采集或共享目的，列明对应的信息采集、使用规则；
- 对于涉及多次采集或共享个人生物识别信息，宜通过弹窗或跳转声明页面或链接的方式再次向个人信息主体进行告知，并取得个人信息主体的明示同意；
- 原则上不存储原始个人生物识别信息，可根据业务模式，选择仅存储摘要信息、在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能或在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像等。

---

[12] 参见程啸：《加强个人生物识别信息法律保护》，载https://baijiahao.baidu.com/s?id=1654775537833936974&wfr=spider&for=pc，2020年1月4日。

[13] 参见《生物识别信息保护：“你”真的是你吗？》，载https://zhuanlan.zhihu.com/p/32647279，2018年1月8日。

[14] Art. 9 GDPR Processing of special categories of personal data. https://gdpr-info.eu/art-9-gdpr/.

[15] 《个人金融信息保护技术规范》（JR/T 0171—2020）第6.1.3 d）条。

（二）增强个人信息主体对个人信息的管理能力

现行《规范》	10月征求意见稿	新版《规范》
（一）保障个人信息主体自主选择		
无	5.3 不强迫接收多项业务功能 当产品或服务提供多项需收集个人信息的业务功能时，个人信息控制者不应违背个人信息主体的自主意愿，强迫个人信息主体接受产品或服务所提供的业务功能及相应的个人信息收集请求。对个人信息控制者的要求包括： a) 不应通过捆绑产品或服务各项业务功能的方式，要求个人信息主体一次性接受并授权同意其未申请或使用的业务功能收集个人信息的请求。 b) 应把个人信息主体自主作出的肯定性动作，如主动点击、勾选、填写等，作为产品或服务的特定业务功能的开启条件。个人信息控制者应仅在个人信息主体开启该业务功能后，开始收集个人信息； c) 关闭或退出业务功能的途径或方式应与个人信息主体选择使用业务功能的途径或方式同样方便。个人信息主体选择关闭或退出特定业务功能后，个人信息控制者应停止该业务功能的个人信息收集活动； d) 个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应频繁征求个人信息主体的授权同意； e) 个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应暂停个人信息主体自主选择使用的其他业务功能，或降低其他业务功能的服务质量； f) 不应以改善服务质量、提升个人信息主体体验、研发新产品、增强安全性等为由，强迫要求个人信息主体同意收集个人信息。	5.3 多项业务功能的自主选择 当产品或服务提供多项需收集个人信息的业务功能时，个人信息控制者不应违背个人信息主体的自主意愿，强迫个人信息主体接受产品或服务所提供的业务功能及相应的个人信息收集请求。对个人信息控制者的要求包括： a) 不应通过捆绑产品或服务各项业务功能的方式，要求个人信息主体一次性接受并授权同意其未申请或使用的业务功能收集个人信息的请求； b) 应把个人信息主体自主作出的肯定性动作，如主动点击、勾选、填写等，作为产品或服务的特定业务功能的开启条件。个人信息控制者应仅在个人信息主体开启该业务功能后，开始收集个人信息； c) 关闭或退出业务功能的途径或方式应与个人信息主体选择使用业务功能的途径或方式同样方便。个人信息主体选择关闭或退出特定业务功能后，个人信息控制者应停止该业务功能的个人信息收集活动； d) 个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应频繁征求个人信息主体的授权同意； e) 个人信息主体不授权同意使用、关闭或退出特定业务功能的，不应暂停个人信息主体自主选择使用的其他业务功能，或降低其他业务功能的服务质量； f) 不得仅以改善服务质量、提升使用体验、研发新产品、增强安全性等为由，强制要求个人信息主体同意收集个人信息。
附录C 保障个人信息主体选择同意权的方法 内容主要包括征求同意的实现方法，提供了功能模板交互式界面的设计。	附录C 实现个人信息主体自主意愿的方法 1）区分基本业务功能与扩展业务功能，分别提出了实现告知同意的方法 2）提供交互式功能界面设计以供参考	附录C 实现个人信息主体自主意愿的方法 1）区分基本业务功能与扩展业务功能，分别提出了实现告知同意的方法 2）提供交互式功能界面设计以供参考
（二）个人权利保护		
7. 个人信息的使用 7.4 个人信息访问 7.5 个人信息更正 7.6 个人信息删除 7.7 个人信息主体撤回同意 7.9 个人信息主体注销账户 7.10 个人信息主体获取个人信息副本 7.11 响应个人信息主体的请求 7.12 申诉管理	7. 个人信息的使用 7.8 个人信息访问 7.9 个人信息更正 7.10 个人信息删除 7.11 个人信息主体撤回**授权**同意 7.12 个人信息主体注销账户 7.13 个人信息主体获取个人信息副本 7.14 响应个人信息主体的请求 7.15 申诉管理	8. 个人信息主体的权利 8.1 个人信息访问 8.2 个人信息更正 8.3 个人信息删除 8.4 个人信息主体撤回授权同意 8.5 个人信息主体注销账户 8.6 个人信息主体获取个人信息副本 8.7 响应个人信息主体的请求 8.8 **投诉**管理

现行《规范》	10月征求意见稿	新版《规范》
（二）个人权利保护		
7.9 个人信息主体注销账户 对个人信息控制者的要求包括： a) 通过注册账户提供服务的个人信息控制者，应向个人信息主体提供注销账户的方法，且该方法应简便易操作； b) 个人信息主体注销账户后，应删除其个人信息或做匿名化处理。	7.12 个人信息主体注销账户 对个人信息控制者的要求包括： a) 通过注册账户提供服务的个人信息控制者，应向个人信息主体提供注销账户的方法，且该方法应简便易操作； **b) 宜直接设置便捷的注销功能交互式页面，及时响应个人信息主体注销请求；** **c) 受理注销账号请求后，需要人工处理的，应在承诺时限内（原则上不超过十五天）完成核查和处理；** **d) 注销过程进行身份核验需要个人信息主体重新提供的个人信息不应多于注册、使用等服务环节收集的个人信息；** **e) 注销过程不应设置不合理的条件或提出额外要求增加个人信息主体义务，如注销单个账户视同注销多个产品或服务，要求个人信息主体填写精确的历史操作记录作为必要注销条件等；** **f) 注销账户的过程需收集个人敏感信息核验身份时，应明确对收集个人敏感信息后的处理措施，如达成目的后立即删除或匿名化处理等；** g) 个人信息主体注销账户后，应**及时**删除其个人信息或做匿名化处理。 **注：因法律规定需要留存的个人信息应妥善保管，不能将其再次应用于业务场景。**	8.5 个人信息主体注销账户 对个人信息控制者的要求包括： a) 通过注册账户提供产品或服务的个人信息控制者，应向个人信息主体提供注销账户的方法，且方法简便易操作； ~~宜直接设置便捷的注销功能交互式页面，及时响应个人信息主体注销请求；~~ **b) 受理注销账户请求后，需要人工处理的，应在承诺时限内（不超过15个工作日）完成核查和处理；** **c) 注销过程如需进行身份核验，要求个人信息主体再次提供的个人信息类型不应多于注册、使用等服务环节收集的个人信息类型；** **d) 注销过程不应设置不合理的条件或提出额外要求增加个人信息主体义务，如注销单个账户视同注销多个产品或服务，要求个人信息主体填写精确的历史操作记录作为注销的必要条件等；** **注 1：多个产品或服务之间存在必要业务关联关系的，例如，一旦注销某个产品或服务的账户，将会导致其他产品或服务的必要业务功能无法实现或者服务质量明显下降的，需向个人信息主体进行详细说明。** **注2：产品或服务没有独立的账户体系的，可采取对该产品或服务账号以外其他个人信息进行删除，并切断账户体系与产品或服务的关联等措施实现注销。** e) 注销账户的过程需收集个人敏感信息核验身份时，应明确对收集个人敏感信息后的处理措施，如达成目的后立即删除或匿名化处理等； g) 个人信息主体注销账户后，应**及时**删除其个人信息或匿名化处理。**因法律法规定需要留存个人信息的，不能再次将其用于日常业务活动中。**

首先，从个人信息主体自主选择的角度，新版《规范》承继了10月征求意见稿中新增的“不强迫接受多种业务功能”以及“区分业务功能，提出实现个人信息主体自主意愿的方法”的内容。其中“不应通过捆绑产品或服务各项业务功能的方式，要求个人信息主体一次性接受并授权同意其未申请或使用的业务功能收集个人信息的请求”等要求，对于某些集团企业的个人信息保护政策体系的合规性，特别是采用集团统一个人信息保护政策文本的情形，可能会产生影响，企业可能需要考虑重新评估现存个人信息保护政策体系并进行优化。

其次，就具体个人信息主体权利响应而言，相较于现行《规范》与10月征求意见稿中将个人信息主体权利响应要求划归为“个人信息使用”章节之下的做法，新版《规范》将个人信息主体权利响应单独成章，从整体结构上对标准体系进行了规整，也凸显了标准制定者对个人信息主体权利保护的关注。值得注意的是，新版《规范》在10月征求意见稿已对个人信息注销权增添具体要求的基础之上，又针对企业“无独立账户体系，注销单个账号等同注销多个产品或服务”的情况，提供了合规解决方案，以期达到不影响企业其他业务功能正常运作及维护消费者体验的双重效果。

在网络产品和服务不断升级与更迭的今天，相关个人信息的利用方式也越发的复杂。个人信息主体一方面享受着多样化服务带来的多重多效体验，另一方面也面临着个人权利被侵害的风险，如何切实保障个人信息主体的自决权与决策的透明性，进而逐步实现数据权利本身向个人信息主体的让渡，成为了标准制定

者关注的重点之一，而从最本源的授权同意有效性出发，对新业态下自主决定权的保障及常规个人信息权利响应的维护，增强个人信息主体对个人信息的管理能力，是实现数据权利让渡的基础要求（注：有关个人信息主体对用户画像的自主管理的分析内容请见要点三）。在实践中，我们也不乏看到，如谷歌、百度、OPPO等公司已就注册用户全览及自主管理个人信息提供了Dashboard工具，详尽列明了用户在使用服务过程中的授权情况及存储的详细个人信息，并相应地赋予了用户利用工具行使对留存的个人信息增删改查的权利，[16]以更好地应对向个人信息主体进行数据权利让渡的潮流与趋势。同时，在《个人信息安全规范》修订的过程中，我们也注意到了标准制定者对企业的正常业务运营的考虑，从规范角度出发，为企业提供合规路径，化解可能的业务困局。随着网络服务与产品的升级与商业模式的转变，我们可以预见，标准制定者也将针对新产品新服务提供过程中产生的个人信息主体权利的全新问题及可能的企业发展困境提出更进一步的解决思路。

基于上述总结的新版《规范》对增强个人信息主体管理个人信息能力的要求，我们建议企业：

- 除了通过《个人信息保护政策》或声明等授权文本的方式确保获取个人信息主体的授权同意，保障个人信息自主意愿之外，在具体业务功能设计过程中，避免为取得授权而对个人信息主体进行骚扰；同时，在产品设计环节通过交互界面优化，保障关闭相应服务功能的便捷性；
- 结合集团型业务开展的具体情形，包括不同业务之间的运营主体、业务关联性等情况，在综合评估基础上对相应个人信息保护政策体系进行优化；
- 设置便捷的注销账户方法，不设置以注销为由收集多于服务环节所需的个人信息等障碍，在承诺时间内及时响应个人信息主体的主要要求，并在设计环节通过对内部数据管理系统的优化与调整，确保用户注销后的有效数据及时删除、匿名化或至少从生产系统内的移出；
- 若多个产品或服务之间存在必要业务关联关系，而注销某个产品或服务的账户，会导致其他产品或服务的必要业务功能无法实现或者服务质量明显下降的，向个人信息主体进行详细说明；
- 在企业已建立大账号体系且针对单个产品或服务设置独立账号的情况之下，可采取对该产品或服务账号以外其他个人信息进行删除，并切断账户体系与产品或服务的关联等措施实现注销；
- 在收集环节对法律法规规定需要留存的数据予以识别，以便在个人信息主体注销账户之后，对其他没有法定留存要求的数据，及时删除或做匿名化处理；而对有法定留存要求的数据，则妥善保管，但不得将其再次用于日常业务活动中，以便最大限度地保证企业经营运行的合法合规；
- 可考虑建立专门的隐私保护平台，设置用户自主管理个人信息的简易方式。

（三）数据融合的合规实践

现行《规范》	10月征求意见稿	新版《规范》
基于不同业务目的所收集的个人信息的汇聚融合		
无	7.6 基于不同业务目的所收集的个人信息的汇聚融合 对个人信息控制者的要求包括： a) 遵守本标准7.3的要求； b) 根据汇聚融合后个人信息所用于的目的，开展个人信息安全影响评估，采取有效的个人信息保护措施。	7.6 基于不同业务目的所收集的个人信息的汇聚融合 对个人信息控制者的要求包括： a) 应遵守本标准7.3的要求； b) 应根据汇聚融合后个人信息所用于的目的，开展个人信息安全影响评估，采取有效的个人信息保护措施。

[16] Google Dashboard: see at https://myaccount.google.com/dashboard?hl=en.

相较于现行《规范》，新版《规范》中增加了对基于不同业务目的所收集的个人信息的汇聚融合的合规监管要求。具体而言，企业在汇聚融合基于不同业务目的所收集的个人信息时，需要遵守个人信息使用目的限制的相关要求，不能超范围使用个人信息；同时还需要根据汇聚融合后的目的，开展个人信息安全影响评估，采取有效的个人信息保护措施。

大数据时代，数据的聚合使用在数据价值挖掘和创新方面的作用已经不言而喻。“通过对海量沉淀的个人信息的二次或多次使用，大数据可以发现隐藏在这些孤立的数据背后的商业价值与公共性价值。”[17]企业能够通过对基于内部不同业务目的所收集的个人信息、以及从第三方间接获取的个人信息等进行汇聚融合，实现数据的验真与价值提纯，提升单位数据价值密度；个人信息汇聚融合后形成的用户画像、特征标签等还可能用于评价个人信用状况、推送商业广告或其他个性化展示内容。但是个人信息的汇聚融合同样可能存在超出个人信息主体授权范围使用个人信息、消费者歧视等风险；在个人信息汇聚融合过程中，还可能因个人信息控制的移转或共享而引发信息安全担忧。

从个人信息主体权利保护来看，新版《规范》第7.6条的规定，有效地保障了主体在个人信息汇聚融合中的知情权与自决权，防范企业对个人信息的超范围使用；同时个人信息安全影响评估与个人信息保护措施的要求也能够在一定程度上降低信息泄露、转卖或滥用的风险。而对企业而言，如何合规地实现内部不同业务条线所收集的个人信息的汇聚融合，充分挖掘数据的价值则尤为重要。根据新版《规范》的相关要求，企业可能需要：

- 通过个人信息保护政策、其他独立文本、弹窗等形式对汇聚融合不同业务条线中的个人信息的目的、方式、范围等向个人信息主体进行充分的告知并在超出原有授权同意范围时另行征得个人信息主体的同意；
- 根据要求相应开展个人信息安全影响评估并采取个人信息保护措施。

同时，数据融合并不仅限于企业内部自有数据的融合，企业还可能通过与第三方的合作，通过数据转让共享实现内外部数据融合或采用隐私保护、密文计算等方法在“保障数据所有权基础上实现数据的融合应用”[18]……需要提示的是，数据融合是一项复杂的系统性工程，除上述要求外，还可能涉及：

- 更多个人信息保护与行业监管限制。如对于以转让共享为前提的内外部数据融合，在转让共享时可能还需要满足《个人信息安全规范》中个人信息转让、共享的相关要求。个人金融信息还需要满足《个人金融信息技术保护规范》中对共享、转让的信息类型及数据接收方资质的要求等；
- 数据融合必要性基础的建立。具体而言，《网络安全法》第四十一条规定了数据处理的必要性原则；现行《规范》中将其进一步解释为（1）个人信息收集的直接关联、最低频率和最少数量要求；（2）个人信息存储的必需最短时间和超期删除及匿名化等；因此，企业可能需要通过商业模式的搭建建立数据融合的必要性基础；
- 不同主体之间的权利义务分配。包括数据源提供方、数据融合技术供应方、数据融合商业化变现的应用主体等多方主体之间的权利义务关系的确认和利益分配机制的设计等；
- 数据资产及其他类型资产的移转。

总体而言，数据融合已经成为企业挖掘数据价值的重要方式，但同时也面临着相应的监管与合规风险，无论是内部不同业务条线的数据汇聚融合、还是内外部数据的融合，需要在厘清风险的前提下实现合规的数据融合实践，才能助力企业的长远发展（更多有关数据融合的探讨可参见**《“数”年快乐——万字长文说数据融合》**一文）。

[17] 许可：《破解个人信息收集使用“必要原则”困局》，载https://www.secrss.com/articles/11820, 2019年7月1日。

[18]《李伟：做好数据治理，更快更好地推进数字化转型》，载http://www.xinhuanet.com/fortune/2019-12/02/c_1125298138.htm，2019年12月2日。

（四）数据商业化的合规监管

现行《规范》	10月征求意见稿	新版《规范》
（一）用户画像的使用限制		
无	7.4 用户画像的使用限制 对个人信息控制者的要求包括： a) 用户画像中对个人信息主体的特征描述，不应： 1) 包含淫秽、色情、赌博、迷信、恐怖、暴力的内容； 2) 表达对民族、种族、宗教、残疾、疾病歧视的内容。 b) 在业务运营或对外业务合作中使用用户画像的，不应： 1) 侵害保护公民、法人和其他组织的合法权益； 2) 危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序。 c) 除为达到个人信息主体授权同意的使用目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人。例如，为准确评价个人信用状况，可使用直接用户画像，而用于推送商业广告目的时，则宜使用间接用户画像。	7.4 用户画像的使用限制 对个人信息控制者的要求包括： a) 用户画像中对个人信息主体的特征描述，不应： 1) 包含淫秽、色情、赌博、迷信、恐怖、暴力的内容； 2) 表达对民族、种族、宗教、残疾、疾病歧视的内容。 b) 在业务运营或对外业务合作中使用用户画像的，不应： 1) 侵害公民、法人和其他组织的合法权益； 2) 危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序。 c) 除为实现个人信息主体授权同意的使用目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人。例如，为准确评价个人信用状况，可使用直接用户画像，而用于推送商业广告目的时，则宜使用间接用户画像。
（二）个性化展示的使用		
无	7.5 个性化展示的使用 对个人信息控制者的要求包括： a) 在向个人信息主体提供业务功能的过程中使用个性化展示的，应显著区分个性化展示的内容和非个性化展示的内容； 注：显著区分的方式包括但不限于：标明“定推”等字样，或通过不同的栏目、版块、页面分别展示等。 b) 在向个人信息主体提供电子商务服务的过程中，根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的个性化展示的，应当同时向该消费者提供不针对其个人特征的选项； 注：基于个人信息主体所选择的特定位置进行展示、搜索结果排序，且不因个人信息主体身份不同展示不一样的内容和搜索结果排序，则属于不针对其个人特征的选项。 c) 在向个人信息主体推送新闻信息服务的过程中使用个性化展示的，应： 1) 为个人信息主体提供简单直观的退出或关闭个性化展示模式的选项； 2) 当个人信息主体选择退出或关闭个性化展示模式时，向个人信息主体提供删除或匿名化定向推送活动所基于的个人信息的选项。 d) 在向个人信息主体提供业务功能的过程中使用个性化展示的，宜建立个人信息主体对个性化展示所依赖的个人信息（如标签、画像维度等）的自主控制机制，保障个人信息主体调控个性化展示相关程度的能力。	7.5 个性化展示的使用 对个人信息控制者的要求包括： a) 在向个人信息主体提供业务功能的过程中使用个性化展示的，应显著区分个性化展示的内容和非个性化展示的内容； 注：显著区分的方式包括但不限于：标明“定推”等字样，或通过不同的栏目、版块、页面分别展示等。 b) 在向个人信息主体提供电子商务服务的过程中，根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的个性化展示的，应当同时向该消费者提供不针对其个人特征的选项； 注：基于个人信息主体所选择的特定**地理**位置进行展示、搜索结果排序，且不因个人信息主体身份不同展示不一样的内容和搜索结果排序，则属于不针对其个人特征的选项。 c) 在向个人信息主体推送新闻信息服务的过程中使用个性化展示的，应： 1）为个人信息主体提供简单直观的退出或关闭个性化展示模式的选项； 2) 当个人信息主体选择退出或关闭个性化展示模式时，向个人信息主体提供删除或匿名化定向推送活动所基于的个人信息的选项。 d) 在向个人信息主体提供业务功能的过程中使用个性化展示的，宜建立个人信息主体对个性化展示所依赖的个人信息（如标签、画像维度等）的自主控制机制，保障个人信息主体调控个性化展示相关性程度的能力。

除对企业数据融合的实践提出监管要求外，新版《规范》还进一步对用户画像的使用与个性化展示的数据商业化实践加以规范。包括但不限于用户画像的使用不得侵犯公民、法人和其他组织的权益或危害国家安全、荣誉和利益；在业务运营或对外合作过程中尽量避免使用直接用户画像；在业务过程中区分个性化展示和非个性化展示；提供退出个性化展示选项；保障或建议保障个人信息主体对用户画像或标签的自主控制等内容。

正如前文所言，通过个人信息收集、汇聚和分析[19]而形成的用户画像在信用评估、商品推荐和程序化广告等领域有着广泛的应用；大数据和人工智能技术的发展，也使得个性化展示的准确性大幅度提升，并显著提高了产品和服务提供者与用户之间的交互性。[20]但是另一方面，对用户画像和个性化展示的不当利用可能会引发对个人信息主体、国家与社会的危害；例如对个人信息主体知情权利的侵害；部分具有可直接识别性的用户画像的泄露导致对相应主体权益的损害；新闻的个性化展示可能导致信息茧房效应[21]的加剧；基于用户画像和个性化展示进行商品推荐时，可能损害消费者的平等权利等。

从个人信息主体权利保护来看，避免使用直接用户画像有助于降低画像泄露或滥用给个人信息主体造成的风险；个性化展示的区分体现了对个人信息主体知情权的尊重；关闭或退出个性化展示界面、删除个性化展示所依赖的用户画像、标签等选项体现了对主体权利自决的尊重与保障。而从企业角度来看：

- 用户画像作为数据商业化产品的一种，在交易与流通环节中可能受到一定程度的限制，企业在对外提供或使用用户画像时可能需要承担更高的合规义务；
- 企业可能需要选择合适的方式对个性化展示页面与服务进行标识，而对于某些以个性化展示为核心业务功能的企业，可能需要进一步调整自身的商业模式，如在个性化推荐算法系统之外，另行搭建非个人标签化的推荐体系，如单纯按照内容发布时间、社群用户点击总量决定内容顺序等；
- 新闻信息服务、电子商务服务提供商还需保障用户退出个性化展示服务的权利；新闻信息服务提供商还可能需要建立删除或匿名化用户标签、画像的选项；
- 以上内容可能要求相应企业在业务模式、数据管理系统、个人信息主体权利响应机制上进行相应的调整与更新。

结语

《个人信息安全规范》作为《网络安全法》下个人信息保护体系下的重要指引，一方面，为企业完善内部个人信息保护工作提出了具体的实践要求与合规建议，另一方面也为监督部门提供了执法管理的参考依据。历经多次修改，新版《规范》将于今年10月1日起生效实施，在内容上除通过业务功能选择、用户账号注销等规定的优化进一步加强对个人信息主体的权益保护要求外，还结合业界实践对个人生物识别信息、用户画像与个性化展示的应用、基于不同业务目的所收集个人信息的汇聚融合等提出了新的要求。新修订的内容一部分是结合当前企业对于个人信息收集使用的实践而做出的有针对性的要求或建议，“与时俱进”的规范个人信息收集及处理等行为，另一方面对数据融合、个人信息管理能力的新要求反映个人信息保护和利用的新趋势，对企业个人信息保护及利用升级到“2.0”阶段的重要指引。

在数字经济蓬勃发展的今天，如何合法合规地利用和保护重要的数据资源——个人信息将会是很长时间内全球企业关注的一个重要命题。企业的个人信息保护水平不仅是数字驱动经济发展的重要基础，还是企业的综合管理能力的体现。“欲穷千里目，更上一层楼”，企业只有立足于对于个人信息保护的更高要求，合规的发展个人信息利用能力，才能在全球数字经济浪潮中站稳脚跟，走得更远。

（本文发布于2020年03月09日。）

[19] 参见新版《规范》3.8。

[20] 参见谢幸、练建勋、刘政、王希廷、吴方照、王鸿伟、陈仲夏：《个性化推荐系统，必须关注的五大研究热点》，载https://www.msra.cn/zh-cn/news/executivebylines/tech-bylines-personalized-recommendation-system，2018年11月6日。

[21] 信息茧房即Information cocoons，由美国法学教授凯斯·R·桑德斯在《信息乌托邦——众人如何产生知识》一文中首次提出，即“在当今网络环境中,多种类型的海量信息在虚拟空间的聚集，不仅仅提供的是对于‘开放多远’化信息协作模式的‘承诺’，同时也提供了非常巨大的‘风险’。人们可以自由地分享与获取大量的信息，但是同时也可能使自己陷入‘回音室’（EchoChambers）之中，成为偏激错误和‘没道理的极端主义’的摇篮、这种在信息的传播过程中所表现出来的个人只‘听我们选择的东西和愉悦我们的东西的通讯领域’，从而‘作茧自缚’，将自己束缚于像蚕茧一般的‘茧房’之中的现象，”引自彭晓晓：《信息时代下的认知茧房——广告业界与学界的“信息茧房”探析》，2014年。

按图索骥
——图示移动APP个人信息保护的重点

背景

随着互联网技术的发展和手机、平板电脑等移动终端的普及，移动互联网应用（以下简称“APP”）俨然已经成为人们网络生活中最常见的工具，也是网络运营者获取个人信息最便利和常用的方式。APP与个人之间的紧密联系同时意味着它是最容易影响个人信息主体信息安全的领域之一。因此，对个人信息保护的关注在APP领域可以具象化为多项执法监管和专项整治活动的开展，以及与APP相关信息收集使用的指南、规范（包括草案和征求意见稿）的频繁发布。

表1—2019年有关APP的专项活动及相关的指南规范

序号	执法监管、专项整治活动/相关指南规范	发布机构	生效时间
1	《关于开展APP违法违规收集使用个人信息专项治理的公告》	中共中央网络安全和信息化委员会办公室，工业和信息化部，公安部，国家市场监督管理总局	2019/01/25
2	《APP违法违规收集使用个人信息自评估指南》	APP违法违规收集使用个人信息专项治理工作组	2019/03/01
3	《APP违法违规收集使用个人信息行为认定方法（征求意见稿）》	APP违法违规收集使用个人信息专项治理工作组	2019/05/05发布
4	《网络安全实践指南—移动互联网应用基本业务功能必要信息规范》	全国信息安全标准化技术委员会	2019/06/01
5	《电信和互联网行业提升网络数据安全保护能力专项行动方案》	工业和信息化部	2019/06/28
6	《信息安全技术 个人信息安全规范（征求意见稿）》（2019年10月版）	国家市场监督管理总局 中国国家标准化管理委员会	2019/10/22发布
7	《信息安全技术 移动互联网应用程序（APP）收集个人信息基本规范（草案）》	国家市场监督管理总局 中国国家标准化管理委员会	2019/10/24发布
8	《工业和信息化部关于开展APP侵害用户权益专项整治工作的通知》	工业和信息化部	2019/10/31

从APP个人信息保护为出发点，以下我们简要梳理了包括《信息安全技术 个人信息安全规范（征求意见稿）》（2019年10月版）在内，目前我国《网络安全法》下与个人信息保护相关的热点问题、主要监管规定以及专项治理活动中的主要关注点，以期为企业在面临多来源监管规定和执法环境下的个人信息保护合规工作提供参考和思路。

一、 隐私政策与授权同意

在各国的个人信息保护立法实践中，个人信息主体的同意始终是信息处理的重要合法性基础之一。其中隐私政策既是网络运营者向个人信息主体告知个人信息处理规则以获得明确授权的重要途径，也是监管机构评估网络运营者个人信息保护合规性、判断授权同意的有效性重点关注内容。结合2019年以来监管机构对APP收集使用个人信息的多次评估审查，我们对通过隐私政策获得个人信息主体的具体实践要点总结如下：

（一）《隐私政策》应当就哪些信息处理告知个人信息主体并获得授权同意？

序号	法律法规或规范性指导文件	相关内容
1	《中华人民共和国网络安全法》	第四十一条第一款 网络运营者**收集、使用个人信息**，应当遵循合法、正当、必要的原则，**公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意**。 第四十二条第一款 网络运营者……**未经被收集者同意，不得向他人提供个人信息**。
2	《信息安全技术 个人信息安全规范（征求意见稿）》（2019年10月版）	5.4 收集个人信息时的授权同意 对个人信息控制者的要求包括： a) 收集个人信息，应向个人信息主体告知**收集、使用个人信息的目的、方式和范围**，并获得个人信息主体的授权同意； 5.5 隐私政策 对个人信息控制者的要求包括： a) 应制定隐私政策，内容应包括但不限于： 2) 收集、使用个人信息的**业务功能，以及各业务功能分别收集的个人信息类型**。涉及个人敏感信息的，需明确标识或突出显示； 3) **个人信息收集方式**、存储期限、涉及数据出境情况等个人信息处理规则； 4) **对外共享、转让、公开披露个人信息的目的、涉及的个人信息类型、接收个人信息的第三方类型，以及各自的安全和法律责任**；
		8.2 个人信息共享、转让 个人信息控制者共享、转让个人信息时，……应符合以下要求： b）向个人信息主体告知**共享、转让个人信息的目的、数据接收方的类型以及可能产生的后果**，并事先征得个人信息主体的授权同意。
3	《APP违法违规收集使用个人信息自评估指南》	评估项2：清晰说明各项业务功能所收集个人信息类型（包括明示收集个人信息的业务功能、业务功能与所收集个人信息类型一一对应、明示各项业务功能所收集的个人信息类型）
		评估项3：清晰说明个人信息处理规则及用户权益保障（包括用于用户画像、个性化展示的场景和可能对用户的影响；共享、转让、公开披露的目的、个人信息类型和接收方类型）
		评估项5：收集个人信息应明示收集目的、方式、范围（包括使用Cookie及其同类技术收集个人信息的目的、类型、第三方代码、插件方式向第三方传输个人信息的场景）
4	《APP违法违规收集使用个人信息行为认定方法（征求意见稿）》	二、没有明示收集使用个人信息的目的、方式和范围的情形 2. 没有**逐一列出收集个人信息的类型、频率**，特别是针对个人敏感信息； 4. 在申请可收集个人信息的权限时，未**告知收集使用的目的**，如在申请调阅通讯录时没有说明原因； 5.每次要求用户提供个人敏感信息时，如身份证号、银行卡号等，未**同步实时说明原因**；

当数据控制者通过《隐私政策》完成告知并获取个人信息主体的授权同意时，可能需要在隐私政策中列明个人信息的收集规则、使用规则和共享、转让规则。[1]具体而言：

- 列明具体的功能场景，以及与功能场景一一对应的个人信息收集类型，收集和使用目的，其中提供个人敏感信息时需要同步实时说明原因；列明用Cookies及其同类技术收集个人信息的情形中所收集个人信息的目的和类型；
- 列明个人信息的其他使用情形，如用户画像、个性化展示等；
- 列明个人信息转让、共享的目的、涉及的个人信息类型、接收方，列明第三方代码嵌入、插件等方式将个人信息传输至第三方服务器的情形并通过弹窗提示进行明确告知；

对于个人敏感信息的采集，除隐私政策以外，在每次实时采集时，可能还需要通过口头或弹窗形式再次向数据主体说明原因。

（二）确保隐私政策文本的独立性、易读性

序号	法律法规或规范性指导文件	相关内容
1	《APP违法违规收集使用个人信息自评估指南》	评估项1：隐私政策的独立性、易读性（包括APP页面可查、单独成文、4次以内点击可访问、文本文字显示方式易于阅读） 评估项5：收集个人信息应明示收集目的、方式、范围（1、在用户安装、注册或首次开启APP时，应主动提醒用户阅读隐私政策。）
2	《APP违法违规收集使用个人信息行为认定方法（征求意见稿）》	一、没有公开收集使用规则的情形 1. 没有隐私政策、用户协议，或者隐私政策、用户协议中没有相关收集使用规则的内容； 2. 在APP安装、使用等过程中均未**通过弹窗、链接等方式提示用户阅读隐私政策，或隐私政策**链接无效、文本无法正常显示； 3. 进入APP主功能界面后，**多于4次点击、滑动才能访问**到隐私政策； 4.其他违反公开收集使用规则要求的情形。
3	《信息安全技术 移动互联网应用程序（APP）收集个人信息基本规范（草案）》	4. APP收集个人信息基本要求 b）APP 应**在首次运行时通过弹窗等明显方式**向个人信息主体告知收集最小必要信息规则，如隐私政策的核心内容。

当网络运营者尤其是APP运营商在提供隐私政策时，应当以明显方式呈现文本，同时保证隐私政策文本具有独立性、可读性。具体而言：

- 优化APP首次运行时的隐私政策呈现方式，如主动弹窗显示核心内容、或在注册并勾选同意前提供隐私政策文本链接；
- 优化隐私政策在APP内的布局位置，避免多次点击、滑动才能访问的设计；
- 确保隐私政策文本单独成文，并在用户未退出账号登陆的情况下依然能够方便查阅。

[1] 个人信息控制者是指有权决定个人信息处理目的、方式等的组织或个人。

（三）避免未经同意收集、使用、共享个人信息的情形

序号	法律法规或规范性指导文件	相关内容
1	《APP违法违规收集使用个人信息行为认定方法（征求意见稿）》	三、未经同意收集使用个人信息的情形 1. 未经同意就开始收集个人信息，如**APP首次运行、提示用户阅读隐私政策前就开始收集个人信息** …… 9.违背与用户约定，不按隐私政策中的收集使用规则收集使用个人信息；
2	《工业和信息化部关于开展APP侵害用户权益专项整治工作的通知》	（一）违规收集用户个人信息方面 1.“私自收集个人信息”。即**APP未明确告知收集使用个人信息的目的、方式和范围并获得用户同意前**，收集用户个人信息。 （二）违规使用用户个人信息方面 3.“私自共享给第三方”。即**APP未经用户同意与其他应用共享、使用用户个人信息**，如设备识别信息、商品浏览记录、搜索使用习惯、常用软件应用列表等。

网络运营者未经同意收集、使用、共享个人信息的情形，既包括由于隐私政策未能充分披露和告知而导致的“未经同意”，也包括在信息收集时尚未提示用户阅读隐私政策导致的“未经同意”。因此企业可能需要：

- 开展个人信息收集使用及共享的自查、总结并定期更新隐私政策，确保充分完整的披露和告知；
- 在合理范围内前置隐私政策首次出现的场景、使其尽可能多地覆盖后续的信息收集、使用和共享情形，同时核查信息采集尤其是自动化采集的时点、避免在APP提示用户阅读隐私政策前开始的个人信息收集行为；
- 对基于用户行为分析、产品优化目的与合作方共享设备识别信息、商品浏览记录等信息情况进行梳理，在隐私政策中予以明确披露。

二、 最小必要原则

序号	法律法规或规范性指导文件	相关内容
1	《中华人民共和国网络安全法》	**第四十一条** 网络运营者收集、使用个人信息，应当遵循合法、正当、必要原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。**网络运营者不得收集与其提供的服务无关的个人信息**，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。
2	《信息安全技术 移动互联网应用程序（APP）收集个人信息基本规范》	**第4条 APP收集个人信息基本要求；** **附录A 常用服务类型的最小必要信息。**
3	《信息安全技术 个人信息安全规范（征求意见稿）》（2019年10月版）	**第4 d)条** 最小必要——**只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时删除个人信息。**
4	《网络安全实践指南一移动互联网应用基本业务功能必要信息规范》	**第3.3条** 最少够用原则——**不收集与其提供服务无关的个人信息，不申请打开可收集无关个人信息的权限。只收集满足业务功能所必须的最少类型和数量的个人信息，自动收集个人信息的频率不超过业务功能实际所需的频率。**
5	《APP违法违规收集使用个人信息行为认定方法（征求意见稿）》	**第二条第1款 收集使用信息的目的违反合法、正当、必要原则，如仅仅以改善程序功能、提高用户体验、定向推送等为目的收集用户个人信息。** **第四条 违反必要性原则，收集与其提供的服务无关的个人信息的情形。**
6	《互联网个人信息安全保护指南》	**第6.1 b)条** 个人信息收集应获得个人信息主体的同意和授权，**不应收集与其提供的服务无关的个人信息**，不应通过捆绑产品或服务各项业务功能等方式强迫收集个人信息。

一方面， “最小必要原则”要求企业根据其提供服务的内容，明确为实现服务所需的、可收集的最小必要信息。在这方面，企业可能需要：

- 在进行业务或产品数据处理合规性评估时，考虑不采集某项个人信息或降低个人信息采集的精准度是否仍能实现业务和/或产品功能，若是，则可能不符合最小必要原则的要求；
- 若涉及自动化收集个人信息的场景，企业应注意控制自动化收集个人信息的范围、数量及频率，防止收集超过必要性的范畴；
- 因改善服务质量、提升个人信息主体体验、研发新产品不被单独视为基本业务功能，因此基于以上目的的数据采集需以其他基本业务功能数据采集的范围为限，尤其是为了优化算法目的而过度采集用户行为数据可能会受到数据采集最小化的挑战。

另一方面，企业还应当在满足用户授权同意目的之时及时删除相关个人信息。对于长期存储的个人信息而言需具有法律法规的明确依据，或者从用户角度建立个人信息存储的必要性并事先获取其授权同意。

三、 个性化展示

序号	法律法规或规范性指导文件	相关内容
1	《数据安全管理办法（征求意见稿）》	第二十三条 网络运营者利用用户数据和算法推送新闻信息、商业广告等，应当以明显方式标明“定推”字样，为用户提供停止接收定向推送信息的功能；用户选择停止接收定向推送信息时，应当停止推送，并删除已经收集的设备识别码等用户数据和个人信息。 网络运营者开展定向推送活动应遵守法律、行政法规，尊重社会公德、商业道德、公序良俗，诚实守信，严禁歧视、欺诈等行为。
2	《互联网个人信息安全保护指南》	6.3 c) 完全依靠自动化处理的用户画像技术应用于精准营销、搜索结果排序、个性化推送新闻、定向投放广告等增值应用，可事先不经用户明确授权，但应确保用户有反对或者拒绝的权利
3	《信息安全技术 个人信息安全规范（征求意见稿）》（2019年10月版）	对个人信息控制者的要求包括： a) 在向个人信息主体提供业务功能的过程中使用个性化展示的，应显著区分个性化展示的内容和非个性化展示的内容； b) 在向个人信息主体提供电子商务服务的过程中， 根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的个性化展示的，应当同时向该消费者提供不针对其个人特征的选项； c) 在向个人信息主体推送新闻信息服务的过程中使用个性化展示的， 应： 1) 为个人信息主体提供简单直观的退出或关闭个性化展示模式的选项； 2) 当个人信息主体选择退出或关闭个性化展示模式时，向个人信息主体提供删除或匿名化定向推送活动所基于的个人信息的选项。 d) 在向个人信息主体提供业务功能的过程中使用个性化展示的， 宜建立个人信息主体对个性化展示所依赖的个人信息（如标签、画像维度等）的自主控制机制，保障个人信息主体调控个性化展示相关程度的能力。
4	《APP违法违规收集使用个人信息自评估指南》	11. 个人信息的使用规则：如果APP运营者将个人信息用于用户画像、个性化展示等，隐私政策中应说明其应用场景和可能对用户产生的影响。
5	《工业和信息化部关于开展APP侵害用户权益专项整治工作的通知》	4.“强制用户使用定向推送功能”。即 APP 未向用户告知，或未以显著方式标示，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或精准营销，且未提供关闭该功能的选项。
6	《关于开展APP违法违规收集使用个人信息专项治理的公告》	倡导APP运营者在定向推送新闻、时政、广告时，为用户提供拒绝接收定向推送的选项。
7	《APP违法违规收集使用个人信息行为认定方法（征求意见稿）》	三、未经同意收集使用个人信息的情形 4. 利用用户信息和算法定向推送新闻、广告等，未提供终止定向推送的选项。

在现行生效的《个人信息安全规范》中，个性化展示的使用并没有设计独立的条款，但在今年发布的6月版和10月版《个人信息安全规范（征求意见稿）》以及近期的APP专项检查中，个性化展示和定向推送都成为了关注重点之一。从10月版征求意见稿来看，除了对业务功能中普遍使用个性化展示进行了规制，要求通过显著标识区分个性化展示和非个性化展示内容外，第7.5条个性化展示的使用还特殊提及了两类业务，即新闻信息服务和电子商务服务。其中，对新闻信息服务的特殊要求在某种程度上是对美国学者桑斯坦的“信息茧房”理论[2]的回应。而电子商务领域的特殊要求则是部分为了解决“大数据杀熟”[3]问题，同时也与《电子商务法》的要求相适应。[4]

长远来看，在个性化展示方面，企业可能需要：

- 向用户告知或以显著方式标示定向推送或精准营销的用途，同时提供关闭该功能的选项，尤其对于以定向内容推送为核心业务的企业而言可能还面临产品模式的调整；
- 在提供关闭个性化展示功能的基础上，企业还可能需要提供个人信息主体对标签、画像维度的信息的控制，并保障其可以选择对该部分数据删除或匿名化的权利。

四、 注销机制

序号	法律法规或规范性指导文件	相关内容
1	《信息安全技术 个人信息安全规范（征求意见稿）》（2019年10月版）	**第7.12条** 规定了对注销的**具体要求**，例如：提供注销账户的交互式界面、在承诺期限内处理注销请求、不得以注销为由额外收集个人信息并设置注销障碍、注销后及时删除或法定留存的，不得再次用于业务场景等
2	《数据安全管理办法（征求意见稿）》	**第二十一条** 网络运营者收到有关个人信息查询、更正、删除以及用户注销账号请求时，应当**在合理时间和代价范围内**予以查询、更正、删除或注销账号。
3	《APP违法违规收集使用个人信息行为认定方法（征求意见稿）》	**第六条** 规定了未按法律规定提供删除或更正个人信息功能的情形，例如未提供注销功能等
4	《APP违法违规收集使用个人信息自评估指南》	**评估项8 支持用户注销账号**、更正或删除个人信息：应提供注销途径，注销后及时删除个人信息或进行匿名化处理

在当前监管趋严的形势之下，我们建议企业：

- 设置便捷且用户友好的注销交互式界面，不设置如以注销为由收集多于服务环节所需的个人信息等障碍，并及时响应个人信息主体的注销请求
- 在收集环节对法律法规规定需要留存的数据予以识别，以便在个人信息主体注销账户之后，对其他没有法定留存要求的数据，及时删除或做匿名化处理；而对有法定留存要求的数据，则妥善保管，但不得将其再次用于业务场景等，以便最大限度地保证企业经营运行的合法合规。

---

[2] “在他看来，信息茧房意味着人们只听他们选择和愉悦他们的东西。尽管每个人都有自己的阅读偏好是正常的现象，但如果每个人关注的只是自己兴趣内的那一小片天地，他对这以外的世界，就会越来越缺乏了解。这或许不会影响到他个人的生活，但是，在需要公共对话的时候，人们会缺乏共同的 “视角”。而共同“视角”的缺乏，意味着人们对一些事实的判断会出现差异，共识难以形成。同时，信息环境的封闭与狭隘，也可能会进一步固化人们的某些观点与立场。”《一文了解AI时代的数据风险（后真相时代、算法囚徒和权利让渡）》，载https://mp.weixin.qq.com/s/-Y4JLCI-lq1P7io8BobGQg，2019年9月2日。

[3] “‘大数据杀熟’是利用大数据对老客户进行利益宰割。其技术原理是利用平台收集的海量用户信息和数据，生成用户画像。企业基于用户画像对用户进行精准识别和归类，开启个性化推荐，并通过向消费能力高、消费意愿强的用户展示更高的价格来赚取更多利润。”《“大数据杀熟”在线旅游“强监管”呼之欲出》，https://mp.weixin.qq.com/s?src=11&timestamp=1575003095&ver=2003&signature=Qm0lT1cx5wZ8YGY2UFcSgkxbY4fRYv9XClxtpC-bHwhlnCsn8v4HDsAaQAWbxD9lwlQuBSelnF7DoyFLRtBFcVOONw6Sm8fd7xXn1wd-a4XmRr7u7vi2tMZdrwzvnHVO&new=1，2019年11月25日。需要提示的是，有关“大数据杀熟”问题是否真实存在，仍然在探讨之中，但是我们理解，个性化展示和《电子商务法》的相关条款至少从效果层面可以理解为对社会公众热议的“大数据杀熟”问题给予了一定的回应。

[4] 《电子商务法》第十八条第一款规定，电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务的搜索结果的，应当同时向该消费者提供不针对其个人特征的选项，尊重和平等保护消费者合法权益。

五、 共同个人信息控制者的认定和管控

序号	法律法规或规范性指导文件	相关内容
1	《信息安全技术 个人信息安全规范（征求意见稿）》（2019年10月版）	**第8.6条** 对个人信息控制者的要求包括： a) 当个人信息控制者与第三方为共同个人信息控制者时，个人信息控制者应**通过合同等形式与第三方共同确定应满足的个人信息安全要求**，以及在个人信息安全方面自身和第三方应**分别承担的责任和义务,并向个人信息主体明确告知**。 b) 如**未向个人信息主体明确告知**第三方身份，以及在个人信息安全方面自身和第三方应分别承担的责任和义务，个人信息控制者**应承担因第三方引起的个人信息安全责任**。
2	《数据安全管理办法》（征求意见稿）	**第三十条** 网络运营者对接入其平台的第三方应用，应**明确数据安全要求和责任**，督促监督第三方应用运营者加强数据安全管理。**第三方应用发生数据安全事件对用户造成损失的，网络运营者应当承担部分或全部责任，除非网络运营者能够证明无过错。**

考虑到目前我国尚未有关于共同个人信息控制者的明确定义，参考欧盟GDPR的规定，共同个人信息控制者是指，能够共同决定数据处理目的和方式的两个或两个以上的控制者。[5]例如，APP运营商可能需要与第三方地图服务商合作、包括通过内置sdk代码或API接口等方式向第三方地图服务商传输数据以便获取用户的位置信息，以完成推荐或路线规划等服务，APP运营商与该第三方插件服务商共同决定用户位置信息处理的目的和方式，可能被认定为共同个人信息控制者。

具体而言，企业需从以下方面厘清与共同个人信息控制者的事实情况：

- 厘清与共同个人信息控制者数据交互中的数据流，包括但不限于其中是否包含个人信息、个人敏感信息、行业监管数据，以及数据交互的目的、方式等；
- 厘清与共同个人信息控制者交互的合作模式，如是通过线上或线下交互，通过SDK、API端口对接形式，或者报表、邮件形式等与第三方进行数据交互。

基于以上事实梳理，APP运营商需就与共同个人信息控制者的数据交互进行合法合规性评估，包括但不限于：是否以合同、承诺函等形式与共同个人信息控制者进行责任义务的合理分担；是否在隐私政策等文本中向个人信息主体告知共同个人信息控制者的身份及责任承担；是否知道并确认个人信息共享后的存储安全和进一步使用等情况。基于上述评估，企业最终需证明已审慎履行其对第三方/个人信息共同控制者的注意和监管义务，减轻在发生因第三方引起的数据安全事件时公司承担的责任。

结语

从以上的执法动态和规范指南中不难发现，监管部门对APP领域的关注已经从最初的隐私政策扩展到对APP权限获取、SDK使用、APP网络接口漏洞等多方面[6]的评估和关注，从基本的隐私政策文本内容深入到互联网移动终端的技术和商业模式的层面。

另一方面，APP本身的整改和进一步的规范要求只是个人信息保护的第一步，在可预期的未来，对个人信息保护的规范将继续向更深层次的技术内容和商业模式扩展，从爬虫技术到大数据商业模式、从人脸识别技术到人工智能领域，个人信息保护的规范制度将会随着监管部门对行业的深入了解和国内外个人信息保护动态的深入把握而不断深化。在个人信息保护进入深水区的情况下，企业更需要在深入了解自身个人信息保护实践和商业发展需求的基础上，紧跟个人信息保护发展动态和行业发展趋势、宏观与微观结合，在实现自身有序发展的同时不断提升合规水平，纵然面对 “乱花”般繁复的监管要求，依然能看清前行的路。

（本文发布于2019年11月29日。）

[5] 参见欧盟GDPR第26条。

[6] 2019年10月，中国信息通信研究院安全研究所发布了《2019金融行业移动App安全观测报告》，对13327款金融行业App的高危漏洞、恶意程序、SDK风险、违规索权、安全加固等五个方面展开评估。《App违法违规收集使用个人信息行为认定方法（征求意见稿）》中对App客户端嵌入第三方代码、插件（如sdk）等情形进行了规制。

星光奉献给长夜
——儿童个人信息保护的亮点和启示

谈到儿童，大家脑海里可能出现的仍然是“儿童急走追黄蝶”或者“蓬头稚子学垂纶”等与世隔绝的印象，但在数字时代，儿童早已通过网络与社会零距离接触。线上儿童教育、AI交互式玩具和线上游戏等网络产品和服务既让孩子们早早享受到网络的便利，同时也引发了家长们深深的担忧，如何在科技迅速发展的今天保护孩子们的童真？“白鸽奉献给蓝天，星光奉献给长夜”，在成人都逐渐无所适从的数据时代，家长们略显无力的自问“我拿什么奉献给你，我的小孩”？

儿童的网络生活无可避免，我们便需要从多维度来思考如何保护儿童网络生活中的合法权益。国家互联网信息办公室（以下简称“**网信办**”）政策法规局曾特别有心地在2019年5月31日下午6点01分发布《儿童个人信息网络保护规定（征求意见稿）》（以下简称“**《征求意见稿》**”）（请见文章《<儿童个人信息网络保护规定（征求意见稿）>要点评析》）。短短两个多月后，网信办于2019年8月23日正式发布了《儿童个人信息网络保护规定》（以下简称“**《规定》**”），从个人信息保护和儿童权益两个维度正式确定了儿童个人信息网络保护的原则和框架。《规定》的颁布，不仅昭示着我国未成年人权益保护向网络空间的迈步，也是我国建立信息安全立法体系的一大重要举措。在个人信息保护专门法律缺位的背景下，《规定》中熠熠生辉的“星光”将有助于指明我国个人信息保护的方向。

一、《规定》概述

（一）第一部针对儿童的个人信息保护的专门立法

从立法形式上看，《规定》以国家网信办第4号令的形式颁布，并以《网络安全法》、《未成年人保护法》为上位法依据，既承继了《网络安全法》“为未成年人提供安全、健康的网络环境”、保护网络空间个人信息的原则性要求，也秉持了《未成年人保护法》对未成年人隐私及相关权益的关注与保护。作为我国第一部针对儿童的个人信息保护的专门立法，《规定》不仅具有立法领域上的综合性，更具有保护主体上的针对性。

（二）适用范围——线上与线下的“网络保护”

《规定》对适用范围也予以明确，即适用于通过网络从事收集、存储、使用、转移、披露儿童个人信息等活动。如我们此前针对《规定》征求意见稿的分析，从立法逻辑自恰的角度，《规定》中所述“网络”也会沿用《网络安全法》中的定义，即“由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统”。这意味着，实践操作中如企业在线下采集儿童个人信息，但此后如其所采集的儿童个人信息通过在线信息系统存储或进行其他处理的，同样可能构成“通过网络”处理儿童个人信息，进而适用《规定》。

（三）保护主体——正式明确“儿童”的定义

《规定》对于其所保护的权利主体——儿童的定义予以明确，是指不满十四周岁的未成年人（《规定》第二条）。这与我国此前颁布的一些规范性指引中对于儿童的界定相一致[1]。参考国外针对儿童个人信息保护的法规，可以看出，域外各司法辖区对

[1]《信息安全技术 个人信息安全规范》将14周岁以下儿童个人信息作为个人敏感信息予以特别保护。

于儿童个人信息权利主体的年龄认定各有不同，例如欧盟《通用个人数据保护条例》（“GDPR”）针对十六岁以下儿童使用特定的网络服务设置了特殊的“同意”机制，又如美国《儿童网络隐私保护法》（“COPPA”）将未满十三周岁的未成年人作为该法的具体保护对象。《规定》的这一界定充分考虑了不同年龄阶段未成年人的心智和认知能力，以及对自身行为后果的承受能力，同时也兼顾了网络运营者在个人信息保护注意义务上的合理限度，一定程度上也能够与我国《民法总则》规定的限制民事行为能力人民事法律行为效力的认定相自恰[2]。

（四）更详细的保护原则

相比于《网络安全法》中对于个人信息收集、使用的一般性原则（如合法、正当、必要的原则等），《规定》对于儿童个人信息保护也提出了更有针对性的原则要求，包括正当必要、知情同意、目的明确、安全保障、依法利用五大原则（《规定》第七条）。这一原则规定承继了《网络安全法》条文所明确的个人信息保护要求，构成《规定》中儿童个人信息保护各项细化条款的总领依据，为网络运营者对于儿童个人信息的保护工作提供了整体的方向性指引。此外，相较于此前发布的《征求意见稿》，《规定》还专门以禁止性规定明确任何组织和个人不得制作、发布、传播侵害儿童个人信息安全的信息，对《未成年人保护法》和《网络安全法》中为未成年人营造健康良好网络信息环境的保护宗旨予以重申[3]。

（五）多方一体的保护体系——监护人+互联网行业组织等

与成人个人信息保护的不同，儿童因其自身人生观和价值观仍处于发展和形成阶段，对于来自社会的危险和对其权利的侵害可能缺乏认知。除了加强对儿童自身的个人信息保护以外，更需要社会、企业、家庭和学校共同努力，共同呵护儿童个人信息的安全。因此，《规定》中对于儿童监护人（《规定》第五条）和互联网行业组织（《规定》第六条）也分别施加了教育引导儿童和加强行业儿童个人信息保护自律的要求，以期通过多方一体的保护体系，使得儿童个人信息的保护体系能够真正有效运转。

二、“特别的爱给特别的你”-儿童信息保护的特殊设置

《规定》在《网络安全法》个人信息保护一般条款的基础上，针对儿童这一特殊群体的个人信息保护设置了特别规则。这意味着网络运营者在此后的个人信息合规工作上，除进行常规的个人信息合规审查外，还应特别注意对儿童群体予以“特殊照顾”，主要体现在以下方面：

（一）设置儿童信息保护规则、用户协议和专人负责儿童个人信息网络保护的要求

首先，《规定》第八条要求网络运营者应当设置专门的儿童个人信息保护规则和用户协议。这意味着，网络运营者仅为网络产品或服务提供一份隐私政策或用户协议可能无法满足要求，还需针对儿童群体准备专门的个人信息保护文本和用户协议。相应的，这一要求也将引发企业未来在产品中如何适时向儿童群体展示专门的隐私政策和用户协议文本这一实践操作上的思考。例如，对于游戏产业的网络运营者而言，其用户群体通常包含较大规模的儿童群体。而游戏运营者通常不具备如教育、医疗等行业能够直面其服务对象的能力，对于儿童群体的识别需付出一定的核验成本，且可能无法达到百分之百的精确度。在不确定用户是否为儿童群体的情形下，如何向其精确展示适用于该群体的隐私政策和用户协议版本，同时又如何做到与此后针对不同群体的同意机制相挂钩，都是企业在未来实践操作上值得探索的问题。

《规定》第八条也要求网络运营者应指定专人负责儿童个人信息的保护工作。相对于此前《征求意见稿》提出的“设立个人信息保护专员或者指定专人负责儿童个人信息保护”，《规定》对于企业内部儿童个人信息保护的人员要求更为明确和直接。

（二）监护人的事先授权同意基本要求和实践难题

由于儿童对于可能存在的社会危险和对其个人权益的侵犯缺少认知，《规定》要求网络运营者在处理儿童个人信息之前获得其监护人的授权同意。具体而言，《规定》分别规定了以下网络运营者需首次或再次获得监护人的授权同意的情形：

- 网络运营者收集、使用、转移、披露儿童个人信息的

[2] 我国《民法总则》规定8周岁以上的未成年人为限制民事行为能力人，可以独立实施纯获利益的民事法律行为或者与其年龄、智力相适应的民事法律行为。

[3] 《未成年人保护法》第三十四条规定，禁止任何组织、个人制作或者向未成年人出售、出租或者以其他方式传播淫秽、暴力、凶杀、恐怖、赌博等毒害未成年人的图书、报刊、音像制品、电子出版物以及网络信息等。此外，《网络安全法》第十三条规定，国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

（《规定》第九条）；

- 告知事项发生实质性变化的（《规定》第十条）；
- 因业务需要，确需超出约定的目的、范围使用的（《规定》第十四条）。

获取监护人同意的儿童个人信息保护理念，与美国COPPA和欧盟GDPR趋同[4]。但是，监护人同意的模式也同样存在着难以落实和可能实质增加企业合规成本的问题：

- 对于面向普通公众提供产品和服务的网络运营者而言，其不具有识别儿童及其个人信息的动机。以手机产品为例，若要将注册账户的儿童识别出来，可能需要额外收集儿童的出生日期。对于企业而言，不但额外采集了个人敏感信息需要满足一系列相关安全保护的要求，而且也可能因为儿童故意填写错误的出生年月日期而导致企业的儿童个人信息保护机制难以实际落实。
- 尽管通过邮件或短信方式向监护人发送了通知，但仍难以确保监护人身份及授权同意的真实性。以游戏产品为例，首次下载并激活游戏软件的儿童可以填写错误的监护人联系方式，从而假扮监护人身份给予网络运营者对其数据处理的授权同意。

因此，以监护人授权同意为核心，美国COPPA和欧盟GDPR还通过调整儿童个人信息特殊保护的适用范围，设置监护人同意以外的其他补充机制以期实现保护儿童个人信息安全与避免过多增加企业合规成本之间的平衡，例如：

1. 面向普通公众、无法或无动机识别其用户中有儿童的运营者，可以不受儿童隐私保护专项法案的管辖

受COPPA管辖的运营者分为两类：（1）面向儿童的运营者；（2）面向一般大众的运营者实际知道（actual knowledge）其用户中有儿童或者其有意识地通过面向儿童的运营者收集信息。COPPA还通过举例的方式对于“实际知道”的认定标准进行了列举。例如，对于游戏行业而言，如何是专门针对儿童开发或者收到了父母的投诉，表明对其特定的儿童用户有明确认知。

明确这个分类对于企业进行合规管理有重要的现实意义，对于无法或无动机识别其用户中有儿童的运营者而言，其往往仅需要满足事后儿童信息保护合规的要求[5]。

2. 获得监护人同意的具体方式

目前我国对于获得监护人同意的具体方式尚没有明确的要求。为了有效保障监护人同意机制的落地实施，美国COPPA和欧盟GDPR分别对获得监护人同意的具体方式进行了高标准要求。但是另一方面，只要运营者采取了符合要求的验证措施，就被认为已尽到了合理义务。即使儿童通过虚假手段完成了验证，仍然可以被认为是有效的[6]。

3. 监护人同意的例外情形

之前《征求意见稿》中列举的明示同意的例外情况在正式《规定》中已经被删除。一方面，这是与《网络安全法》

[4] 美国COPPA要求，在收集、使用和披露儿童的任何个人信息前须直接通知（direct notice）其父母，并取得父母“可验证的同意”（verifiable parent consent）。此外，欧盟GDPR也要求，向年龄不满 16 周岁的儿童提供信息社会服务的过程中处理其个人数据的，只有或至少在获取了该儿童监护人的同意或授权的情况下才满足第六条将同意作为数据处理合法性依据的要求。

[5] 因此，在实践中，对于一般受众网站，大部分会在隐私政策中明确要求：我们的产品、网站和服务主要面向成人。儿童不得创建自己的用户帐号，因此我们不会在明知的情形下收集儿童的信息。如果我们发现自己收集了儿童的个人信息，则会设法尽快删除相关信息。

[6] 参见 16 CFR § 312.5 Parental consent。

有关个人信息处理均需获得数据主体授权同意保持一致；但是，另一方面，这也导致一些紧急情况、偶发且对儿童权益影响不大的数据处理情形，仍然面临需获得监护人的授权同意。美国COPPA和欧盟GDPR均列举了不经监护人同意而直接获取儿童个人信息的场景，如在符合一定条件的情况下，运营者可以收集Cookie等永久标识；[7]或者在直接向儿童提供预防或咨询服务时，不必取得儿童监护人的同意[8]。

我国未来对于儿童个人信息的保护是否会借鉴境外立法的经验，例如对于企业专门面向儿童提供服务的认定标准、监护人授权同意的例外情形等，仍然值得关注。

（三）明确信息存储的要求

在儿童个人信息的存储安全上，《规定》明确要求网络运营者应当采取加密等措施存储儿童个人信息。对比《网络安全法》规定网络运营者应当采取技术措施和其他必要措施确保其收集的个人信息安全，可以看出，《规定》对于技术措施做了进一步明确，将采取加密措施作为确保儿童个人信息存储安全的强制性要求。这一要求与《信息安全技术 个人信息安全规范》（“**《安全规范》**”）中对于个人敏感信息的存储要求保持一致。这一规定也将可能对企业未来的个人信息存储策略产生一定影响。企业可从商业需求及成本控制的角度，基于《规定》对儿童个人信息存储安全的强制性要求，对于儿童个人信息与一般个人信息选择不同的存储方案，如混同存储还是隔离存储等。

（四）第三方交互儿童个人信息的要求

《规定》第十六条、第十七条是对网络运营者与第三方交互儿童个人信息场景下的特别规定。其中，第十六条规定了委托处理场景下，网络运营者应对受委托方及委托行为等进行安全评估外，还对委托协议的内容及对受托方义务提出了更加明确的要求。这些要求在总体方向上与《安全规范》中有关个人信息委托处理的规定保持一致，同时也针对儿童个人信息保护作出明确或特殊性规定，例如明确受托方应按照法律、行政法规的规定处理儿童个人信息，且不得转委托等。这意味着，对于从事数据处理服务的企业而言，其不仅需按照委托方的要求处理儿童个人信息，对于《规定》就儿童个人信息保护作出的特殊规定，也应当同样遵循，且不得再就委托方的委托处理事项转委托于他人。这显然对于数据处理者的注意义务和个人信息合规工作提出了更加明确和更高水平的要求。在未来的数据处理服务过程中，提供数据处理服务的企业应格外关注委托方提供的数据中是否可能包含儿童个人信息，并在委托协议的签署以及后续的处理服务中审慎待之。

此外，《规定》第十七条同时强调，网络运营者向第三方转移儿童个人信息的，应当自行或者委托第三方机构进行安全评估，将《安全规范》所要求的安全评估流程在儿童个人信息保护的场景下上升为强制性的义务。据此，安全评估将成为未来企业转移儿童个人信息的前提和必要条件，在进行相应的商业操作和安排前，企业也应适时注意，为安全评估留足充分的时间。

---

[7] 只有在同时满足以下两个条件的例外情况下，运营者不需要取得父母同意：（1）运营者除了永久标识外未收集儿童的任何其他个人信息；并且（2）运营者收集的永久标识仅为提供网站或网络服务的内部支持（internal operations）之用途，不用于任何其他目的。通过永久标识和儿童保持联系或者将永久标识披露给第三方，均属于用作了其他用途。参见16 CFR, §312.5 Parental consent，(c) Exceptions to prior parental consent。

[8] 参见GDPR的背景引言第38段。

（五）内部访问权限要求

《规定》第十五条从访问权限的角度明确了企业内部儿童个人信息的管控要求，即以“最小授权”为原则，为企业内部人员访问儿童个人信息设定严格的访问权限，控制儿童个人信息知悉范围。除技术上控制访问权限外，《规定》也要求企业从流程审批的角度对工作人员访问儿童个人信息予以控制，即应当经过儿童个人信息保护负责人或者其授权的管理人员审批，记录访问情况，并采取技术措施，避免违法复制、下载儿童个人信息。与《规定》在儿童个人信息存储要求上的规定类似，这一访问控制要求同样可能对企业未来个人信息的存储策略产生一定影响。一定程度上，将儿童个人信息有别于一般个人信息进行单独存储，或在个人信息混同存储情形下对儿童个人信息进行特殊的识别设置（如标签标记等），才可能在实践操作上与《规定》有关访问权限控制的要求相匹配。

（六）不得披露儿童个人信息的原则与例外

网络运营者被要求不得披露儿童个人信息，但法律、行政法规规定应当披露或者根据与儿童监护人的约定可以披露的除外（《规定》第十八条）。该条体现出对儿童个人信息的严格保护的同时也给予了合理的弹性。

（七）删除权的特别规定

对于儿童个人信息的删除出现在两个场景：（1）儿童或者其监护人要求网络运营者删除其收集、存储、使用、披露的儿童个人信息的，网络运营者应当及时采取措施予以删除，尤其是在网络运营和违法法律法规规定或双方约定、超出目的范围后者必要期限处理儿童个人信息、儿童监护人撤回同意的情况下（《规定》第二十条）；（2）停止运营产品或者服务的，应当立即停止收集儿童个人信息的活动，删除其持有的儿童个人信息，并将停止运营的通知及时告知儿童监护人（《规定》第二十三条）。

与普通个人信息删除的要求相比[9]，《规定》赋予了儿童监护人随时撤回同意的权利，可能造成企业儿童数据处理的不稳定性。此外，企业可能需要额外收集和保留儿童监护人的联系方式，以便在停止运营时及时告知儿童监护人。

三、企业合规建议与立法展望

我国大多数网络运营者已经采取了多种措施来加强个人信息保护工作，《规定》的出台则要求网络运营者针对儿童个人信息保护更有针对性的设置，比如：

- 针对儿童群体准备专门的个人信息保护文本和用户协议；
- 在企业内部为儿童群体匹配专门的个人信息保护人员；
- 在收集、使用和披露儿童的任何个人信息前设法取得监护人的同意；
- 采取合理措施保护已收集到的儿童个人信息的保密性、安全性和完整性，特别是在分享给第三方前需采取安全评估确保第三方的数据保护水平；
- 在相关目的实现或者监护人撤回同意后，设计数据删除机制，确保及时删除儿童信息。

《规定》的发布，明确了儿童个人信息保护的体系架构，作为继《民法总则》、《网络安全法》出台后的第一部针对个人信息保护的部门规章，更是对未来可能出台的《个人信息保护法》的要点和体例设计具有重要借鉴意义。

从儿童权益保护角度来看，全社会一直在推动儿童权益的保护，而在数据时代，个人信息作为主要的竞争资源，其收集和使用如何兼顾经济发展和儿童权益的保护是无法避免的难题。但我们依然相信大家对于“祖国的花朵”都心存善念，尽力为他们创造一个洁净、安全的成长环境，尽可能地让他们保留对世界最初真实、善良和美好的认知。

（本文发布于2019年08月26日。）

[9] 依据《网络安全法》第四十三条，个人发现网络运营者违反法律、行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息。

你的“饼干”安全吗？
——Cookie 与个人信息保护

摘要

Cookie追踪功能的日益强大引发了数字用户对其可能侵犯隐私、泄露个人信息的普遍担忧。Cookie为什么可能侵犯隐私，泄露个人信息？欧盟、美国和中国如何看待cookie相关的个人信息保护问题？企业又该如何合规地吃下这块“饼干”？

在格林童话《汉泽尔与格莱特》的世界中，小朋友通过在路上洒下小饼干屑的方式标记他们走过的路，最终走出了黑暗的森林。在数字世界中，网络运营者同样可以通过“cookie”追踪用户行为，记录并获取用户的访问信息[1]，实现统计网站访客数量、精准营销、记录用户喜好、操作等功能。这里的cookie是指用户浏览或访问网站时，各网站服务器在用户的本地设备（例如电脑、手机等）上安装和存储的小型文本文件，它通常包含有标识符、站点名称、号码和字符。

Cookie追踪功能的日益强大引发了数字用户对其可能侵犯隐私、泄露个人信息的普遍担忧。在隐私和个人信息保护越来越受重视的时代背景下，各国家/地区也越加重视对cookie的法律规制。那么，cookie为什么可能侵犯隐私，泄露个人信息？各主要司法辖区如何看待cookie相关的个人信息保护问题？相关的法律法规源起何方，又有何特点？在以下内容中，本文将首先介绍cookie的技术特征，在此基础上分别介绍欧盟、美国和中国的相关规制情况，并简要探讨相关合规建议，以飨读者。

一、此cookie非彼饼干也

就像口味不同的饼干一样，cookie根据各自的技术特点、用途和功能可以分为不同种类。

按照存储时间的长短，cookie可分为会话缓存（session cookie）和持久缓存（persistent cookie）。session cookie一般只在浏览器上短期保存，通常关闭浏览器时即被系统清除。这种cookie不会写入硬盘，通常也不收集有关用户的信息。持久缓存则写入硬盘并保存在设备中，下一次用户返回时，网站仍然可以对它进行调用，这也是我们中绝大多数人所熟悉的cookie。

按照网站主体的不同，cookie可以分为第一方缓存（first-party cookie）和第三方缓存（third-party cookie）。第一方缓存由用户访问的网站放置于用户终端设备，例如，当电商平台A设置一个cookie用来记录小明在购物车里放了十盒趣多多，即为第一方缓存。第三方缓存则是由与用户访问的网站以外的其他第三方放置在用户设备上的cookie，例如，假设广告营销公司答应帮助趣多多进行宣传推广，并与电商平台约定在其网站上放置广告，那么，当小明访问某电商平台时，广告网络会传送一个趣多多的广告到小明查看的页面，并在他电脑上放置一个cookie。

第三方缓存通常基于定向广告等目的放置，因此也被称为追踪缓存（tracking cookie）。在实践中，许多广告营销公司基于与广告商之间的合作，会与大量其他网站签约并向其提供广告，当小明访问这些网站时，广告营销公司可以再次调用此前小明访问电商平台A时放置的cookie，也就是说，广告营销公司可以在多个网站上追踪小明的行为。严格来讲，cookie只是本地设备上的临时存储文件，虽然这些文件可以通过简单的编辑器查看，但其本身无法从用户的设备收集数据。cookie也不是病毒，它无法在用户的设备上安装恶意软件。但cookie可能被网络运营者恶意地使用，沦为侵害他人权利的工具。

二、欧盟cookie规则的发展

作为数据保护领域的先驱与标杆，欧盟早在多年前从保护在线隐私的角度处发，针对cookie进行了专门的立法，并随着对数据保护和cookie的认识不断加深，不断完善和补充其规则体系。

（一）Cookie同意规则的出现和转变

1997年，欧盟针对电信领域个人数据处理中的隐私权保护问

[1] 例如用户的身份识别号码、密码、用户访问该站点的次数和时间、用户浏览页面的记录等。

题出台了《电信行业数据保护指令》（97/66/EC）[2]；2002年，欧盟颁布《电子隐私法令》（e-Privacy Directive）[3]，将适用范围扩展至覆盖互联网上的数据传输；其中规定，用户的电子通信终端设备上存储的任何信息均属于用户的隐私信息，应受到相关欧盟法律的保护。监测软件、网站信标、隐藏标示符及其他类似设备（例如cookie）可能会被放置在用户终端设备上，用以收集用户的信息。使用该等设备应仅限于合法目的并获得用户的知情同意[4]。

欧盟关于cookie的同意规则经历了从2002年e-Privacy Directive“选择退出（opt-out）”到2009年修订版e-Privacy Directive[5]“选择加入（opt-in）”的变化。2002年e-Privacy Directive只要求网站告知用户，并提供选择退出的机会，就可以在用户的终端设备上存储cookie[6]；2009年，欧盟对“e-Privacy Directive”进行了修订，在用户的终端设备上存储cookie不再能基于默认同意，而是从选择退出改为了选择加入，即，需要用户主动选择同意[7]。

（二）GDPR影响下的新进展

2016年公布、2018年实施的《欧盟通用数据保护条例（GDPR）》[8]明确特定类型cookie即构成个人数据。GDPR指出，网络设备、应用、工具、协议中留存的cookie痕迹如果具有唯一指向性，这些cookie痕迹可生成个人画像或档案从而识别到具体自然人，即具有身份识别性[9]。GDPR第26条前言说明，当数据可被用来直接或间接识别自然人时，其就是个人数据/信息。由此可见，GDPR明确了可以直接或与其他信息结合识别到特定自然人的cookie数据即为个人数据，受GDPR规制。

2017年1月，欧盟委员会提出了《隐私和电子通信条例》（Regulation on Privacy and Electronic Communications）[10]。该条例作为GDPR的特别法[11]，意欲取代当前的《电子隐私指令》，旨在规制电子通信服务并保护与用户终端设备相关的信息，使这一领域的立法要求与GDPR相协调。

E-Privacy Regulation针对cookie以及网站信标、图像像素等其他类似设备识别技术的使用提出了更为严格的规则。例如：

（1）只有在使用cookie是为用户提供服务所直接必需或者网站运营者已获得用户的同意的情况下，网站才能访问用户的手机或电脑等设备、收集设备类型、浏览器型号等信息。

也就是说，cookie的使用一般需要用户同意，但在一些特定情况下，不需要用户的同意，例如，在电子通信网络中传输信息所必要的、提供用户请求的信息社会服务所必要的、或是用于测量网页访问人数。具体而言，可能包括用于在一次会话中用户登录后识别用户的验证cookie、用于在一次会话中播放视频或音频内容而存储技术数据的多媒体播放器cookie、用于一次会话中存储语言或字体偏好的用户界面定制化cookie等。不过，即便这些cookie的使用无需获得用户同意，对用户就此进行告知仍然是一种推荐的做法。

（2）针对cookie的同意更难获取，因为该等同意必须符合GDPR中的相同标准，即必须有数据主体明确的肯定性确认行为。这意味着一些现有的做法需要重新审视，例如，仅展示标语，声明继续使用网站就构成同意可能将难以满足法律的要求。

在GDPR体系下，数据主体的同意必须是：

---

[2] Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector.

[3] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[4] Paragraphs 24 and 25 of 2002 E-Privacy Directive.

[5] DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.

[6] Article 5.3 of the 2002 E-Privacy Directive.

[7] Article 2(5) of the 2009 E-Privacy Directive.

[8] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[9] Paragraph 30 of the GDPR.

[10] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC.

[11]《欧盟<隐私与电子通信条例>草案评述》，曹建峰、李金磊，腾讯研究院。

- 自由作出；
- 具体；
- 在充分告知的基础上作出；以及
- 是数据主体不含糊的意思表示。

总体而言，在欧盟法律体系下，cookie由于具有特定个人识别性，被多部立法明确规定为个人数据，受到相应保护；在这一立场不变的前提下，随着数据保护法律制度的更新换代，cookie领域的特别立法亦不断完善和推进，从选择退出到选择加入的转变集中体现了欧盟对于规制cookie的严格态度。

三、美国：缺乏针对cookie的明确规定

美国在个人数据的保护方面的立法路径与欧盟不同，联邦层面没有专门针对个人信息保护的立法，相关的内容散见于行业规定以及州层面的立法。例如，规制健康医疗领域数据的《健康保险可携与责任法》（Health Insurance Portability and Accountability Act），保护儿童在线隐私的《儿童在线隐私保护法》（Children's Online Privacy Protection Act）等。这种倾向也影响到美国针对cookie的立法。一般而言，并没有法律明文规定禁止使用追踪缓存，联邦贸易委员会也不将追踪缓存的使用本身解读为不公平或欺诈行为。

目前，与cookie联系较为紧密的法律包括《联邦消费者欺诈与滥用法》（Federal Consumer Fraud and Abuse Act），其曾被用于基于行为广告目的使用cookie的公司。州层面例如加州也要求当使用cookie收集消费者在不同网站上的活动时，需进行相应的披露。不仅如此，《联邦贸易委员会法》（Federal Trade Commission Act）也被当作法律依据来管理/起诉不当披露其使用追踪缓存的行为。

自2011年起，美国出台了各种法案，但后来由于难以在建立标准和可行的立法方面达成一致，均以撤回或失败告终。其中，为了保护网上用户的隐私，让用户有权选择不被第三方网站跟踪，美国曾尝试引入“请勿追踪（Do Not Track）”立法。请勿追踪源自“Do Not Call”规则，依据该规则，电话推销员不能电话联系选择了退出的人。但是，目前多数网站均选择了无视请勿追踪请求，因此联邦贸易委员会意图推动的请勿追踪计划也成了一纸空文。

总体而言，美国对于cookie的使用采用的不是“选择加入”而是“选择退出”机制；其整体立法侧重的不是对使用cookie本身的规制，而是从保护用户权益不受损害的角度通过侵权等方面的法律进行管理。

四、中国：cookie是否属于个人信息？

Cookie是否属于个人信息的问题曾经经历了多年的讨论，随着《中华人民共和国网络安全法》（“《网安法》”）和国家标准《信息安全技术-个人信息安全规范》（“《个人信息安全规范》”）[12]的出台，cookie是否属于个人信息的判断有了较为明确的官方意见。

（一）Cookie同意规则的出现和转变

在国内司法实践中，对个性化推荐服务即定向广告cookie（追踪缓存）的性质认定存在认识上的分歧。2013年的“cookie第一案”反映了此种争议。原告诉称，其在使用百度搜索引擎搜索“减肥”“丰胸”等关键词并浏览相关内容后，在某些网站就会相应地出现与关键词高度相关的广告。原告认为百度公司未经其知情和选择，即记录和跟踪了所搜索的关键词，将其兴趣爱好等特点等显露在相关网站上，并对浏览的网页进行广告投放，侵害了其隐私权。

一审法院认定追踪缓存是个人隐私。二审法院认为其虽具有隐私性质，但不属于个人信息。其认为：网络用户通过使用搜索引擎形成的检索关键词记录，虽然反映了网络用户的网络活动轨迹及上网偏好，具有隐私属性，但这种网络活动轨迹及上网偏好一旦与网络用户身份相分离，便无法确定具体的信息归属主体，不再属于个人信息范畴。

在于“cookie”第一案的判断学术界存在很多的争论。二审法院认定，cookie与网络用户身份的分离使得cookie缺乏直接指定向个人的可能性，但更多的学者质疑，与cookie同步收集的信息包括服务的使用情况、IP地址、访问日期和时间、设备信息

[12] 由中国国家标准化管理委员会发布，为推荐性国家标准，不具有强制效力，但可作为企业合规的参照。

等，是否有可能与cookie相结合，能够指向特定用户。[13]

随着大数据技术的发展以及国际上对于“个人信息”认定标准的进一步深化讨论，《网安法》和《个人信息安全规范》对于cookie是否应该被认定为“个人信息”的问题提供了更为清晰的判断标准。

（二）《网安法》和《个人信息安全规范》对追踪缓存属性的再思考

2017年6月1日实施的《网安法》中对个人信息的定义即采取了直接识别和间接识别相结合的认定标准。[14]此外，2017年12月29日发布的《个人信息安全规范》进一步指出，判定某项信息是否属于个人信息，应考虑两条路径：

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。《个人信息安全规范》附录A将包括网站浏览记录、软件使用记录、点击记录在内的个人上网记录均列明为个人信息。《网安法》和《个人信息安全规范》对于个人信息的认定一定程度上参考了国际上普遍被认可的学说，同时也充分认可大数据关联分析技术能够通过结合多类数据提高指定特定个人的可能性。

如上所述，在当前的技术水平下，用户的网站浏览记录等追踪缓存信息与终端设备信息、账户信息等相结合即可很容易地识别到特定个人，可能会被认定为个人信息。在目前尚无针对cookie的特殊规则的情况下，对其进行收集、使用和任何处理，理论上均应遵守《网安法》及其他相关法律法规、国家标准对个人信息保护的一般要求。这些要求主要包括，应当在收集个人信息时征得用户的同意，并遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围。同时，不得泄露、篡改、毁损收集的个人信息；未经被收集者同意，不得向他人提供个人信息。此外，还应当采取技术措施和其他必要措施，确保收集的个人信息安全，防止信息泄露、毁损、丢失。

五、企业如何吃下这块“饼干”？

尽管各个国家对于cookie数据收集和使用等行为的规制可能有所不同，但在互联网企业全球化运营及数据全球流动的背景下，企业应结合中国和欧盟等主要司法辖区中国际通用的原则，对自己收集和使用cookie数据的行为进行自我检查和评估。具体而言，我们建议企业首先应当：

（一）考察cookie的使用情况和必要性分析

确认自身所使用的cookie种类、性质、第一方还是第三方、与用户其他信息关联度等特点，并据此逐一检查cookie的使用是否是实现某项功能所必须，是否一定需要用户同意，以及是否有任何非侵入的替代方案等。

（二）评估各类cookie对用户隐私的影响

虽然目前并未在法律规定层面明确需要将cookie进行进一步地分类，但从企业合规的角度出发，对用户行为介入越深入的cookie可能会对用户隐私造成更大的影响，从而给企业带来更大的合规风险，因此需要优先级更高的同意获取等合规措施安排。

（三）针对每一类cookie评估其所需要符合的“同意”要求

针对不同种类cookie，评估取得同意的不同要求。例如，第一方缓存的使用不需要获取数据主体的知情同意，但所有第三方缓存和持久缓存的使用均需获得数据主体的知情同意。[15]此外，还应针对每一类cookie评估合理的获取同意方式。例如，对于具有主页等主体交互页面的网站，采用弹窗等相应技术实现直接向用户要求同意的方式会较为有效；而对于一些注册界面为用户交互页面的网站，通过使用条款或隐私政策进行告知也不失为一种方式，尽管在进行更新时仍可能需要通过其他方式进行告知的补充，但也能极大地减少用户同意的成本。此外，对于一些cookie使用非常重要、具有持续性的网站而言，比如在线视频观看的网站，由于cookie对于用户行为的介入较深，使用目的包括个性化推荐等对用户体验造成影响可能较大，因此为用户提供cookie设置界面和按钮，甚至通过单独的跳转页面实现告知和用户同意，能够为网站提供更多的合规保障。

（四）将语言通俗化

以通俗易懂、不含晦涩技术术语的语言进行告知，在数据保护领域的立法中成为了一个越来越普遍的规则。由于用户的技术水平通常有限，过于复杂和技术化的表述将使得告知流于形式，因此，为保证对用户的告知满足充分知情同意的要求，网站在专门的cookie政策或提示中应注意将语言通俗化，避免普通用户的理解障碍，影响用户同意的效力。

注：本文首发于律商网。
（本文发布于2018年08月08日。）

[13] 参见《反转的法律天平 – 我国cookie隐私第一案判决》， 2015年10月，王融，中国信息通信研究院。

[14]《网安法》第76（5）条：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。

[15] 详见EU advisory body on data protection - Working Party 29: Opinion 04/2012 on cookie consent exemptions.

中国推进个人信息保护

2017年3月15日，全国人大通过了《中华人民共和国民法总则》（“**《民法总则》**”）。该总则为计划于2020年颁布的民法典的首章。在第十二届全国人大第五次会议闭幕会上，出席代表2838人，以2782票赞成的高票通过《民法总则》。《民法总则》将于2017年10月1日起施行。

《民法总则》第111条[1]对个人信息保护作出了规定，是《民法总则》的亮点之一。个人信息保护于2016年10月31日公布的《中华人民共和国民法总则（草案二次审议稿）》（“**《二次审议稿》**”）[2]中首次提出，意在遏制互联网时代猖獗的个人信息非法收集、加工和交易。《二次审议稿》第109条规定：“自然人的个人信息受法律保护。任何组织和个人不得非法收集、利用、加工、传输个人信息，不得非法提供、公开或者出售个人信息。”

相较于《二次审议稿》，2017 年 3 月 15 日最终通过的《民法总则》第 111 条则进一步规定，“任何组织和个人应当确保依法取得的个人信息安全”，强调了信息获得者保护信息的法律责任。

一、《民法总则》中与个人信息保护相关的亮点

个人信息保护纳入《民法总则》为中国未来制订专门的个人信息保护单行法或细则确立了法律基础，被认为是一项突破性的创举。

虽然中国此前在多部法律法规中规定了个人信息保护的相关内容，但均未对个人信息的所有权归属作出明确规定。传统民法仅保护个人的隐私权。然而，个人信息的范围要比个人隐私宽泛得多，也与隐私不同，个人信息同时具有人格和财产属性。

此外，有专家认为《民法总则》第111条关于个人信息保护的规定首次确立了个人对个人信息享有民事权利，进而确定了个人信息的所有权归属。对于个人信息泄露的情况，第111条也为受害人提供了通过侵权主张向违法者寻求赔偿的法律依据。

二、当前中国在个人信息保护领域的主要立法

在《民法总则》通过之前，中国近年来一直努力构建个人信息保护的法律体系。以下为中国在信息保护领域的法规一览表。

年份	法规	内容
2012年	全国人民代表大会常务委员会发布《关于加强网络信息保护的决定》	将“能够识别公民个人身份和涉及公民个人隐私的电子信息”纳入保护范围
2013年	工业和信息化部发布《电信和互联网用户个人信息保护规定》	对电信业务经营者、互联网信息服务提供者收集和使用个人信息作出规定

[1] “自然人的个人信息受法律保护。任何组织和个人不得非法收集、利用、加工、传输个人信息,不得非法提供、公开或者出售个人信息。”

[2] “自然人的个人信息受法律保护。任何组织和个人应当确保依法取得的个人信息安全，不得非法收集、使用、加工、传输个人信息，不得非法买卖、提供或者公开个人信息。”

年份	法规	内容
2013年	中华人民共和国国务院于2013年1月21日发布《征信业管理条例》	对征信业务相关的个人信息的收集、使用、存储、加工作出规定
2015年	全国人大常委会颁布《中华人民共和国刑法修正案（九）》	将“违反规定，向他人出售或者提供公民个人信息”的行为定性为犯罪行为
2016年	2016年11月7日颁布的《中华人民共和国网络安全法》（《网络安全法》）	首次从立法层面定义“个人信息”，对“个人信息”进行了不完全列举
2016年	全国人大常委会颁布《中华人民共和国电子商务法（草案）》	明确对网络交易中涉及的个人信息保护作出规定
2017年	2017年2月4日国家互联网信息办公室发布《网络产品和服务安全审查办法（征求意见稿）》	明确了在审查网络产品和服务的安全性和可控性时，应考虑“产品和服务提供者利用提供产品和服务的便利条件非法收集、存储、处理、利用用户相关信息的风险”这一重要因素

如上所列，近年来中国在涉及银行金融、通信和电子商务等各领域的民事、刑事和行政立法方面做出了不懈努力，为信息安全和个人信息保护构建了法律框架。可以预期今后中国将制定更多的法规，全面落实个人信息保护工作。

三、在指导下收集和处理个人信息

对于在经营过程中收集、处理和使用个人信息的公司而言，信息/数据合规至关重要。为了向顾客提供更好的产品和服务，公司在开发个人信息或数据的商业价值的同时应当审慎收集和使用个人信息，并确保所收集信息的安全性。应制定符合法律法规的服务条款和隐私政策；应在专业指导下极为谨慎地处理数据交易、数据画像、数据跨境传输等问题。

四、保护作为重要竞争优势和商业资源的个人信息

值得注意的是，最近社交网络平台新浪微博诉脉脉的不正当竞争诉讼中[3]，法院在判决中指出“数据的获取和使用，不仅能成为企业竞争优势的来源，更能为企业创造更多的经济效益，是经营者重要的竞争优势与商业资源”。尽管法院并没有进一步讨论个人信息的所有权属性，亦未明确社交网络平台对经营中合法取得的个人信息所享有的权利，判决仍然确立了一项原则，即信息可被视为经营活动中的一种重要竞争优势，这与近年来全球各司法辖区对数据或“大数据”将如何影响竞争政策的讨论是一致的[4]。经营者应将按照合法隐私及数据处理政策收集并控制的个人信息，作为其重要商业资源予以保护。

因此，经营者在确保正当使用个人信息的同时，还应当防止其他竞争者不当“窃取”其所掌握的个人信息。建议公司建立内部数据保护机制，避免竞争者未经授权获取任何数据。此外，与第三方进行数据交易时，应确保拟定的合同明确约定拟交易数据的范围和数据保护义务。事前对第三方的网络环境安全进行尽职调查也十分重要。

大数据的收集、处理和使用在公司的业务运营中发挥越来越重要的作用，全球化也进一步促进了数据在全世界范围内的传输和使用，跨国企业应时刻关注中国及其他司法辖区在个人信息保护方面的立法和监管进程。我们将继续向企业提供中国及其他司法辖区的个人信息保护方面的新进展，确保企业能够正当、合法地使用个人信息。

（本文发布于2017年04月12日。）

[3] 北京知识产权法院，（2016）京73民终588号

[4] 各司法辖区的竞争执法部门和学术机构已发布报告探讨新技术时代大数据如何影响竞争。这些报告包括（但不限于）《竞争法与数据》、《欧洲数据保护专员对大数据时代基本权利统一执法的意见》、《数据驱动型经济 竞争方面的挑战》、美国联邦贸易委员会报告《大数据：包容工具抑或排斥工具》。

2017年，大数据合规离我们有多远？

大数据是近年来的热门话题，大数据产业也被各国政府列为重要的经济增长点。比如美国政府就曾先后发布《大数据研究和发展倡议》和2014年全球“大数据”白皮书的研究报告《大数据：抓住机遇、守护价值》，鼓励和支持大数据产业。2015年9月，我国国务院也发布了《关于印发促进大数据发展行动纲要的通知》，首次在国家层面对大数据发展进行顶层设计，旨在激活中国大数据的资产价值，大力推动大数据发展和应用。此外，2016年发布的《国民经济和社会发展第十三个五年规划纲要》提出，拓展网络经济空间，推进数据资源开放共享，实施国家大数据战略。

目前数据已经成为战略性资源，可以预见的是我国大数据产业也将迎来快速发展的黄金时期。据贵阳大数据交易所数据显示，预计到2020年，中国大数据产业市场规模将由2014年的767亿元扩大至8228.81亿元。

在大数据产业蓬勃发展的今天，尽管数据的创新应用将为政府治理、公共服务和产业发展等多个方面带来巨大潜能，但大数据基于自身特性所带来的特殊法律风险不容忽视，需要我们深入了解并予以防范。由于数据本身权利归属的不确定性，且大数据产业的基础在于多源数据之间关联和因果关系的分析和推断，使得大数据在采集、存储、分析、流通和商用的规范等方面对很多传统法律理念提出了挑战。

一、欧美大数据合规的发展

欧美等国家已经认识到大数据时代合规的风险，通过各类立法或司法实践尝试为大数据产业的各个环节提供指引，寻求在个人信息保护、数据安全、跨境数据传输等法律方面和大数据产业经济发展之间的平衡。

（一）个人信息保护

以个人信息保护为例，美国个人信息保护立法体系主要由1974年通过的《隐私法》以及一些特殊领域的一系列专门法构成。由于立法较早，现有法律法规对于规制大数据时代下新型的信息交换模式和信息来源显得有些滞后，美国通过司法实践和指导性文件的方式予以规范、指引。

比如，1971年制定的《公平信用报告法》（Fair Credit Reporting Act）规范的对象是提供消费者信用调查服务的机构（Consumer Reporting Agencies 或 CRAs），一般仅包括信用局、雇佣背景审查公司和其他信用调查机构。 然而，大数据时代下出现了新型的信息来源，即“数据掮客”（Data Broker）。和传统机构严格按照传统信息渠道调查不同，数据掮客将一些包括社交网络平台信息在内的非传统型数据汇编，并通过大数据分析的方式从各类信息中寻找关联性并最终较为完整地建立个人档案。由于数据掮客提供的个人档案内容完整且准确，已经获得了市场的青睐。然而如果数据掮客不属于消费者信用调查机构，则《公平信用报告法》无法适用，个人信息权利无法得到保障。因此，美国法院通过判例的方式确认“数据掮客”受到《公平信用报告法》规制。在美国诉Spokeo公司案中，联邦贸易委员会认为在线掮客Spokeo通过收集线上和线下的多样数据并分析得出的个人档案，且被用于雇佣调查，因此应该适用《公平信用法》。最终Spokeo和联邦贸易委员会达成了和解[1]。而在美国诉Instant Checkmate案件中，即便Instant Checkmate和Spokeo一样在网站上声明其不属于消费者信用调查机构，Instant Checkmate不得不和联邦委员会议达成和解并接受处罚[2]。

此外，个人信息保护在大数据时代的一大难点在于，如果分析的数据种类和数据量足够，任何信息都可以被认为是与特定个

[1] United States v. Spokeo, Inc., (C.D.Cal.June 12, 2012).

[2] United States v. Instant Checkmate, Inc., (S.D.Cal. filed Mar.24, 2014)

人相联系的信息，个人信息和非个人信息在大数据的时代背景下边界愈发模糊。美国联邦贸易委员会也意识到个人信息保护中的个人信息认定的困难，在2012年发布了《在一个充满快速变化的时代，保护消费者隐私——2012年关于隐私权的建议》（“《建议》”）。《建议》中将保护的消费者个人信息范围扩大到自然人以外的电脑、手机等设备。这是因为从当前的网络环境和数据分析能力下，关联的设备和使用设备的个人总是能被对应联系。此外，联邦贸易委员会还说明了个人信息脱敏的合理措施，具体包括匿名化处理、统计抽样、合成数据、或干扰数据等方式。

欧盟在个人信息保护立法上尽管比美国稍晚，在1981年才签署了第108号条约《有关个人数据自动化处理之个人保护条约》，但近期公布的《欧盟数据保护通用条例》（General Data Protection Regulation, “《条例》”）创新性的增设了个人信息权利。《条例》第20条充分考虑到大数据时代数据转移的必要性，规定了“个人数据可携权”使得用户可以无障碍地将其个人数据从一个信息服务提供者处转移至另一个信息服务提供者。《条例》第17条确认了“个人数据遗忘权”：当用户依法撤回同意或者数据控制者不再有合法理由继续处理数据时，用户有权要求删除数据；数据控制者不仅要删除自己所控制的数据，还要求数据控制者负责对其公开传播的数据，要通知其他第三方停止利用并删除。《条例》增设的权利“不仅极大增强了数据主体对于个人数据的控制能力，也对企业如何保障实现数据主体的权利提出了具体的要求，对企业的制度建设、措施配置、业务流程乃至IT系统设计产生直接影响”。[3]

（二）数据安全

在数据安全方面，欧盟《条例》的出台被认为是数字时代“去除障碍，释放机遇”的重大举措。如上文所述，《条例》在欧盟1995年《数据保护指令》的基础上扩大了数据主体的权利，同时也强化了数据控制者的义务，设置了数据保护官（DPO）、数据保护影响评估（DPIA）等机制，实施数据处理者严格问责机制，并就数据传输制定了更加完善的规则。

例如，《条例》规定对于设立地在欧盟的机构来说，符合法定情形的情况下，机构必须设立DPO。法定情形包括政府部门及公共机构作为数据控制者的，机构核心业务涉及日常地以及系统性地监控数据主体、处理特殊类型的个人数据等。DPO必须具备数据保护专业知识和技能，有能力且能独立地履行职责。《条例》还规定对于高风险的数据处理活动，要事先进行数据保护影响评估。《条例》虽然没有对何为“高风险”进行界定，但明确在以下情形下，应当事前评估：对个人特征的系统性评价（该评价会对数据主体产生法律上的影响）、对大量敏感数据的处理以及对公共领域大规模的系统性监控[4]。

此外，《条例》的另一亮点在于数据泄露通知制度的设置。《条例》要求控制者应当在24小时内向监管机构报告个人数据的泄露情况。如果通知没有在24小时内完成，则应该解释延误原因。如果数据泄露可能会给数据主体的隐私带来消极的影响，例如身体伤害等，相关的控制者必须毫不延误的通知数据主体，以便个人及时采取措施。通知应说明个人数据违反的性质，并且提供降低风险的建议。在数据分析与数据挖掘技术日趋成熟的大数据时代，黑客和恐怖分子窃取数据的机会增加，手段更加高明和不易察觉，数据泄露产生的诸如身份盗窃、欺诈行为、数据滥用或者声誉受损的不利影响会扩大化，规定数据泄露的通知义务，可以提醒数据被泄露的个人采取防范措施，尽可能地降低风险和伤害。

类似地，美国联邦通信委员会于2016年12月2日公布的《宽带和其它电信服务中用户隐私保护规则》（Protecting the Privacy of Customers of Broadband and Other Telecommunications Services，“FCC新规”）也对相关运营商设定了信息泄露情况下的通知义务。具体而言，除非运营商能合理地确定数据泄露不会对受影响的客户造成合理的危害风险，在发生信息数据泄露的情况下应及时通知受影响的客户、FCC、联邦调查局和特勤局。针对数据泄露的不同严重程度，FCC新规从通知对象和通知时间等方面对运营商提出了不同要求。[5]

（三）其他

除个人信息保护和数据安全以外，欧美还对大数据应用的多个环节的其他问题进行了广泛的讨论，其中包括数据所有权归属、数据质量、数据标准化、数据交易追责等问题。由于大数据已经作为核心经济资产被社会认可，考虑到大数据的经济价值以及可能带来的竞争优势，欧盟、美国等司法辖区近年来已开始关注大数据可能产生的垄断问题。美国、欧盟、西班牙、德国、法国等各地的竞争执法机构先后发布了大数据和反垄断的相关研究报告，结合实践分析大数据对于反垄断执法的影响。美国反垄断主管机关已经开始在审查企业合并时考虑大数据对市场进入的影响。在2014年的Bazaarvoice / Power-Reviews合并案中，美国司法部经审查最终认定在“评级及评论平台”市场上数据本身会成为一种市场进入障碍。即便在非数据市场（non-digital market）上，法国和欧盟也在不同的案件中认定数据由于其稀缺性有可能导致进入障碍或者使得企业拥有数据优势（data advantage）[6]。

---

[3]《欧盟数据保护通用条例》详解，王融。

[4] 见《欧盟数据保护通用条例》第35条。

[5] 见《隔耳有“墙”——从美国FCC新规则谈个人信息保护新趋势》，金杜律师事务所，宁宣凤、吴涵、黎辉辉、王诗笋。

[6] 见French Competition Authority, Decision No.13-D-20 of 17.12.2013,以及European Commission, “EDF/Dalkia en France”, COMP/M.7137。

二、中国大数据合规的挑战和机遇

（一）挑战

尽管中国关于信息数据的立法不多，但对于信息和数据合规问题一直很重视。 在个人信息保护的私法领域，虽然我国民法并没有确认“个人信息权利”，但早在2010年颁布的《最高人民法院关于审理旅游纠纷案件适用法律若干问题的规定》就首次提及“个人信息”概念[7]。全国人大于2012年发布的《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》正式将“能够识别公民个人身份和涉及公民个人隐私的电子信息”纳入保护范围。[8]2016年11月7日审议通过的《中华人民共和国网络安全法》（“《网安法》”）则对个人信息做了不完全列举并首次从立法层面对个人信息进行了界定。

在大数据安全方面，《网安法》用整个第三章共19条的篇幅，为包括网络服务提供者在内的网络运营者规定了一系列保护“网络运行安全”方面的要求和义务。其中的第21条明确规定，国家实行“网络安全等级保护制度”，并要求网络运营者按照这一制度的要求履行其网络运行安全保护义务。[9]《网安法》还对于“关键信息基础设施”要在网络安全等级保护制度的基础上实行重点保护，明确了关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家安全审查。[10]

然而对比欧美国家大数据合规的立法和实践，目前中国大数据合规还面临着缺乏具有操作性的指南的问题。比如我国对于个人信息的界定仍然沿用了欧盟的传统路径，即以“可识别性”为核心标准。然而，包括《网安法》在内的法律法规并未对怎样的信息或数据会被认定为具有“个人可识别性”进行详细界定，“单独或与其他信息结合识别个人身份”的标准仍然抽象、缺乏操作性。个人信息认定如果没有进一步的指引，将导致个人信息与非个人信息的边界模糊化，个人信息的潜在范围无限扩张，法律适用面临极大的不确定性。另一方面，个人信息脱敏或匿名的应用日益广泛，企业将面临着经脱敏的信息也很难排除被重新识别可能性的棘手困境。

此外，与主要司法辖区目前强调数据本地存储和限制数据跨国分享的立法和实践一致，《网安法》明确规定个人信息必须存储在我国境内，即“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据”必须存储在我国境内，并且从原则上规定了该等信息不得向境外传输。[11]然而，“关键信息基础设施认定标准”，以及“数据出境评估方法”目前仍未出台，给《网安法》的执法和企业合规带来不确定性。

最后，目前我国对于大数据的立法和实践还停留在建立框架阶段，对于其他一些重点问题，比如数据交易各个环节的合规问题以及大数据可能引发的垄断风险等还未引起足够关注。

（二）机遇

挑战历来与机遇并存。在中国大数据立法和执法缺少实施细则的前提下，其他司法辖区的经验值得我们学习和借鉴。比如跨境数据传输，欧盟《条例》在欧盟1995年《数据保护指令》的基础上细化并完善了数据转移合法机制。欧盟《条例》原则上规定“欧盟公民的个人数据仅能转移到与欧盟同等保护水平的国家”，同时又从充分性决定、有约束力的公司规则、标准合同条款等多方面详细规定了合法转移机制所涉及的规则，使其更具有操作性。其他比如“个人信息的认定标准”、“信息脱敏的合理措施”、“用户默示和明示的判断标准”等难点问题也可以参考其他司法辖区的实践。

在数据信息全球流通的背景下，企业学习和借鉴其他司法辖区的经验也有着一定的必要性。这是因为跨境运营企业一方面需要考虑不同司法辖区对跨境数据传输的不同规则及限制，同时也需要考虑其在某一司法辖区内与数据相关的活动是否有可能受到其他司法辖区规则的规制。

以欧盟条例为例，其适用范围从过去的属地主义扩展到了属人主义。具体而言，对于成立地在欧盟的机构而言，适用范围虽无变化，但强调了无论数据处理的活动是否发生在欧盟境内，都统一遵循条例的规定；对于成立地在欧盟以外的机构而言，则适用属人因素，只要其在提供产品或服务的过程中处理了欧盟境内个体的个人数据，将同样适用条例。换句话说，不论是传统行业，还是电子商务、社交网络等新兴领域，只要涉及向欧盟境内个人提供服务并处理个人数据，都将需要适用《条例》， 因此跨境经营企业在内部数据合规上必须参考《条例》的规定。 简而言之，在大数据行业发展的推动力下，跨国企业可能需要结合各个司法辖区的数据合规规则，建立相对统一、完整、标准的数据合规体系。

2017年已经到来，大数据产业将进入快速发展的黄金时期，大数据合规问题已经箭在弦上。我们将密切关注全球大数据合规的动态，和企业一起迎接大数据时代的机遇和挑战。

（本文发布于2017年01月26日。）

---

[7] 司法解释第九条规定“旅游经营者、旅游辅助服务者泄露旅游者个人信息或者未经旅游者同意公开其个人信息，旅游者请求其承担相应责任的，人民法院应予支持”。

[8] “国家保护能够识别公民个人身份和涉及公民个人隐私的电子信息；任何组织和个人不得窃取或者以其他非法方式获取公民个人电子信息，不得出售或者非法向他人提供公民个人电子信息。”

[9] 《网络安全法》来了！——企业应该知道的五件事，作者金杜律师事务所商务合规部蒋科、杨楠。

[10] 《网络安全法》第35条。

[11] 《网络安全法》第37条。

个人信息保护的百万罚单时代来了？

2016年11月7日，全国人大常委会审议通过了《中华人民共和国网络安全法》（“网络安全法”），该法将于2017年6月1日正式实施。一经发布，网络安全法即引起社会各界的广泛关注，“网络空间主权”、“网络安全等级保护”、“关键信息基础设施”等一系列概念顿时成为了社会讨论的热点话题。

而网络安全法的另外一大亮点是其中关于个人信息保护的相关条款。个人信息保护法的草案曾于2008年提交国务院立项审查，但此后立法进程即停滞不前。因此，在网络安全法出台之前，我国个人信息保护规则仅散见于多部不同的法律法规和规范性文件中，如《侵权责任法》、《刑法》、《治安管理处罚法》、《消费者权益保护法》和《全国人大常委会关于加强网络信息保护的决定》等。网络安全法的出台为个人信息保护制度开创了多个“首次”，尤为引人注目。

一、新标杆树立，开创四大“首次”

• 首次在法律层面确立了一般意义上“个人信息”的概念，成体系地在法律层面确定了个人信息保护的基本规则

网络安全法第七十六条规定，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、身份证号码、个人生物识别信息、住址、电话号码等。

“个人信息”及其他类似概念，如“个人电子信息”[1]、“个人金融信息”[2]以往散见于不同的法规和规范性文件中。而网络安全法首次在法律层面确立了一般意义上的“个人信息”，进一步扩大了个人信息的保护范围。一方面，个人信息不再要求有特定的记录方式，即通过任何方式记录下来的信息都将被包括在内；另一方面，网络安全法中“个人信息”的概念强调可识别性，即使是通过与其他信息结合才能识别身份的信息，也属于网络安全法保护的个人信息。

• 首次明确了禁止向他人提供个人信息的例外情形

网络安全法规定，未经被收集者同意，不得向他人提供个人信息。而与此同时，网络安全法首次明确了上述禁止性规定的例外，即如果特定信息经过处理无法识别特定个人，并且不能复原，则不受上述限制。

根据此前的相关规定，收集个人信息均要求经个人同意方可进行，并未设置例外条款。事实上，由于经过处理无法识别特定个人且不能复原的信息很难指向特定个人，利用此类信息侵害个人合法权益的可能性也较小。因此，在国家鼓励和推动大数据产业发展的大背景下，网络安全法给予脱敏信息在侵权领域的“豁免性”地位，有利于保障利用脱敏信息进行数据挖掘及其他方面研究行为的合法性与积极性，推动数据产业的发展。

• 首次在法律层面规定特定个人信息的存储位置，维护国家信息安全

网络安全法对**关键信息基础设施运营者**的个人信息存储地点提出了特殊要求，要求在我国境内运营中收集和产生的个人信息

[1] 见《全国人大常委会关于加强网络信息保护的决定》。

[2] 见《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》。

和重要数据应当在我国境内存储。

目前，我国仅在某些特殊领域有对个人信息存储位置的要求。例如，根据中国人民银行的有关规定，在中国境内收集的个人金融信息的储存、处理和分析应当在中国境内进行，银行业金融机构不得向境外提供境内个人金融信息。鉴于关键信息基础设施的认定尚无明确规定，该条款加大了企业存在个人信息过程中面临的潜在风险和不确定性。

• 首次在法律层面明确了违反个人信息保护规则的行政责任

根据网络安全法的规定，侵害个人信息相关权利时，将面临警告、没收违法所得、罚款、暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证和吊销营业执照等法律责任。其中对直接责任人员的罚款数额可达十万元，对网络运营者的罚款数额更可高达一百万元。

此前，对违反个人信息保护规则的法律责任，具体的罚则散落于《全国人大常委会关于加强网络信息保护的决定》、《刑法》、《治安管理处罚法》、《消费者权益保护法》等各部独立法律法规及规范性文件之中。相较于此前的规定，网络安全法对违法行为的罚款力度明显提高；此外，与《全国人大常委会关于加强网络信息保护的决定》相比，网络安全法增加了对直接责任人员的罚款，并且明确了侵犯个人信息情节严重时的多种罚则，即新增了责令暂停相关业务、停业整顿以及吊销营业执照。

二、体系性归纳，收集个人信息“有规可循”

网络安全法第四章针对收集、使用个人信息做出的规定，将此前散落在多个法律法规中关于个人信息保护的一般规则进行了体系性的归纳。为便于大家理解，我们将这些规则整理如下。

规则类型	规则内容	
基本原则	网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则。	
信息收集	• 公开收集、使用规则； • 明示收集、使用信息的目的、方式和范围； • 需要取得被收集者的同意。	
信息使用	使用范围	网络运营者对于个人信息应当严格保密，其不得向他人提供个人信息。特定信息经过处理无法识别特定个人且不能复原的除外。
	使用方式	网络经营者应当采取技术措施和其他必要措施确保其收集的个人信息的安全性，避免信息的泄露、篡改和毁损。
信息处理	依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。	

三、高位法确认，维护个人权利“有法可依”

在确立个人信息保护基本规则的基础之上，网络安全法更在若干方面进一步拓展了个人信息的权利范围，为公民的个人信息提供了更为全面的保护。

• 拓展公民知情权

网络安全法第二十二和第四十二条规定，在发生或可能发生信息的泄露、篡改和毁损，或发现其网络产品、服务存在安全缺陷、漏洞等风险时，网络运营者或者网络产品、服务提供者应当及时告知客户。

因此，企业在开展业务的过程中如需收集、使用公民个人信息，不仅应当告知信息收集和使用的规则、目的、方式和范围，更需注意在发生或可能发生潜在危机时及时履行告知客户的法定义务，以便客户采取应对措施、降低潜在损失。**这就要求企业完善内部危机应对机制，更为密切地关注信息安全，以便在突发情况下及时、有效地做出应对。**

• **明确泄露信息删除权**

网络安全法第四十三条规定，网络运营者收集、使用个人信息违反法律规定或双方约定的，个人有权要求删除。也就是说，个人不仅在网络运营者违法收集信息的情况下有权要求删除相关信息，还可以网络运营者违反双方约定为由要求删除信息。

实际上，网络安全法对删除权的确定与收集使用信息需遵循的正当性、必要性原则一脉相承——无论是违反法律规定，还是违反双方约定的收集使用信息的范围和期限，即意味着企业失去了留存使用信息的合理理由，依法应当删除相关信息。**因此，从合规角度，企业在制定与用户的合同条款时需对有关收集使用信息的合同约定内容予以充分关注，从企业内部制度设计的角度降低潜在风险。**

• **确立错误信息更正权**

网络安全法第四十三条规定，网络运营者收集、存在的个人信息有错误的，个人有权要求予以更正。

此前，我国仅在个别领域对此种权利有明确规定，例如《个人信用信息基础数据库管理暂行办法》曾规定个人有权向征信管理部门就错误信用信息提出异议。[3]此次，网络安全法则从更广泛的意义上赋予了个人信息主体更正错误信息的权利。

四、拭目以待，企业合规依然“任重道远”

鉴于网络安全法中有关个人信息保护规则的适用主体为网络经营者，而网络安全法中“网络经营者”[4]与“网络”[5]的概念都极为宽泛，在没有进一步具体规定的情况下，很难将某一特定类型的经营者排除在适用范围之外。换言之，网络安全法在法律层面规制个人信息保护的主体范围达到了前所未有的广度。

网络安全法首次成体系地从法律层面对个人信息保护制度的相关规则进行了梳理和确认，并强化了法律责任，为企业收集、使用个人信息提出了更高的要求。而部分规定的具体操作规程尚待明晰和完善，也为企业建立健全内部的信息安全管理机制带来了新的挑战。此外，网络安全法并未明确依法承担保护个人信息职权的监管机构，这在一定程度上也增大了执法的不确定性。

从合规经营的角度，企业应对个人信息保护给予充分重视，制定和完善企业与用户、以及与第三方就个人信息收集使用签订的合同文本及其他相关政策，并密切关注相关立法的发展以确保企业经营合规性。值得注意的是，中央网信办网络安全协调局局长日前表示，为更好地保护个人信息，中央网信办正在着手制定个人信息收集规范标准。可以预见，企业未来在收集使用个人信息过程中将面临着日趋严格的法律规制。我们将与企业一同密切关注个人信息保护立法与执法的发展。

（本文发布于2016年11月15日。）

[3]《个人信用信息基础数据库管理暂行办法》第十六条和第二十条规定，“个人认为本人信用报告中的信用信息存在错误（以下简称异议信息）时，可以通过所在地中国人民银行征信管理部门或直接向征信服务中心提出书面异议申请”；经过核查确认信息登载错误后，“征信服务中心……应当在2个工作日内对异议信息进行更正”。

[4]网络安全法第七十六条，（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

[5]网络安全法第七十六条，（五）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

“人面不知何处去”
——人脸数据采集及使用的权利边界

近年来，人工智能应用逐渐落地，其中尤以人脸识别最为典型[1]。新技术固然给日常生活带来了种种便利，但因为人脸包含生物识别特征的特殊属性，相关争议从未停止[2]。在瑞典，一所中学因使用人脸识别系统被认定违反《通用数据保护条例》，收到瑞典数据保护机构的首张罚单；在美国伊利诺伊州一起集体诉讼案中，某知名公司被指控滥用人脸图像数据，最终不得不支付5.5亿美元的隐私和解金；在我国，人脸识别技术在金融等领域已有广泛应用，但人脸信息的滥用、泄露和安全问题也层出不穷[3]。

本文将从我国法律法规有关人脸信息保护的不同角度出发，针对人脸应用的不同场景，结合海外相关的立法和执法案例，试探讨不同场景下人脸数据采集、使用的权利边界，人脸数据采集及使用的合规界线。

一、传统人脸法律的保护路径

（一）肖像权保护的外延扩展

人脸往往与肖像有着紧密关联。通常意义的肖像指通过绘画、摄影等方式在一定物质载体上所反映的特定自然人可以被识别的外部形象，而法律意义上的肖像是指自然人因其外部特征而享有的一种人格利益[4]，因此当自然人的脸作为最能反映其外部形象的身体部分出现在绘画、照片、视频中时，自然人当然享有肖像权。肖像权在我国受到民法保护，根据《民法通则》[5]的规定，肖像权侵权须以“未获本人同意”与“以营利为目的”作为构成要件。但司法实践与学理中，均认为如依此将侵害肖像权的行为限定于“以营利为目的”过于狭隘。

近年来，随着科技的发展，肖像权保护也受到了新的挑战。一方面，社交软件的广泛应用和摄影技术的高速发展，使我们的肖像可通过多种途径被轻易取得；另一方面随着换脸等技术的发展，只需要简单操作手机屏幕，我们的肖像就能被不法商人制作成虚假广告谋取利益，也可能被制作成足以以假乱真的色情视频、假新闻用来打击报复、敲诈勒索，使得人的人格权益与财产权益受到严重威胁。去年发布的《民法典人格权编（草案三审稿）》也对近来火热的AI换脸予以关注，进一步明确了对肖像权的规制，其中删去了“以营利为目的”的侵权要件，规定丑化、污损，利用信息技术手段伪造等方式侵害他人肖像，或擅自制作、使用、公开他人肖像的行为都可能构成肖像权侵权[6]。

---

[1] 来自国金证券行业研报显示：全球40%的人工智能企业都涉及计算机视觉。另有市场咨询公司预测，2019年全球人脸识别市场的规模预计为32亿美元，到2024年该市场规模将达到79亿美元，复合年增长率高达16.6%。

[2] “人脸和其他生物的特征数据，比如和指纹之间存在一个巨大区别是，它们可以远距离起作用。任何人只要有手机都能拍摄一张照片供人脸识别程序使用。”李甜, 唐金燕, 陈溢波. 人脸识别安全之考[EB/OL] http://paper.people.com.cn/rmzk/html/2019-12/10/content_1960803.htm. 2019-10-26.

[3] 姚佳莹, 黄姝静. 人脸识别管放之争：一眼认出藏匿逃犯, 一键兜售人脸[EB/OL]. https://finance.sina.com.cn/stock/hyyj/2019-12-15/doc-iihnzahi7725008.shtml. 2019-12-15.

[4] 杨立新. 人格权法论[M]. 北京：人民法院出版社, 2002. 459.

[5] 第一百条 公民享有肖像权，未经本人同意，不得以营利为目的使用公民的肖像。

[6] 第七百九十九条 任何组织或者个人不得以丑化、污损，或者利用信息技术手段伪造等方式侵害他人的肖像权。未经肖像权人同意，不得制作、使用、公开肖像权人的肖像，但是法律另有规定的除外。

（二）人脸作为隐私保护的客体

随着人脸识别等技术的飞速发展，人脸的可识别性、天然的唯一性使其被应用于安检、追踪逃犯、支付等多个领域，为人们的生活带来安全与便利的同时，人脸的隐私保护问题也得到了更多的关注。去年发布的《民法典人格权编（草案）》[7]首次在立法层面给予“隐私”明确的定义，即自然人不愿为他人知晓的私密空间、私密活动和私密信息等，规定任何组织或个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权，并在第八百一十二条[8]进一步列举了一些可能构成侵犯隐私权的具体行为，例如APP未获取权限即访问用户相册、在他人住宅外安装摄像头等。立法层面的进展可以看出隐私权保护得到了更多的关注。在国外，多国政府也对人脸识别带来的隐私权担忧作出回应，美国多个城市先后出台禁令禁止公权力机构使用人脸识别技术，欧盟此前也曾计划颁布人脸识别技术禁令，在五年内禁止在公共场所使用人脸识别技术[9]。

二、人脸数据作为个人信息保护的客体

除了传统人脸保护的规则随着科技的发展日益完善，人脸作为能反映特定个人身份的属性还可能被认定为个人信息中较为敏感的一类，即个人生物识别信息，并受到相应规制。除了遵守一般个人信息的保护要求，以GB/T 37036.3-2019《信息技术 移动设备生物特征识别 第3部分：人脸》以及最新出台的推荐性国家标准GB/T 35273-2020《信息安全技术 个人信息安全规范》（“新版《个人信息安全规范》”）[10]和JR/T 0171-2020《个人金融信息技术安全规范》为例，我国对于人脸作为个人生物识别信息的收集和使用施加了更为严格的要求。

尽管随着人脸识别技术的广泛应用，将其作为个人生物识别信息进行保护的法律法规正在日益完善，然而这些法律法规在各类新型应用场景下的适用仍然面临着诸多的挑战。当人脸数据的采集和使用行为不仅反映人脸主体的利益，还牵涉到社会的公共利益和企业的正当权益时，如何在保障人脸数据的隐私和安全同时，仍然能实现企业和公权力机关等其他主体基于不同目的对人脸数据予以收集和使用的正当诉求，是值得探讨的问题。

三、人脸数据的采集场景及相关分析

（一）人脸识别应用场景的分类

大致而言，人脸识别的场景可以分为三种类型：

- **1:1人脸识别模式主要是用于身份验证：**1:1人脸识别技术是一种静态对比，比较两个人的相似度。主要是利用图像处理技术从图像中提取人脸特征值，计算机对当前人脸与人像数据库进行快速人脸比对，并得出是否匹配的过程。
- **1:N人脸识别模式主要是用于行业场景落地：**1:N人脸识别技术是在海量的人像数据库中找出当前用户的人脸数据并进行匹配。N的数目在千万级。典型场景如电子班牌、物业小区、新零售的客户识别等。
- **N:N人脸识别模式主要用于政府机关：**是1:N的延伸，即同时对多张人脸进行人脸检索，是通过计算机对场景内所有人进行面部识别并与人像数据库进行比对的过程，是动态人脸比对。应用场景主要为公共安防、天网系统等。

以下我们将选取人脸识别的若干典型场景，分析每种类型下人脸识别应用可能存在的合规问题和各方参与主体对于人脸数据采集及使用的权利边界。

1. 1:1人脸识别模式下的身份验证

1:1人脸识别的应用场景主要为人脸手机解锁、人证合一，通常应用落地场景为手机厂商寻找有算法识别技术的软件供应商为其内置SDK，辅助代码移植，使其手机不将人脸传输至服务器，而是在本地即拥有人脸识别解锁的能力[11]。

在现行《个人信息安全规范》中也指出，“如果产品或服务的提供者提供工具供个人信息主体使用，提供者不对个人信息进行访问的，则不属于本标准所称的收集行为”并例举了离线导航软件在终端获取用户位置信息的事例。因此我们理解，在这种情况下，从现行《个人信息安全规范》而言，如果人脸数据仅在本地化存储，且人脸识别技术的提供者和产品或服务提供者均不对人脸数据进行访问，产品或服务的提供者被认定为收集的可能性会显著降低。如此一来，人脸数据本地化可能引发的问题则包括：

---

[7] 第八百一十一条 自然人享有隐私权。任何组织或者个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。隐私是自然人不愿为他人知晓的私密空间、私密活动和私密信息等。

[8] 第八百一十二条 除法律另有规定或者权利人同意外，任何组织或者个人不得实施下列行为：（一）搜查、进入、窥视、拍摄他人的住宅、宾馆房间等私密空间；（二）拍摄、录制、公开、窥视、窃听他人的私密活动；（三）拍摄、窥视他人身体的私密部位；（四）收集、处理他人的私密信息；（五）以短信、电话、即时通讯工具、电子邮件、传单等方式侵扰他人的生活安宁；（六）以其他方式侵害他人的隐私权。

[9] 蒋琳. 周三欧盟将发布人工智能白皮书 公共场所人脸识别五年禁令被取消[EB/OL]. https://m.mp.oeeee.com/a/BAAFRD000020200218266354.html. 2020-2-18.

[10] 新版《个人信息安全规范》将于2020年10月1日生效。

[11] 2017年，当苹果首次在iPhone X中应用Face ID面部识别进行加密认证和解锁时，Face ID的安全性曾引发广泛质疑，苹果公共政策副总裁Cynthia Hogan回应“用户的脸部信息数据将会被加密，并且只会存储在本地”。仲平. 苹果：iPhone X的Face ID数据只会存储在本地并加密[EB/OL]. https://www.ithome.com/html/iphone/330287.htm. 2017-10-17.

（1）不将人脸数据本地化处理认定为采集行为的目的何在，目前我国法律法规和《个人信息安全规范》有关个人信息采集、使用的要求是否可以在人脸数据本地化场景下予以部分或全部的豁免？

由于人脸数据本地化处理，相比于上传至云端而言，企业对其进行进一步使用和信息泄露的风险降低。在企业对该信息的控制权和使用权减弱的同时，现行《个人信息安全规范》也希望相对降低企业对于该信息采集的责任义务要求。然而，从个人信息主体权益保护的角度而言，个人信息采集、使用的要求并不能在人脸数据本地化处理的场景下被完全豁免。例如：

推荐性国家标准GB/T 37036.3-2019 《信息技术 移动设备生物特征识别 第3部分：人脸》[12]中则将移动设备生物特征识别分为本地识别[13]和远程识别两种模式，而无论是本地识别还是远程识别，都需要参考借鉴相应的标准要求。其中，根据安全要求[14]的相关规定，在采集用户人脸样本前，仍应向用户明确告知所提供的产品或服务收集、使用用户人脸数据的规则，并获得用户的授权同意。

同时，人脸数据的本地化存储还需要保障个人信息主体对数据的控制权；例如苹果在2019年8月宣布在“默认情况下不再保留Siri交互的录音”并且允许用户在系统设置中关闭语音唤醒功能；“亚马逊的语音助手Alexa为用户提供了不同级别的隐私保护设置，如查看语音记录或删除所有录音”，类似地包括允许用户在关闭Face ID功能时同时删除此前收集的人脸图像和面部特征信息等。

（2）如果人脸数据的本地化处理不被认定为产品或服务的提供者的个人信息采集行为，那么应当由谁来承担本地化人脸数据处理的安全保护责任？

尽管本地化的存储和非接触式处理，但根据《网络安全法》中对网络产品、服务的安全性要求[15]，以及其他国家标准、行业规范等内容的规定，产品或服务的提供者仍然有义务采取必要的措施保障人脸数据在本地存储的安全，包括但不限于“设置人脸特征采集超时处理机制”、建立“移动设备可信环境”、“人脸特征项提取后的人脸样本不可恢复地删除”、“本地识别模式中的人脸数据的保密性和完整性”等[16]。

2.1：N人脸识别模式下的行业场景：如何获得消费者的明示同意？

1:N的人脸识别是商业实践中最为常见的应用方式之一，其典型应用场景包括但不限于刷脸支付、无人零售等；但在实践中，二者却又有所不同。

刷脸支付

对支付行业而言，2019年也被称为“刷脸支付元年”[17]。2019年8月，中国人民银行（**“央行”**）提出“探索人脸识别线下支付安全应用……突破1：N人脸辨识支付应用性能瓶颈，由持牌金融机构构建以人脸特征为路由标识的转接清算模式……”[18]，从监管角度释放“人脸支付业务发展的积极信号”[19]；10月，中国银联携手60多家银行机构与产业合作伙伴发布智能支付产品“刷脸付”，通过“刷脸”和支付口令即可完成付款[20]……对刷脸支付的探讨应当区分线上和线下两类场景，其中“线下刷脸支付技术已较为成熟”[21]，但即便如此线下刷脸支付也面临着人脸数据采集和存储、使用的合规性、数据安全的相关限制[22]。

从数据源头开始，刷脸支付面临的首要挑战是如何保证人脸数据收集的合规性，特别是新版《个人信息安全规范》中收集个人生物识别信息的单独告知并征得个人信息主体明示同意[23]的要

---

[12] 该标准将于2020年5月1日施行。

[13] “即人脸特征采集模块、人脸特征存储模块和人脸特征比对模块均在移动设备中实现，并在人脸特征采集模块中进行质量判断和呈现攻击检测”

[14] GB/T 37063.3-2019 《信息技术 移动设备生物特征识别 第3部分：人脸》第9条 安全要求

[15] 《网络安全法》第二十二条第一款，“网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。”

[16] GB/T 37063.3-2019 《信息技术 移动设备生物特征识别 第3部分：人脸》

[17] 2022年刷脸支付用户将达7.6亿[EB/OL]. http://www.gd.xinhuanet.com/newscenter/2019-11/22/c_1125262424.htm. 2019-11-22

[18] 中国人民银行关于印发《金融科技（FinTech）发展规划（2019-2021年）》的通知

[19] 之邪. 评《人脸识别线下支付行业自律公约》（试行）[EB/OL]. http://m.mpaypass.com.cn/news/202002/05101242.html. 2020-02-25.

[20] 刷脸支付国家队入场！银联携AI四小龙突围阿里腾讯[EB/OL]. https://www.jiqizhixin.com/articles/2019-10-29. 2019-10-29

[21] 央行李伟：刷脸支付线上线下场景应区分[EB/OL]. https://new.qq.com/omn/20190924/20190924A0OP9M00.html. 2019-09-24.

[22] 包括但不限于GB/T 35273-2020《信息安全技术 个人信息安全规范》、JR/T 0171-2020《个人金融信息保护技术规范》中个人生物识别信息、C3类别用户鉴别信息的收集、存储、使用和共享等方面的要求。以及中国支付清算协会印发的《人脸识别线下支付行业自律公约（试行）》中涉及“安全管理、终端管理、风险管理和用户权益保护”等内容 。

[23] “收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意。” GB/T 35273-2020《信息安全技术 个人信息安全规范》第5.4条。

求？在现有的线下刷脸支付实践中，用户在开通相应的刷脸支付功能时，一般需要事先在对应的App上先行开通刷脸支付功能，通常会在相应功能界面上提供特定《刷脸支付用户协议》或《刷脸支付个人信息保护政策》文本并要求用户输入支付密码或其他可以验证账户身份的要素；在线下实际使用前，消费者还需要先主动在众多支付方式中选择“刷脸支付”，在做出选择后终端设备才会开始采集人脸数据。就前述环节而言，是否可以将开通刷脸支付功能时的文本视为单独告知，用户通过输入支付密码等方式完成业务开通的行为视为明示同意？如果认为新版《个人信息安全规范》中的“单独告知与明示同意”对告知与同意的时点有着更为严格的要求，个人信息主体在线下付款环节，在众多支付手段中的主动选择刷脸支付的这一行为，能否实现“告知与同意”从开通到使用之间的跨越？抑或者企业要在线下刷脸机器中完成《刷脸支付用户协议》或《刷脸支付个人信息保护政策》的内置、并在每次选择唤醒刷脸支付时，先行弹窗完成文本展示并要求消费者勾选同意，才能满足合规的要求？鉴于后者可能带来消费者时间成本、企业运营成本的显著增加和刷脸支付手段的效率降低，其要求的正当性基础是否充分？又是否有必要且能够通过利益衡量的测试？这些问题或许有待于进一步的探讨。

同时，刷脸支付除了涉及人脸数据的采集外，还与个人信息主体的交易安全密切相关。尽管客户本人生理特征要素可以作为支付交易的验证要素之一，但可能并不适宜作为唯一要素[24]；同时考虑到人脸数据，相比于其他如指纹、虹膜等生物识别信息，采集行为具有非接触性，相应个人信息主体感知可能性也更低，更需要通过其他验证要素完成安全性的补强，实现“安全与便捷”的兼顾[25]。目前实践中常用的包括手机号码后四位以及口令支付密码，根据监管机构的态度，二者在信息本身的保密性、作为验证要素的安全性方面可能存在一定的差异。同时，在此之外是否还可以选择其他的验证要素，在保障刷脸支付的便捷同时不断提升其安全性，维护个人信息主体的交易安全与财产安全，可能也是刷脸支付未来需要思考的问题。

此外，刷脸支付并非是一项孤立存在的产品，而是一个庞大的产业链和商业生态系统，其中除了刷脸支付服务的直接提供者外，还可能涉及消费者、商户、硬件设备制造商、人脸识别技术服务商、存储服务商等诸多主体，消费者（即个人信息主体）的人脸数据可能以原始图像、摘要信息、去标识化后的数据等不同形式在多主体之间流转交互，其中也同样涉及人脸数据的存储。而这一过程同样需要受到诸多法律法规、国家标准、行业规范的限制。例如，根据JR/T 0171-2020《个人金融信息保护技术规范》中用于用户鉴别的个人生物识别信息（C3类别信息）不应共享、转让；新版《个人信息安全规范》中要求“原则上不应存储原始个人生物识别信息”，[26]但同时肯定了“个人信息控制者履行法律法规规定的义务相关的情形除外”……在种种规则交织的情况下，如何通过不同环节、不同程度的数据处理行为使得人脸数据以合理的形式在各主体之间形成有序流转，如何通过协议、审计等方式合理分配不同主体保障人脸数据安全的义务与责任；如何通过合规管理制度和数据安全技术措施评估人脸相关数据的存储必要性并保障人脸数据的存储安全，都是刷脸支付所需要回应的问题。

无人零售

打开手机App界面通过感应器进门，拿起需要的午餐三明治和一瓶果汁，然后大摇大摆走到闸机口，无需付账闸机门自动打开走出商店；这一幕并非是任何“乌托邦”社会的构想，而是发生在美国Amazon Go无人超市的真实场景[27]。随着人脸识别技术在新零售领域的广泛应用和关键赋能，利用含有人脸识别技术的摄像头构建起系统性的客户跟踪和锁定机制，完成顾客的定位，并结合“货架上的压力传感器和红外线探头”感知重量变化等，判断“哪位顾客拿走了多少货物”，最终完成结算，Amazon Go无人超市模式大大节省了消费者的购物时间，提升了购物效率[28]。在中国，2017年曾被业内人士称为“无人零售元年”[29]，但在2年多后的今天，中国无人零售的发展之路并未如美国一般一帆风

[24]《非银行支付机构网络支付业务管理办法》第二十二条中规定支付机构可以组合选用“仅客户本人知悉的要素，如静态密码等”、“仅客户本人持有并特有的，不可复制或者不可重复利用的要素，如经过安全认证的数字证书、电子签名，以及通过安全渠道生成和传输的一次性密码等”和“客户本人生理特征要素，如指纹等”用于对客户使用支付账户余额付款的交易进行验证。

[25] 参见央行李伟：刷脸支付线上线下场景应区分[EB/OL]. https://new.qq.com/omn/20190924/20190924A0OP9M00.html. 2019-09-24.

[26] 可采取的措施包括但不限于：1）仅存储个人生物识别信息的摘要信息；2）在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能；3）在使用面部识别特征、指纹、掌纹、虹膜等实现身份识别、认证等功能后删除可提取个人生物识别信息的原始图像。

[27] 邢逸帆. 亚马逊无人超市开业了，我在里面“偷”了样东西[EB/OL]. https://mp.weixin.qq.com/s/SZidR-lUnL0KWlXJyoumLg. 2018-11-08.

[28] 邢逸帆. 亚马逊无人超市开业了，我在里面“偷”了样东西[EB/OL]. https://mp.weixin.qq.com/s/SZidR-lUnL0KWlXJyoumLg. 2018-11-08.

[29] 杜鑫. 无人零售，无人问津？[EB/OL]. http://www.xinhuanet.com/fortune/2020-01/06/c_1125424311.htm. 2020-01-06.

顺，暂且抛开商业发展不提，**无人零售场景下，人脸数据采集和使用的告知同意、数据的共享与流转、数据安全都面临着合规性的挑战。**

曾有观点提出，无人超市等新零售场景在媒体宣传下，其使用人脸识别技术追踪用户，为用户提供便利的特性如果成为一种公认的常识，那么在商店门口做适当告知，是否可认为步入无人超市的个人已经对生物识别信息被收集有了合理预期[30]，进入商店的行为可以构成对于收集使用行为的同意。但在新版《个人信息安全规范》发布后，对于这一观点的讨论看似已经尘埃落定，考虑到生物识别信息收集“单独告知+明示同意”的要求，“步入”行为已经无法满足现有的合规标准；而企业如何在无人零售场景下完成“单独告知+明示同意”则需要进一步探讨。

与线下刷脸支付相类似的是，无人零售的场景下，消费者往往需要事先下载APP或在其他移动终端注册为相应的会员客户[31]，在这一过程中，企业可以考虑通过单独的《无人零售服务协议》、《无人零售个人信息保护政策》等方式就人脸数据的采集、使用和存储等内容进行单独告知，并要求用户勾选同意。但不同于实践中线下刷脸支付场景中，用户通常会有在多种支付方式中“主动选择”的行为；鉴于消费者在“步入”无人零售店时可能更难被认定为“明示同意”，也更难被用于实现业务开通与信息收集时的告知同意跨越与迁移。对此我们理解，Amazon Go的模式可以提供一些借鉴。即通过设置特定的闸机门或设置其他权限准入机制，为用户提供主动选择和再次表达“同意”的机会，以Amazon Go模式而言，用户在打开App，并将其置于闸机验证时，其行为具有主动性并能够在一定程度上表达自我意愿；同时为进一步加强对用户告知的适时性，还可以考虑通过闸机上的显示屏对进入人脸数据采集区域进行再次提示。

如果认为无人零售的价值仅仅在于缩短用户的单次购物时间，只怕是小觑了智慧零售的商业模式。除了采集人脸数据用于识别消费者的单次购物情况并作为支付结算的依据，智慧零售的智慧更多体现在对消费者行为数据的挖掘与整合，实现线上线下数据的打通[32]。人脸识别系统除了能够识别和提取消费者的面部特征，还可能基于面部特征对消费者的性别、年龄、表情、欢乐度等进行分析[33]，并用于向消费者进行精准推荐，无论是通过店员等人为推荐抑或是在无人零售场景下通过终端优惠券的分发实现推荐行为。在享受便利的同时，问题则在于，这些属性的提取与分析以及后续的使用行为是否已经超过了必要原则的限制，如果是以分发优惠券为目的，是否能够增强这一场景下的人脸数据收集必要性；前述的告知与同意又是否能延及精准推荐与营销之范围？此外，在熟客营销环节，往往还需要涉及人脸数据的回传[34]，前端或系统内的展示[35]及与其他数据的融合，在这一过程中，应当对人脸数据进行怎样的处理？其中不同主体对人脸数据的获取与使用边界如何确定？也是人脸识别在智慧零售场景下引发广泛关注的议题。

3. N:N人脸识别模式下：公权力与私权利的平衡问题

N:N人脸识别的应用场景主要为公共安防、天网系统等。比如公共场所动态监控、缉拿逃犯、人员布控等就是典型的运用N:N人脸识别模式。N:N人脸识别模式下的人脸数据处理，往往存在公共利益与个人数据主体权益间的博弈。

（1）N:N人脸识别模式下的最小化原则应用

面部识别特征作为生物识别特征的一种，在涉及国家安全，如反恐等场景中具有广泛的应用。2019年4月，欧洲议会投票同意建立一个包含公民“身份信息（姓名、出生日期、护照号码和其他身份信息）和生物特征信息（指纹和面部图像）”的“通用身份资源库（CIR）”并向所有边境和执法部门开放，以实现更高效的出入境控制、追踪移民和犯罪分子[36]。而我国的《反恐怖主义法》第五十条则规定，公安机关在调查恐怖活动嫌疑时，可以依照有关法律提取或采集肖像等人体生物识别信息。

---

[30] 类似地，可参考欧盟《基于视频设备的个人数据处理指南（征求意见稿）》（Guidelines 3/2019 on processing of personal data through video devices (version for public consultation)）中将数据主体的预期作为利益衡量中的考虑因素之一（第3.1.3项）。例如，银行客户在银行内或自动取款机前，应当可以预见其可能处于被监控的状态，而大多数情况下员工在办公场所可能不会被认定为有监控的预期。

[31] 如所有首次进入苏宁无人店的用户“在进店前……需通过苏宁金融APP绑定人脸和银行卡，……刷脸进店”，参见：苏宁将在全国新开20家“无人超市”：人脸识别/RFID/大数据技术加持[EB/OL]. https://mp.weixin.qq.com/s/kJK3SaZBXf-EF-xBVL0l9A. 2017-09-27；此外，顾客在进入亚马逊无人超市前，也需要“下载Amazon Go应用软件，登录自己的亚马逊账号并绑定一张银行卡”，参见：邢逸帆. 亚马逊无人超市开业了，我在里面“偷”了样东西[EB/OL]. https://mp.weixin.qq.com/s/SZidR-lUnL0KWlXJyoumLg. 2018-11-08.

[32] 零售门店使用人脸识别技术的主要法律问题[EB/OL]. https://www.secrss.com/articles/16289. 2019-12-30.

[33] 何智翔，杨睿昕. 新零售下的精准营销利器：人脸属性识别[EB/OL]. https://www.infoq.cn/article/lcy2xDV*161RgvBmj9HY. 2019-06-24.

[34] 零售门店使用人脸识别技术的主要法律问题[EB/OL]. https://www.secrss.com/articles/16289. 2019-12-30.

[35] 如以原始人脸图片信息的形式展现在店员PAD上。参见：零售门店使用人脸识别技术的主要法律问题[EB/OL]. https://www.secrss.com/articles/16289. 2019-12-30.

[36] AI时代 国外生物识别领域新进展有哪些[EB/OL]. 转引自http://ai.qianjia.com/html/2019-09/23_350804.html. 2019-09-23.

我们理解，在这类场景下人脸数据的采集和使用与保障国家安全有着密切的联系，并且往往有相应的法律法规为人脸数据的采集和使用提供合法性基础。但另一方面为保障国家安全采集人脸数据并不等同于漠视隐私、肖像和个人信息的正当权益，2018年6月，联合国在考虑保护隐私和个人数据需要的基础上发布了《联合国关于反恐斗争中负责任地使用与分享生物识别技术的建议实践概要》，就在反恐场景下收集生物识别数据（包括人脸数据）的实践提出了建议[37]；欧盟在2019年最终出台的针对出入境系统使用生物识别技术的指南[38]中将采集指纹的个数从最初版本中的10 降低到了4，其反映的正是在保障国家安全同时兼顾个体隐私和个人信息权益的逻辑，尽量将生物识别特征的采集限定在必要范围内。

就我国目前的实践而言，我们建议在通过法律法规为与国家安全有关的人脸数据采集和使用行为构建合法性的同时，也需要重视对相关采集、使用和存储的技术规范和管理制度的构建，在合理范围内保障人脸主体的隐私和个人信息权益。

（2）N:N人脸识别模式下的比例性原则应用

近期，多段“抗疫情”期间无人机劝退基层群众外出或集聚的小视频在网络上走红，视频中多位群众的面部图像清晰可见，这其实是人脸数据采集和使用在社会治理中的典型应用场景。事实上，不只是疫情期间无人机巡逻的运用，在交通领域，自动识别抓拍系统被广泛应用于抓拍闯红灯的行人[39]，甚至被抓拍的高清面部图像或视频还可能在路口屏幕上滚动播放。

首先，应当肯定无论是无人机监督居民外出还是路口抓拍行人闯红灯，这些社会治理行为本身具有公共属性，与公共利益有着密切的联系。但是另一方面，这种人脸数据的采集和使用也可能对个体隐私和肖像权造成影响。举例而言，如果不考虑疫情的特殊性，带有摄像功能的无人机如果进入院落或通过玻璃拍摄到私人房间内的画面，可能会对个人的隐私造成侵害；行人闯红灯自动抓拍系统将被抓拍的高清面部图像和视频在路口屏幕上滚动播放也可能侵害了主体的社会形象，并带来负面评价；而如果视频图像可以直接或间接识别特定自然人，那么可能还存在未经个人信息主体同意收集信息，侵犯个人信息权益的风险。

在这种情况下，比例原则为公共利益、社会效率与个人权益的平衡提供了思路。在社会治理语境下，比例原则是指社会治理行为应兼顾治理目标的实现和保护相对人的权益[40]。一方面，治理者需要明确在具体的社会治理活动的目的，并在此基础上评估人脸数据的采集和使用对实现该目的是否必要，所谓必要并非要求人脸数据采集是实现相应目的的唯一手段，而是指采用其他替代手段可能会导致目的无法实质完成或效率的显著下降；而在此基础上，还需要进一步考虑人脸数据采集可能给个人主体造成的权益损害，包括受损害权益的性质及程度，以寻得合理的边界。举例而言，这种平衡可能体现在对包含人脸的视频图像存储时间的严格限制。例如欧盟在《基于视频设备的个人数据处理指南（征求意见稿）》[41]规定，通过视频设备采集的个人数据应当在处理个人数据的目的实现后立即删除，通常为保护个人财产安全、收集民事诉讼证据等目的而录制的视频监控图像，能够在1-2天内实现相应目的；如果该视频的存储期限超过72小时，则需要提供更多论证以证明目的合法性和存储的必要性[42]。

（3）N:N人脸识别模式下的公权力对于人脸识别信息使用用途的变更限制

除此之外，“目的变更”也可能为社会治理中人脸数据的超范围使用的规制提供另一种规制路径。在《基于视频设备的个人数据处理指南（征求意见稿）》[43]中，EDPB列举了“安装在停车场围栏以分辨确认损失的视频监控录像因纯娱乐目的在网上发布”的事例，并指出在这种情况下目的已经发生变更。类似地，

[37] AI时代 国外生物识别领域新进展有哪些[EB/OL]. 转引自http://ai.qianjia.com/html/2019-09/23_350804.html. 2019-09-23.

[38] "Specifications for the biometrics used in its Entry/Exit System (EES)" please see Burt, C. EU Sets Biometric Standards for Entry/Exit System [EB/OL]. https://www.biometricupdate.com/201903/eu-sets-biometric-standards-for-entry-exit-system. 2019-05-27.

[39] 如闯红灯抓拍系统可以人脸识别了！http://news.sina.com.cn/c/2017-09-25/doc-ifymenmt6667690.shtml. 2017-09-25. 行人闯红灯自动识别抓拍系统亮相石家庄. http://www.wenming.cn/jwmsxf_294/wmjtx/gddt/201409/t20140928_2206604.shtml. 2014-09-28.等

[40] 吴灿林. 浅谈行政法中的比例原则[EB/OL]. https://www.chinacourt.org/article/detail/2013/11/id/1125301.shtml. 2013-11-11.

[41] EDPB Plenary meeting, Guidelines on Processing of Personal Data through Video Devices (Version for Public Consultation), 2019-07-10.

[42] Whether the personal data is necessary to store or not, should be controlled within a narrow timeline. In general, legitimate purposes for video surveillance are often property protection or preservation of evidence. Usually damages that occurred can be recognized within one or two days. Taking into consideration the principles of Article 5 (1) (c) and (e) GDPR, namely data minimization and storage limitation, the personal data should in most cases (e.g. for the purpose of detecting vandalism) be erased, ideally automatically, after a few days. The longer the storage period is set (especially when beyond 72 hours), the more argumentation for the legitimacy of the purpose and the necessity of storage has to be provided.

[43] EDPB Plenary meeting, Guidelines on Processing of Personal Data through Video Devices (Version for Public Consultation), 2019-07-10.

行人闯红灯抓拍系统的目的本是为了发现违反道路交通法规的行为并根据法律法规进行适当的处罚和教育；但是将闯红灯的片段在路口屏幕上滚动播放并非是法定的惩戒措施，更多是通过曝光的行为引发道德上的压力，而且还可能演变为“娱乐”目的；因此对这种行为是否可以通过“目的变更”加以限制和规范，同样是值得讨论的问题。

（二）不以识别或验证为目的的人脸信息处理

在一些不以识别特定个人的场合中，视频监控、高清摄像机等的使用同样可能会采集人脸图像信息，例如，在自动驾驶领域，应用毫米波雷达、 激光雷达、超声波雷达和/或摄像头实现环境感知和动态物体监测是主流方式[44]，区别于车内摄像头使用人脸识别技术完成驾驶员身份验证、状态监测等功能[45]，以外环境感知为目的的摄像头图像采集并不以识别特定个人为目的，而主要用于识别车辆、行人、车道线、交通标志等图像[46]，在这种情况下人脸图像是否需要受制于人脸数据的相关规范呢？答案可能是肯定的。

其原因在于，尽管在自动驾驶的外环境感知等场景下，含有人脸的图像采集的目的并非是识别图像所关联的特定个人，但是考虑到随着摄像、视频设备的发展，高清的人脸图像使得图像所有者基于该视频影像识别或关联到特定个人成为可能，在此情况下，仅以视频图像的采集目的为由否认人脸数据收集的事实，可能并不具有正当性。类似地，欧盟在《基于视频设备的个人数据处理指南（征求意见稿）》中也指出，“通过视觉或试听系统对某一区域进行自动化监控，……将会收集并保留所有进入监控区域的个人的视觉或视听信息，并能够基于其外表或其他具体因素而识别特定个人，并使得进一步处理相应个人在特定区域的外表与行为等个人数据成为可能”[47]。而当数据处理与特定个人无关，例如无法直接或间接识别特定个人时，视频数据处理不适用于《通用数据保护条例》（“GDPR”）。**因此，在某些人脸图像收集场景中，尽管收集行为本身并不以识别特定个人为目的，如果基于收集的图像能够客观上识别特定个人，则仍然可能需要受到人脸数据的相关规范与限制。**

四、总结

在人脸识别技术不断发展，遍地开花的今天，我们的脸被赋予了更多的内涵与价值，但同时也正面临泄露与滥用的风险。传统的肖像权、隐私权保护模式正受到挑战，个人信息保护成为目前人脸最主要的保护路径。如何在不侵犯人脸数据主体权利的前提下，合法合规地采集并使用人脸数据，正成为各行各业密切关注的话题。从前述场景化分析中不难看出，探究人脸数据采集、使用的权利边界是一个动态的利益衡量过程，可能因不同的数据采集场景、采集和使用方式及目的而产生较大的差异。总体而言，我们对人脸数据采集和使用权利边界的探讨需要：

- 利益衡量要以厘清具体场景下的人脸属性、不同主体的权益为前提；
- 在基于国家安全、社会公共利益等目的采集和使用人脸数据时，遵循比例原则，从采集的范围、保存期限和存储安全性、使用用途的限制等方面进行约束，以兼顾个人隐私、肖像及个人信息权益；
- 在商业化的利用场景中，在保障个人主体权益的同时正视企业在交易行为中的合法权益，平衡人脸数据作为人脸的人格属性和作为数据的财产属性；
- 坚守对人脸数据的保护底线，人脸数据作为与个人主体密切关联的数据，有强烈的人格表征，应当认为对于主体在人脸数据中的某些权益是不可让渡的。

我们期待着未来在实践和立法层面对人脸数据采集、使用边界的进一步探讨和明确，在保护个人权益的前提下，综合考量个人、社会、产业的不同诉求，促进相关产业健康发展[48]，让“人面不知何处去”的担忧，变成“人面桃花相映红”的安心。

（本文发布于2020年03月14日。）

[44] Challey. 自动驾驶的眼睛：激光、毫米波雷达&摄像头三种技术产品之比较[EB/OL]. https://www.eet-china.com/robotics/2777.html. 2019-08-14.

[45] 李玓. 面向智能驾舱的人脸识别技术发展现状及趋势[EB/OL]. http://www.autoinfo.org.cn/autoinfo_cn/content/news/20191012/1843693.html. 2019-12-10.

[46] Challey. 自动驾驶的眼睛：激光、毫米波雷达&摄像头三种技术产品之比较[EB/OL]. https://www.eet-china.com/robotics/2777.html. 2019-08-14.

[47] "systematic automated monitoring of a specific space by optical or audio-visual means… This activity brings about collection and retention of pictorial or audio-visual information on all persons entering the monitored space that are identifiable on basis of their looks or other specific elements. Identity of these persons may be established on grounds of these details. It also enables further processing of personal data as to the persons´ presence and behaviour in the given space"

[48] 喻思南. 数字时代如何保护个人信息 [EB/OL]. http://paper.people.com.cn/rmrb/html/2019-10/16/nw.D110000renmrb_20191016_2-05.htm.

大一统而慎始也
——新型信用监管机制问答

一、背景

2019年7月9日，国务院办公厅发布了《关于加快推进社会信用体系建设构建以信用为基础的新型监管机制的指导意见》（“**《意见》**”）。《意见》以“提升监管能力和水平、规范市场秩序、优化营商环境、推动高质量发展”[1]为目标，建立健全了衔接事前、事中、事后全监管环节，强化以“互联网+监管”为支撑保障的新型监管机制。为信用监管的发展指明了方向。具体而言，信用监管制度包括：

环节	监管机制	责任部门
事前	建立健全信用承诺制度	各地区各部门按职责分别负责
	探索开展经营者准入前诚信教育	各地区各部门按职责分别负责
	积极拓展信用报告应用	发展改革委、人民银行牵头，各地区各部门按职责分别负责
事中	全面建立市场主体信用记录	依据不同事项分别由各地区各部门按职责分别负责或者发展改革委、市场监管总局负责
	建立健全信用信息自愿注册机制	发展改革委牵头，各部门按职责分别负责
	深入开展**公共信用综合评价**∗	发展改革委牵头，各部门按职责分别负责
	大力推进**信用分级分类监管**∗	各地区各部门按职责分别负责
事后	健全**失信联合惩戒对象认定机制**∗	各部门按职责分别负责
	督促失信市场主体限期整改	各部门按职责分别负责
	深入开展失信联合惩戒	发展改革委牵头，各地区各部门按职责分别负责
	坚决依法依规实行市场和行业进入措施	发展改革委牵头，各地区各部门按职责分别负责
	依法追究违法失信责任	各地区各部门按职责分别负责
	探索建立信用修复机制	发展改革委牵头，各地区各部门按职责分别负责

社会信用体系涉及的部门较多，各个行业及地方的监管体系正在逐步建立，我们总结了部分重点行业相关的法规及规章，也将进一步跟踪社会信用体系的构建和监管发展。

下面我们将选取部分可能对企业影响较大的**信用监管制度**（以上“∗”标注），即公共信用综合评价机制、信用分级分类监管制度、失信名单制度，和为信用监管提供重要支撑保障的“互联网+监管”系统进行重点分析，包括未来这些信用监管机制将如何运行、可能对企业经营产生的影响，以及企业防范信用监管体制下合规风险的建议。

[1]《意见》第一条。

二、整体介绍

（一）社会信用体系的主要负责机构有哪些?

根据《意见》内容，信用监管机构包括中央及各地区各部门相关监管机构。对于其中一些重大制度及事项，国家发展和改革委员会（“发改委”）、国家市场监督管理总局（“市场监管总局”）、中国人民银行可能牵头负责。

（二）所有企业是否都需要考虑新型信用监管的规定?

我们建议企业审慎评估和考虑新型信用监管的规定。

首先，新型信用监管机制中涉及行业广泛，其中某些制度可能覆盖所有市场主体。例如，根据《意见》要求，政府有关机构要及时、准确、全面记录市场主体信用行为，失信记录建档留痕。同时《意见》还要求发改委牵头开展对市场主体全覆盖的公共信用综合评价。对于这些制度，企业可能无法主动退出监管领域。

其次，新型信用监管机制可能对企业产生广泛的影响。建立全面的信用记录并深化信用评价的共享和公开公示，扩大信用报告在市场活动中的应用种种举措都意味着企业的信用记录和评价结果可能会产生跨区域、跨行业、跨领域的影响。

最后，新型信用监管机制通过信用分级分类监管、信用承诺、失信联合惩戒等制度强化了信用激励，同时也提高了企业的失信成本。信用评级高的企业和失信企业可能面临的监管强度、市场条件都会产生显著差异。

因此，审慎评估和考虑新型信用监管的规定、积极参与和利用新型信用监管制度、赢取竞争优势，对企业有益无害。

三、公共信用综合评价制度

公共信用综合评价是由发改委牵头负责的，通过整合各类信息对市场主体进行的全覆盖、标准化、公益性的信用评价的制度。[2]公共信用综合评价制度是本次《意见》的重点关注问题之一，其评价结果同时也是信用分级分类监管的重要依据。

（一）监管机构可能收集哪些信息用于开展公共信用综合评价?

新型信用监管体制下，监管机构可能收集企业的司法涉诉、违约失信、违规经营、企业获得的资质许可、荣誉奖励、社会责任履行状况、监管部门评级结果和第三方评级结果等信息[3]用于开展公共信用综合评价信息。

上述信息可能来源于：[4]

- 全国信用信息共享平台**归集**的公共信用信息；
- 政府部门和行业协会**公示**的信用信息；以及
- **互联网披露**的由政府部门介入处理的重大失信舆情事件等。

需要提示的是，信用中国[5]公开的信用信息仅为全国信用信息共享平台归集信息的一部分，企业未公开在信用中国网站但已经为政府所掌握的公共信用信息同样会被应用于公共信用综合评价。

（二）公共信用综合评价的结果如何确定，以及类型有哪些?

公共信用综合评估的结果分为优、良、中、差四个等级，具体评价结果的分析标准尚不清楚。

截至7月底，发改委已经组织国家公共信用信息中心、第三方机构对3300多万家市场主体完成了公共信用综合评价工作。企业如果有失信、税收违法、或统计等领域较严重情形的失信行为、在近一年受到多次行政处罚、违法违规、或负面失信记录较多，被列为“差”级企业的可能性将增大。[6]

值得注意的是，除评级结果以外，从透明度出发，企业可能更为关心的信用信息是否会被量化、以及不同来源信用评价在公共信用综合评价结果中占比以及最终评级结果的统计原理目前尚未有明确解释。

（三）公共信用综合评价结果会被如何利用?

公共信用综合评价结果可能会向社会公开或用于查询、为政府实行分级分类监管提供参考，同时还可能影响企业的市场行为如贷款融资等。

---

[2]《意见》第三条第（六）项。

[3]“（公共信用综合）评价重点围绕受评主体的公共诚信状况和市场信用状况两大方面，根据企业的司法涉诉、违约失信、违规经营等情况，企业获得的资质许可、荣誉奖励，以及社会责任履行情况、监管部门和第三方评级结果等信息进行客观、综合评价。”载https://www.creditchina.gov.cn/xinxigongshi/strqqy/201901/t20190107_142922.html。

[4]“数据主要来源于全国信用信息共享平台归集的公共信用信息，政府部门和行业协会公示的信用信息，以及互联网披露的由政府部门介入处理的重大失信舆情事件等。”载https://www.creditchina.gov.cn/xinxigongshi/strqqy/201901/t20190107_142922.html。

[5]信用中国（CREDITCHINA.GOV.CN）是全国信用信息共享平台的门户网站，主要承担社会信用体系下的信用信息社会公开职能。

[6]“‘差’级企业主要失信事实包括被列为失信被执行人、严重税收违法案件当事人、统计上严重失信企业等较严重情形的失信行为，以及近一年内多次受到行政处罚、违法违规，负面失信记录较多等情形。”载https://www.creditchina.gov.cn/xinxigongshi/strqqy/201906/t20190620_159295.html。

第一，部分公共信用评价结果可能会依据特定规则在信用中国平台上公开。目前，平台会主动公开评级为“优”和两次以上评价结果为“差”的企业名单；其他的评级结果将会逐步开放自查询。[7]

第二，评价结果可能为政府实行分级分类监管提供参考。尽管目前评级为“良”、“中”和单次评级为“差”的企业名单并不会在信用中国网站上公开，但仍然会在政府内部共享，[8]为政府开展分级分类监管提供参考。

第三，公共信用综合评价结果还可能影响企业的市场行为。根据《意见》规定，评价结果还将定期被推送至金融机构、行业协会商会参考使用。[9]例如，在金融机构提供贷款融资等服务时，可能会考虑评价结果，因此企业的融资能力可能受到影响。

四、信用分级分类监管制度

信用分级分类监管是指各地区各部门以公共信用综合评价结果、行业信用评价结果等为依据，对监管对象进行分级分类，根据信用等级高低采取差异化的监管措施。[10]信用分级分类监管是实现事中环节监管的重要手段。

（一）公共信用综合评价结果是否是信用分级分类监管的唯一依据？

尽管公共信用综合评价是信用分级分类监管的重要依据，但并非唯一依据。

除公共信用综合评价外，信用分级分类监管还可能考虑行业信用评价结果、第三方机构信用评价结果等。[11]其中行业信用评价是指由行业协会商会依照法律法规和章程独立开展的、会员企业自愿参与的信用评价工作；[12]而第三方机构信用评价则是由经发改委审核确定的26家综合信用服务试点机构[13]开展的信用评价工作。不同于公共信用综合评价，行业信用评价和第三方机构信用评价是市场化的信用服务，[14]企业在选择是否开展相关信用评价问题上可能会有更大的自主权。

（二）信用分级分类监管是否会加重企业负担？

信用分级分类监管尽管可能会加重失信企业的负担，但也有助于降低信用良好企业的经营成本。

信用分级分类监管并非是单纯的失信惩戒，而是以信用评价结果为依据，实施差异化监管。如将信用情况与监管抽查的比例和频次挂钩，[15]合理降低信用较好的企业抽查比例和频次，提高违法失信企业抽查比例和频次。以海关信用监管为例，2018年海关对高级认证企业进出口货物查验率约为0.52%，比一般信用企业低80%，而失信企业的查验率接近100%。[16]

五、失信名单制度

目前，失信名单主要包括严重违法失信名单和失信联合惩戒对象名单。严重违法失信名单是指，市场监督管理总局在国家企业信用信息公示系统中公示的严重违法失信行为企业名单。[17]失

---

[7] “‘信用中国’网站按期更新和发布评价结果为‘优’级的企业名单，并逐步对评价结果为‘良’‘中’级的企业开放自查询；被评为‘差’级的企业第一次由企业限期自我整改，连续两次及以上评价结果为‘差’级的企业名单即行公示。”载https://www.creditchina.gov.cn/xinxigongshi/strqqy/201906/t20190620_159295.html。

[8] “深入开展公共信用综合评价。……定期将评价结果推送至相关政府部门……参考使用……推动相关部门利用公共信用综合评价结果。”《意见》第三条第（六）项；“以公共信用综合评价结果、行业信用评价结果等为依据，对监管对象进行分级分类。”《意见》第三条第（七）项。

[9] “深入开展公共信用综合评价。……定期将评价结果推送至……金融机构、行业协会商会参考使用。”《意见》第三条第（六）项。

[10] 《意见》第三条第（七）项。

[11] “大力推进信用分级分类监管。……以公共信用综合评价结果、行业信用评价结果等为依据，对监管对象进行分级分类。”《意见》第三条第（七）项。

[12] 《关于进一步做好行业信用评价工作的意见》，商务部、国务院国有资产监督管理委员会，2015年8月5日。

[13] 《国家发展改革委办公厅关于推动开展综合信用服务机构试点工作的通知》，国家发展和改革委员会，2018年10月29日；关于综合信用服务机构试点单位的公示，载http://www.ndrc.gov.cn/gzdt/201810/t20181017_916592.html。

[14] “探索开展市场化信用服务。”《关于进一步做好行业信用评价工作的意见》第一条第（二）项；“加快形成市场化信用服务与公共性信用服务互为补充……的多层次信用服务体系。发挥信用服务机构的作用……为推动社会信用体系建设提供市场化、专业化力量支持。”《国家发展改革委办公厅关于充分发挥信用服务机构作用加快推进社会信用体系建设的通知》，国家发展和改革委员会，2018年2月2日。

[15] 《意见》第（七）条。

[16] 《打造信用监管模式，提高海关监管效能》，信用中国，载https://mp.weixin.qq.com/s?src=11&timestamp=1599013393&ver=2559&signature=7nLbVVyjnsFZBn0uZisHR2ZIlSLPZLDeeNc3CqKJsZyzI2FajI2rK1Z0oTVRP5O4L3pLP8Z8CfHUfgZUJc51Q7ZOuEjU59uUycFMKTWpF4KTxw5Ut9qzbG2P9RjqYgAS&new=1，2019年7月2日。

信联合惩戒对象名单是指，目前在信用中国网站公示公告的各行业监管部门认定的失信情况严重，除本部门惩戒以外，还可能受到国家层面已经签署联合惩戒备忘录的其他业务部门惩罚的对象名单。[18]

（一）企业被纳入失信名单将会面临怎样的后果？

企业被列入失信名单不仅会使企业面临失信惩戒，还可能使法定代表人或负责人面临失信惩戒。

具体而言，被列入相应失信名单的企业可能会面临：

- 行业或市场限制、禁入；
- 重点监管并增加监督检查；
- 剥夺荣誉称号、优惠政策资质；
- 不得获得相关认证；[19]
- 限制取得政府供应土地；[20]
- 一定期限内依法限制参加政府采购；[21]
- 暂停审批科技项目；[22]
- 限制取得生产许可或特许经营资质[23]等失信惩戒措施。

同时，被列入相应失信名单的企业的法定代表人、负责人可能面临吊销个人资质证件（如执业医师注册证）、禁止担任其他企业的法定代表人、负责人；[24]限制在法定期间从事相关行业生产经营活动[25]等惩罚。

（二）企业被纳入失信名单后应该如何应对？

企业被纳入失信名单后，应当及时采取相应的信用修复措施，包括做出信用承诺、完成信用整改、通过信用核查、接受专题培训、提交信用报告、参加公益慈善活动等。对于无法适用信用修复机制的情形，也建议提升合规水平、避免在失信联合惩戒解除后重蹈覆辙。

目前市场监管总局在《严重违法失信名单（修订草案征求意见稿）》第六章规定了信用修复的内容，同时信用中国网站上也提供了信用修复指南等信息。[26]但是，信用修复机制整体仍在探索之中，对于企业具体如何开展信用修复、信用修复完成后的相应制度[27]等问题还需要更清晰的规范指引。值得注意的是，对于特别严重的违法失信行为，企业可能无法通过信用修复退出失信名单，不能解除失信联合惩戒、不能结束失信信息公示，失信记录会长期依法依规予以保留。[28]

六、“互联网+监管”的支撑保障机制

（一）“互联网+监管”系统将如何影响对企业的信用监管？

“互联网+监管”系统下，非接触式监管比例上升，监管机构能够更加精准地发现识别行业风险和违法违规线索，实现对信用风险的预判预警。

---

[17] 符合市场监管总局发布的《严重违法失信名单管理办法（修订草案征求意见稿）》（“《严重违法失信名单（修订草案征求意见稿）》”）中列举的36种情形将会被纳入严重违法失信名单。

[18] “截至2019年8月底，各部门共签署51个联合奖惩备忘录。其中，联合惩戒备忘录43个，联合激励备忘录5个，既包括联合激励又包括联合惩戒的备忘录3个。” 涵盖知识产权（专利）、交通运输工程建设、安全生产、国内贸易流通等诸多领域。载https://www.creditchina.gov.cn/xinxigongshi/liuyuexinzeng/201909/t20190903_167476.html；未来各部门将会按职责继续建立健全失信联合惩戒对象认定及名单管理制度。《意见》第四条第（八）项。

[19] 《严重违法失信管理名单（修订草案征求意见稿）》第十四条。

[20] 《关于对重大税收违法案件当事人实施联合惩戒措施的合作备忘录（2016版）》。

[21] 《关于对海关失信企业实施联合惩戒的合作备忘录》。

[22] 《关于对海关失信企业实施联合惩戒的合作备忘录》。

[23] 《关于对安全生产领域失信生产经营单位及其有关人员开展联合惩戒的合作备忘录》。

[24] 《严重违法失信管理名单（修订草案征求意见稿）》第十四条第（十）项、第十七条。

[25] 《失信企业协同监管和联合惩戒合作备忘录》。

[26] https://www.creditchina.gov.cn/xyxf/lczy/；2019年7月2日，“信用中国”平台发布了《关于发布可承担信用修复专题培训任务的信用服务机构名单（第一批）的公告》，载https://www.creditchina.gov.cn/toutiaoxinwen/201907/t20190702_160567.html；《关于发布可为信用修复申请人出具信用报告的信用服务机构名单（第一批）的公告》。载https://www.creditchina.gov.cn/toutiaoxinwen/201907/t20190702_160566.html。

[27] 《意见》第四条第（十三）项。

[28] 《加快推进社会信用体系建设构建以信用为基础新型监管机制吹风会图文实录》，国务院新闻办公室，载http://www.scio.gov.cn/32344/32345/39620/41042/tw41044/Document/1659716/1659716.htm，2019年7月18日。

《意见》鼓励通过物联网、视联网等非接触式监管方式[29]提升执法监管效率。一方面，非接触式监管比例的上升将有助于减少线下检查对企业生产经营产生的干扰；另一方面，也会降低企业对监管行为的感知，这意味着以“表面工程”或“针对性迎接抽查”的理念开展企业日常经营活动不再可行，企业必须在日常经营的每一环节中切实遵守监管要求。

不同于传统监管主要关注企业已经发生的违法违规行为，大数据手段的运用提高了监管机构预判风险的能力，[30]通过信息监测、在线证据保全、在线识别、源头追溯等功能，监管机构能够更精准地发现识别行业风险和违法违规线索。这意味着，企业不仅可能因实际已经发生的违法违规行为而受到惩处，还可能因潜在的违规风险而收到监管机关的警示或约谈，换言之企业不能仅仅满足于不违法不违规，而需要进一步提升合规水准。

七、企业合规建议

新型信用监管制度的落地，对企业既是机遇也是挑战。结合新型信用监管模式的具体制度，我们谨向企业提供以下合规建议，以帮助企业应对可能出现的情形，防范风险、把握机遇。

- 其一，新型信用监管制度目前仍在建设中，相关的制度规范仍需进一步完善，预计未来大量的制度规范会陆续出台。**因此我们建议企业建立动态监管跟踪法律库，及时关注相关领域的立法及规范制定进展。**
- 其二，新型信用监管制度强调了信用信息的归集共享和公开，企业可能需要在保护公司信息与响应监管要求之间寻求平衡。因此，**我们建议企业关注公开平台的信用信息，对于错误或失效信息及时请求纠正或删除。同时，对于企业认为不宜公开的信息，尝试主动与有关政府部门沟通反应意见和诉求，共同探讨合理合法的信用信息共享、整合和公开范围。**
- 其三，信用分级分类监管、失信联合惩戒对象名单等制度使得新型信用监管体系下企业的失信成本大幅增加，“监管长出了‘牙齿’”[31]。**我们建议企业在事前环节充分了解信用规范及要求，遵守信用承诺，防范失信风险；在事中环节积极主动参与公共及市场信用服务，争取信用高分；在事后环节对于已经产生或不可避免的失信后果，关注信用修复制度，依据监管要求进行失信整改，避免损失扩大。**
- 其四，“互联网+监管”模式的落实有效提升了监管机构对企业监管的有效性和全面性。**我们建议企业严格遵守监管机构的相关规定，不抱侥幸心理、不做表面工程，全面提升日常经营活动的合规水平、切实降低法律风险。**

（本文发布于2019年10月16日。）

[29]《意见》第五条第（十六）项。

[30]《意见》第五条第（十六）项。

[31]《加快推进社会信用体系建设构建以信用为基础新型监管机制吹风会图文实录》，国务院新闻办公室，http://www.scio.gov.cn/32344/32345/39620/41042/tw41044/Document/1659716/1659，2019年7月18日。

“以人为本”
——聚焦央行消费者金融信息保护新规

近来，金融领域个人信息保护的立法、规范推进工作又有新的进展。继今年2月中国人民银行（**“央行”**）发布行业标准《个人金融信息保护技术规范》（JR/T 0171—2020）后，央行又于近日正式颁布了《中国人民银行金融消费者权益保护实施办法》（**“《2020年实施办法》”**）。《2020年实施办法》将于2020年11月1日生效，代替央行此前颁布的《中国人民银行金融消费权益保护工作管理办法（试行）》与《中国人民银行金融消费者权益保护实施办法》（**“《2016年实施办法》”**）。相较于此前两项规范性文件，《2020年实施办法》以中国人民银行令形式颁布，在《2016年实施办法》的基础上升格为部门规章，提升了保护金融消费者权益专门文件的法律效力位阶，有利于进一步规范银行、支付机构的经营行为。

从条款内容上看，《2020年实施办法》延续了《2016年实施办法》的基本体例，对金融机构在金融消费者权益保护层面的行为规范、消费者金融信息进行了专章规定。以下我们将重点考察《2020年实施办法》在金融消费者信息保护规则方面的新变化，探讨银行金融领域消费者个人信息保护的规范趋势。

一、《2020年实施办法》适用于哪些主体?

相对于《2016年实施办法》提到的银行业金融机构、非银行支付机构及“提供跨市场、跨行业交叉性金融产品和服务的其他金融机构”，《2020年实施办法》对其直接适用主体进行了限定，主要包含银行业金融机构以及非银行支付机构两类主体，并明确了银行业金融机构具体涉及的业务场景。[1]

参照适用主体上，《2020年实施办法》在《2016年实施办法》提到的征信机构基础上，增加了**商业银行理财子公司、金融资产管理公司、信托公司、汽车金融公司、消费金融公司、个人本外币兑换特许业务经营机构**。这一规定打消了此前对于“跨市场、跨行业交叉性金融产品和服务的其他金融机构”如何理解，以及证券公司、保险公司等金融机构是否适用《2016年实施办法》的争议与顾虑，而对于汽车金融公司、信托公司等非银行金融机构，在参照适用《2020年实施办法》的规定上也有了更加明确的依据。

二、如何理解“消费者金融信息”的概念?

在了解“消费者金融信息”之前，有必要对“金融消费者”的概念进行明确。《2020年实施办法》延续了《2016年实施办法》的定义，即“购买、使用银行、支付机构提供的金融产品或者服务的自然人”。而对于消费者金融信息，《2020年实施办法》第二十八条将其定义为“银行、支付机构通过开展业务或者其他合法渠道处理的消费者信息，包括个人身份信息、财产信息、账户信息、信用信息、金融交易信息及其他与特定消费者购买、使用金融产品或者服务相关的信息。”结合“金融消费者”的概念，我们理解《2020年实施办法》所提到的“消费者金融信息”将更多指向直接购买、使用金融产品或服务的自然人消费者，这相比于《2016年实施办法》中“个人金融信息”的定义可能存在细微差异。

《2016年实施办法》将“个人金融信息”定义为“金融机构

[1] 根据《2020年实施办法》第二条，具体的业务场景包括：（一）与利率管理相关的；（二）与人民币管理相关的；（三）与外汇管理相关的；（四）与黄金市场管理相关的；（五）与国库管理相关的；（六）与支付、清算管理相关的；（七）与反洗钱管理相关的。（八）与征信管理相关的；（九）与上述第一项至第八项业务相关的金融营销宣传和消费者金融信息保护；（十）其他法律、行政法规规定的中国人民银行职责范围内的金融消费者权益保护工作。

通过开展业务或者其他渠道获取、加工和保存的个人信息，包括个人身份信息、财产信息、账户信息、信用信息、金融交易信息及其他反映特定个人某些情况的信息。”该定义一定程度上将非自然人消费者购买、使用金融产品或服务场景下的个人信息也囊括其中，例如企业/机构客户场景下收集的企业联系人信息、高管信息等。相比之下，《2020年实施办法》将所保护的信息与“消费者”相关联，这是否意味着《2020年实施办法》在消费者金融信息保护层面排除了机构客户场景下个人信息处理的适用，有待进一步明确。

三、《2020年实施办法》在消费者金融信息保护规则上有什么新变化?

总体上，《2020年实施办法》对于消费者金融信息保护的规则更为全面，一方面从立法技术上将消费者金融信息的收集、存储、使用、加工、传输、提供、公开合并为“消费者金融信息处理”，统一作为消费者金融信息保护规则的约束行为，另一方面结合一般消费领域的消费者权益保护机制和一般个人信息保护规则，对金融行业涉及的消费者信息及相关权益保护提出了要求，并对有关的罚则进行了明确。

（一）消费者金融信息保护层面的“知情权”保障

《2020年实施办法》在一般性的合法、正当、必要的收集原则基础上，强调银行、支付机构应当征得金融消费者或其监护人**明示同意**，并列举了违反消费者明示同意原则的具体情形进行说明，例如变相强制收集消费者金融信息，不同意提供金融信息即拒绝提供金融产品等。相较于《网络安全法》体系下，收集个人信息一般要求征得个人信息主体**同意**，收集个人敏感信息要求征得个人信息主体**明示同意**的规则，《2020年实施办法》对征得金融消费者同意义务的设置更为严格，一定程度上反映金融领域个人信息的敏感性。同时，《2020年实施办法》也明确了“明示同意”的除外情况，即“法律、行政法规另有规定的除外”，以与其他个人信息及数据保护的既有规范进行有效衔接。

《2020年实施办法》也从保障金融消费者知情同意权利的角度，制定了银行、支付机构在金融消费者拒绝提供信息情形下的处理原则，即不得以消费者不同意为由拒绝提供金融产品或服务，但如存在金融消费者不能或拒绝提供必需信息，或者在致使银行、支付机构无法履行反洗钱义务的情况下，银行、支付机构可以适当考虑对消费者的金融活动采取限制性措施，或依法拒绝提供金融产品或服务。这一规定平衡了金融行业在保障金融交易安全和金融秩序层面的监管诉求，与银行、支付机构履行其法定反洗钱义务的要求进行了有效衔接。

此外，《2020年实施办法》延续了《网络安全法》、《消费者权益保护法》对于消费者/个人信息主体的知情权保障，要求银行、支付机构公开收集、使用消费者金融信息的规则，明示收集使用消费者信息的目的、方式和范围，并留存相关证明资料。同时，《2020年实施办法》延续并明确了使用格式条款明示金融消费者信息处理情况的可行性，也对格式条款的文本内容作出了明确要求。

（二）营销活动的特别规范

《2020年实施办法》对于银行、支付机构使用消费者金融信息进行营销活动进行了专门的要求。具体而言，银行、支付机构收集消费者金融信息用于营销、用户体验改进或者市场调查的，应确保金融消费者自主选择是否同意的权利，且不得因金融消费者不同意而拒绝向其提供产品或服务。同时，银行、支付机构也应当设置明确的退出机制，向金融消费者提供拒绝继续接收金融营销信息的方式。这一规定作为《2020年实施办法》规范银行、支付机构的营销活动的重要规则内容，构成新规中金融消费者合法权益保障的重要方面。

（三）保障消费者金融数据安全

《2020年实施办法》在原有规定的基础上，对银行、支付机构保障金融消费者信息安全层面进行了规则上的重申与发展。一方面，《2020年实施办法》强调了银行、支付机构及其工作人员对于消费者金融信息的保密义务，不得泄露或非法向他人提供，在发生信息安全事件时，《2020年实施办法》对银行、支付机构向金融消费者的告知义务、以及向央行等监管机关的报送义务进行了细化；另一方面，在消费者数据的使用、存储与保管上，要求银行、支付机构建立分级授权为核心的使用管理制度、采取技术措施和其他必要措施妥善保管消费者金融信息等。

（四）金融消费者的投诉响应

《2020年实施办法》对银行、支付机构对金融消费者权益主张的响应机制进行了规定，这对于银行、支付机构在响应消费者行使其与消费者金融信息相关的权利层面同样提供了制度保障。相较于《网络安全法》体系下，数据控制者对个人信息主体权利主张的响应方式，《2020年实施办法》要求银行、支付机构对一般金融消费者权益主张的响应方式更为多样化：例如，银行、支付机构需要按年度发布金融消费者投诉数据和相关分析报告；需要建设金融消费者投诉处理信息系统，对投诉进行正确分类并按时报送相关信息；依法或依约定告知投诉人处理情况；同时，金融消费者对于银行、支付机构不受理投诉的情形，可以向监管机关（央行分支机构）投诉与转交，监管机关需要在收到投诉之日起7日内进行处理；此外，金融消费者还可以向调解组织申请调解、中立评估等等。我们理解，《2020年实施办法》对投诉方式的创新和管理，特别是要求监管机关（央行分支机构）在前期的积极参与，将为金融消费者实现主体权利降低成本，是对现有的个人信息保护体系的有力补充。

（五）违反消费者金融信息保护规则的法律责任

《2020年实施办法》制定了单独的“法律责任”章节，明确

了违反消费者金融信息保护义务的法律后果。虽然《2016年实施办法》第四十七条规定了监管机关规制侵犯金融消费者合法权益行为的措施，但是并非专门针对侵犯消费者金融信息的情形。具体而言，根据《2020年实施办法》第六十条，违反消费者金融信息保护义务可能导致的行政责任形式包括：警告、没收违法所得、罚款、停业整顿、吊销营业执照，记入信用档案并向社会公布等；同时，第六十三条还明确侵犯金融消费者权益的重大案件适用“双罚制”，除了追究银行、支付机构责任外，还将追究对侵害金融消费者权益重大案件负有直接责任的银行、支付机构高级管理人员和其他责任人员相应的行政责任。这一点与《网络安全法》第六十四条等对违反个人信息保护行为进行处罚的思路相类似。

（六）期待信息跨境规则的进一步澄清

值得注意的是，尽管在现行规范下，《个人金融信息保护技术规范》（JR/T 0171—2020）已经设定对个人金融信息的本地化存储要求及跨境规则，《2020年实施办法》删去了《2016年实施办法》有关个人金融信息本地化存储和跨境传输限制的规则条款，预计这一调整对于实践中银行、支付机构因业务需求而须跨境传输个人金融信息适用何种规则将产生较大影响。

实际上，《网络安全法》层面对关键信息基础设施运营者的个人信息和重要数据跨境的要求，对于银行、金融业可能被认定为关键信息基础设施运营者的主体而言，也具有普遍适用的效力。但《2020年实施办法》的这一调整为未来金融行业数据跨境的立法规则预留了空间，除涉及消费者个人相关金融数据跨境需要从行业层面予以特别考虑外，《数据安全法》层面对于“重要数据”保护的制度走向，也同样会对金融行业数据保护及跨境规则产生体系化影响。

结语

《2020年实施办法》从部门规章层面，基于消费者权益保护的上位法视角，在规则上体现为银行、支付机构业务过程中对消费者权益的各方面保护，消费者金融信息保护构成其中重要一环。从个人信息及数据保护的视角出发，银行、支付机构除遵循《2020年实施办法》的要求外，也同样需要关注整体金融行业以及个人信息保护领域的一般性规定。而对于银行、支付机构以外的其他金融机构而言，可以预见的是未来也可能受制于基于金融行业细分维度的专门的信息保护规定。

但对于金融行业的各类机构而言，无论从消费者权益保护角度，还是金融消费者信息保护方面，当前的立法和监管思路都体现了“以人为本”的思路，即重视个体权利，寻求金融行业发展与个人权益的平衡。因此我们建议金融领域的各家企业，破除行业的信息壁垒，不仅加强消费者权益保护工作，更要注重个体权利实现的路径和方式，让包括消费者信息保护在内的合规及权益保护机制透明、便捷和实用。

附：金融消费者信息保护重点条款对比

《2016年实施办法》	《2020年实施办法》
第二十八条 收集个人金融信息时，应当遵循合法、合理、必要原则，按照法律法规要求和业务需要收集个人金融信息，不得收集与业务无关的信息或者采取不正当方式收集信息，不得非法存储个人金融信息；应当采取符合国家档案管理和电子数据管理规定的措施，妥善保管所收集的个人金融信息，防止信息遗失、毁损、泄露或者篡改。在发生或者可能发生个人金融信息遗失、毁损、泄露或者篡改等情况时，应当立即采取补救措施，及时告知用户并向有关主管部门报告。	第二十九条 银行、支付机构处理消费者金融信息，应当遵循合法、正当、必要原则，**经金融消费者或者其监护人明示同意**，但是法律、行政法规另有规定的除外。银行、支付机构不得收集与业务无关的消费者金融信息，不得采取不正当方式收集消费者金融信息，**不得变相强制收集消费者金融信息。银行、支付机构不得以金融消费者不同意处理其金融信息为由拒绝提供金融产品或者服务，但处理其金融信息属于提供金融产品或者服务所必需的除外。** **金融消费者不能或者拒绝提供必要信息，致使银行、支付机构无法履行反洗钱义务的，银行、支付机构可以根据《中华人民共和国反洗钱法》的相关规定对其金融活动采取限制性措施；确有必要时，银行、支付机构可以依法拒绝提供金融产品或者服务。**
第三十一条 金融机构不得将金融消费者授权或者同意其将个人金融信息用于营销、对外提供等作为与金融消费者建立业务关系的先决条件，但该业务关系的性质决定需要预先做出相关授权或者同意的除外。	第三十条 银行、支付机构收集消费者金融信息用于营销、用户体验改进或者市场调查的，应当以适当方式供金融消费者自主选择是否同意银行、支付机构将其金融信息用于上述目的；**金融消费者不同意的，银行、支付机构不得因此拒绝提供金融产品或者服务。银行、支付机构向金融消费者发送金融营销信息的，应当向其提供拒绝继续接收金融营销信息的方式。**

《2016年实施办法》	《2020年实施办法》
第三十条 金融机构通过格式条款取得个人金融信息书面使用授权或者同意的，应当在条款中明确该授权或者同意所适用的向他人提供个人金融信息的范围和具体情形，应当在协议的醒目位置使用通俗易懂的语言明确向金融消费者提示该授权或者同意的可能后果。 金融机构不得以概括授权的方式，索取与金融产品和服务无关的个人金融信息使用授权或者同意。	第三十一条 **银行、支付机构应当履行《中华人民共和国消费者权益保护法》第二十九条规定的明示义务，公开收集、使用消费者金融信息的规则，明示收集、使用消费者金融信息的目的、方式和范围，并留存有关证明资料。** 银行、支付机构通过格式条款取得消费者金融信息收集、使用同意的，应当在格式条款中明确收集消费者金融信息的目的、方式、内容和使用范围，并在协议中以显著方式尽可能通俗易懂地向金融消费者提示该同意的可能后果。
/	第三十二条 **银行、支付机构应当按照法律法规的规定和双方约定的用途使用消费者金融信息，不得超出范围使用。**
第三十二条 金融机构应当建立个人金融信息使用管理制度。因监管、审计、数据分析等原因需要使用个人金融信息数据的，应当严格内部授权审批程序，采取有效技术措施，确保信息在内部使用及对外提供等流转环节的安全，防范信息泄露风险。	第三十三条 银行、支付机构应当建立**以分级授权为核心**的消费者金融信息使用管理制度，根据消费者金融信息的重要性、敏感度及业务开展需要，在不影响本机构履行反洗钱等法定义务的前提下，**合理确定本机构工作人员调取信息的范围、权限**，严格落实信息使用授权审批程序。
第二十八条 在发生或者可能发生个人金融信息遗失、毁损、泄露或者篡改等情况时，应当立即采取补救措施，及时告知用户并向有关主管部门报告。	第三十四条 银行、支付机构应当按照**国家档案管理和电子数据管理等规定，采取技术措施和其他必要措施**，妥善保管和存储所收集的消费者金融信息，防止信息遗失、毁损、泄露或者被篡改。 银行、支付机构及其工作人员应当对消费者金融信息严格保密，不得泄露或者非法向他人提供。在确认信息发生泄露、毁损、丢失时，银行、支付机构应当立即采取补救措施；信息泄露、毁损、丢失可能危及金融消费者人身、财产安全的，**应当立即向银行、支付机构住所地的中国人民银行分支机构报告并告知金融消费者；信息泄露、毁损、丢失可能对金融消费者产生其他不利影响的，应当及时告知金融消费者，并在72小时以内报告银行、支付机构住所地的中国人民银行分支机构。中国人民银行分支机构接到报告后，视情况按照本办法第五十五条规定处理。**
第四十七条 金融机构有侵害金融消费者合法权益的违规行为的，中国人民银行及其分支机构可以采取以下措施： （一）约谈其董（理）事会或者高级管理层； （二）责令其限期整改； （三）向其上级机构、行业监管部门、行业内部、社会通报相关信息； （四）依照《中华人民共和国消费者权益保护法》以及相关法律、行政法规、规章进行处罚； （五）中国人民银行职责范围内依法可以采取的其他措施。	第六十条 银行、支付机构有下列情形之一，**侵害消费者金融信息**依法得到保护的权利的，中国人民银行或其分支机构应当在职责范围内依照**《中华人民共和国消费者权益保护法》第五十六条的规定**予以处罚： （一）未经金融消费者明示同意，收集、使用其金融信息的。 （二）收集与业务无关的消费者金融信息，或者采取不正当方式收集消费者金融信息的。 （三）未公开收集、使用消费者金融信息的规则，未明示收集、使用消费者金融信息的目的、方式和范围的。 （四）超出法律法规规定和双方约定的用途使用消费者金融信息的。 （五）未建立以分级授权为核心的消费者金融信息使用管理制度，或者未严格落实信息使用授权审批程序的。 （六）未采取技术措施和其他必要措施，导致消费者金融信息遗失、毁损、泄露或者被篡改，或者非法向他人提供的。
/	**第六十三条** **对银行、支付机构侵害金融消费者权益重大案件负有直接责任的董事、高级管理人员和其他直接责任人员，有关法律、行政法规有处罚规定的，依照其规定给予处罚；有关法律、行政法规未作处罚规定的，中国人民银行或其分支机构应当根据情形单处或者并处警告、处以五千元以上三万元以下罚款。**

（本文发布于2020年09月23日。）

问答精选
——解读《个人金融信息技术保护规范》

近年来，随着大数据产业的蓬勃发展，“金融+科技”的商业模式持续获得市场青睐。金融机构基于身份认证、反欺诈等不同需求，也促使了大数据技术在金融业务中的应用。随着金融与信息科技的不断融合，个人信息在新的金融产业链中的应用场景和流转范围逐步突破传统认知，如何在金融业新业态下保护消费者的个人信息引发立法和执法部门的关注。2019年，监管部门不仅出台一系列的政策新规，还从不同维度开展多项治理活动。其中，过去一年中对于“套路贷”、非法催收等不法行为的专项查处活动，使得个人信息保护成为金融业产业链的合规重点问题。

此前中国人民银行（以下简称**“央行”**）和我国其他的金融行业监管机构已经在不同的文件中提出过对个人金融信息保护的要求，相关文件可参考下表：

发布时间	监管文件	发布机关
2010年6月	《银行业金融机构外包风险管理指引》	中国银行业监督管理委员会（原）
2011年1月	《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》	中国人民银行
2012年3月	《中国人民银行关于金融机构进一步做好客户个人金融信息保护工作的通知》	中国人民银行
2013年8月	《银行业消费者权益保护工作指引》	中国银行业监督管理委员会（原）
2016年12月	《中国人民银行金融消费者权益保护实施办法》	中国人民银行
2018年5月	《银行业金融机构数据治理指引》	中国银行保险监督管理委员会
2019年10月	《个人金融信息（数据）保护试行办法（初稿）》	中国人民银行
2019年11月	《关于增强个人信息保护意识依法开展业务的通知》	中国互联网金融协会
2019年12月	《中国人民银行金融消费者权益保护实施办法（征求意见稿）》	中国人民银行

在上述背景下，央行和全国金融标准化技术委员会（以下简称**“金标委”**）于2月13日发布了《个人金融信息保护技术规范》（以下简称“**《规范》**”）。《规范》主要从安全技术和安全管理两个维度，对收集、传输、使用、存储、共享、删除、销毁等各环节中的个人金融信息保护提出细致的要求，结合金融行业监管的特色，亦不乏对以《网络安全法》为基础的个人信息保护法律法规体系的创新和有益探索。

从效力上看，《规范》属于推荐性行业标准，本质上属于对本行业企业在个人金融信息保护方面的建议。但在实践中，我们不排除《规范》会成为监管机构在监督检查或开展执法活动时的重要参考依据，因此，《规范》对有关企业仍然具有比较强的指导意义。

本文就将简要分析《规范》中的亮点，并以精选问答的形式探讨其对相关领域的企业可能产生的影响。

• 问题一：我的企业处理什么类型的信息需要参考《规范》的要求？

为了对个人金融信息的全生命周期环节建立安全防护规范，《规范》界定了两大核心概念：“金融业机构”与“个人金融信息”。根据《规范》的规定：

- “金融业机构”包括两类机构，一类是**由国家金融管理部门监督管理的持牌金融机构**，另一类是**涉及个人金融信息处理的相关机构**；[1]
- “个人金融信息”系指金融业机构通过提供金融产品和服务或者其他渠道获取、加工和保存的个人信息。[2]

就主体范围而言，结合金融行业的实践，我们理解，“金融业机构”在现实中除了（1）传统的持牌金融机构，还可能包括（2）为持牌金融机构业务提供基础支持服务而需要处理个人金融信息的企业，例如提供身份验证服务的电信服务商、信息技术提供商、风控服务解决方案提供商、市场营销服务提供商等。相较于对主体的概念界定，《规范》适用于**“提供金融产品和服务的金融业机构”**，这一适用范围似乎并未明确涵盖前述第（2）类机构（例如，涉及个人金融信息处理的云服务提供商）。[3]

就企业合规而言，考虑到《规范》对“金融业机构”、“个人金融信息传输的接收方”（第6.1.2条e项）、“第三方机构（包含外包服务机构与外部合作机构）（第6.1.4.4条）”等主体也设置了相应的合规义务，且从《规范》全面保护“个人金融信息”的编制目的出发，我们建议**落入“金融业机构”的企业均应参考《规范》开展合规工作，对企业运营过程中涉及个人金融信息处理的环节进行对照自查，并在商业可行的范围内参照落实。**

就客体范围而言，《规范》中“个人金融信息”的概念与《实施办法》中“个人金融信息（即金融机构通过开展业务或者其他渠道获取、加工和保存的个人信息）”的概念较为相似，范围较为宽泛。虽然《规范》第4.1条并未明确广泛地列举**“个人常用设备信息（如IMEI、MAC地址、IDFA、软件列表等）”、“个人上网记录（如网站浏览记录、软件使用记录、点击记录等）”**和“个人位置信息（如行踪轨迹、精准定位信息等）”等《个人信息安全规范》附录所明确列举的个人信息，但是《规范》仍然可以通过该条g项的“在提供金融产品与服务过程中获取、保存的其他个人信息”进行兜底规范，甚至可以基于前述个人信息的识别性将其视为C2类别的个人金融信息（即其他能够识别出特定主体的信息）。

考虑到通过移动设备提供金融产品与服务已成大势所趋，设备信息与行为信息在客户身份识别、市场营销、反欺诈与风险控制等领域的使用亦日渐普及，因而在根据《规范》落实合规工作的过程中，金融业机构应当及时**梳理提供产品与服务中涉及处理的所有个人信息**，而不应仅仅限于《规范》明确列举的信息类型，并参照《规范》第4.2条对该等信息进行分级分类，继而相应落实合规要求。

- **问题二：我的企业如何遵照《规范》开展整体合规，大致有哪些步骤?**

就整体架构而言，《规范》在参考《个人信息安全规范》的基础上，先行对“个人金融信息”的范围和类别进行了梳理，继而从“安全技术要求”和“安全管理要求”两个维度详细地阐述了金融业机构在处理个人金融信息时需要遵循的规则。相应地，这一架构也在一定程度上为金融业机构开展内部合规提供了基本的思路和策略。

【企业建议】企业在根据《规范》开展合规工作时，应**率先进行个人金融信息的统计与整理**。具体而言：

- 企业既需要从**静态的数据类型与内容**出发，识别自身日常经营过程中所涉及的个人金融信息，按照《规范》中“C1、C2、C3”的级别进行数据等级划分，并尽可能使之与企业内部既存的数据资产分级得以衔接和协调；
- 企业也需要从**动态的数据生命周期**出发，进一步识别个人金融信息的“收集、传输、存储、使用、删除、销毁”等环节，为后续合规奠定事实基础。值得企业注意的是，在进行动态统计与整理时，企业不仅应该关注个人金融信息在内部的流转，更要关注该等信息在企业内部与外部第三方之间的流转，以避免遭遇来自外部的传递式风险。

另一方面，企业需要从**技术安全**和**管理安全**两个角度，同步开展安全合规，并需要关注《规范》“增强版”的合规要求，例如：

- 《规范》结合个人信息保护与金融行业的特点，创新性地对“个人金融信息销毁”（第6.1.6条）、“汇聚融合”（第6.1.4.6条）与“开发测试”（第6.1.4.7条）等**新环节**提出了要求；
- 《规范》在现有规则的基础上，针对个人金融信息的保护

[1]《规范》第3.1条。

[2]《规范》第3.2条。具体而言，《规范》中的个人金融信息包括账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息及其他反应特定个人某些情况的信息。

[3]这一适用范围可能较此前相关规范性文件中所提及的适用主体更为宽泛。

例如，《中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知》（以下简称“**央行17号文**”）的主要适用主体为“银行业金融机构”，《中国人民银行金融消费者权益保护实施办法》（以下简称“**《实施办法》**”）的主要规制主体为“金融机构（包括在中华人民共和国境内依法设立的为金融消费者提供金融产品和服务的银行业金融机构，提供跨市场、跨行业交叉性金融产品和服务的其他金融机构以及非银行支付机构）”。

拟制了**更为严格的要求**，例如严格限制C2与C3类别信息的收集渠道（第6.1.1条），禁止C2类别信息中的用户鉴别服务信息与C3类别信息的共享与转让（第7.1.3条），要求建立个人金融信息保护制度体系，并明确列举应当制定的管理规定和开展的管理活动（第7.2.1条）等。

因此，在这一过程中，企业将**需要着重关注《规范》所拟定的合规要求与既存合规义务的衔接**，尤其是**网络安全体系下**的《网络安全法》、《个人信息安全规范》与《网络安全等级保护基本要求》等关于个人信息保护和网络运行安全的规定，以及**金融监管体系**下的央行17号文、《中国人民银行关于金融机构进一步做好客户个人金融信息保护工作的通知》与《中国人民银行金融消费者权益保护实施办法》等关于个人金融信息保护的相关要求。

• 问题三：个人金融信息的分级分类和相关要求有哪些？

【新增规定】《规范》首次在普遍意义上明确了个人金融信息的分类分级体系。据报道，《规范》早前版本为《支付信息保护技术规范》，其中将支付信息按敏感程度从低到高分为四级；而正式出台的《规范》则在一定程度上简化了分级体系，将个人金融信息按敏感程度从高到低分为C3、C2、C1三类。其中：

- **C3类别信息**主要为用户鉴别信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成严重危害；
- **C2类别信息**主要为可识别特定用户身份与金融状况的个人金融信息，及用于金融产品和服务的关键信息。该类信息一旦遭到未经授权的查看或未经授权的变更，会对个人金融信息主体的信息安全与财产安全造成一定危害；
- **C1类别信息**主要为机构内部的信息资产，主要指供金融业机构内部使用的个人金融信息。该类信息一旦遭到未经授权的查看或未经授权的变更，可能会对个人金融信息主体的信息安全与财产安全造成一定影响。

【企业建议】事实上，《规范》也承认上述“静态”的定级规则需要**结合实际情况进行具体判断**：一方面，“同一信息”在不同的服务场景中可能处于不同的类别；另一方面，低敏感程度类别的信息经过组合、关联和分析后可能产生高敏感程度的信息（例如，C2类别的用户鉴别辅助信息与账号结合使用可直接完成用户鉴别的，则属于C3类别信息）。因此，如前文所述，**企业应当从静态的数据类型与内容出发和动态的数据生命周期两个维度开展个人金融信息的梳理，以免有所遗漏。**

【业务影响】鉴于在《规范》的分级体系下，C3类和C2类由于敏感程度较高，金融业机构在处理C3和C2类别信息时，需要承担相较于处理C1类别信息更为严格的合规要求。换言之，**位于产业链不同环节的金融业机构将可能需要根据《规范》的要求调整、优化自身的商业模式（尤其是基于“委托处理”模式为金融业机构提供服务的企业，具体详见对问题五的分析和建议）。**

• 问题四：我的企业主要从事To B型业务，什么情形下处理个人金融信息无需征得用户授权同意？

【新增规定】在《个人信息安全规范》征得授权同意收集、使用个人信息的例外情况的基础上，值得注意的是《规范》结合金融行业的业务实践定制了**“用于维护所提供的金融产品或服务的安全稳定运行所必须的，例如识别、处置金融产品或服务中的欺诈或被盗用等”**进行的个人金融信息收集使用无需征得个人金融信息主体授权同意的情形。[4]

【业务影响】实践中，不排除存在个人金融信息主体主观意志上不愿意授权金融业机构在反欺诈、身份验证等场景下采集并使用其个人金融信息，从而导致企业无法按照正常业务的合规逻辑规避可能的业务风险。**因此，此次新增的例外情形能够在一定程度上增强企业基于客户身份识别、反欺诈等业务办理所必需却难以获得用户授权同意收集使用信息时的合规依据支持。**

值得注意的是，尽管《规范》在一定程度上体现出金融行业监管者在个人金融信息保护上的监管态度与思路，**但是考虑到《规范》属于金融行业推荐性标准，其中的例外规定并不必然能够突破《网络安全法》等强制性法律法规规定中的原则性要求。**

【企业建议】为此，金融业机构可提前考虑结合《规范》中的相关规定：

- 梳理与新增例外情况相关的业务，对于确实难以征得客户授权同意的，需规划和完善面对公众和监管者的应对话术和宣传策略；
- 由于个人金融信息的对外共享并未增加如采集使用类似的例外情形，同时也为了避免个人信息非法买卖的风险，在未获得用户授权同意的前提下，金融业企业仍然需谨慎与第三方共享与客户反欺诈或反黑产相关的黑名单信息等；
- 仍需注意个人金融信息采集使用的必要性和正当性，对于个人金融信息的采集类型和频率应当与办理金融业务的风险大小相匹配，且应为实现目的最小范围。

[4]《规范》第7.1.1条d项。

• 问题五：我的企业在个人金融信息委托处理上需要注意什么?

《规范》在委托处理个人金融信息的实践上，提出了较为严格的合规要求，除个人信息保护中常见的合同约定各方权责义务、要求被委托者不得超范围使用、准确记录等要求以外，还进一步提出了更多的技术要求，主要包括：

1. 对数据委托收集的主体限制

【新增规定】《规范》要求**金融业机构不应委托或授权无金融业相关资质的机构收集C3、C2类别信息**。[5]

【业务影响】考虑到《规范》对于C3、C2类别信息的定义十分宽泛且目前有关“金融业相关资质”的定义未有明确规定，**该新增规定可能导致许多非持牌机构在金融信息的收集环节上需要有所调整**，例如可能不再能在业务前端代表金融业企业采集客户KYC、借贷等相关信息。[6]

【企业建议】建议非持牌机构视具体情况调整业务模式，采取替代方案以避免基于金融机构客户的委托对个人金融信息进行直接采集或使用。例如，非持牌机构是否可以考虑发展面向终端消费者（To C）的相关业务。

2. 对委托处理数据的限制

【新增规定】对于个人金融信息的委托处理而言，《规范》相对《个人信息安全规范》新增的要求主要包括：

1）C3类和C2类中的用户鉴别辅助信息，不应委托给第三方处理（第6.1.4.4.条b项）；

2）应对委托处理的信息采用去标识化（不应仅使用加密技术）进行脱敏处理（第6.1.4.4.条c项）；

3）应对外部嵌入或介入的自动化工具（如代码、脚本、接口、算法模型、软件开发工具包等）开展技术检测，并对第三方的收集个人金融信息行为开展审计，发现超出约定行为及时切断接入（第6.1.4.4.条f项）。

【业务影响】首先，对于某些金融业企业的外部合作机构而言，其产品和服务的提供可能必须基于明文的C3类和/或C2类中的用户鉴别辅助信息，如目前接受银行等金融机构委托进行身份核验等的助贷企业，可能必须以客户身份三要素（如姓名、身份证号和手机号码）的获取为业务开展的基础，**依据目前的要求，非持牌机构可能难以再获得明文的上述个人金融信息，因此业务模式可能面临重新调整的需要。**

其次，严格按照《规范》规定来看，**金融企业客户在选择业务和服务的外包方时，将可能不再仅要求对于产品和服务的合规性和业务逻辑进行说明、承诺，还可能需要进一步地针对自动化工具开展技术检测，并对基于委托收集个人金融信息的行为进行审计。**

【企业建议】对于个人金融信息的**被委托方**而言，为避免不同合作方的反复检测和自证，同时合理考虑委托处理环节的脱敏处理要求，建议：

1）考虑采用本地化部署和交付等方式为金融企业客户提供相关产品或服务，通过由客户自行掌握相关服务系统的方式，避免SaaS服务模式下处理禁止委托处理的信息、或者针对被委托处理信息的频繁、多方技术检测成本；

2）有必要时，自行开发面向金融企业客户的技术工具，用于客户全方位了解和掌握相关服务系统运行情况和安全保障状况；

3）如有可能，尽早考虑新的系统架构模式，确保去标识化处理后映射信息仅在客户本地保留，被委托方系统仅对去标识化后不可回溯个人金融信息主体的数据进行处理、分析，进而为客户提供数据分析能力和算法模型构建能力。

对于个人金融信息的**委托方**而言，为了避免向第三方委托处理禁止性信息、保证数据委托处理的合规性，建议：

1）提高自身的技术研发能力，尤其对于禁止委托处理的信息（如用户鉴别用途的个人生物识别信息），尽量使用自身技术予以处理以满足业务经营的需要；

2）建立对于自动化工具应用的全流程管控制度，包括接入前的合规和技术评估、定期审计和应急处理机制等。

• 问题六：什么时候需要应用去标识化和屏蔽技术?

【新增规定】纵观对金融业机构处理个人金融信息的合规要求，“安全防护”可谓是《规范》的核心要求，无论是技术要求还是管理要求，都无不体现着监管机构对个人金融信息的安全追求，包括但不限于**加密技术**在个人金融信息存储与传输环节的应用，**身份鉴别和认证技术**在个人金融信息使用与传输环节的应用，**监控与审计技术**在个人金融信息共享、转让和委托处理环节的应用等。

[5]《规范》第6.1.1.条a项。

[6]搜狐新闻，“央行发布个人金融信息保护技术规范，无资质不得收集KYC等信息”，https://www.sohu.com/a/374602685_676454（发表于2020年2月20日）。

其中，“屏蔽”、“匿名化”与“去标识化”等**脱敏技术**的应用，将可能是对企业合规处理和有效利用个人金融信息最为关键的技术之一。《个人信息安全规范》目前主要对“去标识化技术”的使用进行了概括性的规定。[7]相较而言，《规范》则**在个人金融信息的多个生命周期环节中，明确要求金融业机构适当采用脱敏技术，以提升个人金融信息的安全并降低泄露的风险**。例如：

- **收集：**引导用户输入（或设置）银行卡密码、网络支付密码时，应采取展示屏蔽等措施防止密码明文显示，其他密码类信息宜采取展示屏蔽措施（第6.1.1条）；
- **信息展示：**对通过各类业务界面或后台管理和业务支撑系统展示的个人金融信息，应采取信息屏蔽等处理措施（第6.1.4.1条）；
- **共享和转让：**支付账号及其等效信息在共享和转让时应使用支付标记化技术（按照JR/T 0149-2016）进行脱敏处理（第6.1.4.2条）；
- **委托处理：**对委托处理的信息应采用去标识化等方式进行脱敏处理（第6.1.4.4条）；
- **开发测试：**开发环境、测试环境应使用虚构的或经过去标识化脱敏处理的个人金融信息（第6.1.4.7条）；
- **安全制度体系建立与发布：**建立个人金融信息脱敏管理规范和制度，应明确不同敏感级别个人金融信息脱敏规则、脱敏方法和脱敏数据的使用限制（第7.2.1条）。

从有效利用的角度看，我们也注意到，《规范》针对经脱敏的个人金融信息可能也给予了一定的技术空间。例如，共享、转让经去标识化处理（不应仅使用加密技术）的个人金融信息，且**确保数据接收方无法重新识别个人金融信息主体**的，将可无需向个人金融信息主体告知共享、转让的相关信息，亦无需事先征得个人金融信息主体明示同意（第7.1.3条），这一操作即允许金融业机构在对个人金融信息进行**“有针对性的匿名化处理”**后，适当地降低合规负担。

【企业建议】金融业机构在根据《规范》落实合规工作时，可以考虑**综合参考**《规范》附录A“信息屏蔽”、《支付标记化技术规范（JR/T 0149-2016）》以及《个人信息去标识化指南》等技术指引，进行与相关个人金融信息敏感级别相符的脱敏处理。

实践中，某些金融技术服务提供商由于不具备“金融业资质或牌照”，因而可能将缺乏在个人金融信息采集端的合作机会，而即便是以委托处理作为切入点，前述的技术服务提供商可能仍需承担极为繁重的合规义务。那么，在上述第7.1.3条的指引下，**合规承担能力相对有限的技术服务提供商可能需要考虑以技术能力输出为原则，在去标识化、匿名化技术的帮助下协助金融业机构开展数据分析与模型构建**。即便这种模式可以成立，金融业机构与技术服务提供商也仍需解决一个现实性的前提问题：如何采用技术手段确保脱敏处理的充分性，并以有效的形式呈现这种充分性。

• 问题七：我的企业是否可以不删除个人金融信息？

对于超过必要期限处理的个人金融数据而言，《规范》针对不同的场景提出了“删除”和“销毁”两种处理方式。

1. 删除个人金融数据的要求

【新增规定】依据《规范》的要求，**当属于以下两种情况之一时，金融业机构可以采取技术手段，仅在金融产品和服务所涉及的系统中去除个人金融信息，使其保持不可被检索和访问的状态（换言之，无需进行彻底的物理删除）：**

1）个人金融信息主体的处理超出授权使用目的所必需的最短时限；

2）响应个人金融信息主体要求删除其个人金融信息的请求。[8]

【业务影响】尽管目前《网络安全法》未对个人信息的“删除”予以明确定义，本次《规范》在“删除”的定义上与《个人信息安全规范》的口径基本保持一致，**对于需要多次重复使用同一个人金融信息和/或其衍生信息的金融业机构而言，进一步增强了长期留存数据的合法依据支持，降低了重复采集和汇总分析个人信息的成本。从技术角度看，这一界定也能够避免在大型业务**

[7]《个人信息安全规范》第6.2条，即收集个人信息后，个人信息控制者宜立即进行去标识化处理，并采取技术和管理方面的措施，将去标识化后的数据与可用于恢复识别个人的信息分开存储，并确保在后续的个人信息处理中不重新识别个人。

[8]《规范》第6.1.5条b项。

数据库中彻底物理删除特定数据字段对数据库结构造成的影响，在一定程度上为企业降低技术维护成本。

【企业建议】对于金融业企业尤其是开展多项金融业务的集团公司而言，为了避免各业务条线重复采集、处理数据可能产生的成本，建议：

1）**梳理各业务条线需要重复使用的个人金融数据和衍生信息情况，并予以统一存储和管理；**

2）**对于超出授权使用目的所必需最短时限的上述信息移至冷库，当新的业务触发用户的重新授权同意时，予以再次调用。**

2. 个人金融数据的留存和销毁要求

【新增规定】《规范》对个人金融信息的销毁同样采取了较为严格的口径，尤其针对金融业机构委托、外包或与第三方合作开展个人金融信息处理的情况：

1）因金融产品或服务的需要，将收集的个人金融信息委托给第三方机构（含外包服务机构与外部合作机构）处理的，**“在委托关系解除时（或外包服务终止后），受委托者应按照金融业机构的要求销毁其处理的个人金融信息”**（第7.1.3条c项）；

2）金融业机构应建立外包服务机构与外部合作机构管理制度，其中包含**“通过协议或合同的方式，约束外包服务机构与外部服务机构不应留存C2、C3类别信息”**（第7.2.1条g项）。

【业务影响】如严格按照《规范》要求分析，作为金融机构的服务商/外部合作机构，将可能难以留存C2、C3类别信息，考虑到C2和C3类别可能包含关键的个人金融信息类型，将可能对业务实践和数据留存情况提出较大的合规性挑战。

【企业建议】对于进行身份核验、反欺诈等业务的技术服务提供商而言，可能需要考虑**以本地化部署方式提供相关产品、服务系统，以实现个人金融信息不出金融机构的前提下的算法、模型等技术能力输出。此外，对于无法采用本地化部署提供的产品、服务而言，在可行且必要时，公司应考虑通过技术积累、算法积累等方式逐渐摆脱对个人金融信息及其衍生数据的留存依赖，以尽可能适应《规范》下的严格要求。**

- **问题八：我的企业中不同业务线的数据能否打通，是否能够在行业内将个人金融信息打通？**

【新增规定】2015年，《国务院关于印发促进大数据发展行动纲要的通知》（国发，〔2015〕50号）发布，首次提出“推动跨领域、跨行业的数据融合和协同创新”。至此，推动不同领域的数据融合应用（特别是大数据融合应用）受到政府高度重视。本次《规范》是在金融领域首次提出对于个人金融信息汇聚融合的明确要求（第6.1.4.6条）：

1）汇聚融合的数据不应超出收集时所声明的使用该范围。因业务需要确需超范围使用的，应再次征得个人金融信息主体明示同意；

2）应根据汇聚融合后的个人金融信息类别及使用目的，开展个人金融信息安全影响评估，并采取有效的技术保护措施。

【业务影响】随着普惠金融和大数据产业的发展，打破数据孤岛、实现产业链的数据汇聚融合成了业务办理、打击网络黑产以及发挥数据商业化价值的必然要求。例如，对于银行信用信息缺失或者资质较差的弱势群体而言，金融业企业可能需要从除了央行征信以外的自身各业务条线、以及其他第三方渠道尽可能获取其信用相关信息，并最终形成个人征信画像以实现业务风控目的。

本次《规范》的要求体现了行业监管部门对于数据汇聚融合作为热点问题的重视，未来针对该问题预计会出现更加深入和完善的规定。**企业在汇总分析个人金融信息之前可能需要从合法、正当和必要性方面梳理存在的问题，并设计与业务开展相匹配的数据汇聚融合模式。**

【企业建议】从广义而言，数据的汇聚融合可能包括：（1）同一公司内部不同业务线的数据共享；（2）同一集团内不同关联企业间数据共享；（3）与集团外第三方的数据共享。企业数据汇聚融合是需要技术部门、法律合规部门与产品部门通力协作、集团内部关联公司达成共识、商业逻辑和合规框架并存的大工程，需要公司领导统一思想、大力支持才能完成。针对数据融合的常见问题，建议金融业机构采取以下几方面措施：

1）**原始数据溯源及合规：**以普遍适用的法定义务合规性为评估起点、结合所处行业的监管要求对数据的收集、使用、存储和共享等全生命周期的对存量数据的产生/收集过程和利用方式的合法合规性进行评估；

2）**数据分级分类：**数据分级分类是评估数据的安全性和合规性的重要方法，也为数据融合项目中应用原始数据范围的确定提供了参考；

3）**数据承接主体选择：**通过设立数据中台作为大数据资产层、设立独立的科技子公司等形式承接来自各关联企业的数据；

4）**商业模式搭建：**基于对数据融合与集团原有业务的关联性、数据价值的商业化利用和技术能力等因素考虑，选择C（控制者）-P（处理者）、C（控制者）-C（控制者）模式，甚至更为复杂的C（控制者）-P （处理者）+C（控制者）等模式开展数据汇聚融合；

5）**保证多主体对于数据融合变现的利益：**约定参与各方对

于数据融合变现的利益，以维系整个商业模式的良好平稳运转。

有关数据汇聚融合的具体分析，可参见《“数”年快乐——万字长文说“数据融合”》[9]一文。

• 问题九：我的企业业务场景中可能存在跨境的情况，个人金融信息的跨境传输应该怎么办？

【新增规定】对比《网络安全法》中关键信息基础设施的运营者对个人信息和重要数据进行本地化存储的规定，《规范》对于金融业机构个人金融信息本地化政策的要求更为严格。相比之下，《规范》更清晰地参考了央行17号文[10]和《实施办法》[11]中的意见，要求所有金融业机构“在中华人民共和国境内提供金融产品或服务过程中收集和产生的个人金融信息”都应在境内存储、处理和分析。[12]

跨境合规义务方面，《规范》在《网络安全法》拟制的“业务需要+用户授权同意+安全评估”基本模式基础上，额外增加了**应与境外接收方通过签订协议[13]、现场核查等方式，明确并监督接收方的若干职责义务，体现了与《个人信息出境安全评估办法（征求意见稿）》相似的监管思路。**[14]

【业务影响】如前所述，落入“金融业机构”的企业都需要参考《规范》开展合规工作。

由于央行17号文和《实施办法》早在数年前就已先后强调了金融机构应当在我国境内存储个人金融信息或消费者金融信息，《规范》中本地化的要求对传统的持牌金融机构业务产生的变动不会很大。我们理解，**《规范》的这一规定可能需引起金融业企业的服务提供商的注意**，即使基于自身业务被认定为关键信息基础设施运营者的可能性较小（如市场营销服务企业、归因数据分析企业等），但由于涉及个人金融信息的处理，可能也会被要求遵守本地化存储的要求。

除应根据《网安法》的要求进行个人信息出境安全评估外，上述金融业机构还需要注意与境外的接收方机构签订个人金融信息跨境传输协议，明确约定境外机构的义务。此外，在条件允许的情况下，还应当采取现场核查等方式，监督境外机构对其职责义务的履行情况。

【企业建议】1）为金融机构提供服务的企业，涉及处理个人金融信息的服务器应尽量进行本地化部署；如因业务需要确需使用境外服务而引发数据跨境传输（例如，使用境外SaaS平台完成数据分析），则可能需要考虑遵守个人金融信息跨境传输的要求；

2）金融业机构需梳理个人金融信息跨境的场景，并根据梳理结果与境外接收机构签署协议。在该类协议的内容方面，除明确接收方的保密、数据删除、案件协查等义务外，建议进一步参考《评估办法》中的有关要求，明确个人信息出境的目的、类型、保存时限等事项。[15]

（本文发布于2020年02月23日。）

---

[9] https://mp.weixin.qq.com/s/VAYHAHbch4R_hBuH0hB_jQ

[10] 央行17号文第六点，在中国境内收集的个人金融信息的储存、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，银行业金融机构不得向境外提供境内个人金融信息。

[11]《实施办法》第三十三条第一款，在中国境内收集的个人金融信息的存储、处理和分析应当在中国境内进行。除法律法规及中国人民银行另有规定外，金融机构不得向境外提供境内个人金融信息。

[12] 《规范》第7.1.3条d项。

[13] 国家互联网信息办公室2019年6月发布的《个人信息出境安全评估办法（征求意见稿）》（以下简称“《评估办法》”）要求网络运营者就个人信息出境与境外接收者之间签订的合同或者其他有法律效力的文件应当约定境外接收者有配合用户权利响应、目的限制等义务。

[14]《规范》第7.1.3条d项。《规范》中列举的应当明确的境外机构（接收方）的职责义务包括保密、数据删除、案件协查等。

[15]《评估办法》第十三条，网络运营者与个人信息接收者签订的合同或者其他有法律效力的文件（统称合同），应当明确：

（一）个人信息出境的目的、类型、保存时限。

（二）个人信息主体是合同中涉及个人信息主体权益的条款的受益人。

（三）个人信息主体合法权益受到损害时，可以自行或者委托代理人向网络运营者或者接收者或者双方索赔，网络运营者或者接收者应当予以赔偿，除非证明没有责任。

（四）接收者所在国家法律环境发生变化导致合同难以履行时，应当终止合同，或者重新进行安全评估。

（五）合同的终止不能免除合同中涉及个人信息主体合法权益有关条款规定的网络运营者和接收者的责任和义务，除非接收者已经销毁了接收到的个人信息或作了匿名化处理。

（六）双方约定的其他内容。

此外，《评估办法》第十四条至第十六条还规定了合同中应当明确的跨境传输双方的其他义务。

“柳暗花明又一村”——金融产业链的困局及破局思路

一、前言

当前互联网和数字技术的发展为经济带来了前所未有的活力，在蓬勃发展的数字经济中，数据及其流动是其关键性支撑。[1]在金融行业中，“精准营销、风险控制、客户关系管理决策支持、开放银行”等广泛应用场景[2]推动了金融大数据的发展和数据驱动型业务[3]的开展。充分流动共享的金融数据也是数字经济时代金融科技发展的重要基础。毋庸置疑，数据作为生产要素之一，在金融行业发展和创新中有着不容忽视的价值。

保障数据的充分流动和共享、发挥数据价值的过程依然需要遵守现行的法律法规和监管要求。金融数据尤其是个人金融数据往往存在双重属性，一方面，在金融行业强监管体制下，金融数据在数据收集、存储、处理、使用和共享等方面往往受到金融行业法律法规的严格限制。另一方面，由于个人客户的金融数据往往具有强烈的人身属性，还可能受到个人信息及个人敏感信息保护的规制。

本文拟以个人征信及智能风控等行业为例，分析数据在产业链中流转的困局，并参照境外信用体系的运行经验探讨潜在的疏通个人金融数据流转渠道同时保障金融数据安全、消费者利益的破局思路。

二、金融产业链的构成

除了传统金融机构之外，普惠金融和互联网消费金融的兴起催生出了更多类型的服务提供商。例如，接受金融机构委托汇聚、分析多来源用户信息，并向金融机构提供信贷风控、反欺诈等服务的智能风控企业，以及提供大数据分析、人工智能、机器学习等技术能力的科技公司（智能风控企业和科技公司等统称为新兴市场参与者）。在目前的金融产业链中，非金融机构、金融科技公司以及传统金融机构等市场主体参与其中，并在数据的流转中环环相扣。

以征信产业链为例，在数据的采集阶段，通常数据提供方包括但不限于提供政府数据的公安、社保等政府机构，以及银行、电商、电信运营商等拥有大量反映个人消费、金融状况信息的机构。在数据的处理阶段，参与主体包括：（1）央行征信中心，其通过汇集和分析银行的传统信贷数据，形成客户的信用报告；（2）市场化个人征信机构，以百行征信为例，通过汇集和分析用户在互联网平台、保险公司、老牌征信公司和拥有数据资源的新兴公司数据，形成个人信用报告等征信服务产品；以及（3）智能风控企业，通常为基于大数据、人工智能、机器学习等技术能力，为其他企业提供智能风控策略及相关决策辅助服务的市场主体。

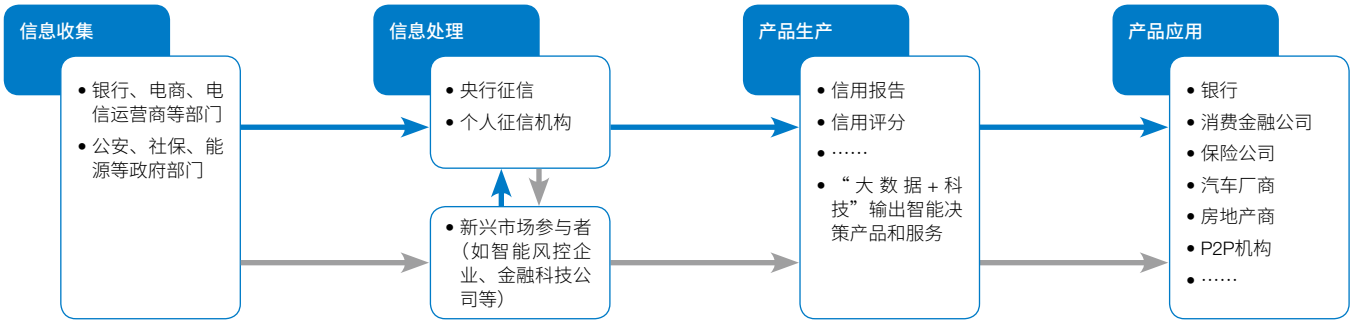


图1—目前涉及个人征信金融产业链的数据流转

[1] 参见陈红娜：《数字贸易中的跨境数据流动问题研究》，《发展研究》2019年第4期，第9-19页。

[2] 参见刘振海、马征、缪凯：《大数据在金融行业的应用现状与发展对策》，《金融电子化》2018年第9期，第20-21页。

[3] 2018年，中国银行保险监督管理委员会（“银保监会”）在发布的《银行业金融机构数据治理指引》中强调银行业金融机构应当加强数据采集的统一管理，明确系统间数据交换流程和标准，实现各类数据有效共享（第二十三条）；实现数据驱动，发挥数据价值（第三十八条）。

三、金融产业链的数据困局表现

总体而言，金融产业链的主要困局是如何在依法合规前提下发展金融科技、促进个人金融信息的有序汇聚融合，为金融业务发展提供源源不断的创新活力，同时防止数据泄露、保证消费者的权益不受损害。[4]

以征信行业为例，考虑到新兴金融服务对于多源信息以及科技能力的需求，央行开始将国家金融信用信息基础数据库以外的市场化征信机构纳入征信服务市场，以形成错位发展、功能互补的格局。然而，对于官方征信机构的信用信息平台建设而言，目前仍面临诸多的挑战有待完善，包括但不限于：如何整合百行征信接入的多源数据以保证可以商业化的输出；如何促进互联网平台股东与百行征信之间的数据共享；[5]以及如何完整市场化征信机构与国家金融信用信息基础数据库的数据整合。

另一方面，从数据量来看，官方征信机构外部产生了很多的数据，这些数据的体量远超信贷数据。大数据公司不仅拥有众多数据，而且数据维度广泛，涉及电子商务、社交、地理位置等等。从实际业务需求来说，在“信用白户”向“有信用记录的人”转换过程中，这些大数据公司拥有的用户线上购物信息、社交信息等可以作为初步信用记录的建立基础。此外，智能风控企业由于具备大数据、人工智能、机器学习等技术能力，其能通过线上线下广泛的数据收集方式和算法研发能力，为金融机构等企业提供更为准确的身份核验、信用评分等服务，从而提升金融机构等企业的风控能力、降低信用审核成本。

但是，目前我国的法律对于这些新兴市场参与者提供的信息属性、是否属于对外提供个人征信服务等未予以明确的界定。这样导致大数据公司、智能风控企业的业务开展持续性和业务范围受到挑战，依旧无法实现征信行业数据的最大限度共享和汇总分析。

四、金融产业链数据困局的原因分析

在我国目前金融业监管背景下，可能阻碍新兴市场参与者参与金融产业链数据使用实践的原因可能包括以下几个方面：

（一）市场准入门槛的设定，导致新兴市场参与者的主体资质和业务性质存在合规方面的不确定性

我国现有法律针对银行、保险公司、证券公司、投资管理公司的业务范围和个人金融信息的流转有较为严格的限制，使得这些金融机构在向新兴市场参与者提供数据和数据使用方面可能受到阻碍。例如，依据《征信业管理条例》的要求，提供个人征信业务的征信机构需取得个人征信业务经营许可证。提供企业征信业务的征信机构，应当向所在地的国务院征信业监督管理部门派出机构办理备案。由于目前仅百行征信一家民营机构获得了个人征信业务的经营许可，从而导致其他提供信用相关信息、数据汇总和信用评级分析企业的主体准入资质存在不确定的因素。此外，《个人金融信息（数据）保护试行办法（初稿）》（以下简称“**《试行办法（初稿）》**”）和《个人金融信息保护技术规范》也分别对于从非持牌金融机构处获取个人信息提出限制。[6]

限制非持牌机构采集和向金融机构提供个人金融信息的初衷，可能是为了确保敏感的个人金融信息不被过多的非金融机构获取并用于金融业务办理以外的其他用途，并因此增加对个人信息主体的侵权风险。然而，随着金融业的科技革新和服务对象的扩大化，非金融机构的大数据能力输出逐渐成为金融机构业务办理的必要条件。市场准入门槛的设定可能限制了金融机构通过非持牌机构获取多头数据以及风险评分，用于提升风控能力、降低信用审核成本的可能性。

（二）数据采集的合法性依据单一，增加了数据流转的困难程度

依据目前的《网络安全法》，对于个人信息采集和使用应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。在金融产业链中，数据的采集体现出来源广泛、类型多样、参与者众多等特点，数据主体本人提供的信息、有关该数据主体的各种公开信息、其他第三方拥有的该数据主体相关信息（如身份识别信息、职业和居住地址信息、个人交易、缴费、纳税记录等）可能被提供金融业务服务的机构直接采集，也有可能被委托服务提供者经过多重交互、共享和分析之后向金融机构提供。由于金融产业链中的各方之间数据交互频繁，实时性强、且交易过程中各方的权益和角色多变，因此对数据的溯源和用户授权的核查往往存在实质性障碍，从而增加了数据合法流转的难度。

（三）个人金融信息向新兴市场参与者流通受限

除了《网络安全法》有关个人信息对外共享的一般限制，个人金融信息和个人信用信息的流转还受制于行业监管部门对于共享数据对象、目的和数据类型的要求。

---

[4] 参见中国人民银行：《金融科技（Fintech）发展规划（2019-2021）》，第一章发展形势部分，2019年8月。

[5] 2019年9月，根据FT报道，阿里巴巴和腾讯拒绝向百行征信提供客户信贷信息。在除中国互联网金融协会的8家股东中，仅3家同意将数据接入百行征信。

[6] 《试行办法（初稿）》中明确要求“金融机构不得从非法从事个人征信业务活动的第三方获取个人金融信息”。此外，在目前央行发布的《个人金融信息保护技术规范》第6.1.1条第a项中，要求金融业机构不应委托或授权无金融业相关资质的机构收集C3、C2类别信息，包括了解客户（KYC）的信息，直接反映个人金融信息主体金融状况的财产、信贷信息等。

以个人金融信息的流转为例，《人民银行关于银行业金融机构做好个人金融信息保护工作的通知》[银发（2011）17号]（以下简称《人民银行第17号文》）要求：“银行业金融机构不得向本金融机构以外的其他机构和个人提供个人金融信息，但为个人办理相关业务所必需并经个人书面授权或同意的，以及法律法规和中国人民银行另有规定的除外”。 可以看出，提供给银行业金融机构的数据对外共享和融合的目的，仅限于个人办理相关业务所必需并经个人书面授权或同意的，以及法律法规和中国人民银行另有规定。类似的限制也出现在金融领域的其他行业监管要求中。[7]以个人信用信息的流转为例，《个人信用信息基础数据库管理暂行办法》第七条规定，商业银行不得向未经信贷征信主管部门批准建立或变相建立的个人信用数据库提供个人信用信息。

对于个人金融信息和个人信用信息的对外共享限制，进一步增加了持牌金融机构将客户信息向非持牌机构共享的难度。如何保证新兴的市场参与者参与个人金融数据使用实践、满足普惠金融和互联网消费金融业务办理、金融科技发展所需的同时，依然能够保证个人信息主体的权益和个人金融信息的安全，是我国目前金融产业链面临的挑战。

五、美国金融链产业构建与个人信息保护的实践

相比于我国更倾向于在保障消费者权益和金融安全秩序的前提下寻求政府监管下有序和限定范围的数据融合共享，美国在金融数据监管方面的态度较为宽松，强调金融数据的广泛自由流通。

（一）多方参与的金融链产业模式

就征信行业而言，由于美国实行典型的市场化征信模式，政府并未通过经营资质许可等手段对主体资质进行监管；而是通过自发的市场运营逐步形成了成熟的征信产业链条；其中个人征信产业主要包含四个环节，即原始信用信息收集；信用信息处理；征信产品生产和征信产品应用。[8]

具体而言，在收集环节，信息提供方包括但不限于提供公开信息的政府机构，提供消费者记录的银行、保险公司、消费信贷机构等，这些机构往往也是征信的授信机构。此外在涉及调查信用报告（investigative consumer report）时，信用局（consumer reporting agency）还可能通过调查消费者的社会关系网获取对消费者的品行等评价信息，如雇主评价信息。

在信用信息处理环节，主要的市场参与主体为信用局，目前美国个人征信行业以三大信用局为核心，并包含上千家地方征信局，[9]这些机构“依附于”三大信用局或者“向其提供数据”。[10]在征信产品生产环节，信用局进行信息处理并生成信用报告，并根据司法机构、雇主、商业银行、保险公司、消费信贷机构等需求方在合法范围内提供。

同时，以FICO为代表的信用评分也是重要征信产品之一，数据分析机构、金融科技公司等从信用局获取信用报告并通过特定模型最终输出信用评分，供信用局或消费者个人查询使用，目前FICO信用分已经成为授信机构重要的风控手段。信用局的另一类产品则是“预选名单”，[11]即根据商业机构制定的某些条件对消费者信用数据进行分析，筛选符合特定条件的消费者的名称和通讯地址，并将名单提供给商业机构。不难发现，美国的金融产业链中所涉及的主体极为多样，包括但不限于政府、传统金融机构如商业银行、保险公司、消费金融机构、信用局、数据分析公司及其他金融科技主体等。

同时根据美国 1966 年颁布的《信息自由法》（Freedom of Information Act）和 1971 年的《公平信用报告法》（Fair Credit Reporting Act）之规定，联邦政府记录或信息，[12] 除列明的例外情况外，原则上会根据请求向任何人（即几乎没有特别的资格限制）提供；而除特定情形外，信用局在收集消费者信用及其他有关信息时也无需征得消费者的同意。1999 年国会通过《金融现代化法案》（Financial Services Modernization Act，又称“Gramm-Leach-Bliley Act”，“GLBA”），肯定了银行、保险公司、投资公司之间广泛的个人信息共享，包括关联公司和非关联公司之间的个人信

[7] 参见证监会《证券基金经营机构信息技术管理办法》第三十四条规定，除法律法规和中国证监会另有规定外，证券基金经营机构不得允许或者配合其他机构、个人截取、留存客户信息，不得以任何方式向其他机构、个人提供客户信息。

[8] 参见《一文带你看清：美国征信行业格局如何，都有哪些玩家》，爱分析，载https://www.huxiu.com/article/174390.html，2016年12月13日；张丽：《美国现代个人征信法律制度研究》，《安徽大学》，2019年。

[9] 参见青川：《金融科技公司都在学习的FICO，是个怎样的存在》，爱分析，载https://www.huxiu.com/article/215415.html?f=member_article，2017年9月20日。

[10] 参见《一文带你看清：美国征信行业格局如何，都有哪些玩家》，爱分析，载https://www.huxiu.com/article/174390.html，2016年12月13日。

[11] 参见张丽：《美国现代个人征信法律制度研究》，《安徽大学》，2019年。

[12] The Freedom of Information Act (FOIA) generally provides that any person has the right to request access to federal agency records or information except to the extent the records are protected from disclosure by any of nine exemptions contained in the law or by one of three special law enforcement record exclusions. Please see at https://foia.state.gov/Learn/FOIA.aspx, cited on March 4, 2020.

息共享。[13] 这些举措在一定程度上保障了除消费者本人外的社会公众、交易相对方对相关信息的权益，也推动了金融数据的流转。

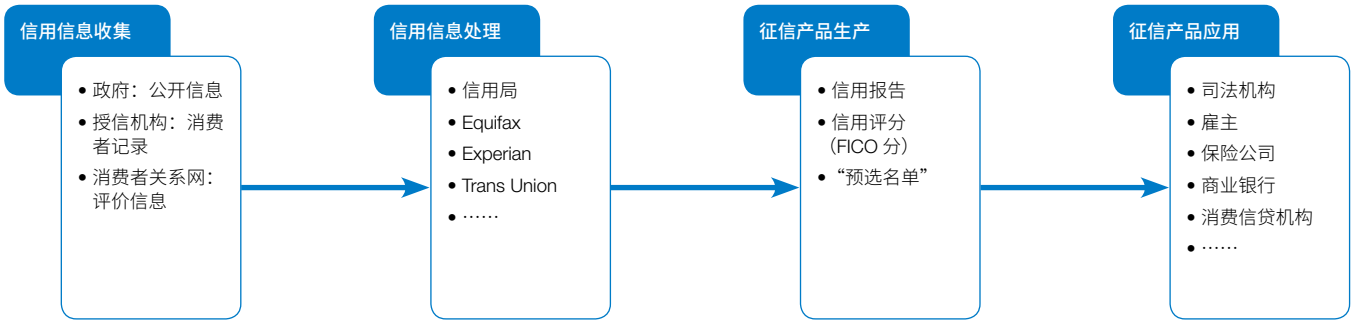


图2—美国个人征信金融产业链的基本构成

（二）金融消费者权益保护（隐私）：对收集、共享个人信息的内容限制

金融数据的自由流转也会带来消费者权益保护、金融信息安全和金融社会秩序与公平等方面的风险。在这种情形下，美国选择通过法律规制各方主体的市场行为、保障消费者权利的方式推动金融数据的良性融合与共享。

在金融数据流转过程中，对消费者隐私和非歧视权利的保护始终是关注的重点问题之一。防止这一现象发生的手段之一，便是通过立法限制在征信活动中收集个人信用信息的范围。具体而言，《公平信用报告法》中限制对医疗信息的共享；1975年发布的《平等信用机会法》（Equal Credit Opportunity Act）要求债权人不得在信用交易中因申请人的种族、肤色、宗教信仰、祖籍国家、婚姻状态等而歧视申请者；[14]《诚实信贷法》（Truth in Lending Act）中禁止因消费者的种族、民族、性别或年龄而剥夺平等信用机会的不公正信贷行为……这些限制和禁止性规定为征信场景下的信用数据收集划定了边界，也保护了金融消费者在征信活动中的权利和利益。

（三）金融消费者权益保护（信息准确性）：以知情权和申诉更正权为核心

目前美国并未限制信用局获取信用信息的来源，广泛的原始信用信息在增强征信行业活力的同时，也难免导致数据质量和信息准确性问题。在这种情况下，美国信用局协会制定的个人征信业务统一标准数据报告和采集格式无疑有助于提升数据的质量和数据处理效率。[15]

同时，**消费者的同意**仍然是数据流转的重要合法性基础之一。如GLBA中肯定消费者有权拒绝与非关联第三方共享信息；美国消费者金融保护局（Consumer Financial Protection Bureau，“CFPB”）在2017年发布的金融数据共享融合的九大原则探讨的也是“经消费者授权的金融数据共享融合”的场景。因此，消费者授权同意在保障隐私的方面仍然发挥着重要作用。

在某些消费者的授权同意不再是数据流转前提条件的场景中（如征信信息的采集和对外共享），即消费者可能无法通过事先的控制保障自己的利益和信用报告信息的准确性，在事后环节的消费者知情权和申诉权保障变得尤为重要。例如，《公平信用报

[13] "In 1999, Congress passed the Financial Services Modernization Act, more commonly known as the Gramm-Leach-Bliley Act (GLBA)…The law authorizes widespread sharing of personal information by financial institutions such as banks, insurers, and investment companies. The law permits sharing of personal information between companies that are joined together or affiliated with each other as well as sharing of information between unaffiliated companies." Schwartz, S. Information Privacy Law.

[14] (a) It shall be unlawful for any creditor to discriminate against any applicant, with respect to any aspect of a credit transaction (1) on the basis of race, color, religion, national origin, sex or marital status, or age (provided the applicant has the capacity to contract); 15 U.S.C. § 1691.

[15] 前引10。

告法》中规定了信用局根据消费者请求，向消费者披露信用报告中的信息、信用信息源、特定时间内信用报告的使用者身份以及过去一年内非由消费者发起的信用或保险交易中的信用报告查询记录等信息[16]的义务。

此外，《公平信用报告法》中还规定了信用局有义务向消费者披露其信用评分成绩及对评分产生不利影响的所有关键性因素等信息[17]；而在银行、保险等机构或雇主使用信用报告时，则同样负有不利决定的告知义务，即应当告知消费者不利决定的作出以及相关的信用局名称与联系方式[18]。其实质是鼓励和保障消费者本人对金融数据的准确性进行核验的权利，以避免和降低错误金融数据流转给消费者权益造成的损失。而为了保障知情权和有效申诉和更正金融数据，《公平信用报告法》及其革新法案[19]还规定了消费者免费或以低价获得相关信息、信用局的申诉响应、原始信用信息提供机构数据异议处理义务等内容。

（四）金融数据安全：建立金融机构的客户数据信息安全保密标准

金融信息的广泛共享不可避免地带来信息安全风险等级的提升。为降低这一风险，保障金融数据安全，GLBA要求相关金融监管机构建立相应的安全标准以保障客户数据信息的安全与保密性[20]。2002年，美国联邦贸易委员会（Federal Trade Commission, “FTC”）发布了相关规则，即金融机构应当开发、实施并维护包含管理、技术和物理防护的全面信息安全系统[21]。根据FTC发布的《2019年隐私和数据安全报告》披露，FTC已经针对Equifax、Dealerbuilt信息安全事件中违反GLB的安全政策与程序义务提起指控；并会在未来提高在数据安全案件中的和解要求，即对公司安全计划开展评估并要求提交遵守安全计划的年度证明。[22]

（五）避免金融数据滥用：限制信用报告的使用场景、特定场景中的共享数据类型和 opt-out 机制

金融数据的共享带来的另一忧患则是金融数据的滥用。典型如信用报告和基于金融数据而开展的营销活动。针对这一类问题，美国监管机构主要通过限制金融数据的使用场景、限制特定场景中的共享数据类型和保障消费者选择退出（opt-out）的权利以避免金融数据滥用和滥用可能带来的危害。例如《公平信用报告法》中规定了信用报告使用的正面清单（Permissible purposes of consumer reports）；1996年的革新法案中要求信用局在向商业机构提供信用报告或其他信用数据，以进行客户拓展和营销时，只能“提供消费者的姓名和住址等用于识别身份的信息，不包括消费者与其具体债权人或其他企业的关系或经历的信息以及消费者报告的查询记录信息”[23]并应当为消费者提供拒绝被纳入该用于进行客户拓展营销的名单的选项。FTC在2003年《电话销售规则》（Telemarketing Sales Rule）[24]中建立了全国性的免扰电话登记簿（Do Not Call Registry），允许消费者将其电话放在限制拨入名单中，表明不愿接听销售电话的意愿。违反该规定进行电话销售的将可能面临高额罚款。上述规定在很大程度上规避或至少降低了金融数据的滥用风险。

概括而言，美国通过《公平信用报告法》等系列法案构建起了金融数据自由流通的法律基础，并在此基础上通过特定类型信息的收集与使用限制、隐私权益保障、消费者知情权与申诉权行使、建立金融机构信息安全保密标准、规范信用报告提供与使用等方面加以约束，保障金融数据的准确性与安全性；同时避免数据过度收集或滥用而对消费者合法权益造成的损害。

六、金融产业链数据困局的破局之路

（一）立法建议

未来个人金融信息的立法趋势，需要在个人金融信息保护和促进信息多方流转两者之间取得平衡。考虑到新兴市场参与者在大数据算法、金融科技产品开发方面的优势，如何确保其合法参与金融数据使用的生态圈，同时保证消费者权益和数据隐私安

[16] 15 U.S.C. §1861g.

[17] 15 U.S.C. §1861g (f).

[18] 15 U.S.C. §1861m(a).

[19] 自1971年以来，《公平信用报告法》曾历经多次修订，故称其为《公平信用报告法》及其革新法案。

[20] 15 U.S.C. §6801.

[21] 15 U.S.C. §314.2(b).

[22] 参见《FTC发布<2019年隐私和数据安全报告>》，载https://www.secrss.com/articles/17541，2020年3月2日。

[23] 15 U.S.C. §1861b (c)(2)，转引自张丽：《美国现代个人征信法律制度研究》，《安徽大学》，2019年。

[24] 16 CFR §310.

全，是值得探讨的问题。目前的立法建议思路包括：

1. 将新兴市场参与者纳入金融业监管的范围

央行颁布的《个人金融信息保护技术规范》将监管的对象定义为金融业机构。除了国家金融管理部门监督管理的持牌金融机构以外，金融业机构的范围还包括涉及个人金融信息处理的相关机构，例如提供身份验证服务的电信服务商、信息技术提供商、风控服务解决方案提供商、市场营销服务提供商等。考虑到个人金融信息的敏感性，对于涉及这些信息处理的服务提供商适用与持牌机构一致的数据处理标准，有利于避免信息被泄露或被滥用对于个人信息主体权益的影响。

2. 统一全行业的数据共享和使用安全标准，保证数据流转的安全可用

对于个人金融信息的委托处理而言，目前《个人金融信息保护技术规范》要求：1）C3类和C2类中的用户鉴别辅助信息，不应委托给第三方处理（第6.1.4.4.条b项）；2）应对委托处理的信息采用去标识化（不应仅使用加密技术）进行脱敏处理（第6.1.4.4.条c项）。因此，对于C2类别中与了解客户相关的信息（包括KYC信息、直接反映个人金融信息主体金融状况的个人财产信息、信贷信息等）而言，经过去标识化或加密技术以后仍然能够委托非持牌机构进行汇总和分析。结合美国引入商业性征信机构的经验，我国监管部门可以建立金融产业链全行业的统一安全标准，以及信息安全事件的应急和响应要求以保障客户数据信息的安全与保密性。

3. 设计征得数据主体同意处理个人金融信息的例外情况，从保障数据主体知情权、申诉更正权、用户退出等多角度兼顾数据主体权益

目前我国的《网络安全法》没有明确设定征得数据主体同意处理个人信用信息的例外情况。但是，考虑到个人征信产业链中众多的中间参与者间频繁的数据交互，并且不良信用信息的流转也可能难以获得数据主体的授权同意，建议对于个人信用信息的收集和信用报告的提供，设计征得数据主体同意的例外情况。[25]例如，借鉴欧盟《通用数据保护条例》，增设基于“履行合同或所必要的数据处理”、“为履行数据控制者的法定义务所必要的数据处理”或者“数据控制者或第三方为追求合法利益目的而进行的必要数据处理”等的其他信息处理合法性理由；[26]借鉴美国《公平信用报告法》、《公平信用和贷记卡披露法》等相关规定，将在满足特殊要求的情况下，对于授权同意的要求予以适当的降低。[27]此外，可以借鉴美国的实践，在金融业务办理所必需的数据处理场景下，通过数据主体知情权、申诉更正权、用

[25] 参见《征信业管理条例》第十五条：信息提供者向征信机构提供个人不良信息，应当事先告知信息主体本人。但是，依照法律、行政法规规定公开的不良信息除外。但是对于金融机构获取该个人不良信息是否事先告知信息主体本人即可而无需获得用户的授权同意，本条里并没有明确的规定。

[26] 参见欧盟GDPR，第6条。

[27] 依据美国《公平信用报告法案》（The Fair Credit Reporting Act，FCRA）第1681b（c）条的规定，消费者报告机构可以在满足以下条件的前提下，无经消费者授权对外提供消费者报告：（i）该交易包括一项确定的信贷或保险要约；（ii）消费者报告机构已遵守第（e）款；和（iii）消费者实际上没有选择根据（e）款，但是其姓名和地址排除在代理商根据此提供的名称列表中。而该报告的第1681b（e）条赋予了消费者选择退出未授权对外提供报告的权利，即如果消费者通过电话通知报告机构，该退出效力应持续两年，然后到期。如果消费者通过以下方式通知提交已签署的退出表格通知消费者报告提供机构，则该退出在消费者另行通知之前持续有效。

户退出等事后救济措施，达到兼顾数据主体权益的目的。

4. 限制个人金融信息采集和存储的范围

信用信息收集、存储的必要性标准并非是一成不变的，而是需要在考虑多种因素基础上动态平衡的结果，例如所办理具体的业务类型、贷款额度高低或还款周期、使用信息对个人权益的影响程度等都可能影响对收集信息必要性的判定。以美国的《公平信用报告法》为例，消费者报告机构不得包含过于时间过于久远的不良信用信息，例如十年以前的破产程序信息、七年以前的诉讼和判决信息、7年以前已付税的留置权信息、以及超过7年的逮捕，起诉书或记录定罪信息。然而，当针对超过$ 150,000的信用交易、承保超过150,000美元的人寿保险单等提供信用报告时，则可以包含上述的禁止性信息。[28]

5. 鼓励金融科技发展，保障数据流转、汇聚的安全

在《金融科技（Fintech）发展规划（2019-2021年）》鼓励跨地区、跨部门、跨层级数据资源整合应用的背景下，央行已经公开第一批纳入金融科技创新监管的试点应用向社会公开征求意见。其中不乏通过物联网、人工智能和区块链等方式，实现银行数据开放、共享，形成服务提供者、消费者、场景第三方应用开发者多方共生的生态圈方案[29]。同时，对“数据可用不可见”的技术解决方案的探索也已经成为重要的实践之一，通过密态计算、可搜索加密、同态加密等技术[30]对数据进行加密，并确保在可信执行环境中完成计算得出所需数据结果，将有助于降低原始数据直接共享中的隐私泄露风险[31]并进一步保障数据安全。

（二）企业建议

对于企业而言，加强对于数据源准确性和合法性的验证和管控、注重数据内部存储、对外共享的安全和目的限制，是参与金融链数据共享与融合、发挥数据商业化价值的前提条件。

1. 做好数据溯源与数据确权

对金融产业链的参与者而言，无论是内部数据融合还是外部数据获取，都需要首先明确对数据进行溯源，厘清可主张的使用性权益及其边界。

2. 补强数据来源的合法性

基于数据盘点以及溯源、确权的结果，参与者还需相应完善对用户的告知和授权流程、加强对数据提供商数据来源合法性的确认和义务要求。此外，考虑到金融产业链多方主体参与的现状，宜考虑通过加强产业链条各个环节市场主体的合作，使得数据来源合法性的补强“事半功倍”。

3. 优化商业模式

金融行业日趋严格的监管态势也为向银行提供服务的机构提出了更大的挑战，其可能需要从多个方面加大对商业合作模式的改造投入，包括但不限于：

- 增强技术研发能力：从直接输出原始个人信息到衍生数据或者技术能力的输出，从而避免个人金融信息收集和使用的限制；
- 开发面向消费者的新型业务类型：新兴市场参与者可以考虑开发面向消费者的新型业务类型，在不违反法律法规强制性要求的前提下，根据消费者的请求向金融机构提供相关信息；
- 保持商业模式的可持续性：确保优化后的商业模式能够实现盈利才能维持健康的发展。

4. 加强第三方数据管控

从防范合规风险角度来看，个人金融产业链的参与者在对外转让、共享数据时，可能需要：

- 审查第三方的业务资质和实际业务开展情况以判断该第三方非法从事个人征信业务活动的可能性；
- 通过合同约定或根据实际情况（如第三方曾于近期内受到监管部门监察或处罚）要求第三方提供用户授权原始文本、签署数据授权承诺函等，以确保第三方已经取得信息主体的相应授权；
- 开展信息安全影响评估，并通过尽职调查、审计等方式对第三方进行必要的监督。

（本文发布于2020年03月10日。）

[28] 参见FCRA，第1681c（b）条。

[29] 参见《详解央行首批金融科技试点项目：入选依据、技术运用及机构亮点》，零壹财经，载https://www.chainnews.com/articles/897264150003.htm，2020年2月11日。

[30] 参见高少华：《“可用不可见”技术有望成数据保护新趋势》，载http://www.xinhuanet.com/fortune/2019-08/29/c_1210261495.htm，2019年8月29日。

[31] 参见《区块链让数据“可用不可见”，支付宝隐私保护引入技术保障》，载https://www.lieyunwang.com/archives/461074，2019年11月25日。

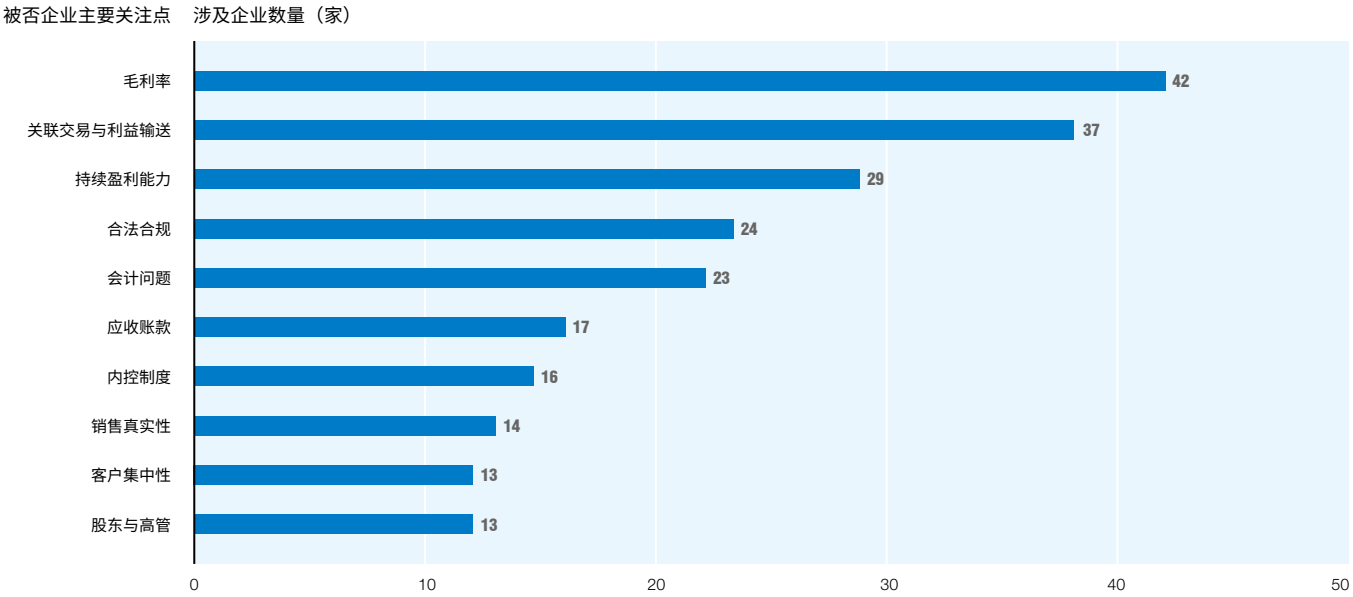
宜未雨而绸缪——企业上市关注的重点数据合规问题

党的十九届四中全会《中共中央关于坚持和完善中国特色社会主义制度、推进国家治理体系和治理能力现代化若干重大问题的决定》首次增列“数据”作为生产要素，提出**“健全劳动、资本、土地、知识、技术、管理、数据等生产要素由市场评价贡献、按贡献决定报酬的机制”**。随着云计算、大数据分析和物联网等技术的持续发展，数据作为国家基础性、战略性的资源以及企业的竞争资产，已经受到各界的认可和接受。**对于拟申请上市的企业而言，数据不可避免地将成为企业资产价值评估的核心与重点。**

另一方面，依托于互联网、大数据、云计算等业务平台的数据驱动型企业，在业务开展的过程中积累了庞杂繁多的各类数据，利用数据商业化进行变现与盈利，将进一步拓宽数据驱动型企业的增值空间。**在企业积极探索数据资产商业化的过程中，如何确保合法合规地获取、流通、应用数据，是企业数据商业化的首要任务，也已经成为证监会重点关注的问题之一，并成为影响企业上市成功与否的重要因素。**2017年至今，已有不少企业申请IPO时被审批机构询问数据合规问题，此类问题甚至成为了一些企业IPO申请被否的原因之一。

一、上市主管机构紧密关注上市申报企业的数据合规

《首次公开发行股票并上市管理办法》、《首次公开发行股票并在创业板上市管理办法》和《科创板首次公开发行股票注册管理办法（试行）》均明确将发行人生产经营符合法律、行政法规的规定，符合国家产业政策作为企业IPO上市的必要条件。发行人作为信息披露第一责任人，应当诚实守信，依法充分披露投资者作出价值判断和投资决策所必需的信息，所披露信息必须真实、准确、完整，不得有虚假记载、误导性陈述或者重大遗漏。数据显示，在IPO未过会的企业的反馈意见中，合法合规问题是出现频率最高的风险关注点之一，数据合规问题作为证监会目前关注的重点，不容忽视。



图：2018年IPO被否企业原因分析[1]

[1] 摘自理脉Legal Miner“2018年IPO审核反馈情况数据分析报告”，http://www.legalminer.com/blog/?p=3307。

自《网络安全法》2017年6月1日正式实施以来，网络安全与数据合规在立法的基础上得到了快速的贯彻，并愈发受到网信办、工信部、公安部等监管部门的重视。基于上市申报过程中的信息披露义务，企业将**不可避免地需要在信息披露过程中直面其数据处理过程可能产生的业务风险，数据处理相关业务商业模式的合法性，及其对企业未来持续发展的影响**。在我们处理的数据合规项目中，主管机构不仅明确关注数据来源、数据处理的普通合法合规问题，并进一步追问涵盖数据采集的方式、对象、价格、趋势、成本等深层次的问题。在部分项目申请上市过程中，主管机构已经不满足于拟上市客户公司对于数据业务所提供的概括性、原则性的说明，而进行**多轮、递进式的问询**，以便获取详尽的答复。

二、上市主管机构提出的数据合规问题综述

根据证监会公开披露的审核公告以及我们的法律实践，我们对上市主管机构对拟上市企业提出的数据合规问题进行了整理，主要可以分为数据来源合法合规问题、数据使用合法合规问题、数据相关的业务经营问题三类。

（一）数据来源合法合规问题

数据来源合法合规性是主管机构关注点的重中之重。以下是上市主管机构提出的部分数据来源合法合规问题的示例：

- 请说明发行人获取用户数据及标签的过程及方法，是否对用户有明示提示，用户授权在法律上是否完备，是否明确告知收集信息的范围及使用用途，发行人获取用户数据的手段及方式是否合法合规；
- 请说明发行人为客户提供数据分析服务时，主要的数据获取途径；
- 请说明要求发行人说明是否对数据来源进行分类，数据采集和应用过程中是否获得用户许可，是否存在侵犯用户权益（隐私权、肖像权等）的情形；
- 请说明发行人采集数据（包括自行采集，也包括向供应商采集）时，是否获得了相关信息主体（及用户）的合法授权，获取用户数据的手段及方式是否合法合规；
- 发行人收到APP专项治理组发出的《关于APP收集使用个人信息相关问题的通知》，APP专项治理工作组要求发行人就收集使用个人信息中存在的问题进行整改。请发行人代表说明；
- 请说明发行人收集、整合、处理、使用数据是否符合《数据安全管理办法》的规定，是否存在违反收集使用规则使用个人信息的情况，发行人相关内部控制措施是否合法合规并得到有效执行。

为答复上市主管机构提出的上述问询，并通过主管机构的审批。我们理解，**首先，企业须确保其自行收集个人信息时已经征得个人信息主体对收集、使用的目的、方式与范围的充分授权同意，并符合收集信息的必要性原则；其次，企业应重视其自行收集个人信息的途径的合法性，如禁止使用非法的爬虫技术从其他网络运营者的平台抓取数据；再者，在从数据供应商间接获取个人信息的场景下，企业还应关注供应商的数据来源合法性，要求供应商就个人信息的充分授权提供有效、充足的承诺与证明，确保授权范围能覆盖企业处理数据的业务需求。**

（二）数据使用合法合规问题示例

数据使用的合法合规，既要求企业在处理个人信息时充分保障个人信息主体的相关权益，也要求企业采取严格的数据安全保护措施。以下是上市主管机构提出的部分数据使用合法合规问题的示例：

- 请说明发行人**使用用户数据是否合法合规**，尤其是商业化变现的合规性，请对照《网络安全法》、《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》、《信息安全技术个人信息安全规范》等法规和司法解释，说明报告期发行人是否存在侵犯用户隐私或数据的情况，是否存在法律风险或潜在法律风险；
- 请说明在报告期内发行人对**个人消费者及企业客户信息等数据资源的使用和维护的合法合规性**，是否存在纠纷或潜在纠纷，并进行风险提示；

- 数据获取、使用、处理等过程的**内部控制制度及执行情况**，对数据安全和个人隐私的**保护措施与手段**，是否出现过个人信息、隐私泄露事件，是否存在纠纷或潜在纠纷；
- 请发行人**说明**其数据供应商的合规性、是否对数据供应商建立完善评价体系、是否向第三方提供数据。

从上述问询示例可以看出，为满足数据使用合法合规的要求，**企业需要重点关注三个方面：其一，在数据使用（包括数据融合）的过程中，应确保不会超出相关个人信息主体的授权范围；其二，做好数据安全管控，采用加密存储、设置访问权限、数据备份、选用多个服务提供商等多重数据安全风险防控措施；其三，严控数据的对外输出，在对外转让、披露、共享个人信息时应获得个人信息主体的充分知情同意，并确保数据转让、共享的接收方具有充足的数据安全保护与管理能力。**

（三）数据相关的业务经营问题

在数据相关的业务经营问题方面，上市主管机构更多关注企业数据相关的商业模式的可持续性和收益情况，以下是主管机构提出的部分数据相关的业务经营问题的示例：

- 报告期各类数据所对应的数据采集方式和供应商、**数据采购成本、数据分析方式、产品服务内容**；
- 在向供应商采购数据的数据采集方式下，**主要的交易对手方、主要交易对手**在报告期内是否发生重大变化，与不同交易对方的采购单价是否存在重大差异及原因；
- 请说明发行人不同来源获取**数据的所有权归属**情况；
- 请说明发行人是否掌握核心数据来源，此种**运营模式是否与同行业可比公司相同或相似**，是否对数据供应商存在重大依赖；
- 针对各主要信息采集内容所对应的劳务费等问题，与同行业可比公司及数据采集市场的比较情况及差异原因。

从上述问询示例中，我们可以看到上市主管机构对于**数据使用权益、数据商业化模式可持续性的关注。为更准确地评估企业的数据使用权益和数据商业化模式，一方面，企业须充分认识其各类数据资产的权益边界，这要求企业对其数据从安全、合规与价值的三个维度开展充分的分级分类评估，进而明确对各类数据分别可提出的权益主张。另一方面，企业应在明确数据资产边界的前提下构建数据资产管理体系，在合规、安全的基础上充分挖掘各类数据作为资产的商业价值。**

三、上市主管机构认定数据业务合法合规性的参考依据

从证监会在审批公告中披露的数据安全相关质询问题描述看，审批部门不仅会对照《网络安全法》、《儿童个人信息网络保护规定》、《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》等已经生效的法律法规和司法解释，还会将国家推荐性标准《信息安全技术个人信息安全规范》（**《个人信息安全规范》**）作为参照依据，**甚至关注APP专项治理工作组公开的整改通知，要求企业对整改通知中披露的数据安全相关问题进行具体说明。**

由此可见，在我国个人信息保护法律法规尚未完整建立的前提下，上市主管机构与网信、公安、工信等个人信息保护行政监管部门一样，会将《App违法违规收集使用个人信息行为认定方法》（**《认定办法》**）、《个人信息安全规范》等监管部门或行业的合规指引和标准作为认定数据业务合法合规性的参考依据。同时，上市主管机构也会慎重考虑上述行政监管部门或其授权机构的行政执法和监管案例。

对于拟申请上市的企业而言，应当对标上市主管机构的评估依据，密切关注最新的数据保护相关的立法动态、数据合规执法和监管趋势。概括而言，企业应当：

（1）严格遵守各监管部门制定的网络安全与数据保护规范性文件，特别是自2019年以来出台的正式文件，包括《网络安全审查办法》、《密码法》、《儿童个人信息网络保护规定》、《网络信息内容生态治理规定》和《认定方法》、《信息安全技术 个人信息安全规范》(GB/T 35273-2020)等，以及可能于2020年出台正式文件的重要草案，如《民法典（人格权编）》、《数据安全管理办法（征求意见稿）》、《网络安全审查办法（征求意见稿）》、《个人信息出境安全评估办法（征求意见稿）》和《个人信息安全规范（第三次征求意见稿）》等；

（2）关注并积极应对日益活跃的多部门数据合规联合执法活动。2019年，中央网信办、工信部、公安部和市场监管总局在全国范围内联合开展的App违法违规收集使用个人信息专项治理取得了阶段性的成果。随着《认定办法》的出台，可以预见，网络安全与数据保护严格执法必将持续；

（3）以各执法部门发布的执法公告与案例为鉴，随着执法活动的深入，监管部门会通过公告或通报的形式对外公开具体的执法案例，如工信部《关于侵害用户权益行为的App通报》（第一批于2019年12月底发布，第二批于2020年1月初发布）。企业在开展数据合规工作的过程中，宜持续跟踪公开的执法案例，相应调整自身的产品、服务设计与合规实践。

四、重点数据合规问题应对之数据来源合法合规

数据收集是数据全生命周期的起点，数据来源的合法合规是数据处理、数据商业化开发的前提条件。通常企业收集用户数据的来源主要包括：（1）直接面向用户收集；（2）从公开网络平台或半公开网络平台采集用户数据；（3）从合作方间接获取用户数据。**针对不同的数据来源，企业不仅应当采取不同的合规措施和应对方案，确保数据来源的合法性，还应该形成数据处理记录或其他必要的自证合规的记录材料。**

（一）直接面向用户收集——授权同意

在目前既有的法律法规体系下，对个人信息的处理仍以“授权同意”为核心展开。为了从源头保证和提升数据的质量，企业应当注重商业模式的优化和调整，为数据采集、数据可持续处理奠定合规基础。

企业应当基于公司实际的数据处理情况和需求，依据《认定方法》、《个人信息安全规范》的相关规定，重新审查和评估企业现有的隐私政策和其他用户告知授权文本的合规性；根据最新的监管要求和执法监督案例，对各产品业务线的隐私政策和其他用户告知授权文本进行针对性的完善，不仅要确保数据处理合法性中授权同意的获取，同时也应当在遵守必要性原则的前提下以合理、合法的方式预留后续发展的空间。值得注意的是，信安标委公开的《信息安全技术 移动互联网应用（App）收集个人信息基本规范（法律意见书）》列出了地图导航、网络约车、即时通讯、博客论坛、网络支付、新闻咨询、网上购物等21种常用服务类型收集的最小必要信息，服务类型最小必要信息涉及的最小必要权限范围。

按照当前的监管要求，企业应当在隐私政策和其他授权文本中，根据收集使用个人信息目的（包括委托的第三方或嵌入的第三方代码、插件），逐一列出收集使用个人信息的目的、方式、范围，否则存在被认定为“未明示收集使用个人信息的目的、方式和范围”。对于存量的可能存在授权瑕疵的数据，企业应当尝试通过隐私政策推送或更新的方式，再次取得用户的补充授权。如果无法取得补充授权，企业应当对存在瑕疵的用户进行数据清洗与分类，并对高风险的数据进行数据隔离或删除。避免因对外法律文本的缺失或不足引发各方对企业合规性程度的质疑和挑战。

（二）从公开网络平台或半公开网络平台采集用户数据

除用户主动提供、企业运营APP时网络系统自行收集的个人信息以外，为提升用户数据的价值，部分企业会自行或委托第三方通过爬虫技术从公开网络平台或半公开网络平台抓取数据，与企业直接收集和企业从供应商处获取的数据进行融合和商业化使用。

爬虫技术是互联网企业普遍运用的网络信息搜集技术，为数据收集者提供了极大的便利。但同时，爬虫技术的滥用也可能对其他网络运营者的正常经营造成不利影响，如导致网页瘫痪、侵犯他人知识产权等合法权益，从而可能引发民事乃至刑事责任。自2019年9月以来，公安机关就对未经授权使用爬虫技术等非法获取个人信息的行为进行查处。企业应重新审视自身数据获取手段和方法的合规性，尤其应当避免从违法违规的供应商采购数据，或者采用可能破坏目标网络平台信息系统的技术进行数据采集，以免构成“非法获取计算机信息系统数据罪”或者“侵犯公民个人信息罪”。

除刑事责任以外，不当使用爬虫技术也有可能引发诉讼争议。尽管现行的法律法规并未对于个人信息等相关的数据财产权益做出任何明确的规定，但国内多个典型的互联网不正当竞争纠纷案件（包括淘宝（中国）软件有限公司与安徽美景信息科技有限公司不正当竞争纠纷案（（2018）浙01民终7312号）、北京淘友天下技术有限公司等与北京微梦创科网络技术有限公司不正当竞争纠纷案（（2016）京73民终588号）等）都认可了网络平台对其数据资产的权益，行业、法律实务界和学术界也逐步认可了网络平台之间共享用户数据的“三重授权原则”，即**“用户授权平台方+平台方/第三方授权+用户授权第三方”**。企业在未取得上述三重授权的前提下，通过爬虫技术从第三方网络平台不当采集数据，也有可能构成不正当竞争的行为。

（三）从合作方间接获取用户数据

数据驱动型企业虽积累了大量的数据和相关模型能力，但内部的数据源总是或多或少存在一定的欠缺，此时，外部第三方数据源将成为产品功能实现中重要的“生力军”。但谈到第三方数据源，以下数据合规问题将无法绕开：（1）供应商数据来源合法吗？（2）供应商的用户授权是否能够覆盖企业处理数据的所有业务需求？（3）如何核查第三方数据源的合法性？

为此，企业应当按照以下步骤确保引入的数据供应商数据来源的合法合规性：

（1）核实引入第三方数据源的必要性和可行性；

（2）要求第三方数据源就用户授权提供有效、充足的承诺与证明；

（3）确保第三方数据的用户授权范围足够覆盖企业处理数据的业务需求；

（4）制定《外部数据采购管理制度》并严格按其提请流程。

五、重点数据合规问题应对之数据使用合法合规

（一）数据融合的合规重难点

数据融合是挖掘数据资产价值的重要手段，目的在于利用多渠道、多元化的数据，形成更加完善的用户画像，其中必然涉及大量用户个人信息与行业监管数据的收集与处理。因此，数据融合的合规重难点在于，从源头与过程把握相关数据的安全保障与合法利用。

就“源头控制”而言，首先，在数据使用（包括数据融合）的过程中，企业应确保不会超出相关个人信息主体的授权范围。在满足数据处理必要性的前提下，考虑到针对超出初始范围的个人信息处理活动再获得授权的可行性较低，企业应注意在初始授权范围中保留一定的弹性空间，以尽可能符合目的关联性的要求。同时，企业应当梳理数据融合涉及的个人信息与行业监管数据，以便识别合规风险，确认在数据处理中可能面临的合规要求（如在数据采集、存储、使用或共享方面的要求）。

就“过程控制”而言，企业应当根据具体的数据融合商业模式（同一实体内打通vs同一集团内打通），确定企业在数据融合中的角色定位（数据控制者、数据处理者还是共同数据控制者）。在确定数据处理角色后，企业可以根据具体的数据处理角色，以合同、尽职调查、审计等方式促进合作方相应权利义务关系的落实。

更多数据融合相关的介绍可以参见本刊中《**“数”年快乐——万字长文说“数据融合”》一文**。

（二）数据对外共享的管控责任

数据流通才能最大化地实现数据的价值，但数据的流转也增大了数据泄露等数据安全风险。根据《网络安全法》、《个人信息安全规范》等相关法律法规和标准规范，对于个人信息而言，企业在对外转让、披露和共享收集的个人信息时应当承担严格的注意义务：

1、个人信息主体的授权同意：企业应当在对外共享收集的个人信息前，充分告知共享、转让个人信息的目的、数据接收方类型和可能的后果；

2、协议管控数据接收方（包括接入平台的第三方）：通过合同等方式明确双方角色定位，并据此规定个人信息接收方的责任和义务，在发现接收方违反法律法规或约定处理个人信息时立刻要求停止该行为与采取补救措施；

3、必要的安全风险评估：企业在向他人提供个人信息前，应当评估可能带来的安全风险，但特殊情况除外，如从合法公开渠道收集且不明显违背个人信息主体意愿；个人信息主体主动公开；经过匿名化处理等；

4、数据共享记录留存：留存与第三方交互、共享个人信息的日志记录、合同文本，作为企业自证合规的材料文本。

（三）数据安全风险控制

数据安全是个人信息保护和处理的前提条件，数据泄露、灭失对企业带来的毁灭性打击已足以敲响警钟，同时也会带来媒体的广泛关注。

为保障数据存储的安全合规，企业应将安全合规思维纳入到产品设计过程中：

1、及时采取风险分散措施，例如选用多个服务提供商、数据本地备份等；

2、及时采取风险控制措施，例如选择合格服务提供商、完善与服务商之间的权利义务约定等；

3、适当采取风险对冲措施，例如购买商业保险等。

另一方面，随着产品功能的初步确定，功能调用完成或者服务结束后，数据如何处置也会成为数据驱动型企业的难题。根据当前的监管要求，在服务结束后或具体数据处理目的实现后，原则上，个人信息控制者应当及时删除或匿名化相关个人信息。

六、重点数据合规问题应对之数据相关的业务经营问题

（一）明确数据资产权益边界

发掘数据资产的商业价值，需要以清晰的权益边界为前提和基础；数据权益与权属不清，则意味着交易必然存在瑕疵，监管层面存在疑问，相应地也伴随着法律风险。数据权属的准确认定目前在立法和实践中仍缺乏一致性意见，而权益的边界亦错综复杂。

（二）数据资产管理体系构建

寻求权益主张空间奠定了数据资产固定的理论基石，但为了确保数据资产的实际形成和价值发挥，企业仍需要相应构建必要的数据资产管理体系，以求能得到及时、准确的数据支持和服务。考虑到数据资产具有较强的流动性，因而在构建数据资产管理体系时，除遵循基本的数据治理规则以外，还需要加强对数据价值的梳理和管控。具体而言，分为：

（1）第一步：定义**数据**资产，包括特定模型下的数据资产盘点、数据资产的分级与分类；

（2）第二步：管理数据资产，包括数据资产安全管理和数据资产价值管理。

更多数据权益及数据资产相关的介绍可以参见本刊中《**平安夜里说平安——“数据资产”的误区与合规条件**》一文。

对于拟上市的企业而言，上述数据合规问题需要从技术、商业和合规多个层面来梳理及整改。总的来说，数据合规工作“宜未雨而绸缪，毋临渴而掘井”，为保证企业上市计划的顺利实施，建议企业尽早启动数据合规工作，结合自身业务建立合规体系，才能在上市过程中提交满意的答卷。

（本文发布于2020年01月13日。）

敢为天下先
——特区培育数据要素市场的契机与合规要点

2020年10月11日，国家以设立经济特区40周年为契机，在中央改革顶层设计和战略部署下，支持深圳实施综合授权改革试点。中共中央办公厅、国务院办公厅印发了《深圳建设中国特色社会主义先行示范区综合改革试点实施方案（2020－2025年）》（简称《方案》），支持深圳率先完善要素市场化配置体制机制，加快培育数据要素市场。具体而言，深圳应当率先“完善数据产权制度，探索数据产权保护和利用新机制，建立数据隐私保护制度。试点推进政府数据开放共享。支持建设粤港澳大湾区数据平台，研究论证设立数据交易市场或依托现有交易场所开展数据交易。开展数据生产要素统计核算试点。”[1]

当前全球各国逐渐认识到数据本身蕴藏的经济价值与改造能力，纷纷强化“数据主权”的理念并提出愈发严苛的监管要求。在此背景下，我国数据立法呈现出以个人信息及重要数据保护为核心，构建基本法律、行政法规、司法解释、部门规章及国家标准等立体的综合监管规则框架。但在数据法律监管方面日趋严格的同时，国家也高度重视信息时代数据要素的经济价值，继续以数据安全、个人信息保护为基础，逐步有序完善数据要素产权制度，为大数据作为生产要素流通赋权。

企业在改革推进的过程中，应当充分理解数据要素相关的改革方案政策，高度重视并遵守以国家安全、网络安全、个人信息保护为核心的数据法律体系，积极参与到数据要素市场培育的改革方案实践之中。

一、数据产权制度完善

（一）数据产权制度现状

在数字经济快速发展的浪潮下，数据的经济价值与功能效用被逐渐挖掘，数据成为企业间乃至国家间重要的竞争资源。随着中央对数据市场要素属性与地位的进一步确认，建立健全数据产权保护规则体系成为保障数字经济稳步发展的重点课题。事实上“数据产权”这一概念并不陌生，早在2016年国务院所印发的《“十三五”国家信息化规划》附件中就曾将“加强数据资源管理，建立数据产权保护、数据开放、隐私保护相关政策法规和标准体系”作为重点任务交由国家发展改革委、中央网信办等多个部门共同负责。而在此后国务院以及各省的多份文件中，也纷纷将探索完善建立健全数据产权保护机制作为重要工作任务予以提及。

相较于一般的有形资产，数据本身的无形性和易复制性导致企业在进行数据积累和应用过程中，可能会产生诸多关于数据归属的纠纷争议，不同主体就数据分别能够主张怎样的权益，仍是悬而未决的核心问题。纵观目前我国及全球数据相关立法，就上述问题均尚未有明确的定论。而现有司法实践也多从不正当竞争、侵犯商业秘密、违反协议约定使用等具体等场景下为企业的数据权益提供有限的保护路径。现有保护方式与保护力度都存在局限与不足，不能从经济产权的基础上，理顺数据流通产业链条，加快数据生产要素变现的安全转化。

（二）深圳尝试确立数据产权

值得注意的是，今年7月的《深圳经济特区数据条例（征求意见稿）》（简称“《条例（征求意见稿）》”）中创设性提出“数据权”的概念，将“数据权”定义为“权利人依法对特定数据的自主决定、控制、处理、收益、利益损害受偿的权利”，并规定“自然人对其个人数据下依法享有数据权”、“公共数据属于新型国有资产，其数据权归国家所有”、“数据要素市场主体

[1] 中共中央办公厅 国务院办公厅印发《深圳建设中国特色社会主义先行示范区综合改革试点实施方案（2020－2025年）》。

对其合法收集的数据和自身生成的数据享有数据权”，尝试解决数据要素产权配置问题，明确不同主体对于数据的财产属性与归属，从根本上解决数据活动中主体权利、义务以及责任边界不清晰的问题，为数据要素市场的培育在政策扶持的基础上提供法律依据。

虽然《条例（征求意见稿）》尝试规定个人、企业及国家分别就不同数据享有数据权，但并未就数据权属的主体认定提供指引，同时未就数据权的具体使用方式提供行为认定依据。因此，当三者就同一数据分别主张权利时，可能较难对各主体的权利边界进行界分，较难规范数据权的行使的认定，从而难以解决衍生的要素分配问题。深圳作为我国改革开放的先锋，《条例（征求意见稿）》的公布获得了国家政策的有力支持，虽然还存在着法律位阶与具体实践的疑问，但《条例（征求意见稿）》的公布已经有利的向社会传达了我国数字产权立法的决心与进程提速的重要信号。

（三）企业数据资产建设

在数据产权制度完善的过程中，现有数据产权实践有待相关立法及政策进一步落实指引。当前，公私法相结合、全方位多层级的数据保护规则体系正逐步完善，对于企业而言，应当以《民法典》、《网络安全法》、《侵权责任法》与各行业相关法律法规、行政规章所确立的网络安全数据保护体系为指引，自主做好企业数据资产、体系的完善工作，实现数据资产价值，具体而言：

- **夯实网络及数据安全建设。**目前，外部网络侵入与内部人员泄漏公司数据，已经成为企业数据安全与资产风险的重大隐患。保证网络及数据安全是企业开展日常业务、商业化使用数据的基础与前提。企业应以强调“主动防御、动态防御”的等保0推进数据安全，同时积极建立数据安全风险控制机制，并通过访问权限控制、数据调取审批流程、技术防控措施等多种手段进一步加强内部数据安全管控。
- **重视数据合规体系建设。**随着数据与个人信息保护相关立法及国家标准相继出台，《个人信息保护法（草案）》于近日提请审议，同时，监管部门数据执法的力度与广度呈现不断加强的趋势。因企业数据合规工作的欠缺，给企业带来负面影响事件屡见不鲜。因此企业应加强业务数据全生命周期合规管理，积极梳理业务中所涉及的个人信息、重要数据及其他行业数据，并严格参考相关法律法规、国家标准及行业标准的要求合法合规收集、使用、共享、存储相关数据。
- **积极探索集团内部数据融合打通路径。**集团企业旗下业务条线丰富多元，涉及不同行业和领域，能够获取大规模、多属性、跨领域的数据。在合法合规的基础上，整合集团内部数据将为企业发展带来极大的便利，推动业务转型升级，充分发挥数据资产价值。
- **固定数据资产，发挥数据价值。**企业应当继续重视既有法律体系对于数据相关的经济产权保护，利用数据库、商业秘密、软件著作权等现有法律体系，稳固数据资产的框架。同时，企业应结合自身实际情况，根据不同维度对数据资产进行分级和分类，全方位地规划数据资产的信息模型，有效夯实对于数据资产的管理。

二、大湾区数据平台建设

（一）中央政策与地方政府立法为大湾区成立数据平台特别赋能

本次《方案》的发布，是在国家政策支持与立法规范集中出台的背景下，系统完善数据产权与核算探索，为大数据交易论证与实践提供了制度保障与法律依据。今年3月出台的《中共中央国务院公布关于构建更加完善的要素市场化配置体制机制的意见》（简称《意见》），首次明确**将数据作为第五大生产要素，体现数据要素的重要性及价值。**其次，6月发布的《中华人民共和国数据安全法（草案）》（简称《安全法（草案）》），明确了在安全基础上，鼓励数据作为生产要素有效流通，**使数据交易平台服务既符合政策指引，又得到法律认可。**再次，深圳7月发布的《条例（征求意见稿）》**对数据安全法进行详细解读，尝试规范不同的数据产权。**最为重要的是，本次制定的《方案》，将明确落实加快培育数据要素市场体制机制，并将改革成果提上日程。

（二）大湾区数据交易中心优势地位

作为新型生产要素，国家鼓励海量数据流动。大数据重要的价值在于其数据样本的大规模、多属性、跨领域、真实性，能够产生聚集规模的经济效应。大数据交易平台的建设可以打破信息孤岛及行业信息壁垒，通过大数据交易的形式，挖掘海量高价值数据，满足数据市场多样化需求，完善产业生态环境，推动智慧经济，并对改革各方面的赋能具有深远意义。自国内第一个数据交易平台成立后，数据交易中心的管理与交易模式具备了一定的探索，形成了一定的交易规模，然而国内大数据交易还处于初级阶段，产权制度有待立法完善，交易规范尚未统一，整体发展模式也处于摸索过程中。

大湾区覆盖中国互联网产业较为成熟的11座城市，市场丰富庞大，数据保有量与数据需求整体为国内第一，具备形成数据生态产业化的规模效应。同时，大湾区行业丰富，数据种类与衍生数据服务丰富，适宜作为对不同类型数据产权与核算规范方式的探索试点，有利于产生协同效益。第三，大湾区覆盖三个司法管辖区域，有利于进行不同司法辖区数据交易、监管、争议的制度探索与研究。

（三）大数据交易市场关注问题

在产权明确的基础上，大数据交易市场需要以国家安全、数

据安全、个人信息保护等安全要义为核心，探索数据要素流动的动态平衡。一方面，平台作为管理者，将对数据存储的收集与管理、对企业资质鉴别、交易备案进行顶层设计，保障交易合法安全；另一方面，平台作为交易过程的参与者，应当会同企业探索安全便利的交易模式，协助企业变现。具体而言：

- **在数据交易合规的问题上，监管机构、平台应当共同探索大数据交易的资质与监管模式，事前确保大数据交易合法。**企业应当重新检视数据业务顶层设计，挖掘盈利增长点，及时做好数据开放交易的业务转型合规应对。
- **在数据收集存储的问题上，平台应当会同监管机构制定并落实大数据治理标准，确立数据标准化与更新机制，确保平台数据的清洁性、真实性及时效性，为数据商品流通清除障碍。**同时，企业应当重视保有数据分类，全面清洗、梳理、盘点已有数据资产，为数据资产交易做好准备。
- **在数据交易变现的问题上，企业应当积极参与到大数据交易当中。**主动探索数据商品的供求关系价格特点，为平台提供多行业、多模式、多场景的交易样本，既可以验证数据产权制度的合理性，也可以探索数据核算的可行性。
- **在数据交易安全的问题上，平台应当充分探索区块验证技术的优势，归纳研究企业数据交易实例问题。**注重数据交易使用限制、审计、保密条款的设计，制定模范条款，防止大数据泄露与不正当竞争给行业链条造成恶性冲击。
- **在数据交易监管与争议解决问题上，存在数据于港澳司法管辖区流动场景。**这为企业、监管与司法机关在数据跨境流动的场景下，提供了难得的低风险实践环境。必将有助于积累中国大数据治理经验，树立未来国际大数据合作的主导地位，意义非凡。

三、开展数据核算与统计试点

（一）数据作为数字时代生产要素的交易价值

国家高度重视数据交易变现与资本核算的探索，明确数据产权并进行核算统计是数据成为安全、公允、合法资产的两个基本前提。数据核算统计，是确立数据会计的计量与描述方法。确立数据要素的核算统计，将把数据的交换价值推向交易场景更为广阔活跃的资本市场，为公司的运营与资本市场变革增添新型动力。

（二）数据定价和数据核算统计的实践经验

自2015年国务院发布的《促进大数据发展行动纲要》指出“建立健全数据资源交易机制和定价机制”以来，市场在数据交易定价的实践中积极探索，形成了一些以行业数据、使用场景因素而异的交易变现与计量方法的阶段性成果。但大数据要素复杂的权属制度安排，与其特异于传统生产要素的经济特性，将导致数据要素核算统计机制与现有会计制度存在不小差异。

国内外实践对于大数据的定价主要基于两种方式，一是基于博弈论的协议定价，即数据拥有者和数据购买者通过协商对价格达成统一，这是目前应用较为广泛的数据定价方法；另一种是可信第三方定价，在拥有者无法准确针对数据进行定价的情况下，可委托可信第三方进行交易。我国数据交易平台，目前主要采取根据数据量、完整性、时间跨度、稀缺性等质量指标，对数据交易进行统计与定价。

（三）数据定价和数据核算的难点与探索方向

围绕着数据要素充盈市场经济的需求，从《公司法》《证券法》等要素资本融、投、管、退的法律体系与安全与规范来看，探索数据核算主要存在统计核算和会计资产核算两个并行方向。主要难点在于对海量、高速、实时更新的数据资产进行多维度的统计困难，与对异质数据、区分应用场景、数据二次开发等所带来的价值估算困难。具体而言，数据作为承载信息的载体，其价格既与数据体量的多少相关，又与数据质量的高低相关，更与特定的应用场景相关，因而很难制定出明确且公允的定价依据和标准。加之数据异质化和非标准化，以及交易双方关于交易数据的信息不对称等因素，使得数据定价更为困难。在建立粤港澳大湾区数据平台的过程中，可考虑从以下方面入手：

- **发展区块技术与可信计算，为数据核算提供有效的统计验证方式。**在探索核算机制的过程中，可以充分借鉴区块技术，区分应用场景与数据颗粒，进行分门别类的针对性统计。经过系统地归纳各行业大数据交易情况，结合现有会计制度，探索迭代出一套合理、公允的核算方式，防止出现数据泡沫。
- **探索数据资产在不同司法辖区资本市场中流通得的统一模式。**在不同资本市场中，如何协调大湾区不同司法辖区核算标准，确保数据资产安全与资本有效地流动，也将成为一个核算统计实践研究方向。

四、推进政府数据开放共享

（一）政务数据开放法律依据与现状

2015年发布的《促进大数据发展行动纲要》指出，应形成公共数据资源合理适度开放共享的法规制度和政策体系，以此为基础，《政务信息资源共享管理暂行办法》对政务信息资源目录编制、分类与共享、提供与使用等方面提出要求。[2]随后，各省市陆

[2] 政务信息/数据资源与政府的数据概念类似，可归纳为政务部门在依法履行职责过程中制作或获取的，以一定形式记录、保存的各类数据资源。公共数据（资源）的概念略有不同，除政务部门的数据资源外，其还包括具有公共管理和服务职能的企事业单位在依法履职或提供公共管理和服务过程中收集或产生的数据资源。

续出台相关规定，加快推动与落实政务信息系统互联和公共数据共享、开放与利用。[3]政府数据共享分为无条件共享、有条件共享与不予共享。[4]数据共享应以共享为原则，不共享为例外，被列入有条件共享和不予共享的政府数据需有法律法规和规章为依据，同时应当明确有条件共享的政府数据的具体共享条件。类似地，政府数据开放也分无条件开放、有条件开放和不予开放。[5]《公共信息资源开放试点工作方案》还要求政府数据开放应满足完整性、机器可读性、格式通用性等要求。

目前，深圳市政府数据开放平台位于全国政务数据开放前列，已自主编制了可下载的开放数据目录，并同步定制了相关数据集开发的应用。同时，深圳平台已为部分有条件开放的数据集开设了申请功能，并提供了多种应用规范格式。企业通过申请使用政府的数据，形成了一批具有高商业价值的政府数据产品，如利用疫情开放数据开发的“城市疫情场所地图”，通过标注疫情场所信息，卓有成效的为市民进行了风险提示。

（二）政府的数据共享与开放的实践问题与展望

政府的数据开放对建设法治政府、整合社会数据资源、发展壮大数字经济而言具有重要意义，但在积极实践的过程中也有诸多问题丞待解决。在现有规定方面，企业应当以《行动纲要》、《政务资源暂行办法》、《试点工作方案》为指导，关注《广东省政务数据资源共享管理办法（试行）》与《深圳市政务信息资源共享管理暂行办法》、《条例（征求意见稿）》细化规定的开放规则体系，了解政府数据共享与开放模式，一方面积极参与开发利用政府数据完善服务生态，另一方面确保遵守监管要求，合法合规使用政府的数据，具体而言：

- **积极探索对政府数据的利用与开发模式。**考虑到政府有限的基础设施资源与信息技术水平难以满足公众对开放数据的需求，形成以政府主导监管，将数据治理和平台的运维托管给企业第三方的合作方式，将是主要解决思路之一。当下，政府数据合作开放盈利模式与监管模式仍需要进一步明确，企业应把握机会，积极参与到与政府合作模式的探索之中，实现电子政务与企业数字化转型的双赢。
- **与政府共同探索政府数据的资本合作模式。**《条例（征求意见稿）》为政务数据的国有产权性质进行了确认，政务数据开放属于生产要素的投入，同时政府数据开放需要大量的运维与治理成本，那么按照要素投入分配收入，政府数据开放应当收取合理对价。企业作为政府数据开放的支持主体，应当与政府共同探索具体的资本合作模式，并且明晰双方的责任边界。
- **企业使用政府数据应当遵守一定的义务并承担相应责任。**企业作为政府数据开放的利用者与数据成果的最终输出者，在使用政府数据时应签订数据开放使用协议，明确数据开放者与处理者的双方权责，同时，企业需特别注重全面履行数据处理者的法定与约定义务。

结语

深圳经济特区成立40年，积累了独一无二的改革开放经验，成就了世界瞩目的改革开放成果。《方案》为深圳下一步加快培育数据要素市场的探索提供了有力的政策支持，也提出了明确的成果要求。企业应当以现有的数据合规、网络安全、个人隐私保护等法律体系做好风险合规治理，积极参与到数据要素市场改革建设当中，抓住数据改革机遇，彰显社会责任担当。

根据金杜多年在网络安全与数据合规业务的深耕，总结出以下几点企业频发有待解决的合规问题：

- **加强企业数据合规与网络安全体系的顶层设计。**合理决策，确定数据资产管理体系的构建方向，以满足业务开展中必要的数据流动需求；
- **关注企业数据资产管理制度构建与安全评估。**树立动态数据分级分类制度与资产安全观，增强企业数据资产管理制度对改革方案落实的弹性应对；
- **重视企业内部数据资产盘点。**加强对个人信息与非个人信息的区分，自觉地对行业数据、特殊敏感数据类型分类；
- 加强数据的隔离与共享机制。探索数据中心多样化部署方案设计，满足大湾区不同司法辖区的法律监管；
- **区分梳理数据业务场景。**以数据全生命周期的特点设计安全合规尽职调查，审慎履行企业注意义务；
- **探索数据处理/交易协议的执行与审计。**明确数据处理/交易协议的权利义务范围，重视审计条款设计与执行，做到自证合规，规避风险。
- **将国际业务布局纳入工作考量。**重视跨境数据业务，关注GDPR等较为成熟的国际数据立法，为“双循环”的外循环做好准备。

（本文发布于2020年10月16日。）

[3] 政府数据共享指政务部门各部门之间的共享；数据开放指政务部门面向政务部门之外的其他主体提供数据；而数据利用则是指数据开放过程中获得数据的主体对数据的利用。

[4] 无条件共享类：可提供给所有政务部门共享使用的政府数据；有条件共享类：可提供给相关政务部门共享使用或仅能够部分提供给所有政务部门共享使用的政府数据；不予共享类：不宜提供给其他政务部门共享使用的政府数据。

[5] 有条件开放公共数据是指可以部分提供或者需要按照特定条件提供给自然人、法人和非法人组织的公共数据；不予开放公共数据是指涉及国家安全、商业秘密和个人隐私，根据法律、法规等规定不得开放的公共数据；无条件开放公共数据是指除有条件开放和不予开放以外的公共数据。

解读网信办《关于做好个人信息保护利用大数据支撑联防联控工作的通知》

一、背景

2020年初，举国上下全力战“疫”，国务院建立联防联控机制加强相关部门统筹协调，在阻击疫情的同时，全力组织企业复工复产，加强重点物资的统一调度。据报道，工信部已召开疫情防控大数据支撑服务工作调度会，提出加强联防联控，运用大数据分析，支撑服务疫情态势研判[1]。其他政府部门也与各科技企业联动，通过大数据加强疫情防控力度。

但值得特别警惕的是，在阻击疫情的过程中，已经在多地出现侵犯个人信息相关的案例和新闻，如1月浙江警方通报的泄露涉湖北籍人员身份资料的案件[2]、2月云南警方通报的泄露新型冠状肺炎患者信息[3]和湖南益阳发生的公职人员泄露确诊患者个人信息[4]等事件，广泛引发了普通公民尤其是确诊者、疑似者、密切接触者等重点人群对于自身隐私及个人信息泄露的担忧。

针对上述情况，2月3日，国家卫生健康委员会已公开发布《关于加强信息化支撑新型冠状病毒感染的肺炎疫情防控工作的通知》，其中对于加强网络信息安全、切实保护个人隐私安全等提出了概括性要求[5]。2月9日，中央网络安全和信息化委员会办公室（以下简称“**网信办**”）公开发布《关于做好个人信息保护利用大数据支撑联防联控工作的通知》（以下简称“**《通知》**”），及时地再次强调了此次疫情联防联控工作中的个人信息保护、大数据支撑等事项，重申了疫情紧急时需关注和遵循的个人信息保护底线。

二、《通知》解读

《通知》全文仅6个条款、不足800字，但内容丰富、涉及范围广泛。下文我们将逐条为《通知》各个条款“划重点”，提示有关企业在处理战“疫”数据时需要注意的个人信息保护问题。

第1条：“各地方各部门要高度重视个人信息保护工作，除国务院卫生健康部门依据《中华人民共和国网络安全法》《中华人民共和国传染病防治法》《突发公共卫生事件应急条例》授权的机构外，其他任何单位和个人不得以疫情防控、疾病防治为由，未经被收集者同意收集使用个人信息。法律、行政法规另有规定的，按其规定执行。”

重点：疫情管控目的下突破个人信息告知同意原则的例外情况应由法律及行政法规明确规定且依法取得有关部门授权

根据我国《网络安全法》及相关配套措施的规定，在收集使用个人信息前，应当取得个人信息主体的授权同意。在本次抗击疫情的特殊背景下，企业为抗击疫情目的收集使用甚至相互共享的个人信息能否以“与公共安全、公共卫生、重大公共利益直接相关”或“法律法规规定的其他情形”作为例外情况，从而无需征得个人信息主体同意成为了近期社会各界关注的焦点问题之一。

针对这一问题，《通知》第1条传递出两条明确的信息：**（1）虽然《网络安全法》并未就例外情况明确说明，但以法理而言，告知同意原则仍有例外情形；（2）适用个人信息告知同**

[1] 参见工业和信息化部官网发布的新闻动态《工业和信息化部调度部署疫情防控大数据支撑服务工作》，链接：http://www.miit.gov.cn/n1146290/n1146402/n7039597/c7646188/content.html，最后访问时间2020年2月10日。

[2] 参见湖北网警巡查执法公众号文章《公安部网安居局：疫情防控，网警在行动！》，链接：https://mp.weixin.qq.com/s/3UPpMM1ZT2A1J9NWFXKazQ，最后访问时间2020年2月9日。

[3] 参见人民网报道《云南警方暂缓拘留泄露确诊患者信息的医务人员》，链接：http://society.people.com.cn/n1/2020/0208/c1008-31576842.html，最后访问时间2020年2月9日。

[4] 参见中国经营网报道《海量涉疫情个人信息泄露 两地公安做出行政拘留处罚》，链接：http://news.sina.com.cn/o/2020-02-05/doc-iimxyqvz0398976.shtml，最后访问时间2020年2月9日。

[5] 参见国家卫生健康委员会官网，链接：http://www.nhc.gov.cn/guihuaxxs/gon11/202002/5ea1b9fca8b04225bbaad5978a91f49f.shtml，最后访问时间2020年2月9日。

意原则的例外情形必须取得法定授权，该法定授权的依据应当是法律以及行政法规另行规定，不包括部门规章及其他规范性法律文件。为此，利用大数据为抗击疫情提供支持的企业在收集、使用个人信息时仍应严格遵循《网络安全法》等法律法规确立的告知同意规则，取得个人信息主体的授权。如需适用授权同意原则的例外情形，除符合疫情防控的使用目的限制外，企业还应进一步取得国家卫生健康部门等有关部门依据《网络安全法》、《传染病防治法》等有关法律及行政法规的合法授权，否则“任何单位和个人不得以疫情防控、疾病防治为由，未经被收集者同意收集使用个人信息”。

第2条：“收集联防联控所必需的个人信息应参照国家标准《个人信息安全规范》，坚持最小范围原则，收集对象原则上限于确诊者、疑似者、密切接触者等重点人群，一般不针对特定地区的所有人群，防止形成对特定地域人群的事实上歧视。”

重点：疫情联防联控需求下收集、使用个人信息应坚持最小范围原则，不得形成“事实歧视”

《通知》第2条要求参照《信息安全技术 个人信息安全规范》（以下简称“《安全规范》”），坚持最小范围原则[6]，即仅处理为满足所获授权同意所需的最少个人信息。而根据《安全规范》第5.2条[7]的进一步阐释，收集个人信息的最小化要求还可进一步分解为：1）收集个人信息的类型应当与拟实现的目的（通常情况下为业务功能，疫情下则为疫情防治）具有直接关联，2）自动采集时采用最低频率和3）间接获取时仅采集最少数量的个人信息。这意味着，企业在为抗击疫情目的而收集个人信息时：

- **仍应当严格落实最小范围/最小化原则的相关要求，不得无限制、过度收集个人信息**：例如，为监测乘坐交通工具的乘客体温状况时，可相应采集乘客身份和体温信息，而不应在未发现乘客体温异常时采集乘客职业、籍贯、婚姻状况等内容；
- **应确保收集个人信息的频率最小、必要**：例如，社区经授权后全面筛查人口流动情况，可对返乡人员的身份、来源地区、交通工具等必要内容进行一次性登记，但通常不应采用强制佩戴智能定位设备、获取移动设备实时定位等方式过度采取返乡人员的位置信息等；
- **间接获取个人信息时合理控制最小数量**：例如，具有大数据分析技术的企业为有关部门提供密切接触人群相关的数据分析时，应确保从相关数据源处获得的个人信息类型、数量为最小、必要，避免获取非密切接触人群的相关个人信息。

此外，《通知》也特别提到了个人信息收集对象限制，即“原则上限于确诊者、疑似者、密切接触者等重点人群，一般不针对特定地区的所有人群”。一定程度上，这也是网信办对近期泄露病患信息、行踪轨迹等问题的直接回应。近来，部分地区泄露病患、外地返乡人员个人信息的案件和新闻引发了广泛的社会关注。例如，浙江某地一社区工作人员将内部工作资料中涉湖北籍人员的资料外泄，遭到公安机关和纪检部门处罚[8]；云南某地的几位医务人员和医院工作人员因散布医院电脑记录的患者信息遭到公安机关处罚[9]。在这类案例中，泄露的个人信息在一定程度上体现出部分人员对来自特定地区人员的差别态度，不可避免地为全国上下一致战“疫”的努力造成了不良影响，而这也正是《通知》所强调的、应防止的“事实歧视”问题。

---

[6]《信息安全技术 个人信息安全规范》（GB/T 35273—2017）第4条“个人信息安全基本原则”之d)“最少够用原则”规定，除与个人信息主体另有约定外，（个人信息控制者）只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时根据约定删除个人信息。

[7]《安全规范》第5.2条“收集个人信息的最小化要求”

对个人信息控制者的要求包括：

a）收集的个人信息的类型应与实现产品或服务的业务功能有直接关联。直接关联是指没有该信息的参与，产品或服务的功能无法实现；

b）自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率；

c）间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量。

[8]同前注1。

[9]同前注2。

第3条：“为疫情防控、疾病防治收集的个人信息，不得用于其他用途。任何单位和个人未经被收集者同意，不得公开姓名、年龄、身份证号码、电话号码、家庭住址等个人信息，因联防联控工作需要，且经过脱敏处理的除外。”

重点：重申个人信息使用的目的限制和公开规则

一方面，考虑到抗击疫情的特殊背景，相关企业在提供大数据支撑服务时，难以避免地涉及到诸多可能构成《安全规范》定义的个人敏感信息；同时，因社会上下的高度关注，对个人信息的超范围利用所可能引发对个人信息主体的损害程度也相应增加。因此，《通知》第3条额外强调了利用大数据为联防联控提供支持的企业，需要特别关注数据使用的目的限制。为此，相关企业在接受国家有关部门或医疗机构委托或授权，进而收集、处理个人信息时，应格外关注疫情防控目的下适当、合理的个人信息使用范围，避免超范围使用、超范围留存等可能不符合目的限制的行为。

另一方面，从个人信息的公开来看，在近期的疫情个人信息泄露案件中，已经出现个人信息主体的多种个人信息，如姓名、身份证号码、工作单位（就读学校）、家庭详细地址等在未经其许可的情况下被公开。[10]针对这样的实践情况，《通知》在第3条对个人信息的公开规则进行了重申，即原则上禁止因疫情防治需要而未经个人同意公开其个人信息。但值得注意的是，《通知》也兼顾了疫情下的信息公开需要，指出“经过脱敏处理的”个人信息，在疫情防控工作必要的前提下，将不再需要个人信息主体的授权同意。通常“脱敏处理”有不同的实际做法包括匿名化及去标识化处理。根据《网络安全法》第四十二条，“经过处理无法识别特定个人且不能复原的”信息通常被认定为进行匿名化处理，可不受个人信息主体同意的限制。而对于去标识化处理后的个人信息通常仍被认定为个人信息，因此根据《通知》要求，除法定授权可公开的个人信息以外，基于联防联控工作需要，采用何种办法进行“脱敏”处理需要引起企业的关注。

第4条：“收集或掌握个人信息的机构要对个人信息的安全保护负责，采取严格的管理和技术防护措施，防止被窃取、被泄露。”

重点：严格落实网络和数据安全保障措施

《网络安全法》对网络运行安全和网络信息安全作出了分别规定，特别是根据第四十二条，“网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失”。对于利用大数据为联防联控提供支持的企业而言，作为个人信息等数据处理的具体执行者，理当按照《网络安全法》等相关法律法规要求，落实技术和管理层面的安全保障措施。

为此，《通知》第4条要求采取严格的管理和技术防护措施，保障个人信息的安全，一定程度上是对现有法律要求的重申。此外，疫情涉及的个人信息类型和敏感性各异，不排除涉及个人敏感信息的情形，并可能较一般时期引发更为广泛和深远的社会影响。为此，我们建议，相关企业应更为积极、主动地参照更高、更严的技术标准和管理要求采取相关保障性措施，保护个人信息等数据安全。

第5条：“鼓励有能力的企业在有关部门的指导下，积极利用大数据，分析预测确诊者、疑似者、密切接触者等重点人群的流动情况，为联防联控工作提供大数据支持。”

重点：鼓励社会各界共同参与战“疫”

如本文开篇所述，抗击疫情目前已是举国上下高度关注，社会各界群策群力的一项工作。因此，为发挥散落各行各业的数据资源价值、共同积极应对疫情，《通知》第5条也明确鼓励有能力的企业利用自身在大数据方面的技术积累，为抗击疫情提供必要的支持。

同时，《通知》也清晰地指出，相关企业提供在利用大数据提供技术支撑时，应遵照有关部门的指导。而这也对从事大数据支持的相关企业提出了一定的挑战，尤其是一旦企业经授权承担面对公众的信息公开或发布等相关职能时，将可能需要把相对概括的指导内容转化为公众易理解、可接受的信息内容。此时，除前文所述相关要求外，企业还需额外关注具体数据、信息发布的具体名义、发布信息的形式、数据详细程度以及准确性等多方面问题。

---

[10] 同前注2。

[11] 参见China Law Insight，链接：https://www.chinalawinsight.com/2020/02/articles/compliance/%e7%96%ab%e6%83%85%e9%98%b2%e6%8e%a7-%e5%90%8c%e8%88%9f%e5%85%b1%e6%b5%8e-%e7%96%ab%e6%83%85%e4%b8%8b%e5%81%a5%e5%ba%b7%e5%8c%bb%e7%96%97%e6%95%b0%e6%8d%ae%e5%85%b1%e4%ba%ab/，最后访问时间2020年2月10日。

第6条：“任何组织和个人发现违规违法收集、使用、公开个人信息的行为，可以及时向网信、公安部门举报。网信部门要依据《中华人民共和国网络安全法》和相关规定，及时处置违规违法收集、使用、公开个人信息的行为，以及造成个人信息大量泄露的事件；涉及犯罪的公安机关要依法严厉打击。”

重点：强调社会共同监督、有关部门依法及时处置

在信息技术格外发达的今天，各类信息都在以曾经难以想象的速度通过信息网络传递，而个人信息保护作为应对疫情工作下不容忽视的重要一环，自疫情开始以来就引发了国家有关部门的关注。国家卫健委此前发布的《关于加强信息化支撑新型冠状病毒感染的肺炎疫情防控工作的通知》中就已经强调疫情防护要切实保障个人隐私安全。公安部和各地公安机关也已多次通报惩治泄露个人信息违法行为的情况。

除公权力机构的主动执法以外，《通知》第6条提出，任何组织和个人均可向网信、公安部门举报违法收集、使用、公开个人信息的行为，强调社会各界的共同监督作用，同时明确网信部门和公安部门各自的依法处置职责，凸显出疫情下同步保障公民个人信息权益的导向与趋势。而这也为企业敲响了个人信息保护的警钟，即便在疫情防治为先的背景下，也应当切实采取措施，合法合规收集、使用个人信息。

三、结论与建议

亚里士多德曾提出“公平就是比例相称”，并最终演变为比例原则这一具有普遍意义的法治规律。《通知》的价值和意义不仅在于强调利用大数据支撑联防联控工作的安排，更在于对个人信息保护规则底线的重申，希望在公共利益与个人合法权益即使在应急事件下的仍需要追求平衡，体现出难能可贵的“以人为本”思路。

此前，我们曾针对疫情防控中不同主体对于健康医疗数据[11]以及政务数据[12]合规问题进行探讨。《通知》针对个人信息保护，为拟参与到此次疫情联防联控中的企业等社会主体提供明确的指引。按照《通知》的指引和要求，我们建议所有拟基于自身数据能力参与到此次疫情联防联控的相关企业至少注意下列合规要点：

- **关注所提供的大数据支撑能力的合法性，加强与相关部门的合作**：如前所述，目前个人信息的收集和使用仍缺乏面向企业主体的明确法定例外，相关企业将自身数据能力对外输出用于疫情防控相关支持的，仍应基于《传染病防治法》等法定例外规定下明确授权的有关部门要求进行。
- **落实网络安全义务，切实保障相关网络与数据安全**：由于企业作为个人信息等数据的实际掌控和处理者，在提供大数据支撑联防联控能力时，相关企业更应当重点关注相关网络与数据安全的保障，尤其应当注意避免对于日常业务经营下积累的数据造成影响。
- **合理进行内部环境隔离和权限管控**：疫情下的大数据支撑服务与企业的日常业务经营存在本质的区别。为此，在可行的前提下，企业应尽量采取逻辑层面乃至物理层面的环境隔离完成相关个人信息等数据的处理流程，并单独建立访问该等环境的权限管控机制，以避免相关个人信息的过度访问和泄露风险。
- **被有关部门授权进行数据共享和公开时，合理确定实现共享和公开的方式和范围**：一方面，相关企业在对外提供疫情下的大数据支撑服务时，在可行情况下应尽量采用统计结果、分析成果等数据形式而非原始数据，另一方面，在进行数据公开时，针对具有隐私属性或较强个人识别性的个人信息类型，应注意事先采用脱敏、去标识等技术处理，避免对个人信息主体造成过度的影响。此外，从共享和公开的范围上看，也应合理关注涉及的数据特点，充分考虑特定数据类别不宜共享和公开的法律性质，避免过度共享与公开。有关不同场景下健康医疗数据的流转问题，可详见金杜网络安全与数据合规团队的相关文章。
- **严格遵循疫情防控的目的限制，合理备份与记录**：一方面，如《通知》要求，相关企业应严格限制因疫情防控而收集的个人信息使用范围，避免用于无关的商业化利用目的；另一方面，相关企业也应关注基于疫情防控目的而收集和衍生的个人信息留存时限，一旦卫生健康部门提出要求或疫情宣告结束，应及时删除原始数据与相关分析成果，确有必要时考虑采用冷储存备份等方式保留必要记录。

（本文发布于2020年02月10日。）

[12] 参见China Law Insight，链接：https://www.chinalawinsight.com/2020/02/articles/compliance/24626/，最后访问时间2020年2月10日。

疫情防控下的数据资源流转与公开问题

目前，国家各级卫生健康部门及疾控部门是新型冠状病毒相关疫情防控工作的先锋队伍，指导、协调各地各级医疗机构展开患者确诊、隔离、救治、防护的工作。与此同时，此次突发公共卫生事件的应急处理也需要国家其他部门的积极参与和协调。例如农业、林业、动物疫病防控等多部门在野生动物管控方面的协调配合；交通运输部门及时开展人员追踪；社区街道工作机构对于社区人员流动的管理；市场监管、民政等部门针对疫情防控期间民众的基本生活物资保障的协调联动，等等。建立针对疫情的高效联防联控机制，是应对突发公共卫生事件的重要基础。

接下来，我们希望以疫情防控下的信息资源共享与公开为出发点，进一步分析如何保障疫情相关的政务信息资源在不同政府部门之间有序传递，如何在保障公众对于疫情传播与防控情况知情权利的基础上，实现疫情相关数据资源的合理公开使用。

一、正当时——突发事件应对下的数据流转与公开

（一）突发公共卫生事件下数据资源流转

我国在传染病防治、突发事件应对领域的法律、行政法规对于包括疫情控制在内的突发公共卫生事件信息的流转提供了上位法支持。

表一 突发公共卫生事件信息流转

法律法规	适用范围	数据资源互通机制
《突发事件应对法》	突然发生，造成或者可能造成严重社会危害，需要采取应急处置措施予以应对的自然灾害、事故灾难、公共卫生事件和社会安全事件。[1]	建立国家和地方层面的突发事件信息系统。[2] 县级以上地方各级人民政府与上级人民政府及其有关部门、下级人民政府及其有关部门、专业机构和监测网点的突发事件信息系统实现互联互通，加强跨部门、跨地区的信息交流与情报合作。[3] 县级以上人民政府认为可能发生重大或者特别重大突发事件的，应向上级人民政府报告，并向上级人民政府有关部门、当地驻军和可能受到危害的毗邻或者相关地区的人民政府通报。[4] 县级以上地方各级人民政府汇总分析突发事件隐患和预警信息，必要时可组织相关部门、专业技术人员、专家学者会商，对发生突发事件的可能性及其可能造成的影响进行评估。[5]

[1] 参见《中华人民共和国突发事件应对法》第三条。
[2] 参见《中华人民共和国突发事件应对法》第三十七条。
[3] 参见《中华人民共和国突发事件应对法》第三十七条。
[4] 参见《中华人民共和国突发事件应对法》第四十条。
[5] 参见《中华人民共和国突发事件应对法》第四十条。

法律法规	适用范围	数据资源互通机制
《染病防治法》	鼠疫、霍乱等甲类传染病，传染性非典型肺炎、艾滋病等乙类传染病，以及流行性感冒、风疹等丙类传染病。[6]	国务院卫生行政部门应当向国务院其他有关部门和各省级人民政府卫生行政部门通报全国传染病疫情以及监测、预警的相关信息。[7] 毗邻的以及相关的地方人民政府卫生行政部门应互相通报本行政区域的传染病疫情以及监测、预警的相关信息。[8] 县级以上地方人民政府卫生行政部门应当向本行政区域内的疾病预防控制机构和医疗机构通报相关信息。[9] 县级以上人民政府有关部门应向同级人民政府卫生行政部门通报。[10] 解放军卫生主管部门应向国务院卫生行政部门通报。[11] 动物防疫机构和疾病预防控制机构应互相通报动物间和人间发生的人畜共患传染病疫情以及相关信息。[12] 港口、机场、铁路疾病预防控制机构以及国境卫生检疫机关在发现传染病线索时应向国境口岸所在地的疾病预防控制机构或者所在地县级以上地方人民政府卫生行政部门报告并互相通报。[13]
国务院《突发公共卫生事件应急条例》	突然发生，造成或者可能造成社会公众健康严重损害的重大传染病疫情、群体性不明原因疾病、重大食物和职业中毒以及其他严重影响公众健康的事件。[14]	国务院卫生行政主管部门建立重大、紧急疫情信息报告系统。[15] 国务院卫生行政主管部门应向国务院有关部门和省级人民政府卫生行政主管部门以及军队有关部门通报。[16] 县级以上地方人民政府有关部门，应向同级人民政府卫生行政主管部门通报。[17] 突发事件发生地的省级人民政府卫生行政主管部门，向毗邻省级人民政府卫生行政主管部门通报。[18]
国务院《国家突发公共卫生事件应急预案》	适用于突然发生，造成或者可能造成社会公众身心健康严重损害的重大传染病、群体性不明原因疾病、重大食物和职业中毒以及因自然灾害、事故灾难或社会安全等事件引起的严重影响公众身心健康的公共卫生事件。[19]	建设医疗救治信息网络，实现卫生行政部门、医疗救治机构与疾病预防控制机构之间的信息共享。[20] 各有关部门和单位要通力合作、资源共享。[21] 国务院卫生行政部门向国务院各有关部门和各省级卫生行政部门以及军队有关部门通报情况。[22] 疾病预防控制机构之间通报对传染病病人、疑似病人、病原携带者及其密切接触者的追踪调查情况。[23]

可以看出，在包括传染病在内的突发公共卫生事件中，各级卫生行政管理部门、疾病预防控制机构以及各级人民政府、军队等，均构成公共卫生事件相关信息首要的通报主体与对象。通报的数据资源不仅包括各类传染病疫情、公共卫生事件的具体情况，也概括性地包含与疫情或事件相关的信息，理论上授权政府及有关责任部门全渠道掌握、互通各类疫情相关信息。这对于保障疫情防控相关责任部门完整掌握疫情的各类信息资源，帮助责任部门进行及时、必要的防控决策，将各类疫情排查、管控、保障措施落到实处等至关重要。

另一方面，如前文所述，疫情控制不仅仅限于针对患者的确诊、隔离、救治、防护以及相关医疗健康数据的流通，在疫情爆发期间，针对包括患者在内的人民群众基本生活保障与健康防护

[6] 参见《中华人民共和国传染病防治法》第三条。
[7] 参见《中华人民共和国传染病防治法》第三十五条。
[8] 参见《中华人民共和国传染病防治法》第三十五条。
[9] 参见《中华人民共和国传染病防治法》第三十四条。
[10] 参见《中华人民共和国传染病防治法》第三十五条。
[11] 参见《中华人民共和国传染病防治法》第三十五条。
[12] 参见《中华人民共和国传染病防治法》第三十六条。
[13] 参见《中华人民共和国传染病防治法》第三十二条。
[14] 参见《突发公共卫生事件应急条例》第二条。
[15] 参见《突发公共卫生事件应急条例》第十九条。
[16] 参见《突发公共卫生事件应急条例》第二十三条。
[17] 参见《突发公共卫生事件应急条例》第二十三条。
[18] 参见《突发公共卫生事件应急条例》第二十三条。
[19] 参见《国家突发公共卫生事件应急预案》1.4。
[20] 参见《国家突发公共卫生事件应急预案》6.1.1。
[21] 参见《国家突发公共卫生事件应急预案》1.5。
[22] 参见《国家突发公共卫生事件应急预案》4.2.2。
[23] 参见《国家突发公共卫生事件应急预案》4.2.4。

还将依托各疫情防控参与部门在各自职责范围内的积极落实与信息流转。（详见表二 疫情防控下常见数据流转场景）。针对特定疫情的防控工作，同样需要关注不同疫情防控参与部门之间的有序信息资源互通。对此，法律法规对于特定场景的信息流转也提供了一定依据，例如在《突发事件应对法》下，地方政府部门出于突发事件影响评估的目的，在必要情况下可组织相关部门、专业技术人员、专家学者会商；在《国家突发公共卫生事件应急预案》中，也对各有关部门之间的资源共享提出了概括要求。

针对此次新型冠状病毒肺炎，国家卫生健康委员会在一月中下旬牵头成立了“应对新型冠状病毒感染的肺炎疫情联防联控工作机制”（下称“联防联控工作机制”），成员单位含32个政府部门，下设疫情防控、医疗救治、科研攻关、宣传、外事、后勤保障、前方工作等工作组。[24]联防联控工作机制的成立，为参与疫情防控的成员单位之间明确职责，分工协作，形成防控疫情的有效合力起到了至关重要的作用，也为成员单位之间就疫情相关数据资源的流转互通搭建了平台。例如，联防联控工作机制于1月23日发布的“肺炎机制发〔2020〕2号”文件就强调各地交通运输、海关、边检等部门卫生管理和检疫工作的相关信息须向卫生健康部门通报。

表二 疫情防控下常见数据流转场景

疫情防控工作场景	参与部门	信息数据内容
患者救治与管理	卫生健康部门、疾控部门、医疗机构等	病患基本信息、临床检验信息、诊疗观察记录、其他病历记录等
人员排查	交通部门、海关边检部门、文化旅游部门、社区工作部门、公安部门等	人员基本信息、行踪轨迹信息、居住地信息、亲属关系信息等
民生基本生活保障	市场监管部门、民政部门、发展改革部门、交通部门、水电气公共企业等	物价信息、物资运输流通信息、产品资源供应信息等
物资捐赠与补给	民政部门、交通部门、海关边检部门、外汇部门等	捐赠物资类型、数量、来源、捐赠人及机构基本信息，捐赠数额信息，捐赠人银行、财务账号及交易信息，外汇业务信息等
疫情科研攻关	科技部门、卫生健康部门、疾控部门等	患者病历记录，包括发病过程、诊疗过程、诊疗方案、诊疗记录，药物实验信息等
医保工作	社会保障部门、财政部门等	确诊病患病历信息、诊疗记录等
…	…	…

（二）突发公共卫生事件下数据资源公开

对于传染病等疫情事件的防控，除依赖于医疗机构及政府部门的积极措施外，更离不开公众的配合参与。保障公众对于疫情发展及管控情况的知情权利，是建立普通民众对于疫情事态的正确认知、提升民众对于疫情防护措施的理解与重视程度的重要方法。在传染病和突发公共卫生事件应对领域，建立疫情信息公开机制同样是相关法律法规明示的必然要求。

[24]《国家卫生健康委会同相关部门联防联控　全力应对新型冠状病毒感染的肺炎疫情》http://www.nhc.gov.cn/xcs/fkdt/202001/d9570f3a52614113ae0093df51509684.shtml

表三 突发公共卫生事件信息资源公开基本要求

法律法规	疫情信息资源公开的责任机关	公开的信息资源范围
《突发事件应对法》	履行统一领导职责或者组织处置突发事件的人民政府。[25]	有关突发事件事态发展和应急处置工作的信息。[26]
	国务院卫生行政部门。[27]	全国传染病疫情信息。[28]
《传染病防治法》	省级人民政府卫生行政部门。[29] （传染病暴发、流行时，国务院卫生行政部门负责向社会公布传染病疫情信息，并可以授权省、自治区、直辖市人民政府卫生行政部门向社会公布本行政区域的传染病疫情信息。）	本行政区域的传染病疫情信息。[30]
国务院《突发公共卫生事件应急条例》	国务院卫生行政主管部门，必要时可授权省、自治区、直辖市人民政府卫生行政主管部门。[31]	突发事件的信息。[32]
国务院《国家突发公共卫生事件应急预案》	各级人民政府和卫生行政部门。[33]	突发公共卫生事件的信息或公告。[34]
《卫生部法定传染病疫情和突发公共卫生事件信息发布方案》	卫生部授权各省、自治区、直辖市卫生行政部门发布辖区内信息。[35]	- 法定传染病疫情：甲、乙类传染病发生的总体情况、重大疾病的分布情况，重大疫情的控制情况以及丙类传染病的基本情况等。 - 突发公共卫生事件个案信息：突发公共卫生事件性质、原因，发生地及范围，发病、伤亡及涉及的人员范围，处理措施和控制情况，发生地强制措施的解除等。 - 突发公共卫生事件总体信息：严重影响公众健康的突发公共卫生事件的总体情况、分布情况，包括发生各类各级突发公共卫生事件的起数、涉及的发病和伤亡人数、应急处置情况等。[36] - 传染病疫情、食品安全和职业安全的预警信息。[37]

[25] 参见《中华人民共和国突发事件应对法》第五十三条。
[26] 参见《中华人民共和国突发事件应对法》第五十三条。
[27] 参见《中华人民共和国传染病防治法》第三十八条。
[28] 参见《中华人民共和国传染病防治法》第三十八条。
[29] 参见《中华人民共和国传染病防治法》第三十八条。
[30] 参见《中华人民共和国传染病防治法》第三十八条。
[31] 参见《突发公共卫生事件应急条例》第二十五条。
[32] 参见《突发公共卫生事件应急条例》第二十五条。
[33] 参见《国家突发公共卫生事件应急预案》4.2。
[34] 参见《国家突发公共卫生事件应急预案》4.2。
[35] 参见《卫生部关于印发<卫生部法定传染病疫情和突发公共卫生事件信息发布方案>的通知》第一点。
[36] 参见《卫生部法定传染病疫情和突发公共卫生事件信息发布方案》第二点。
[37] 参见《卫生部法定传染病疫情和突发公共卫生事件信息发布方案》第三点。

就本次疫情防控工作而言，国家及地方各级卫生健康部门在疫情数据的更新和公布工作中承担了重要角色。例如，国家卫生健康委员会在其官网主页设置了疫情发展的通报专栏，定期更新新型冠状病毒肺炎疫情的最新情况，如确诊病例、疑似病例和死亡病例数据[38]等。在信息资源公开的范围上，相关法律、行政法规从制度建立的角度对信息公布和公开机制同样进行了概括性的规定。而《卫生部法定传染病疫情和突发公共卫生事件信息发布方案》则对公共卫生事件的公开内容做了细化。作为突发公共卫生事件信息发布制度的具体实践，本次疫情防控工作中铺天盖地而来的信息资料，则从更加微观的角度帮助我们具体了解突发公共事件所公开的信息资源类型。以下是我们根据公开渠道信息总结的，由各级各类官方机构公开的与本次疫情防控相关的信息数据示例：

表四 目前公开的疫情防控信息数据示例

信息数据类别	信息数据内容示例
疫情总体数据	- 全国各地确诊病例数、疑似病例数、死亡病例数、治愈病例数、密切接触者数量等统计数据 - 各类病例的全国各省市分布情况、日增长情况
脱敏后个体病患信息	- 个体病例基本信息、病史、发病过程、救治过程 - 病患出行轨迹，乘坐交通工具信息 - 病患停留、居住地信息 - 病患亲属关系信息
迁徙数据	- 春节及疫情爆发期间全国各地人口流动数据 - 春节及疫情爆发期间各省市每日迁入及迁出人口来源地及占比信息
医疗支援信息	- 部分地区医疗救援队伍及成员相关信息 - 部分医疗物资援助及捐赠相关数据，包括援助/捐赠物资类别、援助/捐赠数量等
诊疗研究信息	- 针对病毒开展的特效药及诊疗方案的研究情况
…	…

在上述信息内容中，不乏存在政府机构与具有数据分析能力的大数据平台公司合作发布相关信息的情形。例如，国家预警信息发布中心与百度联合推出了疫情大数据的实时查询服务。[39]通过二者联合建立的疫情实时大数据报告平台，普通公众即可快速了解疫情的事实分布情况，并可查询不同省市在疫情爆发期间的人口迁入和迁出情况。除此之外，公众还可在该平台上查询与病患是否同乘交通工具、全国各地确诊小区位置等。根据该平台的数据说明，平台数据主要来源于国家及各省市区卫建委、各省市区政府、港澳台官方渠道公开数据。

二、虑深远——突发事件应对下数据资源流转的合理边界

以上从我国在突发公共卫生事件应对中的政府机构之间信息资源流通制度，结合本次新型冠状病毒肺炎防控的相应实践做法，可以窥见主管机构在处理和应对突发事件背景下，为切实做好事件防控工作而在信息资源流转方面的基本路径。但另一方面，除原卫生部发布了针对法定传染病疫情和突发公共卫生事件信息发布方案外，目前对于疫情等类似公共卫生事件涉及的信息流转规则尚无统一规定，本次针对新型冠状病毒肺炎的各类防控文件也主要宏观强调了信息互通和公开发布的要求。在疫情爆发的当下，日益发展的数据分析技术为政府机关有效掌握各类疫情相关数据提供了极大的便利，如何设定这些数据的流转使用的边界，是当下和未来突发事件应对需要研究和落实的问题，也是治理能力现代化的必经之路。

（一）疫情防控下数据资源互通的具体规则

谈及突发公共卫生事件下的政府部门协作与数据资源互通共

[38] http://www.nhc.gov.cn/xcs/xxgzbd/gzbd_index.shtml.

享，则自然会联想到当下引发热烈讨论的政务大数据共享问题。在推行电子政务的政策背景下，全国各地政务数据整合共享工作正如火如荼开展，这为我们讨论突发事件背景下数据的互通提供了一个有力切入点：相较于一般情形下的数据共享，突发事件应对中的数据互通有何不同特点？是否能够合理沿用一般政务数据共享的规则与思路?

相比之下，我国现行法律法规及政策文件能够为一般情形下的数据共享提供更为完整和体系化的规范指引。早在2006年，国家信息化领导小组印发的《国家电子政务总体框架》就强调了以“政务信息资源开发利用为主线，建立信息共享和业务协同机制”；国务院于2015年印发的《促进大数据发展行动纲要》则明确指出数据的开放共享是国家数据战略的核心，并将“加快政府数据开放共享，推动资源整合，提升治理能力”列为三大任务之首；2016年颁布的《政务信息资源共享管理暂行办法》（下称“《暂行办法》”），则以行政法规的形式对政务部门间政务信息资源共享工作进行规范。在此背景下，各地政府纷纷积极响应，制定并发布政务数据共享的相关政策规范已成为各地的普遍做法。

《暂行办法》将政务信息资源定义为“政务部门在履行职责过程中制作或获取的，以一定形式记录、保存的文件、资料、图表和数据等各类信息资源”[40]，且规定了一系列的信息共享原则，包括“以共享为原则、以不共享为例外”、“需求导向，无偿使用”、“统一标准，统筹建设”、“建立机制，保障安全”[41]等，要求建设各级共享平台，按照“无条件共享”、“有条件共享”、“不予共享”的数据资源共享类型，制定各地各级政府部门数据资源目录[42]，形成以共享平台为依托的数据资源共享管理体系。

从政务信息资源定义出发，不难理解在突发公共卫生事件应对过程中，包括卫生健康部门在内的各政府部门为履行疫情防控工作而形成、获取的信息资料均可落入政务信息资源的范畴，参与疫情防控的政府部门为履行各自职责所需而获取、使用其他部门数据资源或向其他部门提供数据资源理论上也可以适用。不过，由于公共卫生事件的突发性质和紧迫程度，使得相较于常规的政务信息共享，疫情防控相关信息的互通需求更加迫切。并且，突发事件往往可能引起严重的社会危害，从降低事件的影响程度和最大限度内保障公共健康等社会公共利益角度来看，政府机构之间在数据资源的互通范围和机制上也有一定合理理由保持相对的灵活性。

当然，这一灵活性诉求确乎有赖于统一的规范文件给予指引。除了常规的政府数据资源共享制度可供参考外，针对突发事件的应急规范文件则更加对口和贴近疫情防控状态下各政府部门联动与信息资源共享工作。如前所述，我国已颁布了《国家突发公共卫生事件应急预案》，但针对各部门的信息资源互通尚缺乏专门的规定和具体细则。据此，可以考虑在相关的应急预案中，适当参考常规数据资源共享的流程条件，增加突发情形下的政府信息流转工作指引，不仅能够便利各政府部门依法有序开展数据资源共享，也进一步提高了疫情防控工作的透明度，提高政府公信力。例如，可要求各政府部门针对突发事件形成类似的数据资源目录。此前国家发展改革委和中央网信办印发的《政务信息资源目录编制指南（试行）》作为常规政务信息资源目录编制的指引文件[43]，也可对各政府部门编制突发事件应对下数据资源目录提供参考指引。

此外，数据资源共享的标准化也可成为统一数据资源共享规则指引的有力措施。我国多项国家政策均强调要充分发挥标准化在数据开放共享工作中的作用[44]，全国信息技术标准化技术委员会大数据标准工作组也积极响应政策要求，组织研制了多项数据开放共享的国家标准草案，旨在建立数据开放共享衡量标准和评价方法。针对突发事件下的数据资源共享，也可考虑根据不同政

[39] https://voice.baidu.com/act/newpneumonia/newpneumonia?fraz=partner&paaz=gjyj

[40] 参见《暂行办法》第二条。

[41] 参见《暂行办法》第五条。

[42] 参见《暂行办法》第二章及第三章。

[43] 国家发展改革委 中央网信办关于印发《政务信息资源目录编制指南（试行）》的通知，http://www.gov.cn/xinwen/2017-07/13/content_5210203.htm

[44] 例如，国务院《促进大数据发展行动纲要》就提到要“提升政府数据开放共享标准化程度”。

府部门在突发事件应对中承担的不同职责和与因职责关联所需要获取的数据信息类型，针对数据的共享主体、共享程度设计相对统一的划分标准。

（二）数据资源流转的合理边界

除政府数据资源共享外，在大数据时代个人信息相关权益的合理保护一直以来也是广为关注和讨论的话题。以个人信息保护为例，《网络安全法》、《民法总则》等在法律层面原则上要求个人信息的收集、使用以“正当、合法、必要”为原则，以获得“个人信息主体同意”为先决条件[45]。

在此前的文章中，我们对于政府部门从各渠道获取、共享医疗健康以及其他与疫情防控密切相关的信息过程中所可能涉及的个人信息及健康医疗数据保护问题进行了场景化的剖析。但仍需要解决的问题在于，即便能够在信息获取的渠道和类型上建立一定的合法和必要性基础，如何保障信息收集的合法依据支持后续数据流转和公开？

1. 数据资源的互通

如前所述，疫情防控背景下不同政府部门收集的各方信息不乏指向特定患者或其他特定个人的多类型数据，包括个人的基本资料、行踪轨迹以及相关的诊疗救治信息。这些信息数据均有可能构成疫情相关信息，作为《传染病防治法》中各级卫生行政部门、疾控部门及人民政府以及相关部门互相通报的数据客体，理论上是政府部门履行法定义务所必须互通的内容。如果上述数据中包括个人信息，在无法或者无法及时获取个人信息主体同意的场景下，《传染病防治法》以法律层级的规定，在法理上不排除能够作为个人信息主体同意原则的例外情况。但需要进一步确认的问题在于：

（1） 对于其他部门而言，例如对于在疫情防控工作性质上与病患排查、诊疗救助存在一定距离的其他联动部门（例如服务于海外物资捐赠工作的外汇及海关部门）如需获取具体病患的个人信息，是否也需要建立一定的必要性基础。

（2） 突发事件中的数据流转，比如《突发事件应对法》要求各级人民政府及相关部门之间的突发事件信息系统实现互联互通是否能够为疫情防控背景下各相关部门实现疫情相关信息的完全互通提供法律依据，涉及个人信息流转时，无需获得个人信息主体同意。

国外在突发公共卫生事件数据资源共享方面的制度建设值得我们思考：

- **信息共享内容的明确列举**

欧盟于2013年通过的《欧洲议会和欧盟理事会关于严重的跨境健康威胁的决定》（下称“《决定》”）[46]，在欧盟成员国国家层面内建立了针对严重的健康威胁的早期预警和响应系统（EWRS，即Early Warning and Response System），为欧盟委员会和各成员国机构之间建立了信息互通渠道。《决定》同时明确欧盟委员会或相关成员国主管当局在满足特定的条件应当通过EWRS发出警报告知，并对警报告知的具体内容进行了明确列举，其中包含“接触追踪目的所必需的个人数据”[47]。而针对该等个人数据的共享，《决定》明确应符合“95指令”[48]等个人数据保护规则，同时对于该等个人数据可共享的机构范围以及留存时间等进行了限制。

- **个人数据保护规则的多项合法依据**

欧盟的个人数据保护制度本身设置多项除“知情同意”以外的个人数据处理的合法性基础，从而能够为公共健康事件应对中

[45]《网络安全法》第四十一条第一款规定，网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。《民法总则》第一百一十一条规定，自然人的个人信息受法律保护。任何组织和个人需要获取他人个人信息的，应当依法取得并确保信息安全，不得非法收集、使用、加工、传输他人个人信息，不得非法买卖、提供或者公开他人个人信息。

[46] Decision No.1082/2013/EU of The European Parliament and of The Council of 22 October 2013 on Serious Cross-Border Threats to Health and Repealing Decision，参见 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D1082&from=EN。

[47] 根据《决定》，接触追踪（contact tracing）是指为追踪暴露于严重的跨境健康威胁源且有感染疾病危险或已感染疾病的人而采取的措施。

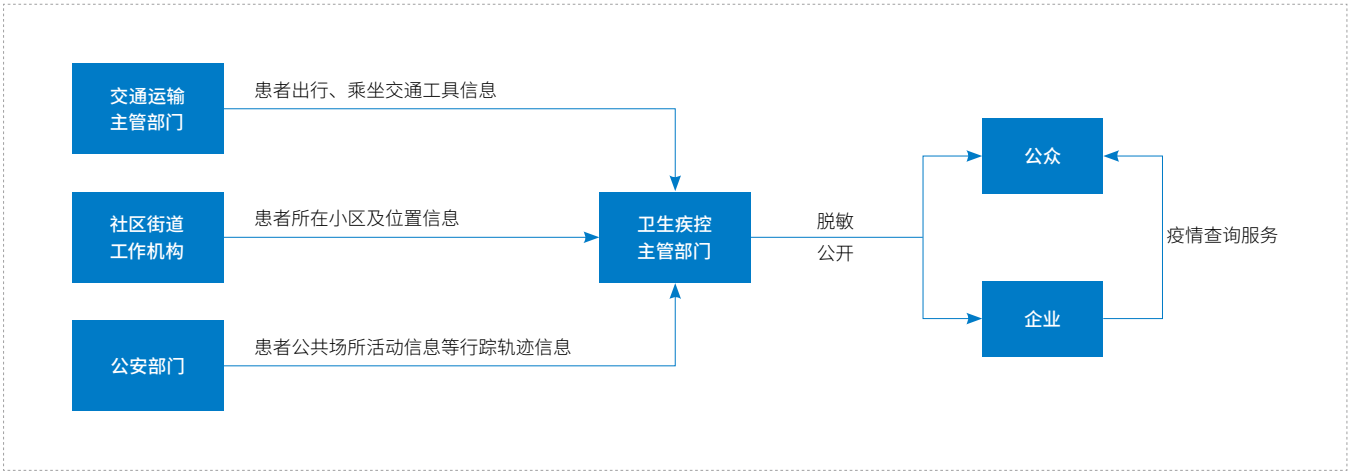
[48] 随着欧盟《通用数据保护条例》（GDPR）的生效，我们理解当前GDPR对于个人数据保护的相关规则将在《决定》中替代“95指令”的适用。

个人数据的处理活动提供适当的法律依据。例如，如为保护数据主体重大利益或其他自然人重大利益而必须处理个人数据，为了公共利益或基于公共职能执行任务而处理个人数据的，均能够建立个人数据处理的合法基础。而在针对公共健康事件信息共享机制中，《决定》对于个人数据共享的时空范围限定也进一步确保了欧盟个人数据保护下个人数据处理原则的具体落实，从而形成公共健康事件信息共享与个人数据保护的有效衔接。

2. 数据公开

相对于政务互通，疫情相关数据的公开由于面向广大不特定公众，同时可能涉及直接个人的高度敏感信息，因此对于个人信息主体相关权益的保护更应慎之又慎。

图一：疫情相关数据流动示例



比如，在确诊患者密切接触者排查工作中，由于人员流动的复杂性，想要精确找寻确诊患者在交通、差旅、公共场合密切接触过的所有人员往往存在较大的难度。此时将患者的出行轨迹及户外活动信息向社会公开，由密切接触人员自行申报则成为人员排查的有效措施，而这难免会涉及确诊患者的住址、行踪轨迹信息的公开。在这一场景下，确诊患者相关信息的披露范围则应当受到必要性的检验。此时，为实现人员排查目的的必要，确诊患者可能与外界人员产生接触的特定时间、特定位置（例如何时乘坐了哪一趟航班、何时在哪一商场购物等）则足以帮助公众识别其是否与确诊患者接触，对于与该确诊患者有关的其他信息（如姓名等），相关机关在信息资源公开的过程中则应慎重对待。此外，如前所述，为有效开展疫情防控的信息资源公开工作，政府机关在部分场合也会与具备相应数据分析能力的企业合作开展疫情信息的对外公布。而另一方面，这些公开的信息数据也将成为其他企业用于向公众提供疫情信息相关服务的重要数据资源。这同样对于政府部门信息公开过程中的个人信息保障提出了要求。考虑到相关公开数据将可能成为企业未来商业化使用的资源素材，无论是在政企合作背景下向企业输送相关数据资源，还是依据职权自行公开相关数据的场景，对于涉及个人隐私的相关数据资源公开共享予以合理限制，具有一定的必要性。

结语

随着疫情在全国范围内扩展，作为这场疫情阻击战的参与者，普通公众从公开渠道获得各种疫情信息，能切实感受到各地政府部门在防控措施上更加谨慎和周密。疫情数据严密监视着病毒的扩散路径，并为政府控制疫情的正确决策和高效行动提供有力的支撑。

疫情防控工作离不开多个政府部门的积极联动，疫情相关的数据信息在各部门之间的有序流转将进一步提升各部门的联动效能和执行力度，相关数据的有序公开也将有助于提升政府工作服务的透明度，建立广大民众对于疫情防控的普遍意识。对政府数据互通和公开的法理研究是帮助提高政府现代化治理能力的关键和前提。以此次疫情为契机，完善政府数据有序流转和公开，厘清突发事件与常规场景下数据流转的关系，将对提升政府现代化治理能力作出贡献。

（本文发布于2020年02月09日。）

同舟共济——不同场景下健康医疗数据流转的合规路径

引言

因突发、新型、危重等特点，新型冠状病毒肺炎已经被纳入法定乙类传染病管理，采取甲类传染病预防、控制措施，且迅速升级引发全国绝大部分省区市启动重大突发公共卫生事件一级响应。举国上下全力战“疫”，各级卫生疾控部门、医疗机构为疫情防治前赴后继，各民生部门、研究机构、各类企业、组织和个人都在竭尽所能的出谋划策。作为法律服务工作者，我们也需要贡献微薄之力，希望通过对数据共享合规机制的探讨，在抗击疫情的大背景下，更加细致地分析如何通过数据的合规共享与调配，为打赢疫情防治阻击战提供支持。

一、“无形”的帮手——数据资源调配

近日，科技部在通知中提出，“加强有关实验数据、临床病例、流行病学统计等数据、成果的开放共享，共同做好防控新型冠状病毒肺炎科技应对工作”，而国家卫生健康委员会（“卫健委”）也同样在通知中指出，“强化与工信、公安、交通运输等部门的信息联动，形成公路、铁路、民航、通讯、医疗等疫情相关方多源数据监测、交换、汇聚、反馈机制，利用大数据技术对疫情发展进行实时跟踪、重点筛查、有效预测，为科学防治、精准施策提供数据支撑”[1]。

如前述不同部委的通知中所强调的，最大可能有效识别病毒携带者、统筹公众预防也是目前传染病防治关键，都离不开健康医疗数据资源的合理共享与调配。作为被共享与调配的主角，健康医疗数据在现有法律体系下存在相对广泛的内涵。

（一）现有健康医疗数据体系

通常而言，从法律定义上看，健康医疗数据主要包含人口健康信息、病历信息、人类遗传资源和医疗健康大数据等多种数据类型（具体概念请见下表），涉及的主体多为各级各类医疗卫生计生服务机构、相关科研机构、高等学校、医疗行业企业等。

健康医疗数据	数据概念
人口健康信息	是指依据国家法律法规和工作职责，各级各类医疗卫生计生服务机构（含中医药服务机构）在服务和管理过程中产生的人口基本信息、医疗卫生服务信息等人口健康信息。[2]主管机构官方解读人口健康信息主要包括全员人口、电子健康档案、电子病历以及人口健康统计信息等。[3]
病历信息	是指医务人员在医疗活动过程中形成的文字、符号、图表、影像、切片等资料的总和，包括门（急）诊病历和住院病历。[4]
人类遗传资源	包括人类遗传资源材料和人类遗传资源信息。人类遗传资源材料是指含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料。人类遗传资源信息是指利用人类遗传资源材料产生的数据等信息资料。[5]
健康医疗大数据	是指人们疾病防治、健康管理等过程中产生的与健康医疗相关的数据。[6]

[1] 参见《国家卫生健康委办公厅关于加强信息化支撑新型冠状病毒感染的肺炎疫情防控工作的通知》。

[2] 参见《人口健康信息管理办法（试行）》第三条。

[3] 参见：http://www.nhc.gov.cn/mohwsbwstjxxzx/s8553/201405/d22d7df3236f4b4fadb9e34bbb5e1901.shtml （访问日期：2020年2月5日）。

[4] 参见《医疗机构病历管理规定》第二条。

[5] 参见《中华人民共和国人类遗传资源管理条例》第二条。

[6] 参见《国家健康医疗大数据标准、安全和服务管理办法（试行）》（以下简称“《健康医疗大数据管理办法》”）。

（二）特殊时期健康医疗数据范围和控制主体的拓展

而在特殊情况（如传染病疫情防控时）下，如卫健委在其通知中所提及的，除医疗卫生行业主体和主管机构外，更多相关行业和领域的多种主体将实际加入到应对的队伍之中，例如在本次疫情下提供重要支撑的交通运输行业主管部门与企业、电信行业企业、地图与数据服务行业企业等。

这些主体一方面从个人用户处接收各类数据，另一方面也在提供服务中产生、衍生出更多种类的相关数据，不排除在一定程度上扩展了通常大家认定的健康医疗数据范围。例如，为确保追踪风险人群的迁移情况，这些人群的行踪轨迹、出行情况就成为了疫情下重要的健康医疗数据资源，风险人群的身份信息将有必要与提供数据支撑的大数据行业企业共享，最终合理筛选并形成决策支持的数据依据。类似的，为筛查和管理密切接触者、疑似病例，具有武汉旅居史的个人所乘坐公共交通工具的记录，虽然通常属于个人出行记录而非医疗相关数据，但在疫情下就可能因公共卫生的考量而发生本质变化，在构成受到法律保护的个人信息之外，也成为重要的健康医疗数据资源。

不过，前述主体将不再仅仅来源于医疗卫生相关行业，本身的业务、能力和资源亦各有不同，掌握的数据资源展现形态也千变万化，同时也不可避免地面临各行业的具体监管规则限制。为了“化零为整”，健康医疗数据资源的协调、调配虽不易被感知，但具有极为重要的地位。以疫情防控为例，通常可能发生的数据资源调配和共享需求如下：

数据共享目的	数据内容	主要数据需求主体
确诊与疑似病例筛查	个人基本信息 临床症状与检验结果（病历记录）	医疗机构
疫情隔离与人口迁移管控	个人基本信息 隔离方式 隔离医学观察记录	负责隔离的社区、住宿服务企业等主体
	位置与定位信息 行踪轨迹、出行记录 密切接触人群记录	电信运营商、网约车等企业机构
	职业信息（工作单位、职业等）	雇主企业
诊疗与研究	患者基本信息 病程和治疗反映（病历记录） 治疗方案 其他临床和诊疗中相关的数据	医疗机构、检验机构
治愈患者的后期追踪、并发症防治	病历 诊疗方案	医疗机构

也正是为此，在此次新型冠状病毒疫情下，国务院应对新型冠状病毒感染的肺炎疫情联防联控机制及各部委均不同程度地对相关健康医疗数据的共享提出了一定的要求：

文件名	发文时间	涉及主体	数据共享等具体要求
《文化和旅游部办公厅 国家文物局办公室关于做好新型冠状病毒感染的肺炎疫情防控工作的通知》	2020年1月22日	旅行社等市场主体	对旅游团队人员进行排查，及时将当地卫生健康部门确诊的或疑似团队游客病例报告当地文化旅游主管部门，由其上报文化和旅游部。
《关于严格防治通过交通工具传播新型冠状病毒感染的肺炎的通知》	2020年1月23日	交通运输、民航、铁路等部门（单位）、有关运营企业	在火车、汽车、飞机、船舶等交通工具上发现病例或疑似病例后： 1）立即通知前方最近设有留验站的城市的车站、港口客运站、目的地机场； 2）有关运营企业应向卫生健康部门提供与病例同舱或同一车厢的乘客和其他与病例有密切接触的人员信息。
《关于加强新型冠状病毒感染的肺炎疫情社区防控工作的通知》	2020年1月24日	街道（乡镇）和社区（村）、社区	充分利用大数据的手段，精准管理来自武汉的人员，确保追踪到位，实施医学观察。

文件名	发文时间	涉及主体	数据共享等具体要求
《交通运输部关于统筹做好疫情防控和交通运输保障工作的紧急通知》	2020年1月29日	交通运输部门	1）客运、出租车、网约车等相关交通运输企业应向卫生健康部门报送同一交通工具内与病例密切接触人员的信息； 2）除因疫情防控需要向卫生健康等部门提供外，不得向其他机构、组织或者个人泄露有关信息、不得擅自在互联网散播。
《交通运输部新型冠状病毒感染的肺炎疫情联防联控工作通知》	2020年1月30日	省级交通运输主管部门、应急运输车辆运营企业	1）建立应急运输车辆台账，具体到车辆号牌、车辆类型和驾驶员； 2）发挥卫星定位导航车载终端作用，随时掌握最新运力动态分布。

（三）健康医疗数据现有规制

然而，值得注意的是，由于健康医疗数据的内涵与外延存在一定的弹性，同时与个人之间往往具有不可分割的联系，现有法律体系下，健康医疗数据可能受到不同角度规则体系的交叉监管。而出于个人信息保护等方面的权益平衡考虑，这些监管要求往往在健康医疗数据对外共享的规制上采取了较为审慎和严格的态度。

以人口健康信息、病历信息、人类遗传资源和健康医疗大数据这四类最主要的健康医疗数据类别为例，通常与数据共享相关的限制就包括：

- **人口健康信息**：以授权利用为原则，以提高医学研究、科学决策和便民服务水平为目的，分类管理，逐步互联共享。
- **病历信息**：《医疗机构病历管理规定》（以下简称“《病历管理规定》”）中对于病历的保管、复制、查阅进行了严格的限制规定，除为患者提供诊疗服务的医务人员，以及经卫生计生行政部门、中医药管理部门或者医疗机构授权的负责病案管理、医疗管理的部门或者人员外，原则上，其他任何机构和个人不得擅自查阅患者病历。
- **人类遗传资源**：符合伦理原则，通过伦理审查，不得危害中国公众健康、国家安全和社会公共利益；尊重提供者隐私，取得事先知情同意，并保护其合法权益；特别的，境外主体仅在经批准后，通过与中方单位合作的方式开展涉及人类遗传资源的国际合作科学研究。
- **健康医疗大数据**：国家卫生健康委员会（以下简称“国家卫健委”）负责按照国家信息资源开放共享有关规定，建立健康医疗大数据开放共享的工作机制，统筹建设健康医疗大数据上报系统平台、信息资源目录体系和共享交换体系；体系内，不同等级用户按权限共享，并确保在授权范围内使用相关数据。除此之外，任何单位和个人不得擅自利用和发布未经授权或超出授权范围的健康医疗大数据，不得使用非法手段获取数据。

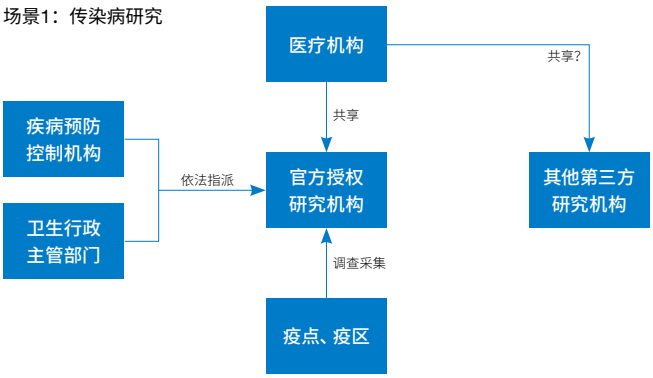
基于以上，不难看出，健康医疗数据具有集合性质，并非边界绝对清晰的单一法律概念，因而涉及到不同的法律规则体系；同时，健康医疗数据的外延可能随着社会生活现状的变化尤其是在应急状态下具有一定的弹性。在此前提下，同样可以清楚判断的是，健康医疗数据具有极高的价值，在日常生活和特殊时期均能发挥重要的作用，但这些价值与作用的发挥，尤为依赖对健康医疗数据进行合理的流转和调配。而现行法律体系下，为兼顾个人信息等基本权益，健康医疗数据的共享往往受到较为严格的限制，这也相应为掌握各类健康医疗数据的机构、企业和组织提出了很高的合规要求，以确保法律规则与价值发挥之间的平衡点。

二、场景分析：健康医疗数据的共享思路

为更加具体地分析健康医疗数据如何顺利在不同主体之间流转，结合目前疫情防治的大背景，在目前《传染病防治法》建立的传染病监测、预警和其他发现机制发现传染病之后，我们选取了具有典型意义的数据共享实践进行如下的场景化分析。

场景1：传染病研究

在发现传染病后，为及时指导传染病的医疗救治和防控工作，通常需要迅速地对传染病进行流行病学、病因病机、诊断治疗、预防控制的全面研究。但如此次疫情所呈现的，医疗机构由于处在医疗救治活动的一线阵地，研究力量有限，疾病预防控制部门和卫生行政主管部门授权的研究机构和其他第三方研究机构的研究力量将成为重要的补充。



图示 1 传染病研究场景下数据共享示意图

根据《传染病防治法》规定，官方授权研究机构（即指疾病预防控制机构和卫生行政部门指派的、与传染病有关的专业技术机构）“可以进入传染病疫点、疫区进行调查、采集样本、技术分析和检验”[7]。而与官方授权研究机构不同的是，其他第三方研究机构无法进入疫点、疫区，因此其研究的数据来源将只能依靠医疗机构的分享。然而，虽然部分类型健康医疗数据具有可行的共享路径，但《病历管理规定》原则上禁止除为患者提供诊疗服务的医务人员以外的其他机构和个人擅自查阅患者病历。为此，医疗机构虽可能在疫情下需要第三方研究力量提供支持，但在目前的法律规则下仍难以在未经患者充分授权的情况下，直接向第三方研究机构共享完整的病历记录等健康医疗数据。

如前所述，我国现行立法高度强调了对患者个人隐私的尊重和保护，但实践中也容易对疫情下医疗机构向第三方研究机构求援形成限制。从域外的立法经验来看，美国《1996年健康保险流通与责任法案》（下称“HIPPA”）体系下的数据分类规则方式可能有一定的借鉴意义。HIPPA及随后发布的隐私规则、安全规则区分了不同层次的健康医疗数据类型，含受保护的健康信息（Protected Health Information，PHI）、可识别个人的健康信息（Individually Identifiable Health Information）、受限制数据集（limited data sets）、脱敏信息（De-Identified Information）。其中，某些类型的健康医疗数据可能在无需患者个人授权时，即可使用或向其他主体提供，例如基于传染病通知与疾病防控的目的使用和共享PHI的数据，以及基于医学研究目的使用和共享受限制数据集。

对于健康医疗数据如何共享挖掘更大的价值是当前我国医疗行业监管立法的重点之一，一定程度上也吸收了其他司法辖区的先进经验。2019年4月公布的《信息安全技术 健康医疗数据安全指南》（征求意见稿，下称“《指南》”）已经采纳了受限制数据集[8]的概念，并提供部分数据共享和披露相关的例外规定，例如，基于科学研究、医学/健康教育、公共卫生或医疗保健操作目的，使用或对第三方披露受限制数据集时，无需患者授权[9]。

考虑到目前《指南》仍未生效，对于抗击疫情一线的医疗机构和急切希望贡献力量的第三方研究机构而言，涉及健康医疗数据的共享虽以疫情应对优先，但也应当切实做好必要、合理的合规应对措施。具体而言，医疗机构为疫情研究确有必要向第三方研究机构提供健康医疗数据（如病例数据、临床检验和诊断情况、生物样本数据等）的，除在可行的情况下以授权同意书等方式取得患者授权以外，我们也建议数据共享各方尽量采取多方面的保障措施，包括但不限于：

（1）确保订立必要的书面协议，明确数据共享各方的权利义务，要求数据接收方严格建立隔离环境，限制该等健康医疗数据的使用和留存范围，以避免发生泄漏和不当利用；

（2）可行时适当引入卫生行政主管部门和疾病预防控制机构作为授权主体，以确保合法性基础；

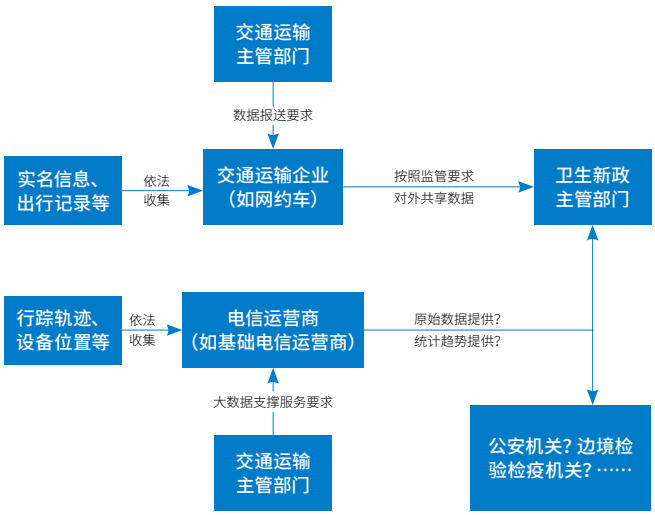
（3）合理参照HIPPA和《指南》中的受限制数据集等概念，切实进行疫情下病例数据的去标识化和匿名化，保护患者个人隐私等基本权利。

此外，仍值得一提的是，由于健康医疗数据的敏感性，前述分析并不针对境外研究机构。换言之，即便在疫情下，中国境内医疗机构向境外研究机构共享传染病例相关的健康医疗数据，仍可能受到人口健康信息、人类遗传资源等监管体系的严格规制，需要事先履行相应的审批、申报等法定程序；同时，该数据共享行为还将不可避免地构成健康医疗数据的跨境传输行为，而考虑到健康医疗数据（尤其是疫情下的健康医疗数据）还可能构成重要数据，医疗机构本身也可能落入关键信息基础设施的范围中，有关数据跨境传输的监管要求（包括但不限于安全评估与审批要求）也同样值得该等场景下的医疗机构及其合作伙伴关注。

场景2：传染病疫情隔离与追踪

在疫情控制措施中，隔离措施被认为是阻断传染病传播扩散的最有效手段之一，也同时是传染病防治中最困难、涉及主体类型和数据共享最复杂的任务。而为了切实完成隔离措施，如前所述，不同行业和企业对外共享该等健康医疗数据时的可行性和合规性问题，可能需要视情况具体分析。以下我们选取交通运输行业和电信行业作为代表进行对比。

场景2：传染病疫情控制



图示 2 传染病疫情控制场景下数据共享示意图

[7]《传染病防治法》 第四十八条

发生传染病疫情时，疾病预防控制机构和省级以上人民政府卫生行政部门指派的其他与传染病有关的专业技术机构，可以进入传染病疫点、疫区进行调查、采集样本、技术分析和检验。

[8]参见《指南》第3.8条，即“经过基本的去标识化处理，但仍可识别相应个人的、需要保护的个人健康医疗数据集”。

[9]参见《指南》第7条。

首先，交通运输企业基于在购票、用户管理等方面的实名制要求，天然地对于人口流动情况（含出行记录、位置定位等）具有精确统计和分析的便利。该等实名认证信息以及相应的人口流动情况在疫情下可能被扩展纳入健康医疗数据的范畴内，但目前《传染病防治法》《网络安全法》《突发事件应对法》等相关法律中仅对于实物物资和人员等的紧急调集做出了授权性规定，并未明确涉及数据资源的调配。

好在此次新型冠状病毒疫情下，交通运输主管部门所发布的《关于统筹做好疫情防控和交通运输保障工作的紧急通知》（下称“《交通部紧急通知》”）从行业主管部门层面向客运、出租车、网约车等交通运输企业提出了要求，即向卫生行政主管部门报送病例密切接触人员信息；同时，《交通部紧急通知》也一定程度上为交通运输企业为抗击疫情提供数据资源的支持提供了行政监管执法层面的依据和支持。为此，基于《交通部紧急通知》，相较于共享数据的合法性基础外，交通运输企业更需要关注涉及的数据类型（字段范围）、准确程度、共享方式（主动提供或依请求提供）、数据接收对象（直接向卫生行政主管部门提供或向其指定的机构提供）等。

而相对应的，基础电信运营商等电信企业基于其对移动基站接入信号、移动设备漫游情况等技术资源的掌握，也对于特定设备持有人的具体行踪轨迹、位置信息拥有及时的了解，理论上同样可以为疫情下的人口迁移分析提供准确、实时的数据基础。不过，如前所述，目前传染病和公共卫生事件相关法律法规中并未明确对于疫情下健康医疗数据的调用进行明确规定，同时《电信条例》和《电信和互联网用户个人信息保护规定》要求，“电信业务经营者及其工作人员不得擅自向他人提供电信用户使用电信网络所传输信息的内容”[10]，“电信业务经营者、互联网信息服务提供者及其工作人员对在提供服务过程中收集、使用的用户个人信息应当严格保密，不得泄露、篡改或者毁损，不得出售或者非法向他人提供”[11]。

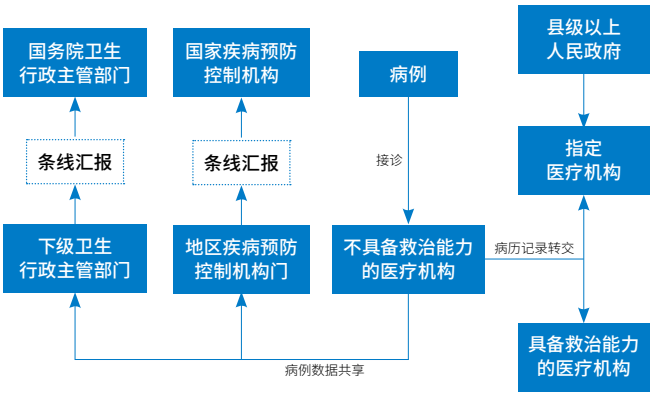
在此前提下，目前工信部门同样紧密安排，为疫情提供大数据支撑服务[12]，但也更为强调“疫情态势研判、疫情防控部署以及对流动人员的疫情监测、精准施策”，并未要求电信企业进行数据对外共享。因此，相较于交通运输企业，电信企业所掌握的行踪轨迹、位置信息等数据虽然也同样可能被扩展纳入疫情下的健康医疗数据概念范围中，但由于通信行业直接涉及通信自由等更为基本的公民权利，同时也缺乏明确的法律和行政执法要求作为基础，其对外共享相关数据将面临更为实质的合规限制。

为此，虽然疫情的爆发引发了健康医疗数据在各类主体之间的流转需求，但不同行业和企业对外共享相关数据时的可行性仍然需要根据自身所处的行业特性和法律监管要求进行相应判断。

场景3：医疗救治

对于确诊和疑似患者，入院诊断和治疗是当务之急。目前传染病的疾控防治多以条线垂直管理，如本次新型冠状病毒肺炎作为单一条线，在应急指挥部的要求下，从国家到省、地区、县市、乡镇的进行纵向统筹和汇报。但同时，传染病“条强块弱”的管理方式在面对新型冠状病毒肺炎这种突发的公共卫生事件时，不论是从诊疗方式的互通有无、床位或医疗物资的统一调配，还是在满足医疗资源紧缺下患者入院、转院的需求，区域内、跨区域医疗机构间的合作显得尤为迫切和重要。

场景3：医疗救治



图示 3 医疗救治场景下数据共享示意图

[10] 参见《电信条例》第六十六条，“电信用户依法使用电信的自由和通信秘密受法律保护。除因国家安全或者追查刑事犯罪的需要，由公安机关、国家安全机关或者人民检察院依照法律规定的程序对电信内容进行检查外，任何组织或者个人不得以任何理由对电信内容进行检查。

电信业务经营者及其工作人员不得擅自向他人提供电信用户使用电信网络所传输信息的内容。”

[11] 参见《电信和互联网用户个人信息保护规定》第十条。

[12] 参见新华网报道《工信部调度部署疫情防控大数据支撑服务工作》，网址：http://www.xinhuanet.com/politics/2020-01/26/c_1125503905.htm，最后访问时间2020年2月6日。

从诊疗角度出发，医疗机构间具有共享需求的信息多为患者的病历信息和传染病病程及治疗方案信息。传染病防治要求设立指定医院，并且“医疗机构不具备相应救治能力的，应当将患者及其病历记录复印件一并转至具备相应救治能力的医疗机构。”[13]然而在目前医疗资源紧张的情况下，并非所有患者均可入住指定医院，这样非就诊医院专家一并参与新型冠状病毒肺炎的救治成为切实需求。

非诊治医院的专家参与救治需要在医疗机构间共享患者的原始病历。然而《病历管理规定》对病历借阅、复制有着严格要求，并未明确非就诊医院的医务人员出于诊疗目的是否可以不受限地查阅患者病历，我们注意到即使出于科研目的，其他医疗机构对于病历查阅也需提出申请获得同意，且查阅的病历资料不得带离患者就诊医疗机构。当前，面对传染病隔离要求的大环境，多方、远程会诊和研讨治疗方案都是必要做法。应对病历共享的不确定性，鉴于卫生行政主管部门和疾病预防控制机构在疫情下汇集了大量患者病历信息，接诊的医疗机构可考虑（1）申请卫生行政主管部门和疾病预防控制机构统筹医疗机构间病历信息共享工作；同时（2）通过获得患者授权的方式，为诊疗目的在医疗机构间共享病历信息。此外，《传染病信息报告管理规范（2015年版）》要求区域信息平台或医疗机构的电子健康档案、电子病历系统应当具备传染病信息报告管理功能，并要逐步实现与传染病报告信息管理系统的数据自动交换功能，这也为医疗机构间与疾病预防控制机构间的信息共享提供了可能路径。

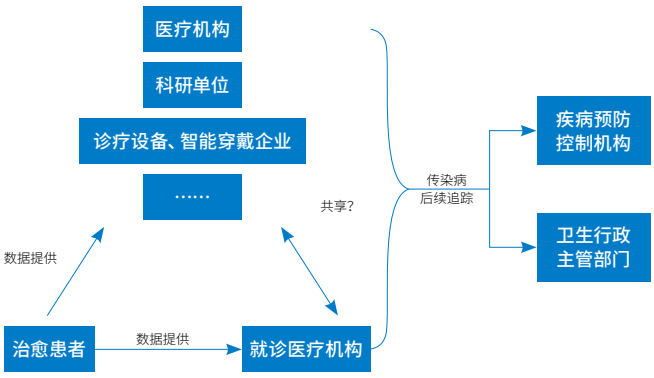
对于医疗机构间病历信息的共享，医疗机构也需做好数据传输、存储、使用的安全措施，注重其中的隐私保护和数据分级分类，应通过身份鉴别和授权控制加强用户管理，做到行为可管理、可控制、可追溯。医疗机构可参考《国家健康医疗大数据标准、安全和服务管理办法（试行）》中的要求，严格规范不同等级用户的数据接入和使用权限，并确保数据在授权范围内使用。对于在此过程中，涉及的数据存储、运维、信息技术产品和服务提供的第三方也应保证其在授权范围内提供服务。此外，鉴于病历信息中可能存在被认定为人类遗传资源的信息，在选择共享数据的医疗机构和服务提供商时，医疗机构还应注意可能发生的数据出境问题。

场景4：疫情后的应对

如上所述，疫情防控期间，由于当前突发公共卫生事件的性质，很多应对措施出于应急的目的具有特殊性，也可能打破常态化下健康医疗信息可被获得的主体范围，诸如交通、住宿、旅行社等企业主体都参与到疫情防治中，并获得大量的疫情或患者信息。

当疫情褪去，这些其他企业主体应妥善处理获得的疫情、患者相关信息。在没有患者或有权主管机构、医疗机构等明确授权的情况下，各组织、主体对这些数据的处理应以疫情防治目的为限，且注意保护患者隐私。此外，为控制疫情，大量个人信息也成集合式地被收集，例如同一家庭人员、与确诊患者乘同一高铁车厢的人员、同一办公室人员，相关主体之后应遵守个人信息的规则处理这些信息，如需进一步传染病追踪研究，需单独获得相关人员的同意。

场景4：疫情后的应对



图示 4 疫情后应对场景下数据共享示意图

此外，对于治愈患者的追踪治疗和医学帮助也切实需要各医疗机构间健康医疗信息的共享。从治愈患者需求出发，例如多家医院间的横向病历共享需要健康医疗大数据平台的进一步完善，可考量患者是否有权授权打通本人在多家医院间的诊疗记录；当援助武汉的医生回到原地方，患者的远程医疗，甚至智能医疗穿戴设备等方面的科研跟踪均有待仅一步完善。这里都离不开目前患者就诊医院对外的数据提供。

在没有突发公共卫生应急的前提后，前文所述的一些打破原健康医疗信息共享限制的例外将不再存在。此时，基于上述进一步处理健康医疗数据的需求，在中国现行法律法规基础上，健康医疗数据相关应用过程通常由政府或授权机构所主导，且现行有效的监管规定中未能明确医疗数据的商业化使用规则。

治愈患者和后续就诊医疗机构之外的第三方，需从人口健康信息、人类遗传资源、病历、健康医疗大数据等行业规制下，甄别其所处的场景和环节，分情况评估。第三方的数据共享可考虑不同的路径：（1）第三方以数据处理者的身份，以合作医疗机构的名义进行处理；（2）第三方以数据控制者身份，与合作医疗机构开展合作。两种方式下，第三方在数据处理、留存、目的把控、合规义务程度上均有不同。为此，第三方为合法取得健康医疗数据，通常需要进行合理的商业模式设计，例如引入患者授

[13]参见《传染病防治法》第五十二条。

权，构建三方关系进而主张相关数据来源于患者本人授权，进而降低合作中可能面临的合规风险。此外，健康医疗数据对外方的利用限制较为严格，尤其是在涉及中国人类遗传资源的合作上，要求外方不得在中国境内采集、保藏中国人类遗传资源，不得向境外提供中国人类遗传资源，利用中国人类遗传资源的国际合作也仅可以通过与中方合作的方式进行，且需经国务院科技部批准。

三、结论与建议

健康医疗数据一直在医学发展和传染病防控中扮演着重要的角色，随着信息技术的发展，健康医疗大数据成为行业新的驱动力。在本次疫情下暴露出的数据资源调配问题仅仅是冰山一角，健康医疗数据在各类主体之间的流转如何兼顾不同的数据类别和法律体系的交叉监管，合理管控常态下的法律规则底线和疫情防控等特殊情况中的必要例外，是需要长时间探讨但同时亟需解决的问题。

目前我国应对疫情的响应机制下，政府部门的中心化作用提供了极高的应对效率，但也一定程度上掩盖了目前健康医疗数据共享路径中的一些值得研究和澄清的问题，例如健康医疗数据的跨境传输性质认定、合规路径，例如疫情状态下的研究成果归属等。

在这样的法律背景下，企业主体，尤其是医疗机构、相关研究机构和掌握大量可能潜在构成健康医疗数据的其他企业主体，除常规经营下的数据合规措施以外，还应当更加重视公共卫生事件、网络安全事件等特殊状态下的应对措施，重点关注：

（1）提前规划，切实建立公共卫生事件、网络安全事件等特殊状态下的响应预案，确保机构内部及时响应与行动；

（2）区分常态化经营和特殊状态下的数据对外共享通道，重点关注特殊情况下向主管部门的必要数据共享机制；

（3）及时、全面梳理自身掌握且可用的健康医疗数据等数据资产，合理构建必要的数据资产分级分类体系，提前拟定不同类别数据和场景下的配套细则，为启动应急响应预案后提供实践指引。

（本文发布于2020年02月07日。）

六个月倒计时！
《生物安全法》中的数据合规赛道

2020年10月17日，《中华人民共和国生物安全法》（以下简称“《生物安全法》”）经全国人大常委会审议通过，将自2021年4月15日（我国第5个全民国家安全教育日）起正式实施。《生物安全法》的出台，标志着我国在法律层面将生物安全纳入国家安全体系，国家将统筹生物技术的健康发展和生物安全风险的防范，与时俱进，全方位保护我国生物安全。

本文将从数据合规（个人信息和重要数据的管理与保护）角度，讨论《生物安全法》对企业提出的具体要求。

一、《生物安全法》概览

（一）出台背景

《生物安全法》出台适应了国际国内生物技术发展和生物安全风险防范的需要。20世纪以来，生物技术发展日新月异，生物技术不断在医学、农业、工业、环境、能源等领域展现出巨大的潜力，正在引发新的科技革命，并有可能从根本上解决世界人口、粮食、环境、能源等影响人类生存与发展的重大问题，生物经济的蓝图被越来越深刻地描绘。

- **医疗领域：**以干细胞、基因测序和编辑、生物芯片等核心技术突破为基础，新兴生物技术在医学领域的广泛应用，不仅极大地改造了传统的医药产业，还使得医疗技术的核心从末端的疾病治疗，逐步走向前端的诊断和预防，并打开了未来个性化医疗的大门；
- **农业领域：**生物科技的“绿色革命”引领现代种植业和养殖业正在发生翻天覆地的变化；
- **能源领域：**越来越多的国家努力寻找更加经济高效绿色的能源替代方案，生物乙醇、生物柴油、生物发电、生物氢等生物质能在全球能源生产消费中的比重越来越大；
- **传统制造业领域：**工业生物技术的突破，使传统化工、造纸、食品等工业领域的制造工艺发生质的变化，不仅提高了生产效率，还降低了污染物排放。

有预测认为，除了上述已经被生物技术改变的四大领域，在2025年之后，当人类跨入生物经济成熟期，生物技术将对那些现在看起来似乎与生物学没有关联的更多产业发生作用，并最终对整个人类经济社会发展产生重大影响。[1]在此背景下，大部分发达国家均相继发布了国家级生物安全法律法规、发展战略和纲要。例如，美国先后颁布了《公共卫生安全与生物恐怖准备与应对法》《生物盾牌法案》《生物防御和大流行性疫苗与药物开发法案》《国家生物安全防御战略》等综合性管理生物安全法律或发展战略，针对具体生物产品还颁布了《联邦食品、药品和化妆品法案》《生物制品管制法》等法案；日本发布了《生物技术战略大纲》《生物战略 2019——面向国际共鸣的生物社区的形成》

[1] 引自国家发改委创新和高技术发展司发布的《将生物经济加速打造成继信息经济后的重要新经济形态》，链接https://www.ndrc.gov.cn/fzggw/jgsj/gjss/sjdt/201703/t20170316_1154666.html，2020年10月20日最后访问。

等生物安全战略，以及《重组DNA工作准则》《重组DNA实验准则》《实验室生物安全指南》等专项规范。

（二）立法目的

《生物安全法》开篇名义将生物安全纳入国家安全范畴，维护生物安全成为维护国家安全的重要组成部分，其直接立法目的则指向生物安全风险的防范和生物安全技术健康发展，前者为保障人民生命健康、保护生物资源和生态环境，后者为推动构建人类命运共同体、实现人与自然和谐共生。两项目的相辅相成，《生物安全法》将以法律形式保障生物技术稳定健康发展的同时，确保人民生命健康和生态系统相对处于不受威胁的状态。

基于《生物安全法》立法目的，对企业而言，无论在生物技术开发还是提供相关产品和服务过程中，均应以保护人民生命健康和生态环境为原则。

（三）适用范围和管理对象

《生物安全法》管理对象广泛，科研院校、医疗机构以及企事业单位和相关个人均应遵守《生物安全法》相关规定。对医疗机构和企事业单位而言，从事下列活动时，应特别注意生物安全合规：

- 防控重大新发突发传染病、动植物疫情；
- 生物技术研究、开发与应用；
- 病原微生物实验室生物安全管理；
- 人类遗传资源与生物资源安全管理；
- 防范外来物种入侵与保护生物多样性；
- 应对微生物耐药；
- 防范生物恐怖袭击与防御生物武器威胁；
- 其他与生物安全相关的活动。

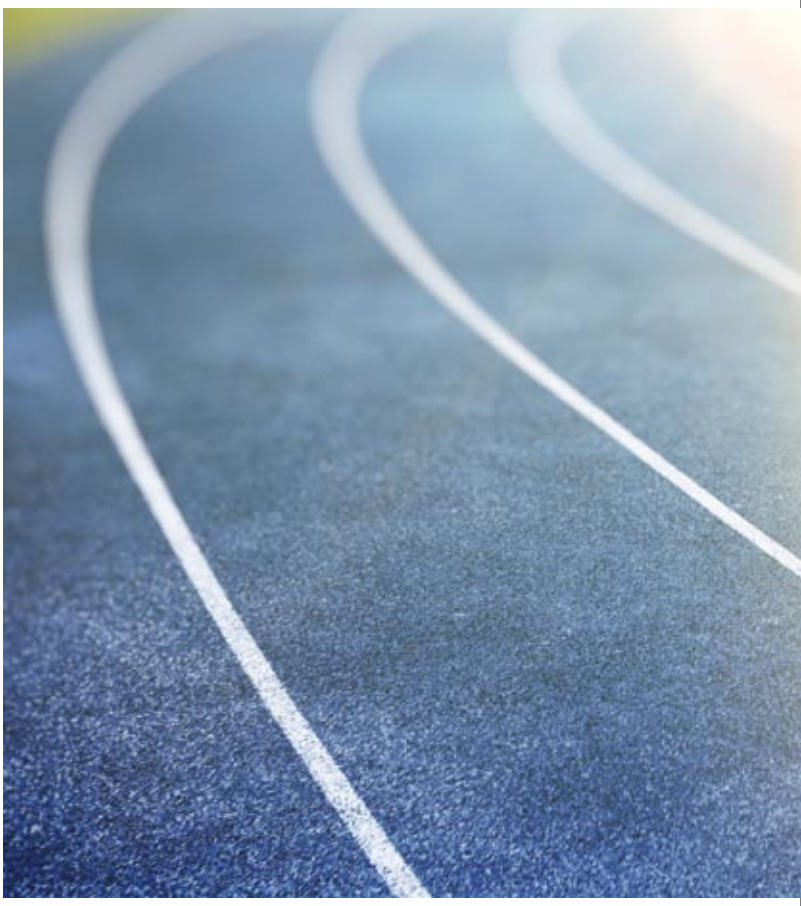
二、《生物安全法》对企业数据合规工作的“问答题”

（一）医疗、体检机构等面对突发传染病或动植物疫情应注意哪些方面？

《生物安全法》明确国家生物安全工作协调机制将组织建立国家生物安全风险监测预警体系，提高生物安全风险识别和分析能力，同时授权相关部门建立新发突发传染病、动植物疫情、进出境检疫、生物技术环境安全监测网络。在国家生物安全风险监测预警体系下，企业在个人信息和重要数据管理和保护方面需要注意以下方面：

1. 突发传染病或动植物疫情的报告义务

根据《生物安全法》第二十九条，任何单位和个人发现传染病、动植物疫病的，应当及时向医疗机构、有关专业机构或者部门报告；医疗机构、专业机构及其工作人员发现传染病、动植物疫病或者不明原因的聚集性疾病的，应当及时报告，并采取保护

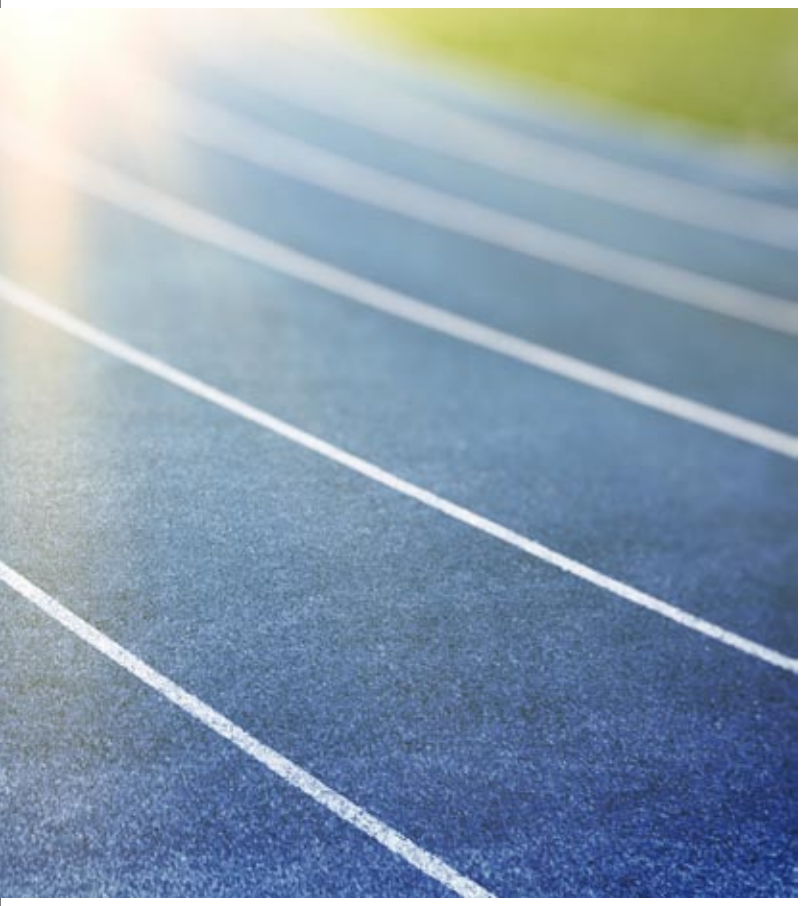


性措施。该要求与《中华人民共和国传染病防治法》（“《传染病防治法》”）、《突发公共卫生事件应急条例》《重大动物疫情经济条例》所规定的传染病预防预警机制、动物疫情监测机制一脉相承。

结合上述法律法规要求，企业发现员工感染或疑似感染传染病的，应当及时向医疗机构和传染病预防控制机构和/或卫生行政主管部门报告。医疗机构和相关专业机构（如能够检验传染病病毒的体检机构、第三方检验机构）在履行报告义务的同时，还应严格遵循《病原微生物实验室生物安全管理条例》等实验室生物安全相关要求，分类管理微生物与实验室，加强实验室感染控制，合理、合规处理实验活动废物，提前制定实验室环境污染应急预案等。

2. 生物安全信息发布限制与个人信息保护

《生物安全法》确立了生物安全信息发布制度，授权国家生物安全工作协调机制成员单位根据职责分工发布国家生物安全总体情况、重大生物安全风险警示信息、重大生物安全事件及其



调查处理信息等重大生物安全信息，由国务院有关部门和县级以上地方人民政府及其有关部门根据职责权限发布其他生物安全信息，并要求任何单位和个人不得编造、散布虚假的生物安全信息。由此，《生物安全法》明确了相关国家机构和各级政府及有关部门是生物安全信息发布的唯一渠道，医疗、体检机构和相关企业不得自行发布生物安全信息，更不能编造、散布虚假的生物安全信息。当前正处于新冠疫情防控特殊时期，新冠疫情病例的确诊信息也可能属于生物安全信息，医疗、体检机构等宜注意对该等信息的发布是否受到限制。

此外，根据2020年2月中央网信办公开发布的《关于做好个人信息保护利用大数据支撑联防联控工作的通知》，任何单位和个人还应注意以下方面：

- **目的限制：**为疫情防控、疾病防治收集的个人信息，不得用于其他用途；
- **授权同意原则：**除国务院卫生健康部门依据《中华人民共和国网络安全法》（“《网络安全法》”）《传染病防治法》《突发公共卫生事件应急条例》授权的机构外，其他任何单位和个人不得以疫情防控、疾病防治为由，未经被收集者同意收集使用个人信息，任何单位和个人未经被收集者同意，不得公开姓名、年龄、身份证号码等个人信息；
- **最小范围原则：**收集联防联控所必需的个人信息应参照国家标准《信息安全技术 个人信息安全规范》，坚持最小范围原则，收集对象原则上限于确诊者、疑似者、密切接触者等重点人群，一般不针对特定地区的所有人群，防止形成对特定地域人群的事实上的歧视；
- **安全保护义务：**收集或掌握个人信息的机构要对个人信息的安全保护负责，采取严格的管理和技术防护措施，防止被窃取、被泄露。

（二）医疗机构和企业在生物技术开发研究时需注意哪些方面？

《生物安全法》提出国家加强对生物技术研究、开放和应用活动的安全管理，禁止企业从事危及公众健康、损害生物资源、破坏生态系统和生物多样性等危害生物安全的生物技术研究、开发与应用活动。结合《生物安全法》及相关法律法规的要求，在生物技术开发研究时，企业应注意履行下述义务：

1. 遵循伦理原则

《生物安全法》第三十四条要求企业从事生物技术研究、开发和应用活动应当符合伦理原则，第四十条明确企业从事生物医学新技术临床研究，应当通过伦理审查，并在具备相应条件的医疗机构内进行；进行人体临床研究操作的，应当由符合相应条件的卫生专业技术人员执行。

目前，针对生物技术开发研究的伦理原则所指向的具体内容和审查方式尚待配套法律法规加以明确，但在生物医药方面，至少需要遵循《中华人民共和国药品管理法》（“《药品管理法》”）、《药品注册管理办法》《药物临床试验质量管理规范》（“GCP”）、《涉及人的生物医学研究伦理审查办法》（“《伦理审查办法》”）等法律法规对药品研发和临床试验伦理审查的相关规定，即具有医疗机构执业许可证，且以研究者和临床试验机构的身份参与药物研发与临床试验的企业，必须具有负责药物临床试验伦理审查的伦理委员会，并在药物临床试验开展前通过伦理审查。

此外，对于基因诊断技术而言，涉及处理人类遗传资源的环节也应当通过伦理审查。具体请参见下文从事人类遗传资源相关活动应适用的伦理审查相关规定。

2. 风险防控与应急预案

《生物安全法》确立了生物安全风险调查评估制度和生物安全应急制度、生物安全事件调查溯源制度，授权有关部门在必要时对企业生物技术研发所涉及的生物安全风险进行评估，并在发生生物安全事件后进行应急响应。对企业而言，为防控生物安全风险、更好地应对生物安全事件，应当注意以下合规要点：

- **风险防控管理：**从事生物技术研究、开发与应用活动的单位应当对本单位生物技术研究、开发与应用的安全负责，采取生物安全风险防控措施，制定生物安全培训、跟踪检查、定期报告等工作制度，强化过程管理；
- **事前审批备案和应急预案：**从事高风险、中风险生物技术研究、开发活动，应当由在我国境内依法成立的法人组织进行，并依法取得批准或者进行备案，还应当进行风险评估，制定风险防控计划和生物安全事件应急预案，降低研究、开发活动实施的风险；
- **追溯管理：**购买或者引进列入管控清单的重要设备和特殊生物因子，应当进行登记，确保可追溯，并报国务院有关部门备案。

提请企业注意的是，在制定风险防控方案和安全事件应急预案过程中，还需要结合《国家突发公共卫生事件应急预案》《突发公共卫生事件应急条例》和《网络安全法》《个人信息安全规范》等法律法规和国家标准的要求，特别关注个人信息和生物安全相关重要数据的管理和保护，包括但不限于：

- **安全措施：**采取有效技术和制度保障措施（如采取加密、备份等手段）保护生物技术开发研究过程中收集、产生的个人信息和重要数据，以防未经授权访问与信息泄露；
- **应急预案：**在生物安全事件应急预案中加入个人信息和重要数据保护及数据安全事件应对的相关内容，并明确数据安全事件发生后向有关部门和个人信息主体的报告和告知义务；
- **处理活动记录：**为方便生物安全事件发生后追根溯源以及更好地应对可能的行政调查，企业可以根据业务功能和授权情况区分个人信息和重要数据的处理目的、使用场景，以及委托处理、共享、转让、公开披露、是否涉及出境等情况，同时记录各类活动所涉及的个人信息和重要数据类型、数量、来源以及参与活动各环节的信息系统、组织或成员。

（三）医疗机构和企业在保护人类遗传资源时应做到哪些方面？

人类遗传资源包括人类遗传资源材料和人类遗传资源信息。其中，人类遗传资源材料是指含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料；人类遗传资源信息是指利用人类遗传资源材料产生的数据等信息资料。[2]人类遗传资源安全是维护国家生物安全的重要方面之一，其关系到公众健康、国家安全和社会公共利益，一直以来受到国家的高度重视。

早在1998年，我国即颁布了《人类遗传资源管理暂行办法》（“《暂行办法》”），《暂行办法》是我国最早出台的关于人类遗传资源的行政法规。其后，《人类遗传资源管理条例》（“《管理条例》”）颁布实施，在《暂行办法》的基础上对人类遗传资源作出了更加全面、明确且细化的规定，对人类遗传资源的采集、保藏、利用和对外提供进行了规制，并强调应当符合伦理原则，需按照国家相关规定进行伦理审查等。此次公布的《生物安全法》在第二条就明确了从事“人类遗传资源与生物资源安全管理”活动将适用该法，并在“人类遗传资源与生物资源安全”一章中以八个条款对涉及人类遗传资源和生物资源的相关活动作出了进一步明确规定，在一定程度上延续了《管理条例》中的相关规则。

尤为值得注意的是，本次《生物安全法》首次在法律层面明确强调了人类遗传资源的主权问题。根据《生物安全法》第五十三条第二款，“国家对我国人类遗传资源和生物资源享有主权”。这一规定意味着我国对于人类遗传资源具有国内的最高权力和国际上的独立自主权利，可排除任何外来干涉，人类遗传资源将和国家领土、领空一样，具有不可忽视的重要性，成为影响国家安全的重要资源。

《生物安全法》除了针对国家对人类遗传资源的管理和监督问题作出了明确规定外，其针对医疗机构和相关企业在人类遗传资源的采集、保藏、利用和对外提供方面更是提出了不同程度的合规要求。根据《生物安全法》，医疗机构和相关企业在从事人类遗传资源相关活动时，应当注意以下合规问题：

1. 在采集、保藏和利用人类遗传资源前应完成必要的事前审批

对于采集我国重要遗传家系、特定地区人类遗传资源或者采集国务院科学技术主管部门规定的种类、数量的人类遗传资源，保藏我国人类遗传资源，以及利用我国人类遗传资源开展国际科学研究合作，应当经过国务院科学技术主管部门批准。但对于临床诊疗、采供血服务、查处违法犯罪、兴奋剂检测和殡葬等为目的采集和保藏人类遗传资源及开展的相关活动，则不受前述事前审批的要求。

此外，对于利用我国人类遗传资源开展国际科学研究合作的，还应当保证中方单位及其研究人员全过程、实质性地参与研究，依法分享相关权益。结合《管理条例》，国际合作科学研究过程中的所有记录以及数据信息等应完全向中方单位开放，并向中方单位提供备份。

[2] 参见《生物安全法》第八十五条及《人类遗传资源管理条例》第二条。

2. 应当符合伦理原则

根据《生物安全法》第五十五条，采集、保藏、利用、对外提供我国人类遗传资源，应当符合伦理原则，不得危害公众健康、国家安全和社会公共利益。此外，根据《管理条例》，采集、保藏、利用、对外提供我国人类遗传资源，均应当按照国家有关规定进行伦理审查。

目前，针对人类遗传资源的伦理审查内容及方式等仍需相关配套措施加以明确，但在涉及人类遗传资源的生物医学研究方面，医疗机构和相关企业应至少符合《伦理审查办法》的相关规定。根据《伦理审查办法》，从事涉及人的生物医学研究的医疗卫生机构是涉及人的生物医学研究伦理审查工作的管理责任主体，应当设立伦理委员会。伦理委员会应当建立伦理审查工作制度或者操作规程，保证伦理审查过程独立、客观、公正，并应当符合知情同意原则、控制风险原则、免费和补偿原则、保护隐私原则、依法赔偿原则及特殊保护原则等伦理原则。在个人信息保护方面，为切实保护受试者的隐私，对于在生物医学研究过程中搜集到的受试者的个人信息，《伦理审查办法》明确要求（搜集主体）应如实将这些个人信息的储存、使用及保密措施情况告知受试者，未经授权不得将受试者个人信息向第三方透露。

同时，《伦理审查办法》还对伦理审查中需要提交的材料、重点审查的内容、批准研究项目的基本标准等作出了详细规定，为医疗机构和相关企业从事涉及人类遗传资源的生物医学研究活动提供了重要指引，也意味着对医疗机构和相关企业提出了更高的合规要求。

此外，当前大量生物人工智能技术发展迅速，因此通常涉及的伦理审查除了人口遗传资源等相关医疗伦理相关的验证以外，还需要考虑人工智能本身的“伦理尺度”。

以美国和欧盟为例，美国白宫在2019年6月发布了《国家人工智能研究发展战略计划》2019更新版（The National Artificial Intelligence Research And Development Strategic Plan: 2019 Update），其中明确将人工智能中的伦理道德问题作为研发战略之一。同一时期，欧盟于2019年4月发布了《可信赖人工智能伦理准则》（Ethics Guidelines for Trustworthy AI），将“人工智能技术须满足伦理道德原则及价值”作为人工智能发展的一项基本要素，并明确伦理原则应包括尊重人类自主性、防止侵害，以及公平性和明确性。

我国国务院在2017年发布的《新一代人工智能发展规划》中就认识到人工智能发展的伦理问题，提到了关于“初步建立人工智能法律法规、伦理规范和政策体系，形成人工智能安全评估和管理能力”的战略目标规划。[3]2019年，国家新一代人工智能治理专业委员会发布了《新一代人工智能治理原则——发展负责任的人工智能》，其中明确提出“和谐友好、公平公正、包容共享、尊重隐私、安全可控、共担责任、开放协作、敏捷治理”八项原则。[4]当下，随着人工智能的复杂化发展，医疗机构和相关企业在运用人工智能技术从事人类遗传资源相关活动时，更要注意生物医学伦理与人工智能伦理的平衡。

3. 对外提供我国人类遗传资源时应履行的义务

根据《生物安全法》，将我国人类遗传资源材料运送、邮寄、携带出境，应当经国务院科学技术主管部门批准。此外，向境外组织、个人及其设立或者实际控制的机构提供或者开放使用我国人类遗传资源信息，应当向国务院科学技术主管部门事先报告并提交信息备份。其中，为取得相关药品和医疗器械在我国上市许可，在临床试验机构利用我国人类遗传资源开展国际合作临床试验、不涉及人类遗传资源出境的，不需要获得前述批准，但在开展临床实验前也应向国务院科学技术主管部门进行必要的备案。

值得注意的是，与《管理条例》一致，《生物安全法》明确规定境外组织、个人及其设立或者实际控制的机构不得在我国境内采集、保藏我国人类遗传资源，不得向境外提供我国人类遗传资源。结合我国现有相关规定来看，境外组织、个人及其设立或实际控制的机构目前仅可通过与中方单位合作的方式开展国际合作科学研究，而研究过程中的所有记录以及数据信息等应完全向中方单位开放，并向中方单位提供备份。

此外，2019年底，科技部办公厅发布了《关于开展全国人类遗传资源行政许可管理专项检查有关工作的通知》（“《专项检查通知》”）[5]，科技部联合有关部门于2019年12月—2020年2月开展了人类遗传资源行政许可管理专项检查，表现出行政执法层

[3]参见《国务院关于印发新一代人工智能发展规划的通知》，
链接：http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm，2020年10月20日最后访问。

[4]参见《发展负责任的人工智能：新一代人工智能治理原则发布》，
链接：http://www.most.gov.cn/kjbgz/201906/t20190617_147107.htm，2020年10月20日最后访问。

[5]参见科技部政务服务平台网站，链接：https://fuwu.most.gov.cn/html/tztg/qt/20191230/123123237.html，2020年10月20日最后访问。

面对人类遗传资源的高度关注。在生物安全的重要性日益凸显的情况下，涉及人类遗传资源的相关医疗机构和企业将面对更严格的合规挑战。

（四）《生物安全法》对境外企业的数据获取和利用提出了哪些限制?

如上文所述，在人类遗传资源方面，《生物安全法》明确禁止境外组织、个人及其设立或者实际控制的机构在我国境内采集、保藏我国人类遗传资源，禁止向境外提供我国人类遗传资源。除此之外，《生物安全法》第五十八条还规定，境外组织、个人及其设立或者实际控制的机构获取和利用我国生物资源，应当依法取得批准。

生物资源涵盖范围广泛，包含实体的生物资源和非实体的生物资源，如生物样本数据、试验数据等。境外企业在获取和利用这些生物数据时，还可能受到同属于国家安全体系下的《网络安全法》及其配套措施的规制。根据网信办《数据安全管理办法（征求意见稿）》（“《管理办法》”），网络运营者向境外提供重要数据前，应当评估可能带来的安全风险，并报经行业主管监管部门同意；行业主管监管部门不明确的，应经省级网信部门批准。根据《管理办法》附则，重要数据是指一旦泄露可能直接影响国家安全、经济安全、社会稳定、公共健康和安全的数据，如未公开的政府信息，大面积人口、基因健康、地理、矿产资源等。其中，“大面积人口”、“基因健康”等领域中的特定类型数据均可能涉及生物数据。因此，对于境外企业在获取和利用生物资源时，除应受到政府科学技术、自然资源、生态环境等主管部门的监管外，对于生物数据还会受到网络安全领域（即个人信息与重要数据保护）的交叉监管。

此外，上述《专项检查通知》中明确要求检查单位法人主体对于人类遗传资源国际合作、出境等活动规章制度的建立和完善情况，以及获批项目中人类遗传资源出境情况、国际合作知识产权分享与安排情况等。

综合上述，对于境外企业来说，应识别其所获取和利用的生物资源种类及其在不同监管领域的法律身份，谨慎梳理各个部门的监管要求，积极应对各类审批、备案等前置程序。特别地，在生物数据方面，企业还可通过数据脱敏、处理统计级数据等方式以缓解多部门监管带来的合规压力。

小结和建议：

《生物安全法》规定了生物安全风险监测预警制度、生物安全风险调查评估制度等十一项具体的生物安全制度，全方位、多层次、多角度地建立了我国生物安全的风险防护体制，适应了国际、国内生物技术发展和生物安全风险防范的需要，为防范和应对生物安全风险、保障人民生命健康、保护生物资源和生态环境、促进生物技术健康发展等提供了立法层面的保障。

从法律的角度来看，《生物安全法》串联了《传染病防治法》《环境保护法》等相关法律以及《突发公共卫生事件应急条例》《人类遗传资源管理条例》等行政法规，使得我国生物安全在风险防控、技术开发与应用、防范生物恐怖与生物武器威胁等环节第一次形成了立体的保护体系。

从企业的角度来看，由于《生物安全法》的目的是平衡生物安全风险的防范和生物安全技术的健康发展，在对国家提出新要求的同时，也意味着相关企业应承担更多的责任和义务。因此，建议相关企业在《生物安全法》生效之前，全面检查现有生物安全体系是否能够应对《生物安全法》的具体要求，并针对识别出的风险及时采取应对措施。具体来说：

1. 对于医疗机构、体检机构等与传染病防治相关的企业

对于传染病防治相关企业来说，其一方面应当在突发传染病和动植物疫情的情况下，及时履行报告义务，并采取保护性措施；另一方面，企业应注意不得自行发布生物安全信息，不能编造、散布虚假生物安全信息，并注意履行个人信息保护的相关义务。

2. 对于药品企业、医疗器械企业等与生物技术开发研究相关的企业

对于药品、医疗器械等企业，在生物技术开发研究时，其一方面应当遵循伦理原则，通过伦理审查；另一方面，为防控生物安全风险、更好地应对生物安全事件，企业应当注意风险防控管理，并在制定风险防控方案和安全事件应急预案过程中特别关注个人信息和生物安全相关重要数据的管理和保护。

3. 对于医疗机构等与人类遗传资源相关的企业

对于涉及人类遗传资源相关活动的企业来说，其在人类遗传资源的采集、保藏、利用和对外提供时，应当完成必要的事前审批、备案等程序，并及时核查是否存在应报未报或超出审批范围开展相关活动的情况；此外，企业从事相关活动时还应当符合伦理原则，不得危害公众健康、国家安全和社会公共利益，并应重点关注对外提供我国人类遗传资源的情况。

4. 对于涉及我国生物资源的境外企业

对于涉及我国生物资源的境外企业来说，其需要更加全面地梳理生物安全风险，识别合规要求，履行必要的审批和备案制度，并严格避免法律所禁止的生物资源跨境传输情形，以更加谨慎的态度应对跨境合作中的生物安全风险；特别地，在生物数据方面，企业还应当注意网络安全领域（即个人信息与重要数据保护）的交叉监管。

（本文发布于2020年10月22日。）

“管中窥豹”——《生物安全法》前瞻及现行生物安全相关监管体系回顾

随着新型冠状肺炎疫情防控工作进入攻坚阶段，社会各界关于此次疫情的讨论与研究也越发深入。2020年2月14日，中央全面深化改革委员会第十二次会议上指出，“把生物安全纳入国家安全体系”，“尽快推动出台生物安全法，加快构建国家生物安全法律法规体系、制度保障体系”。生物安全法作为国家安全法律体系下的重要组成部分，在特殊时期进一步引发了社会各界的关注。

本文将旨在梳理我国生物安全立法的演进，回顾现行生物安全相关立法下的重点合规问题，以“管中窥豹”的形式，和大家一起前瞻《生物安全法》相关立法动向和发展方向。

一、《生物安全法》前瞻

生物安全一般是指由现代生物技术开发和应用对生态环境和人体健康造成的潜在威胁，及对其所采取的一系列有效预防和控制措施。[1]自1992年联合国环境与发展大会签署《21世纪议程》（Agenda 21）和《生物多样性公约》（Convention on Biological Diversity）后，生物安全开始引起国际社会的普遍重视。

（一）立法进展

随着生物技术和基因工程产品越来越多地进入到我们的日常生活，无论是从实验室生物安全、病原微生物，还是从基因工程和转基因、生物技术开发等来看，我国此前均已不同程度地构建了相关监管体系与要求。（可参见本文附录 现行生物安全相关法律框架梳理）

从时间进展来看，生物安全法的提出和制定不单是对此次疫情的点对点反映，更是针对“我国生物安全面临新形势、新问题和新任务”而制定的一部“具有基础性、系统性、综合性和统领性”的法律。[2]

实际上，早在2015年，我国科学家首次在实验室编辑人类胚胎基因时就引发了全球关注，[3]而后2018年我国诞生世界首例基因编辑婴儿的报道，[4]更是普遍引起国内外对于基因安全等生物安全话题的广泛探讨。为此，全国人大常委会2019年立法工作计划初次审议项目早已将生物安全法列入[5]，同年10月21日，生物安全法草案（以下简称“《草案》”）即首次提请十三届全国人大常委会审议[6]。

---

[1] 参见百度百科“生物安全”词条，链接：https://baike.baidu.com/item/%E7%94%9F%E7%89%A9%E5%AE%89%E5%85%A8/1278251?fr=aladdin，最后访问2020年2月25日。

[2] 参见《生物安全法草案首次提请最高立法机关审议》，全国人大网，载http://www.npc.gov.cn/npc/swaqflf003/201910/111c430fdb4447fa83fddeb2071eb5e8.shtml，2019年10月22日。

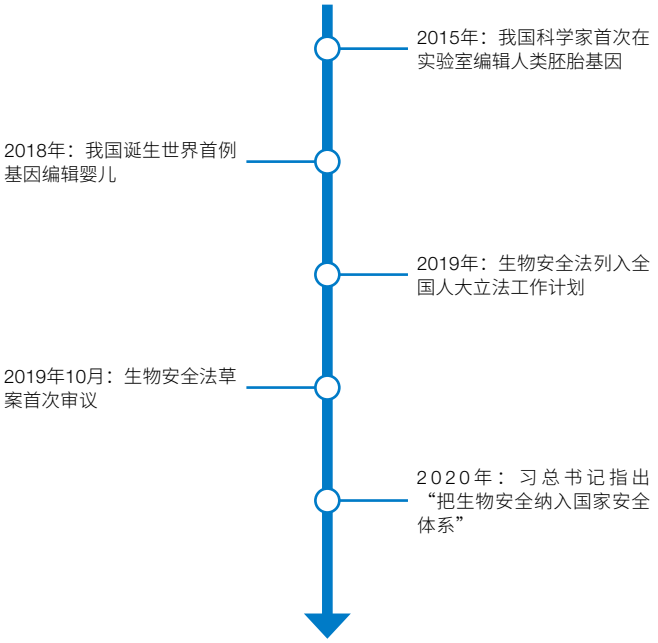
[3] 参见《中国科学家首次成功修改人类胚胎DNA》，丁香园，载http://paper.dxy.cn/article/105725?trace=related，2015年4月24日。

[4] 参见《世界首例免疫艾滋病的基因编辑婴儿诞生》，新京报网，载http://www.bjnews.com.cn/news/2018/11/26/524936.html，2018年11月26日；

参见《科技部：“基因编辑婴儿”被明令禁止》，新华网，载http://www.xinhuanet.com/tech/2018-11/28/c_1123776229.htm，2018年11月28日。

[5] 参见《全国人大环境与资源保护委员会公布2019年工作重点 6个立法项目将于今年完成阶段性目标》，中国人大网，载http://www.npc.gov.cn/npc/c199/201904/18e4b07e39c147f5bdcd17cd7ae96090.shtml，载2019年4月2日。

[6]前引1。



图示 1 我国生物安全立法进展部分重要时点示意图

截至目前，《草案》仍处于修改和审议过程中，据公开报道，《草案》的后续版本即将进入二次审议过程。[7]可以预见的是，待其通过并生效后，《生物安全法》将一定程度上统领我国未来生物安全的立法方向，并和《网络安全法》等国家安全法律体系一样，衍生、发展出更为广阔和丰富的内涵。

（二）主要内容

《草案》共计七章75条，聚焦生物安全领域主要问题，重点涉及生物资源安全保护、生物技术发展促进、防范生物及生物技术侵害国家安全等。

据报道，《草案》规范、调整的范围分为八大类：一是防控重大新发突发传染病、动植物疫情；二是研究、开发、应用生物技术；三是保障实验室生物安全；四是保障我国生物资源和人类遗传资源的安全；五是防范外来物种入侵与保护生物多样性；六是应对微生物耐药；七是防范生物恐怖袭击；八是防御生物武器威胁。

整体而言，《草案》适当借鉴和参考了《生物多样性公约》《卡塔赫纳生物安全议定书》（Cartagena Protocol on Biosafety）以及《中国国家生物安全框架》等国内外的先进立法、国际协议和研究经验等基础性内容，一方面针对当前国家生物安全挑战，着力构建国家生物安全体系，划定生物技术发展边界，对生物战、重大新发突发传染病（如非典、非洲猪瘟、新型冠状肺炎）及动植物疫情等传统生物威胁，以及新的生物威胁作出防范，明确社会各方面的生物安全责任，为公共管理部门、社会组织和公民个人的权利义务关系提供制度安排保障。

另一方面，《草案》也充分考虑我国在生物技术研发、基础设施建设上与先进国家之间的差距，将国家生物安全能力建设纳入法律，明确政策扶持和发展促进，这将为生物安全相关产品的迅速崛起带来重大机遇。

（三）监管蓝图

不难想象，由于生物安全不可避免地涉及到生物材料和资源的生产、管理，生物材料和资源可用于医疗健康、食品药品等多个行业，同时又与传染病防治、公共卫生安全紧密相关，涉及的监管部门较多。

在我国目前的监管实践中，生态环境部的监管职能中明确覆盖生物安全相关监管，其下设的自然生态保护司同时承担国家生物安全管理办公室工作，负责工作包括生物多样性保护、生物物种资源（含生物遗传资源）保护、生物安全管理，以及有关国际公约国内履约工作。[8]此外，与生物安全相关的监管部门至少包括自然资源与农业主管机构（自然资源部、农业农村部）、健康医疗主管机构（国家卫生健康委员会）、科学技术主管机构（科学技术部）、国家安全与应急管理主管机构（国家安全部、应急管理部）、进出境监督管理机构（海关总署）、药品监督管理机构（市场监督管理总局管理的国家药品监督管理局）等，涉及的部委机构数量占国务院组成部门总数量的三分之一。

在此背景下，为充分兼顾现有部门职能、统筹发挥合力，《草案》明确实行“协调机制下的分部门管理体制”，在充分发挥分部门管理的基础上，对于争议问题、需要协调的问题，将由协调机制统筹解决。

为此，值得期待的是，《草案》在现行监管基础上规划了“分部门管理+协调机制”的监管蓝图，一定程度上从法律层面确立了不同部委之间的合作方式。同时，仍有待进一步立法澄清的是该等协调机制如何能够有效、具体运行的问题，包括但不限于常设机构、定期沟通机制、信息共享机制和协同执法机制等保障性措施的配套和落实。此外，更为重要的一点，也是企业最为关注的，是该等协调机制下是否以及如何提供统一的对外窗口和沟通渠道，以避免因同一事项引发不同行业、领域监管要求导致的疏漏等。

[7] 参见《常纪文：加快构建国家生物安全法律法规体系》，国务院发展研究中心网站，载https://www.drc.gov.cn/DocView.aspx?chnid=4&leafid=4&docid=2900225，2020年2月17日。

[8] 参见生态环境部网站，链接：http://www.mee.gov.cn/zjhb/bjg/sts/，最后访问2020年2月23日。

（四）《草案》亮点

除前文所述内容以外，《草案》还进一步提出了诸多值得关注和肯定的亮点要求，包括但不限于：

1. **建立通用制度体系。**《草案》作为统领性法律，构建了如监测预警体系、标准体系、名录清单管理体系、信息共享体系、风险评估体系、应急体系、决策技术咨询体系、海关监管制度等具有通用性质的诸多制度体系，将为相关监管要求的具体实施和落实提供保障和指引。
2. **政策保障与罚则并举。**《草案》以专章形式对国家生物安全能力建设和发展进行了规定，涉及加大经费投入、基础设施建设、人才培养、政策扶持等多方面措施。同时，《草案》也对于违法违规责任进行了强调，不仅对生物技术谬用等行为明确了相应的责任及处罚，填补了法律空白，还进一步对国家公职人员不作为或者不依法作为行为的处罚规定。保障与罚则并举，生物安全相关制度的实施将更具有保障性和确定性。
3. **立足现实、适度前瞻。**除在法律责任部分对生物技术谬用等社会事件进行响应以外，《草案》还在不同部分体现出对社会现状和舆论关注的反映，包括但不限于对微生物耐药、防范外来物种入侵与保护生物多样性等的规范和关注。同时，《草案》相较于国外普遍的生物安全立法思路的一大特点是，在基因技术与转基因成果的关注以外，对生物恐怖袭击、生物武器威胁予以全新的关注，体现出立法者对生物安全重要性和未来战略价值的前瞻。但同时，值得企业关注的是，生物安全的地位提升，不可避免地伴随着行业整体将更为深入、彻底地落入到监管视野中，对企业的整体合规水平必将提出额外的挑战与要求。

二、现行生物安全相关重点合规问题

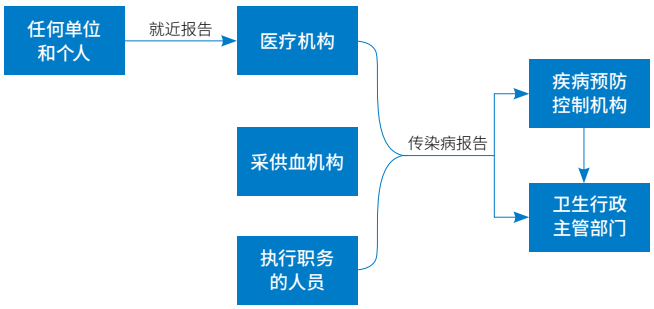
除《草案》外，我国现行法律体系中已经通过不同层级、不同效力的法律法规、规章和标准等，对生物安全相关的实践提供了指引，涉及领域包括但不限于传染病防控、人类遗传资源安全保护、生物技术研究开发与应用、实验室生物安全、基因工程和转基因、伦理管理等，详情可参见本文附录 现行生物安全相关法律框架梳理。

相关企业在我国现行法律框架下需关注的诸多合规问题无疑也将成为《草案》规范的重点，本文谨以传染病防控、人类遗传资源安全和生物重要数据为例进行分析。

（一）传染病防控

为妥善应对以此次新型冠状病毒肺炎疫情为例的传染病等生物安全事件，往往需要一个迅速而有效的识别和发现机制。在我国目前以《传染病防治法》《突发公共卫生事件应急条例》为核心的法律框架下，除卫生行政主管部门主动开展传染病预防和预警外，通常传染病疫情会在不同的地区，被不同机构或个人处首次发现。此时，需要向适当的主体报告和提供可能与该等传染病相关的统计数据和生物数据，将至少涉及医疗机构向疾病预防控制机构和健康卫生主管部门的生物数据共享。

场景：传染病发现



图示 2 传染病发现场景下数据共享示意图

该报告行为是《传染病防治法》中明确的法定义务要求。一方面，除疾病预防控制机构外，医疗机构和采供血机构及其执行职务的人员发现符合报告条件的传染病及疫情时，均应当根据属地化原则履行报告义务。任何单位和个人发现传染病病人或者疑似传染病病人时，应及时向附近的疾病预防控制机构或者医疗机构报告。

根据《传染病信息报告管理规范（2015年版）》，虽然报告内容与病历记录之间可能具有较高的重合度或者根据电子病历形成，而医疗机构原则上禁止对外提供患者病历记录，但考虑到发现传染病时的数据上报是根据《传染病防治法》的法定义务，目前的法律体系已经为医疗机构在该场景下对外共享健康医疗数据提供了明确的例外规定。此外，如此次疫情下各级医疗机构及相关部门、机构的通力合作，导致特定传染病的病原体及特征（如病毒结构、基因测序结果、毒株等），也同样具有极强的共享和流转需求。

为此，在该场景下，以主要的数据输出方——医疗机构为例，除疾病诊治的一线任务外，还可能同时涉及多个领域的法定义务要求，包括但不限于：

1. 严格遵循《病原微生物实验室生物安全管理条例》等实验室生物安全相关要求，分类管理微生物与实验室，加强实验室感染控制，合理、合规处理实验活动废物，提前制定实验室环境污染应急预案等；
2. 应严格按照《传染病防治法》及相关配套措施的具体要求履行报告义务，确保报告对象、报告渠道的准确、完备；
3. 严格落实《传染病信息报告管理规范（2015年版）》中对于信息系统安全和资料保存等方面提出的相关要求，保护

患者个人隐私，避免传染病数据泄露或被不当利用。

而从传染病防控的环节来看，传染病发现与报告仅是防控的开端，对公共卫生事件应对机制的考验才刚刚开始，而后续不同场景下同样将涉及多方面的健康医疗数据流转问题。

（二）人类遗传资源安全

作为生物资源的重要类别，人类遗传资源的安全和保护很早就得到了各国立法者的高度重视。

以美国为例，1996年由美国国会颁布的《健康保险携带和责任法案》（Health Insurance Portability and Accountability ACT, HIPAA）和2008年美国总统签署的《反基因歧视法》（Genetic Information Nondiscrimination Act）均对人类遗传资源的隐私安全进行规制，并提出了不伤害原则、知情同意原则、维护个人遗传机密性等人类遗传资源管理和保护的原则。

同时期，我国于1998年颁布《人类遗传资源管理暂行办法》（“《暂行办法》”），确立了人类遗传资源分级管理、统一审批制度，澄清了科学技术主管部门和卫生行政主管部门共同承担监管责任（后于2012年统一归口科技部管理[9]），并设立了中国人类遗传资源管理办公室负责日常工作。2019年5月，《暂行办法》的继任者——《人类遗传资源管理条例》（“《管理条例》”）颁布并于同年7月1日起施行，其沿袭了《暂行办法》的精神，对人类遗传资源合理利用的态度更加明确、体例上更加全面、内容上更加具体，罚则也更加细化。

2019年底，科技部办公厅发布《关于开展全国人类遗传资源行政许可管理专项检查有关工作的通知》，决定于2012年12月至2020年2月开展人类遗传资源许可管理专项检查（“专项检查”），通过“单位自查”“属地检查”和“项目组抽查”相结合的方式，全面检查相关单位在人类遗传资源相关活动中的合法合规性，表达了监管层面对人类遗传资源的新态度和新动向。

按照《管理条例》规定，目前人类遗传资源的采集、保藏、利用、对外提供等各环节均存在不同程度的合规要求。结合专项检查的关注重点，目前而言，人类遗传资源的合规收集、利用方面，相关企业至少应重点关注以下合规问题。

1. 所涉及的各个环节是否完成必要的事前审批、备案等行政程序。

本次专项检查的重点之一，即核查是否存在应报未报或超出审批范围开展涉及我国人类遗传资源活动的情况。这一定程度上延续了此前科技部公示6家单位的处罚决定书[10]所表明的监管态度。

具体而言，前述行政程序主要包括：

（1）涉及采集我国重要遗传家系、特定地区人类遗传资源[11]或者采集国务院科学技术行政部门规定种类、数量的人类遗传资源的，需经科技部批准，并满足相应条件；

（2）保藏我国人类遗传资源、为科学研究提供基础平台的，需经科技部批准，并满足相应条件；

（3）利用我国人类遗传资源开展国际合作科学研究的，应由合作双方共同向科技部提出申请，如发生合作方、研究目的等重大变更，应办理变更审批；

（4）为获得相关药品和医疗器械在我国上市许可，在临床机构利用我国人类遗传资源开展国际合作临床试验而不涉及人类遗传资源材料出境的，应向科技部备案。

2. 企业内部相关管理制度是否建立完善。

例如，是否已具有负责人类遗传资源管理的内部部门设置，是否建立并落实人类遗传资源保藏管理制度要求等。专项检查中，在检查主体责任落实情况时，人类遗传资源采集、保藏、国际合作、出境等活动规章制度的建立和完善情况被明确为重点考察的内容之一。

3. 人类遗传资源采集过程是否合法合规、取得授权。

例如，按照《管理条例》规定，相关单位采集我国人类遗传资源时，应事先告知人类遗传资源提供者采集目的、采集用途、对健康可能产生的影响、个人隐私保护措施及其享有的自愿参与和随时无条件退出的权利，并征得人类遗传资源提供者书面同意。

随着《网络安全法》等法律法规的陆续落地，社会整体个人信息保护意识相应增强，专项检查也相应将人类遗传资源材料提供者知情同意的落实情况作为重点检查内容之一，一定程度上也是人类遗传资源提供者保护与个人信息主体保护制度的接轨。

4. 重点关注是否涉及对外提供我国人类遗传资源的情况。

根据《管理条例》，将我国人类遗传资源材料[12]以运送、邮

---

[9] 参见2012年《国务院关于第六批取消和调整行政审批项目的决定》。

[10] 参见科技部政务服务平台网站，链接：https://fuwu.most.gov.cn/html/jcxtml/20181218/2837.html?tab=xzcf，最后访问2020年2月24日。

[11] 根据2015年科技部公布的《人类遗传资源采集、收集、买卖、出口、出境审批行政许可服务指南》，重要遗传家系包括遗传性疾病或特定体质特征发生在家族式的（2代及以上）、有血缘关系的群体的遗传资源，如哮喘、癌症等多发疾病。特定地区人群遗传资源包括特殊环境下长期生活，并且在体质特征或生理特征方面有适应性性状发生的人群遗传资源，如地理隔离人群（海岛和陆岛人群、处于地理隔离的少数民族聚居群体等）。

[12] 根据《管理条例》，人类遗传资源材料是指含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料，人类遗传资源信息是指利用人类遗传资源材料产生的数据等信息资料。

寄、携带等方式出境的，应经科技部批准并取得出境证明；将人类遗传资源信息对外提供的，应向科技部备案并提交信息备份。如可能影响我国公众健康、国家安全和社会公共利益的，还应通过科技部组织的安全审查。

尤为值得注意的是，根据《管理条例》规定，外国组织、个人及其设立或者实际控制的机构不得在我国境内采集、保藏我国人类遗传资源，不得向境外提供我国人类遗传资源，仅可以通过与中方单位合作的方式开展国际合作科学研究，并且该等国际合作过程还需满足一系列相关条件，包括但不限于中方的实质性参与、研究记录和数据完全面向中方单位开发并提供备份、研究成果需由双方共同申请专利并共有专利权等。

不难发现，《管理条例》对于我国人类遗传资源向境外的提供等可能涉外的场景提出了相对严格的监管要求。类似的，本次专项检查也同样高度关注人类遗传资源的出境情况、国际合作知识产权分享与安排情况。

实际上，随着“生物安全应归于国家安全”这一认知的广泛普及，各国对遗传资源和生物安全的意识和管理将有可能与网络安全类似，逐渐提升至国家战略层面，例如美国和英国已于2018年相继发布《国家生物安全防御战略》（National Biodefense Strategy）和《英国生物安全战略》（UK Biological Security Strategy），提出了生物安全方面的风险认知强化以及防御体系的建立。为此，从未来的监管发展来看，生物安全的重要性越发提升，而相关人类遗传资源则更加可能面临严格的合规要求，也更可能对相关企业、单位的合规应对措施提出更为艰巨的挑战。

（三）生物安全与重要数据

生物安全涵盖范围很广，尤其是从生物资源的展现看，虚拟的生物样本数据、试验数据等非实体的生物资源和实体的生物资源一样，都是生物安全话题下的保护对象。为此，由于生物数据的发现、收集、存储、追溯、数据库建立和分析均可能对于生物技术研发和生物资源价值利用产生重要影响，生物数据的保护同样是生物安全的重要一环。

不过，虽然生物安全已明确纳入国家安全体系，但目前我国立法中，对于生物数据的整体保障水平和关注度仍有待进一步提升。举例而言，与生物安全法同属国家安全体系下的《网络安全法》，已针对性提出“关键信息基础设施”、“重要数据”等关键概念，并对于这些可能对于国家安全、国计民生、公共利益造成重大影响的客体、对象予以了重点保护。而在现有立法成果中，“关键信息基础设施”和“重要数据”的具体范围均尚未能够明确划定，但从已形成和发布的《关键信息基础设施确定指南》、《信息安全技术 数据出境安全评估指南（征求意见稿）》（“《出境指南》”）等未生效的征求意见稿等文件中看，“关键信息基础设施”所主要针对的行业中与生物安全密切相关的仅医疗卫生行业，而“重要数据”的范围则主要体现在《出境指南》的附录中，其中共提出了27大类重要数据，但除“A18.人口健康”“A21.食品药品”等部分行业中的特定类型数据可能涉及生物数据外，同样并未对于生物技术、生物制品或其他生物相关行业下的生物数据予以特别关注。

不过，虽然生物相关行业及行业数据尚未得到充分的立法关注，但在生物安全的重要性有了本质不同的背景下，生物数据的安全和保障将成为一个网络安全和生物安全的交叉地带，需要“双管齐下”，才能予以最佳保护。同时，也不难预测，在日渐丰富的网络安全立法体系支持下，生物数据将很快成为生物安全法下的一个重要话题。

为此，对于相关企业而言，在立法不断推进、涉及交叉监管地带的情况下，细致梳理业务实践可能涉及的合规义务，立足现有监管要求并适当考虑未来监管趋势，合理拟定经营策略和合规体系，将成为一项极具挑战的任务。

三、小结与建议

随着生物安全成为世界各国维护国家安全的重要制度组成部分，在《中国国家生物安全框架》制定20年后，《草案》作为我国第一部生物安全领域的统一、综合立法，将起到提纲挈领的重要价值。同时，如其第一条中所述的，《草案》作为我国生物安全立法的重要进展，其重要目的在于“促进人类命运共同体建设”，表达了对全人类福祉的良好骐骥，也将有助于中国积极参与全球生物安全领域共同治理的体现。

从立法的角度看，生物安全法的积极作用值得期待，包括但不限于：（1）理顺不同制度体系之间的关联，通过统一的协同机构建立必要的沟通机制；（2）构建不同主体、不同层次的信息共享体系，兼顾国家安全和发展需要，既守住底线，又为生物资源及相关数据的流转和利用提供清晰的路径参照。但同时，生物安全立法仍任重而道远，《草案》目前仍未通过，配套措施也尚不成熟。此外，除实体生物材料和样本以外，生物技术的开发和生物资源同样可能以数据等非实体形态存在或体现，对于该等非实体生物资源的保护，无论是因循“重要数据”的立法思路（如人口健康信息、药品开发过程中的动物与人体试验数据等），还是另辟蹊径建立对生物资源及生物数据的管控要求，均值得后续的立法工作进一步解答。

而从企业的角度看，在现行监管框架下，生物安全相关业务实践通常可能涉及交叉监管领域，需要切实梳理涉及行业及相关法定义务。为此，企业一方面需要更加关注实体和虚拟两个层面的生物安全，对于自身所掌握和持有的实体生物资源、研究数据、样本数据等及时进行盘点与分级分类，进而根据分级分类结果识别、落实法定义务。同时合理制定并严格落实内部管控措施（如实验室物理访问权限、生物数据利用权限、对外数据交互安全基线等）；另一方面，相关企业也应当参照现有法律法规、国家标准、行业标准等规定内容，切实建立内部责任制度，以内部责任追究确保相关保障措施的有效性，避免生物安全事件带来的不利后果。

而进一步考虑目前的立法趋势，未来对于企业而言，关注生物安全将成为更为普遍的合规要求，这也要求相关企业密切关注立法动态，并根据自身情况，采取相应的应对措施，具体而言：

1. **对合法持有和保管相关生物资源的境内企业而言**，一方面应当关注和期待生物安全法可能提供的合规商业化路径，发挥既有资源的价值，另一方面可能需要进一步探索新的技术思路（如人工智能技术的应用等），以实现生物资源的共同开发、利用；
2. **对于有相关需求和开发能力的境内企业而言**，除切实履行必要的行政程序（如审批、申报、备案等）外，在生物技术和生物制品等相关产品的研发过程中，还应充分吸取此前相关事件的经验，重点关注伦理审查和道德伦理要求，避免因技术或产品研发突破社会公众可接受的合理必要限制；
3. **对境外企业或存在与境外合作需求的涉外企业而言**，则可能需要更为全面和审慎地梳理、识别潜在的合规要求。由于涉及境外的生物技术和生物产品开发和提供过程将很难避免生物资源（无论是实体还是虚拟形态）的跨境传递，该等传递过程中的安全保障将成为一大挑战。从实体生物资源上讲，一旦泄露或处置不当即可能引发生物入侵、生物安全事件等不利后果，而从生物数据等虚拟资源上讲，构成人口健康信息、人类遗传资源等数据类型均可能面临明确的跨境传输限制。为此，更为通畅、彻底的国际合作无疑有益于生物技术的整体进步，但考虑到前述安全和合规保障的必要需求，我们建议境外企业或涉外企业应更加审慎地对待生物安全合规事宜，并提前准备备选合规策略（如适当本地化、技术处理方案等），以应对跨境合作中的生物安全风险。

附录 现行生物安全相关法律框架梳理

涉及领域	主要监管机构	重点法律法规	重要监管要求（部分）
传染病防控	卫生健康委员会及各级政府卫生健康机构等	《中华人民共和国传染病防治法》	- 将传染病分为甲、乙、丙三类，就传染病预防，疫情报告、通报和公布，疫情控制，医疗救治，传染病防治工作的监督管理、保障措施和法律责任等进行规制 - 疫情防控，特别是疫情信息监测、预警、通报与信息发布等环节中，不得泄露涉及个人隐私的有关信息、资料
		《突发公共卫生事件应急条例》	- 针对重大传染病疫情、群体性不明原因疾病、重大食物和职业中毒等严重影响公众健康的突发事件的预防与应急准备、报告与信息发布、应急处理工作进行了规定，同时明确了各级医疗卫生机构和相关单位的法律责任
		《中华人民共和国传染病防治法实施办法》	- 就传染病的预防、疫情报告、传染病控制进行了具体明确，特别就疫情的上报时限进行了规定 - 规定医务人员未经县级以上政府卫生行政部门批准，不得将就诊的淋病、梅毒、麻风病、艾滋病病人和艾滋病病原携带者及其家属的姓名、住址和个人病史公开
		《关于做好个人信息保护利用大数据支撑联防联控工作的通知》	- 要求除国务院卫生健康部门依法授权的机构外，其他任何单位和个人不得以疫情防控、疾病防治为由，未经被收集者同意收集使用个人信息 - 收集联防联控所必需的个人信息应参照国家标准《个人信息安全规范》，坚持最小范围原则，收集对象原则上限于确诊者、疑似者、密切接触者等重点人群，一般不针对特定地区的所有人群，防止形成对特定地域人群的事实上歧视
		《突发公共卫生事件与传染病疫情监测信息报告管理办法》	- 规定了突发公共卫生事件和传染病疫情发布内容，包括突发公共卫生事件和传染病疫情的性质，原因，发生地，范围，发病、伤亡及涉及的人员范围，处理措施和控制情况及发生地的解除

涉及领域	主要监管机构	重点法律法规	重要监管要求（部分）
人类遗传资源安全保护	科学技术部及各级政府科技主管部门等	《中华人民共和国人类遗传资源管理条例》	- 针对人类遗传资源的采集和保藏，利用和对外提供进行了规制，强调了科学技术行政部门的服务和监督职能，明确了相关单位和个人违法和买卖人类遗传资源的法律责任 - 采集、保藏、利用、对外提供我国人类遗传资源，应当符合伦理原则，按规定进行伦理审查 - 外国组织、个人及其设立或者实际控制的机构不得在我国境内采集、保藏我国人类遗传资源，不得向境外提供我国人类遗传资源 - 不得买卖人类遗传资源
		《人类遗传资源管理暂行办法》	- 确立了人类遗传资源分级管理、统一审批制度，规定了申报与审批条件，明确了知识产权处理原则
		《人类遗传资源采集、收集、买卖、出口、出境审批行政许可事项服务指南》	- 对申请开展人类遗传资源采集或收集活动应具备的条件，外方参与的人类遗传资源采集、收集或研究活动应具备的条件，申请开展人类遗传资源出口、出境活动应具备的条件等进行了规定
生物技术研究开发与应用	科学技术部及各级政府科技主管部门	《生物技术研究开发安全管理办法》	- 生物技术研究开发安全管理实行分级管理。从事生物技术研究开发活动的法人、其他组织对生物技术研究开发安全工作负主体责任，应制定本组织各类风险等级生物技术研究开发安全事故应急预案和处置方案，对生物技术研究开发安全事故进行快速有效处置，并向上级主管部门报告
		《生物技术研究开发安全管理条例（征求意见稿）》	- 就开展高风险生物技术研究开发活动应符合的条件进行规定，就生物技术研究开发的安全风险控制与处置进行规制，明确科学技术行政部门的服务与监督责任和相关单位违法操作的法律责任
实验室生物安全	生态环境部、卫生健康委员会及各级政府环境、兽医、卫生主管部门	《病原微生物实验室生物安全管理条例》	- 就病原微生物的分类和管理，实验室的设立和管理，实验室感染控制等进行了规定，明确了卫生主管部门、兽医主管部门、环境保护主管部门的监督管理责任
		《病原微生物实验室生物安全环境管理办法》	- 对病原微生物实验室实行分级管理，要求实验室妥善收集、贮存和处置其实验活动产生的危险废物，防止环境污染；制定环境污染应急预案，发生泄露或者扩散后应立即应急处置
物种入侵防范与生物多样性保护	国家林业和草原局及各级林业主管部门	《引进陆生野生动物外来物种种类及数量审批管理办法》	- 引进陆生野生动物外来物种的应当采取安全可靠的防范措施，防止其逃逸、扩散，避免对自然生态造成危害。需要从境外引进陆生野生动物外来物种的应向林业主管部门提出申请
病原微生物管理	卫生健康委员会及各级政府卫生健康机构等	《人间传染的病原微生物菌（毒）种保藏机构管理办法》	- 规定了人间传染的病原微生物菌（毒）种保藏机构的职责、保密义务，申请保藏机构应当具备的条件，保藏活动应当符合的规范等，保藏机构应当制定严格的安全保管制度并制定应急预案
伦理管理	卫生健康委员会及各级政府卫生健康机构等	《涉及人的生物医学研究伦理审查办法》	- 涉及人的生物医学研究应当符合知情同意、控制风险、免费和补偿、保护隐私、依法赔偿和特殊保护原则，应做到尊重和保障受试者是否参加研究的自主决定权，切实保护受试者的隐私，如实将受试者个人信息的储存、使用及保密措施情况告知受试者，未经授权不得将受试者个人信息向第三方透露
基因工程和转基因	科学技术部及各级政府科技主管部门	《基因工程安全管理办法》	- 对基因工程按安全等级分级管理，从事基因工程工作的单位，应当依据遗传工程产品适用性质和安全等级，分类分级进行申报，经审批同意后方能进行；从事基因工程工作应当根据安全等级，确定安全控制方法，制定安全操作规则

感谢赵天琦对本文所做的贡献。

（本文发布于2020年02月25日。）

竹杖芒鞋轻胜马：
医疗大数据发展和合规管理并重

前言

在大数据经济“热火朝天”的景象中，医疗行业经营者应当不被纷扰的经济利益所诱惑，把守合规的“红线”。同时，尽管相比于国外较为成熟的商业化模式和监管体系，国内医疗大数据如何开放和共享尚不明确，但我们更应当在医疗大数据开发的“底线”之上，发挥优势，积极创新和发展合规的医疗大数据行业。

伴随着技术的迅速发展，大数据分析在数据密集型与数据驱动型的医疗领域扮演着日益重要的角色。通过各方资源的整合和数据的交互，医疗行业经营者正不断地加强对疾病的理解，加快医学科技的创新，从而推动新型医药产品与医疗器械的研发，寻求更优的治疗方案，提升医疗服务及其相关衍生产业的整体水平与质量。

在医疗行业经营者尝试打破数据孤岛、消除数据壁垒的过程中，数据安全与隐私保护的合规问题也逐渐凸显。在现有的法律法规框架下，医疗数据在性质上可能构成多种受保护的数据类型，而不同的法律法规又对不同的法律责任主体及其具体义务进行规范，无疑为医疗行业经营者的合规工作增加了复杂度。如何在合规的前提下充分挖掘、发挥医疗数据对行业经营者、对产业生态与技术迭代的积极作用，是医疗行业经营者当前亟需解决的难题。

一面是“互联网+医疗健康”政策的鼓励与推动下商业发展和技术创新的强烈需求，一面是与医疗数据处理活动紧密相关而又错综复杂的合规监管要求，如何梳理合规的差距并在此基础之上创新发展医疗大数据产业？基于我们以往的经验和国内外的立法背景，我们理解要分四步走：

- 识别医疗数据性质与类型；
- 确定医疗数据责任主体;
- 整合医疗数据合规要求；和
- 梳理数据权益。

一、识别医疗数据性质与类型

合规工作从来都始于事实发现，在医疗数据合规领域亦不例外。如前所述，为了最终整合并形成适用于自身的医疗数据合规方案，医疗行业经营者首先应当关注、识别现行法律法规中主要规则下的医疗数据性质，对照梳理内部医疗数据的类型，并以此作为合规切入点之一。在下表中，我们列举了在医疗数据合规领域受保护的典型数据类型，以及其对应的监管规则（不完全摘录）。

医疗数据类型	法律概念界定	主要监管规则
健康医疗大数据	指在人们疾病防治、健康管理等过程中产生的与健康医疗相关的数据。	• 《国家健康医疗大数据标准、安全和服务管理办法（试行）》 • 《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》
人口健康信息	指依据国家法律法规和工作职责，各级各类医疗卫生计生服务机构在服务和管理过程中产生的人口基本信息、医疗卫生服务信息等人口健康信息。	• 《人口健康信息管理办法（试行）》 • 《“十三五”全国人口健康信息化发展规划》
病历（电子病历）	• 病历：指医务人员在医疗活动过程中形成的文字、符号、图表、影像、切片等资料的总和，包括门（急）诊病历和住院病历； • 电子病历：指医务人员在医疗活动过程中，使用信息系统生成的文字、符号、图表、图形、数字、影像等数字化信息，并能实现存储、管理、传输和重现的医疗记录，是病历的一种记录形式，包括门（急）诊病历和住院病历。	• 《医疗机构病历管理规定》 • 《电子病历应用管理规范（试行）》 • 《电子病历系统功能规范（试行）》 • 《关于进一步推进以电子病历为核心的医疗机构信息化建设工作的通知》
人类遗传资源	人类遗传资源包括人类遗传资源材料和人类遗传资源信息。 人类遗传资源材料是指含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料。 人类遗传资源信息是指利用人类遗传资源材料产生的数据等信息资料。	• 《人类遗传资源管理条例》 • 《人类遗传资源采集、收集、买卖、出口、出境审批行政许可事项服务指南》
医疗器械领域的健康数据	标明生理、心理健康状况的私人数据（“Private Data”，又称个人数据“Personal Data”、敏感数据“Sensitive Data”，指可用于人员身份识别的相关信息），涉及患者隐私信息。	• 《医疗器械网络安全注册技术审查指导原则》

值得医疗行业经营者关注的是，一方面，不同法律法规中对医疗行业相关数据的界定差异显著，部分采取囊括式的界定方式，较大范围地涵盖医疗行业经营过程中可能涉及的相关数据，如“健康医疗大数据”与“人口健康信息”。这种界定方式主要体现国家对医疗行业数据整体的监管态势，从战略高度与原则层面对经营者的数据处理活动提出纲领性的要求—从《人口健康信息管理办法（试行）》到《国家健康医疗大数据标准、安全和服务管理办法（试行）》的演进也在一定程度上印证了这一观点。而部分数据类型的界定则伴有“场景化”的倾向，其中以“（电子）病历”、“人类遗传资源”与“（医疗器械中的）健康数据”三者尤为明显，对这类数据的合规考察则需要更多地结合其定义中所设定的场景与条件进行，而不能主观臆断。

另一方面，上表中强调的医疗数据类型仅仅是从医疗行业的监管角度出发所整理的情况，但医疗行业数据同样在《网络安全法》的数据监管体系中也有特殊要求。例如，《个人信息安全规范》中则将“个人健康生理信息[1]”明确列为“个人（敏感）信息”；《数据出境安全评估指南（征求意见稿）》的附录A“重要数据识别指南”中也将部分医疗行业相关的数据包括在内，例如“A.18 人口健康”与“A.21 食品药品”等两个类别。而针对《网络安全法》体系下的合规要求，则需要同步参照《网络安

[1] 具体包括个人因生病医治等产生的相关记录，如病症、住院志、医嘱单、检验报告、手术及麻醉记录、护理记录、用药记录、药物食物过敏信息、生育信息、以往病史、诊治情况、家族病史、现病史、传染病史等，以及与个人身体健康状况产生的相关信息，及体重、身高、肺活量等。具体参见《个人信息安全规范》附录A“个人信息示例”和附录B“个人敏感信息示例”。

全法》《个人信息安全规范》《个人信息出境安全评估办法（征求意见稿）》《数据安全管理办法（征求意见稿）》等规范，并以其为起点梳理具体的合规义务。换言之，在开展医疗数据合规工作的过程中，医疗行业经营者既要关注医疗行业规范的具体要求，也不能忽视《网络安全法》体系下对“个人（敏感）信息”与“重要数据”的合规监管——两大维度缺一不可。

二、确定医疗数据责任主体

法律权利义务关系的落实，始终需要依靠法律主体进行。相应地，在识别医疗数据性质与类型的同时，医疗行业经营者数据合规的下一步骤则是确认具体规范下的法律责任主体，即明确自身是否直接受制于特定的法律法规及其他规范性文件。在数据性质与类型准确识别的基础之上，责任主体身份的确定将在很大程度上决定了特定企业所需遵循的医疗数据合规要求。

• 相关企事业单位

《国家健康医疗大数据标准、安全和服务管理办法（试行）》下的责任单位范围不仅仅包括传统的医疗机构，还包括相关的企事业单位。因此，相关企事业单位（如在疾病健康管理、临床决策支持、医疗研发等领域开展业务的医疗大数据企业）也应符合健康医疗大数据有关的合规要求。

同时，我们也注意到，《国家健康医疗大数据标准、安全和服务管理办法（试行）》的第三十一条似乎有意区分了健康医疗大数据的“责任单位”与其“服务提供商”，从表述方式上看两个术语应该有所区别而不应混同，但从概念界定上看“服务提供商”也很有可能构成“责任单位”。因此，如何处理和协调二者在实际监管执法中的定位与关系，将有待主管部门提供进一步的澄清与实践。

• 医疗机构

各级各类医疗机构由于拥有大量各类的第一手医疗数据，是最为重要的行业主体之一，在挖掘医疗数据价值的同时，应尤其注意数据安全和隐私保护相关的合规义务。各级各类医疗机构在《国家健康医疗大数据标准、安全和服务管理办法（试行）》《医疗机构病历管理规定》《人口健康信息管理办法（试行）》等规定下均为直接的责任主体。

• 人类遗传资源利用单位

根据《人类遗传资源管理条例》，相关科研机构、高等学校、医疗机构、企业可以根据自身条件和相关研究开发活动需求，利用人类遗传资源开展研究开发活动。

需要注意的是，在阐述适用范围时，《人类遗传资源管理条例》不仅仅限定了主体与对象，也明确指出本条例主要规制人类遗传资源的“采集、保藏、利用、对外提供”，而“为临床诊疗、采供血服务、查处违法犯罪、兴奋剂检测和殡葬等活动需要，采集、保藏器官、组织、细胞等人体物质及开展相关活动，依照相关法律、行政法规规定执行”，二者并不是“或”而是“并”的关系，更多地是针对现实中同一事物在法律上存在的差异性规定，企业在推进合规的过程中应当按需适用。

• 医疗器械产品注册人

随着网络技术发展，越来越多的医疗器械具备网络连接功能以进行电子数据交换或远程控制。具备相关功能的医疗器械产品生产商/注册人，则应当根据《医疗器械网络安全注册技术审查指导原则》的要求落实履行相应的网络安全义务。

与上文同理，如特定的医疗行业经营者被认定构成《网络安全法》下的关键信息基础设施运营者（尤其是“医疗卫生”被明确列举在《关键信息基础设施安全保护条例（征求意见稿）》的重要行业和领域范围中）或网络运营者，那么将进一步构成《网络安全法》及其配套性措施下的义务主体，进而需要在医疗数据合规工作中一并适用网络安全领域的合规要求。

此外，企业在开展具体的合规时，确定医疗数据责任主体的工作不应仅仅停留在法律层面，还应在合理的程度内考虑现实中可能发生的协议安排，即不能只着眼于法律法规直接、明确适用的主体类型，还需要进一步结合数据合作项目的实际情况，考察合作方是否将其直接受制的法律法规要求转化、传导为合作协议中的安排，从而在一定程度上“转嫁”或“分摊”合规负担。

三、整合医疗数据合规要求

在识别医疗数据性质与类型、确定医疗数据责任主体的基础之上，医疗行业经营者则需要综合不同法律法规中的合规要求，整合适用于自身的医疗数据合规方案。由于现实中的一种医疗数据可能具有多重法律属性，从而受制于不同的监管要求，我们将在下文尝试梳理典型法律法规中医疗数据生命周期各环节的主要合规义务。

• 医疗数据的收集

人口健康信息的采集原则上应当遵循“一数一源、最少够用”的采集原则，即所采集信息应符合业务应用和管理要求，严格实行信息复核程序，避免重复采集、多头采集。

相较而言，采集我国人类遗传资源，应当事先告知人类遗传资源提供者采集目的、采集用途、对健康可能产生的影响、个人隐私保护措施及其享有的自愿参与和随时无条件退出的权利，并征得人类遗传资源提供者的书面同意。采集重要遗传家系、特定地区人类遗传资源等还应取得国务院科学技术行政部门的批准。

对构成个人信息的医疗数据采集，根据《个人信息安全规范》的要求，直接收集时应获取被收集者的同意（构成个人敏感信息的，还应当获得明示同意）；间接收集时，应要求个人信息提供方说明个人信息来源，并对其合法性进行确认，同时应了解已获取的个人信息处理的授权同意范围。如以经营为目的收集个

人敏感信息或重要数据，按照《数据安全管理办法（征求意见稿）》，应当向所在地网信部门备案，此外企业内部应当明确数据安全责任人。

• 医疗数据的使用

《医疗机构病历管理规定》对病历的使用具有严格限制。具体而言包括：（1）目的限制——医疗机构及其义务人员应严格保护患者隐私，禁止以非医疗、教学、研究目的泄露患者病历资料；以及（2）主体限制——除特定主体（患者、医务人员、经授权负责病案管理/医疗管理的部门或者人员等）外，其他任何机构和个人不得擅自查阅患者病历。

对于人口健康信息，责任单位应当建立综合利用工作制度，授权利用有关信息，并且其利用目的应限制于提高医学研究、科学决策和便民服务水平。然而，《人口健康信息管理办法（试行）》本身并未就该等工作制度的制定有更进一步的明确要求。

对于人类遗传资源的利用，如涉及外方单位，应当与中方单位以合作的方式开展，同时经国务院科学技术行政部门批准。

对医疗器械领域的健康数据而言，《医疗器械网络安全注册技术审查指导原则》要求在与非注册申请人预期的设备或系统相连接时，应保证自身网络安全，并明确与其预期相连设备或系统的接口要求。

• 医疗数据的存储

就病历数据而言，门（急）诊病历原则上由患者负责保管，经患者或者其法定代理人同意，也可以由医疗机构负责保管，保存时间自患者最后一次就诊之日起不少于15年。住院病历由医疗机构负责保管，保存时间自患者最后一次住院出院之日起不少于30年。而《电子病历应用管理规范（试行）》则明确要求，电子病历数据所依赖的电子病历系统应对操作人员进行身份识别，并确保操作记录可查询、可追溯，同时应设置医务人员书写、查阅、修改的权限和时限。

对人口健康信息而言，应具备符合有关规定要求的数据存储、容灾备份和管理条件。同时，责任单位应实施痕迹管理制度，建立、修改和访问人口健康信息的用户，均应通过严格实名身份鉴别和授权控制，做到行为可管理、可控制、可追溯。

而根据具有迭代意义的《国家健康医疗大数据标准、安全和服务管理办法（试行）》的相关规定，针对健康医疗大数据的存储，医疗机构及相关企事业单位应采取数据分类、重要数据备份、加密认证等措施，并同时施行电子实名认证和数据访问控制措施，严格规范不同等级用户的数据接入和使用权限，并确保相关数据在授权范围内使用。

• 医疗数据的跨境传输

健康医疗大数据原则上应当存储于境内服务器，因业务需要确需向境外提供的，应按照相关法律法规及有关要求进行安全评估审核；相较而言，人口健康信息则存在严格的本地化处理义务。值得注意的是，《人口健康信息管理办法（试行）》对于人口健康信息的本地存储义务并未规定任何的例外情景，其明确要求“不得将人口健康信息存储于境外服务器，不得托管、租赁在境外的服务器”。换言之，一旦医疗数据属性上构成人口健康信息，其跨境传输活动将被严格禁止。

与人口健康信息不同的是，人类遗传资源在特定条件下可以跨境传输。根据《人类遗传资源管理条例》，利用我国人类遗传资源开展国际合作科学研究，或者因其他特殊情况确需将我国人类遗传资源材料运送、邮寄、携带出境的，应符合特定条件，并取得人类遗传资源材料出境证明。考虑到人类遗传资源在一定程度上也可能构成人口健康信息（从而承担着本地化的义务），而人类遗传资源的中外合作项目在实践中似乎并未遭遇显著的合规障碍，这一看似“矛盾”的规则要求应如何解读和协调，仍有待主管部门的进一步澄清。

此外，关键信息基础设施运营者对于其境内运营中所收集产生的个人信息和重要数据具有本地存储义务。如因业务需要，确需向境外提供的，应当进行安全评估。

值得医疗行业经营者高度关注的是，在整合医疗数据合规方案的时候，我们应该采用“就高不就低”的基本原则。如前所述，同一主体、同一数据在特定场景下可能具备不同的法律属性，因而针对该主体与数据对象，合规工作应该综合选用最严格的要求，以整合为应对交叉监管的合规方案。

例如，医院档案室中存放的患者X光片影像资料，其在法律意义上将存在多种定性，包括病历（《医疗机构病历管理条例》）、人类遗传资源（《人类遗传资源管理条例》）、人口健康信息（《人口健康信息管理办法（试行）》）、健康医疗大数据（《国家健康医疗大数据标准、安全和服务管理办法（试行）》）、个人（敏感）信息与重要数据（《网络安全法》）等。相应地在存在跨境传输需求的场景下，原则上医院需要综合考虑多个法律法规及规范性文件中的要求，选择更为严格的选项，即《人口健康信息管理办法（试行）》中设定的数据本地化义务作为合规方案，已达到“全面合规”的根本目的。

四、梳理医疗数据权益

在通过数据类型、确认主体、合规要求三大步骤之后，医疗行业经营者应该能较为清晰地了解自身的合规责任和义务。但在合规责任和义务之上，医疗行业经营者实践中可能更为关心如何进一步利用医疗大数据，达成商业化目的。遗憾的是，目前对于医疗数据商业化仍未有比较明确的指南或者被认可的商业模式，医疗行业经营者仍处于“摸着石头过河”的阶段。

“他山之石可以攻玉”。很多的医疗行业经营者在国内法律法规对医疗数据开放尚不明确的态度下，选择参考比如美国的HIPAA法案（Health Insurance Portability and Accountability Act）等境外的规定，试图在保证数据安全的前提条件下，开发医疗数

据的商业潜力。在坚持促进医疗大数据发展和合规管理并重的原则下，我们理解医疗行业经营者对于医疗数据的商业化开发还需要重视医疗数据权益的梳理，把准医疗数据商业化的“底线”。比如，从个人信息的角度，从“个人信息控制者”和“个人信息处理者”的角色定位来区分不同经营者对于医疗数据的处理目的和范围的边界；根据医疗机构、医疗研究机构、技术服务提供商等自身的经营和服务范围，以及提供服务中衍生数据的来源和相关投入，在法律法规允许的范围内通过协议等方式划分对于不同颗粒度的医疗数据的权益范围。

五、企业合规建议

正如弗吉尼亚大学法学院健康法领域的Margaret Riley教授所评论：“隐私至关重要。但如果我们仅仅关注于加强个体的管控，将会损害研究。[2]”对于医疗数据予以充分的信息安全和隐私保护并不意味着医疗数据禁止被利用以实现特定的商业价值。尽管如此，医疗行业作为严监管行业，医疗行业经营者在运营中应时刻把握本文中所阐述的医疗数据合规基本思路，即识别医疗数据性质与类型，确定医疗数据责任主体，整合医疗数据合规要求，并密切关注自身合规义务的履行情况。

同时，与开展常规数据合作合规项目相类似，在开展医疗数据的商业合作中，医疗行业经营者均应该着重关注合同条款的订立与尽职调查的适用。一方面，合同条款作为合作各方法律权利义务关系的基础，应当完备地阐述各方在具体法律角色定位下所承担的义务。既应该纳入法律法规、监管规定、重要国家标准的具体合规要求，确保绝不触及底线规范，也需要结合具体的合作项目安排，对可能存在的数据合规风险节点以及要求合作方承诺与保障的内容进行定制化设计，并适时根据法律法规与监管规定，在必要的情况下对合同进行补充约定，以保证合同条款的完整性。另一方面，作为在开展具体商业合作前对合作方必要资质与能力的考察活动，尽职调查在医疗数据合规方面显得尤为重要。鉴于医疗数据合规工作既包含安全技术层面（如数据安全防护能力）的内容，也包含法律裁量层面（如数据处理行为的必要性）的内容，通过自身或聘请的专业机构针对合作方在数据合规方面的资质与能力进行背景审查，既能核实合作方在谈判阶段所述合规情况的真实性，也能尽早发现合作方在数据处理方面可能存在的纰漏，以推动合作项目的后续顺利开展。

除了上文整理的若干典型规范中的医疗数据合规义务外，在医疗数据开发和应用的过程中，医疗行业经营者还应当注意的一般性合规要求包括：

- **收集环节：**直接从患者处收集时，应就相应的数据处理活动取得有效授权；对涉及从第三方处获取医疗数据的企业而言，应当对数据提供方、涉及的数据种类与类型等进行合法性确认；
- **使用环节：**使用适当的技术措施保障数据安全，在能够实现相关使用目的的范围内，尽量对医疗数据进行匿名化或去标识化处理，尤其是针对姓名、身份证号码以及能够唯一标识特定患者的信息；
- **存储环节：**落实有关数据分类、重要数据备份、加密认证等措施保障数据存储安全；
- **跨境传输环节：**医疗行业经营者首先应判断其是否基于特定的主体身份或数据类型具有数据本地存储义务（如主体为关键信息基础设施运营者，或数据类型为人口健康信息），同时注意满足相关跨境传输要求，并尽可能仅传输匿名化后、无法识别特定个人的数据；
- **其他合规义务：**
  ① 成立专门的数据管理部门，并制定专门的责任人；
  ② 及时落实网络安全等级保护：根据2011年发布的《卫生行业信息安全等级保护工作的指导意见》，三级甲等医院的核心业务信息系统等原则上应不低于第三级，并且对第二级以上信息系统，应当报属地公安机关及卫生行政部门备案；
  ③ 建立网络安全事件应急响应机制并定期检测；
  ④ 服务提供商管控：选择医疗数据服务提供商时，应确保其符合国家和行业规定及要求，具备履行相关法规制度、落实相关标准、确保数据安全的能力，建立数据安全管理、个人隐私保护、应急响应管理等方面管理制度。

（本文发布于2019年09月17日。）

[2] "WHY IT'S TIME TO RETHINK THE LAWS THAT KEEP OUR HEALTH DATA PRIVATE"，https://www.theverge.com/2019/1/29/18197541/health-data-privacy-hipaa-policy-business-science.

“花径不曾缘客扫，蓬门今始为君开”
——《中华人民共和国人类遗传资源管理条例》简析

20世纪50年代，DNA双螺旋结构被阐明，正式揭开了生命科学的新篇章，开创了科学技术的新时代。随着人类遗传密码全部被破解，基因在DNA分子水平上得到新的概念。此后2000年6月，中美英法德日六国科学家也共同宣布，人类基因组工程项目的基因组草图绘制正式完成，后续计划ENCODE项目则进一步解析了人类基因组中的功能性元件。时至今日，人类遗传资源已广泛地应用于刑事侦查、司法鉴定、生物医药、疾病诊断与治疗等多个领域，与人类的生活息息相关。

随着基因工程技术的迅猛发展，人类遗传资源的重要意义早已不仅仅局限于其对生命科学研究的重大推动作用，更成为了影响国家公众健康和战略利益的重要资源。正是因为意识到人类遗传资源的重要性，我国著名遗传学家谈家桢先生在1997年呼吁要保护我国的基因资源，成功推动了中国基因组研究的发展，推动了1998年类基因组北方中心和南方中心正式成立，推动了《人类遗传资源管理暂行办法》（以下简称“《暂行办法》”）的颁布实施。[1]

在之后的十几年间，随着国际形势与实践的发展，在人类遗传资源管理上出现了不少新情况与新问题，如2018年的“基因编辑婴儿”事件等等，引发了行业和社会的广泛探讨。如何有效地保护我国人类遗传资源并促进其合理利用，如何在法律规范与监管落实上作进一步完善，成为了人类遗传资源领域亟待解决的重要任务——这也正是《人类遗传资源管理条例》（以下简称“《管理条例》”）出台的现实背景。

一、《管理条例》的四大亮点

2019年的《管理条例》沿袭了1998年《暂行办法》的整体精神，并在《暂行办法》的基础上，整合了部分此前规定在科技部2015年7月2日公布的《人类遗传资源采集、收集、买卖、出口、出境审批行政许可服务指南》（以下简称“《服务指南》”）中的内容。二者相比较，《管理条例》的变化主要体现在，国家对人类遗传资源合理利用的态度更加明确、体例上更加全面、内容上更加具体、罚则更加细化。

（一）条款体例优化

《管理条例》的一大显著特征即是，在《暂行办法》的基础上，对整部法规的体例进行了完善，从之前的“总则-管理机构-申报与审批-知识产权-奖励与处罚-附则”的结构调整为目前的“总则-采集和保藏-利用和对外提供-服务和监督-法律责任-附则”，就处理人类遗传资源的全流程进行了规定，包括采集、保藏、利用、对外提供等环节，并且明确了监管机构的权力与职能，细化了违反规定处理人类遗传资源的法律责任，相较之前的版本更加全面、清晰，便于企业依照规定采取合适的措施。

（二）核心内容具化

《管理条例》对《暂行办法》中提到的多项规定进行了进一步细化，监管的态度更加明确，具体要求相较《暂行办法》而言也更为实际可操。事实上，我们注意到，除了沿用或更新《暂行

[1]《条例出台，我国重要人类遗传资源将“大有可为”》，载http://www.moj.gov.cn/news/content/2019-06/10/zcjd_236558.html，2019年6月10日。

办法》的相关规定，《管理条例》对若干细节问题的规定来自于科技部的《服务指南》和《<人类遗传资源采集、收集、买卖、出口、出境审批行政许可服务指南>的常见问题》（以下简称“《问题解答》”）[2]。

首先，《管理条例》在《暂行办法》的基础上进行了一些细化、明确化的规定。例如，《管理条例》第七条对外国组织与个人及其设立或者实际控制的机构采集、保藏、向境外提供我国人类遗传资源予以明确禁止。又如，第三十一条明确专家的意见将作为审批决定的参考依据。

其次，《管理条例》也对《暂行办法》有一定的澄清和细化。例如，第二十条对利用我国人类遗传资源开展生物技术研究开发活动或者开展临床试验进行了规定。不仅如此，《管理条例》第四章针对行政部门的职责，增加了诸多此前未在《暂行办法》中明确列出的规定，包括科学技术行政部门对电子政务的建设、对人类遗传资源活动各环节的监督检查的义务、对审批备案事项的指导、投诉举报的具体方法等。

此外，《管理条例》的部分规定也直接来源于《服务指南》和《问题解答》的相关内容。例如，《管理条例》第三条，其中对为临床诊疗、采供血服务、查处违法犯罪、兴奋剂检测和殡葬等活动需要，采集、保藏器官、组织、细胞等人体物质及开展的相关活动的规定，则来自于《服务指南》中的规定；《管理条例》第十条关于禁止买卖遗传资源的规定，同样来源于《服务指南》。

在下表中，我们对《管理条例》中对企业与个人在人类遗传资源的采集、保藏、利用、对外提供等环节中提出的主要要求进行了梳理，以供参考：

处理环节	义务内容	对应条款	一语短评
采集	**告知与同意** 采集人类遗传资源需首先告知人类遗传资源提供者采集目的、采集用途、对健康可能产生的影响、个人隐私保护措施及其享有的自愿参与和随时无条件退出的权利，并征得其书面同意。	第十二条	值得注意的是，《管理条例》对于人类遗传资源提供者的保护采用了类似个人信息主体保护的制度，具体体现在第九条、第十二条、第三十九条中
	采集前的审批 若采集的人类遗传资源属于我国重要遗传家系，特定地区人类遗传资源，或者采集国务院科学技术行政部门规定种类、数量的人类遗传资源，则应当满足采集主体、采集目的、采集方案、伦理审查、管理措施、采集物资等方面进一步的条件，并经国务院科学技术行政部门批准。	第十一条	审批条件与《服务指南》中规定的条件基本一致
保藏	**保藏前的审批** 保藏我国人类遗传资源、为科学研究提供基础平台的，应当满足保藏主体、保藏目的、保藏方案、人类遗传资源来源、伦理审查、管理措施、保藏物资等方面进一步的条件，并经国务院科学技术行政部门批准。	第十四条	此为《管理条例》对于遗传资源的保藏新增加的规定，在《管理条例》发布前，涉及人类遗传资源的审批仅有人类遗传资源的采集和收集、以及人类遗传资源的出口和出境两项，也未对人类遗传资源保藏单位的义务作出明确要求。
	保藏单位的义务 保藏单位应当（1）确保人类遗传资源的安全；（2）记录人类遗传资源保藏情况，妥善保存人类遗传资源的来源信息和使用信息；（3）向国务院科学技术行政部门提交年度报告。	第十五条	
利用	**外方单位利用遗传资源的途径** 外方组织及外国组织、个人设立或者实际控制的机构需要利用我国人类遗传资源开展科学研究活动的，需采取与我国科研机构、高等学校、医疗机构、企业合作的方式进行。	第二十条	这一要求在此前《暂行办法》中有暗指的可能，并未明确提出

[2] 参见标题，载https://www.most.gov.cn/bszn/new/rlyc/cjwt/，2019年6月12日。

处理环节	义务内容	对应条款	一语短评
利用	**利用前以及重大变更的审批** 利用我国人类遗传资源开展国际合作科学研究的，应当符合一定条件，并由合作双方共同提出申请，经国务院科学技术行政部门批准。如合作方、研究目的、研究内容、合作期限等重大事项发生变更，则应当办理变更审批手续。 为获得相关药品和医疗器械在我国上市许可，在临床机构利用我国人类遗传资源开展国际合作临床试验、不涉及人类遗传资源材料出境的，不需要审批，但是应当向国务院科学技术行政部门备案。	第二十二条、第二十三条	• 国际合作项目的审批条件与《服务指南》中规定的条件基本一致，更新的是申请主体由中方变更为中外双方 • 第二十三条关于变更审批的规定来自于《问题解答》，但在《管理条例》中并未明确合作协议是否仅能在变更审批通过后方可生效 • 《管理条例》颁布前，根据2017年12月1日起实施的《为获得相关药品和医疗器械在我国上市许可，利用我国人类遗传资源开展国际合作临床试验的行政审批流程》 为获得相关药品和医疗器械在我国上市许可，利用我国人类遗传资源开展国际合作临床试验的，可以简化审批流程。而即将生效的《管理条例》则直接取消了这一要求，进一步简化相关手续
	协议签订的要求 开展国际合作科学研究，合作双方应签订合作协议，对成果的使用权、转让权和利益分享办法作出明确、具体的约定	第二十五条	与《暂行办法》基本一致
	中方参与要求 利用我国人类遗传资源开展国际合作科学研究，应当保证中方全过程、实质性地参与研究，研究过程中的所有记录以及数据信息等完全向中方单位开放并向中方单位提供备份。	第二十四条	在《暂行办法》的基础上更加明确地提出了保护中方单位利益的要求
	成果分配 如就产生的成果申请专利，应由合作双方共同提出申请，专利权归合作方双共有。其他科技成果的权益分享办法由合作协议约定：协议没有约定的，合作双方都有权使用，但向第三方转让须经双方同意，所获利益按双方贡献大小分享。	第二十四条	与《暂行办法》基本一致
	报告义务 合作双方应当在国际合作活动结束后6个月内共同向国务院科学技术行政部门提交合作研究情况报告	第二十六条	在《暂行办法》的基础上新增提交合作研究情况报告的义务
对外提供	**人类遗传资源材料的对外提供** 确需将我国人类遗传资源材料以运送、邮寄、携带等方式出境的，应当符合规定条件，并取得国务院科学技术行政部门出具的人类遗传资源材料出境证明，这些条件包括：（一）对我国公众健康、国家安全和社会公共利益没有危害；（二）具有法人资格；（三）有明确的境外合作方和合理的出境用途；（四）人类遗传资源材料采集合法或者来自合法的保藏单位；（五）通过伦理审查。	第二十七条	与《服务指南》中规定的条件基本一致
	人类遗传资源信息的对外提供 将人类遗传资源信息向外国组织、个人及其设立或者实际控制的机构提供或者开放使用的，应当向国务院科学技术行政部门备案并提交信息备份，如果可能影响我国公众健康、国家安全和社会公共利益的，还应当通过国务院科学技术行政部门组织的安全审查。	第二十八条	《暂行办法》本身对于人类遗传资源的定义以及涵盖的范围相对模糊，导致在实践中对此的理解存在一定误区，认为只要样本不出境，就不需要进行审批，或认为只有人类遗传资源实体样本需要申报，其产生的相关信息不需要申报。 按照《问题解答》。上述理解均属误解，人类遗传资源材料（样本）所产生的信息同样受到保护。《管理条例》则明确指出人类遗传资源包括人类遗传资源材料和人类遗传资源信息两类，并对这两类人类遗传资源的保护分别进行了规定。

（三）政策风向利好

《管理条例》相较《暂行办法》的另一显著区别是，其中含有较多的国家政策性表述，体现出国家对于人类遗传资源采集、保藏、利用、对外提供等方面既积极促进开发、又谨慎保护、保护和开发利用并重的态度。根据《管理条例》第六条、第十三条、第十六条至第十九条、第二十九条可以看出，国家支持合理利用人类遗传资源开展科研活动，促进生物科技和产业创新、协调发展。

与此同时，根据《管理条例》第一条、第八条、第二十七条、第二十八条也可以看出，目前国家对于遗传资源利用坚持的原则更倾向于维护公众健康、国家安全和社会公共利益，而不仅仅是1998年的“加强人类基因的研究与开发，促进平等互利的国际合作和交流”。这也与前文提到的保护人类遗传资源的举措相呼应，例如重要遗传家系和特定地区人类遗传资源实行申报登记制度、外方需与中方合作利用遗传资源、将人类遗传资源信息对外提供或开放使用的备案与安全审查要求等。

（四）法律责任完善

与《暂行办法》中的政策风向一脉相承的是其中规定的罚则，侧重于对境外机构以及境内的外方机构获得遗传资源的监管，仅对三种情形规定了罚则，即（1）我国单位和个人未经批准私自出口、出境人类遗传资源材料或者向外方机构或者个人提供人类遗传资源材料的；（2）国（境）外单位和个人未经批准私自采集、收集、买卖人类遗传资源材料或私自出口、出境人类遗传资源材料的；以及（3）管理部门工作人员因玩忽职守、徇私舞弊造成技术秘密泄漏或人类遗传资源流失的。

而《管理条例》则以较大篇幅增加了罚则方面的规定，具体而言，增加了需承担法律责任的情形、具化了各项法律责任的形态。目前《管理条例》规定的法律责任覆盖了境内外单位与个人未经批准采集、保藏、利用、对外提供人类遗传资源或未经备案的情形，采取欺骗手段获得行政许可的情形，采集、保藏、利用、对外提供遗传资源不符合要求的情形，买卖遗传资源的情形等均规定了单位与个人的责任，为执法部门提供了有力的依据。例如，未经批准采集、保藏、利用、对外提供人类遗传资源的，可能导致国务院科学技术行政部门责令停止违法行为，没收违法采集、保藏的人类遗传资源和违法所得，处50万元以上500万元以下罚款，违法所得在100万元以上的，处违法所得5倍以上10倍以下罚款。

二、《管理条例》的实践关注

（一）处理规则如何落实

作为行政法规，《管理条例》的法律位阶较高，在一定程度上将有利于推动人类遗传资源的安全保护与合规利用，且针对人类遗传资源的采集、保藏、利用和对外提供活动设定了较为明确的要求，但是考虑到此前由《暂行办法》、《服务指南》以及科技部提供的指引所构成的实践工具已具备较为成熟的操作基础，《管理条例》中具体条文中的部分要求如何落实，以及如何与此前的实务操作要求相衔接，可能仍有待立法与执法部门的进一步澄清与明确。

例如，在《问题解答》中，国际合作中的中方单位系指“大陆境内的内资科研机构、高等学校、医疗机构、企业”，而外方单位系指“外国组织及外国组织、个人设立的境内外机构（含港澳台地区组织、企业或个人及设立的机构）”。相较而言，在《管理条例》中，中方单位则指“我国科研机构、高等学校、医疗机构、企业”，而外方单位则指“外国组织及外国组织、个人设立或者实际控制的机构”。一方面，《管理条例》可能需要澄清，其中方单位的概念中是否对相关实体的股本结构存在限制或要求，即是否与《问题解答》所指的范围相一致。另一方面，《管理条例》则拓展了外方单位的范围，以囊括由外国组织、个人实际控制的机构。然而，在实践中，如何界定“实际控制”的标准，主要考察股权比例、议事机构表决权，或是其他因素，将有待进一步澄清。

又如，《管理条例》的第十一条针对需要科技部批准的人类遗传资源采集行为进行了规定。我们注意到，《服务指南》对“重要遗传家系”和“特定地区人类遗传资源”均提供了必要的界定，但是针对“采集国务院科学技术行政部门规定种类、数量的人类遗传资源”的情况，目前并未形成明确的量化标准，以致于难以为企业提供必要的实践指引。又如，《管理条例》第十六条针对保藏基础平台和数据库的开放，以及国家对人类遗传资源的依法使用作出了概括性的规定；然而，“开放”所依据的“国家有关规定”，以及国家使用中所依据的“法”，在实践中具体可能涉及哪些法律法规和规范性文件，亦有待主管部门与行业实践的进一步阐明。

此外，我们还注意到，《管理条例》虽针对中外单位“利用我国人类遗传资源开展国际合作科学研究”的行为拟制了较为具体的规则要求，针对境内单位“采集、保藏、利用、对外提供人类遗传资源”的行为则仅提供原则性的指引，如“不得危害我国公众健康、国家安全和社会公共利益”（第八条），“尊重人类遗传资源提供者的隐私权，取得其事先知情同意，并保护其合法权益”，“遵守国务院科学技术行政部门制定的技术规范”（第九条），以及“禁止买卖人类遗传资源”（第十条）。因此，如“中方单位”需要单独开展人类遗传资源的利用活动，可能需要遵守或参照哪些规定等类似的问题，将是相关企业在实践操作中不可回避，无法绕开的难题。

（二）交叉监管如何应对

作为医疗行业数据的重要组成部分，人类遗传资源（信息）始终面临着医疗行业与网络安全领域（即个人信息与重要数据保护）的交叉监管。此处所述的“交叉监管”，系指由于受监管主

体的重叠，使得不同领域的多重规则对同一数据均施加监管要求。通常，相关规则的切入角度与关注点存在差异，以致该等数据应对监管的合规难度较大。实践中，交叉监管在医疗、金融和交通等敏感行业体现得较为显著，行业规范与网络安全领域规则的双重规制使得一种数据将会在境内面临多重监管要求。

例如，从主体属性来看，境内公立医院X既构成“医疗机构”，也构成“网络运营者”，还构成“健康医疗大数据安全和应用管理的责任单位”，因而X在为病患提供医疗服务过程中所采集的医学影像资料将可能在法律上构成多种性质的数据，比如：

- 《网络安全法》下的“个人信息”（和《个人信息安全规范》下的“个人（敏感）信息”）；
- 《数据出境安全评估指南（征求意见稿）》下“A.18人口健康”领域的“重要数据”；
- 《医疗机构病历管理条例》下的“病历（资料）”；
- 《人口健康信息管理办法（试行）》下的“人口健康信息”；
- 《国家健康医疗大数据标准、安全和服务管理办法（试行）》下的《健康医疗大数据》。

相应地，上述法律法规中的监管要求，均将适用于境内公立医院X处理该等医学影像资料的活动；如企业Y拟与医院X开展医学影像资料的合作，将可能在事实上也面临相关的交叉监管要求。

相类似地，作为“利用人类遗传资源材料产生的数据”，人类遗传资源信息也很有可能进一步构成“个人（敏感）信息”、“人口健康信息”、“健康医疗大数据”，以致同样面临医疗行业与网络安全领域的交叉监管。例如：

- 《网络安全法》针对个人信息的收集和使用设定了基本的原则与规则；[4]
- 《人口健康信息管理办法（试行）》和《健康医疗大数据管理办法》则针对医疗机构向第三方提供相关数据拟制了授权利用的制度设置（主要限于提高医学研究、科学决策和便民服务水平的目的），但并未提供进一步的规则指引；[5]
- 如上所述，《管理条例》针对中方单位“采集、保藏、利用、对外提供人类遗传资源”的行为则主要提供原则性的指引。

在这种情况下，如企业拟与一医疗机构开展人类遗传资源信息的合作项目，则可能需要考虑应对医疗机构在事实层面“传递”至合作伙伴的合规要求，例如授权机制的设置，与安全技术和管理措施的落实。

又如，在跨境传输方面，根据《网络安全法》（及其配套措施）、《健康医疗大数据管理办法》的相关规定，网络运营者与责任单位可以在按照相关法律法规及有关要求进行安全评估（和审批/备案义务）后向境外传输，但是《人口健康信息管理办法（试行）》中的相关规定则实质性地限制了相关数据的跨境传输。具体而言，《人口健康信息管理办法（试行）》第十条明确规定，“不得将人口健康信息在境外的服务器中存储，不得托管、租赁在境外的服务器”。因此，如企业拟将人类遗传资源信息跨境传输至境外服务器，则很有可能违反此处的禁止性规定。

三、企业合规启示

考虑到我国是多民族的人口大国，具有独特的人类遗传资源优势，因而为发展人类遗传资源开发、生命科学和相关产业提供了得天独厚的条件。纵使如此，合规才能创造价值，面对人类遗传资源监管领域崭新的行政法规，如何有效应对新规对商业模式的潜在影响，并在规则中寻找可落地的商业解决方案，将是企业不可回避的核心问题。

• 关注既存商业模式，避免产生直接冲突

如前所述，除了增加若干合规控制项外，《管理条例》更多是在《暂行办法》的基础上，进一步细化“采集、保藏、利用、对外提供人类遗传资源”等相关活动的规范，为企业提供更多的合规实践指引。相应地，企业应当首先关注既存的商业模式，根据《管理条例》的具体要求，确定当前的经营方式是否与相关要求存在直接、明确的冲突，并识别可能存在的合规差距，为后续的合规工作奠定必要的事实基础。

• 梳理交叉监管要求，建立全面合规体系

考虑到交叉监管的存在，企业应识别其在不同监管领域的法律身份，关注经营行为中所涉及的“人类遗传资源（材料和信息）”在可适用法律法规中的法律属性，并谨慎梳理相关规范中的监管要求。尤其在大数据分析、交互提供、跨境传输构成日渐常见的数据商业化环节的时代，企业更应重视判别交叉监管规则的兼容性，筛选符合监管要求和商业目的的方案，并视具体情况采取数据脱敏、省略非必要字段、处理统计级数据等方式，缓解交叉监管带来的合规压力。

• 密切关注实践指引，积极应对备案报批

虽然《管理条例》已正式出台并将于2019年7月正式生效，若干条款在实践中如何落实可能仍依赖于《服务指南》以及主管部门的进一步澄清。因此，如企业在经营活动中涉及“采集、保藏、利用、对外提供人类遗传资源”的活动，应当密切关注立法与执法部门的具体操作，在实践中识别和总结有关部门的工作思路，并结合自身实际，筹备根据《管理条例》实施后需要进行的备案、报批或报告等工作，以积极的姿态应对相关的合规要求。

[4] 主要参见《网络安全法》第四十条至第四十四条。

[5] 参见《人口健康信息管理办法（试行）》第十四条，以及《健康医疗大数据管理办法》第二十二条。

（本文发布于2019年06月13日。）

春风先发苑中梅——《国家健康医疗大数据标准、安全和服务管理办法（试行）》解读及启示

互联网时代，大数据已成为耳熟能详的时髦词汇。大数据分析和应用技术的蓬勃发展，逐渐赋予数据实际的“生产力”。在此背景下，国家卫生健康委员会（下称“卫健委”）于2018年7月12日正式下发《国家健康医疗大数据标准、安全和服务管理办法（试行）》（下称“《管理办法》”），并于2018年9月13日向社会公布。《管理办法》重申了此前政策性文件中的有关要求，从标准制定、主体行为、行业监管等层面对规范健康医疗行业大数据的应用与管理设定了更为具体的规则，对于健康医疗行业从事大数据开发与应用具有实践指导意义。

一、《管理办法》的制定背景与内容提要

• 制定背景

国务院于2015年颁布的《促进大数据发展行动纲要》已充分意识到大数据的应用价值，为全面推进我国大数据发展和应用设定了目标。其中，医疗健康管理和服务大数据应用体系作为公共服务大数据工程建设的一部分被提上日程。

此后，针对医疗健康行业，国务院先后又颁布了《国务院办公厅关于促进和规范健康医疗大数据应用发展的指导意见》、《国务院办公厅关于促进“互联网+医疗健康”发展的意见》等政策性文件，为稳步实现健康医疗大数据应用、医疗健康信息数据共享等提出了更具有针对性的要求；而《网络安全法》及其相关配套措施的颁布和实施也为医疗行业在互联网运行安全和信息安全角度提供了一般性的法律指引。

因此，为了进一步规范医疗行业数据的管理，并推动“互联网+”与大数据技术在医疗行业的应用，《管理办法》应运而生。

• 何为健康医疗大数据?

《管理办法》首先对健康医疗大数据的来源、内涵和外延进行了明确。《管理办法》第四条规定，健康医疗大数据，是指在人们疾病防治、健康管理等过程中产生的与健康医疗相关的数据。而，《管理办法》第二条则对上述数据的来源进行了进一步说明，主要涵盖我国公民在中华人民共和国境内所产生的健康和医疗数据。

• 哪些是健康医疗大数据应用与管理的监管机关?

《管理办法》第五条规定了办法的适用范围。根据该条，县级以上卫生健康行政部门（含中医药主管部门，下同）、各级各类医疗卫生机构、相关单位及个人所涉及的健康医疗大数据的管理均适用《管理办法》。

此外，《管理办法》第六条第一款明确国家卫建委（含国家中医药管理局）以及县级以上各级卫生健康行政部门负责相应行政区域的健康医疗大数据管理工作。

• 哪些机构可能受到《管理办法》的约束?

除上述第五条提及各级各类医疗卫生机构、相关单位及个人所涉及的健康医疗大数据的管理均适用《管理办法》外，该办法第六条第二款更是进一步明确，各级各类医疗卫生机构和相关企事业单位是健康医疗大数据安全和应用管理的责任单位。

可以看出，《管理办法》对责任主体采取了相对宽泛的定义。除各级各类医疗卫生机构外，涉及健康医疗大数据安全和应用管理的“相关企事业单位”也被纳入责任主体范畴，需要根据《管理办法》的要求落实相关义务。

•《管理办法》对主管机关和责任单位提出了哪些要求?

从法规文本结构来看，《管理办法》从标准管理、安全管理和服务管理三个方面对健康医疗大数据应用过程中各相关单位的责权利予以明确。

其中，标准管理涉及各级卫生健康管理部门针对健康医疗大数据行业的标准体系建设中的角色定位；安全管理和服务管理则主要涉及责任单位在健康医疗大数据应用各个环节中的安全管理、操作规程和技术规范，以及提供健康医疗大数据服务过程中的管理制度、服务规程、数据安全等。

此外，《管理办法》还通过专门章节强调了卫生健康行政部门加强监督管理、监测评估的职责，并要求建立健康医疗大数据安全管理工作责任追究制度。具体见下表：

标准管理	
基本原则	- 政策引领、强化监督、分类指导、分级管理
各级卫生健康行政部门职责	- 国家卫建委：统筹规划、组织制定全国健康医疗大数据标准并监督指导标准应用；加强健康医疗大数据技术产品和服务模式的标准体系及制度建设，组织对标准应用效果评估工作等； - 各省级卫生健康行政部门：监督指导评估标准的本地应用，指导和监督标准体系在本省域内落地执行等。
多方参与协作机制	- 择优确定健康医疗大数据标准起草单位和负责人，由各相关单位组成协作组参与标准起草工作； - 鼓励医疗卫生机构、科研教育单位、相关企业或行业协会、社会团体等参与健康医疗大数据标准制定工作； - 发挥各市场主体的积极主动性，建立激励和促进标准应用实施的长效管理机制。

安全管理	
安全管理总体内容	- 数据采集、存储、挖掘、应用、运营、传输等多个环节中的安全和管理，包括国家战略安全、群众生命安全、个人信息安全的权责管理工作
安全管理总体内容	- 建立健全相关安全管理制度、操作规程和技术规范，落实“一把手”责任制； - 依照国家有关保密规定对涉及国家秘密的健康医疗大数据的安全、管理和使用进行严格管理； - 采取数据分类、重要数据备份、加密认证等措施保障健康医疗大数据安全； - 按照国家网络安全等级保护制度要求，加强健康医疗大数据相关系统安全保障体系建设，提升关键信息基础设施和重要信息系统的安全防护能力； - 相关系统的产品和服务提供者应当遵守国家有关网络安全审查制度； - 严格规范不同等级用户的数据接入和使用权限，建立严格的电子实名认证和数据访问控制； - 建立健全健康医疗大数据安全管理人才培养机制； - 建立健康医疗大数据安全监测和预警系统，建立网络安全通报和应急处置联动机制。

服务管理	
总体要求	- 遵循医学伦理原则，保护个人隐私
责任单位主体责任	- 按照国家授权实行“统一分级授权、分类应用管理、权责一致”的管理制度，并建设相应的健康医疗大数据信息系统作为技术和管理支撑； - 确保采集健康医疗大数据行为合乎标准、程序和规范，严格实行信息符合终审程序，并做好数据质量管理； - 具备符合要求的数据存储、容灾备份和安全管理条件； - 健康医疗大数据应当存储在境内安全可信的服务器上，因业务需要确需向境外提供的，应当按照相关法律法规及有关要求进行安全评估审核； - 选择健康医疗大数据服务提供商应确保其符合国家和行业规定及要求； - 责任单位委托有关机构存储、运营健康医疗大数据，委托单位与受托单位共同承担健康医疗大数据的管理和安全责任； - 责任单位发生变更时，应当将所管理的健康医疗大数据完整、安全地移交给承接延续其职能的机构或本行政区域内的卫生健康行政部门； - 责任单位向社会公开健康医疗大数据时，应当遵循国家有关规定，不得泄露国家秘密、商业秘密和个人隐私，不得侵害国家利益、社会公共利益和公民、法人及其他组织的合法权益； - 创造条件规范使用健康医疗大数据，推动部分健康医疗大数据在线查询。
主管单位要求	- 建立健康医疗大数据开放共享的工作机制，加强健康医疗大数据的共享和交换，统筹建设健康医疗大数据上报系统平台、信息资源目录体系和共享交换体系。

二、《管理办法》对企业的指引与启示

总体而言，《管理办法》对于作为责任主体的“各级各类医疗卫生机构和相关企事业单位”在推动健康医疗大数据应用方面的制度设计、安全规程、服务规范等均作出了较为具体的指导性要求。然而，我们也注意到《管理办法》对客体对象与主体范围规定相对宽泛，广大从事健康医疗大数据的企事业单位需要从数据类型以及主体认定等多个角度确定自身的责任和义务范围。

一方面，如前所述，《管理办法》将“健康医疗大数据”定义为“人们疾病防治、健康管理等过程中产生的与健康医疗相关的数据”。由于“大数据”本身包括“大量”（Volume）、“高速”（Velocity）、“多样”（Variety）、“低价值密度”（Value）和“真实性”（Veracity）等内涵，健康医疗大数据的范围已经超出现行法律法规中已经出现、现实中较为典型的医疗行业相关数据（如（电子）病历、人类遗传资源、人口健康信息等），还应包括在这些过程中产生的、与健康医疗相关的数据，例如为判断特定个人健康状况所依据的背景信息（如生活作息数据等）。然而，由于《管理办法》并未对健康医疗大数据作任何举例说明，也未能对何种数据构成“与健康医疗相关的数据”进行具体澄清与说明，同时考虑到大数据关联分析技术中通常对于“相关性”有着相对广泛的判断，因此依据《管理办法》的基本原则，实践中企业判断自身处理的数据是否构成健康医疗大数据可能存在难度。

另一方面，《管理办法》将各级各类医疗卫生机构和相关企事业单位作为健康医疗大数据安全和应用管理的责任单位，而对于哪些企事业单位构成此处的“相关”单位，办法并未予以明确。相较而言，医疗行业某些既有法律规范对于行业的其他重要数据的责任单位界定较为清晰，例如《人口健康信息管理办法（试行）》对责任单位的界定则相对明确，仅指“各级各类医疗卫生计生服务机构（含中医药服务机构）”，并明确该等机构“负责人口健康信息的采集、利用、管理、安全和隐私保护”。

从规范健康医疗大数据应用和管理的角度出发，我们无法排除责任单位的范围可能与健康医疗大数据的控制和处理挂钩。具体而言，如有关企业在日常运营过程中能够收集、处理与医疗卫生机构所能接触的健康医疗数据相类似的数据，如专门从事个人医疗健康检查的服务机构或者从事健康医疗行业的研究机构，如果能够获得疾病防治、健康管理等过程中产生的与健康医疗相关的数据，则仍有可能被归类于《管理办法》的责任单位范畴。同时我们也注意到《管理办法》中，也对“健康医疗大数据服务提供商”以及“存储、运营健康医疗大数据”的受托单位的管理和安全义务提出了要求。因此，从事健康医疗大数据行业的企事业单位的首要任务应当厘清自身定位，从而明确相应的责任和义务范围。

作为具体面向健康医疗大数据的第一部法律规范，并不排除相关主管部门会通过制定具体实施细则、国家标准，或是采用“宽进严出”的执法模式，为企业提供进一步的指引。换言之，企业如正在开展或拟开展与健康医疗大数据相关的管理或应用业务，应当密切关注相关的立法与执法动态。

此外我们也注意到，《管理办法》对责任单位提出的各类要求，尤其是安全管理和服务管理中有关数据安全制度、数据共享、跨境等流转规则的设定，与《网络安全法》及其相关配套法律法规和国家标准的规定存在显著的呼应，在一定程度上构成对医疗行业“责任主体”网络安全义务的重申和强调——从这个角度看，《管理办法》将有可能为企业的日常合规提供一定有益的指引。我们理解，在《管理办法》正式出台之前，健康医疗行业机构（或企业，如适用），以及相关数据本身就可能具备多重属性，从而受制于不同的规则体系。具体而言：

规则体系	体系内容
网络安全	**主体范围** - 网络运营者（以《网络安全法》为核心的相关规则体系，如有待正式出台的《网络安全等级保护条例》） - 关键信息基础设施运营者（以《网络安全法》第三章第二节为核心的相关规则体系，如有待正式出台的《关键信息基础设施安全保护条例》）
	客体范围 - 个人（敏感）信息与重要数据（以《网络安全法》第三十七条与第四章为核心的相关规则体系，包括但不限于《个人信息安全规范》，以及有待正式出台的《个人信息和重要数据出境安全评估办法》与《数据出境安全评估指南》等）
健康医疗行业	**主体范围** - 主要为各级各类医疗机构（以《医疗机构管理条例》为核心的行业监管法规，包括但不限于《卫生行业信息安全等级保护工作的指导意见》、《涉及人的生物医学研究伦理审查办法（试行）》、《医疗机构临床实验室管理办法》等）
	客体范围 - 人口健康信息（《人口健康信息管理办法（试行）》） - 病历（《医疗机构病历管理规定》） - 电子病历（《电子病历应用管理规范（试行）》） - 人类遗传资源（《人类遗传资源暂行办法》） - 处方（《处方管理办法》） - 其他

规则体系	体系内容
科学数据	客体范围 - 科学数据（《科学数据管理办法》）

由此可见，即使在《管理办法》尚未出台的时期，健康医疗行业的有关机构在处理相关“数据与信息”过程中，同样也需要承担和履行着相应的合规义务。《管理办法》实际上将此前健康医疗行业从业机构的相关合规义务（尤其是根据《网络安全法》与《人口健康信息管理办法（试行）》）进行类型化梳理，并结合健康医疗大数据行业自身特点，提炼、整合最为核心与关键的义务，从而形成了《管理办法》“安全管理”与“服务管理”两章的主要内容。

例如，《管理办法》中第十七至十九条倾向于强调责任单位的网络安全等级保护义务（如“一把手”责任制、采取技术措施保障数据安全、容灾备份与数据归档、网络安全等级定级与测评等），相关规定在《网络安全法》第二十一条（网络运营者的网络安全保护义务）与第三十四条（关键信息基础设施运营者额外的网络安全保护义务）、《人口健康信息管理办法（试行）》第九条中可寻端倪。又如，《管理办法》中第三十条对健康医疗大数据本地化存储的要求，也可以在《网络安全法》第三十七条、《人口健康信息管理办法（试行）》第十条等条款中发现相当的要求；《管理办法》第十二条关于“责任单位变更”的规定与第二十条关于“健康医疗大数据系统的产品和服务提供者”技术支持与服务的要求，同样可以分别在《人口健康信息管理办法（试行）》第十二条、第十九条处找到可供借鉴与参考的原型。

基于以上，我们理解，“责任单位”对《管理办法》中相关义务的履行，也一定程度上在事实上满足了《网络安全法》对网络运营者的特定要求，并落实了健康医疗行业对有关机构与企业的部分规定。同时，需要企业关注的是，《管理办法》对健康医疗大数据从业者合规义务的厘清，并不仅是单纯的套用，更是具有行业与产业特点的要求。例如，《管理办法》第二十三条关于“建立电子实名认证和数据访问控制”的规定，则是显著体现了立法者对健康医疗大数据的敏感程度与重要程度的考量，要求落实痕迹管理与访问行为全程留痕。

三、结语

如何合规地进行大数据应用，尤其是商业化应用，是广大企业关心的重点，而大数据时代的规范和合规离不开“安全”与“个人信息保护”两大主题。《管理办法》主要从这两个维度，明确健康医疗大数据标准管理、安全管理、服务管理中的责权利，对统筹标准管理、落实安全责任、规范数据服务管理方面具有重要意义。对于从事健康医疗大数据的企事业单位而言，我们建议依照《管理办法》以及现行医疗行业的其他法律法规开展下列合规工作：

1. 从企业自身定位以及与第三方的法律关系出发，厘清自身在健康医疗大数据流转中的角色，并明确自身的责任和义务；
2. 梳理自身掌握的数据类型，对可能属于健康医疗大数据的数据从来源合法性、存储及使用的安全和合规性等多个方面进行评估；
3. 结合网络运营者以及关键信息基础设施运营者在网络运行安全方面的义务，评估企业对于健康医疗大数据安全性的保障措施，包括但不限于网络产品与服务安全、人员管理、权限控制和制度建设等；
4. 对于健康医疗大数据的应用，首先明确企事业单位对于数据能够主张的权利范围，其次分析用户授权等数据来源合法性因素与使用范围之间的目的及方式差距，最后通过协议及尽职调查等严格把握与第三方的数据交互的安全及合规。

健康医疗大数据是促进人类健康医疗事业必不可少的要素，更是国家重要的基础性战略资源，其他国家比如美国早在十几年前就颁布了如健康保险携带和责任法案（Health Insurance Portability and Accountability Act），增强隐私保护和个人信息安全保护。健康医疗大数据行业也是我国众多行业中针对行业标准、安全与服务制定管理办法的先行者，健康医疗大数据将是大数据规范管理的“苑中梅”，其他行业的大数据规范管理办法也将“樱杏桃梨次第开”。

健康医疗行业仅仅是众多与前沿技术（如大数据、云计算、物联网、人工智能、区块链等）结合的重要行业之一。随着前沿技术与商业实践的结合愈加紧密，可以预见的是，更多行业的大数据管理办法将有针对性地出台，以更好地协调技术与商业的发展关系，务求在个人信息与隐私安全得到充分保护的前提下，相关产业能在技术力量的推动下得到长足发展。因此，企业既要寻找法律要求与商业需求的平衡点，充分发挥数据与技术所带来的竞争优势；在核心商业模式下未有定论的领域，应注重对理论研究的同步跟进，积极寻找推动和塑造法律规则体系的方式与路径，争取利益分配规则的红利；同时，还应密切关注立法态势和执法动向，及时调整自身可能处于灰色地带的业务实践，时刻更新商业模式，在完备的合规中创造更大的价值。

（本文发布于2018年09月18日。）

“数”年快乐
——万字长文说“数据融合”

引言

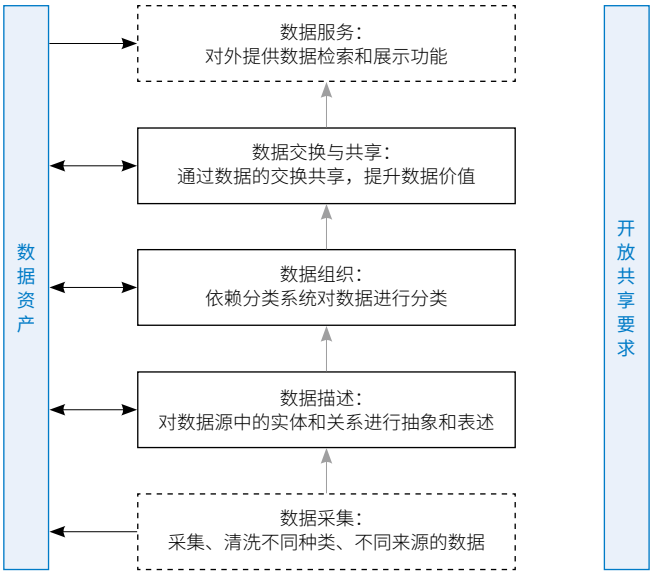
在当前数据价值被广泛认知并逐渐形成数据资产的前提下，企业无论通过爬虫等自动化收集工具获取公共互联网的公开信息，或是与第三方数据源通过Open API等方式共享数据面临的成本都日益提高。此外，数据本身的不同属性（个人信息、重要数据等）使得数据外部共享受到多执法机关的关注和交叉监管，企业获取外部数据的合规风险也面临着不小的挑战。

因此，随着企业获取外部数据成本和风险的增加，企业对于自有数据的深度挖掘显得尤为重要，企业内部“数据共享”、“数据打通”甚至“数据融合”已经成为企业数字化转型或者发挥数据资产价值最大化的重要工作。然而值得注意的是，上述工作并不仅仅是通常理解的建立数据中台，完成技术上数据无条件共享和互惠，而应当是在符合法律法规及行业监管要求的前提下，从数据融合的商业逻辑和数据合规等多个角度构建的大工程。

本文将从数据融合的定义、涉及的常见法律问题和合规建议三方面，详细地和大家探讨数据融合的路径和合规要点。

一、数据融合的定义

尽管数据融合已经成为企业数据化战略中的常见表述，但对其具体的内涵目前尚未有统一的定义。不同的研究、讨论中对相关概念的内涵和外延解释并不相同。有研究认为，数据融合是通过表达手段和工具将不同来源的数据进行整合，以获得更高质量信息的一种形式化框架（data fusion is a formal framework in which are expressed means and tools for the alliance of data originating from different sources. It aims at obtaining information of greater quality）。[1]GB/T 36625.1-2018《智慧城市 数据融合 第一部分：概念模型》指出在智慧城市的场景下，会“通过采集与汇聚不同种类、不同来源数据，依次通过数据描述、数据组织和数据交换共享三个过程实现数据融合的功能，最终通过数据服务对外提供数据检索和展示等功能”，也就是说数据融合概念模型包含了（1）数据采集、（2）数据描述、（3）数据组织、（4）数据交换与共享和（5）数据服务共五个部分及（1）数据资产和（2）开放共享两个支撑要素。



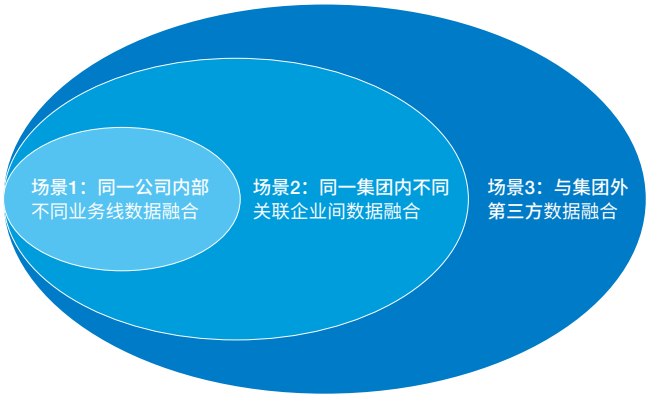
[1] Wald, L., 1998. Data fusion: a conceptual approach for an efficient exploitation of remote sensing images. In: Proceedings of the 2nd conference "Fusion of Earth data: merging point measurements, raster maps and remotely sensed images", published by SEE/URISCA, Nice, France, pp. 17-23.

从数据融合的实践来看，既有以政府公共数据为基础的数据融合如智慧城市、也有企业作为私主体开展数据融合、挖掘数据价值如数据中台。就基于公权力机关主导的如智慧城市、金融全行业的数据融合我们未来会专门撰文探讨和分享，以下是企业开展数据融合较为典型的场景：

场景1示例：电商平台A公司，除传统的电子商务平台服务以外，同时会通过平台向用户提供小额借贷服务。为了提供更精准的服务，A公司希望可以打通两条产品线的数据库，根据用户的消费能力和消费习惯调整贷款额度、贷款利息。

场景2示例：B集团内的众多子公司分别从事银行、保险、证券、信托以及其他实业业务。基于用户申请贷款前的金融风控目的，B集团将下属众多子公司收集的多类数据相结合用于资信调查、反欺诈等多个目的。

场景3示例：C和D公司经营各自的在线视频网站，为提升网站个性化推荐的准确性和广告效益，与X公司竞争，两家公司决定共享用户数据形成更为精准的用户画像。



本文将重点分析上述场景1和场景2情况下企业内部数据融合的场景以及可能涉及的法律问题，[2]包括但不限于：

1. • 数据融合的范围确定，如数据融合的行业主体限制要求
2. • 数据融合的目的和模式架构选择，如在公司内部搭建数据中台或新设子公司承接各业务条线汇总数据和分析
3. • 个人信息的多主体、多目的共享法律基础，如个人信息融合的必要性问题、个人信息融合的用户授权同意
4. • 数据融合可能涉及的其他问题，如数据资产转移的限制

二、数据融合涉及的常见法律问题

（一）数据融合的范围确定：数据融合的行业主体限制要求

作为数据融合的第一步，企业需要考虑将多大范围的数据进行融合。在划定范围时需要重点考虑的问题包括行业监管规定对于共享数据的目的和数据类型的限制。

以金融行业为例，从保障客户金融数据的安全和保密性角度出发，人民银行和证监会等行业监管机构对于金融机构对外共享业务数据此前都有限制性要求。例如，《人民银行关于银行业金融机构做好个人金融信息保护工作的通知》[银发（2011）17号]（以下简称《人民银行第17号文》）要求：“银行业金融机构不得向本金融机构以外的其他机构和个人提供个人金融信息，但为个人办理相关业务所必需并经个人书面授权或同意的，以及法律法规和中国人民银行另有规定的除外”。 可以看出，提供给银行业金融机构的数据对外共享和融合的目的，仅限于个人办理相关业务所必需并经个人书面授权或同意的，以及法律法规和中国人民银行另有规定。类似的限制也出现在金融领域的其他行业监管要求中。[3]

除了行业限制，对于与国家安全、社会公共利益密切相关或数据一旦泄露可能对数据主体产生重大影响的重要数据而言，我国通常会颁布相关法律法规限制或禁止数据的采集机构对外（包括集团内其他关联企业）提供相关信息，如人类遗传信息、病例等。[4]

因此，企业在进行数据融合之前应当对拟用于数据融合的数据范围进行审查，确保不会包含上述法律禁止对外共享的数据和用途，从而可能导致汇总数据行为本身以及经过综合分析后得出的结果（如用户画像）皆存在数据来源方面的合规风险。

[2] 考虑到相比于公司内部或与关联企业间的数据共享，与集团外第三方共享数据在安全保护和使用用途等方面更加难以管控，因此可能需要采取更为严格的事先数据安全影响评估以及对第三方提出有关共享数据安全保护和使用限制的严格义务要求。

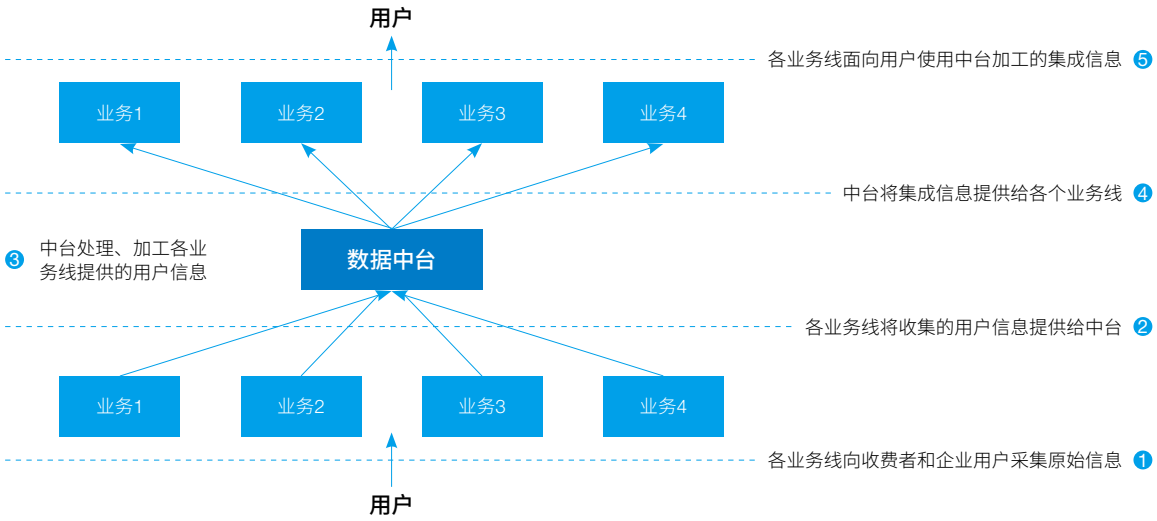
[3]《证券基金经营机构信息技术管理办法》第三十四条规定，除法律法规和中国证监会另有规定外，证券基金经营机构不得允许或者配合其他机构、个人截取、留存客户信息，不得以任何方式向其他机构、个人提供客户信息。

[4] 依据《人类遗传资源管理暂行办法》第四条，国家对重要遗传家系和特定地区遗传资源实行申报登记制度，发现和持有重要遗传家系和特定地区遗传资源的单位或个人，应及时向有关部门报告。未经许可，任何单位和个人不得擅自采集、收集、买卖、出口、出境或以其他形式对外提供；依据《医疗机构病历管理规定（2013版）》第十五条，为患者提供诊疗服务的医务人员，以及经卫生计生行政部门、中医药管理部门或者医疗机构授权的负责病案管理、医疗管理的部门或者人员外，其他任何机构和个人不得擅自查阅患者病历。

（二）数据融合的目的和模式架构选择

根据不同的数据融合目的，企业可以选择不同的模式架构，而不同模式面临的法律风险和现实困难不尽相同。篇幅关系，以下仅探讨典型的C-P以及C-C模式，更为复杂的比如C-P+C等模式的风险会另行探讨：

1. 通过公司内部搭建数据中台承接汇总数据和分析



以银行业为例，在大数据技术应用等背景下，数据共享成为了最受关注的问题。例如，为满足客户风控目的的需要，银行通常会通过自建数据中台汇总行内各业务条线的客户信息，以形成客户金融风控的画像并确定行内对该客户的统一授信额度或金融评分。

第一、角色认定（C-P模式）

在公司内部搭建数据中台承接汇总数据和分析场景下，各业务条线的运营部门因为有权决定其客户信息被委托处理的目的和方式，可能被认定为数据的控制者。数据中台的运维部门可能被认定为各业务条线运营主体的数据处理者，代表各业务条线处理数据并将产生的数据处理结果反馈给各业务条线使用。

第二、数据汇总分析的目的限制

数据中台作为数据的处理者本身不能基于自身的目的收集和使用数据，而是需要严格按照各业务条线的要求处理数据包括个人信息。因此，除非获得用户的授权同意，在某条业务线委托数据中台汇总数据的目的实现或关系解除时，数据中台不得再保存来自该业务条线的数据，尤其是个人信息和基于个人信息形成的数据汇总分析结果（如风控评分数据）。在其他业务条线发起类似请求时，数据中台可能需要重新进行数据的汇总和分析。

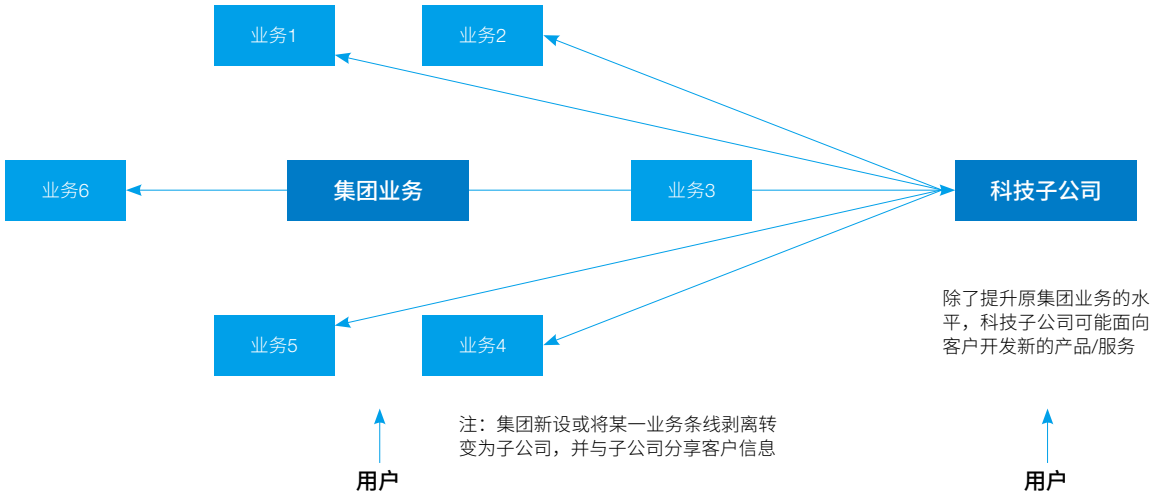
第三、数据融合的安全保障和合规限制

在各业务条线获得用户授权汇总风控数据之前，理论上，数据中台需对各业务条线数据进行物理或逻辑的分区存储、互不混淆，各业务条线不能够直接接触或获得其它业务条线的任何数据，此外，数据中台由于承接了来自各业务条线的数据，其自身的安全性及技术标准需要达到各条线自身合规所应该达到的最高标准，以及从事该等业务所应当遵从和符合的相关法律规定、技术标准和要求。

除了系统建设的要求，各业务条线可能还需要与数据中台签署数据处理的委托协议，明确数据中台作为数据处理者的责任和义务。[5]

[5] 依据《信息安全技术 个人信息安全规范》第8.1条的要求，个人信息控制者委托处理个人信息时，应要求受委托者：1）严格按照个人信息控制者的要求处理个人信息。如受委托者因特殊原因未按照个人信息控制者的要求处理个人信息，应及时向个人信息控制者反馈；2）如受委托者确需再次委托时，应事先征得个人信息控制者的授权；3）协助个人信息控制者响应个人信息主体提出的请求；4）如受委托者在处理个人信息过程中无法提供足够的安全保护水平或发生了安全事件，应及时向个人信息控制者反馈；5）在委托关系解除时不再保存个人信息。

2. 通过在集团外新设子公司承接汇总数据和分析（C-C模式）



与集团内搭建数据中台进行数据委托处理的模式不同，企业也可以通过设立集团外科技子公司作为汇总数据的承接主体实现数据融合。在金融混业经营等背景下，我国银行或金融控股公司相继成立了各自的金融科技子公司。相对于数据中台而言，科技子公司具备了更为独立的数据研发能力和数据使用目的，其通过专业化的研发模式快速推进科研创新，服务于公司业务的同时还可以自行开发新的数据产品、开拓新的业务。从央行发布的《金融控股公司监督管理试行办法（征求意见稿）》可以看出，监管部门对于金融控股公司与其所控股机构之间的客户信息共享在满足一定条件的前提下也持鼓励态度。[6]

第一、角色认定（C-C模式）

除了接受集团各业务条线的委托处理客户信息以外，科技子公司可能还会以自己的名义对外提供数据融合以后的产品。[7]因此，科技子公司作为集团外的第三方可能被定为共享客户信息的数据控制者。相对于C-P模式而言，C-C模式下使得将融合数据用于新的用途成为可能。

第二、重新建立个人信息用于原有业务以外其他用途的法律基础

依据我国《网络安全法》（以下简称“《网安法》”）的要求，网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则。对于各业务条线业务办理以外的数据处理目的，科技子公司需要额外设计商业模式满足个人信息处理的必要性原则要求。以科技子公司提供集团内部统一会员服务为例，其可能需要与集团一同设计各业务条线数据融合的积分计划和权益互换机制，从而建立数据融合和新的业务服务之间的必要性（详见以下个人信息融合的必要性分析）。此外，就个人信息使用的合法性而言，企业如何确保在数据融合互通的新业务场景下获得个人信息主体对数据在整体系统中进行处理的有效授权，是数据融合互通合规问题的重中之重（详见以下个人信息融合的用户授权同意分析）。

第三、数据融合的安全保障和合规限制

集团与科技子公司之间可能需要梳理数据交互的类型、目的并通过合同等形式，共同确定各自应满足的个人信息安全要求，以及在个人信息安全方面，集团母公司和科技子公司应分别承担的责任和义务，并向个人信息主体明确告知。值得注意的是，集团作为数据共享方而言，可能需要对外承担因共享个人信息对个

[6] 依据央行2019年7月26日发布的《金融控股公司监督管理试行办法（征求意见稿）》第二十二条，金融控股公司与其所控股机构之间、其所控股机构之间可以共享客户信息、销售团队、信息技术系统、运营后台、营业场所等资源，发挥协同效应。金融控股公司可以在集团内部建立金融控股公司与其所控股机构之间、其所控股机构之间的协同机制，对集团各项资源进行合理配置。在开展业务协同时，金融控股司、其所控股机构应当依法以合同等形式明确风险承担主体，防止风险责任不清、交叉传染及利益冲突。此外，第二十三条还规定，金融控股公司及其所控股机构在集团内部共享客户信息时，应当确保依法合规、风险可控并经客户书面授权，防止客户信息被不当使用。金融控股公司所控股机构在提供综合化金融服务时，应当尊重客户知情权和选择权。

[7] 以银行科技子公司为例，其术输出方式主要有软件输出、云平台输出、开放平台输出、咨询服务输出四种模式。参见《重磅！6大银行金融科技子公司，有了这么多大布局！》，搜狐，载http://www.sohu.com/a/313232984_670374，2019年5月9日。

人信息主体合法权益造成损害的相应责任。[8]此外，如果集团涉及将数据资产转移至科技子公司则还可能引发公司法、合同法方面的要求和限制（详见以下数据融合可能涉及的其他问题—数据资产转移的限制分析）。

第四、集团内各业务部门与子公司的权益分配问题

数据融合项目下会涉及多方主体，其中既包括原始数据的来源方，如同一集团内实际开展业务并收集数据的各业务部门或关联公司，还可能包括输出技术能力的科技子公司。通常而言，科技子公司会是数据融合变现利益的直接受益人，但对于提供原始数据的集团内业务部门或各关联公司而言，其提供的数据对于数据融合模式下数据使用效率和数据商业价值的提升，以及由此而产生的成本优化、运营效率提升以及直接的经济利益同样具有不可忽视的贡献。

如果集团内的业务部门和关联企业无法参与数据融合变现的利益分配环节，则缺乏持续参与数据融合项目的动力；甚至，如果各方未能在数据融合项目开展前就变现利益的分配达成一致，部门和关联企业出于维护并充分利用数据资产价值的考量，可能不会参与该项目。因此，数据融合的多主体在数据融合变现情况下的利益分配问题是实现数据融合的一项重要考虑因素。

（三）个人信息的多主体、多目的共享法律基础

在数据融合项目中，尽管会涉及企业信息、统计数据等非个人信息，但数据融合大多出于在挖掘或预测个人的消费习惯等与个体相关度高的目的，因此个人信息的合规共享、挖掘和融合是数据融合项目中不可避免的问题。

1. 个人信息融合的用户授权同意

个人信息主体同意是个人信息处理（包括融合）的重要合法依据，也是个人信息主体行使其他权利的先决条件，例如修改权、删除权等等。依据我国《网安法》第四十一条的要求，“网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意”。尽管我国在法律法规方面尚未就“明示收集、使用信息的目的、方式和范围”的标准予以进一步详细说明，但从目前颁布的国家推荐性标准和监管机构执法角度而言，对用户告知的要求日趋严格。

就数据融合而言，企业可能需要说明跨业务条线个人信息汇总分析的目的、方式和范围，如果是基于业务办理所必需的数据融合，可以在整体隐私政策中予以披露并获得用户的授权同意；如果提供原母公司产品或服务的附加功能（如精准化广告营销）或者基于金融科技子公司自身目的进行数据融合，则需要使用更为显著的方式，以单独文本的形式就数据融合的工作原理、可能涉及的产品、数据融合的范围和拒绝数据融合可能产生的影响等内容另行告知用户。当用户拒绝时，可不提供相应的附加功能或新的产品/服务，但不应以此为理由停止提供原母公司的核心业务功能，并应保障相应的服务质量。[9]

除了隐私政策说明书的内容需要规范，另一方面隐私政策披露的格式本身将极大地影响隐私政策说明书发挥应有的效果。将所有的隐私政策内容都集中到说明书上，看似可以保证消费者了解所有的情况，然而实际上，由于阅读隐私政策说明书需要花费大量的成本，一旦隐私政策冗长晦涩或埋藏过深，将会事实上降低用户的可读性。

在欧盟，以Google案为例，法国数据监管机构CNIL指出Google实施的数据处理数量特别庞大且具侵犯用户权益的可能性较大，相对而言，Google隐私政策中有关数据处理的描述则相对过于简单，不符合GDPR要求的数据处理透明性要求。具体而言，CNIL认为：（1）公司将数据处理目的、数据存储时长或者用于个性化广告目的的数据类型信息分散在多份文件中告知用户，用户需要通过繁杂的多步骤才能完全访问和知晓上述信息；（2）针对可能对用户权益造成极大侵害（如数据泄露）的约20种服务的数据融合和处理而言，Google在隐私政策中的说明过于笼统，用户无法知晓自身个人信息被处理（包括融合打通）的程度，[10]尤其是对于个性化广告营销的数据处理而言，Google未明确说明合法性基础是基于“用户同意”或“合法利益”；（3）Google未明确披露某些数据的保存期限。[11]因此，企业在设计用户告知以实现用户知情权时，需要考虑是否通过简短说明与完整说明相配搭、隐私政策与业务协议相呼应等方式让用户能够更为清晰的理解数据融合涉及其个人信息的收集和使用情况，以及可能对其造成的影响。

2. 个人信息融合的必要性问题

尽管企业已经获得个人信息主体的同意，但并不意味者个人信息融合满足《网安法》第四十一条规定的必要性原则。国家推荐性标准《信息安全技术 个人信息安全规范》（以下简称“《个人信息安全规范》”）中将《网安法》第四十一条规定的数据处理必要性原则进一步解释为：（1）在收集个人信息时需满足直接关联、最低频率和最少数量的要求；（2）个人信息保存应为实现目的所必需的最短时间，超出上述个人信息保存期限后，应

---

[8] 参见《个人信息安全规范》第8.2（e）条。

[9] 参见《个人信息安全规范》第5.5（b）（2）条。

[10] CNIL认为，Google各类文件中关于目的的描述如“在内容和广告方面提供个性化服务、确保产品和服务的安全、提供和开发服务等”，在实施处理范围及其后果方面过于笼统。且数据收集的描述也分散在各文件中，描述也模糊，因此不准确也不完整。

[11] 关于保存期限有一类为“由于特定原因，信息会长时间保存”，这种表述并没有表明任何明确的期限或用于确定该期限的使用标准，该表述违反了GDPR规定必须提供的信息。参见朱玲风：《从数据融合角度分析CNIL处罚谷歌案（DPO社群成员观点）》，载https://mp.weixin.qq.com/s/G3kU1rE72lyP2LwOmO8ulw，2019年3月19日。

对个人信息进行删除或匿名化处理。

首先，就公司内部各业务条线委托数据中台汇总个人信息而言，可能面临数据汇总范围是否为原业务办理所需的直接关联、最低频率和最少数量的挑战。以基于客户风控目的汇总数据为例，诚然数据融合的范围越广越能形成精准的个人信用或金融画像，从而有利于降低金融机构在贷前审批、贷中管理和贷后催收中的风险。但是，在金融机构扩大信息收集范围的同时，其数据合规方面的必要性风险也随之增加，主要体现在：（1）当数据融合的范围达到一定程度后，额外收集并汇总分析用户个人信息不再能实质性发现并降低用户欺诈或违约的风险，因此在这种情况下，数据融合可能会被认定为超出提供产品和服务的目的过量收集个人信息；（2）对用户通讯录或APP输入语料的监测可能侵犯公民通讯自由和通讯秘密，相对于风控目的而言可能被认定为超出了必要的限度。

其次，就科技子公司汇总母公司各业务条线数据用于用户画像和母公司多产品的精准广告营销而言，该个人信息的处理活动并非原母公司各业务条线提供核心业务产品和服务所必需，可能存在违反《网安法》有关收集、使用个人信息必要性的原则要求。对于希望使用数据融合结果用于产品/广告营销的业务条线或子公司而言，可能需要从消费者的视角如设计用户体验计划、增值服务等机制重新建立数据融合与为消费者提供额外服务的必要关联。

（四）数据融合可能涉及的其他问题——数据资产转移的限制

除了以上数据合规的风险，在集团母公司将原有业务和数据转让给子公司的情况下，还可能涉及公司法和合同法下的资产（硬件、软件、数据）转让和人员转移问题。因此，需要至少考虑的问题包括：

1. 签约主体的变更

从法律性质上看，原集团与客户之间构成业务办理的合同关系，子公司如果通过资产收购从集团获得运营相关业务和获取相关数据的权利，会导致原服务相关法律文件（包括但不限于用户协议、隐私政策等）一方主体的变更。根据《合同法》的规定，经当事人协商一致，可以变更合同，且一方可以将其合同中的权利、义务的全部或部分转让给第三人。合同主体的变更涉及合同权利和义务的一并转让，根据《合同法》第88条的规定，合同权利和义务一并转让的，应当经过合同相对方同意。因此，从合同法的视角而言，对于新设子公司承接原集团业务和数据需要获得相关业务办理用户的同意。

2. 决策程序

通常情况下，一个业务板块的剥离（或者收购）以及关联交易可能需要相关主体董事会或者股东会的批准。因此，新设子公司对于原集团业务和数据资产的承接可能需要经过以下程序：集团内部决策程序、签署资产转让协议、资产交付。

3. 估值与定价

对拟转让业务可能需进行资产评估，并参考评估价值确定交易金额，以减小交易风险。

三、企业数据融合的建议

在各行各业普遍考虑对公司内外部数据融合的当下，金融行业更是将数据向第三方开放和共享作为未来推进开放银行发展的前提条件。[12]企业数据融合后的巨大潜力也吸引公司纷纷开展数据中台的搭建工作。但如上所述，即使是更为简单的企业内部数据融合也应当是需要技术部门、法律合规部门与产品部门通力协作，集团内部关联公司达成共识，商业逻辑和合规框架并存的大工程，需要公司领导统一思想、大力支持才能完成。

针对企业数据融合的常见问题，我们进一步建议：

（一）原始数据溯源及合规

对企业而言，数据的采集是数据融合的始点，采集数据质量的高低会直接影响企业开展数据融合的成本和合规风险。“错误数据、异常数据、缺失数据等‘脏数据’产生”[13]，影响数据的完整性和准确性，还可能给全局数据的融合互通造成实质性障碍。因此我们建议企业：

- 以普遍适用的法定义务合规性为评估起点，结合所处行业的监管要求对数据的收集、使用、存储和共享等全生命周期的对存量数据的产生/收集过程和利用方式的合法合规性进行评估。
- 制定并实施统一的数据采集标准和统计口径，以避免在后续数据融合场景中出现对“同一数据源在不同关联公司的表述不同”或“看似相同的数据实际含义大相径庭”[14]的情况，保障数据的一致性，为不同业务线或关联企业间的数据融合和分析奠定良好基础。

（二）数据分级分类

数据分类是《网安法》下网络运营者应当遵守的安全保护义务之一，[15]而从数据融合的角度来看，数据分级分类是评估数据的安全性和合规性的重要方法，也为数据融合项目中应用原始数

[12] 开放银行（Open Banking），根据Gartner的定义，是指在法律和监管保障数据安全性的前提下，银行通过开放客户账户信息系统等方式，向已经授权可信第三方服务商及其他合作伙伴等共享数据、算法、交易、流程和其他业务功能的模式。解决好数据共享带来的问题和挑战，是开放银行能否成功的关键。

[13]《李伟：做好数据治理 更快更好地推进数字化转型》，载http://www.xinhuanet.com/fortune/2019-12/02/c_1125298138.htm，2019年12月2日。

[14] 前引〔13〕。

[15]《网安法》第二十一条第（四）项。

据范围的确定提供了参考：

- 就分类而言，企业应当根据收集数据的主体、收集数据的业务、具体的数据收集场景、收集数据的类别、具体的数据字段逐层对数据进行分类；此外企业在对数据分类的时候，还应当依据普遍适用的法律合规要求和行业特定的监管标准对数据的合规性进行评估，并将是否合规作为数据分类的标签之一在分类结果中进行体现。
- 就分级而论，企业需要在数据分类的基础上结合数据的信息内容、数据的敏感程度、数据的法定和约定保密性等情况，对数据的安全属性进行评级。
- 最终企业需要以数据分级分类结果为依据，在综合考虑数据本身的价值、平衡数据安全性和商业价值的基础上合理划定数据融合的原始数据范围。[16]

（三）数据承接主体的选择

如前所述，企业可以通过多种模式开展数据融合，包括但不限于通过设立数据中台作为大数据资产层、设立独立的科技子公司承接来自各关联企业的数据等方式。就数据中台模式与科技子公司模式的选择而言，企业可能需要考虑以下因素：

- 从数据融合与集团原有业务的关联性而言，数据中台模式由于建立在企业内部，通常会更加强调与业务的协调和匹配企业自身的业务需求，因此如果企业开展数据融合的主要目的是为了企业自身的业务运营服务，数据中台的模式可能更有助于实现数据与业务的融合、并及时贴合业务需求进行相应调整；而相比之下，科技子公司模式下，由于科技子公司与提供数据的关联公司之间是相互独立的实体，二者之间的关系更类似于数据服务提供者和数据服务使用者，因此在与集团内关联企业沟通、了解服务需求方面可能会稍有劣势。
- 从数据价值的商业化利用和技术能力角度来看，数据中台模式主要是作为企业内部的辅助者，为企业自身的数据处理和使用提供技术支持；而科技子公司除了向集团内的关联企业提供数据服务和技术赋能外，更多地是依托于集团内丰富的数据资源，作为独立主体提供数据产品和技术产品，实现数据价值的输出。以金融行业的科技子公司为例，根据零壹智库所发布的《商业银行科技战略案例库》，部分股份制银行已“将金融科技提升到总战略高度”[17]，并将科技子公司作为推进技术成果落地应用的重要窗口。 在这种情况下，对科技子公司的技术能力也相应提出了更高的要求，因此企业在选择数据融合的具体模式时，还需要考虑现有的数据技术能力。
- 除此之外，企业自身所处的行业以及数据监管的强度也是应当纳入模式选择中的考量因素之一。通常而言，如果企业或其关联公司所处的为强监管的行业或者在业务开展过程中涉及较多的敏感数据、保密性数据，则在企业内部建立数据中台开展数据融合的合规性风险可能会低于将数据提供给第三方科技子公司用于数据融合的情形。

（四）商业模式的搭建

从合规角度来看，数据融合的商业模式搭建需要满足必要性原则，即企业需要从消费者的视角建立数据融合与为消费者提供服务的直接关联。

- 建立统一账号或会员机制是实现多业务线数据或关联实体间数据融合必要性的重要路径之一，但并不是唯一的途径。企业应当充分考虑业务的特性，从数据融合后可能为用户带来的增值利益出发研究数据融合的商业逻辑，同时激励用户额外授权同意企业整合并分析其数据。

（五）多主体对于数据融合变现的利益

数据融合各方能够主张各自对数据融合变现的利益主要有两项依据：

其一是原数据持有方（如集团内业务部门或关联公司）作为原始数据的持有人参与了数据融合项目，且其所拥有的原始数据在项目中对于数据融合后商业价值的提升做出了相应的贡献；在这种情况下，汇总数据的承接方（如科技子公司）可能需要结合对各业务部门或关联企业所持有的参与数据融合项目的原始数据进行价值评估，其中价值评估既需要考虑原始数据的绝对价值，也需要考虑其在数据融合项目中可能贡献的相对价值，并以评估结果为基础通过协商最终确定该部分的利益分配。

其二如我们在前文所提示，实现数据融合的商业模式中满足必要原则且用来激励客户授权同意的权益往往是由原数据持有方向客户提供，集团内业务部门或关联企业可能需要付出相应的成本。我们同时建议在约定变现利益的分配时对于该部分有所体现，作为集团内业务部门或关联企业投入成本的反馈或补偿，以维系整个商业模式的良好平稳运转。

总而言之，企业内部数据融合需要在商业逻辑通顺和合法合规的前提下进行。考虑到数据融合后的驱动力，企业不应当“因噎废食”，因为融合工作的复杂性而“望而却步”。但同时企业更不应该对于数据融合的合规风险“熟视无睹”，忽视数据合规可能引发的民事、行政甚至刑事责任。如同合规的数据资源才有可能变成数据资产一样，合规的数据融合才能助力企业发展，让企业在大数据经济浪潮下走的又稳又远。

（本文发布于2020年01月02日。）

[16] 例如，根据我国台湾地区《金融控股公司子公司间共同营销管理办法》第11条的规定，金融控股公司子公司间交互运用客户资料时，如果没有法令的另外规定，或者经客户签订契约或书面明示同意者，所共享使用的数据不得包含客户姓名或地址以外之其他数据。

[17]《8家股份制银行科技战略布局：对内成立金融科技子公司，对外寻求合作》，载https://bank.hexun.com/2019-12-17/199712200.html，2019年12月17日。

平安夜里说平安
——“数据资产”的误区与合规条件

目前似乎各界已经对于数据成为一种独特的“资产”达成了共识。“谁掌握数据，谁就掌握了未来”、“数据就是第一生产力”、“洞悉先于人，数据赢天下”等已经成为市场广为人知的商业口号。数据价值挖掘、数据资产管理随之成为当下最热门的话题，只需“百度一下”，便能收获各类挖掘数据价值、管理数据资产的“良方妙策”。但从法律技术的角度来看，对于数据资产的价值管理，仍有诸多的疑问。

例如

- 在数据权属/权益尚未明确界定的前提下，未确权的数据何以成为“资产”？
- 对于数据的物理控制与数据“资产”之间有多长的距离？
- 数据的质量控制是构成数据“资产”的充分条件吗？
- 合法合规收集的数据其商业化的合规路径有哪些？

我们将通过此文换个思路来探求数据资产的真实面目，确保数据资产合法合规地变现。

一、数据资产的定义与价值内涵

目前已有国家标准明确提供了数据资产的定义：“数据”是指关于客体的知识的可再解释的形式化表示，以适用于通信、解释或处理[1]；“资产”是指对组织有潜在价值或实际价值的物品、事物或实体[2]；“数据资产”是指以数据为载体和表现形式，且能够持续发挥作用并带来经济利益的数字化资源[3]。然而，企业要挖掘数据资产的价值，不能止步于定义，更需要从“资产”的共性和数据的特性两个方面出发，深刻理解数据资产的核心问题。

（一）“资产”的共性——数据的经济价值

首先，“资产”强调资源对企业具有潜在或实际价值，能为企业带来稳定、持续的经济利益。获取数据并不等于获取资产，数据作为资产的价值往往始于积累，即通过数据规模的不断增长赋予数据新的用途。

数据价值往往体现在内部和外部两个方面，数据的内部价值主要通过数据在企业生产运营中的作用体现。例如，对一个人长期的消费记录进行统计分析，可获得其众多的消费特征，如其消费偏好、消费习惯，甚至可以通过其消费的商品类别、消费金额等推断这个人的身份、年龄等；持有这些数据的企业，则可以通过对数据进行统计分析，实现人群属性画像，从而进行自身产品的精准营销、产品设计或提升服务；此时，数据已经开始具备参与企业生产运营过程的能力，具备提升经营效率、优化产品结构、实现营业创收的价值，即数据已具备了成为企业资产的条件。而数据的外部价值更为企业和投资者所关注，除了利用数据统计分析来提供企业运营效率、提升自身产品/服务的质量和转化率，企业还可以利用自身掌握的数据来开拓新的商业模式、打通多个产品线的关联，甚至可以发展出金融风控、基于数据的技术输出、为第三方产品广告营销提供策略等直接变现的模式，让数据变为可“流通”的资产。

但为确保数据转型为能够带来持续经济利益的资产，企业必须早在数据的获取与积累阶段即确保数据的合法合规，明确数据正当使用的范围。例如，在获取个人信息时，企业即应征得个人信息主体的关于收集数据的同意，并获得后续将数据逐步提炼为资产的每个数据处理场景的充分授权。若数据从源头和用途上不合法合规，则无论怎样通过数据积累来赋予其新的用途，得到的成果不仅无法有效地应用于企业的生产运营，成为企业的资产，还可能成为企业的重大合规隐患。

[1]《GB/T 5271.1-2000 信息技术 词汇 第1部分：基本术语》，国家质量技术监督局，2000年发布。

[2]《GB/T 33172-2016 资产管理 综述、原则和术语》，国家质量监督检验检疫总局，2016年发布。

[3]《GB/T 37550-2019电子商务数据资产评价指标体系》，国家市场监督管理总局，2019年发布。

（二）“数据”的特性——“数据资产”的权益边界

其次，相比于传统意义的有形资产，“数据”具备可复制性和易流通性的特点，并且承载着相同信息的数据，可以在物理上被多个主体所复制、持有或控制。这便使得数据资产的权属/权益问题变得扑朔迷离：数据究竟应归数据的源头生产者所有，还是归处理数据的平台所有，还是应被个人信息的主体所有？

现有法律法规还未就数据权属的认定做出定论。在理论研究领域，最高人民法院曾将《大数据时代数据权利保护研究》作为2018年度司法重大研究课题，召集多方专家展开论证探讨，提出建立综合数据权利保护机制，包括立法、司法和行政执法等[4]。但由于数据牵涉多方利益和价值考量，截至目前各界也尚未就数据权属认定，乃至数据权属是否存在等问题达成一致。

然而，企业依然可以在司法实务层面找到一些关键的前提问题的解答：企业究竟对其数据资产享有法律所保护的什么利益？近几年常有企业对他人擅自使用其所持有数据的行为发起的不正当竞争诉讼，在此类案件中法院肯定了企业通过其自身经营活动长期积累的数据信息可以构成重要的竞争优势和商业资源。例如，“新浪诉脉脉”案中，法院认为新浪微博经其用户授权而收集并进行商业利用的数据可以为该企业创造更多的经济效益，是企业重要且受法律保护的商业资源[5]；“淘宝诉安徽美景”案中，法院认为虽然企业对记录网络用户信息的原始网络数据只能依其与用户的约定享有使用权，但淘宝大数据产品的数据内容是经过网络运营者的分析过滤、提炼整合等大量劳动投入和匿名化处理的结果，企业对此享有独立于用户的财产性权益[6]；“谷米诉元光”案中，法院认为经企业收集、加工、分析、编辑、整合的数据具有实用性并能够为权利人带来经济利益，企业对此享有财产性权益，受到《反不正当竞争法》的保护[7]。

不难看出，无论是从数据的经济价值出发，还是从数据资产的权益视角出发，数据资产的形成与价值挖掘均应重视两个的前提问题：（1）重视对数据的分级分类和分析整合，不断提升数据的经济价值；（2）数据在全生命周期的收集、处理均合法合规。同时，在数据权属/权益尚不明朗的情况下，需要利用现行法律法规的工具来搭建固定数据资产的框架，比如软件著作权、数据库权利、商业秘密等。（详见下图）

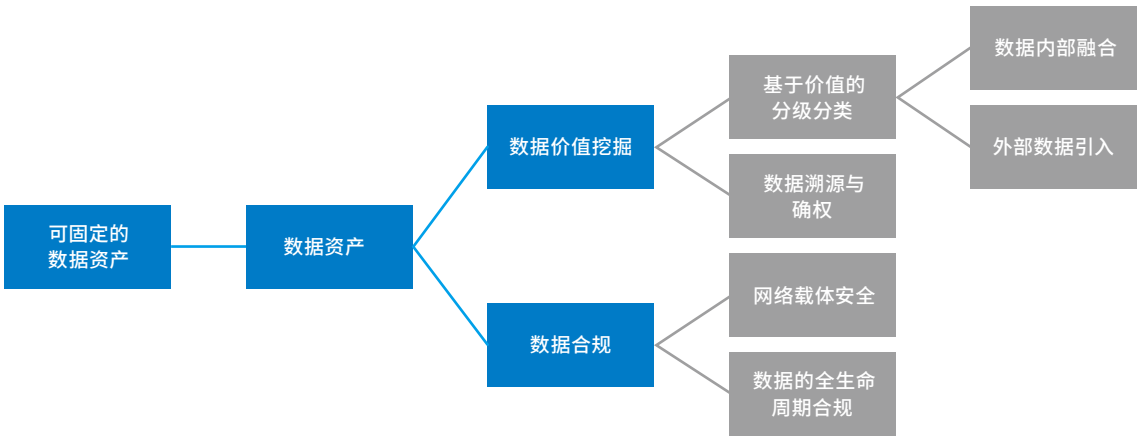


图1 数据成为资产的基本前提

[4] 最高人民法院2018年度司法研究重大课题《大数据时代数据权利保护研究》开题论证会成功举行，https://www.tsinghua.edu.cn/publish/law/3567/2019/20190318135047670983257/20190318135047670983257_.html。

[5] 见北京知识产权法院(2016)京73民终588号民事判决书。

[6] 见杭州市中级人民法院(2018)浙01民终7312号民事判决书。

[7] 见深圳市中级人民法院(2017)粤03民初822号民事判决书。

二、数据资产的实现前提

（一）数据内外部价值的逻辑

行业经常提到的企业“大数据能力”，除要求企业具备收集、获取海量数据的能力外，更须建立在企业能够充分挖掘和探索海量数据“价值”的基础之上——而后者才是构成数据资产的根本前提。通常而言，数据“价值”的挖掘往往要求企业从数据采集阶段做起，依循数据处理的不同环节和流程，建立层层递进的数据挖掘逻辑，自内而外有效实现数据的有效梳理和应用。

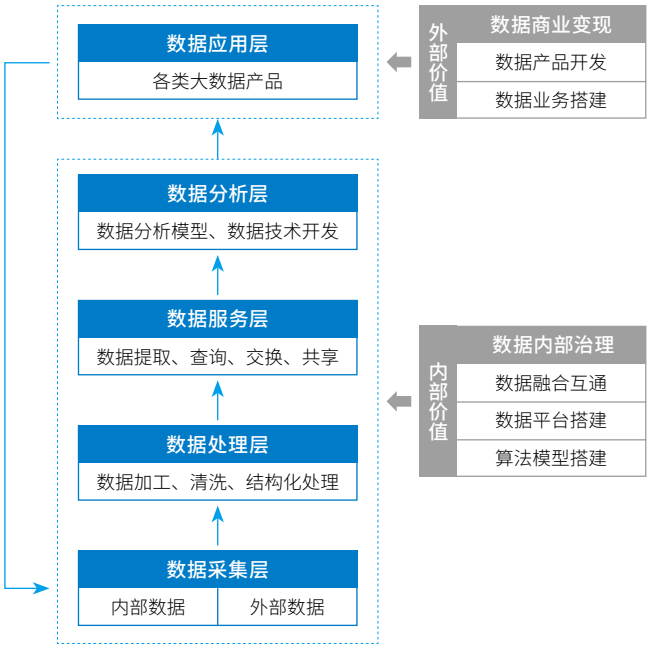


图2 数据的“价值”挖掘[8]

如上图所示，结合数据整体的生命周期，对于数据的“价值”挖掘一般而言主要可以分为内部价值挖掘和外部价值变现。

内部价值挖掘阶段，可分四个步骤：（1）数据采集层：企业通过自身业务、互联网公共渠道或第三方等各方渠道实时获取数据；（2）数据处理层：按照一定规则对数据进行加工、清洗和结构化处理，去除冗余、杂质，严格把控数据质量；（3）数据服务层：构成底层数据库与前端数据技术开发的桥梁，为前端技术开发提供数据提取、查询、交换、共享的通道；以及（4）数据分析层：重点利用所提取的底层数据，进行数据相关技术的开发，如进行算法训练、完善数据分析模型等。在外部价值变现阶段，则需要企业在内部数据及技术开发体系建立的基础上，结合企业的市场定位开发不同类型的产品，服务于不同类型的目标客户，为企业营利创收。而同时，企业对外的产品与业务服务又可同时为企业收集、获取大量的原始数据，反哺企业内部的数据累积，形成由内而外的价值循环。例如，电子商务平台通过收集海量用户的商品浏览记录和交易记录，结合用户提交的性别、年龄等身份信息，通过整合、分析这些信息的关联关系，构建不同消费群体的画像。在帮助平台了解自身消费者构成的基础上，形成数字化的营销产品并向平台上的商家提供精准触达的营销服务，不仅能够帮助商家与平台有效创收，还能进一步带动消费者留下更多的交易记录，以助平台实现消费者数据的不断更新与利用，完成营销产品功能的优化验证。

可以看出，数据外化价值的挖掘能够直接帮助企业实现内部数据的商业变现，为企业带来“货真价实”的营业收入。但不容忽视的是，如果企业在内部的数据挖掘工作上出现“无效率”、“不到位”的情况，例如出现数据处理和流转上的管控断层或者在数据质量把控上不过关，则必然影响到数据的可用性，那么数据外化价值的实现则必然失去生长根基。因此，做好内部数据处理流程的管控，是企业有效掌控数据“资产”的必要前提和必需工作。

（二）数据资产价值的衡量要素与前提

如前所述，无论是对于企业内部的数据价值挖掘，还是对于外部的数据商业变现而言，对企业所持有数据的有效梳理和引用，对数据管理流程进行严格把控，将是实现企业“数据资产”价值最大化的有效方式。而判断企业数据的数据管控工作是否有效，最直接的判断因素则是关注数据自身的质量问题。但需要强调，在数据安全和数据合规呼声日益高涨的当下，仅仅关注数据质量对于企业持续发掘并长期维持数据价值而言远不足够。如因缺乏安全与合规意识导致数据泄露或数据使用违规，不仅不利于数据价值的持续维护，甚至导致企业数据被污染，对企业整体数据资产造成毁灭性打击。

1、基本条件——数据本身的质量

一般而言，数据的价值直接体现为数据的信息含量，信息含量越丰富，则越能从中提炼尽可能多的有指示意义的信息，帮助企业判断数据中隐含的人、事、物及各自之间的关联关系。但是，数据信息含量的指示意义必须建立在数据本身的准确性上，而准确性又与数据的真实性、时效性、完整性紧密关联。对于缺乏准确性的数据，由于无法从中提炼正确的信息，即使信息含量再多也终究徒劳。

[8] 图示参考艾瑞咨询，《艾瑞：大数据产业持续繁荣，数据资产管理需求升级》，http://report.iresearch.cn/content/2017/12/272131.shtml。

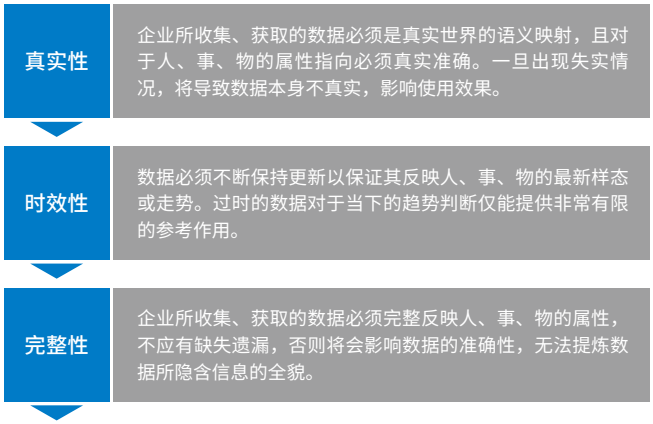


图3 数据准确性的保障要素

2、基本保障——基于数据安全的分级分类

数据价值的实现离不开对于数据本身的安全保障。网络作为数据的普遍载体，其安全性是数据处理安全的重要基础。我国《网络安全法》对于网络运营者在建设、运营网络或者通过网络提供服务的安全要求予以明确，在数据处理上，明确要维护网络数据的完整性、保密性和可用性。此外，《网络安全法》进一步指出网络运营者应采取数据分类、重要数据备份和加密等措施履行其安全保护义务，并对不履行该等安全保护义务的行为设置了相应的罚则。如根据《网络安全法》第五十一条，对拒不改正或导致危害网络安全的网络运营者处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。另外，如企业面对监管部门责令还拒不采取改正措施，导致严重后果的，还可能触犯《刑法》中拒不履行信息网络安全管理义务罪，受到刑事处罚。

从履行网络安全保护义务角度出发，基于安全的数据分类构成网络运营者履行其法定义务的应有之意。而另一方面，企业采取的数据保护措施也将切实为其挖掘、实现数据价值的过程提供有效的安全防线。一旦企业疏于履行该等义务，导致发生数据泄露事件或存在数据安全隐患的，将直接导致企业遭受执法机关的行政乃至刑事调查，承担相应法律责任。皮之不存，毛将焉附，得不到足够安全保障的数据，其价值的挖掘和实现也将大打折扣。此外，对于企业通过分析整合数据来提升其经济价值并将数据转型为数据资产，数据的分级分类起到了基础性的关键作用。

由于企业收集或处理的数据往往种类繁多，且敏感程度不同，不同类型和敏感程度的数据则必然存在安全保障上的不同层次的需求。为此，除对数据进行分类外，还应针对不同类型、不同敏感程度的数据识别各自的安全级别，对不同安全级别的数据实施恰当的安全保护措施。虽然我国在数据的分类分级上尚未形成统一的法律规范要求，但部分国家标准或行业标准（及征求意见稿）提供了数据资产分类分级的详细指引，如金融行业《证券期货业数据分类分级指引》、《信息安全技术 大数据安全管理指南》等对企业建立分类分级制度仍具有较强的参考意义。

3、价值前提——数据的合规保障

司法实践以个别判例方式，在反不正当竞争法意义上肯定了企业对其付出努力所获得或持有的“数据资产”主张一定的财产性权益，但这并不意味着这些数据资产可由企业任意使用其控制的数据。如前文所述，数据在其全生命周期的处理均合法合规，是挖掘数据资产价值的大前提。

数据的非竞争性、非排他性一方面便利了数据的自由流动，另一方面也降低了企业获取、使用数据的违法成本。倘若企业手中的数据系通过违法手段获得，或者在收集、使用过程中侵犯了法律所保护的正当权益，则不仅使得企业落入违法禁地，还将极大减损其数据资产的巨大价值。例如，前段时间陷入刑事调查风波的多家大数据公司，均涉嫌以非法手段获取个人信息而陷入查封扣押、停业倒闭的窘境。

我国《网络安全法》确立了我国网络安全领域网络信息安全保护的总领规则。从数据层面，《网络安全法》着重强调了个人信息的安全保护，这与我国几乎同期发布的《民法总则》所强调的自然人的个人信息受法律保护相互呼应。除此之外，我国《网络安全法》对于个人信息以外的另一类数据——重要数据也给予了特定规则（主要是出境规则）上的关注。当然，在网络安全语境下，不同行业领域，特别是敏感行业内对于行业数据使用、处理的特别规定也需引起企业足够重视。最后，数据之上还可能隐含他人享有的或因国家强制性规定所保护的合法权益，不当使用也会引发民事侵权、行政违法甚至刑事责任的风险。下表对数据所可能包含的受法律保护的客体进行了概要梳理：

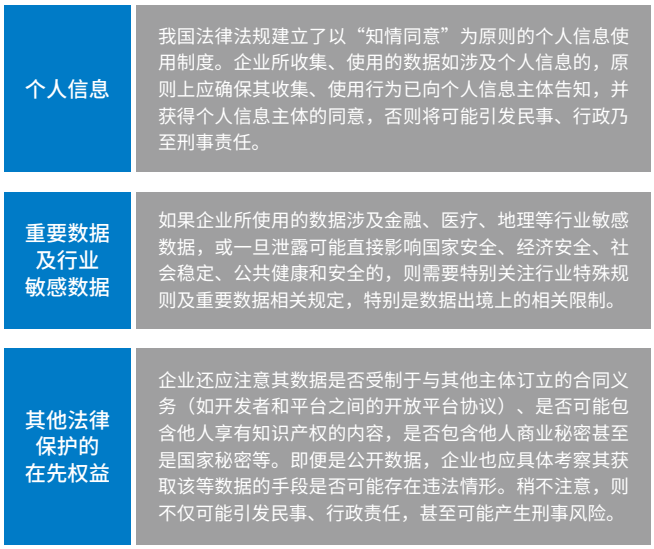


图4 数据处理的合规重点

三、留给企业的平安夜功课

（一）基于合规与价值的分类分级——厘清数据合规脉络及数据的价值

一般企业都已经在对标行业基本要求的基础上，制定适用于自身情况的数据分类标准。但大多数企业的数据分类分级仅仅考虑到了数据安全，比如将数据分类为高度机密、机密及一般等三类，而忽略了“数据资产”中合规性和价值的分级分类要素，导致后期对于数据资产进行合规性评估以及数据资产估值时往往无从下手。

实践中，企业应全面梳理自身不同类别、不同来源的各项数据，并将数据的业务属性、安全属性、合规义务以及价值因素同时纳入考量，根据自身实际情况建立数据分级机制。下图展示了数据分类分级的一般逻辑。诚然，对于企业特别是集团企业而言，因业务条线纷繁且彼此交错关联，在数据分类识别及分级管控上要更为复杂，并不能一蹴而就。企业应更多基于自身业务特点，在参考相关国家及行业标准的基础上，有步骤地实现不同业务条线的数据分类梳理。

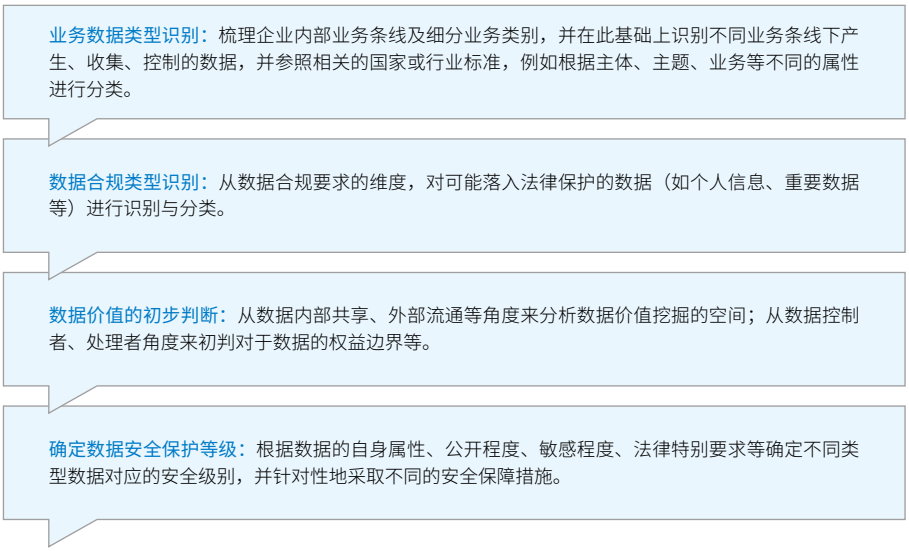


图5：数据分类分级过程概要

（二）数据融合互通

由于全球数据合规趋严的形势，数据的商业化利用和价值挖掘势必面临更为艰巨的挑战。一方面，数据合规性要求的逐步上升导致可用或容易利用的数据类型和范围急剧减少；另一方面，在“数据引领未来”的意识带动下，企业对于所持数据的自我保护意识愈发强烈，进一步加剧了企业之间对于数据资源的争夺。随着企业获取外部数据成本日益提高，企业对于自有数据的深度挖掘显得尤为重要。而如前所述，不同业务数据的互通融合，特别是同时运营多种类业务的企业在集团层面将其各业务线所处理、控制的数据进行打通与融合，将成为企业最大化发掘、应用数据价值的有效途径。数据融合互通的本质目的在于利用企业多渠道、多元化的数据，形成更加完善的用户画像，帮助企业基于客户需求精准开发潜力产品，有效实现商业推广。但在数据融合过程中，企业也将不可避免地涉及大量个人信息、重要数据等行业监管数据的收集与处理。因此，数据的安全与合规保障，是数据融合互通工作中不可或缺的价值视角；特别是对于各业务中收集的个人信息，企业如何确保在数据融合互通的场景下获得个人信息主体对数据在整体系统中进行处理的有效授权，是数据融合互通合规问题的重中之重。

不可否认的是，数据资产化是数据经济时代的必经之路，未来数据资产估值、甚至数据资产的证券化可能也指日可待。但和所有资产管理的前提一样，数据的合规性和资产中价值因素如何分析及固定将是企业首要考虑的问题。考虑到近期国家各执法机构对于个人信息保护、金融信息利用等数据合规的频繁执法活动，企业在进一步累积数据资产的同时，要重点关注数据资产的合规性，隔离外部数据风险并充分挖掘企业内部数据价值。

总而言之，数据资产确实是企业在数据经济时代的竞争力表现之一，但同时不合规的数据不仅无法形成为资产，更有可能为企业的长期发展“埋雷”。在企业谋求商业利益的同时，应当就数据全流程的合规、数据商业化的合法性等问题审慎分析，以免半路“夭折”。

（本文发布于2019年12月24日。）

“数据主权”浪潮下企业如何构建全球数据管理体系——兼评美国《国家安全与个人数据保护法》提案

引言

2019年11月18日，美国国会共和党参议员，参议院司法委员会犯罪、恐怖主义与国土安全小组主席Josh Hawley向参议院提交第2889号提案——《2019国家安全与个人数据保护法》（National Security and Personal Data Protection Act of 2019）[1]（“《提案》”），再次引发了各方关于数据保护、跨境传输等方面话题的热议。尽管目前《提案》仅处于提交参议院的阶段，在其正式通过生效前，至少还需要参议院、众议院的通过并最终由总统签署，但《提案》基于安全目的的规则设置凸显了“数据主权”的理念，值得所有企业警惕，并提前布局做出应对方案。

一、《提案》的目的和主要内容

一言以蔽之，为阻止用户数据向中国和其他可能威胁美国国家安全的国家传输[2]，《提案》界定了特别关注国家（Country of Concern，“COC”，包含中国、俄罗斯等）[3]和特别关注科技公司（Covered Technology Company，“CTC”）[4]。《提案》对涉及COC及CTC的用户数据（User Data，其中用户包含拥有美国国籍、持有美国护照的citizen，以及拥有居民身份residency的自然人）[5]收集、使用、存储和传输进行了重点关注，也相应提出了一些普适的通用要求。具体而言：

[1] S.2889-National Security and Personal Data Protection Act of 2019，参见https://www.congress.gov/bill/116th-congress/senate-bill/2889/text?q=%7B%22search%22%3A%5B%22National+Security+and+Personal+Data%22%5D%7D&r=1&s=2，2019-11-26.

[2] "cuts off the flow of sensitive data to China and countries that similarly threaten America's national security", Senator Hawley Introduces Bill to Address National Security Concerns Raised by Big Tech's Partnerships with Beijing, https://www.hawley.senate.gov/senator-hawley-introduces-bill-address-national-security-concerns-raised-big-techs-partnerships, 2019-11-18, 2019-11-26.

[3] 参见《提案》Sec.2 (2)中规定，即“中国、俄罗斯以及其他经国务卿认定可能对数据隐私保护和数据安全造成的国家”。

[4] 参见《提案》Sec.2 (3)中规定，即在州际贸易和涉外贸易中提供基于数据的在线服务（如网站、互联网应用）或提供基于数据的在线服务并可能影响州际贸易或涉外贸易的，且（A）在COC注册成立的公司及其子公司，或（B）由COC国民或COC公司持有多数或控制股权权益的公司及其子公司，或（C）其他需要遵守COC的法律规定、并使得COC获得美国公民或居民的用户数据且无法提供与美国宪法和法律相当程度的自由和隐私保护的公司。

[5] 参见《提案》Sec.2 (6)中规定，即由任何一家提供数据为基础的服务的企业（如网站或互联网应用）获得的，任何标识、关联、描述、可产生联系或可合理连接到一个美国公民或美国居民的信息，而无论该等信息是直接向该等企业提交的、由该等企业自行观测所衍生的还是从其他第三方用任何方式取得的。

重点条款	针对CTC	通用要求	重点解读
数据收集	**最小化原则** 仅能收集为运营网站、服务或应用所必需的最小限度的用户数据[6]	N/A	借鉴了主流数据保护立法的思路，对CTC收集使用用户数据提出了较高的要求，可能对CTC的数据使用目的等产生限制，一定程度上可能提升CTC的运营成本、限制技术发展的空间
数据使用	**次要用途限制** 禁止将收集的用户数据用于次要用途，含定向广告、不必要的共享、以及发展人脸面部识别技术[7]		
用户权利	**访问权、删除权**[8]		
报告义务	定期（至少每年）向相关部门进行报告[9]		
数据传输	禁止向COC直接或间接传输任何用户数据或可能用于破译该数据的信息（如加密密钥）[10]		对CTC而言，即便是在美国境外收集的美国公民或居民的用户数据将可能无法本地化存储，涉及COC国家的用户数据及相应密钥的传输也将可能受到严格限制
数据存储	不得在位于美国境外（或任何与美国订立司法协助协议的国家）的服务器或存储设备上存储任何美国公民或居民的用户数据或可能用于破译该数据的信息[11]	禁止在COC境内的服务器或存储设备上存储在美国境内收集的个人用户数据或可能用于破解该数据的信息[12]	
例外情形	（1）CTC为提供与COC无关的、司法或军事协助的目的收集、使用、保留、存储或共享用户数据；和（2）共享内容传输的情形（即用户生产内容的目的即是与其他用户共享，如社交媒体信息、电子邮件信息）[13]		
罚则	刑事责任（5年以下监禁）及民事责任[14]		

不难看出，《提案》从美国公民和居民的用户数据角度切入，对于跨国开展业务的CTC（尤其是涉及COC国家的企业），建立了明确的数据回传美国和本地化存储要求，同时对于用户数据的输出进行了严格管制，一旦严格实施很可能切断向COC传输美国公民和居民的用户数据的路径。此外，尤为值得关注的是，《提案》中明确提出了定向广告和人脸识别技术相关的数据使用限制，定向广告是目前大数据主要商业应用之一，而人脸识别技术则是个人真实身份标识的重要获取方法，如按照其中规定严格执行，相关企业甚至整个行业将面临巨大的变革。

一方面，《提案》的严格规定很可能脱胎于对美国国家安全的高度关注，但同时，《提案》一定程度上也在规制思路和要求等方面映射出其他主要司法辖区数据立法的影子，显露出其与“数据主权”浪潮之间同样密不可分的联系。

二、安全与法律秩序的重构：“数据主权”浪潮

事实上，“数据主权”或者说数据资源控制立法的浪潮，早已不是新鲜话题。随着大数据、云计划、物联网以及移动互联网等新一代信息技术的普及推广，个人数据的安全保护以及数据资源的开发利用已迅速在主要司法辖区之间铺开，不同国家/地区对于数据安全和数据资源的高度重视不约而同地具化成为数据本地化和跨境数据传输等法律规则。

以《提案》为例，其表达出对美国公民或居民的用户数据控制意愿，一定程度上延续了美国《澄清域外合法使用数据法案》（CLOUD Act）中肯定美国执法机关对美国企业“控制”的境内外数据均享有“主权” 的思路[15]。类似的，欧盟《通用数据保护条例》（GDPR）也以普遍适用（即包含所有针对欧盟用户提供产品和服务的企业）的同等保护水平从安全角度建立了个人数据

[6] 参见《提案》Sec.3 (a) (1).
[7] 参见《提案》Sec.3 (a) (2).
[8] 参见《提案》Sec.3 (a) (3).
[9] 参见《提案》Sec.3 (a) (6).
[10] 参见《提案》Sec.3 (a) (4)及Sec.4 (a) (1).
[11] 参见《提案》Sec.3 (a) (5).
[12] 参见《提案》Sec.4 (a) (2).
[13] 参见《提案》Sec.3 (b).
[14] 参见《提案》Sec.5 (b), (c)和(d).
[15] 上海社会科学院互联网研究中心：《全球数据跨境流动政策与中国战略研究报告》，https://www.secrss.com/articles/13274，2019-08-28，2019-11-26。

外流的管控体系，俄罗斯、印度等国家/地区也纷纷通过本地化等规则、以期确立对数据的控制。与其他司法辖区类似，中国《网络安全法》及《数据安全管理办法（征求意见稿）》中也从网络安全和数据安全等角度提出了部分数据本地化和出境安全评估的要求，反映出对数据管控的考量和关注。

综合而言，从立法技术上看，目前各司法辖区主要通过两种路径确立对数据的控制：

（1）以地域为主的控制，即对司法辖区内收集、产生的数据提出控制要求，例如印度中央银行要求位于印度的支付企业在印度本地存储数据；

（2）以本地公民和/或居民为主的控制，即对收集本司法辖区公民和/或居民数据的企业或组织进行控制，例如《提案》等。

同时采取两类路径“双管齐下”无疑将得到更好的数据管控收效，但也引发了秩序重构的紧迫必要性。以美国CLOUD Act和欧盟GDPR为例，对于在美国设立的而在欧盟境内存储用户数据的企业（例如CLOUD Act立法背景下的微软公司），按照美国CLOUD Act规定，美国国内司法部门将有权向其调取境外存储的数据证据；相对的，GDPR则对个人数据从欧盟输出进行了严格的限制，除非满足充分性认定、保障措施、国际协议等前提条件，个人数据将难以对外传输。为此，该等企业一旦面临美国国内司法部门的调取要求，将需要在美国和欧盟两类法律体系之间进行协调和应对。

如前所述，一定程度上，这样的法律秩序重构将无法避免短期内的冲突与矛盾，尤其是当全球化的跨国企业尚未能在数字经济时代发展出完善的全球性合规应对实践时。事实上，欧盟数据保护委员会也在2019年7月10日的报告中指出，“美国的CLOUD Act并不能够为GDPR框架下将个人数据传输给美国提供充足的法律基础……GDPR或其他欧盟成员国法律下控制个人数据的服务提供者很可能会面临美国法与GDPR之间的法律冲突。[16]”

三、构建全球数据管理体系的应对思路与常见模式

在这样的时代背景下，面对重新构建过程中的法律秩序，全球化的跨国企业既然不能改变政治和立法走向，势必需要迅速进化、适应这一“浪潮”，构建合理、合规而业务高效的全球数据管理体系，进而实现业务发展与合规义务的平衡。

首先被提出的是成本较高的解决方案——本地化，无论是微软进入中国云服务的成功经验，还是在华运营20年的SAP于今年提出的“中国加速计划”都是本地化的典型案例。一定程度上，部分或完全的本地化能够不同程度地避免了不同司法辖区规则的协调，但高昂的基础设施建设成本、核心研发力量的分散化挑战、数据融合的阻碍、企业内部数据安全制度无法统一等弊端和限制也实质上限制了本地化方案的适用性。

为此，从体系建设成本、业务与数据的关联、数据安全和监管政策要求等多个角度出发，实践中开始逐渐形成不同的全球数据管理体系构建思路。目前而言，根据我们对实践的了解，常见的三类全球数据管理体系如下表所示：

数据管理体系	单极中心化体系	多极区域化体系	分散本地化体系
构建形式	构建全球单个巨型数据中心及单一控制主体，以最大化数据融合效应并降低成本	按照需求，分别构建多个区域数据中心和控制主体；该等体系下存在不同的实现方式，例如全域数据建立多极中心，部分数据区域化部署等	分散程度最高的本地化数据中心和控制主体方案，相对纯粹的本地化
主要优势	• 基础设施建设成本低； • 数据融合效应强，利于数据价值的有效开发； • 利于建立统一的管控和安全措施； • 中心化体系节约对接和交互成本。	• 特定区域内数据流通顺畅； • 部分形成数据融合效应； • 一定程度上协调不同司法辖区的法定义务； • 区域中心交互速度较快，实时性有所保障。	• 有效避免数据跨境限制，分散履行当地法定义务； • 数据实时性强，对业务支持弹性大； • 分布式存储，能够避免数据泄露等负面事件影响的扩散。
潜在不足	• 不同法律体系下法定义务协调成本高； • 可能面临较多跨境规则的限制； • 数据的实时性面临挑战。	• 仍部分受数据跨境规则限制； • 相较于单极中心化体系的建设成本更高； • 区域之间的数据流转受限； • 区域的划定和数据控制主体选择需要综合考虑。	• 体系建设的成本最高； • 数据分散、较难形成聚合效应； • 不同地区的数据安全标准难以统一管控； • 高精尖科技、商业秘密等敏感信息难以管控。

[16] Lauren Morris: Cloud Acts Conflicts with GDPR, EDPB says, https://globaldatareview.com/international-transfers/cloud-act-conflicts-gdpr-edpb-says, 2019-7-15, 2019-11-26.

数据管理体系	单极中心化体系	多极区域化体系	分散本地化体系
常见典型示例	以重基础设施、研发成本投入为典型特点的行业/企业，如航空领域电子客票处理服务领域、AI技术开发、银行金融业等	适用性相对较强，兼顾建设成本和业务实时性等需求的场景，如云计算平台等	具有极强的数据交互实时性要求或高度监管等特别考虑的行业/企业，如自动驾驶服务（测绘与地图严格监管要求）、音视频服务（交互实时性要求与监管要求）等

当然，随着不同司法辖区之间的法律秩序逐步重构完成，具体法律体系之间的义务协调也随之推进，例如美国与英国已就CLOUD Act项下合作达成协议[17]。相应的，企业构建全球数据管理体系的思路和模式仍处于不断发展和丰富过程之中。

此外，在构建全球数据管理体系的过程中，企业不仅需要针对个人数据与用户数据进行仔细考量，其他类别的数据同样可能引发合规关注和问题，比如技术出口管制等，需要企业切实进行合理评估。

四、合规建议

综上所述，在“数据主权”的浪潮下，无论是自建IDC还是选择合格供应商构建全球数据管理体系，我们建议各类型企业均应当采取更为审慎和主动的态度回顾自身业务，并相应及时采取细致和全面的应对措施。

首先，为确保全球数据管理体系的构建思路具有坚实、可靠的事实基础，企业需要对自身业务中的数据需求、技术需求和合规要求进行完整明确、层次清晰的事实梳理：

（1）全面盘点自身业务开展过程及所形成的数据管理体系中可能涉及的数据类型，并合理进行分类分级；

（2）审视各类业务场景中的数据需求和合规要求，评估相关法律风险，尤其是针对存在数据跨境、产品/服务跨境、业务主体跨境等情况的业务场景；

（3）基于事实梳理的情况，建立并不断完善网络安全与数据合规体系，以公开、透明、经得起检验的合规措施自证。

其次，对于不同类型、规模、行业的企业而言，在前述通用的应对思路基础上，还需要进一步根据自身情况相应进行更具针对性的策略选择。

（1）对于大型跨国企业而言，由于自身可能直接落入到各司法辖区有关本地化和跨境限制等规则的义务主体范围中，我们相应建议：

a）在事实梳理过程中，除上述要点外，此类企业还应着重强调不同司法辖区业务之间的业务关联性和数据融合、打通的必要性，为后续决策提供基础；

b）在风险评估和决策阶段，此类企业需要重点、优先、及时解决顶层架构问题，合理决策，确定数据管理体系的构建方向；尽量避免不同国家/地区业务条线和主体之间“各自为战”、“野蛮生长”；以银行金融业为例，对于业务特性中天然具有跨境基因的行业，从总部/总行层面务必应对全球发展情况进行统筹规划方案，可以考虑核心业务系统采用单极体系节约成本，部分边缘系统和数据本地化部署提升访问效率和避免过度的数据跨境传输等；

c）最后，对于大型企业而言，巨大的规模导致了“缓慢的转身”，而信息时代瞬息万变的不止是市场，还有技术发展和监管要求；为此，跨国企业应重点注意避免僵化和依赖特定的某一类体系构建思路，根据业务发展、立法发展和技术发展等实际情况，提前规划、预留空间，并适时果断切换与迭代，采取最为适宜而合理的全球数据体系；举例而言，曾经被普遍认同和采用的全球统一CRM系统和DMP平台，对于跨国企业的员工、客户管理和数据资源积累起到了举足轻重的作用，然而在现有立法背景下，这些单极化体系的合理性、必要性都将值得所有企业再度思考。

（2）对于其他类型的企业（例如本地化的企业）而言，一方面可能因未达到特定的监管标准（例如未构成中国《网络安全法》下关键信息基础设施运营者）而不受本地化规则或跨境限制的影响；但另一方面，这些企业也同样可能因与大型跨国企业建立合作关系等原因受到目前立法潮流的影响；为此，即便自身业务中并不明确落入本地化、跨境限制等规则之中，企业也需要在合理开展数据盘点和业务盘点的基础上，构建对外提供产品/服务过程中的合规风险管控防火墙，例如业务协议的完善与更新、与合作方之间的数据权益明确分配等。

最后，从外部影响的反馈上看，企业还应当紧跟立法和执法趋势，根据实际情况调整应对策略；同时，对于可能产生重大影响的立法思路和草案（例如《提案》），通过立法意见、听证会、公开媒体等多种可行渠道表达来自于企业的意见，以争取更为有利的规则趋势。

（本文发布于2019年11月27日。）

[17] 参见https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists, October 3, 2019.

“数”往知来
——封禁APP背后的数据博弈

引言

2020年6月29日，印度新闻信息部发布消息称，印度信息电子与技术部援引《信息技术法案》（the Information Technology Act）第69A部分第2009条，禁止用户在印度境内访问（Blocking）59款中国移动应用，理由在于以上移动应用以非法方式窃取用户数据传输至境外服务器，可能损害印度的主权以及国家安全与公共秩序。[1] 全球范围内，基于安全目的对于数据跨境的限制和审查早已不是新闻，更重要的是“数据主权”思想渐渐融入到各国的立法和执法活动中。印度此举再次引发各方关注，跨国企业应当提高警惕，对于潜在数据安全及合规风险提前应对，建立符合国际立法趋势和竞争形势的全球数据跨境顶层设计，并将数据资产的思路贯彻到企业日常经营管理中。

一、印度的数据跨境规则

此前，印度在数据跨境自由流动与数据本地化之间持较为中间的态度。[2] 一方面逐步推进数据本地化政策，另一方面设置了数据本地化的豁免情形，并对数据分级分类实行不同的数据本地化要求。以个人数据为例，印度《个人数据保护法草案》[3]（Personal Information Protection Act，以下简称“《个人数据保护法案》”）将个人数据分为三类，根据《个人数据保护法案》第33条与第34条，我们理解，印度实现个人数据跨境传输的路径通常有三种：

一般个人数据	没有作出限制，可以自由传输至境外
敏感个人数据	满足第34条第（1）款条件时，可以传输至境外
关键个人数据	原则上禁止传输至境外，例外地满足第34条第（2）款列举的医疗急救事由或获得中央政府允许时，可以传输至境外

[1] 参见https://pib.gov.in/PressReleasePage.aspx?PRID=1635206。

[2] 参见上海社会科学院互联网研究中心：《全球数据跨境流动政策与中国战略研究报告》，https://www.secrss.com/articles/13274，最后访问于2020年6月30日。

[3] 尽管2018年《个人数据保护法草案》尚未生效，但在实践中该草案已具有较强的指导意义。

判断个人数据的敏感或关键程度，需要对具体的数据处理场景进行个案分析。此次受到波及的59款移动应用涉及多个领域，包括短视频、浏览器、地图、跨境电商、游戏、社交、安全软件、新闻、图片编辑、邮件、音乐、直播、翻译等，包含大量个人数据的处理。但是，这些个人数据是否都属于敏感个人数据或关键个人数据并不能直接判定。由于场景众多、数据量较大，可能很难逐一论证移动应用处理数据的合法性，并且由于各场景情况不同，通常也较难实现直接禁止访问全部移动应用的处罚效果。

但是，在《个人数据保护法草案》体系之外，印度现行的《信息技术法案》第69A部分还赋予了政府基于特定目的，禁止公众访问任何形成、传输、接收、存储或托管在任何计算机资源中的数据的权力。其中，第69A部分所规定的特定目的包括，保护印度主权及保护国家安全与公共秩序，维持与外国友好关系，以及防止煽动实施与前述有关的任何可识别罪行等。这一条款为印度限制或禁止向境外传输的数据类型提供了一定的弹性空间，即除了《个人数据保护法草案》中的个人敏感数据或关键个人数据，任何类型的数据只要被政府认定为有损害以上目的的风险，都有可能被禁止访问。

基于保护国家主权、数据主权等对数据跨境传输作出限制，不排除是一国为保护国内数字产业经济发展或国内其他利益而综合考量的结果。但是，由于政府在认定是否发生损害国家主权、数据主权的风险时具有较大的裁量权，对于涉及数据跨境传输的企业而言，常会面临较大的不确定性与风险。因此，援引类似规定前通常应进行谨慎地论证，否则轻易地触发类似规定引发限制数据出境的后果，将给跨境经济活动带来较大地危害。

二、其他法域的数据跨境规则及实践

出于国家安全、数据安全等因素限制数据跨境活动并不局限于印度，全球范围内，不同法域针对数据跨境活动可能具有不同程度的限制，全部或部分的数据本地化规则成为各国数据主权立法体系中的重要组成部分。

美国

以美国为例，保护国家安全、数据安全等是其在实践中限制数据跨境活动的重要理由。2018年颁布生效的美国《澄清域外合法使用数据法案》（the Clarifying Lawful Overseas Use of Data (CLOUD) Act, 以下简称“CLOUD Act”）将美国执法机关的数据“主权”延伸至美国企业“控制”的境外数据。2019年共和党议员向参议院提交关于《2019国家安全与个人数据保护法》（National Security and Personal Data Protection Act of 2019）的提案，通过专门立法的方式对该问题作出细致规定，其条款的设置也充分凸显了美国“数据主权”的理念，例如明确要求跨国开展业务的特别关注科技公司（Covered Technology Company, CTC）将数据回传美国和本地化存储，同时对用户数据的输出进行了严格管制等。

欧盟

欧盟主要通过《通用数据保护条例》（General Data Protection Regulation，以下简称“GDPR”）及《非个人数据在欧盟境内自由流动框架条例》对数据跨境传输进行规制，推动数据在欧盟境内的自由流动。欧盟对于与区域外的数据跨境传输提出了条件限制（例如充分性认定、约束性公司规则、标准数据保护条款等）。而作为对CLOUD Act中“数据主权”及其规则的回应，欧盟数据保护委员会（European Data Protection Board）曾发布报告表示，“CLOUD Act可能与GDPR第48条，即仅在基于国际协议的基础上认可域外法院命令”进而向欧盟境外传输个人数据的规则存在冲突。[4]

日本

日本的数据跨境传输制度可能相对更为宽松，目前日本尚未就国家安全、数据主权的事由作出具体规定。以个人数据为例，除某些特殊的国际协议或数据保护水平的互认外，日本《个人信息保护法》就一般性的个人数据跨境传输所提供的合法路径主要限于以下三种情形，即征得数据主体同意、接收国获得个人信息保护委员会认可具备同等保护水平或接收方具备完善的数据保护体系等。

其他

其他法域在实践中也已经出现针对数据跨境的监管处罚。例如，法国数据保护机构（the French Data Protection Authority）2019年对一家建筑公司开出罚单，其中一个原因就在于该公司在将拨打营销电话过程中收集的数据传输到非欧盟地区的呼叫中心提供商的过程中，未采取有效的数据跨境传输措施。又如，俄罗斯虽然本身不绝对禁止个人数据出境，但是要求数据首次存储必

[4] Lauren Morris, CLOUD Act Conflicts with GDPR, EDPB says, Global Data Review, https://globaldatareview.com/international-transfers/cloud-act-conflicts-gdpr-edpb-says，最后访问于2020年7月1日。

须在俄罗斯的服务器上。[5] 2020年3月，两家互联网巨头因为拒绝将数据存储在俄罗斯服务器而遭到俄罗斯法院的高额处罚等。

三、“数据主权”下的数据跨境规则与企业全球数据资产管理体系

尽管在数据跨境传输的具体监管规则设计和监管强度上可能有所不同，但各国均不约而同地将数据（特别是个人数据）的跨境传输作为数据保护体系构建中的重要一部分，其背后所反映的正是“数据主权”或者 “确保对数据资源及价值的控制”的立法理念。与此同时，不同司法辖区的数据跨境监管路径及具体规则设计上的差异，也为企业在多司法辖区业务开展过程中的“全球”数据管理体系构建和合规成本提出了考验。

实践中，为了满足企业在特定司法辖区业务运营中的合规义务，包括但不限于数据安全、行业监管规则、数据与国家安全等；同时考虑到（1）实际的数据管理体系建设成本，如数据中心等基础设施建设成本、信息流转及沟通成本；（2）业务对数据的需求，特别是数据的实时性与全面性之间的动态平衡等因素，实践中逐渐形成了三种常见的全球数据管理体系构建思路，即：

1）单极中心化的数据管理体系：在全球构建单个巨型数据中心及单一控制主体，作为数据的存储及处理的核心“大脑”，将业务所在的司法辖区收集和产生的数据传输至唯一的数据中心，实现中心化的数据处理；

2）多极区域化的数据管理体系：按照需求，对全球业务所在的司法辖区进行区域性划分，在对应区域内选择合适的司法辖区构建区域数据中心并设置控制主体，作为区域内数据存储及处理的关键性节点，保障区域内数据的自由流通。同时通过其他通路设计在一定程度上保障区域间数据的交互以及与总部之间的数据交互；

3）分散本地化的数据管理体系：根据监管的要求实现全部或较高程度的本地化部署，在业务所在的主要司法辖区，结合业务对数据的需求以及监管规则，部署本地化数据中心并设置对应的控制主体、较大程度地限制数据向境外传输的情形，仅在对数据进行必要处理或满足特定监管规则情况下就进行有限的数据跨境传输和交互。

对于以上三种数据管理体系，可能在基础设施建设及数据交互沟通成本、数据的融合与价值开发、数据安全（特别是数据泄露）风险、数据内部合规制度构建及审查等方面都存在不同之处，特别是考虑到某些行业、企业的业务运营需求以及监管机构的关注重点等要素，三种数据管理体系可能在常规意义上会适用于不同类型的行业和业务（有关三种全球数据管理体系的构建形式、优劣势分析及实践应用的更多信息，请参见“数据主权”浪潮下企业如何构建全球数据管理体系——兼评美国《国家安全与个人数据保护法》提案[6]一文）。

四、全球数据跨境的顶层设计与数据资产管理体系

企业只有在全面厘清自身业务中的数据类型、数据需求、业务所在司法辖区的监管规则及其适用情况的基础上，充分考虑自身的数据安全管理能力、信息沟通交互能力、合规成本等要素，才能选择出最适合的数据管理体系。除了既存的数据跨境、产品及服务等情况外，从动态发展的视角来看，我们建议企业在构建数据管理体系时还需要结合未来（特别是中短期的）业务发展规划、监管规则变化趋势，为数据管理体系的构建保留一定的弹性空间。

同时从“数据主权”概念下公权力对于数据资源的限定可以充分理解数据对于社会及企业的价值和带来的竞争力，企业应当从数据资产的角度来规划和管理自身的数据，从安全、合规、融合和价值四个维度来建立企业的数据资产池，并通过技术、合规及商业的管理方法来保护和管理数据资产，最大限度发挥数据资产的驱动力。

在中国企业“走出去”的时代趋势之下，本次的印度执法活动再次为中国企业的海外业务运营敲响了警钟。“数”往知来，在数据主权理念日益受到重视、数据跨境传输的立法规则及执法活动不断加强的今天，企业在面临相关执法时是否能够实现“迅速”“优雅”的转身，通过对全球数据跨境及资产管理体系的有效构建和有机调整，降低相关法律风险，提升在海外业务运营中的市场竞争力，对于企业而言至关重要。

（本文发布于2020年07年02日。）

[5] 参见https://www.huntonprivacyblog.com/2019/12/02/cnil-fines-french-construction-company-for-infringements-when-placing-marketing-voice-to-voice-calls/，最后访问于2020年7月1日。

[6] https://mp.weixin.qq.com/s?src=11&timestamp=1593552113&ver=2433&signature=2Q3zUg1x13626hFH25yHY-oXZ57gXsaUJFMj*6n9sGML67mu7XlFAw9DLfgoAVtMlSlOEIS*hUKeON4y6KPB40U4GVCAJuGSq9bd1sc49jgmpKkB0PLc7t1s8E98lmtJ&new=1.

投资出行领域，数据是金矿还是烫手山芋？

随着智能手机的普及，近几年兴起的专车、顺风车、共享单车、分时租赁等移动出行平台， 改变了人们的出行方式。为享受这些移动出行平台带来的便捷，人们需要下载并注册相关的应用软件（App） 。可能很少人会注意到或认真关注这些应用软件背后的平台收集了多少个人用户数据（“个人数据”）以及如何使用这些数据。

事实上，在用户使用“新出行”平台的时候，这些平台默默收集了海量的个人数据，并基于所收集的个人数据形成了大数据，用以分析个人出行路线、个人喜好等重要信息。这些信息是进行精确的内容推荐和广告推送的基础，具备极高的商业开发价值，从而成为投资人眼中的“金矿”。但投资人挖掘“数据金矿”需要一双“慧眼”——不论是投资前的尽职调查，还是投资后的平台融合，都需要格外关注数据产业的合规问题，以避免将“数据金矿”变成“烫手山芋”。

一、“新出行”平台，收集个人数据的魔法棒？

注册成为“新出行”平台用户的时候，通常会有勾选是否接受用户协议和隐私政策的选项。只有在选择接受用户协议和隐私政策时，才能成为其用户并使用相关平台的出行服务。隐私政策为标准条款，用户只能勾选是否接受，并无修改的权限，相信大部分的人出于使用平台服务的目的会直接勾选。但如果在勾选之前多花几分钟点开并阅读隐私政策，会发现里面“藏着”相关平台收集何种个人数据以及如何收集、处理、使用、存储所收集的信息的 “大秘密”。

根据几家具有代表性的“新出行”平台公布的隐私政策，出于平台运营和安全管理的需要，其收集的个人数据可以分为以下几类：

个人信息类别	具体内容
个人身份和账户信息	姓名、身份证号、电话号码、电子邮件地址、账户密码和安全信息等
个人出行数据	地理位置信息、行程起止地、路线轨迹、时长、里程数等
个人财产信息	银行卡号或第三方支付账户名、支付安全码、付款记录等
个人设备信息	所用设备型号、类型和状态、网络质量数据、服务日志等

如果使用汽车分时租赁服务，则需要额外提供更多的个人信息，比如照片、面部识别特征、性别、年龄、职业信息、征信信息、是否有犯罪记录、是否有不良行为记录、驾驶证等[1]。

根据《信息安全技术 个人信息安全规范》（GB/T35273-2017）（“个人信息安全规范”）的规定，“新出行”平台收集的上述信息（包括地理位置信息）均属于个人信息的范畴，并且其中的大部分信息（如个人身份和账户信息、财产信息、出行轨迹）亦属于个人敏感信息。为讨论方便，上述个人数据统称为“个人信息”。

[1] 为分析方便，暂不考虑汽车共享服务模式中平台为平台管理目的而收集的服务提供者（比如驾驶员）的个人信息。

在行家眼里，这些“出行”个人信息因为频率高[2]、数据直接和延展性高[3]成为了最优质的数据来源。由此，各类“新出行”平台也成了投资人眼中的“香饽饽”，估值一路水涨船高。

二、尽职调查，数据合规怎么看？

成熟的投资人在投资“新出行”平台之前，会对其进行全面的尽职调查，其中包括法律、合规方面的尽职调查。由于“新出行”平台收集、处理和使用海量的个人信息， 而这些信息又是平台的核心资产，对其进行数据合规方面的调查是尽职调查的重要组成部分。数据合规的尽职调查通常包含以下几个层面，数据合规体系、合规的执行以及监督等。

领域	关注重点
数据合规体系	（1）用户协议中是否存在关于个人信息的条款，是否符合法律规定和规范？ （2）是否存在隐私政策？隐私政策是否符合个人信息相关的法律规定和规范（比如相关政策是否符合合法、正当、必要的个人信息收集和使用原则）？ （3）是否存在内部的数据管理流程（包括数据的收集、处理、使用、存储、共享等）方面和个人信息安全事件处理的规定以及该等流程规定是否符合个人信息相关的法律规定和规范？ （4）内部数据流程管理规定与对外发布的隐私政策是否一致？
数据合规的执行	（1）数据的收集：个人信息的来源、收集范围、获取途径以及授权方式是否明确且合法有效，且符合隐私政策的规定
	（2）数据的使用： - 是否根据与用户的用户协议和隐私政策使用个人信息，对授权数据的使用（用于互联网营销或其他业务）是否超过授权范围和必要的限度？ - 个人信息的存储是否与隐私政策一致且符合个人信息相关的法律规定和规范； - 对于个人敏感信息，是否有特殊的处理方式？ - 对需要访问个人信息的员工是如何进行权限授权的？相关授权安排是否超过用户的授权范围和必要的限度？ - 是否对个人信息的规范使用采取了相应风险控制措施，相关措施是否规范、有效？
	（3）数据的共享： - 隐私政策是否已经说明与关联方共享数据的目的、涉及的个人信息类型、接收个人信息的第三方类型？ - 是否存在与关联方或第三方分享个人信息的情形？该等数据共享是否获得了用户的明确授权？是否超过必要的限度？ - 是否存在与数据共享相关的业务合同，其中的约定是否符合隐私政策和法律规定和规范？
数据合规监督	（1）是否存在定期的内部数据合规审查和数据合规培训？如何处理合规审查中发现的问题？ （2）是否因数据合规问题被任何主管部门调查或处罚过？

如上所述，在进行数据合规尽职调查中，要特别注意一致性的问题，即相关平台的数据政策是否符合相关法律规定和规范、内外政策是否一致以及实践中数据合规的执行（即数据的收集、处理等流程）与隐私政策是否一致。如果尽职调查中发现目标“平台”存在严重的数据不合规，比如数据收集和使用严重超出隐私政策的范畴或存在倒卖个人信息的情形，投资人可能需要综合评估相关平台的资产价值和数据风险而后决定是否值得继续投资。

除了上述关于数据是否合规的调查以外，投资人还要关注相关平台上述数据的商业化空间来合理评估“数据资产”的价值。众所周知，互联网经济的一大特点在于“羊毛出在猪身上”，数据商业化也有类似的逻辑。比如数据的价值不仅体现在能够进一步提高产品和服务质量，还在于能够帮助平台“洞察”用户，进一步了解用户的消费习惯，从而挖掘和开发新的商业模式，通过盈利来“反哺”平台，并进一步扩大用户数量，获得更多的用户数据，周而复始，循环不断。但上述商业模式很重要的一点在于

[2] 据报道仅某网约车单平台每日新增的轨迹原始数据就达70TB+。

[3] 出行与个人的社会层级、消费习惯密切相关，从而能够基于相关数据进行群体行为、商圈人流分析。

平台利用数据开发新商业模式的合规性。如果平台对于特定数据仅仅处于数据处理者的地位，或者间接地收集用户数据，则平台对于这些数据在超出最初收集目的以外的应用则应当受到严格控制，这些数据的商业化价值也将大打折扣。但如果平台能够直接“触达”用户，并能够有合理的商业逻辑“引诱”用户同意进一步以新的目的使用数据，则“盘活”了用户数据，为数据商业化在合规的基础上创造了获利的空间。

为了配合投资人进行尽职调查，就个人信息而言，被投资平台是否可以“知无不言、言无不尽”呢？或者投资人是否可以要求相关平台将其收集的个人信息全部上传以便进行核实？答案是否定的。因为一方面核实相关平台收集的每项个人信息对于投资人而言并非必要，而另一方面相关平台如直接上传其收集的个人信息至尽调数据库，必然违反其关于隐私条款中关于信息共享的规定。如果投资人确有必要了解用户数据的相关状况，以衡量目标公司的价值，作为目标公司的平台可只提供其用户的统计数据，或经过脱敏处理的用户相关数据即可。

三、投资协议，数据问题怎么办？

以个人信息为基础的数据是“新出行”平台性的核心资产，投资协议（如增资协议、股权转让协议、资产转让协议等）不能对此避而不谈。为防范因数据问题而产生的潜在投资风险，基于尽职调查的结果，投资协议中一般应包括数据相关条款，比如：

（一）陈述、保证条款

投资人要求作为平台的目标公司（“拟投资平台”）及其实际控制人（实际控制人作为平台创始人通常会是投资协议的一方）就数据各个层面的合规问题作出陈述和保证，比如数据的收集、处理、使用、存储、传输始终符合适用法律法规的规定，不存在因数据不合规而被相关主管部门调查、处罚的情形。

（二）交割前提条件、交割前或交割后承诺

对于尽职调查中发现拟投资平台数据合规方面的问题，可视情况严重与否设置为交割前提条件、要求实际控制人和拟投资平台承诺在交割前或交割后的一段时间内予以整改或补救。如设置为交割前提条件，则该项条件不成就时，投资人可以选择不交割从而终止投资项目。

（三）赔偿条款

如果在尽职调查中发现拟投资平台在数据合规方面存在较大风险，可以要求就数据合规可能导致的损失设置特别赔偿条款。即如果投资人因项目交割之前拟投资平台在合规方面的问题而导致的损失，可要求实际控制人和目标公司对投资人进行赔偿。

四、投资完成，数据融合怎么用？

对于某些投资人而言，其投资（通常为股权收购或资产（业务）收购）的初衷之一在于整合相关平台以实现数据整合、平台融合的协同效应。那么投资完成后，被投资平台的个人信息可以直接共享或进行跨境传输吗？中国个人信息监管规定给出的答案并非完全一致。

依据《网络安全法》的要求，个人信息的收集、使用以“明示+用户同意”为前提。理论上说，收购、兼并、重组等过程中的个人信息共享、转让也属于个人信息使用的形式之一，仍然需满足用户同意的要求。

《个人信息安全规范》明确规定，个人信息原则上不得共享、转让。当个人信息的控制者（即平台）发生收购、兼并、重组等变更时，个人信息控制者应当：

- 向个人信息主体告知有关情况；
- 变更后的个人信息控制者应继续履行原个人信息控制者的责任和义务，如变更个人信息使用目的时，应重新取得个人信息主体的明示同意。

换言之，如果由于发生收购、兼并、重组导致相关平台的收购方（即投资人）成为个人信息的控制者时，该收购方应继续履行原来平台所履行的关于个人信息保护的责任和义务且平台对用户个人负有告知义务；而如果收购方变更个人信息使用目的，则需要重新获得相关个人用户的明示同意。

但是，如果将隐私政策认定为平台与个人信息主体之间有关其数据收集、使用的约定，在隐私政策中涉及的个人信息控制者即平台发生改变时，根据《合同法》中变更合同履约方需要当事人协商一致的原则，则上述收购、兼并、重组而整合相关平台时即需要获得用户同意，而非仅仅在变更个人信息使用目的时需要明示同意。因此，《个人信息安全规范》的上述规定与《网络安全法》、《合同法》并不完全一致。考虑到《个人信息安全规范》不具有法律效力，在收购、兼并、重组等变更时，个人信息控制者仅向个人信息主体告知有关情况但未取得其同意，可能存在一定的法律合规风险。

而从另一方面来讲，通常情况下，不论是进行股权收购或资产收购，收购方希望获取收购后的平台的数据的目的通常与该平台的隐私政策不完全一致，即信息的使用目的存在变化。由此，即便根据《个人信息安全规范》，这种平台/业务的融合通常需要重新获得相关个人的明示同意。因此，稳妥起见，收购方整合相关平台以实现数据整合、平台融合之前，应事先获得相关个人用户的明示同意。

以近期某综合性平台并购某移动出行平台为例，在该移动出行平台被并购一周年之际，其用户通过App弹窗收到一封确认函，内容大致如下：

- 并购方拟在征得用户同意的前提下，打通移动出行平台和并购方的综合性平台的账号，届时并购方将共享移动出行端的各类数据；
- 用户选择不同意，则不会实施其用户数据的共享，该用户还可以继续通过移动出行平台App使用车辆；

- 用户选择同意，将可以使用移动出行平台账号登录并购方App，也可以在App内使用车辆并查看到行程记录等各类历史数据。

由此可见，移动出行平台的各类数据，如与并购方共享，并购方将会与其原有的其他数据整合并为整个并购方平台的目的利用相关数据，不但移动出行平台收集的个人信息的使用目的将发生变更，个人信息控制者也发生了改变。为符合个人信息保护关于知情同意这一最基本的要求，移动出行平台和并购方须就上述变更获得个人用户的同意。上述确认函基本符合知情同意的要求。

此外，如果因为平台整合导致需要向境外传输个人信息，则需要格外谨慎。根据《网络安全法》的规定，关键信息基础设施运营者需要将其在中国境内运营过程中收集和产生的个人信息和重要数据存储在中国境内，因业务需要确需出境的，则应进行安全评估。而国家互联网信息办公室2019年6月13日发布的《个人信息出境安全评估办法》（征求意见稿），则有意将有关个人信息出境的安全评估扩展适用于所有的竞争者，并且还明确规定，个人信息的跨境传输前应当向所在地省级网信部门申报个人信息出境安全评估。除网络运营者的数据出境义务有所增加外，对于关键信息基础设施运营者的数据出境要求甚至上升到了国家安全的层面——2019年5月21日发布的《网络安全审查办法（征求意见稿）》将“大量个人信息和重要数据出境”作为关键信息基础设施运营者启动网络安全审查的条件之一。可以看出，在国际贸易局势日渐严峻的当下，国内有关数据出境的立法也愈发呈现趋严态势，虽然该等立法尚处在征求意见稿阶段，但这种趋严性的规定或多或少代表了监管机构当前对个人信息跨境传输的态度，也进一步向当下进行涉及数据资产、业务交易，特别是跨国性质的投资和并购交易参与者“敲响警钟”。企业应密切关注相关立法和执法的态度走向，并适时对投资并购交易的流程安排作出适当的调整，例如可考虑在交割之前，在数据进行跨境转移之前，适时对数据所可能包含的个人信息、重要数据进行识别，及时做好内部安全评估工作，在必要情况下还应考虑设置数据本地化存储的措施，以防未来有关法律条文的生效引发数据跨境合规问题，避免其可能导致的业务停摆、交易被迫中止等法律和商业风险。

值得一提的是，除了上述个人信息保护的角度外，在进行数据和平台融合时还需要从反垄断法的角度进行评估。如果两个平台之间某种程度上构成竞争者，需要评估相关数据的共享是否构成敏感信息的交换并具有限制竞争的效果。另外，企业所拥有的数据资产也将一定程度上对企业的市场份额、市场力量评估产生影响。对于拥有海量数据资产的企业之间的投资收购交易，有可能被认为是“数据巨头”之间的“强强联合”，从而可能引发反垄断审查机关的一系列竞争关注。例如，在一例社交媒体并购交易中，欧盟委员会在其审查决定中就已或多或少提及数据的聚合对并购方市场力量所可能造成的影响。而此后欧盟委员会因并购方在审查期间提供误导性信息（即并购方在审查期间称无法让两大平台的用户账户完成自动匹配，而实际上将并购方用户ID与被并购方用户ID进行自动匹配的技术可能性早在2014年就已经存在）从而对并购方处以1.1亿欧元罚款。这一事件充分反映了反垄断执法机构在互联网领域的投资并购案件中对于数据聚合可能影响市场竞争格局问题的关注。

（本文发布于2019年06月28日。）

无“数据”，怎“车联”？
——“车联网”数据类核心业务法律监管刍议

一、把握“车联网”法律监管的主线——“两端”+“一点”

“车联网”，又称“智能网联汽车”，顾名思义，就是实现汽车功能及使用的“网络化”和“智能化”。车联网自21世纪第二个十年起，在中国方兴未艾，其应用场景和业务类型呈现出迅速多样化、扩展化的发展趋势。我们在此引用清华大学汽车产业与技术战略研究院赵福全教授等对车联网所做的服务分类[1]：

表1 车联网的服务分类

服务类型	服务内容
安全服务	自主式安全驾驶辅助、协同式安全驾驶辅助、车辆安全监控和救援、远程控制、隐私安全
节能服务	协同式节能驾驶、节能路径规划、驾驶行为分析和提醒、车辆状态监控、公共交通效率提升
信息服务	通信及网络服务、互联网内容服务、导航服务和LBS、个人定制服务、企业数据服务、软件服务
交通服务	交通信息服务、高速公路交通管理、公共交通管理、车队管理、特殊车辆管理
保障服务	汽车维修、汽车配套服务（停车、加油、充电、保养等）、汽车金融和保险、汽车租赁和共享、汽车销售、其他用车相关服务（酒店预订、旅游、智能家居控制等）

由上表可见，广义上的车联网产业及业务的覆盖范围是十分广泛的，包括了“车辆在全生命周期内产生的全部信息交换，涵盖车辆研发、生产、销售、使用、回收等各个环节”[2]。换言之，车联网使得由人、车和路这三项要素所构成的传统线下汽车生态环境，一跃而成为一个独立的且流动于路面之上的“第三网络空间”（区别于居家和办公网络空间）。正因如此，从法律角度来看，对车联网的监管必然是一项综合性的系统工程，既涉及到汽车制造、销售、维修、支持养护等传统线下行业，更触及通信、互联网、智能交通管理等线上行业乃至人工智能、自动驾驶等新业态、新技术。由此，对于有意布局并进入车联网产业的市场主体来说，从看似庞杂的车联网法

[1] 参见：刘宗巍、匡旭、赵福全，《中国车联网产业发展现状、瓶颈及应对策略》，载于《科技管理研究》2016年第4期，第122页。

[2] 同上。

律监管“迷宫”中梳理出一条可供实操借鉴的“主线”，就显得尤为重要。笔者认为，抓住这条主线，关键就在于把握车联网产业的“两端”和“一点”，即“汽车生产企业”和“最终用户”这两端，以及在这两端之间的产业链条上流动、交互的“数据/信息”这一点。

就“两端”而言，一方面，汽车生产企业位于整个车联网产业的最前端，面对着车联网的快速发展，汽车生产企业需要思考并回答其汽车产品在技术上如何实现智能互联、在业务模式中如何融入车联网、面对监管怎样做到恰当地“有所为有所不为”等一系列有可能决定其自身未来生存命运的重大问题；另一方面，用户作为车联网产业的最下游和全部车联网服务的最终对象，其权益保障、特别是对其个人信息和数据安全的保护，既应成为监管的重点，也理应被纳入所有车联网业务经营主体的合规义务范围内。

而就“一点”而言，由上表可以看出，不论是车联网产业的哪一个服务大类，都必须依托“数据/信息”这个核心要素。例如，如果离开了数据/信息的收集、传输、分析处理、反馈等环节，则上表中的安全、节能、信息等服务将根本无法开展。同时，车联网为数据/信息所搭建的是一个双向乃至多向的自由流动平台，这既包括数据/信息从用户车载端流向相关车联网服务提供商，也包括服务提供商向用户端提供数据反馈结果或特定类型的信息内容，还包括数据/信息在上下游服务提供商间的点对点或链条式流动。因此可以说，数据/信息正是车联网的生命线之所在，无数据/信息则无车联网。

基于此，笔者认为，对于相关市场主体、特别是汽车生产企业来说，结合车联网典型应用场景，把握住相应的数据/信息类核心业务，便可掌握进入车联网服务市场的“钥匙”。就此我们注意到，市场上已经出现了车企与互联网巨头合作布局若干项车联网核心业务的实例。而工信部、国家发改委和科技部于2017年4月6日联合印发的《汽车产业中长期发展规划》明确提出“到2020年……智能网联汽车与国际同步发展；到2025年……智能网联汽车进入世界先进行列”、“到2020年，汽车DA（驾驶辅助）、PA（部分自动驾驶）、CA（有条件自动驾驶）系统新车装配率超过50%，网联式驾驶辅助系统装配率达到10%……到2025年，汽车DA、PA、CA新车装配率达80%，其中PA、CA级新车装配率达25%，高度和完全自动驾驶汽车开始进入市场”等一系列车联网具体发展目标，并且特别要求要“围绕跨领域大数据的应用，创新出行和服务模式，推动汽车企业向生产服务型转变……到2020年，智能化水平大幅提升；到2025年，骨干企业研发、生产、销售等全面实现一体化智能转型”。由此可见，汽车生产企业正面临着布局并进入车联网服务市场的黄金机遇和重要关口期。

二、数据/信息类核心业务资质及外资准入一览

如上所述，汽车生产企业作为车联网产业布局的最前端，无疑是构建车联网最重要、也最具积极性的主体之一。因此，汽车生产企业对于车联网的法律监管，特别是其中涉及数据/信息并具有典型应用意义的核心业务的资质许可、市场准入等法律问题，有必要做到心中有数，方能在具体业务方案的制定和实施中确保有的放矢。

基于此，我们在下表中列出了在典型的车联网应用场景下，与数据/信息的收集、存储、处理、提供等各环节紧密相关的6大类业务（包括第二大类下的4个子类），并分别呈现其牌照许可、外资准入限制等方面的监管现状，以期为包括汽车生产企业（特别是外资车企）在内的意图涉足该等车联网核心业务的市场主体提供清晰而简明的监管指引。

1. 在线数据处理与交易处理业务（B21）[3]	
典型应用场景描述	服务提供商通过公用通信网或互联网，借助车载端软硬件，收集汽车配置、运行、行驶、油耗等数据，对该等数据进行实时或准实时分析、处理并将结果反馈给用户（即车主），以实现改进汽车性能、辅助驾驶等目的，或直接对车载端电子设备进行远程网络控制、状态监控等。[4]

[3] 该编号为该类业务在工信部《电信业务分类目录（2015年版）》下的编号；以下第2-5项同。

[4] 该项业务还包括“交易处理业务”，即如淘宝、京东之类的提供第三方交易服务的经营性电子商务平台；因此，如果车联网直接纳入此类第三方交易平台服务，如可以在车载端平台实现汽车相关类的网上购物，则也会构成该项业务，但从公开信息我们并未查询到目前已存在此类车联网应用场景。

1. 在线数据处理与交易处理业务（B21 ）	
业务符合性要点[5][6]	（1）利用各种与公用通信网或互联网相连的数据处理应用平台，如车载端面向用户的接入和处理平台以及服务提供商的后端数据处理平台； （2）通过公用通信网（如移动蜂窝通信网）或互联网； （3）对连接到网络的电子设备进行控制和/或数据处理； （4）为用户提供；**因此，如果只是为内部研发、工艺改进等非面向用户的目的，则不应构成。**
所需牌照	增值电信业务经营许可证
外资准入限制	外资比例不超过**50%** [7]
2. 信息服务业务（B25） [8][9]* * 根据具体应用场景的不同，车联网有可能触及该项业务项下的多个子类，分别参见以下第2.1-2.5项。	
2.1 信息发布平台和递送服务	
典型应用场景描述	服务提供商为用户提供一个信息平台，用户可以通过该平台选取并将服务提供商和/或第三方提供的应用软件等信息内容下载到自己的车载端并进行后续使用，典型如一个可直接在车载端访问的“应用商店”。
业务符合性要点	（1）第三方可在该平台上发布文本、图片、音视频、应用软件等信息内容； （2）服务提供商可按用户需要向用户指定的终端如其车载端递送、分发该等信息内容。
所需牌照	增值电信业务经营许可证
外资准入限制	应用商店：在**上海自贸区内**外资比例可达**100%**（企业注册地和服务设施均需在上海自贸区内）[10]；**在上海自贸区外**外资比例不超过**50%** 非应用商店：外资比例不超过**50%**
2.2 信息即时交互服务	
典型应用场景描述	用户可通过车载端软硬件，即时发送和接收音视频、文本、图片、文件等信息内容，典型如直接在车载端收发短信息、进行语音通话等（但借助车载端与手机等通讯设备的蓝牙连接进行的语音等信息交互除外）。
业务符合性要点	（1）利用公用通信网或互联网并直接借助运行在车载端的软硬件； （2）用户可“即时”收发语音等各类信息内容。
所需牌照	增值电信业务经营许可证
外资准入限制	外资比例不超过**50%**

[5] 该部分列出上方所描述的典型应用场景与该项业务相关定义、范围的主要相符之处；以下各项同。

[6] 参见《电信业务分类目录（2015年版）》第B21项。

[7] 参见《外商投资电信企业管理规定（2016修订）》第六条。

[8] 参见《电信业务分类目录（2015年版）》第B25项。

[9] 在此值得注意的是，一些特定类型的信息内容的网络提供行为，还有可能因受制于其他相关领域的监管而需要取得其他牌照，如《网络出版服务许可证》、《网络文化经营许可证》、《信息网络传播视听节目许可证》等。

[10] 参见《工业和信息化部、上海市人民政府关于中国（上海）自由贸易试验区进一步对外开放增值电信业务的意见》之二（一）。

2.3 信息搜索查询服务	
典型应用场景描述	用户可通过车载端的软硬件（如浏览器），直接检索、查询网页信息、文本、图片、音视频等信息，即一个车载端的“搜索引擎”。
业务符合性要点	（1）服务提供商自行进行信息收集与检索、数据组织与存储、分类索引、整理排序等活动，即并非在车载端内置第三方的搜索引擎服务； （2）用户可直接在车载端进行信息检索查询并获取搜索结果。
所需牌照	增值电信业务经营许可证
外资准入限制	外资比例不超过50%
2.4 信息保护和处理服务	
典型应用场景描述	服务提供商借助运行在车载端的客户端软件，在线为用户提供车载端病毒查杀、信息保护、垃圾信息拦截等服务。
业务符合性要点	（1）借助用户车载端的客户端软件和服务提供商的后端平台共同提供服务； （2）相关服务具有在线性和实时性。
所需牌照	增值电信业务经营许可证
外资准入限制	外资比例不超过50%
2.5 其他向用户提供信息内容的服务	
典型应用场景描述	服务提供商借助运行在车载端的软硬件，为用户推送天气、路况、新闻、财经等各类信息内容。
业务符合性要点	（1）服务提供商要自行进行信息的采集、整理、发送等活动； （2）信息内容能够被直接推送至用户的车载端。
所需牌照	增值电信业务经营许可证
外资准入限制	外资比例不超过50%
3. 互联网资源协作服务业务（B11[11]）	
典型应用场景描述	用户可借助车载端软硬件，将汽车配置、运行、行驶、油耗等数据（如相关历史记录信息）传输并存储至服务提供商的“云平台”上，并可后续随时进行访问、使用、读取等操作；抑或是直接使用服务提供商部署在其云平台上的应用软件以实现特定功能，并接受其提供的相关运行管理服务。这可被认为是一种车载端的“云服务”。
业务符合性要点	（1）服务提供商运行相关云服务设备和/或资源，如创建一个可从车载端直接访问的云服务平台； （2）提供的服务包括数据存储、互联网应用开发环境、互联网应用部署和运行管理等，并满足“随时获取、按需使用、随时扩展、协作共享”等特点。
所需牌照	增值电信业务经营许可证
外资准入限制	作为“互联网数据中心（IDC）业务”的一个子类，该项业务不向外资开放（合格的港澳资本除外）

[11] 参见《电信业务分类目录（2015年版）》第B11项。

4. 呼叫中心业务（B24[12]）	
典型应用场景描述	汽车生产企业或其他类型的汽车相关产品或服务经营主体（如道路救援企业），委托设有呼叫中心系统、数据库、话务员坐席等的服务提供商，代其向用户提供有关该委托主体的业务咨询、信息咨询、数据查询等服务；用户可借助车载端软硬件，通过公用通信网或互联网，访问服务提供商建立的呼叫中心系统和/或数据库，并以语音等方式获取前述服务。
业务符合性要点	（1）服务提供商需“自建”相关服务设施，特别是通过信息采集、加工、存储等建立数据库； （2）“自建他用”，即服务提供商必须是受其他企事业等单位的委托，为委托方的用户提供服务；**而如果是“自建自用”，如一家车企自行设立呼叫中心系统、数据库等，为其自己的用户提供相关业务咨询、信息咨询等服务，则不构成该项受监管的增值电信业务，而仅为一般性的产品售后或技术支持服务。**
所需牌照	增值电信业务经营许可证
外资准入限制	在**上海自贸区内**外资比例可达**100%**（企业注册地和服务设施均需在上海自贸区内）[13]；在**上海自贸区外**外资比例不超过**50%**
5. 存储转发类业务（B23[14]）	
典型应用场景描述	用户直接利用车载端软硬件，实现语音信箱、电子邮件等功能。
业务符合性要点	（1）服务提供商需借助语音信箱系统、电子邮件系统等“存储转发机制”； （2）所实现的依然是信息的收发、存储等数据/信息类功能。
所需牌照	增值电信业务经营许可证
外资准入限制	在**上海自贸区内**外资比例可达**100%**（企业注册地和服务设施均需在上海自贸区内）[15]；在**上海自贸区外**外资比例不超过**50%**
6. 互联网地图服务	
典型应用场景描述	用户直接利用车载端软硬件，在车载端可显示的地图上实现地理位置定位、地理信息标注等功能。
业务符合性要点	（1）服务提供商必须是地理位置定位、地理信息上传标注、地图数据库开发等“互联网地图服务”[16]的提供者； （2）该项服务的提供必须以车载端软硬件所收集和提供的GPS数据等地理位置信息为基础； **（3）尽管如此，特别值得注意的是，汽车生产企业在车载端预装可采集地理位置信息的硬件如GPS模块等，或者汽车生产企业借助该等硬件或辅助软件，收集车辆地理位置信息并通过互联网进行传输、存储等，该等行为本身并不足以使汽车生产企业被认定为提供了互联网地图服务；只有当这些地理位置信息被汽车生产企业与其所掌握或开发的地图信息相结合，并由其以可在地图上标显的方式反馈给用户，使得用户可以实现定位、导航等功能时，汽车生产企业自身才构成提供互联网地图服务；而作为当前车联网最主要的应用场景之一，汽车的车载导航功能所用到的互联网地图服务，往往是由有资质的第三方互联网地图服务提供商所提供的，而非由汽车生产企业自行提供。**
所需牌照	测绘资质证书[17]
外资准入限制	外资比例不超过**50%** [18]

[12] 参见《电信业务分类目录（2015年版）》第B24项。

[13] 参见《工业和信息化部、上海市人民政府关于中国（上海）自由贸易试验区进一步对外开放增值电信业务的意见》之二（二）。

[14] 参见《电信业务分类目录（2015年版）》第B23项。

[15] 参见《工业和信息化部、上海市人民政府关于中国（上海）自由贸易试验区进一步对外开放增值电信业务的意见》之二（一）。

[16] 参见《地图管理条例》第三十三条。

[17] 参见《地图管理条例》第三十三条。

[18] 参见《外国的组织或者个人来华测绘管理暂行办法（2011修正）》第八条第二款第（三）项。

三、给汽车生产企业的路径选择提示

对于汽车生产企业而言，在产品的最前端生产环节就开始进行车联网业务的布局，例如开发为其产品专门定制的品牌化服务，并直接在车载端完成相关配套软硬件的安装调试，对于增强其产品的竞争力和市场差异化、打造用户更为依赖的闭合车联网生态系统、维护和增加其品牌价值和吸引力、保护其核心技术和知识产权等，都是十分有利的。而市场上已经有车企开始这样做。给汽车生产企业的路径选择提示

在此情况下，鉴于上表所列的牌照及外资准入限制要求，车企特别是在华外资车企在进行该等车联网业务的布局时，自然就会面临两条不同的路径选择，即在法律所允许的范围内自行投资并从事相关业务，或是与有资质的第三方服务提供商开展合作。就该项选择，除了必须要考虑成本、知识产权保护、合作伙伴选取乃至企业整体发展战略等商业因素之外，至少还应纳入对以下两方面法律监管因素的评估和考量：

1. 准入环节所面临的监管门槛。这不仅包括外资车企就具体业务所面临的外资准入限制乃至禁止，还包括所有车企想要申领相关牌照都必须满足的其他一系列资质要求，例如申请增值电信业务经营许可证所要求的人员、服务设施、技术方案、信息安全保障措施等诸多方面的条件。

2. 运营环节所面临的信息安全保护义务。以《网络安全法》的出台为重要标志，我国正在不断加强对网络个人信息和数据的保护，相应地，包括网络服务提供者在内的网络运营者也在面临不断加大的信息安全保护义务。而上表所列出的车联网数据/信息类核心业务无一例外都落入网络服务的范畴，因此其提供商在日常运营中必然将直接受制于此类信息安全保护义务。

据此，对于车企来说，在判断难以满足相关牌照申领要求、或者不想让自己承担过重的信息安全保护义务的情况下，与有资质的第三方服务提供商合作，由其直接向用户提供相关服务，显然是一种更为合理的选择。反之，即便决定自行从事相关业务，车企也仍需要进行更为详尽的和符合个案的法律评估；而如果车企意欲涉足的车联网业务已经超出本文所重点讨论的数据/信息类核心业务的范畴，则还将有必要对相应监管要求和合规。

（本文发布于2017年05月25日。）

蹴鞠场边万人看，秋千旗下一春忙
——体育运动信息的利用、发展和法律保护

“蹴鞠场边万人看，秋千旗下一春忙”，全球体育事业正处在高速发展的时期，体育大数据的应用，尤其是在竞技体育中的使用不仅加速发展进程，甚至有可能颠覆竞技体育的形式和规则。体育大数据在运动员选材、赛事数据分析、结果预测等方面发挥日益重要的作用，将促使体育大数据迎来广泛应用的“春天”。与此同时，对于个人主体信息权利的保护，也是目前我国乃至于全球在数据立法中的重点关注领域。体育行业由于其实践的特殊性，在运动员及其他相关体育运动信息收集、使用，以及信息的权利归属等方面都体现出了不同于一般个人信息保护的行业特性，如何在保障运动员个人信息与隐私的同时，实现对体育组织、赛事组织的正当利益的维护，并进一步挖掘与提升体育大数据的商业价值，是我们未来需要持续关注的话题。

体育运动信息种类繁多，可以泛指为涵盖在各种运动语言文字、图像、影像中的可以反映体育运动事物和特征的各种信息。本文中的体育运动信息，特指体育运动中运动员、教练员训练和参赛过程中形成的相关信息。随着大数据采集、预处理、存储和分析技术的进一步提高和在竞技体育领域内的广泛使用，特别是一些科技产品通过采集并分析运动员、教练员在日常训练和参加比赛的过程中的身体、语音等数据可以达到提高甚至预判运动员体能和赛时成绩的效果，这些产品的合规开发与应用,不仅涉及到运动员、教练员个人信息保护，还涉及相关信息的权利归属、信息安全等一系列有待法律规制和明确的问题，我们逐步展开讨论。

一、体育运动信息的采集类别和采集方式

（一）我国国家队训练数据的采集

2018年，国家体育总局发布了《体育总局科教司关于加强国家队训练数据和信息规范管理的通知》（体科字〔2018〕135号），文中提出重视和加强各国家队训练数据和信息的采集、存储和管理，是当前提高科学训练质量和科技助力效果的迫切需要，并明确了国家队训练数据的采集类别和指标如下：[1]

序号	数据分类	指标描述
1	运动员基本信息	姓名、性别、籍贯、民族、出生年月、运动项目、运动等级，初始训练时间，启蒙教练，省队教练，国家队教练，历年国内、国际参赛成绩和相关比赛数据，获得的各类奖励和荣誉，等。
2	运动员来源单位信息	单位名称、法定代表人、统一社会信用代码、单位地址、联系人及联系方式，等。
3	训练计划和执行情况	训练计划包括：国家队各组年度计划、阶段计划和周计划，执行情况，运动员训练计划完成质量评分，等。

[1] 参见《体育总局科教司关于加强国家队训练数据和信息规范管理的通知》（体科字〔2018〕135号），国家体育总局，2018年11月7日。

序号	数据分类	指标描述
4	训练过程机能指标监控情况	包括日常监控和过程监控两部分。日常监控包括国家队各组机能监控年度、阶段和周测试计划，国家队各组运动员每次生理生化监控数据，如血常规、血尿素、免疫球蛋白、血氧饱和度、晨脉，等。根据测试结果提出意见和建议。过程监控针对不同训练阶段（如冬训、夏训、赛前）的具体安排，记录训练负荷量（如训练时间和距离）和强度（如速度、频率和强度分级），动态观察训练负荷变化，并采用血乳酸、心率、血尿素、肌酸激酶、睾酮、皮质醇、铁蛋白和免疫球蛋白等指标阶段性评价训练负荷，分析训练负荷特征，完成分析报告，提出改进措施。
5	各类训练指标（体能、专项能力和专项成绩）的测试、测验情况	国家队运动能力的测试、测验项目和计划，运动员在国家队内部组织的各类体能测试、专项能力测试和专项测试成绩及排名，等。
6	运动员技、战术诊断与分析	国家队年度及阶段技、战术诊断和分析计划，每次技、战术诊断和分析的各类指标参数及结果（生物力学分析、动作捕捉、视频剪辑分析），教练组和相关技术专家评议意见及后续改进措施，下一次测试结果及改进效果评估，等。
7	运动员大赛选拔相关数据	国家队参加国际大赛的选拔办法、标准及积分排名办法，国家队选拔测试（比赛）的项目指标和实测数据，选拔内部排名，人选确定程序及文件公示，等。
8	运动员伤病及康复	国家队运动员伤病情况调查，治疗方案及效果，康复训练计划及实施效果，等。
9	运动膳食及营养管理	计算能量消耗，制定营养食谱，运动员就餐统计及摄入、消耗计算，基于体重和体脂百分比动态监控的评估效果，等。
10	科技攻关项目的数据管理	各科技助力攻关项目申报立项书，各攻关项目预期结果及时间节点，推进情况评估分析，以及攻关项目推进过程中的所有测试数据，等。
11	国家队参赛总结管理	国家队参加每次国际比赛的训练参赛总结，教练员、运动员、科研、医务、体能等各组提交的总结分析，等。
12	国际信息情报	主要对手备战情况信息，主要对手体能、技战术和比赛数据收集汇总，规则变化，国际新技术、新手段、新方法跟踪，等。

从上表中可以看出，我国国家队训练数据和信息既包括运动员姓名、肖像、隐私、生理指标等信息，又包括其在相关体育项目中体能、运动习惯、身体条件、训练情况、技术特征、运动轨迹以及国家队比赛情况总结、主要竞争对手备战参赛情况等等。

考虑到体育运动信息的类型多样，其可能具有多重属性，需满足不同法律法规的要求。例如，对于运动员身体状况、病例信息、DNA等信息的采集，可能同时触发我国有关个人信息、重要数据、人口健康信息甚至人类遗传资源信息的法律法规要求；国家队的训练、参赛情况，涉及国家队运动员训练计划、参赛战术等涉及到国家秘密信息收集和保护的问题；竞争对手的参赛情况、训练数据的收集也涉及到如何合规获取此类信息的问题。

（二）比赛数据的采集——以奥运会等国际大型赛事为例

国际性的体育赛事在组织筹办和商业运作的过程中，因涉及不同国籍的参赛成员（运动员、辅助人员等）、志愿者和媒体的信息注册，以及向观众提供票务、餐饮、住宿服务等市场运营行为，均无法避免对个人信息的收集与处理。

2018年平昌冬奥会中，在参赛运动员向国际单项运动协会申报参赛的报名表中，即包含运动员的体育运动信息采集的归属问题的约定。申请表第二项要求运动员对个人数据的采集与使用作出承诺：

“个人数据处理：2018年平昌冬奥会、国际奥委会和韩国当局需要访问某些信息，尤其是为了确保2018年奥运会赛事的安全、管理认证、比赛和成绩，进行反兴奋剂工作、防止操纵比赛并向参赛者和媒体提供服务。

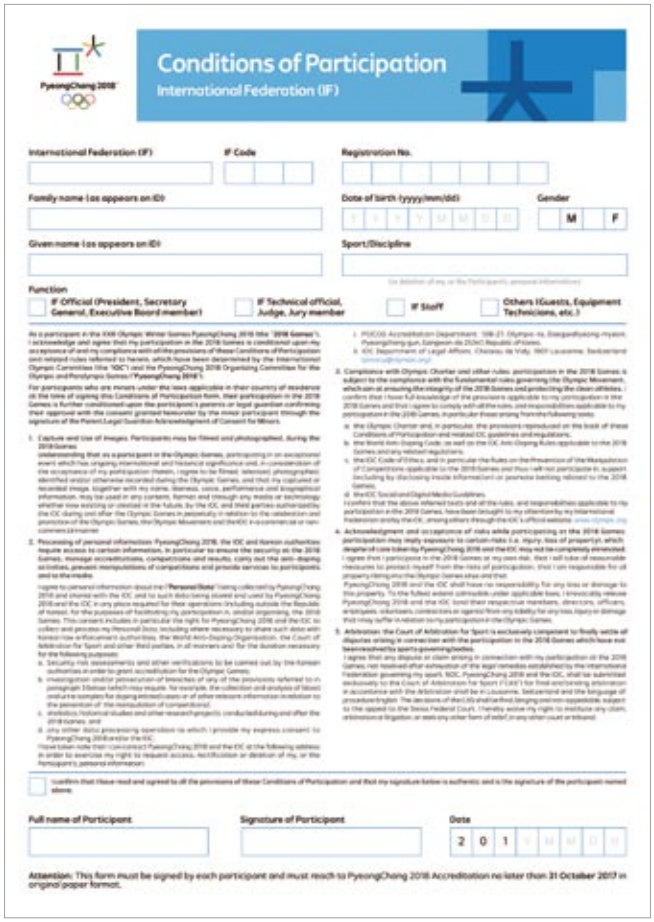
参赛者同意：本人个人数据，由平昌奥组委收集并与国际奥委会共享。平昌奥组委及国际奥委会存储、使用的此类数据，可因运营所需在任何地方（包括韩国以外的地区）进行存储、使用，以方便本人参与和（或）筹办2018年奥运会。本同意书特别同意平昌奥组委和国际奥委会采集和处理本人的个人数据，并允许其在需要时与韩国执法部门、世界反兴奋剂组织、国际刑事法院、国际体育仲裁院分享相关数据以必要的方式分享本人的数据：

a. 韩国当局为授予认可奥运赛事进行的安全风险评估和其他核查；

b. 调查和（或）起诉违反以下任何规定的行为，包括但不限于反兴奋剂工作的血样、尿样检测等等；

c. 在奥运赛事期间或之后进行数据统计、历史研究和其他研究项目；

d. 参赛者明确同意平昌奥委会和国际奥委会进行任何其他的数据处理操作。”



Conditions of Participation

International Federation (IF)

International Federation (IF) | IF Code | Registration No.

Family name (as appears on ID) | Date of birth (yyyy/mm/dd) | Gender

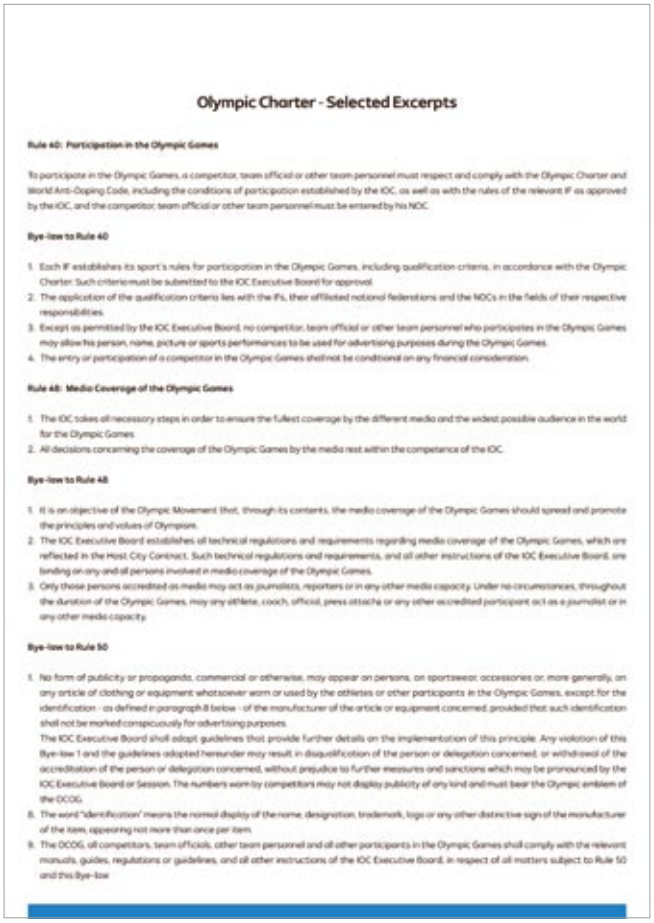
Given name (as appears on ID) | Sport/Discipline

Function

IF Official (President, Secretary General, Executive Board member) | IF Technical official, Judge, Jury member | IF Staff | Others (Guests, Equipment Technicians, etc.)

Full name of Participant | Signature of Participant | Date

Attention: This form must be signed by each participant and must reach to PyeongChang 2018 Accreditation no later than 31 October 2017 in original paper format.



Olympic Charter - Selected Excerpts

Rule 40: Participation in the Olympic Games

To participate in the Olympic Games, a competitor, team official or other team personnel must respect and comply with the Olympic Charter and World Anti-Doping Code, including the conditions of participation established by the IOC, as well as with the rules of the relevant IF as approved by the IOC, and the competitor, team official or other team personnel must be entered by his NOC.

Bye-law to Rule 40

1. Each IF establishes its sport's rules for participation in the Olympic Games, including qualification criteria, in accordance with the Olympic Charter. Such criteria must be submitted to the IOC Executive Board for approval.
2. The application of the qualification criteria lies with the IFs, their affiliated national federations and the NOCs in the fields of their respective responsibilities.
3. Except as permitted by the IOC Executive Board, no competitor, team official or other team personnel who participates in the Olympic Games may allow his person, name, picture or sports performances to be used for advertising purposes during the Olympic Games.
4. The entry or participation of a competitor in the Olympic Games shall not be conditional on any financial consideration.

Rule 48: Media Coverage of the Olympic Games

1. The IOC takes all necessary steps in order to ensure the fullest coverage by the different media and the widest possible audience in the world for the Olympic Games.
2. All decisions concerning the coverage of the Olympic Games by the media rest within the competence of the IOC.

Bye-law to Rule 48

1. It is an objective of the Olympic Movement that, through its contents, the media coverage of the Olympic Games should spread and promote the principles and values of Olympism.
2. The IOC Executive Board establishes all technical regulations and requirements regarding media coverage of the Olympic Games, which are reflected in the Host City Contract. Such technical regulations and requirements, and all other instructions of the IOC Executive Board, are binding on any and all persons involved in media coverage of the Olympic Games.
3. Only those persons accredited as media may act as journalists, reporters or in any other media capacity. Under no circumstances, throughout the duration of the Olympic Games, may any athlete, coach, official, press attaché or any other accredited participant act as a journalist or in any other media capacity.

Bye-law to Rule 50

1. No form of publicity or propaganda, commercial or otherwise, may appear on persons, on sportswear, accessories or, more generally, on any article of clothing or equipment whatsoever worn or used by the athletes or other participants in the Olympic Games, except for the identification - as defined in paragraph 8 below - of the manufacturer of the article or equipment concerned, provided that such identification shall not be marked conspicuously for advertising purposes.
The IOC Executive Board shall adopt guidelines that provide further details on the implementation of this principle. Any violation of this Bye-law 1 and the guidelines adopted hereunder may result in disqualification of the person or delegation concerned, or withdrawal of the accreditation of the person or delegation concerned, without prejudice to further measures and sanctions which may be pronounced by the IOC Executive Board or Session. The numbers worn by competitors may not display publicity of any kind and must bear the Olympic emblem of the OCOG.
8. The word "identification" means the normal display of the name, designation, trademark, logo or any other distinctive sign of the manufacturer of the item, appearing not more than once per item.
9. The OCOG, all competitors, team officials, other team personnel and all other participants in the Olympic Games shall comply with the relevant manuals, guides, regulations or guidelines, and all other instructions of the IOC Executive Board, in respect of all matters subject to Rule 50 and this Bye-law.

此种在参赛者报名表中获得参赛者对于个人信息数据在各领域全面授权的操作方式，有国际奥委会和《奥林匹克宪章》、《主办城市合同》等奥运会重要文件的支持。根据《奥林匹克宪章》，国际奥委会是奥林匹克运动的最高权威并领导奥林匹克运动，奥运会是国际奥委会的专有财产，国际奥委会拥有与之有关的所有权利和数据。[2]国际奥委会在与主办城市及国家奥委会签订的合同中，规定了运动员数据归属及其收集、跨境传输的详细要求。

以2020年东京奥运会为例。2013年东京都政府、日本奥委会与国际奥委会签订《主办城市合同》第27条“奥运会信息和

[2] Host City Contract for the Games of the XXXII Olympiad in the year 2020-Tokyo: Preamble B : WHEREAS, according to the Olympic Charter, the IOC is the supreme authority of and leads the Olympic Movement, and the Olympic Games are the exclusive property of the IOC which owns all rights and data relating thereto, in particular, and without limitation, all rights relating to their organisation, staging, exploitation, broadcasting, recording, representation, reproduction, access and dissemination in any form and by any means or mechanism whatsoever, whether now existing or developed in the future, throughout the world in perpetuity.

知识管理”中明确约定：1、任何形式、存储介质或具有显性或隐性特质的数据均为国际奥委会的专有财产[3]。2、未经国际奥委会事先明确的书面批准，组委会和主办城市不得将此类内容提供给第三方[4]。3、而组委会和主办城市应当在国际奥委会的任何合理要求下免费共享，并确保在奥运会的筹划、组织、筹资、筹办过程中发挥关键运营作用的相关政府当局、第三方服务提供商和赞助商，向国际奥委会免费提供其有关奥运会的筹划、组织、筹资、筹办过程中的所有信息、知识和专门知识，其中包括参赛者信息。[5]

2022年北京冬奥会签署《主办城市合同》的时间较早，其规定的奥运信息和知识管理的内容与东京2020奥运会相似，并额外强调了国际奥委会对主办城市、国家奥委会和奥组委在赛事筹办过程中采集的信息及其相关权益、冠名、利益，享有永久的专有权。同时，要求组委会应当在信息采集过程中确保取得所需的授权和权益，以保证国际奥委会可以在奥运赛事后仍可以使用或授权第三方使用相关信息。[6]

二、我国国家队运动员体育运动信息的权利归属

在我国运动员加入国家队之前，各个运动协会或管理中心会与该运动员签署有关运用运动员肖像、姓名、声音等以及其他与运动员人格和身份有关的各种标识进行统一商业推广和宣传的商业开发合同，获得运动员的相关授权进行统一的保护和使用。

但也应注意到，目前我国运动管理机构对于运动员体育运动信息的使用和保护尚未形成完整的体系，大多采取运动员同意的方式进行采集，这一做法与奥运会中采集体育运动信息的方法基本一致。但在国际体育运动信息保护领域，仍有许多做法值得借鉴。

三、奥运会体育运动信息使用和保护方式的发展

自欧盟制定的《一般数据保护条例》（General Data Protection Regulation， GDPR）于2018年5月25日生效后，其超严格的数据保护标准，对体育领域国际赛事和各国体育数据保护的影响不容忽视。奥运会作为全球性顶级体育赛事更是第一时间响应。在国际奥委会为2026年第25届冬奥会候选城市准备的《主办城市合同-原则》与其在2018年6月更新的《主办城市合同-操作要求》中，明显提高了对数据保护的重视。

在《主办城市合同-原则》中，国际奥委会增列了第32条“数据保护”条款。增加了对组委会和主办城市收集、使用和处理运动员信息的规范性要求。要求主办城市、国家奥委会和组委会在履行《主办城市合同》之义务时，在信息注册、交通、食宿、反兴奋剂和医疗、赛事科技、票务、火炬传递和数字媒体等领域，需要处理赛事相关者的个人数据，应当仅出于履行《主办城市合同》义务之目的处理此类个人数据，并遵守所有适用的数据保护法律法规。[7]

新的《主办城市合同》还要求，主办城市、国家奥委会、奥组委承诺配合国际奥委会处理所有赛事相关者的个人数据，包括：（1）将所有隐私政策、数据使用条款或类似的合同条款提交国家奥委会事先书面批准；（2）与国际奥委会签订数据处理、数据共享或类似的合同以确保在履行《主办城市合同》时合法合规的处理赛事相关方的个人数据；（3）应要求为国际奥委会履行数据保护法规时提供必要的帮助；（4）确保在数据保护法规允许的最大范围内，使国际奥委会可以免费使用各个领域赛事相关方的个人数据。[8]

同时，在2018年6月更新的《主办城市合同-操作要求》中在奥运赛事筹办的各个环节还增列了对数据保护的诸多细节，[9]也为北京2022冬奥会的数据保护工作提出了新的要求。

从上述情况可知，奥运会通过《奥林匹克宪章》、《主办城市合同》、《主办城市合同-原则》、《主办城市合同-操作要求》等系列条约和协议，建立了多层级、全领域的赛事利益相关方的数据使用与保护体系。

结合奥运会对体育运动信息的使用与保护，回到我国现状，考虑到现有单层次的运动员“同意”很难作为我国运动管理机构

[3] Host City Contract for the Games of the XXXII Olympiad in the year 2020-Tokyo: 27.c).

[4] Host City Contract for the Games of the XXXII Olympiad in the year 2020-Tokyo: 27.d).

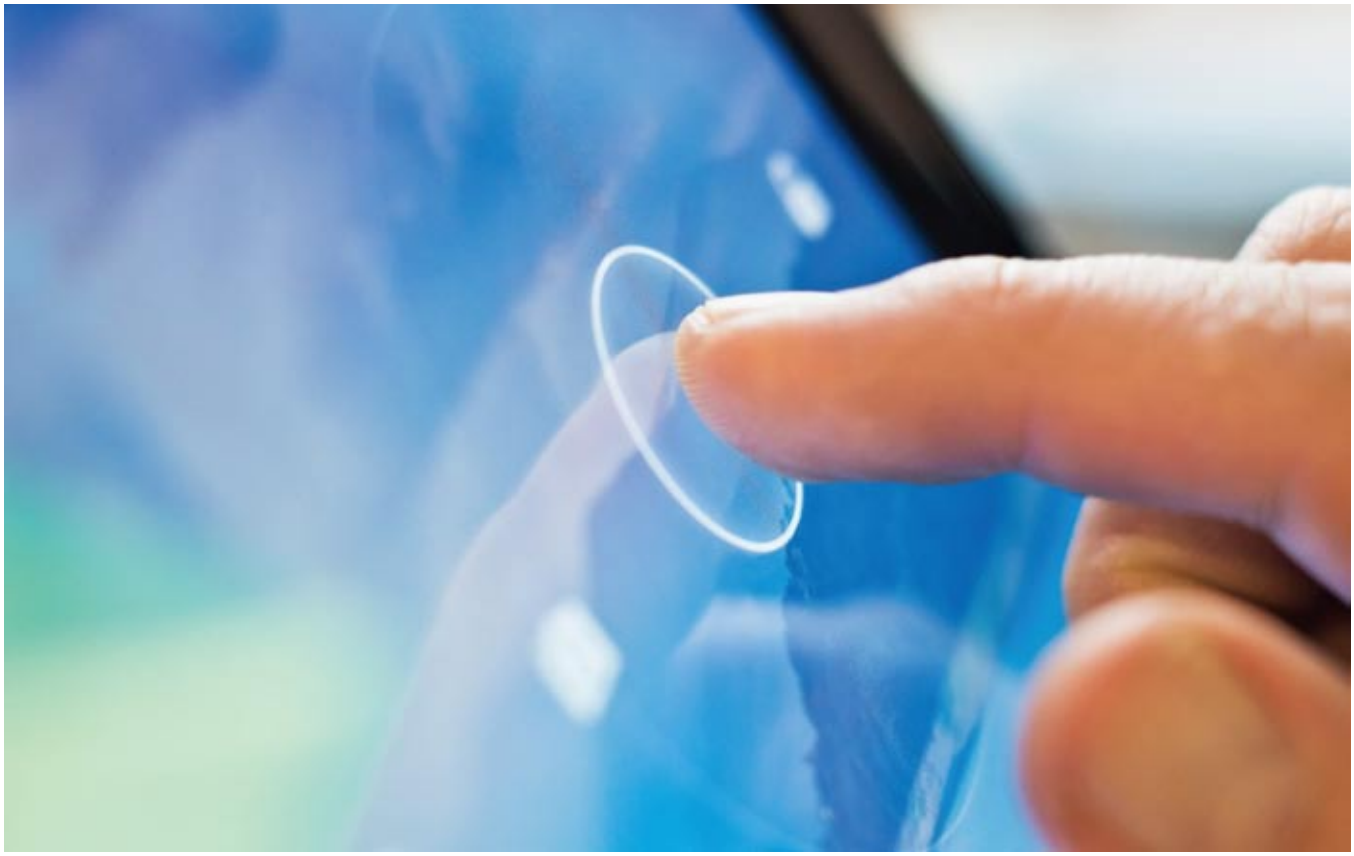
[5] Host City Contract for the Games of the XXXII Olympiad in the year 2020-Tokyo: 27.c).

[6] Host City Contract for the Games of the XXIV Olympiad Winter Games in the year 2022: A 28.

[7] Host City Contract for the Games of the XXV Olympiad Winter Games in the year 2026，A 32.1.

[8] Host City Contract for the Games of the XXV Olympiad Winter Games in the year 2026，A 32.2.

[9] Host City Contract - Operational Requirements, 2018.6.



越来越多层次、全方面使用体育运动信息的合规依据，恐也将为在运动员训练及商业开发中使用体育运动信息带来许多困难。我们初步认为，合理区分运动员体育信息的不同类型，考虑建立多层次的运动员体育信息授权体系，设立体育运动信息的数据保护措施，是我国体育管理机构的“数字体育”、“科技体育”发展的必然之势。

四、 体育大数据的合法合理应用和分析

（一）体育信息的存储和安全保护

随着大数据技术在竞技体育方面的应用逐渐深入，体育运动信息的价值也受到越来越多的重视与认可，但与之相对应地，体育信息的存储和安全保护也面临着更大的挑战。2015年6月，美国司法部门曾宣布将着手调查美国棒球联盟中某球队涉嫌入侵竞争对手网络数据库，获取对手球队信息和交易信息事件，[10]2019年，某欧洲足球队工作人员在社交媒体上泄露球队信息而被球队开除……前述信息泄露事件及其所带来的严重后果反映了重视体育信息存储和安全保护的必要性。

首先，从个人信息和隐私保护角度而言，尽管由于体育行业的特殊实践，运动员“通过个体的协商，同意或拒绝……对数据的收集和利用”[11]可能存在障碍，但对个人信息主体（即运动员）信息自决权的限制并不能因此免除球队、赛事组织方、其他第三方数据收集和使用者对通过合法方式取得的运动员个人信息的存储和安全保护义务。因此保障体育信息存储安全并建立必要

[10] 参见《大数据是数字体育营销的优势所在，但谁来照顾隐私？》，载https://m.jiemian.com/article/530534.html，2016年2月3日。

[11] 参见徐伟康、徐艳杰、郑芳：《大数据时代运动员数据的法律保护》，《天津体育学院学报》2019年34卷第5期，第456-460页。

的安全保护措施是相关主体应负的合规义务。

其次，除个人信息安全义务外，体育运动信息的存储和安全保护还可能与隐私保护、商业秘密、体育竞技道德规范等密切相关。鉴于存储的体育信息中并不仅限于运动员的个人信息和隐私，还可能包括球队信息例如球队的首发阵容、战术战略等非个人信息或隐私内容，对于这类信息，个人信息或隐私保护能够提供的合法性支撑相当有限；此外，隐私的侵权通常需要以“公开”和“造成他人损害”[12]为要件，但在大数据体育的语境中，非法获取体育运动信息的第三方（特别是竞争对手或者数据分析公司），往往并不需要公开所获取的运动员隐私信息，而是通过对数据进行分析，用于作为之后的比赛参考依据或用于获取非法利益，很难以隐私侵权要求其承担相应责任。但另一方面，在符合相关要件的情况下，这类信息可能在特定的时点被认定为商业秘密，同时以非法方式获取上述信息还可能被认定为有碍体育竞技的公正性、违背行业规范与道德。

就体育运动信息存储与安全保护实践而言，除因网络攻击导致的信息泄露外，内部人员泄密也是导致体育信息泄露的最主要原因。对于后者，可以考虑通过采取去标识化的前端数据展示、访问权限控制、保密义务约束等方式降低信息泄露的风险。例如，对于某些体育训练中应用训练数据实时采集设备与分析系统的场景，可以考虑对前端训练数据和实时结果进行合理的去标识化展示，以降低数据直接泄密的风险；同时对于访问结果数据库的人员进行差异化访问权限控制，包括特殊数据库的双因素或多因素认证，批量下载、导出数据的特殊审批流程等；除此之外，还可以通过员工保密协议、员工手册以及保密奖惩规定等方式约定员工应负的保密义务，并鼓励对泄密行为的监督与举报等，以进一步降低员工泄密的可能性。

（二）比赛数据实时分析及科技仪器应用对于公正性的挑战

除了前述的体育信息的存储与安全保护，大数据下数据实时分析技术在竞技体育中的应用还带来了另一项挑战——比赛的公正性。事实上，对比赛数据的收集，分析赛事情况和竞争对手的比赛习惯等，并用于调整运动员的战术安排，抓取获胜关键的实践并非是近期才出现的。早在2005年，某知名互联网巨头就利用应用软件追踪了“网球四大满贯赛事的8000多场比赛，每场比赛收集了4100万个数据点，包括5500多个分析模型”并总结“制胜关键指标（Key to the Match）”。[13]“美国四大联盟[14]中雇佣体育数据分析师的球队比例分别为97%，57%，80%和23%”。[15]除此之外，对此前体育比赛的视频回放、关键数据点的提取和竞争对手的分析等早已成为竞技体育中普遍应用的策略；竞技体育的各方利用自有的数据能力和科技能力，以更好地实现对数据的分析和评估似乎无可厚非。

但是当数据实时分析技术的发展意味着在比赛过程中，双方或其中一方可以通过对比赛数据的收集和实时处理反馈数据分析结果，包括对当场比赛中运动员的竞技状况、运动员行为的分析及影响概率、乃至于比赛方案和战略布局的推荐等[16]内容，又不免引起追问——这类科技的引入和应用是否会造成本场比赛的非公正情况，违背了竞技体育的初衷？举例而言，在传统棒球比赛中，利用二垒接球跑者肉眼观察对方捕手暗号以通知本队打者和教练席已成为比赛中的常见行为，[17]但球队使用摄像机专业用于

[12] 参见《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》第十二条 网络用户或者网络服务提供者利用网络公开自然人基因信息、病历资料、健康检查资料、犯罪记录、家庭住址、私人活动等个人隐私和其他个人信息，造成他人损害，被侵权人请求其承担侵权责任的，人民法院应予支持……

[13] 参见马国全、杨建文、张虎祥、田宇：《大数据在体育科学中的应用及思考》，《河北体育学院学报》2015年第2期，第11-16页。

[14] 美国职业棒球大联盟（MLB）、美国职业橄榄球联盟（NFL）、美国职业篮球联盟（NBA）、国际冰球联盟（NHL）。

[15] 宋昱：《基于区块链的体育大数据集成与传播创新研究》，《成都体育学院学报》2018年第6期，第61-67页。

[16] 参见杨春然：《论大数据模式下运动员隐私的保护》，《体育科学》2018年第2期，第82-90页。

[17] 参见罗骢：《美国职棒联盟比赛发生作弊事件，工具是Apple Watch》，载http://www.qdaily.com/articles/44899.html，2017年9月6日。

拍摄对方捕手的暗号手势，或通过高科技设备加速传递捕捉到的暗号信息[18]的行为则最终被认定为引发了对比赛公正性的怀疑，并对结果造成了损害。美国职棒大联盟主席评价这类“作弊”行为称“这种行为已经引发了其他球队球员、管理阶层、球迷以及媒体怀疑比赛的公正性。尽管无法认定这些作法对比赛结果的实际影响有多大，但某种程度的确对比赛造成重大伤害”。

由此观之，依托于科技设备和数据实时分析技术的大数据体育在提高竞技体育的训练效率、提升体育训练与比赛胜率的同时，也必须要回应其可能引发的公正性质疑，而究竟二者的边界在何，可能还需要结合更多有关大数据体育实践、体育伦理等内容进一步探讨分析。

（三）大数据分析的准确性和数据主体权益救济

除了在竞技比赛中的直接运用，体育大数据还可能应用于对运动员先天条件、身体素质的评估与选拔过程中，又称“选材”[19]。例如，“美国职业棒球队大联盟奥克兰‘运动家球队’的总经理比利·比恩（Billy Beane）”摒弃了传统的击球率作为球员选拔标准，通过大数据分析最终确定了“上垒率”与比赛胜负之间的关联，并以此作为球员选拔的依据最终“在2002年的美国联盟西部赛事中夺得冠军”[20]。相比于传统的选材逻辑，大数据分析的方法允许在评估过程中暂时跨越复杂的因果关系，直接建立从数据到结论的关联性，[21]使得人们更有能力发现一些可能超出常规理解以外的关联关系，并以此作为选拔适当的运动员人才、提升训练效率的依据。

但另一方面，对因果关系的跨越意味着大数据分析的结果很难通过因果关系进行论证。同时由于在大数据计算特别是深度学习模式下，还存在算法透明度和可解释性方面的技术障碍，数据分析的准确性和可信赖性可能因此而受到损害。而如果该种结果被作为决策的决定性依据，还将可能给相关的个人造成权益上的损害。例如，2014年法国足球运动员卢瓦克·雷米曾因未能通过体检而错失转会利物浦俱乐部的机会，究其原因是俱乐部将其“病例、日常信息与其过去比赛、训练有关的大数据”结合分析并得出“其心脏存在着异常的结论”[22]；但“利物浦委托的心脏专家和医生都认为，雷米的情况并不影响其参加高水平的比赛”[23]。在这种情况下，应当认为大数据的分析是雷米错过转会机会的重要乃至于决定性因素。

就体育大数据场景而言，保障相关个人信息主体对不利决定的知情权，以及自动化决策结果的申诉权可能对于大数据结果的准确性和个人权益的维护至关重要。具体而言，参照美国在《公平信用报告法》（Fair Credit Reporting Act）[24]中的不利决定告知要求（即要求信用报告的使用者在部分或全部基于信用报告而做出不利于消费者的决定时，应当通过口头、书面或电子方式通知消费者并告知相关的信息），[25]在部分或全部基于大数据体育数

---

[18] 前引17。

[19] “科学选材是根据不同运动项目的特点和要求，用现代科学的手段和方法，通过客观指标的测试，全面综合评价和预测，把先天条件优越、适合从事某项运动的人才从小选拔出来，进行系统培养，并且不断地监测其发展趋势的一个过程”，参见：余竹生、沈勋章、朱学雷：《运动员科学选材》，上海中医药大学出版社，2006年；转引自马国全、杨建文、张虎祥、田宇：《大数据在体育科学中的应用及思考》，《河北体育学院学报》2015年第2期，第11-16页。

[20] 前引13。

[21] 前者需要在回答“为什么”的基础上确定选材标准；而后者则可以直接通过对“是什么”的客观实践的分析与总结，选择合适的人员。

[22] 参见杨春然：《论大数据模式下运动员隐私的保护》，《体育科学》2018年第2期，第82-90页。

[23] SIMON Y. Harry Redknapp shock at Loic Remy's Liverpool medical mystery[EB/OL]. http://www.express.co.uk/sport/foot-ball/493019/Harry-Redknapp-s-shockat-Loic-Remy-s-medical-mystery.

[24] 15 U.S.C. §1681.

[25] 15 U.S.C. §1681(m)(a) "if any person takes any adverse action with respect to any consumer that is based in whole or in part or any information contained in a consumer report, the person shall (1) provide oral, written, or electronic notice of the adverse action to the consumer; (2) provide to the consumer written or electronic disclosure (A) of a numerical credit score as defined in section 1681g(f)(2)(A) of this title used by such person in taking any adverse action based in whole or in part on any information in a consumer report; and (B) of the information set forth in subparagraphs (B) through (E) of section 1681g(f)(1) of this title…"

据分析结果做出不利于运动员等的决定时，决定的作出者也应当保障个人信息主体的知情权，包括但不限于不利决定的做出、主要的依据信息等。此外，我国GB/T 35273《信息安全技术 个人信息安全规范》[26]及欧盟《通用数据保护条例》（“GDPR”）中还对信息系统自动决策机制的使用加以规范，包括但不限于“向个人信息主体提供针对自动决策结果的投诉渠道，并支持对自动决策结果的人工复核”[27]。类似地，对于在体育领域广泛应用大数据技术并将大数据分析结果作为有关决定作出的重要或唯一根据的场景中，不妨参考借鉴以上对个人信息主体的知情权和申诉权的保障机制，以进一步保障大数据分析的透明度、提升分析结论的准确性并维护相关个人信息主体的权益。

（四）与第三方大数据分析公司的安全、合规与权益

大数据体育的发展对数据分析能力提出了更高的要求，从我国现有实践来看，第三方大数据分析公司是数据分析能力的主要提供者，运动员、体育管理者、赛事主办方等在开展大数据体育实践时，往往需要与第三方合作共享部分体育数据以完成数据的挖掘与分析。

从数据安全角度而言，数据分析平台的本地化部署与云平台模式之间的安全风险可能存在一定差异。同时，考虑到体育运动信息中包含个人敏感信息，特别是生理生化监控数据、伤病情况、就餐统计及摄入、消耗计算等内容，根据个人信息保护的法律框架，对该部分信息的共享和转让除须获得个人信息主体的同意[28]外，还需要满足必要原则[29]、个人信息安全影响评估[30]等相关要求。

另一方面，对于某些由体育组织与第三方数据分析公司合作开展的数据分析项目，双方对于原始信息的使用、基于原始信息训练的模型及模型输出的结果等权益及所附带的经济利益的固定、分配也同样是值得关注的问题。具体而言，第三方数据分析公司能够在何种范围内使用由体育组织、运动员等提供的原始体育运动信息？对于基于原始体育运动信息生成的衍生数据（derivative data），体育组织和第三方数据分析公司分别能够拥有何种权利？如何通过版权、商业秘密等手段对数据分析模型进行权益的固定与保护？如何通过对模型的使用和输出结果的权属分配实现双方之间的利益平衡？这些问题可能都需要体育组织与第三方数据分析公司在合法合规的前提下通过商业性的谈判与协商实现利益最大化与双赢的目标。

五、结语

随着体育大数据的发展，在竞技体育运动中体育运动信息在运动员选材、赛事数据分析、结果预测等方面发挥着越发重要的作用。与此同时，对个人信息保护的重视，也日益成为我国乃至于全球在数据立法中的重点关注领域。体育行业由于其实践的特殊性，在运动员及其他相关体育运动信息收集、使用，以及信息的权利归属等方面都体现出了不同于一般个人信息保护的行业特性，如何在保障运动员个人信息与隐私的同时，实现对体育组织、赛事组织的正当利益的维护，并进一步挖掘与提升体育大数据的商业价值，是我们未来需要持续关注的话题。

（本文发布于2020年03月17日。）

[26] 包括现行的GB/T 35273-2017《信息安全技术 个人信息安全规范》和将于2020年10月1日生效的GB/T 35273-2020《信息安全技术 个人信息安全规范》。

[27] GB/T 35273-2020《信息安全技术 个人信息安全规范》第7.7条c）项。

[28] 有关体育行业的授权同意的特殊性，请参见本文第二部分。

[29] 根据《网络安全法》第四十一条，“网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则……”

[30] 指“针对个人信息处理活动，检验其合法合规程度，判断其对个人信息主体合法权益造成损害的各种风险，以及评估用于保护个人信息主体的各项措施有效性的过程。”GB/T 35273-2020《信息安全技术 个人信息安全规范》第3.9条。

被操纵的“民主”
——欧盟GDPR首张执法通知的警示

宪政与民主，一直以来都是西方社会引以为傲的制度体系，公众投票的选择决定着整个社会的未来走向。然而，在大数据时代，当基于数据的“精准营销”不再局限于商业领域，而是用来影响选民政治偏好时，人们不禁心生疑惑：“我所投下的那一票，真的是我的自由意志（free will）吗？”

这一疑问在英国脱欧公投于2016年通过后彻底爆发，410余万英国公民在脱欧公投通过后发起请愿，质疑公投的有效性。随后，随着媒体曝光和英国信息专员办公室（Information Commissioner's Office，以下简称“ICO”）的介入，此次英国脱欧公投背后的种种纠葛逐渐浮现。随着英国脱欧后续一系列事件的发酵，全社会对个人数据价值和影响力有了新的认知。

2018年9月底，ICO公布了对加拿大AggregateIQ公司（AIQ）开出的执法通知（Enforcement Notice）。该执法通知是欧盟《通用数据保护条例》（General Data Protection Regulation，以下简称“GDPR”）生效以来的首张执法通知。随后，2018年10月24日，ICO更新的执法通知中，要求AIQ在配合完加拿大执法机构调查之后，于30天之内把所持有的英国个人信息删除。

该案在全球引发广泛关注。一方面，该案涉及剑桥分析（Cambridge Analytica）在脱欧公投中为Leave EU竞选团队提供选民数据这一重要事件，影响着英国和欧盟乃至全球的未来经济和政治走向；另一方面，该案所涉及的AIQ公司并非欧盟内企业，而是一家加拿大公司，而ICO基于GDDR域外适用相关条款对其进行处罚。

2018年5月25日，欧盟GDPR正式实施。在此之前，英国脱欧公投亦早已引发全世界的关注。不过，出乎所有人意料的是，这两件引发全球关注的重大事件，会因为英国ICO的一项调查而关联起来。

随着让世界惊讶的脱欧公投结果的公布，引发了对公投结果的有效性和公正性的质疑，410余万英国公民在脱欧公投通过后发起请愿，质疑公投的有效性，不少媒体纷纷爆料揭秘公投背后可能存在的黑幕。随后ICO果断介入开始调查，牵涉出Facebook、剑桥分析及其母公司SCL Election（“SCL”）、AIQ等多个相关方。其中，ICO针对AIQ发出的直接以GDPR为法律依据的执行通知成为了自GDPR正式实施以来备受瞩目的第一次出击。

一、英国人民是如何“被脱欧”的?

2016年6月24日，英国脱欧公投结果公布，支持脱欧选民（52%）超过了支持留欧选民（48%）。这一结果与公投前长期的民调相悖，不仅让英国前首相卡梅伦引咎辞职，也引发了大批公众和媒体对公投结果有效性和公正性的质疑。

2017年初，经媒体曝光，英国政治咨询公司剑桥分析（Cambridge Analytica）在脱欧公投中与Leave EU竞选团队合作，并为其提供有关选民针对性数据服务，大量投诉和证据被提交至ICO。随后，经初步证据评估，英国信息专员（Information Commissioner，以下简称“专员”）宣布ICO将就此事展开调查。

ICO调查的一个关键因素是剑桥分析与SCL、AIQ之间的联系和可能被滥用的数据，以及针对Facebook用户投放脱欧广告的行为。而此前，剑桥分析与Facebook之间的数据共享案例已另有论断。

剑桥分析与Facebook之间的数据纠葛早在2013年就已产生。彼时，剑桥大学的研究人员亚历山大•科根（Aleksandr

Kogan）在Facebook上开发了一款名为“this is your digital life”的应用，并获得了约27万用户。用户在使用这款应用时授权其获取社交关系及好友信息。基于授权，此应用通过Facebook的开放应用程序编程接口顺利获取了Facebook上近5000万人的用户数据，包括近一百万英国用户数据。随后，科根将这些数据共享给了剑桥分析，用于针对性的竞选广告推送。2015年Facebook得知后屏蔽了该应用，并要求科根和剑桥分析删除所有用户信息，但并未进一步跟踪和追究。

随着ICO调查的推进，2018年初，剑桥分析前雇员克里斯托弗•威利（Christopher Wylie）向英国议会与ICO作证指出，AIQ与剑桥分析的母公司SCL之间存在多年以来的合作关系，里斯托弗•威利表示，早在2014年，SCL即与AIQ合作开发了一款名为RIPON的软件，主要应用Facebook数据来确定选民的特征。

由于案情复杂、牵涉重大，ICO动用了超过40名调查人员全职投入本案，共认定了172个利益相关组织和285名相关自然人，并针对其中30个组织展开了正式调查，同时对约100名自然人展开了访谈、问询等正式会面。[1]根据付款信息、访谈结果等线索，调查团队发现了AIQ与剑桥分析和各个竞选团队之间的潜在关系。证据显示，大量数据从剑桥分析流向AIQ，AIQ再使用这些数据帮助政治竞选团队定向投送政治类广告。例如，在2016年6月23日的英国脱欧公投投票前，AIQ代表脱欧游说组织Vote Leave对Facebook上的电子邮件地址投放广告，以影响其在脱欧公投上的态度和投票决定。所有这些广告的付款均由SCL支付，这笔广告费在2016年4月15日至2016年6月23日期间约为200万美元。

截至目前，案件整体仍在调查过程中，而ICO基于掌握的事实已分别针对Facebook、剑桥分析及其母公司SCL、AIQ等多方采取了相应的执法行为。其中，针对AIQ发出的执法通知直接以GDPR为法律依据，而对Facebook等主体发出的执法文件均未明确以GDPR为法律依据。

二、ICO如何抽丝剥茧

从执法通知的结论来看，ICO已经初步认定AIQ违法获取并处理了英国公民的个人数据，并用于未经授权的定向政治广告推送等目的。由于涉及到英国脱欧等敏感政治行为，同时本案属于ICO和GDPR第一次共同应对欧盟以外的企业，ICO对AIQ的行为和角色进行了细致的认定，即便是在初步的执法通知中，也对执法对象、行为时间、适用法律、地域范围、数据使用行为、目的等多个要点一一进行了分析与论述。

从执法对象来看，根据GDPR和英国《数据保护法案》（DPA）的规定，“数据控制者”是指“能单独或与他人决定个人数据的处理目的和方式的自然人或法人、公共机关、部门或其他机构”，“该数据处理的目的及方法依照欧盟法或成员国法决定，数据控制者或数据控制者认定的具体标准可由欧盟法或成员国法律规定。”由于AIQ本身为一家以大数据分析为主要产品与服务的数据分析公司，在不考虑地域范围的前提下，以自身名义对外提供产品和服务，基于数据分析、政治广告定点推送等目的，收集相关主体个人数据并进行分析、处理，ICO认定其构成GDPR和DPA下的“数据控制者”。

从行为发生时间和法律法规实施时间来看，根据GDPR的相关规定，通常情况下其不具有溯及力。为此，在其正式实施前所发生的违法行为，ICO也仅依据了1998年的DPA作出执法决定。不过ICO亦指出，虽然所涉的个人数据是AIQ在GDPR生效之前收集的，但在新法规生效后，AIQ继续保留和处理相关个人数据，其非法处理行为一直在延续，因此可以适用新生效的GDPR。

从地域范围上看，由于时间上已能适用GDPR的规定，则根据GDPR第3条关于地域范围的规定，除与位于欧盟境内营业场所相关的个人数据处理行为将不分地域地受GDPR管辖以外，对设立于欧盟境外的数据控制者或处理者而言，在两种情况下仍可能受到GDPR的管辖，即：(a) 向欧盟内的数据主体提供商品或服务，无论是否需要付款；(b) 对欧盟境内数据主体行为的监控。[2]为此，虽然AIQ为一家设立于加拿大的数据分析机构，但由于其间接从Facebook上大量收集欧盟公民的个人数据，并对这些数据主体的行为喜好、政治偏向进行分析，最终定向推送政治类广告宣传，虽然这些广告宣传行为并不需要数据主体付款，但仍可构成服务的提供，从而导致受GDPR管辖。

从数据获取后的使用来看，AIQ代表脱欧游说组织Vote Leave对脸书上的电子邮件地址投放了218个广告，ICO调查后认为这些政治宣传广告目的的数据处理行为并未能够被证明已经取得数据主体的明确授权同意，因此认定AIQ的数据处理行为并不满足GDPR第5条关于数据处理合法性的规定。

基于前述分析，虽然ICO尚未掌握足够的证据以证明AIQ所获取的个人数据的具体来源和来源方，但基于现有调查结果和证据证明，ICO认为已足够认定AIQ违法获取、处理了英国公民的个人数据，并用于了未经授权的定向政治广告推送等目的。此外，2018年5月31日，AIQ向专员承认其仍然保存英国公民的个人数据，这些个人数据被存储在一个代码库中，此前一直受到第三方

[1] 参见ICO针对本案发布的中期调查报告：Investigation into the use of data analytics in political campaigns Investigation update, 11 July 2018。

[2] 参见GDPR第3条地域范围。

未经授权的访问。因此，基于执法通知，ICO要求AIQ在30天内停止其用于数据分析、选举宣传或其他宣传广告目的的、英国或欧盟公民的个人数据。不过，随后AIQ提出申诉，否认之前被指的、与剑桥分析之间的关系，主张其行为完全符合法律法规的要求，并未进行任何非法收集处理公民个人数据的行为，AIQ未曾从剑桥分析不正当获取的Facebook数据或数据库，也从未有过访问权限。2018年10月24日，ICO对执法通知进行了更新，要求AIQ在配合完加拿大执法机构调查之后，于30天之内把所持有的英国个人信息删除，若逾期未合规，AIQ将面临2000万欧元或全球营业额4%的罚款。

三、案例警示与展望

尽管本案中，ICO最终会向AIQ开出多少金额的罚单，仍然是一个未知数，但作为GDPR的第一击已经值得企业警惕，同时本案一定程度上也开启了GDPR活跃执法序幕，欧盟各国的数据执法机构相继开始实质性执法，比如2019年初法国数据保护机构CNIL向Google发出的5000万欧元罚单。

企业需要清楚的认识GDPR的执法实践已紧随其生效实施而逐步开展，条款规定中备受关注的域外适用效力和高昂罚则已初显威力。GDPR第3条关于地域范围的规定中，针对设立于欧盟境内的数据控制者或处理者，如符合“向欧盟境内数据主体提供产品或服务”或“监控欧盟境内数据主体行为”，则也受GDPR管辖。这使得即便企业在欧盟境内并未设立实体，也可能受到GDPR的规定影响。此外，最高可达全球营业额4%的高昂罚则，也迫使所有企业不得不重视GDPR带来的威慑力，曾经抱有的一丝侥幸，也被Google案中5000万欧元的罚款彻底击碎。

其次，对于企业而言，合法、合规的数据获取来源将毫无疑问地成为数据处理过程的重要合法性基础。个人数据的收集作为数据处理过程的开端，直接影响着数据处理全过程的合法性判断。本案中，AIQ后续的数据存储和使用过程很可能并未直接违反GDPR等数据保护法律规定，其申诉主张中也多次强调其行为完全符合法律法规的规定。然而，其数据来源的不合法和处理目的未经同意直接导致其从源头上无法满足GDPR的数据处理合法性前提，因此，合法合规的数据来源对企业而言无疑将成为数据处理以及数据合规的重要基础。

再次，不同司法辖区数据保护执法机构的跨境合作远比一般预期的密切。一般认为，由于非设立于欧盟境内的企业在欧盟并无实际可供各欧盟成员国数据执法机构接触、调查或限制的财产和营业场所，GDPR广泛的域外适用效力将大打折扣。然而，本案中ICO积极与加拿大数据监督执法机构展开配合，彼此共享信息，并通过加拿大数据执法机构向AIQ施压，迫使AIQ与其合作，并最终令AIQ承认违法数据处理行为。值得关注的是，执法机构间长效协作机制和跨境执法的开展仍有待进一步观察。

仍然值得强调的是，一套完善的内部制度与行为准则将为企业提供可靠的风险防火墙。本案中，诸多的证据均来自于涉案企业的雇员或前雇员行为，这些员工行为几乎被完整地视作了AIQ等企业主体的行为而被执法机构挑战。而一个完善的内部数据合规制度和行为准则则可能为企业提供足够可靠的风险隔离措施，例如我国“雀巢员工侵犯公民个人信息案”中，雀巢公司即依靠自身内部合规制度中明确禁止员工“以非法形式获取、使用个人信息”等类似规定成功与员工的个人行为之间进行分割，建立了风险防火墙，最终避免了员工个人行为被认定为企业行为的风险，成功地在刑事案件中抽身而退。对于大型企业而言，员工人数众多，统一不同员工涉及个人数据的行为存在客观困难，尤其是对于数据依赖型企业而言，员工为了获取可用的数据源，很可能出现无法顾及或不愿考虑数据合规性的情况，导致合规风险从不合格数据源向企业流转。因此，提供准确、合格的行为准则，建立责任完善的内部数据合规制度，将必然成为大型企业在数据合规工作中的重要组成部分。

最后，除了企业需要关注数据合规以外，作为每一个公民更要提高个人信息保护的意识。或许我们已经习惯接受个性化广告，享受定制化服务的便利，但我们是否意识到这些“个性化”及“定制化”的服务都基于对我们个人信息的挖掘和分析。如果“个性化”和“定制化”成为常态而且不被我们所知，我们不禁要怀疑，我所见的世界是真实的世界，还是商家想让我看到的世界？当这些精准的推广不仅仅在商业领域中应用，更被用于影响个人信息主体的潜在意识，则让人不寒而栗。“民主”是人类文明的骄傲，被认为是人类文明发展的基础。但一旦“民主”决定的基础来源于对个人信息主体潜移默化的影响，则被操纵的“民主”将带领人类文明去向何方？

小结

在互联网时代里，数据的价值和作用不容小觑。在众多数据类型中，个人数据是真实个人特征和行为的记录和反映，对于个人权利而言影响巨大。这样的影响不仅仅是通常受到人们关注的隐私问题和自主选择问题等，甚至也涉及到选举权利、政治独立和思维自主等作为人的基本权利。

个人数据的使用，小则可能影响个人生活便利，大则可能影响国家未来走向。正是如此，数据保护立法更加需要为个人主体权利提供足够的保护，以确保这类数据被合法、正当地使用。从ICO的这次执法活动中，我们也看到了数据保护法在个人隐私领域以外的更宽广和深层次的意义和价值。

不过，值得一提的是，正是由于个人数据可能有的巨大影响和作用力，其中的商业价值也同样合理保护和充分利用。为此，如何保护个人权利尚可能有一定的解决方案与回答，然而如何确保商业利益和个人权利的平衡，例如如何确保数据被合法地用于正确的用途，无疑仍然是一个巨大的挑战。

（本文发布于2019年04月。）

以技术为名，慷他人之慨？
——从爬虫谈数据权益

引言

网络的普及彻底改变了现代人的生活方式。从清晨到日暮，从商务工作到娱乐休闲，互联网的影响层层渗入、无处不在，其打破了空间的阻隔，跨越了时间的维度。在信息时代，一方面，人们在互联网上寻找、获取和接受着海量信息，享受着互联网带来的高效和快捷；另一方面，人们也在互联网上主动、积极地分享生活细节，发表看法、评论。

正如卞之琳在《断章》中所说：“你站在桥上看风景,看风景人在楼上看你。明月装饰了你的窗子，你装饰了别人的梦。” 网络的极强交互性使得你在浏览互联网上触手可及的信息的同时，你的信息也正在被分享、被使用、被分析。无论是出于记录生活、彰显个性、引起关注还是其他目的，这些被人们主动公开的数据借由互联网的互联互通的公开属性，能够便捷地被大量好友、关注者甚至是陌生人所浏览、阅读。

毋庸置疑，在大数据时代，各类信息蕴含着丰富的商业价值，一场围绕数据的竞争角力拉开帷幕并愈演愈烈，纷争也接踵而至。这些信息到底为谁所有、为谁所用，公平竞争规则又将如何界定?

有人将数据比作未来的石油，不难想象，数据背后的巨大价值将成为企业展开竞争的宝贵竞争资源。数据之战早已打响，而下文所讨论的大众点评网诉百度以及hiQ诉Linkedin两个案件则将争议核心聚焦于如何利用公开的用户数据。

有趣的是，在这场纷争之中，小小网络爬虫扮演着重要的角色... ...

在《夏洛的网》中，美国作家埃尔文·布鲁克斯·怀特为我们讲述了一只小小蜘蛛的温暖故事。这只名叫“夏洛”的蜘蛛虽然渺小，但却凭借自己的智慧和善良，通过谱写一张张爱的大网，成功拯救了他的好朋友小猪威尔伯的生命，最终自己的生命却走向了尽头。

随着我们步入互联网+时代，互联网正推动着各个行业不断发生变革，原有的社会经济结构被打破，人们的生活方式也因为互联网发生着日新月异的变化。而就在这张史无前例、覆盖全世界各个角落的巨大互联网之上，同样活跃着无数小小的“网络蜘蛛”。

网络蜘蛛（web spider），又称“网络爬虫”（web clawer），是一种按照一定的规则，自动地抓取万维网信息的程序或者脚本。网络爬虫如它的名字一般，爬行至网络的各个角落，抓取各类数据。

当然，网络爬虫的所行之处并不总是鲜花与掌声，网络管理者们对来路不明的爬虫随意抓取自己的数据往往心怀抵触。几乎是与爬虫技术诞生的同时，反爬虫技术也应运而生。除了技术的较量之外，随着互联网的发展，在爬虫的世界里于1994年萌生出了君子协议，即Robots协议（又称“爬虫协议”）。Robots协议现今是国际互联网界通行的道德规范，作为网络爬虫访问网站时要查看的第一个文件，网站通过Robots协议告知爬虫哪些页面可以抓取，而哪些页面则“闲人免进”。在互联网的世界中，Robots协议“防君子却难防小人”，遵守Robots协议老老实实抓取数据的爬虫被认为“好爬虫”，而无视规则随心所欲任意爬取数据的爬虫们则会被贴上“坏爬虫”的标签。

然而，在大数据时代的当下，数据的巨大价值令网络运营者们呼唤着更加清晰明确的数据收集和使用秩序。在Robots协议之上，人们对于如何才能成为一只“好爬虫”也从《反不正当竞争法》、《反垄断法》等法律法规的层面上提出了更严苛的要求。

一、由用户点评引发的硝烟——大众点评诉百度案

汉涛公司所经营的大众点评网创建于2003年，是中国领先的本地生活信息及交易平台，也是全球最早建立的独立第三方消费点评网站。

作为一家致力于为网络用户免费提供商户信息、消费评价、优惠信息、团购等服务的网站，通过长期的经营，大众点评网站上已累积了大量的商户信息，并通过吸引消费者真实体验发布评论而累积了大量网络用户对商户的点评。用户评论通常包括商家环境、服务、价格等方面信息，并可附上照片。

这些公开的点评信息不但吸引着互联网用户来大众点评网阅读、浏览，同时也默默地吸引来了嗅觉敏锐的网络爬虫们。

在众多爬虫之中，有一群来自百度的网络爬虫。这群爬虫是一群遵守规则的“好爬虫”，当其爬行至大众点评网站后，第一步先老老实实地访问了大众点评网站上的Robots协议（http://www.dianping.com/robots.txt）。鉴于该协议并未对百度搜索引擎抓取大众点评网用户的点评信息进行任何限制，爬虫们方才开启了爬取工作。

这些被爬取的数据之后被百度纳入百度旗下的百度地图等产品之中。百度地图除了提供定位、地址查询、路线规划、导航等常用地图服务外，还为用户提供商户信息查询、团购等服务。当网络用户使用百度产品进行搜索时，既可以通过关键字搜索商户，也可以先定位当前地址，然后通过附近商户列表查找商户。在商户页面中，百度会向用户提供商户地址、电话、用户点评等信息。对于其中餐饮类商户，其搜索出来的点评信息显示了大量爬虫的劳动果实，即来源于大众点评网的点评，而直接由百度用户撰写的点评数量却不多。这些点评信息中，来源于大众点评网的点评为原封不动地复制，同时标注了“大众点评”标识，并且在点评后设置了指向大众点评网的链接。除百度地图外，用户在百度知道中搜索餐饮商户名称时，百度也会提供来自大众点评网的点评信息。

2017年，大众点评网就百度利用爬虫技术手段抓取，并在百度产品中大量显示大众点评网站上的点评信息，以不正当竞争为由将百度告上了法庭。

（一） 一审法院：大量、全文使用点评信息不具有正当性

在案件的一审中，法院认为，涉及信息使用的市场竞争行为需要充分尊重竞争对手在信息的生产、收集和使用过程中的辛勤付出。对于判断相关信息使用的竞争行为是否具有不正当性应当考虑以下四个方面因素：（1）信息是否具有商业价值，能否给经营者带来竞争优势；（2）信息获取的难易程度和成本付出；（3）对信息的获取及利用是否违法、违背商业道德或损害社会公共利益；（4）竞争对手使用的方式和范围。

法院首先肯定了点评信息的商业价值，认为点评信息是汉涛公司的核心竞争资源之一，能为其带来竞争优势。潜在的消费者可以通过点评获取有关商户服务、价格、环境等方面的真实信息，帮助其在同类商家中作出选择。其次，点评信息需经过长期经营积累，点评类网站很难在短期内积累足够多的用户点评，而汉涛公司为运营大众点评网付出了巨额成本。再次，点评信息由网络用户自愿发布，大众点评“获取、持有、使用”该点评信息未违反法律禁止性规定，也不违背公认的商业道德，通过法律维护点评信息使用市场的正当竞争秩序，有利于鼓励创新，造福消费者。最后，鉴于百度行为具有明显的“搭便车”“不劳而获”的特点，法院认为百度大量、全文使用大众点评的点评信息的行为违反了公认的商业道德和诚实信用原则，具有不正当性。

而对于Robots协议，法院肯定了该协议是互联网行业普遍遵守的规则，违反该协议抓取网站内容将可能被认定为违背公认的商业道德，从而构成不正当竞争。然而，法院进一步认为，遵守Robots协议的行为并非就一定不构成不正当竞争。Robots协议仅涉及“数据的抓取行为”是否符合公认的行业准则问题，而不能解决抓取后的“使用行为”是否合法的问题。百度的搜索引擎抓取涉案信息并不违反Robots协议，但这并不意味着百度可以任意使用上述信息，百度应当本着诚实信用的原则和公认的商业道德，合理控制来源于其他网站信息的使用范围和方式。

同时，法院在认定百度是否构成不正当竞争时，格外关注了不同版本百度产品对于点评信息的使用程度。早期版本的百度产品由于仅显示少量、非全文的点评信息，此种信息使用方式被法院认为是符合商业道德和诚实信用原则的，因而不构成不正当竞争。

值得注意的是，《反不正当竞争法》中并未对信息使用这一类别的竞争行为进行明确规定，法院最终通过第2条[1]原则条款，认定百度行为构成不正当竞争。[2]

（二）二审法院：“模仿自由”应结合“大数据”时代背景

二审法院认可了一审法院的结论，认为百度使用大量来自大众点评网点评信息的行为，已构成不正当竞争行为。

二审法院认为，大众点评网上的信息有很高的经济价值，是汉涛公司的劳动成果。百度没有经过汉涛公司的许可，在百度地图中大量使用点评信息，这种行为本质上属于未经许可使用他人劳动成果。法院进一步分析认为，考虑到“模仿自由”，汉涛公司所主张的应受保护的利益并非绝对权利，并不必然意味着应当得到法律救济，只要他人的竞争行为本身是正当的，则该行为并不具有可责性。然而，在大数据时代的背景下，信息所具有的价

[1]《反不正当竞争法》第2条规定：“经营者在市场交易中，应当遵循自愿、平等、公平、诚实信用的原则，遵守公认的商业道德。本法所称的不正当竞争，是指经营者违反本法规定，损害其他经营者的合法权益，扰乱社会经济秩序的行为。”该条为《反不正当竞争法》的一般条款，条款适用一般需满足三个要件：一是法律对该种竞争行为未作出特别规定；二是其他经营者的合法权益确因该竞争行为而受到了实际损害；三是该种竞争行为因确属违反诚实信用原则和公认的商业道德而具有不正当性或者说可责性。

[2] 判例全文请参见上海汉涛信息咨询有限公司诉北京百度网讯科技有限公司等不正当竞争纠纷案一审民事判决书（（2015）浦民三（知）初字第528号）。

值超越以往任何时期，愈来愈多的市场主体投入巨资收集、整理和挖掘信息，如果不加节制地允许市场主体任意地使用或利用他人通过巨大投入所获取的信息，将不利于鼓励商业投入、产业创新和诚实经营，最终损害健康的竞争机制。因此，市场主体在使用他人所获取的信息时，仍然要遵循公认的商业道德，在相对合理的范围内使用。

为了划定正当与不正当使用信息的边界，法院综合考虑了诸多因素，包括：百度的行为是否具有积极效果；百度使用的信息是否超出了必要的限度；百度使用的信息如果超出必要范围是否对市场秩序产生影响；百度所采取的“垂直搜索”技术是否影响竞争行为正当性的判断等。

综合各种因素，法院认为百度的行为一方面丰富了消费者的选择，具有积极的效果；但另一方面，汉涛公司对点评信息的获取付出了巨大的劳动，具有可获得法律保护的权利。最终，法院在考量了信息获取者的财产投入、信息使用者自由竞争的权利以及公众自由获取信息的利益之后，确立了信息使用规则应当遵循“最少、必要”的原则。结合以上，法院认为百度通过搜索技术抓取并大量全文展示来自大众点评网的信息，已经超过了必要的限度，构成不正当竞争。[3]

对比新浪诉脉脉案[4]，我们可以感知中国法院对于平台上的用户数据使用的态度相对较为严格，并且在一定程度上认可平台通过劳动投入而对于其经营平台上的用户信息在竞争法层面享有的相对财产权利。值得注意的是，《信息安全技术 个人信息安全规范》第5.4条对于征得授权同意的例外情形作出规定，即如果被收集的个人信息是个人信息主体自行向社会公众公开的，个人信息控制者收集、使用个人信息无须征得个人信息主体的授权同意。平台用户数据是否可以被认定为是该条中的“自行向社会公众公开的信息”而无须被用户授权还有待讨论，至少我们能够肯定的是，在中国目前的司法态度上，即便是平台上的公开信息，第三方在抓取和使用过程中也需符合“最少、必要”的合理性要求，以尊重经营产生该用户信息的平台的劳动成果，甚至是需要得到经营该用户信息平台的授权同意。

二、公开简历信息的爬虫与反爬虫之战——hiQ诉领英案

同样是在2017年，美国加利福尼亚北区联邦地区法院也处理着一件由爬虫所引发的就用户公开数据获取和使用规则的争议。

争议双方的一方为领英公司。领英成立于2002年，是微软旗下全球最大的职业社交平台，全球拥有超过5亿的领英用户。用户可以在领英网站上建立个人档案，包括教育经历、工作经历和技能等信息。同时，用户可以在平台上自由选择不同程度的隐私保护。具体而言，用户可选择他们的履历档案完全私密，或选择（1）被其在网站上的直接关联用户可见；（2）被更广泛关联的社交圈可见；（3）被所有领英用户可见；或（4）完全公开。若是用户选择完全公开，则无论是不是领英用户，任何人都可以通过网络搜索引擎检索到其已经授权完全公开的全部履历档案信息。

另一方为一家数据分析公司——hiQ公司。hiQ公司成立于2012年，是一家为世界五百强公司开创人力资源管理工具的数据分析公司。

鉴于领英是职业社交领域内最领先的平台，hiQ的商业模式完全依赖于hiQ爬虫所爬取的领英用户的公开档案信息。具体而言，hiQ公司所派出的网络爬虫们将领英网站上用户分享的完全公开信息抓取来作为原始数据，在hiQ公司收集与分析之后，将相关数据处理结果出售给企业。hiQ针对雇主的产品主要有两种：（1）“监控者服务”：为雇主分析哪些员工存在高离职风险；（2）“技能地图”：从深度和广度提供雇员所拥有的技能信息。

在对hiQ公司爬虫的抓取行为的长期忍耐之后，领英于2017年5月发函要求hiQ立即停止数据抓取行为，并利用各式技术手段阻止hiQ爬虫继续获取领英用户的公开信息。

领英的行为将hiQ爬虫拒之门外，这使得hiQ完全不能正常进行任何经营活动。在无法与领英友好达成解决方案后，hiQ向加州法院起诉，并且向法院申请颁发临时禁止令，以禁止领英拒绝hiQ的数据抓取行为。加州法院裁定向hiQ颁发临时禁止令，要求领英停止相关行为。[5]

在裁决中，法院就hiQ公司行为是否违反美国《计算机欺诈与滥用法》（CFAA），是否违反加州宪法规定的言论自由，是否违反加州《反不正当竞争法》（UCL）等分别进行分析。

就反不正当竞争法层面，裁决指出，加州《反不正当竞争法》的管辖对象不仅仅限于条文中明确规范的反不当竞争行为，也涵盖了可能违反反不正当竞争法基本原则和精神的其他行为。换而言之，即使是对于加州的《反不当竞争法》没有明确规定的行为，只要证明该行为能够对竞争市场造成相似或者更大的损害也可被确定具有违法性。从某种程度上说，美国法院在本案中也采取了类似于我国反不当竞争法原则性条款的分析思路。

法院最终倾向性地选择支持了hiQ的爬虫爬取行为，主要是考虑到领英在相关市场上的领先地位，其采取的禁止性措施违背了竞争法精神；同时，从信息自由流通的角度看，鉴于用户已选

[3] 判决全文请参见北京百度网讯科技有限公司与上海汉涛信息咨询有限公司、上海杰图软件技术有限公司不正当竞争纠纷案二审民事判决书（（2016）沪73民终242号）。

[4] 该案中确立了OpenAPI合作模式下的三重授权原则，即“用户授权平台+平台授权第三方+用户授权第三方”模式，具体操作分为三步：第一步，用户需授权开放平台收集其数据及其授权平台可再授权第三方收集用户数据；第二步为第三方获得平台的授权；第三步，用户再明确授权第三方收集其在平台上的数据。判决全文请参见北京淘友天下技术有限公司等与北京微梦创科网络技术有限公司不正当竞争纠纷案二审民事判决书（（2016）京73民终588号）。

[5] 裁决全文请参见hiQ Labs, Inc. v. LinkedIn Corp., 273 F. Supp. 3d 1099 (N.D. Cal. 2017).

择公开信息，领英的做法违背了公共利益。

hiQ在论证领英的行为违反了竞争法精神时指出：其一，考虑到领英在职业社交市场（professional networking market）的领先地位，想要获得相关信息作为原始数据进行进一步分析，几乎不可能绕开领英另起炉灶；其二，领英所在的职业社交市场和hiQ所在的数据分析市场（data analytics market）不具有相互替代性，是竞争法下不同的产品市场。领英以其在职业社交领域的垄断地位，利用了hiQ对领英用户信息依存度高的特点阻断hiQ获取信息，从而封锁其他竞争者进入数据分析市场。

在裁决中，法院指出《谢尔曼法》禁止公司利用垄断地位获得竞争利益或者摧毁其他竞争者。法院认为，hiQ就领英在职业社交网络市场占据着支配地位进行了更有力的主张。此外，法院注意到领英还有进军数据分析市场的能力和计划，几乎在领英宣布进军数据分析市场的同时，领英开始制裁hiQ并切断了hiQ的数据获取方式，限制了hiQ数据获取的技术。法院认为，领英进军数据分析市场的行为和阻碍hiQ数据抓取的行为密切相关，从而认为其试图不当地将其在职业社交网络中的市场力量，传递至数据分析市场。

此外，从公共利益的角度，法院在裁决中称，选择公开其信息的用户更可能已经预期到他们的公开个人资料将被搜索、挖掘、整合及分析。另外，如果赋予领英这样的私人实体以任意理由阻止他人访问其网站上公开可见信息的权力，将对互联网所承诺的公共话语和信息的自由流动造成威胁。

在其他公司作为“法庭之友”所提交的意见书中[6]，与大众点评网案类似，也试图强调网站获取信息的难易程度和成本付出，以及竞争对手使用的方式和范围。例如，Craglist提交了一份诉讼支持就论证了领英获取信息、累积用户所付出的成本资源。Craglist的论证思路非常类似于我国法院就大众点评网一案的分析过程：虽然不管是Craglist还是大众点评网，上面的用户信息均是靠用户自己提供，但是收集以达到一定规模的过程耗费大量人力、物力和财力。就Craglist而言，该公司作为二手交易平台自1995年成立以来投入了大量成本用于把获取的信息进行分类，从而形成了汽车、租房等等分类交易平台。此外，Craglist还需投入大量资源用于保护用户信息，使用户浏览信息更方便、快捷、安全。[7]美国一家房地产交易公司CoStar作为“法庭之友”，也提交了意见书，论述CoStar如何花费大量精力雇用专业信息人员对市场信息进行收集、整理和加工，而且这样的数据库极大地便利了市场交易。[8]但是，上述意见未得到法院认可。

最终，法院向hiQ颁发了针对领英的临时禁止令。目前，领英一方已上诉。

三、对比研究，探寻中美司法逻辑差异

上述两个案件的共同关键问题在于，网站上用户公开提供的信息应如何界定使用规则。可以感知，两国法院的态度、立场均存在差异。

笔者在下列表格中简单梳理了两个案件的异同之处：

		大众点评诉百度案	hiQ诉领英案
案情总结		百度大量抓取大众点评网用户的公开点评信息，在使用百度产品所呈现的搜索结果中**直接呈现**。大众点评遂将百度诉至法院。	hiQ抓取领英用户公开信息，以该述信息作为原始数据，处理后将**分析结果**提供给hiQ客户。领英采取技术手段阻碍hiQ的爬取行为，hiQ遂将领英诉至法院。
相似点	**数据收集方式**	均是基于网络公开用户数据的爬虫抓取行为。	
	核心问题	针对网站上用户公开信息的收集、使用规则应如何界定。	
	分析角度	认定原被告为存在竞争关系的竞争者，并基于竞争法展开分析。	

[6] 出于对法院判决既判力和商业影响的考量，在美国诉讼中，第三方公司可以作为“法庭之友”(Amicus Curiae)提供意见书(Amicus Curiae Briefs)，用来佐证观点或者解释法律，以协助诉讼进行。

[7] See Perry J. Viscounty, Gregory G. Garre, Brief of Amicus Curiae Craigslist, Inc. in Support of Defendant/Appellant linkedin Corp.

[8] See Nicholas J. Boyle, John S. Williams, Eric J. Hamilton, Brief of Amicus Curiae Costar Group, Inc., in Support of Appellant and Reversal.

		大众点评诉百度案	hiQ诉领英案
差异点	具体行为	百度通过爬虫爬取数据后，将他方网站公开用户点评信息直接呈现在产品搜索结果中。	hiQ将爬虫爬取的他方网站公开用户数据作为分析的原始数据，最终输出分析结果。领英运用反爬虫技术，阻止了该爬取行为。
	相关市场	大众点评网和百度两者在为**用户提供商户信息和点评信息**的服务模式相似，争夺同样的网络用户群体，具有竞争关系。	领英有意进入**数据分析领域**，跟诸如hiQ在内的其他数据分析公司展开竞争。
	落脚点	百度大量全文展示来自大众点评网的信息，使用方式超过必要限度，未遵循“最少、必要”原则，不具有正当性。	领英有意封锁竞争者进入数据分析市场；以任意理由阻止第三方利用爬虫抓取平台上用户的公开数据，会对信息自由流动造成威胁，不具有正当性。
	效力	法院终审判决。	临时禁止令裁决（已被上诉）。
	结局	被爬取方获胜，爬虫方落败。	爬虫方初战告捷。

根据上表分析可知，两个案件案情的相似点在于均是围绕具有竞争关系的经营者之间就公开数据资源的利用所引发的争议，具体数据收集方式均涉及从公共网络上的爬虫数据抓取行为。

差异点在于使用方式上，大众点评案中，百度将从大众点评网所抓取的用户点评信息直接大量复制纳入自己旗下的产品中。而在领英案中，hiQ虽然同样在领英网站上抓取了公开的用户信息，但hiQ将其所抓取的领英用户信息进行了进一步的分析和处理，从而将数据分析成果而非原始数据本身作为自己的产品。

在大众点评案中，法院的逻辑在于，涉案双方在提供商户信息/点评信息这个领域展开竞争，而百度大量复制大众点评网用户评论的行为，超出了对他人所获取的信息的合理使用范围，未遵循“最少、必要”原则，违背了公认的商业道德。而在hiQ案中，法院的逻辑在于，涉案双方在数据分析市场具有竞争关系，不可不当阻碍其他竞争者对自己网站上的公开原始数据的获取，以封锁其进入数据分析市场中。

由此可以看出，中国法院在大众点评案中较为注重对于个体竞争者在平台数据累积过程中付出的辛勤劳动，从而认可用户数据（即使具有一定的公开性）作为其宝贵的竞争资源应当获得竞争法层面上的保护，被赋予一定的财产权利；而美国法院则更为注重对于信息自由流通对不同市场中的繁荣竞争的重要性。

四、爬虫的背后，数据权属知多少

上述案件虽然是由爬虫所引发的不正当竞争法争议，但其最根本、最核心的问题仍是数据使用规则，以及更进一步的数据权属问题。数据之上到底有何权益在学界也是争议纷纷。数据权属类别可能包括以下几种主张：

（一）个人主体的人格权

学界传统上主张赋予数据主体对于数据，特别是个人信息的人格权。数据人格权的模式是基于隐私权，再根据网络信息的实践进行一定的变通形成的。但是，隐私权和数据人格权是完全不同的概念。隐私权主要关注个人不愿意公开的各种私生活信息或生活秘密等，而数据人格权保护的是没有公开甚至已经公开的权利。然而，根据数据人格权的观点，数据并不是一种财产权益。这一理论因此难以在大数据时代下适应数据资产化的经济需求和实际情况，仍无法确定性地解决数据权属问题。

（二）数据财产权

在数据活动日渐频繁复杂，数据经济随之蓬勃发展的情况下，个人信息人格权保护的简单模式，与数据经济的实际运行要求直接发生冲突，难以有效调和个人和企业基于个人信息和数据的利益关系，企业数据经营的保障和动力都很脆弱，不利于其发挥创造性。

基于此，莱斯格（Lessig）教授提出数据财产化（data propertization）理论，即应认识到数据的财产属性，通过赋予数据以财产权的方式，来强化数据本身的经济驱动功能，以打破传统法律思维之下依据单纯隐私或信息绝对化过度保护用户而限制、阻碍数据收集、流通等活动的僵化格局。

数据财产化的思路下，数据财产权又可分为个人数据财产权主张和企业数据财产权主张。个人数据财产权主张通过创设一种新型财产权，认为个人对个人数据享有优先的财产权，企业在交易个人数据的时候将可能对个人隐私产生极大伤害，并产生难以预计的信息安全问题，大范围失控的数据交易也将为违法活动提供温床。

企业数据财产权主张则从物权角度研究数据产权问题，认为核心是促进数据产业发展。为了促进数据产业的发展，企业应享有收集、整理数据获得的劳动成果。大众点评案中法院认识到企业在收集信息过程中投入的大量人力物力财力，形成一种劳动

成果。虽然法院不倾向于直接赋予企业就其数据享有的“劳动成果权”，但是在认定企业数据是否被第三方不当使用时，考量了数据的商业价值和企业为实现数据商业价值所付出的努力。在领英案中，虽然法院没有详细论述，但在“法庭之友”的书面陈述中，Craglist等也均主张对于企业花费大量精力用以实现特定商业价值的数据应该保护。

（三）知识产权–著作权

有观点认为，在关于数据交易的专门法规出台之前，知识产权制度是解决数据产权问题，对数据产业者赋权的解决办法之一。企业投入人力、物力将个人信息进行脱敏、分析、建模之后形成的数据具有创造性，而其分析的技术、模式、方式等也具有独创性，因此企业对数据的处理技术和生成结果应当拥有知识产权，如著作权、专利权等。但知识产权制度本身存在一定的局限性，因此这一观点存在着一些难以解决的矛盾，例如，由于著作权本身存在的地域性等特点，与数据流动性等数据价值实现的必要前提存在冲突，因此除数据应具备可著作权性的相应条件以外，以著作权为基础的数据权属观点还面临数据流动问题的困扰。

（四）数据库邻接权

大部分数据并不具有原创性，而是一种自动产生、收集、加工的实时数据，因此数据通常难以受到著作权保护。但是，对收集、整理的数据整体，可以通过数据库邻接权来进行保护。1996年，欧盟通过了《关于数据库法律保护的指令》(以下简称“《数据库指令》”)，用以直接保护因不符合独创性标准而无法受到著作权法保护的数据库。《数据库指令》第1条规定了一种独立意义的专有财产权，为期15年，权利的获得无须以认定汇编作品为前提，只要数据库制作人在内容收集、核准和提供等方面有实质性投入，数据库制作人就可以获得这种特殊权利，包括：通过许可合同转移、转让、授予他人；防止任何第三方对数据库内容的全部或实质内容进行提取和再利用。

（五）商业秘密及保密义务

将数据上附着的权利类型划归于商业秘密及保密义务的主张主要可用于保护商业数据中具有保密意义和价值的数据类型，即以“秘密性”“价值性”作为特征。以欧盟为例，这一主张的法律基础来自于2016年颁布的《关于保护未披露的技术诀窍和商业信息（商业秘密）防止非法获取、使用和披露的第2016/943号（欧盟）指令》以及各成员国国内的立法。商业秘密及保密义务的观点指出，商业秘密的保护和保密义务与个人信息保护之间存在一定的相似性，如未经同意收集的违法性、擅自公开的违法性、合同约定对于保密义务的影响作用等。虽然网络上的公开信息相对较难主张构成商业秘密，但鉴于网络经营者通过技术措施可以使得数量众多的用户信息汇聚集合难以被他人所知悉，因而也有可能主张具有“秘密性”，但可能较为牵强。

在目前有关数据权属的争议中，从我国现行立法与司法实践来看，更多的是从《反不正当竞争法》第2条的一般原则性规定，考虑数据抓取、使用行为是否具有不正当性，一定程度上从侧面认可相关企业就数据的财产权利，但更加明晰的使用规则和权属划分仍在进一步摸索之中。

五、展望

数据的地位在大数据时代无异于新型“石油”。正如石油需要经过加工、提炼后投入到各种工业产品的生产过程中一样，数据也需要经过相应的加工处理，运用到不同行业领域之中，即实现数据的商业化。大量的公开数据使得一些企业看到商机，力图探索实现数据商业化路径，以更大程度实现数据价值的发挥，这也是更高社会效益产出的必由之路。在数据资源的争夺之中，网络爬虫发挥着重要作用，爬虫与反爬虫的拉锯战也愈演愈烈。其背后所引发的如何界定数据权属和数据使用规则，尤其是针对公开数据商业化问题，引起了热烈讨论与关注。

大众点评案虽然已得到终审判决，但在大数据时代下公开数据的使用规则仍不清晰。如果认定点评信息是大众点评网的劳动成果，应享有竞争法下一定的财产权利，那么该述权利的外延又在哪里？是否能如领英案中对第三方抓取网站公开数据进行技术阻隔？目前，我们尚无法得出定论，领英案也仍在进一步审理过程中，值得密切关注下一步进展。但我们从上述案件能够感知到，中国法院对于用户数据使用更为审慎，前有微博诉脉脉案的三重授权原则，后有大众点评诉百度案的合理原则分析，而美国法院则似乎更看重数据的自由流通对市场竞争的积极效应。有待我们思考的是，如何在数据保护和数据利用、流通之间更好地寻求平衡点，以充分发挥数据的价值的同时，维护、保障数据安全。

结语

数据毫无疑问将在未来扮演越来越重要的角色，然而，数据使用规则及更深一层的数据权属这一大数据时代的核心问题，仍远未能达成共识。

可以预见，在数据商业化的浪潮之中，将来有关大数据产品权益的争议将越来越多，如何明确数据相关的权益问题，厘清数据使用规则以最大程度地保护、促进竞争，无论是对于学界还是对于司法实践都是不可回避的。只有更好地平衡数据保护和信息自由流通这一天平，才能有效维护大数据时代下的商业竞争秩序，小小爬虫也才能更好地为企业创造价值。

（本文发布于2019年02月。）

谨于言而慎于行：
互联网信息内容服务管理新规出台

根据《中华人民共和国网络安全法》（以下简称“**《网安法》**”）、《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》，国家互联网信息办公室（以下简称“**网信办**”）制定并于2017年8月25日公布了《互联网跟帖评论服务管理规定》（以下简称“**《跟帖评论规定》**”）和《互联网论坛社区服务管理规定》（以下简称“**《论坛社区规定》**”），两规定将于2017年10月1日起施行。两大新规的新鲜出炉丰富了互联网信息内容执法的领域，体现了网信办对于落实互联网信息内容管理，依法治理传播网络谣言或违法不良信息等破坏网络传播秩序行为的决心，但同时新规中针对用户和互联网服务提供商行为和责任的新规定也引发了业内的高度关注。

本文针对《跟帖评论规定》和《论坛社区规定》的主要条款和要求进行梳理和分析，进而从实际操作角度分别说明跟帖评论服务提供者、论坛社区服务提供者及用户在目前的规定下可能面临的行为要求或限制，并提出合规建议。

一、两项规定的主要内容

总体而言，本次网信办出台的两项规定从执法目的、执法依据、执法范围、执法主体、执法监管内容、公民权益保护、互联网服务提供者主体责任、制度建设、监督举报和法律责任等多个方面对互联网跟帖评论及论坛社区服务进行具体而细致规范，并通过对“跟帖评论新产品、新应用、新功能”的安全评估制度确保规定的实施能够适应互联网环境下变化多端的产品和服务形式，保障内容监管措施的有效性。

以下是有关两大规定主要内容的简要梳理。

《跟帖评论规定》		
	规定内容	对应条款
适用范围	**跟帖评论服务**，是指互联网站、应用程序、互动传播平台以及其他具有新闻舆论属性和社会动员功能的传播平台，以发帖、回复、留言、“弹幕”等方式，为用户提供发表文字、符号、表情、图片、音视频等信息的服务。	第二条
强化了各地网信办的属地管理责任	加强**监督管理执法**工作	第三条
	对跟帖评论新产品、新应用、新功能进行**安全评估**	第四条
	对跟帖评论服务提供者开展**信用评估**	第九条
	对跟帖评论服务提供者安全管理**责任追究**	第十一条、第十二条
保护公民权益	建立健全用户信息保护制度。	第五条第（二）项
	禁止跟帖评论服务提供者及其从业人员通过干预舆论、误导公众舆论方式非法牟利	第七条
	加强技术保障，及时发现跟帖评论服务存在的安全缺陷、漏洞等风险，并采取补救措施。	第五条第（六）项
	建立健全违法信息公众投诉举报制度	第十条

《跟帖评论规定》		
	规定内容	对应条款
网站（跟帖评论服务提供者）的主体责任要求	落实实名制要求	第五条第（一）项
	建立用户信息保护制度	第五条第（二）项
	建立先审后发制度	第五条第（三）项
	加强弹幕管理	第五条第（四）项
	建立信息安全管理制度	第五条第（五）项
	采取技术保障措施	第五条第（六）项
	加强审核编辑队伍建设	第五条第（七）项
	配合有关主管部门依法开展监督检查工作，提供必要的技术、资料和数据支持	第五条第（八）项
其他	与注册用户签订服务协议，履行相应告知义务	第六条
法律责任		第十二条

《论坛社区规定》		
	规定内容	对应条款
适用范围	**互联网论坛社区服务**，是指在互联网上以论坛、贴吧、社区等形式，为用户提供互动式信息发布社区平台的服务。	第二条
确立监督管理执法机构及属地监管原则		第三条
鼓励建立健全行业自律和行业准则		第四条
论坛社区服务提供者义务	落实主体责任，建立健全各项信息安全管理制度，加强人员建设和提供技术支持	第五条
	与用户签订服务协议，规定并告知用户权利义务	第六条
	加强对其用户发布的信息的管理	第七条
	落实用户真实身份信息认证，同时保护用户身份信息	第八条
	不得通过发布、转载、删除信息或者干预呈现结果等手段，谋取不正当利益	第九条
	遵守法律法规和公序良俗，承担社会责任	第十条
	建立健全违法信息公众投诉举报制度	第十一条
法律责任		第十二条

二、用户网络行为需自律

加强互联网信息内容管理，需要互联网服务使用者（用户）、互联网服务提供者与监督管理机关的共同参与。从互联网服务使用者角度来看，两项规定为用户使用互联网服务、尤其是跟帖评论和论坛社区发帖等行为提供了指引，并限制向不遵照指引的用户提供互联网服务，比如严重失信的用户可能被列入黑名单，从而被停止提供服务，并禁止通过重新注册等方式使用跟帖评论服务。[1]

[1]《跟帖评论规定》第九条；类似规定还可见《论坛社区规定》第六条。

（一）水军等干预、误导公众舆论行为将受到规制

随着互联网的发展，网络水军一度在网络上盛行。通过雇佣水军、运营机器人或程序手段等方式，宣传“虚假消息、传销讯息、色情暴力内容或一些妄图引起关注的帖子”。《跟帖评论规定》第七条第二款明确规定“跟帖评论服务提供者和用户不得利用软件、雇用商业机构及人员等方式散布信息，干扰跟帖评论正常秩序，误导公众舆论”，直接限制了利用水军传播不良网络讯息、干扰网络秩序的行为。

同时，跟帖和发帖的实名制将有利于限制通过一人在同一论坛社区重复申请大量账号或利用机器人或程序申请大量账号来完成的人工或机器“水军”行为。跟帖评论制度审核管理、实施巡查以及新闻信息跟帖评论先审后发和加强互联网服务提供者对用户发布信息的管理等制度也有利于及时发现违法违规内容，采取有效应对措施，降低“水军”行为的危害性。[2]

（二）虚拟身份信息也需审查，互联网信息内容审查未留死角

尽管《跟帖评论规定》针对的是“互联网跟帖评论服务”，但从网信办的规定中不难看出，互联网跟帖评论信息内容的监管并不仅限于狭义的发帖内容，还包括其他通过发帖行为或在发帖环节中可能公开反映在互联网中的信息。

《论坛社区规定》第八条第2款规定“互联网论坛社区服务提供者应当加强对注册用户虚拟身份信息、版块名称简介等的审核管理，不得出现法律法规和国家有关规定的内容”。换言之，如果用户通过将含有“网络谣言、污言秽语、”“虚假广告、血腥暴力、侮辱诽谤、泄露个人隐私”的信息放置入前台虚拟名称之中来变相公开或传播违法违规信息，也同样会落入互联网内容执法的规制范围。[3]由此可见，跟帖服务评论的外延并不仅止于狭义的发帖内容，互联网信息内容审查将全面监管跟帖服务各个环节中可能的公开信息表达。

（三）“弹幕”属跟帖评论方式，跟帖评论新方式受限

弹幕作为一种新兴的互联网评论功能，是近年来互联网用户评述和沟通的重要方式之一。与普通评论不同的是，前者通常会在帖下长期存在，而弹幕只会在“视频中特定的一个时间点出现”。本次发布的《跟帖评论规定》第五条第（四）项规定，“提供‘弹幕’方式跟帖评论服务的，应当在同一平台和页面同时提供与之对应的静态版信息内容。”静态版信息审核制度将有利于落实弹幕内容先审后发制度、保障和便捷公众对违法弹幕信息的监督投诉举报。[4]

此外，本次将新兴的弹幕监管问题单独进行规定，反映了互联网信息内容监管机构关注互联网发展现状、从现实问题出发合理制定监管政策的科学性和严谨性。结合《跟帖评论规定》第四条规定的监管机关针对跟帖评论新产品、新应用、新功能进行事先安全评估，不难看出制度旨在保证监管能够紧跟互联网发展，避免互联网服务提供者利用新产品、新应用、新功能逃脱监管的可能性，体现了互联网内容监管的前瞻性。但同时业内也有担心这种超前的监管方式，是否会限制新产品、新应用、新功能的更新速度，阻碍互联网信息内容发布方式的创新。

（四）用户分级及信用评估制度，互联网行为有迹可循

《论坛社区规定》明确用户不得利用互联网论坛社区服务发布、传播法律法规和国家有关规定禁止的信息，并针对“情节严重的”行为，要求“服务提供者将封禁或者关闭有关账号、版块”。除对“情节严重”的互联性信息内容发布行为予以禁止外，《跟帖评论规定》还提出了建立跟帖评论服务用户分级管理制度和跟帖评论行为信用评估体系，长期跟踪监管用户的互联网信息内容发布行为。在用户分级管理制度和信用评估体系下，跟帖评论服务的提供者将以用户的既往评论行为为依据，对用户跟帖评论服务行为进行信用评估，并根据信用等级确定服务范围及功能。

同时，互联网服务提供者对于发布违反法律法规和国家有关规定的内容，除了采取警示、拒绝发布、删除信息、限制功能、暂停更新、关闭账号等措施外，还将保存相关记录。这意味着，用户的跟帖评论行为不仅有迹可循，并且既往的行为将可能影响其此后享受跟帖评论服务的权限，严重者可能被停止服务，并禁止通过重新注册等方式使用跟帖评论服务。其目的是鼓励用户提高互联网行为的规范意识，自主规范互联网行为，对其在互联网上的一言一行承担应负的责任。

---

[2] 有关实名制制度的要求可参见《跟帖评论规定》第五条第（一）项和《论坛社区规定》第八条。

[3] 《国家互联网信息办公室有关负责人就<互联网跟帖评论服务管理规定答记者问>》，http://www.cac.gov.cn/2017-08/25/c_1121541844.htm；《国家互联网信息办公室有关负责人就<互联网论坛社区服务管理规定>答记者问》，http://www.cac.gov.cn/2017-08/25/c_1121541845.htm。

[4] 有关弹幕服务的规定还可参考国家网信办2016年发布的《互联网直播服务管理规定》。

（五）对用户网络行为的自律要求

有鉴于两项规定的要求，我们建议互联网服务使用者（用户）：

- 在使用跟帖评论服务或其他相关服务时，主动进行个人身份信息验证，配合实名制规定；
- 对含有不当信息内容的前台虚拟名称或其他个人信息，如账号主页的个人简介等，及时予以更正或删除；
- 在参与互联网平台活动，实施发帖、跟帖等行为时，审慎注意发帖、跟帖内容，遵守法律法规、社会公德。不发布法律法规和国家有关规定禁止的信息内容；
- 使用前应当签订服务协议，明确互联网服务的管理规定及相关法律法规义务，增强互联网行为的自律性。

三、互联网服务提供者“任重而道远”

（一）实名制要求将加重互联网服务提供者个人信息收集和保护的责任和义务

两项新规不仅为用户的行为提供了指引，也对互联网服务提供者提出了新的要求。以实名制问题为例，今年6月生效的《网安法》第24条就已经规定了“网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。”

而《跟帖评论规定》和《论坛社区规定》则分别规定了跟帖评论服务提供者和论坛社区服务提供者应当按照“后台实名、前台自愿”的原则，[5]要求用户通过真实身份信息认证后注册账号，对于未认证真实身份信息的用户不得提供跟帖和信息发布服务。此举意味着互联网服务提供者将掌握用户个人的真实身份信息。一方面，实名制的规定有利于对跟帖评论和网络论坛社区的环境整肃和不良信息的监督管理；另一方面实名制下，互联网跟帖评论服务提供者和论坛社区服务提供者的后台将会处理大量的用户个人信息，互联网服务提供者需要严格遵守《网安法》以及相关配套细则对于用户个人信息收集、使用的限制以及对于个人信息的保护要求。具体而言：

1. 实名制将进一步要求加强隐私政策的合规工作

《网安法》第四十一条明确要求个人信息的收集、使用需要遵循“合法、正当、必要的原则”，并要求“公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意”。互联网服务提供者在实名制要求下，需要严格遵守《网安法》的要求完善隐私政策。

此外，由于实名制要求可能需要用户提供个人敏感信息（比如身份证号码等），我们也建议互联网服务提供者根据即将出台的《信息安全技术 个人信息安全规范》，在隐私政策中完善对于个人敏感信息收集和使用的特殊要求。

2. 实名制将对数据商业化提出更高的要求

不可否认的是，大数据技术的发展使得数据不仅成为互联网服务提供者的“竞争资源”，也成为具有巨大市场价值的“数据资产”。根据《网安法》第四十二条，“未经被收集者同意，不得向他人提供个人信息”，个人信息仅在“经过处理无法识别特定个人且不能复原的”情况下，可以未经个人主体同意而向他人提供，因此实践中彻底脱敏后的个人信息可以作为商品自由流通。

然而，在实名制下，由于互联网服务提供者都将掌握用户的真实身份，“用户数据”之间的关联性将使得数据直接或者间接指向特定用户的可能性更大，互联网服务提供者之间的数据流动使得个人信息的脱敏要求将更为严格。

3. 实名制要求互联网服务提供者加强个人信息的安全防护

由于互联网服务提供者将掌握大量的个人信息甚至个人敏感信息，其遭受黑客攻击以及其他原因等导致的数据泄露风险也相应增加。互联网服务提供者应该严格按照《网安法》对于网络运行安全及网络信息安全的要求，加强网络安全防护工作。互联网服务提供者在根据规定积极落实用户实名制要求的同时，也应当对网站（网络服务提供者）安全防护和用户个人信息保护给予高度重视，以避免可能产生的个人信息泄露和其他法律风险。

[5]《论坛社区规定》第八条；《跟帖评论规定》第五条第（一）项。

（二）互联网服务提供者需落实主体责任和内部合规工作

网站（互联网服务提供者）的主体责任问题并非是第一次出现。2016年8月，网信办就曾在网站履行网上信息管理主体责任专题座谈会上明确提出了落实主体责任的八项要求。[6]

此外，互联网服务提供者还需要加强内部监管和主动接受外部监督。对内部监管而言，需要加强对自身及从业人员的监督，禁止为谋取不正当利益或基于错误价值取向，采取有选择地删除、推荐跟帖评论等方式干预舆论。就外部监督而言，互联网服务提供者应当通过建立完善有效的公众投诉举报机制和及时的受理处置制度来主动接受外部监督，并就举报受理落实情况接受国家和地方网信办的监督检查。

有鉴于两项规定的要求，我们建议互联网服务提供者在提供服务时：

1. 积极落实平台主体责任，包括但不限于：
   - 落实实名制要求，鼓励新增用户进行实名注册，并做好既有用户的身份信息验证工作；同时对用户的网络虚拟名称、个人主页简介等公开信息内容进行规范。
   - 加强对用户发布信息的管理工作，如新闻信息的先审后发制度、提供弹幕信息的静态版内容、进行跟帖评论的实时巡查等。
   - 结合网站（互联网服务提供者）或提供服务的实践情况，加强制度建设，包括信息安全保护制度、互联网服务与管理细则、用户身份信息安全保障制度、应急事件处置与报告制度、用户信用评估及分级制度、违法违规信息处置及记录留存制度等，并从技术、人员等方面予以配合。

2. 遵守安全评估规定，在提供新闻信息服务相关的新产品、新应用、新功能时，主动提交相应的互联网信息内容监管机构（国家或省级网信办）申请安全评估。

3. 考虑实名制落实后互联网服务提供者对用户个人身份信息的防护义务，加快建立完善的互联网信息脱敏和保密制度、实施相应技术脱敏和保密措施，履行应尽的网络安全和个人信息保护义务。

4. 建立有效的内部监管体系，避免互联网服务提供者及工作人员在监管信息时的不当举措；主动接受外部监督，包括完善公众举报接收及处置机制以及配合主管机构的执法监督检查等。

四、短评：追求商业价值与承担社会责任的平衡

从近期互联网立法趋势来看，互联网行业行政监管呈现出行政执法部门外部监管、互联网服务提供者主体责任以及互联网用户自律的多层管理结构。可以预见的是在未来互联网行业监管中，为了应对互联网行业的高速发展和复杂多样性，互联网服务提供者将扮演越来越重要的“中间人”角色。以《跟帖评论规定》里提到的两层信用管理制度为例。一方面，网信部门对网站的信用档案和失信黑名单，要定期进行信用评估；另一方面网站对网民需实施信用管理，建立严重失信用户的黑名单，停止对黑名单用户提供服务，并禁止其重新注册。不仅如此，随着互联网服务提供者的社会影响与日俱增，要求互联网服务提供者承担一定“社会责任”的呼声愈来越高，比如在《论坛社区规定》第十条中就规定互联网论坛社区服务需要“尊重社会公德，遵守商业道德，诚实信用，承担社会责任。”

不可否认，随着互联网的迅猛发展，互联网已经成为重要的社会经济、文化和政治平台，与社会公众的日常生活有着紧密的联系。由于互联网平台的发展已经触及社会公共利益，有必要要求其承担与主体能力相当的社会责任。但与此同时，我们也需要考虑互联网平台作为商业主体，有追求商业价值的天性。为平台施加过于严苛的社会责任可能会增加企业运营成本、降低日常运作的效率甚至影响企业的创新。因此对互联网平台服务提供者主体责任、个人信息和网络安全保障义务的设定可能需要立法、执法部门与互联网企业的深入沟通，参考其他司法辖区经验和我国互联网发展的现状，力争实现创造商业价值与促进社会利益之间的良性循环。同时，互联网企业也需密切关注国家网信部门对于互联网行业执法的规定出台，以确保在自身合规建设时能充分参考法律法规规章的规定，并在面临行政执法时积极应对和配合，最大限度内维护企业自身的合法权益。

感谢实习生张乐健对本文的贡献。

（本文发布于2017年08月29日。）

[6] 论坛社区规定》第五条；《跟帖评论规定》第五条。

欲善其事，先利其器
——解读《互联网信息内容管理行政执法程序规定》

2017年5月2日，国家互联网信息办公室（“网信办”）在其官方网站上连续发布了《网络产品和服务安全审查办法（试行）》（“《审查办法》”）、《互联网新闻信息服务管理规定》（“《管理规定》”）以及《互联网信息内容管理行政执法程序规定》（“《程序规定》”）。本文将介绍《程序规定》的特色以及主要内容。

如果说《管理规定》是在2005年规定的基础上的“老瓶换新酒”，《程序规定》则是《网络安全法》（“《网安法》”）下出台的第一部程序性部门规章。和《审查办法》“画龙画虎先画骨”的立法技术不同，《程序规定》在《行政处罚法》的基本原则下做到“统一协调、面面俱到、内外兼修、与时俱进”，为此后监管执法工作提供了重要的法律依据，可谓是互联网信息内容管理行政执法所仰仗的“利器”。

一、统一协调

《程序规定》的出台，不仅意味着互联网信息内容管理的行政执法程序从此有章可循，也标志着互联网信息内容管理的执法工作正式进入“统一协调执法”的时代。

在此之前，互联网信息内容管理工作职责相对分散，2011年修订后的《互联网信息服务管理办法》针对不同领域的互联网信息内容的管理就有所规定，其第十八条指出：“新闻、出版、教育、卫生、药品监督管理、工商行政管理和公安、国家安全等有关主管部门，在各自职责范围内依法对互联网信息内容实施监督管理”。[1]此外，《互联网等信息网络传播视听节目管理办法》、《互联网视听节目服务管理规定》以及《互联网文化管理暂行规定》都含有关于互联网信息内容管理方面的相关条款，均要求有关主管部门在职权范围内相应负责。

直至2014年，国务院发布《关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》（“《通知》”），将全国互联网信息内容的管理工作授权至国家网信办，并由其负责监督、管理和执法。我们理解这一举措将有利于统一互联网信息内容管理的行政执法工作，也符合国家网信办从国家战略层面统筹、协调涉及各领域的网络安全和信息化重大问题、推进我国互联网领域立法与执法顶层设计的定位。在援引《通知》作为立法依据的基础上，《程序规定》的出台将可能意味着正式将互联网信息内容管理工作统一由国家网信办协调。

但如《管理规定》第六、二十一、二十八条所述，《管理规定》也要求互联网信息服务提供者符合电信、互联网视听节目、网络出版等服务领域的监管要求，因此《程序规定》的出台是否就意味着将前述已有的行政法规和部门规章中涉及互联网信息内容的执法都需要参照《程序规定》执行，仍然需要进一步的澄清。

二、面面俱到、兼收并蓄

作为《网安法》下第一部专门的执法程序规定，《程序规定》一改以往执法程序“形销骨立”的立法风格，结构上参考诉讼法等法律的体例，内容上更为“丰满”。

《程序规定》开宗明义地在首章“总则”明晰了基本原则

[1] 请见《互联网信息服务管理办法》第十八条。

与制度，而后以六章条款分别针对执法过程中的“管辖”、“立案”、“调查取证”、“听证、约谈”、“处罚决定、送达”和“执行与结案”等问题进行了具体、详实的规定。

具体而言，在重申行政执法的基本原则后，《程序规定》就进一步明确了执法两大方面的基本制度——行政执法督查制度与执法人员资格管理制度。[2]前者要求下级执法部门应当接受上级执法部门的督促与检查，在外部监督层面确保高效执法；后者则针对执法队伍的培养，对执法人员提出了培训考试（考核）、持证上岗的资质要求，在内部建设层面提升执法水平。

而在执法程序的具体规定中，《程序规定》借鉴了诉讼法与基本行政执法的内容架构，将各个执法环节抽丝剥茧，为互联网信息内容管理构造了一套定制的行政执法程序。无论是对不同情况下不予立案的处理，还是调查取证中针对不同证据形式的特殊规定，《程序规定》都尽其所能地作出具体规定，为执法人员与当事人提供了有效的指引。

三、内外兼修、透明执法

《程序规定》在具体执法程序方面的规定非常详尽，为执法人员与行政当事人都提供了高度透明的执法流程与文件范本。

具体而言，一方面，《程序规定》将网信部门作为行政执法机关与行政当事人之间的权利义务关系进行清楚界定，为行政当事人行使权利、履行义务提供了切实的帮助。以听证为例，《程序规定》则规定在作出特定类型的行政处罚决定前，执法机关有义务“告知当事人有举行听证的权利”；同时也要求当事人“应当在被告之后三日内提出……逾期未要求听证的，视为放弃权利”。[3]另一方面，《程序规定》还披露了行政执法机关内部所必须遵从的工作流程，为监督执法与当事人维护合法权益提供了必要的保障。例如，如上所述，《程序规定》第三章关于立案的规定中，不仅仅明确界定了执法部门启动案件调查与立案的基本标准，更明晰了执法机关内部的工作流程，分情况具体说明不予立案的理由与处理情况，为监督执法提供了基本依据与保障。类似的规定还包括《程序规定》第三十一条针对调查终结后案件承办人撰写《案件处理意见报告》的相关要求。

此外，值得注意的是，除了《程序规定》本身的条款外，网信办此次立法还公布了互联网信息内容管理执法中可能涉及的文件范本，并要求下级执法机关进行参照定制，[4]显著提升了执法内容的透明度与监督执法的可行性，更有利于规范不同地区、不同级别的执法行为，维护网信部门作为互联网信息内容执法部门应有的权威与公信力。

四、与时俱进、科学执法

除了前述的特征，《程序规定》还在调查取证方面引入了电子证据、网络巡查、远程取证等证据领域先进的概念与执法手段。

《程序规定》第二十条明确定义了“电子证据”[5]。相较于《最高人民法院关于适用<中华人民共和国民事诉讼法>的解释》第一百一十六条的规定，《程序规定》中的定义与互联网信息内容的执法现实更为贴近。此外，我们理解，《程序规定》还通过不完全列举的方式，以实际例证说明电子数据的具体类型，进一步增强了执法过程中认定电子数据的可操作性。

此外，第二十一条中涉及的“网络巡查”以及第二十九条的“远程取证”均是网络执法领域先进的执法手段。我们注意到，在文化部2012年颁布的《网络文化市场执法工作指引（试行）》中，就存在针对“网络巡查”、“远程取证”以及“电子数据分析与认定”的专章规定，且相关规定也具有较高的可操作性。[6]尽管网信部门在其实际执法过程中所实施的网络巡查与远程取证，是否会对工作指引中的规定进行援引或者参照仍需留待实践作进一步的明确，但引入证据领域前沿的执法手段本身已经体现了《程序规定》“与时俱进、科学执法”的态度。

以下，我们将对《程度规定》主要内容进行详细的梳理：

（一）主要内容概述

《程序规定》包括正文和附件两部分。正文总则部分首先明确了国家和地方网信办的执法主体地位，其作为“互联网信息内容管理部门”，依法对“违反有关互联网信息内容管理法律法规规章的行为”实施行政处罚。总则部分也对网信办执法工作进行了原则性规定，如执法工作应遵循公开、公平、公正原则，建立行政执法督察制度，建立健全执法人员培训、考试考核、资格管理和持证上岗制度等。其次，正文部分对网信办处理行政执法案

[2] 请见《程序规定》第四条和第五条。

[3] 请见《程序规定》第三十三条。

[4] 请见《程序规定》第四十八条以及相关附件。

[5] 请见《程序规定》的二十条第二款：“电子数据是指案件发生过程中形成的，以数字化形式存储、处理、传输的，能够证明案件事实的数据，包括但不限于网页、博客、微博客、即时通信工具、论坛、贴吧、网盘、电子邮件、网络后台等方式承载的电子信息或文件。电子数据主要存在于计算机设备、移动通信设备、互联网服务器、移动存储设备、云存储系统等电子设备或存储介质中。”

[6] 请见《网络文化市场执法工作指引（试行）》第三章、第四章和第六章的相关规定。

件的执法程序进行了细化，明确了案件管辖、立案、调查取证、听证、约谈、决定、执行等各环节的具体程序要求。此外，《程序规定》附件部分对列明了执法过程中常用的文书范本，对网信办执法过程中涉及的各类法律文书进行了统一性的规范。

（二）执法管辖规则

《程序规定》对互联网信息内容违法行为的管辖规则进行了明确，包括地域管辖、级别管辖、移送管辖、指定管辖等，具体内容如下：

具体规定			法律依据
地域管辖	• 违法行为发生地的网信部门 • 违法行为发生地：实施违法行为的网站备案地，工商登记地（工商登记地与主营业地不一致的，应按主营业地），网站建立者、管理者、使用者所在地，网络接入地，计算机等终端设备所在地等		第六条
级别管辖	• 国家网信办	应当由自己实施行政处罚的案件以及全国范围内发生的重大、复杂案件	第七条
	• 省级网信办	本行政区域内重大、复杂案件；省级网信办还可依据法律法规规章，结合本地区实际，制定本行政区域内级别管辖的具体规定	
	• 市（地、州）级以下网信办	本行政区域内行政处罚案件	
移送管辖	• 两个以上网信部门对同一违法行为均有管辖权时，由先行立案的互联网信息内容管理部门管辖 • 必要时可移送主要违法行为发生地的网信部门管辖		第八条第一款
	• 网信部门发现案件不属于其管辖的，应及时移送有管辖权的网信部门		第十条第一款
	• 网信部门对依法应当撤销互联网新闻信息服务许可、吊销互联网新闻信息服务许可证的，应当提出处理建议，并将取得的证据及相关材料报送原发证的网信部门，由原发证部门依法作出是否撤销许可、吊销许可证的决定		第十三条
指定管辖	• 两个以上的网信部门出现管辖争议无法协商解决的，报请共同上一级网信部门指定管辖		第八条第二款
	• 下级网信部门因特殊原因不能行使管辖权的，可报请上级网信部门管辖或指定管辖		第九条第二款
	• 受移送的网信部门认为移送不当的，应报请共同上一级网信部门指定管辖，不得再次移送		第十条第二款
	• 上级网信部门接到管辖争议或者报请指定管辖请示后，应在十个工作日内作出决定，并书面通知下级部门		第十一条
管辖变通	• 上级网信部门认为必要时，可以直接办理下级网信部门管辖的案件，也可将自己管辖的案件移交下级办理		第九条第一款

除上述提及的网信部门系统内的管辖规则外，《程序规定》第十二条还明确了跨部门的案件移送规则，即网信部门如发现案件属于其他行政机关管辖的，应当依法移送有关机关；若发现违法行为涉嫌犯罪的，应当及时移送司法机关。

（三）执法办案程序

《程序规定》对网信办执法流程进行了详细规定，主要包括立案、调查取证、听证、约谈、处罚决定、送达、执行、结案等环节，各环节主要内容如下表所示。

立案前	• **初查措施：**询问、勘验、检查、鉴定、调取证据材料等，不得限制初查对象的人身、财产权利。（第二十二条第一款）
立案	• **立案条件：**有涉嫌违法的事实；依法应当予以行政处罚；属于互联网信息内容监督管理行政处罚的范围；属于本互联网信息内容管理部门管辖（第十五条第一款） • **立案时限：**七个工作日内报负责人批准立案；特殊情况下可以延长至十五个工作日（第十五条第二款） • **承办人员：**确定两名以上执法人员为案件承办人（第十五条第二款）
调查取证	• **执法要求：**执法人员不得少于两人，并应当出示执法证。必要时可聘请专业人员进行协助。（第十八条第一款） • **保密义务：**执法人员对在办案过程中知悉的国家秘密、商业秘密、个人隐私、个人信息应当依法保密（第十八条第四款） • **取证类型：**电子数据、视听资料、书证、物证、证人证言、当事人的陈述、鉴定意见、检验报告、勘验笔录、现场笔录、询问笔录等（第二十条） • **责令改正：**对已有证据证明违法事实成立的，应当出具责令改正通知书，责令当事人改正或者限期改正违法行为（第三十二条） • **先行登记保存：**在证据可能灭失或者以后难以取得的情况下，经网信部门负责人批准，执法人员可以依法对涉案计算机、服务器、硬盘、移动存储设备、存储卡等涉嫌实施违法行为的物品先行登记保存，并在7日内作出处理决定（第二十七、二十八条）
听证、约谈	听证 • **适用范围：**拟作出吊销互联网新闻信息服务许可证、较大数额罚款等行政处罚决定（第三十三条） • **时限要求：**当事人在被告知后三日内提出；网信部门在听证七日前向当事人送达《举行听证通知书》，告知其时间地点（第三十四条） 约谈 • 网信部门作出行政处罚决定前，可以根据有关规定对其实施约谈，谈话结束后制作《执法约谈笔录》（第三十五条）
陈述、申辩	• **形式要求：**由网信部门填写《行政处罚意见告知书》，告知当事人拟作出行政处罚的违法事实、处罚的理由和依据，以及当事人依法享有的陈述、申辩权（第三十六条第一款） • **时限要求：**当事人应在收到告知书之日起三个工作日内提出陈述、申辩（第三十六条第二款）
处罚决定、送达	• **程序要求：**拟处罚决定应报网信部门负责人审查（第三十七条） • **复杂、重大案件的处理：**对情节复杂或者重大违法行为给予较重的行政处罚，网信部门负责人应当集体讨论决定（第三十八条） • **送达：**《行政处罚决定书》应当在宣告后当场交付当事人；当事人不在场的，应当在七日内依照民事诉讼法的有关规定送达当事人（第四十条）
执行、结案	• **当事人义务和权利：**在规定期限履行义务；有权提起复议、诉讼（第四十一条、第四十三条） • **跨部门案件处理：**违法行为需由电信主管部门关闭网站、吊销互联网信息服务增值电信业务经营许可证或者取消备案的，转电信主管部门处理。（第四十二条） • **强制执行：**当事人逾期不复议或起诉也不履行处罚决定的，可申请法院强制执行（第四十四条）

结语：利其器，为善其事

《程序规定》作为《网安法》下第一部专门的程序性部门规章，内容涵盖了从基本执法原则和制度、以及各个具体的执法环节，对网信部门执法活动的开展与落实将具有重要的现实意义。尤其是其中针对执法过程中从立案到结案各步骤的具体规定，对企业面临行政执法时如何应对并维护自身合法权益将具有重要的参考作用。此外，《程序规定》一并公布执法过程中可能涉及的附件文本这一举措，也显著提升了执法的透明度。

值得注意的是，“工欲善其事必先利其器”，而“利其器”也可能“为善其事”。《程序规定》的出台不仅使得互联网信息内容管理工作有章可循，其内容细致科学已经为行政执法提供了明确的操作指南。可以预见的是，《程序规定》将有助于互联网信息内容管理工作的迅速开展。因此，企业将需要在《程序规定》的基础上，也要密切关注国家网信部门在实际执法中可能适用的实体规则，以确保在自身合规建设时能充分参考法律法规规章的规定，并在面临行政执法时积极应对和配合，在最大限度内维护企业自身的合法权益。

（本文发布于2017年05月05日。）

开启互联网新闻监管新时代
——《互联网新闻信息服务管理规定》述评

2017年5月2日，国家互联网信息办公室（“**国家网信办**”）发布了《互联网新闻信息服务管理规定》[1]（“**《规定》**”）。如下文所述，相较于国务院新闻办公室（“**国新办**”）和前信息产业部于2005年联发的旧版《规定》（“**2005规定**”），此次的新规着眼于近十多年间互联网业态的高速发展，特别是近年来网络自媒体的广泛普及及其传播手段的多样化，确立了一系列崭新的监管思路和进路，从而为我国互联网新闻的监管开启一个新时代。

一、制定背景：全面落实国家网信办对互联网新闻的监管

在《规定》出台前，我国专门监管“互联网新闻信息服务”的法规是2005规定，彼时这一监管权限尚在国新办手中。2014年8月26日，国务院印发《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》（国发〔2014〕33号），正式将全国“互联网信息内容”的监管权限全面授权给当时重新组建的国家网信办。据此，国家网信办于2015年4月29日发布《关于变更互联网新闻信息服务单位审批备案和外国机构在中国境内提供金融信息服务业务审批实施机关的通知》，正式明确了其审批互联网新闻信息服务单位的职能。因此，《规定》的出台标志着国家网信办对互联网新闻信息服务所享有的监管权限的全面落地，也理顺了国务院的上级授权与国家网信办的下级监管职能间的关系，而不再使国家网信办处于“有权”却“无据”的境地[2]。

而另一方面，作为行将实施的**《网络安全法》**（“《网安法》”）所确定的网络安全领域的核心监管部门，国家网信办在《规定》中不仅将《网安法》明确列为立法依据之一，而且将《网安法》下的信息安全保护、用户实名制等要求有机融入《规定》对互联网新闻信息服务的监管，凸显了在全新的自媒体态势下，对于互联网新闻除业务监管和舆论监管以外的第三重重要监管维度即“网络安全监管”，从而使《规定》直接成为《网安法》的重要配套措施之一。

二、监管进路转变：变“主体设立监管”为“服务许可监管”

从2005规定到《规定》，互联网技术的快速发展和网络使用的普及彻底改变了互联网新闻的业态，即一方面，从原有的某些特定的掌握新闻信息资源的互联网新闻发布单位，大大扩展至人人都可制造时事评论类新闻信息的“自媒体生态圈”；另一方面，如下表所示，“互联网新闻信息服务”本身的内容也随技术发展而发生了很大变化，原有的某些服务类型（如时政类电子公告服务）甚至已几近消失，而代之以公众号、微博、网络直播等现已十分普遍的类型：

2005规定	《规定》
本规定所称互联网新闻信息服务，包括通过互联网登载新闻信息、提供时政类电子公告服务和向公众发送时政类通讯信息。（第二条）	通过互联网站、应用程序、论坛、博客、微博客、公众账号、即时通信工具、网络直播等形式向社会公众提供互联网新闻信息服务，……包括互联网新闻信息采编发布服务、转载服务、传播平台服务。（第五条）

在这方面，前后两种不同监管模式间的后续实践衔接值得关注。例如对于诸多已从国新办处取得“网站登载新闻业务”许可证的新闻类门户网站来说，这一业务类型在《规定》下已不存在。而2005规定也未明确此前已颁发的许可证的有效期。因此，这类已持证主体是否需申领新证，目前尚不明确。此外值得注意的是，《规定》[3]完全保留了2005规定[4]对于外资进入互联网新闻信息服务的严格禁止，以及对与外资开展相关业务合作的安全评估要求。因此，外资原已面临的准入禁止并未发生任何变化。正因如此，当前对互联网新闻的监管必须反映并因应这一全新态势。为此，《规定》不再因循2005规定所采用的以“新闻单位”

[1] 请参见：http://www.cac.gov.cn/2017-05/02/c_1120902760.htm。

[2] 因此也值得注意的是，《规定》并未废止2005规定，而是规定如有不一致之处，则以《规定》为准（请参见《规定》第二十九条）。

[3] 请参见《规定》第七条。

[4] 请参见2005规定第九条。

和“非新闻单位”之分，对提供互联网新闻信息服务的“单位”的“设立”进行分类审批或备案制监管的思路；而是改之以对“互联网新闻信息采编发布服务、转载服务、传播平台服务”这三大服务类型进行许可式监管，发以《互联网新闻信息服务许可证》，并通过设定《互联网新闻信息服务许可证》有效期和申请续办的程序加强持续监管。在这一新的监管模式下，除了对其中的特定服务类型（采编发布服务）设定额外的更严格的准入条件[5]之外，不论申请者是否为新闻单位，其所面临的申请条件[6]和材料要求[7]都是一致的。由此可见，《规定》大大弱化了申请者的新闻单位属性，而更为强调其在人员配置、内容审核、技术保障、信息安全等服务提供方面的资质。

三、自媒体监管：全方位确立传播平台的主体责任

《规定》的一大亮点，就是其充分注意到了近年来自媒体生态与互联网新闻的日益紧密结合，并就此确立了以下一系列有的放矢、可以实操的监管措施：

第十三条	传播平台服务提供者必须按照《网安法》第二十四条，要求用户提供真实身份信息，否则不得为其提供服务。
第十四条	传播平台服务提供者必须与用户签订协议；为用户开设公众号的，必须审核其账号信息、服务资质、服务范围等信息，并向所在地省级网信办分类[8]备案。
第十一、十二条	包括传播平台服务提供者在内的所有互联网新闻信息服务提供者都必须设总编辑，并由总编辑对信息内容负总责；还必须健全信息发布审核、公共信息巡查、应急处置等信息安全管理制度，以此来确保信息内容的日常合规。
第十六条	包括传播平台服务提供者在内的所有互联网新闻信息服务提供者发现违法违规内容的，都必须采取立即停止传输、消除等措施，保存有关记录并报告主管部门。

除上述措施外，笔者注意到《规定》中还有两项监管要求在事实上也可能达到监管自媒体的效果。其一是第十五条，即要求转载服务只能转载“国家规定范围内的单位发布的新闻信息”，这就堵死了借“转载服务”之名、随意传播自媒体类互联网新闻信息的可能；其二是第十七条，即要求服务提供者在“应用新技术”或“调整增设具有新闻舆论属性或社会动员能力的应用功能”的情况下，必须报网信办进行服务安全评估，这实际上是为今后在技术上出现新的传播手段所做的准备，从而使《规定》对自媒体的监管不致因为技术的发展而沦为一纸空文。由此可见，《规定》对以自媒体形式传播的互联网新闻信息的监管，主要是着眼于传播平台的提供者，而非在其之上发布信息的一个个用户自身。这符合当前互联网服务监管的基本逻辑，即抓平台而非抓用户，透过抓平台来间接辐射平台上的用户。从以上措施可以看出，《规定》监管自媒体的核心在于“内容”，通过确立平台在注册-签协议-日常监管-事后处置这一全链条中的主体责任，确保用户及其发布在平台上的内容既要“看得见”，更要“管得着”，而不允许出现用户无从追溯、内容随意发布的互联网新闻“法外之地”。

结语：“大网络监管”的概念正在浮出水面

《网安法》实施在即，其所传递出的同时兼顾“内容安全”、“信息安全”、“技术安全”等的监管思路，在《规定》中已经有了一定程度的运用和体现。就《规定》本身所监管的互联网新闻信息服务而言，这一方面要求相关服务提供者明晰并落实自己的主体责任，特别是平台提供者既要做互联网新闻信息的传播者，更要扮演好“内容防火墙”的角色；另一方面也要求用户在享受互联网带来的信息发布便利的同时，更要实名出现、谨言慎行，不触碰法律所划定的“红线”。

而《规定》所引发的一个颇值得思考的点在于，对于互联网新闻这种以多种样态，如文字、图片、音视频等呈现的信息内容，其所涉的不同领域的监管之间是否应建立起某种内生性的统一逻辑和协调机制？在这方面，笔者注意到《规定》明确要求互联网新闻信息服务提供者在遵守《规定》的同时，也要符合电信（互联网信息服务）、互联网视听节目、网络出版等服务领域的监管要求[9]。这就在实际上使《网安法》所统领的“大网络监管”的概念呼之欲出，即在保持各行业主管部门监管权限的同时，将《网安法》对于“内容安全”、“信息安全”、“技术安全”等的要求以协调一致的方式渗透进各个单行法规和各行业主管部门的监管实践之中，从而使服务提供者和用户不论进入哪个具体服务领域，都可以遵行统一的行为标准，这无疑将有利于企业等市场主体在一种相对稳定和可期待的监管环境中开展网络经营活动。

（本文发布于2017年05月04日。）

[5] 请参见《规定》第六条第二款。《规定》第八条还特别要求，采编业务和经营业务必须分开，非公有资本不得介入采编业务。

[6] 请参见《规定》第六条。

[7] 请参见《规定》第十条。

[8] 如何分类尚有待明确。我们理解可能会基于开设公众号的用户的主体类型（个人或机构）、发布的新闻信息的种类（如时评类、突发新闻类等）等标准进行分类，对此尚有待进一步观察确认。

[9] 请参见《规定》第六、二十一、二十八条。

第三部分：网络安全

羌笛何须怨杨柳，春风“已”度玉门关
——《网络安全法》元年纪要及展望

2017年是《网络安全法》（以下简称“**《网安法》**”）正式生效施行的元年，也是承前启后的一年。《网安法》是对以往我国各行业网络安全监管制度的一次系统性的梳理，同时在“国家网信部门统筹协调，各行业主管分别负责”的新监督管理体系下，《网安法》的生效施行也标志着我国的网络安全监管进入了新的发展阶段。

事实上，《网安法》2017年6月1日的正式施行，加快了相关的部门规章、司法解释、国家标准的出台速度，目前有多个部门规章和国家标准正在广泛征求公众意见。此外，涉及多个方面的网络安全执法工作也在各个行业内迅速展开，网信部门、电信主管部门、公安部门等都已经在各自职责范围内加大网络安全的执法力度。《网安法》的出台和后续动作一时可谓“东方夜放花千树”，受到了海内外企业、组织与媒体等的多方关注。

一、立法现状

在《网安法》成文之前，我国对于网络安全保护的监管规则多散见于各部委的各项规定中。由于缺乏上位法的框架，监管规则多呈现出“碎片化”的特点，且多个执法机构的监管实践中还可能存在冲突。《网安法》出台的重大意义之一在于，从法律层面梳理了网络安全监管的体系，明确了各执法部门的职责，使得后续配套措施能够“顺理成章”。《网安法》在审议通过至目前生效实施以来，国家互联网信息办公室（以下简称“国家网信办”）与各行业的主管与监管部门、国家与行业的标准制定组织等机构共同协作，根据《网安法》相关条款的规定陆续发布了一系列相关的规定与配套措施，务求为《网安法》中相关制度的实施提供更具体的指引，力争建立一套完整且有效的监管体系。

（下表整理了截止目前网络安全领域主要的立法工作成果和进度）

规范名称	发文机关	发文日期/生效日期
1. 国家战略		
《国家网络空间安全战略》	国家网信办	2016年12月27日
《网络空间国际合作战略》	外交部、国家网信办	2017年3月1日
2. 法律与司法解释		
《网安法》	全国人大常委会	2016年11月7日发布， 2017年6月1日生效
《民法总则》	全国人大常委会	2017年3月15日发布， 2017年10月1日生效
《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》	最高人民法院、最高人民检察院	2017年5月8日发布， 2017年6月1日生效
《电子商务法（草案二次审议稿）》	全国人大常委会	2017年11月7日稿

规范名称	发文机关	发文日期/生效日期
3. 行政规章与其他配套措施		
《关键信息基础设施安全保护条例（征求意见稿）》	国家网信办	2017年7月10日稿
《个人信息和重要数据出境安全评估办法（征求意见稿）》	国家网信办	2017年4月11日稿
《互联网新闻信息服务单位内容管理从业人员管理办法》	国家网信办	2017年10月30日发布， 2017年12月1日生效
《互联网新闻信息服务新技术新应用安全评估管理规定》	国家网信办	2017年10月30日发布， 2017年12月1日生效
《互联网群组信息服务管理规定》	国家网信办	2017年9月7日发布， 2017年10月8日生效
《互联网用户公众账号信息服务管理规定》	国家网信办	2017年9月7日发布， 2017年10月8日生效
《互联网论坛社区服务管理规定》	国家网信办	2017年8月25日发布， 2017年10月1日生效
《互联网跟帖评论服务管理规定》	国家网信办	2017年8月25日发布， 2017年10月1日生效
《互联网新闻信息服务许可管理实施细则》	国家网信办	2017年5月22日发布并生效
《互联网信息内容管理行政执法程序规定》	国家网信办	2017年5月2日发布， 2017年6月1日生效
《互联网直播服务管理规定》	国家网信办	2016年11月4日发布， 2016年12月1日生效
《国家网络安全事件应急预案》	国家网信办	2017年1月10日发布并生效
《网络产品和服务安全审查办法（试行）》	国家网信办	2017年5月2日发布， 2017年6月1日生效
《网络关键设备和网络安全专用产品目录（第一批）》	国家网信办、工信部、公安部、 国家认证认可监督管理委员会	2017年6月1日发布并生效
4. 国家与行业标准		
《个人信息安全规范》	全国信息安全标准化技术委员会	2018年1月2日发布， 2018年5月1日生效
《个人信息去标识化指南（征求意见稿）》	全国信息安全标准化技术委员会	2017年8月25日稿
《关键信息基础设施安全检查评估指南（征求意见稿）》	全国信息安全标准化技术委员会	2017年8月30日稿
《关键信息基础设施安全保障评价指标体系（征求意见稿）》	全国信息安全标准化技术委员会	2017年8月30日稿
《网络产品和服务安全通用要求（征求意见稿）》	全国信息安全标准化技术委员会	2017年8月30日稿
《网络安全等级保护测评过程指南（征求意见稿））》	全国信息安全标准化技术委员会	2016年11月3日稿
《网络安全等级保护测评要求（各部分内容）（征求意见稿）》	全国信息安全标准化技术委员会	第1部分：2016年11月3日稿； 第2部分：2017年1月11日稿； 第3部分：2016年11月3日稿； 第4部分：2017年1月11日稿； 第5部分：2017年1月11日稿。
《数据出境安全评估指南（征求意见稿）》	全国信息安全标准化技术委员会	2017年8月30日稿
《关键信息基础设施识别指南》（制定中）		

从目前立法进展来看，我国网络安全领域的立法体现了全面、创新和多层次的特点。

第一，我国网络安全领域的立法内容丰富全面。《网安法》在 “网络运行安全”与“网络信息安全”两大维度下，分别规定了网络运营者的权利、义务和责任，以及国家为维护网络安全所需要建立的监测预警与应急处置等机制。对于网络运行安全而言，《网安

法》针对网络运营者和关键信息基础设施运营者两类主体，从内部制度、技术措施、采购对象、数据存储和跨境传输等多个方面规定了相应的责任和义务。除一般网络运行安全规定以外，《网安法》梳理了此前散见在不同规范性文件中关于个人信息保护的规定，如在第四章集中整理了网络运营者在保护个人信息安全方面的义务，以及个人信息主体的重要权利，并在第六章中为侵害个人信息权利的行为拟定了相应的法律责任。除此以外，《网安法》还对于网络信息内容管理做出了提纲挈领的要求。在国家网信办后续出台的互联网信息内容管理的部门规章以及规范性文件中，针对网络信息内容管理工作从行业、执法程序以及适用场景等多个方面进行了全面的细化，比如《互联网新闻信息服务管理规定》、《互联网信息内容管理行政执法程序规定》、《互联网新闻信息服务新技术新应用安全评估管理规定》以及《互联网论坛社区服务管理规定》等。

第二，《网安法》及其配套措施从立法技术和内容上都体现了创新性。从立法技术上看，《网安法》一方面梳理总结了行业中的现有规定，除个人信息保护的相关规定以外，比如《网安法》规定的“网络安全等级保护制度”就源于1994年国务院制定的《计算机信息系统安全保护条例》中规定的计算机信息系统安全等级保护制度，该制度在2007年公安部等部门制定的《信息安全等级保护管理办法》中也得到了细化。因此“网络安全等级保护制度”是对于现有制度的总结和归纳。另一方面，《网安法》及其配套措施也在原有的制度上做了创新性的统筹协调。比如，根据《网安法》制定和公布的网络关键设备和网络安全专用产品目录，就避免了多个政府部门分别对网络相关设备和产品进行安全认证及检测所导致的重复认证和检测工作，有利于减少资源浪费，减轻企业负担。

从立法内容来看，《网安法》还首次在法律层面提出了“网络运营者”、“关键信息基础设施”、“网络安全时间应急预案”等新的概念和机制。以“关键信息基础设施”为例，将相继出台的《关键信息基础设施安全保护条例》、《关键信息基础设施安全检查评估指南》、《关键信息基础设施识别指南》及《关键信息基础设施安全保障评价指标体系》等将建立一个围绕“关键信息基础设施保护”的新监管体系。

第三，网络安全领域的规则建立，是通过“战略-法律-法规-国家及行业标准”的次序和层次做到“层层递进，逐步落实”的。两项国家战略《国家网络空间安全战略》与《网络空间国际合作战略》虽然没有拟定具体的权利义务实施规则，但作为我国网络空间安全领域顶层设计的重要组成部分，为具体规则与制度的建立和落实提供了纲领性的指引。《网安法》作为网络安全领域基础性法律，规定了网络运行安全及网络信息安全等领域的基本内容。而最重要的行政法规与相关配套措施，则是《网安法》切实落地推行的重要依据。该类规则通常是基于《网安法》特定的条款，针对其中所涉及的法律主体的权利与义务关系进行具化，从而提供具有法律约束力的规则指引。此外，国家与行业标准也是网络安全领域立法工作的有益补充，即使推荐性标准可能不具备强制约束力，但能在相关法律法规的逻辑框架下对特定问题进行了细化和补充，在一定程度上反映监管态度，并为执法、司法与合规实践提供更具操作性的指引。

总而言之，我国在网络安全领域的立法工作，正从不同的规范层级、不同的法益主体出发全面展开。在国务院的领导、国家网信部门的统筹协调以及各部委的充分合作下，《网安法》配套立法涵盖的内容广泛、形式多样，发展迅速。我们呼吁社会各界站在国家整体网络安全保障战略的高度下，一方面充分参与立法活动，发表意见，确保规则的有效性和实操性；另一方面也广泛关注《网安法》及其配套措施的落实情况，共同推动我国网络安全制度建设。

二、执法动态

随着《网安法》施行以及相关配套措施的陆续出台，国家网信办、地方网信部门与其他执法机关也正逐步有序地开展网络安全领域的执法活动。由于网络安全领域的规定涉及的合规义务较多，而各个执法机关也分别在各自的职责范围内展开执法，目前的执法活动呈现出执法主体和执法内容多样化的特点。我们将典型的执法活动小结如下表：

执法日期	案例内容	执法内容	小评
网络运行安全			
1. 网络安全等级保护制度			
2017年8月	四川省、重庆市、安徽蚌埠、黑龙江哈尔滨、广东广州等多地的网安执法部门根据《网安法》第二十一条（网络安全等级保护制度），对现实中存在的“未定级备案”、“未落实网络安全主体责任”、“未建立网络安全防护技术措施”、“未落实真实身份信息登记和网站备案相关要求”等违法行为进行积极的查处。	《网安法》第二十一条：网络安全等级保护制度	网络安全等级保护制度是保障网络运行安全的基础制度。

执法日期	案例内容	执法内容	小评
2. 网络用户身份管理制度——“网络实名制”			
2017年9月	深圳市三人网络科技有限公司未要求用户提供真实身份信息提供网络电话服务，存在被利用于从事信息通信诈骗活动的安全隐患；此行为被广东省通信管理局责令整改，罚款五万元，并责令停业整顿，关闭网站。	《网安法》第二十四条：网络用户身份管理制度	网络用户身份管理制度一般遵循“后台实名、前台自愿”的原则；网络实名制也同时使得网络服务提供者承担个人信息安全保护的义务。
3. 关键信息基础设施的认定与保护			
2017年8月8日	据PaRR报道，目前国内已有400-500家企业被列入CII名单之中，其中大部分为国有企业。根据《网安法》相关规定，国家互联网信息办公室将每年统筹协调有关部门对CII运营者开展全国性检测；2017年的检测工作已顺利开展。	《网安法》第三十一条：关键信息基础设施的认定与保护	如何识别CII是CII安全保护制度落实的重要和基本前提，而CII安全保护制度的建设与实践则是我国网络安全体系的核心之一。
网络信息安全			
1. 个人信息保护			
2017年9月	中央网信办、工信部、公安部、国家标准委四部门在7月份联合开展隐私条款专项工作，首批评审的十款网络产品和服务包括微信、新浪微博、京东商城、百度地图、航旅纵横、携程网等。该评审于2017年9月底正式结束，各评审部门向参与评审的十款应用均反馈了相应的改进意见，参评企业积极配合，均按照评审要点进行相应整改上线。	《网安法》第四十条至第四十四条：个人信息的保护	隐私政策作为手机用户个人信息的第一道“闸门”，将是个人信息保护工作的第一步。隐私政策的制定和修改应结合产业的特殊性，做到个人信息保护和商业性的平衡。
2017年6月	监管部门对市场中非法交易数据等乱象出手，正式开始清理行动。据报道，公安部公共信息网络安全监察局正在制定专项治理方案，已将调查名单扩大到30多家，业内知名的大数据公司悉数在此次调查范围之内。	《网安法》第四十条至第四十四条：个人信息的保护	随着大数据行业的发展，执法机关将进一步重视大数据企业在数据（尤其是个人信息）收集、使用方面的合法合规问题。
2. 互联网信息内容管理			
2017年8月	北京、广东、浙江、江苏等地网络安全执法部门主动出击，针对平台或网站上“传输法律、行政法规禁止传输的信息”、“传播暴力恐怖、虚假谣言、淫秽色情等危害国家安全、公共安全、社会秩序的信息”或“存在导向不正、低俗恶搞等有害信息”等行为依法进行查处，务求肃清互联网上可能存在影响网络信息安全的不良因素。	《网安法》第四十七条：网络信息管理	互联网信息内容管理，是国家网络安全必不可少的组成部分。互联网平台未来将对信息内容管理承担更大的责任和义务。

从主要的执法案例中不难发现，目前网络安全的执法工作虽然针对的依然是网络安全领域的核心内容，如网络安全等级保护义务、个人信息保护与关键信息基础设施安全防护等，但在具体的执法活动中已逐步呈现出多样化、全面化的趋势。即使相关制度的《网安法》配套措施仍未落地，在事实上并不影响执法机关根据《网安法》中的相关规定对明显违法的行为进行查处。

另外，除传统的行政调查，目前网络安全领域的执法还出现了联合专项检查等新的方式，比如中央网信办、工信部、公安部、国家标准委四部门在7月份联合开展的隐私条款专项工作。可以预见的是，由多个部门联合针对主要企业启动的评审与检查也是未来网络安

全执法的其重要形式之一。通过对主流网络产品与服务的督查，既能够积极带动提升全行业的网络安全合规意识，还可以向社会各界普及网络安全的重要性。

三、展望与建议

（一）配套措施将进一步细化，国家与行业标准值得重视

就立法活动而言，随着网络安全领域规则框架的建立，未来多个《网安法》配套措施的出台将为机关执法以及企业合规提供更为具体的实施规则与操作指引。例如，《关键信息基础设施安全保护条例》与《关键信息基础设施识别指南》将有望正式出台、落地，以便更充分地落实相应的安全保护义务，也有利于国家对关键信息基础设施的防护提供更多的支持与协助。除此以外，《个人信息和重要数据出境安全评估办法》与《信息安全技术 数据出境安全评估指南》也可能在明年定稿并最终颁布，备受关注的数据跨境安全评估的主体、范围和监管方式将最终得到确认。此外，网络安全等级保护制度对应的国家指南将进一步澄清其与传统计算机信息系统等级保护制度之间的关系，并为实际的操作提供更明确的指引。

值得注意的是，网络安全合规工作有着很强的技术性要求，而无论是《网安法》下的部门规章还是规范性文件，其本身性质决定了其不可能为网络安全合规工作提供具体的技术性要求。因此以国家标准与行业标准为代表的“指南性质”文件未来将成为网络安全执法以及企业合规的重要参考性材料。这些国家与行业标准，比如即将生效的《个人信息安全规范》，既能以细致的技术规定和要求指导执法机关的执法以及企业的合规工作，又能够利用其灵活性适应日新月异的技术更迭对法律稳定性所带来的冲击。

（二）网安执法“重点突破”，未来会“全面开花”，执法有望趋于常态化

目前的网络安全执法还处于比较初步的阶段，可以预见《网安法》下比如网络等级保护制度，关键信息基础设施保护以及个人信息保护等重点问题依然会是未来网络安全执法的重点。但随着《网安法》配套措施的落地，其他比如数据跨境传输安全评估、网络产品与服务采购的国家安全审查等执法工作也将全面展开。与此同时，具备充分实体执法依据的互联网信息与内容管理，也可能会根据《互联网信息内容管理行政执法程序规定》正式全面推进执法实践。

另一方面，考虑到网络运营者的范围较广，网络运营者的责任和义务的主体不局限于互联网企业，还可能包括众多传统行业的内外资企业。而对于执法机构而言，随着执法机关之间的协调与分工将进一步明确，以国家网信办为核心、各行业主管部门为骨干的执法体系也将日益完善。由于网络安全问题较多，执法主体力量充实，我们可以预期未来网络安全执法可能成为一种常态。

（三）建议

对立法和执法机构而言，不同于传统行业，网络安全领域有着技术性强、行业更新迅速的特点。在网络空间主权的大背景下，网络安全领域的立法和执法一方面是为了维护网络安全，保障国家安全，另一方面受到充分保护的网络环境也能够增强综合国力，提高企业市场竞争力。因此，我们建议立法和执法机构在规则制定以及实践监管中广泛征求企业及技术专家的意见，充分尊重行业发展的规律，力争做到维护网络安全与增强行业竞争力的双重效果。

对于企业而言，要认识到网络安全合规工作的紧迫性，也要理解网络安全合规工作未来可能为企业竞争力带来的良性影响。树立“技术+合规”的理念，尽早梳理内部网络安全和数据合规的漏洞，建立内部完善的合规制度，利用技术和合规的双重手段确保企业的顺利发展。

目前我国已经成为全球最大的网络市场，根据腾讯安全正式发布的《2017年上半年互联网安全报告》，截至2016年12月，我国网民规模达7.31亿，相当于欧洲人口总量。但令人担忧的是，尽管我国网络经济发展迅速，仍有其他国家对我国网络安全现状持怀疑态度，认为中国缺乏对于网络安全的监管，使得中国网络经济处于高速但不稳定的发展轨道。尽管我国一直以来从未轻视网络安全问题，但缺乏明确的监管体系加剧了他国对我国网络安全的不信任感。随着大数据技术和经济的发展，未来数字经济呈现全球一体化的发展趋势，而数据的跨境流动将不可避免。目前包括中国在内的多个国家和地区已经要求在数据跨境中对数据接收国的网络安全情况进行评估，而遗憾的是中国往往不在被认为具有同等网络安全保护程度的“白名单”内。为了维护我国网络安全、网络主权以及国家安全，同时也为了保障我国在未来全球数字经济中的地位，《网安法》及其配套措施的出台和落地正当其时。面对我国网络安全监管缺位的质疑，我们可以自信地说，羌笛何须怨杨柳，春风“已”度玉门关。同时我们也期望，借着《网安法》的一夜春风，未来我国网络安全发展也能“千树万树梨花开”！

（本文发布于2018年01月10日。）

注：本文首载于律商联讯《中国法律透视》2017年终刊。

《网络安全法》来了！
——企业应该知道的五件事

就在昨天（2016年11月7日），《中华人民共和国网络安全法》（“**《网安法》**”）历时近一年半、在三易其稿后终获全国人大常委会通过，并将于2017年6月1日起正式施行。在整个制订过程中，《网安法》因其对我国网络安全领域的全面规制和重大影响而广受社会各界，特别是经营互联网相关业务的企业的高度关注。本文第一时间从此类企业、特别是在华外资企业的角度，对《网安法》主要条款及要求做一梳理，并总结出企业应该知道的关于《网安法》的五件事。

一、适用范围：境内广泛的“网络服务提供者”均受到规制

《网安法》第二条开宗明义，将其适用范围确定为“**在中华人民共和国境内**建设、运营、维护和**使用网络**”。《网安法》第七十六条第（一）项将“网络”定义为“由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统”，可见网络必须以一定的物理形式存在。据此，我们理解，在我国“境内”使用“网络”至少意味着，相关的使用行为（包括企业为自身业务经营目的而使用网络）必须依托位于我国境内的网络物理设施。换言之，如果一个主体完全在中国境外、利用位于境外的网络设施在线提供服务，即使由于互联网的互联互通性使得在我国境内也可获取该等服务，《网安法》的前述定义似乎并不规范该等主体的行为。但是，这并不意味着《网安法》对该类主体的行为可能在中国境内造成的影响完全放任不管。例如其第五十条规定，如果网信等有关部门发现来源于我国境外的信息属于我国法律法规禁止发布或者传输的，应当通知有关机构采取技术措施和其他必要措施阻断该等信息的传播。

与此同时，《网安法》确立了“网络运营者”这一核心概念，即是指“网络的所有者、管理者和**网络服务提供者**”[1]，其中的“网络服务提供者”即为“通过网络提供服务”的主体[2]。鉴于对该等“服务”未做进一步的限制或明确[3]，《网安法》关于“网络服务提供者”及“通过网络提供服务”的表述的覆盖范围实际上是非常广泛的，可以指向任何使用网络为媒介提供服务的主体，这就不仅包括以网络在线业务为主业的互联网企业，例如目前已十分普及的应用商店、电商平台、网约车平台等，还有可能包括因其线下业务向线上延伸而同样需要借助网络的传统线下企业。由此而言，《网安法》的触手实际上伸向了当前网络服务业态的方方面面。

特别值得注意的是，《网安法》的适用对象并无内外商之别，只要是在我国境内通过网络提供服务，不论是内资还是外资企业，都同等受制于《网安法》的各项规定和要求。但如下文所指出的，《网安法》的某些规定因其特殊性，可能会对在华运营的外资企业产生比内资企业更为显著的影响，因此外资企业需要格外关注《网安法》及其后续实施。

[1] 参见《网安法》第七十六条第（三）项。

[2] 参见《网安法》第十条。

[3] 我们注意到在《网安法》一审稿下，“网络运营者”曾被明确为“包括基础电信运营者、网络信息服务提供者、重要信息系统运营者等”（一审稿第六十五条第（三）项），但在其后的二、三审稿及正式案文中均未再出现，可见立法者对这一定义有意采取了模糊处理的态度。

二、网络运行安全：尚不明朗的“网络安全等级保护制度”

《网安法》用整个第三章共19条的篇幅（接近全文四分之一），为包括网络服务提供者在内的网络运营者规定了一系列保护“网络运行安全”方面的要求和义务。其中的第二十一条明确规定，国家实行“网络安全等级保护制度”，并要求网络运营者按照这一制度的要求履行其网络运行安全保护义务。此外，第三十一条还规定，对于“关键信息基础设施”（详见以下第三部分讨论）要在网络安全等级保护制度的基础上实行重点保护。

值得注意的是，这是我国法律首次提出“网络安全等级保护制度”这一概念。但《网安法》并未进一步阐明该制度的内涵，也没有说明该制度将如何实施以及“网络安全等级”具体又将如何划分和确定。与此相关的是，在《网安法》出台之前，我国已通过相关法规确立了两项涉及网络安全的等级保护制度，分别是“计算机信息系统信息安全等级保护”[4]和“通信网络单元安全分级防护”[5]。前者侧重于对包含网络在内的计算机信息系统实施共分五级的安全保护，后者则专门着眼于对我国境内的电信业务经营者和互联网域名服务提供者管理和运行的公用通信网和互联网（统称“通信网络”）进行单元划分并实施同样共分五级的网络安全防护。由此而言，这两项制度至少在涉及网络及其安全的限度内，与《网安法》确立的“网络安全等级保护制度”间应该存在着交叉或重叠。但鉴于《网安法》的规定尚不明确，我们目前暂无法判断“网络安全等级保护制度”与这两项制度之间的具体关系，也不能确定在未来《网安法》的实施过程中，“网络安全等级保护制度”是将完全取代这两项制度，还是在这两项制度的基础上对其进行某种程度的整合或修改，抑或是完全独立于这两项制度之外单独构建和实施。

就此我们注意到，上述两项制度均基于分级的不同，对计算机信息系统/通信网络的运营者设定了不同的要求。例如，只有第二级以上（直至第五级）的计算机信息系统才需要向公安部门备案[6]，而只有第三级以上的计算机信息系统或第二级以上的通信网络才需要进行定期安全自查或评估或接受定期安全检查[7]。如果“网络安全等级保护制度”也是依循这样的监管思路，那么这对于通过网络提供不同种类和不同风险程度服务的企业判断其未来在《网安法》下担负网络运行安全保护义务的程度有着重要借鉴意义。我们注意到，《网安法》使用了网络服务“**提供者**”、而非“**经营者**”的概念。以“互联网信息服务”为例，按照现有法律规定，“经营性”即有偿互联网信息服务的提供者需要申领ICP证，而“非经营性”即无偿服务的提供者只需进行ICP备案[8]。前者例如一家电商平台，后者例如某一企业仅用于公开发布企业信息、而不涉及任何信息有偿提供的网站。在实践中，这样的电商平台和企业网站在所传递的数据、是否收集用户个人信息、发生网络安全事件的可能性大小、面临的遭受攻击或数据泄露的风险程度、所需要的安全防护措施等各个方面存在根本性不同，如果要求他们在《网安法》之下承担完全同等的网络运行安全保护义务，显然是不合理的。例如，《网安法》第二十一条要求网络运营者“采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月”，并“采取数据分类、重要数据备份和加密等措施”。这些措施对于一家电商平台而言，显然是合理而必要的，但对于一个企业网站来说，不但可能不必要，而且很可能不可行。从这个意义上来讲，我们认为这也是《网安法》在要求网络运营者履行网络运行安全保护义务之前加上“按照网络安全等级保护制度的要求”这一条件的原因。因此，对于任何落入“网络服务提供者”范畴的企业来说，进一步关注“网络安全等级保护制度”的后续发展就显得尤为重要。

当然，相较于尚不明朗的“网络安全等级保护制度”，《网安法》为网络运营者设定的其他一些网络运行安全保护义务已经非常明确。例如第二十四条要求为用户“办理网络接入、域名注

[4] 参见《中华人民共和国计算机信息系统安全保护条例（2011修订）》第九条，以及根据该条由公安部、国家保密局、国家密码管理局和国务院信息工作办公室于2007年6月22日联合发布实施的《信息安全等级保护管理办法》。

[5] 参见工信部发布并于2010年3月1日起实施的《通信网络安全防护管理办法》。

[6] 参见《信息安全等级保护管理办法》第十五条。

[7] 参见《信息安全等级保护管理办法》第十四、十八条；《通信网络安全防护管理办法》第十一、十二条。

[8] 参见《互联网信息服务管理办法（2011修订）》第三、四条。

册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务”的网络运营者在与用户签订协议或确认提供服务时，必须要求用户提供其真实身份信息，否则不得为其提供相关服务。再如第二十八条以一种十分宽泛的表述，再度确认了此前相关法律[9]已为电信业务经营者、网络服务提供者等规定的配合执法义务，并将之适用于所有网络运营者，即要求他们“为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助”。

三、“关键信息基础设施”：《网安法》首次提出但仍留下悬念的概念

在此次《网安法》的出台过程中，最受关注的事项之一便是其首次提出的“关键信息基础设施”这一概念。受关注的原因主要有三：一是按照其目前的定义表述，其潜在的覆盖范围十分广泛，可能影响数量众多的企业；二是其为相关运营者设置了更高的、负担更重的网络安全保护义务；三是下文所述的其对相关个人信息和业务数据传输至境外的独特限制。

值得注意的是，对“关键信息基础设施”界定和范围的表述在《网安法》制订过程中也是三易其稿：一审稿从行业、用途、用户数量等角度划定其范围[10]；二审稿去除了其行业和用途属性，转而强调其在安全方面的特殊重要性[11]；三审稿及正式案文则将其行业特性和安全意义结合起来，同时从这两个角度对其进行界定[12]。但无一例外，各稿均规定，关键信息基础设施的“具体范围”和“安全保护办法”将在《网安法》之外，由国务院另行制定。由此可见，对于如何界定这样一个首次提出并可能在监管实践中产生广泛影响的法律概念，立法者是十分慎重的，也表明立法者和监管者已经注意到了这一概念所引发的关注和讨论，并需要更多时间、通过更深入的研究来厘清其准确的内涵和外延。

因此，在相关配套措施进一步出台之前，对于关注其自身是否会落入“关键信息基础设施运营者”监管范畴的企业来说，《网安法》的确留下了一个很大的悬念。特别是按照《网安法》第三十一条的表述，关键信息基础设施涵盖“公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域”，这是否表示所有已列明的“重要行业和领域”内信息基础设施都自动属于“关键”，此外是否还有其他未列明的“重要行业和领域”等都要留待国务院的规定来明确。

我们注意到《网安法》为关键信息基础设施运营者设定的一些义务，在其他法律法规中能够找到与之相似的规定。例如，《网安法》第三十一条明确将对关键信息基础设施的安全保护建立在网络安全等级保护制度的基础之上；第三十八条则要求关键信息基础设施运营者每年至少自行或委托专业机构进行一次安全风险检测评估。类似地，规定了计算机信息系统信息安全等级保护制度的《信息安全等级保护管理办法》要求安全等级为第三级的计算机信息系统的运营者每年至少进行一次安全自查以及委托专业机构进行一次安全等级测评。如以上第二点中所讨论的，我们目前尚无法判断这两项制度间是否存在或存在着怎样的联系，但就每年至少进行一次安全评估这项要求而言，《网安法》下的关键信息基础设施和《信息安全等级保护管理办法》下的第三级信息系统至少存在着明显的相似之处。当然，这完全不足以在关键信息基础设施和第三级以上计算机信息系统之间划上等号。但我们认为进行这种对比的意义在于，在关键信息基础设施的范围得以明确之前，相关企业至少可以从目前较为确定的类似制度中窥见监管者今后对关键信息基础设施可能的监管路径和思路。

四、个人信息保护：对特定个人信息境外传输的限制

在“网络运行安全”之外，《网安法》的另一侧重点在于保护“网络信息安全”，特别是网络运营者收集和使用的“个人

[9] 例如可参见：《国家安全法（2015）》第七十七、七十九条；《反恐怖主义法》第十八条；《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》之十。

[10] 参见一审稿第二十五条：“国家对提供公共通信、广播电视传输等服务的基础信息网络，能源、交通、水利、金融等重要行业和供电、供水、供气、医疗卫生、社会保障等公共服务领域的重要信息系统，军事网络，设区的市级以上国家机关等政务网络，用户数量众多的网络服务提供者所有或者管理的网络和系统（以下称关键信息基础设施），实行重点保护。”

[11] 参见二审稿第二十九条：“国家对一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。”

[12] 参见三审稿及正式案文第三十一条：“国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。”

信息”的安全[13]。《网安法》将个人信息定义为“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”[14]，与此前已经出台的涉及个人信息保护的法律法规[15]一样，强调其对个人身份的“可识别性”。与此同时，在网络运营者的个人信息保护义务方面，《网安法》也在很大程度上保持了与既有法律法规的一致，例如要求网络运营者收集、使用个人信息应当“遵循合法、正当、必要的原则”，“明示收集、使用信息的目的、方式和范围”，“经被收集者同意”，“公开收集、使用规则”，“不得泄露、篡改、毁损其收集的个人信息”，“未经被收集者同意，不得向他人提供个人信息”，“采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失”等等[16]。

《网安法》在个人信息保护方面引起最大关注的，是其首次在法律层级上对特定个人信息必须存储在我国境内做出明确规定。这里的“特定”并非指个人信息的内容或类型，而是指向其收集主体和渠道，即“关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息”。[17]换言之，并非所有网络运营者收集的个人信息都要存储在我国境内，而仅限于“关键信息基础设施运营者”在其“在中国境内”的“运营活动”中收集和产生的个人信息。这一要求同时还适用于满足前述条件的“重要业务数据”，尽管《网安法》并未指明何为“重要”业务数据。

这就意味着，一旦落入“关键信息基础设施的运营者”范畴，《网安法》将直接影响到其将在中国境内运营过程中收集和产生的个人信息和业务数据向境外传输的行为。而就我们所知，在当前国内外市场已深度融合，内资企业想要“走出去”、外资企业想要“走进来”的大背景下，以企业为主体的个人信息和业务数据的跨境流动在现实中已经十分普遍，特别是对涉及通过互联网提供“信息服务”的企业而言更是如此。因此，关键信息基础设施的范围及其带来的数据传输限制，对部分企业业务的有效乃至正常开展可能会产生根本性影响，甚或造成实质性阻碍。

当然，我们注意到《网安法》为这项限制留了一个缺口，即如果关键信息基础设施运营者出于业务需要，确实需要向境外传输个人信息或重要业务数据，则《网安法》允许其在“按照国家网信部门会同国务院有关部门制定的办法进行安全评估”[18]之后进行该等传输。但在这一办法出台之前，我们无从知晓此类安全评估的门槛，也难以预判这一例外情形的援用难度。此外，在我们看来，“因业务需要，确需向境外提供”这样的表述也为相关部门的自由裁量留下了很大空间。

五、对“网络关键设备和网络安全专用产品”的专门要求

同样出于保障网络安全的考虑，《网安法》在主要规制网络运营者行为的同时，对于“网络关键设备和网络安全专用产品”的相关经营者也设定了专门要求，即此类设备和产品只有“按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供”[19]。这就意味着，一家企业即使不属于网络运营者，只要其从事“销售”或“提供”此类设备和产品的业务，同样需要遵守《网安法》的相关规定。在这方面，《网安法》也留下了一个引子，即规定此类设备和产品的目录将由国家网信部门会同国务院有关部门另行制定。因此，相关企业需密切关注该目录及其他后续措施的出台。

总的来看，《网安法》作为我国网络安全领域的第一部专门大法，其对于维护我国网络安全及规范相关市场主体行为的重要意义不言自明。但也正是由于这种初创性，以及网络安全监管的敏感性和复杂性，《网安法》在定纲立范的同时，仍留下了一系列亟待进一步填补的空白，这些空白很可能将在很大程度上决定《网安法》今后的实际执行效果。而对于广大在华运营的企业来说，只要存在着被纳入《网安法》规制范围的可能性，就有必要认真领会《网安法》的各项既有规定，同时密切关注《网安法》实施的后续动态及相关配套措施的出台，以免因不了解或误读相关监管规定而带来合规风险。

（本文发布于2016年11月08日。）

[13] 参见《网安法》第四章第四十至五十条。

[14] 参见《网安法》第七十六条第（五）项。

[15] 主要可参见《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》、《消费者权益保护法(2013修正)》、《电信和互联网用户个人信息保护规定》等。

[16] 参见《网安法》第四十一、四十二条。

[17] 参见《网安法》第三十七条。

[18] 参见《网安法》第三十七条。

[19] 参见《网安法》第二十三条。

《网安法》生效后不得不知的N件大事

时至今日，我国网络安全领域的基本法《中华人民共和国网络安全法》（“**《网安法》**”）生效已两个多月。在短短的两个多月来，《网安法》在立法层面全面铺开，从“个人信息保护”、“个人信息和重要数据出境安全评估”、“关键信息基础设施（CII）保护”等多个方面预备出台配套法规。从执法层面，监管部门也坚决推动《网安法》的落实，各地都开展了专项执法活动。与此同时，网络运营者之间关于个人信息归属、数据权利人等问题的矛盾也浮出水面，社会各界都聚焦未来《网安法》配套法规和执法活动的动向。

因此，下文将简要梳理和分享《网安法》生效以后“个人信息保护”“CII”与“网络运行安全”领域发生的若干重点事件，供大家参考。

一、个人信息保护

（一）执法

1. 监管部门出手数据乱象，15家大数据公司被查

据媒体报道，2017年5月底至6月初期间，监管部门对市场中非法交易数据等乱象出手，正式开始清理行动，15家大数据公司被列入调查名单，其中几家估值超几十亿。据财新记者报道，“公安部公共信息网络安全监察局正在制定专项治理方案，已将调查名单扩大到30多家，业内知名的大数据公司悉数在此次调查范围之内，不乏已在排队申请IPO计划的公司。”[1]

短评：大数据行业的监管出击可视为《网安法》实施的“预热行动”，并很有可能演变为对大数据行业的全面治理。8月7日出版的《财新周刊》封面报道推出上中下三篇谈大数据产业的灰色一面，强调整肃大数据产业链。随着大数据行业的发展，执法机关将进一步重视大数据企业在数据（尤其是个人信息）收集、使用方面的合法合规问题，如何尽快构建企业内部网络安全和数据合规制度将是企业亟需重视的工作。

2. 四部门联合调查隐私政策，个人信息保护从源头抓起

2017年7月27日，中央网信办、工信部、公安部、国家标准委等四部门联合开展隐私条款专项工作，首批评审的十款网络产品和服务包括微信、新浪微博、京东商城、高德地图、百度地图、航旅纵横、携程网等。[2]

此前，若干组织就曾联合针对1000家网络平台的隐私政策进行调研，发现互联网企业对此的重视程度并不高。在参与测评的1000家网站与APP中，没有一个能够达到隐私政策透明度“高”的标准，超过半数的互联网企业隐私政策透明度为“低”。[3]而此次四部门隐私政策联合评审的重点内容包括明确告知收集的个人信息以及收集方式；明确告知使用个人信息的规则，例如形成用户画像及画像的目的，是否用于推送商业广告等；明确告知用户访问、删除、更正其个人信息的权利、实现方式、限制条件等。

短评：隐私政策作为收集用户个人信息的第一道“闸门”，将是个人信息保护工作的第一步。企业隐私政策的制定和修改首先应该重视国家标准的重要性，同时结合产业的特殊性，做到个人信息保护和商业性的平衡。

---

[1] 张宇哲，吴雨俭，彭骏骏：《整肃数据产业链》，《财新周刊》2017年第31期，2017年08月07日。

[2] 参见《中央网信办等四部门联合开展隐私条款专项工作》，载http://www.cac.gov.cn/2017-08/02/c_1121421829.htm，2017年8月2日。

[3] 参见余瀛波：《千家网络平台测评用户隐私政策透明度 157家得零分》，载http://news.xinhuanet.com/legal/2017-06/01/c_1121067078.htm，2017年6月1日。

3. 打击侵犯公民个人信息犯罪专项行动，严查数据链条

公安部最近披露消息：自今年3月公安部部署开展打击整治黑客攻击破坏和网络侵犯公民个人信息犯罪专项行动以来，截至目前，全国共侦破侵犯公民个人信息案件和黑客攻击破坏案件1800余起，抓获犯罪嫌疑人4800余名，查获各类公民个人信息500多亿条。[4]

以合肥市为例，2017年以来，合肥市公安局组织开展打击整治黑客攻击破坏和网络侵犯公民个人信息犯罪专项行动，共破获黑客攻击破坏类案件5起、网络侵犯公民个人信息犯罪案件53起，抓获犯罪嫌疑人77名，查获公民个人信息数据3亿余条。[5]

警方负责人介绍，“大规模个人信息泄露的源头主要有两个，一个是黑客攻击，另一个是掌握大量个人信息的相关企业、单位、平台的‘内鬼’”。在专项行动中，合肥警方网安、刑侦等多个警种联动，以“追源头、摧平台、断链条”为目标，对网络交易平台、论坛、网站等进行全面排查，梳理了一批非法获取、贩卖、使用公民个人信息的线索，尤其是加大对金融、电信、网络服务提供商等单位内部故意泄露公民个人信息的“内鬼”，以及通过黑客入侵手段获取公民个人信息犯罪行为的查处力度。

短评：除了《网安法》中对个人信息保护规定的责任和义务，《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》（“两高司法解释”），对《刑法修正案（九）》第253条作出解释，明晰了侵犯公民个人信息行为的定罪量刑标准，是目前公民个人信息保护执法的重点依据。由于两高司法解释不仅明确了犯罪行为责任主体，将公司、公司高管及直接业务负责人等都纳入到责任主体范围内，同时也大幅降低了入罪标准，企业亟需制定规范的合规制度以避免可能的刑事责任风险。

（二）立法

除了执法力度的不断加强，《网安法》的出台也加快了相关配套法律规范、国家标准的制定与颁布，为细化个人信息保护方面的实践提供了根据。

1.《个人信息安全规范（报批稿）》成隐私政策文本修改依据

2017年8月1日，高德地图上线新版本App，新版本在用户使用前出现了弹窗服务协议和隐私政策文本，对个人信息收集及使用的范围、限制等进行重点提示。

据报道称，隐私政策文本系根据国家标准《个人信息安全规范（报批稿）》附录修改而成。事实上，早在2016年，《个人信息安全规范》标准制定项目已经在全国信息安全标准化技术委员会立项，并被列为当年的重点标准项目。参加该标准制定工作的包括中国信息安全研究院、中国电子技术标准化研究院、公安部第一研究所、腾讯、阿里巴巴等多家企事业单位。近日高德地图依据《个人信息安全规范（报批稿）》附录修改隐私政策文本的消息如果确认无误，则意味着《个人信息安全规范》的出台近在眼前。

短评：由于网络安全及大数据技术发展迅速，《网安法》以及配套的相关法律法规对于网络安全及个人信息保护仅仅能从宏观层面做原则性规定。根据《网安法》及其配套法律法规制定的国家标准，则内容更为具体，修订周期更短，能够与时俱进，为企业的合规制度提供更具操作性的指引。高德按照相关的国家标准对隐私政策文本进行修订，反映出国家标准在网络安全与个人信息保护领域发挥的积极指导作用。

2. 用户个人信息保护纳入标准制定规划

2017年8月初，工信部印发《移动互联网综合标准化体系建设指南》（“《指南》”）。[6]《指南》提出，到2020年，初步建立起基础标准较为完善、主要产品和服务标准基本覆盖、安全标准有效保障、符合我国移动互联网产业发展需要的标准体系。其中，用户个人信息保护被纳入移动安全标准制定规划之中。

据工信部的信息称，相关标准的内容主要涉及“用户个人信息保护的定义、范畴、分类和分级方式以及针对个人信息管理业务平台和终端的标准”，规范包括用户账号、用户授权以及用户资源方面的数据管理方法、管理架构以及管理范围。目前已形成包括移动用户个人信息管理业务系统技术要求和测试方法、移动用户个人信息管理业务终端技术要求和测试方法、个人信息共享导则等标准，日后还需针对应用商店、终端、应用软件以及用户数据保护等方面进一步制定个人信息保护标准。

短评：移动互联网已经成为目前信息产业中发展最快、竞争最激烈、创新最活跃的领域之一。移动互联网的便捷性和与用户的紧密联系，使得移动互联网企业能广泛地接触到大量的用户数据。用户数据在大数据时代是企业发展最新的驱动力，已经成为企业的竞争资源。如何在充分挖掘数据价值的同时，做好个人信息保护，防止个人信息泄露及滥用将是移动互联网甚至整个互联网行业需要关注的问题。可以预见，如何以国家或行业标准更好地指导企业的个人信息保护实践，也将是主管与监管部门日后工作的关键环节之一。

---

[4]《公安部：打击整治黑客攻击破坏和网络侵犯公民个人信息犯罪专项行动取得阶段性战果》，载http://www.gov.cn/xinwen/2017-07/18/content_5211559.htm，2017年7月18日。

[5] http://hf.ahga.gov.cn/xwfb/201706/23152231zuet.html

[6] 参见《工业和信息化部办公厅关于印发<移动互联网综合标准化体系建设指南>的通知》，载http://www.miit.gov.cn/n1146295/n1146592/n3917132/n4061630/c5757129/content.html，2017年8月7日。

（三）争议

1. 顺风与菜鸟：谁动了谁的用户数据

《网安法》生效当天下午，菜鸟网络即发布《关于顺丰暂停物流数据接口的声明》称，顺丰主动关闭了丰巢自提柜和淘宝平台物流数据信息回传；四个小时后，顺丰回应称是菜鸟单方面切断信息接口。在国家邮政局的及时协调下，各方本着顾全大局、维护市场秩序和消费者合法权益的原则，已达成共识并同意从6月3日午间起，全面恢复业务合作和数据传输。

2. 华为与微信：谁能对手机上的用户信息主张权利

近日，华为与微信在用户数据问题上的争议引发了广泛关注。用户数据的权利归属、应用软件与硬件设备对数据权利主张的边界划分等问题，将会是未来商务实践和司法实践的焦点。

3. 微博与今日头条：如何合法地抓取信息

关于信息抓取和授权的争议也发生在微博与今日头条之间。近日，微博称今日头条在微博毫不知情且未授权的情况下，直接从微博抓取包括自媒体账号内容在内的行为涉嫌侵权，微博将就此进行维权。今日头条方面则声称，其抓取的信息已经获得用户的事先知情同意，用户在是否授权问题上有充分的自主权，因而发布在微博平台上的信息其版权仍然属于用户本人，由用户自主决定是否授权，不涉及微博的知情和授权问题。

短评：在新浪/脉脉案件中，法院已经指出“用户数据已经成为企业愈发重要的经营资源”，可以预见的是未来对作为“经营资源”的用户数据的争夺将日益激烈，其引发的争议也将骤增。无论是顺丰与菜鸟之间的矛盾，华为与微信的纠纷，还是微博与今日头条的争议，在智能设备与物联网日益发达的时代，企业在业务中都会接触到、使用到用户数据。从产品和服务提供商的角度出发，如何尽可能地保护好用户的数据，是网络安全时代无法回避的话题。但同时，针对用户数据权利的问题，虽然我国关于互联网用户数据保护在宏观层面已有立法，但是具体场景下的个人是否完全具有相关信息的所有权，哪些企业能对合法收集的个人信息主张权利等问题，仍有待执法或司法实践进一步明确。

二、CII

（一）立法

1.《关键信息基础设施保护条例（征求意见稿）》揭开CII保护立法进程新篇章

2017年7月11日，国家互联网信息办公室公布了备受瞩目的《关键信息基础设施安全保护条例（征求意见稿）》（“《保护条例（征求意见稿）》”）。[7]CII安全保护制度作为《网安法》建立的若干信息网络安全制度中的核心和重中之重，早在2013年国家信息网络立法规划中就被认定为整个信息网络立法的最基础层。《保护条例（征求意见稿）》对CII范围、运营者安全保护义务、产品和服务安全、监测预警、应急处置和检测评估等一系列事项进行了详细的规定，构建了CII安全保护制度的具体框架。其制度框架要求发挥CII运营者的主观能动性，调动多方资源共享合作，体现了国家将CII筑成“金城汤池”，捍卫网络空间主权的决心。

短评：《保护条例（征求意见稿）》的颁布，也意味着我国CII保护立法工作进一步推进，对CII运营者的日常运营与管理有着重要的指导意义。因此，CII运营者应当尽快开始梳理其内部网络安全制度和体系，比照相关规定项下的义务进行内部调整和校准。

2.《关键信息基础设施识别指南》近在咫尺

根据《保护条例（征求意见稿）》第19条规定，国家网信部门将会同国务院电信主管部门、公安部门等部门制定《关键信息基础设施识别指南》（“《识别指南》”）；国家行业主管或监管部门按照《识别指南》，组织识别本行业、本领域的关键信息基础设施，并按程序报送识别结果。未来相关部门会发布《识别指南》和经识别的各行业CII具体清单，解决目前《网安法》实施过程中所面临的CII范围的不确定性。

短评：《识别指南》的出台将有助于进一步提升CII的准确性，按照行业、领域组织识别CII的方法反映了CII的识别标准是基于行业、领域特点的综合评估， 也反映了识别方法的科学性和合理性。在《识别指南》正式出台之前，企业也可按照自己所处的行业领域、运营方式等进行初步评估，为日后的合规工作做好充足的准备。

（二）执法

1. CII名单初步确定，诸多国企在列

据PaRR报道，目前国内已有400-500家企业被列入CII名单之中，其中大部分为国有企业。消息称，被列入CII名单的企业已被告知此事，而未接获通知的企业暂时将不会被界定为CII运营者。然而，该名单可能会不定期更新，并随着确认工作继续推进，适时发布公告。

根据《网安法》相关规定，国家互联网信息办公室将每年统筹协调有关部门对CII运营者开展全国性检测；2017年的检测工作现已启动，预计将于中共第十九次全国代表大会召开前加速。

[7] 参见《国家互联网信息办公室关于<关键信息基础设施安全保护条例（征求意见稿）>公开征求意见的通知》，载http://www.cac.gov.cn/2017-07/11/c_1121294220.htm，2017年7月11日。

短评：CII安全保护制度的建设与实践将是我国网络安全体系的核心之一。自身网络设施是否构成CII、CII如何具体履行相关网络安全保护义务等也成为了目前企业最为关注的问题。随着《保护条例（征求意见稿）》的颁布与《识别指南》制定工作的推动，CII的范围将日渐明晰，企业应当积极反馈相关部门关于CII的问询，关注相关部门的公告与动态，积极做好应对准备。

三、网络运行安全

1. 重庆市网安第一案

2017年8月初，重庆市公安局网安总队成功查处重庆首例违反《网安法》的行政案件。[8]重庆公安网安总队在日常检查中发现，某重庆当地网络运营商自今年6月《网安法》正式实施以来，在提供互联网服务时存在未依法留存用户登录相关网络日志的违法行为，根据相关规定给予该公司警告处罚，并责令限期整改。

2. 四川省网安第一案

根据四川在线消息，因未落实网络安全等级保护制度，近日宜宾市翠屏区教师培训与教育研究中心被四川省公安厅处一万元罚款，法人代表唐某某被处五千元罚款。这是今年6月1日《网安法》实施以来，四川省公安机关依法处置的第一起违反《网安法》的行政案件。

此外，四川全省公安网安部门表示，下一步，全省将依据《网安法》，进一步加大网络安全监管和执法力度，继续深入开展2017年全省公安机关网络安全执法检查，对未落实网络安全等级保护制度、网络实名认证、侵害公民个人信息等违法行为严格依法查处，切实维护网络信息安全

短评：重庆市和四川省的网络安全第一案都和网络安全运行安全相关。网络日志留存是公安机关依法追查网络违法犯罪的重要基础和保证，能够准确、及时查询到不法分子的互联网日志，可为下一步循线追踪，查获不法分子打下坚实基础。如负责该案执法的重庆公安网安总队也表示，遵守“日志留存”的相关规定，对网站运营者本身也有着极其重要的安全防护作用，不仅能够留存历史数据，更为未来可能发生的安全威胁消除了隐患。

而网络安全等级保护制度是我国现行的网络安全领域重要制度。公安部和标准化主管部门已经制定了信息系统的安全保护等级。《网安法》总结实践经验，对其主要内容做出了规定，进一步加强网络安全等级保护制度的落实。

3. Boss直聘案

东北大学毕业生李文星通过BOSS直聘求职，继而深陷传销组织致死一案暴露了BOSS直聘的重大漏洞后，相关监管部门已经积极介入。北京网信办、天津网信办就BOSS直聘发布违法违规信息、用户管理出现重大疏漏等问题联合约谈BOSS直聘，并责令网站立即整改。[9]

北京网信办相关发言人表示，BOSS直聘在为用户提供信息发布服务过程中，违规为未提供真实身份信息的用户提供了信息发布服务；未采取有效措施对用户发布传输的信息进行严格管理，导致违法违规信息扩散。2017年8月10日，BOSS直聘也发出了官方道歉信，表示自李文星事件发生以来公司采取的三项紧急措施，包括“100%审核认证”、“组建求职安全中心”、“建立平台提醒机制”等。

4. 腾讯微信、新浪微博、百度贴吧网站被立案调查

据国家网信办官网通报，2017年8月13日，国家网信办指导北京市、广东省网信办分别对腾讯微信、新浪微博、百度贴吧立案，并依法展开调查。通报指出，根据网民举报，经北京市、广东省网信办初查，三家网站的微信、微博、贴吧平台分别存在有用户传播暴力恐怖、虚假谣言、淫秽色情等危害国家安全、公共安全、社会秩序的信息。三家网站平台涉嫌违反《网安法》等法律法规，对其平台用户发布的法律法规禁止发布的信息未尽到管理义务。[10]

短评：在信息产业时代，通过发挥网络连通性的影响力，网络平台已经成为了真正的信息高速通道。然而，网络平台的这种特性却也有可能成为垃圾信息和违法信息传播的工具。无论是Boss直聘案还是针对腾讯微信、新浪微博与百度贴吧的调查，可以看出，随着《网安法》的施行及网络运行安全监管工作的深入推进，如何更好规范网络信息平台运营制度和监管责任将是网络运营者，尤其是网络平台合规工作的重点。就目前的执法动态来看，用户协议的免责条款并不能作为网络平台完全免责的抗辩理由，网络平台应当转变身份与观念，由一个网络信息的参与者转变为网络信息的基层管理者，完善平台的事前提示、事后监管以及信息审核等机制，担当平台信息的准入与影响的责任，主动承担网络运营者的安全义务。

（本文发布于2017年08月15日。）

[8] http://www.cqga.gov.cn/jfzx/53137.htm

[9] http://society.people.com.cn/n1/2017/0810/c1008-29460958.html

[10]《腾讯微信、新浪微博、百度贴吧涉嫌违反<网络安全法>被立案调查》，载http://www.cac.gov.cn/2017-08/11/c_1121467425.htm，2017年8月11日。

Petya来袭，网络安全事件应急预案正当其时

一、网络安全事件频发

近期，网络勒索病毒在全球网络空间肆虐，所造成的数据泄露及网络瘫痪对网络运营者造成了严重的经济后果，也对全球网络空间安全带来了极大的挑战。5月爆发的WannaCry勒索病毒袭击了英国、乌克兰等150多个国家，中国国内也有用户受到影响。[1]WannaCry的冲击还未远去，一种被认为是Petya病毒变种的新勒索病毒又开始在全球肆虐，英国、乌克兰、俄罗斯、丹麦等地都已经爆发这种新病毒。[2]

依据最新《诺顿网络安全调查报告》，在新兴市场中，中国是遭受网络犯罪攻击最严重的一个国家。早在2014年，大约2.4亿的中国消费者成为网络犯罪的受害者，经济损失高达7000亿元人民币。[3]在网络攻击和犯罪日益猖獗的情势下，中央网络安全和信息化领导小组办公室（“**中央网信办**”）于2017年1月10日发布了《国家网络安全事件应急预案》（“**《预案》**”）的通知，并在2017年6月27日正式对外公布。中央网信办在各省、自治区、直辖市建立健全国家网络安全事件应急工作机制，显示了中央应对网络攻击、维护信息安全和网络主权的决心。对于企业而言，除了解中央网信办从国家层面的应急措施以外，还应该严格遵守《中华人民共和国网络安全法》（“**《网安法》**”）中对于网络安全的各项要求，从事前、事中、和事后多个角度建立规范制度和自身的应急预案，以应对可能的网络安全事件。

本文将对《预案》的内容进行简要梳理，同时总结企业在预防和应对网络安全事件方面的基本法律义务，并根据经验提示企业应对突发安全事件执行的关键步骤。

二、《预案》介绍

框架	具体内容
网络安全事件的范围	网络安全事件包括有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他事件等。
网络安全事件的等级	依据重要网络和信息系统遭受损失的程度、及对国家安全和社会稳定的威胁程度，网络安全事件可以分为四级：特别重大网络安全事件、重大网络安全事件、较大网络安全事件、一般网络安全事件。
组织机构和职责	• 领导机构：中央网络安全和信息化领导小组 • 办事机构：国家网络安全应急办公室（“应急办”）（设在中央网信办） • 各部门、各省市职责：中央和国家机关各部门、各省（区、市）网信部门具体负责本部门、本行业或本省市的网络和信息系统网络安全事件的预防、监测、报告和应急处置工作。
监测与预警	各省（区、市）网信部门结合本地区实际，统筹组织开展对本地区网络和信息系统的安全监测工作，包括预警监测、预警研判和发布、预警响应、预警解除。

[1] 新浪科技，勒索病毒全球爆发：病毒武器源自美国，发布于2017年5月14日，http://tech.sina.com.cn/i/2017-05-14/doc-ifyfekhi7587061.shtml?cre=zlpc&mod=f&loc=3&r=9&doct=0&rfunc=100。

[2] 新浪科技，Petya勒索病毒攻击源自乌克兰金融科技网站，潜伏5天后集中爆发，发布于2017年6月28日，http://tech.sina.com.cn/roll/2017-06-28/doc-ifyhmtrw4313782.shtml?source=cj&dv=2。

[3] 网易新闻，网络犯罪让中国消费者在2014年损失7000亿元，发布于2015年12月1日，http://news.163.com/15/1201/10/B9OBIPOR00014AED.html。

框架	具体内容
应急处置	网络安全事件发生后，事发单位应立即启动应急预案，实施处置并及时报送信息。各有关地区、部门立即组织先期处置，控制事态，消除隐患，同时组织研判，注意保存证据，做好信息通报工作。对于初判为特别重大、重大网络安全事件的，立即报告应急办。
调查与评估	网络安全事件的调查处理和总结评估工作原则上在应急响应结束后30天内完成。
预防工作	各地区、各部门按职责加强日常预防工作、定期预案演练、开展网络安全基本知识和技能的宣传活动、加强领导干部和有关人员的培训以及加强重要互动期间的预防措施。
保障措施	各地区、各部门应充分利用各种传播媒介及其他有效的宣传形式，加强突发网络安全事件预防和处置的有关法律、法规和政策的宣传，开展网络安全基本知识和技能的宣传活动。

三、网络运营者应对网络安全事件的义务

总体来说，网络运营者对网络安全事件的法律义务可以分为日常的预防工作、事件发生时的应急措施以及事件发生后的总结工作。

（一）日常预防工作

《网安法》和《预案》都对网络运营者网络安全事件的日常预防工作进行了规定，具体包括：

1. 网络安全等级保护

网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。具体包括：

- 确定网络安全负责人，落实网络安全保护责任；
- 采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；
- 采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志；
- 采取数据分类、重要数据备份和加密等措施。[4]

2. 网络产品、服务应当符合国家标准

网络产品、服务应当符合相关国家标准的强制性要求。对于关系国家安全的网络和信息系统采购的重要网络产品和服务，应当依据《网络产品和服务安全审查办法(试行)》的要求经过网络安全审查。[5]

3. 持续的安全维护

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。[6]

4. 网络安全事件应急预案

网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险。[7]应急预案可能包含主要负责人、数据泄露通知机制、补救措施、内部责任划分等内容。

5. 及时补救和报告义务

网络运营者在发现其提供的网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。另外，在可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。[8]

6. 关键信息基础设施运营者定期进行风险评估检测

除此以外，关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。[9]

（二）安全事件发生时的应急机制

在发生危害网络安全的事件时包括发生个人信息泄露、毁

[4]《网安法》第二十一条。

[5]《网安法》第二十二条。

[6]《网安法》第二十二条。

[7]《网安法》第二十五条。

[8]《网安法》第二十二条、第四十一条。

[9]《网安法》第三十八条。

损、丢失的情况时，网络运营者需立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。[10]

依照《预案》的规定，安全事件发生时，网络运营者需及时报告当地网信部门，以及时启动相关部门的应急处置工作。此外，对计算机信息系统中发生的案件，有关使用单位应当在24小时内向当地县级以上人民政府公安机关报告。[11]

相应的，《预案》中也指出，应急办负责网络安全应急跨部门、跨地区协调工作和指挥部的事务性工作，组织指导国家网络安全应急技术支撑队伍做好应急处置的技术支撑工作。

（三）安全事件发生后的总结和合规梳理

由于《预案》规定了网信部门对于安全事件的总结评估机制，企业可能需要与行政部门保持良好沟通以便其完成调查报告包括总结安全事件的起因、性质、影响等，并提出改进措施。此外，我们也建议企业在突发事件后，全方面地梳理内部网络安全制度和规范，做到防患于未然。

发生网络安全事件时企业应如何应对?

总体建议：

- 对任何网络安全事件予以充分重视，不要因为初始判断认为事件影响并非特别严重而草率处理，以防在完全评估其影响后措手不及；
- 在事件发生后立即采取措施控制事态，并评估任何进一步入侵或泄露的可能性；
- 根据事件的具体情形，快速开展网络安全事件影响和严重等级的初步评估、通知相关政府机关或受影响的数据主体、采取措施预防任何进一步的入侵或泄露；
- 积极配合主管机关对事件的调查，在将事件的细节对外公布之前先行咨询主管部门的意见；
- 注意保存能确定事件起因和性质以及应采取的补救措施的证据；
- 确保对事件相关情况进行适当、充分记录，尤其是为控制并降低事件危害所采取的补救措施。

应对网络安全突发事件初期关键步骤：

第一步：采取紧急措施控制事态发展，初步评估事件影响

- 采取控制措施
- 开展初始评估
- 确定通知对象

第二步：评估事件造成的风险，确定应立即采取的措施

- 确定遭到泄露的数据类型
- 确定数据泄露的具体情形
- 确立数据泄露的原因和范围
- 评估泄露事件对数据主体造成的风险

第三步：履行网络安全突发事件通知义务

- 确定通知程序
- 确定通知应包含的具体内容

当前，木马僵尸网络、钓鱼网站等非传统网络安全威胁有增无减，分布式拒绝服务（DDOS攻击）、高级持续威胁（APT攻击）等新型网络攻击愈演愈烈，导致网络安全威胁层出不穷，网络基础设施隐患重重，企业的信息系统安全时刻处在层层危机之中，企业在保护网络安全和用户数据安全方面面临严峻的挑战。

为确保企业的网络安全，同样也是为了降低企业在网络安全事件中的合规风险。我们建议：

- 企业在日常运营中增强网络系统软硬件安全，建立完整的网络安全事件应急预案和相应机制，加强内部员工网络安全知识和技能培训；
- 在发生网络安全突发事件时，应果断采取措施，寻求专业意见，按照相关法律法规履行相关义务，积极配合主管部门的调查，尽最大努力降低风险和损害、减轻企业可能面临的法律责任；
- 在网络安全突发事件结束之后，企业应积极修补系统漏洞，从技术和制度层面增强网络系统安全性，对内部安全事件响应机制进行必要改进和完善，确保相关安全体系和标准符合国家相关法律法规的要求，预防再次发生网络安全事件和数据泄露。

网络安全往往涉及突发事件，如果企业遇到紧急情况，我们设有紧急救助服务机制，将在第一时间帮助企业渡过难关。

（本文发布于2017年06月30日。）

[10]《网安法》第二十五条。

[11]《计算机信息系统安全保护条例》第十四条。

《网络安全法》及其部分配套规定今起实施

2016年11月7日，全国人大常委会审议通过了《中华人民共和国网络安全法》（“**《网安法》**”），该法将于2017年6月1日，也即今日正式实施。为了配合《网安法》的实施，国家互联网信息办公室（以下简称“**网信办**”）在《网安法》出台后陆续发布了一系列配套规定，并将与《网安法》同日实施。除此之外，网信办网络安全协调局负责人还透露，《网安法》实行之日起一年内将有更多的配套规定出台，包括但不限于关键信息基础设施保护办法、个人信息和重要数据出境安全评估办法等。[1]

作为我国网络安全领域的基础性法律，《网安法》的正式施行对于维护我国网络安全及规范相关市场主体行为具有重大意义。本文根据我们前期跟踪发布的法律法规解读，对今日实施的《网安法》和配套规定，及其个人信息保护相关的司法解释进行梳理，并列举未来一年内可能发布的更多相关规定和技术标准，为企业进行网络安全及数据合规提供参考。

一、《网安法》以及配套规定

总体而言，《网安法》一共有七章七十九条，分别从网络安全支持与促进、网络运行安全、网络信息安全、监测预警与应急处置、法律责任五个方面对网络运营者应对网络安全挑战进行了框架性的规定。

回顾《网安法》的立法过程，历时近一年半、在三易其稿后终获全国人大常委会通过。在整个制订过程中，《网安法》因其对我国网络安全领域的全面规制和重大影响而广受社会各界、特别是经营互联网相关业务的企业的高度关注。对于此类企业、特别是在华外资企业而言，需特别注意的《网安法》要点包括：

第一，就适用范围而言，《网安法》的适用对象并无内外商之别，只要是在我国境内通过网络提供服务，不论是内资还是外资企业，都同等受制于《网安法》的各项规定和要求。

[1]《网络安全法》施行前夕，国家网信办网络安全协调局负责人答记者问，http://news.163.com/17/0531/13/CLP45MPI000187VI.html。

第二，就网络运行安全而言，我国法律首次提出“网络安全等级保护制度”这一概念。但《网安法》并未进一步阐明该制度的内涵，也没有说明该制度将如何实施以及“网络安全等级”具体又将如何划分和确定。

第三，《网安法》首次提出“关键信息基础设施”的概念，其受关注的原因主要有三：一是按照其目前的定义表述，其潜在的覆盖范围十分广泛，可能影响数量众多的企业；二是其为相关运营者设置了更高的、负担更重的网络安全保护义务；三是对关键信息基础设施传输个人信息和业务数据至境外的独特限制。

第四，在“网络运行安全”之外，《网安法》的另一侧重点在于保护“网络信息安全”，特别是网络运营者收集和使用的“个人信息”的安全。在这方面，《网安法》进行了诸多首创新的规定，一是首次在法律层面确立了一般意义上“个人信息”的概念；二是首次成体系地在法律层面确定了个人信息保护的基本规则；三是首次明确了禁止向他人提供个人信息的例外情形；四是在法律层面规定特定个人信息的本地化存储要求，以维护国家信息安全；五次首次在法律层面明确了违反个人信息保护规则的行政责任。

第五，同样出于保障网络安全的考虑，《网安法》对于“网络关键设备和网络安全专用产品”的相关经营者也设定了专门要求。因此，一家企业即使不属于网络运营者，只要其从事“销售”或“提供”此类设备和产品的业务，同样需要遵守《网安法》的相关规定。

基于以上《网安法》的总体框架，网信办还发布了以下将于今日（2017年6月1日）生效实施的规定。

（一）《网络产品和服务安全审查办法（试行）》(以下简称“《审查办法》”)

2017年5月2日，网信办发布了《网络产品和服务安全审查办法（试行）》（“**《审查办法》**”），并将于2017年6月1日起正式实施。尽管《审查办法》仅有十六条规定，但其构建了网络产品和服务安全审查的基本制度框架。相比于网信办于2017年2月4日发布的《网络产品和服务安全审查办法（征求意见稿）》（以下简称“**《征求意见稿》**”），试行的《审查办法》在多个方面做出了改进。

具体而言：第一，《审查办法》删除了《征求意见稿》第一条、第二条、第四条第（5）项中的“公共利益”，避免对安全审查的产品和服务的范围以及审查过程中的判断标准进行任意扩大化解释；第二，综合考虑现实商业实践后，《审查办法》将审查起始点从“研发环节”延后至“生产、测试环节”；第三，明确了党政部门或重点行业只要采购的产品和服务属于“关系国家安全的网络和信息系统的重要网络产品和服务”，均应经过网络安全审查，即将“未进行审查”（灰名单）和“未通过审查”（黑名单）的产品和服务完全排除在允许采购的范围之外；第四，一定程度上厘清了，评估报告是针对“网络产品和服务”，而不是对“提供者”安全性和可信性的定性结果；第五，新增的救济途径和罚则条款弥补了《征求意见稿》中的缺失。

（二）《互联网新闻信息服务管理规定》（以下简称“《管理规定》”）和《互联网新闻信息服务许可管理实施细则》（以下简称“《实施细则》”）

网信办分别于2017年5月2日和5月22日发布了《管理规定》和《实施细则》，二者都自2017年6月1日起施行。

网信办在《管理规定》中不仅将《网安法》明确列为立法依据之一，而且将《网安法》下的信息安全保护、用户实名制等要求有机融入《管理规定》对互联网新闻信息服务的监管，凸显了在全新的自媒体态势下，对于互联网新闻除业务监管和舆论监管以外的第三重重要监管维度即“网络安全监管”，从而使《规定》直接成为《网安法》的重要配套措施之一。

另外值得注意的是，《管理规定》不再采用“新闻单位”和“非新闻单位”之分，对提供互联网新闻信息服务的“单位”的“设立”进行分类审批或备案制监管的思路；而是改之以对“互联网新闻信息采编发布服务、转载服务、传播平台服务”这三大服务类型进行许可式监管，发以《互联网新闻信息服务许可证》，并通过设定《互联网新闻信息服务许可证》有效期和申请续办的程序加强持续监管。

《实施细则》规定，获准提供互联网新闻信息采编发布服务的，可以同时提供互联网新闻信息转载服务；获准提供互联网新闻信息传播平台服务，拟同时提供采编发布服务、转载服务的，应当依法取得互联网新闻信息采编发布、转载服务许可。此外，还对许可变更、续办、注销等环节的条件、材料、程序等提出明确要求，进一步完善许可退出机制。

（三）《互联网信息内容管理行政执法程序规定》（以下简称“《程序规定》”）

2017年5月2日，网信办发布了《程序规定》，并将于2017年6月1日起正式实施。《程序规定》在《行政处罚法》的基本原则下做到“统一协调、面面俱到、内外兼修、与时俱进”，为此后监管执法工作提供了重要的法律依据，可谓是互联网信息内容管理行政执法所仰仗的“利器”。

具体而言，《程序规定》要求各管理部门应当建立行政执法督查制度，由上级部门对下级部门的执法行为进行督查。此外，《程序规定》还要求执法人员应当参加相关培训，经考试或考核后持证上岗，务求在执法队伍建设层面提升执法的规范性。而就具体的执法程序要求而言，《审查办法》从管辖、立案、调查取证、听证与约谈、处罚决定与送达、执行与结案等六大板块，较

为全面地规范了国家与地方网信部门的执法行为，为在《网安法》的指导下有效推进互联网信息内容的管理奠定了坚实的程序基础 。

二、个人信息保护的相关司法解释

如上所述，《网安法》除了对维护网络安全、关键信息基础设施保护等层面做出了明确规定之外，还从个人信息定义、个人信息收集、存储、传输、使用等流转环节的限制以及个人信息泄露的行政责任等方面规定了个人信息保护的基本原则。

在《网安法》出台之前，由于我国没有统一制定的个人信息保护法，个人信息保护的主要依据是2012年全国人大常委会颁布的《关于加强网络信息保护的决定》和2013年全国人大常委会出台的《关于修改<中华人民共和国消费者权益保护法>的规定》，以及2009年通过的《刑法修正案（七）》和2015年通过的《刑法修正案（九）》。《刑法修正案》中关于打击侵犯公民个人信息犯罪的条款被普遍认为是个人信息保护的最后底线。

在《网安法》开始实施之际，2017年5月9日最高人民法院、最高人民法院发布的《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》（“**《解释》**”），也将于今日同时正式施行。

《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。第一，相比于《网安法》，《解释》扩大了个人信息的认定范围，将个人信息的定义覆盖到“反映特定自然人活动情况的各种信息”，使得比如行踪轨迹信息等具有某种隐私或私密属性的信息类型也纳入到个人信息的范围中；第二，《解释》明确了“提供”公民个人信息的含义，即“向特定人提供公民个人信息，以及通过信息网络或者其他途径发布公民个人信息的”都属于提供公民个人信息的情形；第三，扩大了非法利用信息网络罪的使用范围，将个人信息交易的网站、微信群、QQ群等形式也明确纳入刑法打击范围；最后，《解释》对于违反信息网络安全管理义务的刑事责任、涉案公民个人信息数量的计算标准予以了澄清。

三、即将发布的相关规定

随着《网安法》的正式实施，相关的配套规定尚待进一步完善，以下是我们对于近期可能发布或生效的配套规定的初步梳理。

序号	即将发布的规定或技术标准	发布时间	《网安法》依据条款
1	个人信息和重要数据出境安全评估办法（征求意见稿）	2017年4月11日	第三十七条
2	信息安全技术 数据出境安全评估指南（草案）征求意见稿	2017年5月27日	第三十七条
3	重要数据识别指南	近期	第三十七条
4	个人信息安全规范	近期	第三十七条
5	网络关键设备和网络安全专用产品目录	近期	第二十三条
6	关键信息基础设施的具体范围和安全保护办法	近期	第三十一条

《网安法》的正式施行标志着我国网络空间领域的发展和现代化治理迈出了坚实的一步。但也由于网络安全监管的敏感性和复杂性，《网安法》在设定总体框架的同时，在实际操作层面仍留下了一系列亟待进一步填补的空白，这些空白很可能将在很大程度上决定《网安法》今后的实际执行效果。对于广大在华运营的企业来说，有必要理解《网安法》及其配套措施的规制范围，持续跟踪既有规定以及执行情况对于企业合规以及商业行为的影响。 我们也将与企业一同密切关注《网安法》执法的发展以及其他配套措施的发布。

（本文发布于2017年06月01日。）

同道而相益，同心而共济
——《网络安全审查办法》的创新与变化

4月27日，国家互联网信息办公室（“**网信办**”）联合12个部门正式发布《网络安全审查办法》（“**《审查办法》**”），该办法将取代此前的《网络产品和服务安全审查办法（试行）》（“**《试行办法》**”），并于2020年6月1日正式实施。《审查办法》从网络安全审查的适用范围、申报流程、评估因素、合规开展（特别是关键信息基础设施运营者（以下简称“**运营者**”）、产品和服务提供者的权益保护）和法律责任等方面做出规定，预示着我国网络安全审查进入新阶段，运营者和相关网络产品和服务供应商应予以高度重视。

“纵观世界，网络安全审查早已是国际潮流和通行做法。”[1]但不同国家在网络安全审查制度构建、审查机构组成、审查流程设计等方面各有不同。本次《审查办法》建立的多部门联席工作机制，有助于打破关键信息基础设施的行业及技术壁垒，达成关键信息基础设施保护的重要共识。为运营者和网络产品和服务提供者设定的不同要求，也帮助不同主体厘清在网络安全审查制度下的责任义务。从监管部门联合到不同市场主体的相互配合，充分体现网络安全，尤其是关键信息基础设施安全防护，需要“同心共济”，团结协作，共同维护安全的网络生态。

本文将回顾我国网络安全审查制度的发展，总结《审查办法》所确定的网络安全审查体系框架、审查制度流程，结合国外网络安全审查制度以及与《审查办法（征求意见稿）》的对比总结重大变化，探讨新的网络安全审查制度对相关市场主体及行业实践的指导意义。

一、网络安全审查制度历史沿革

2016年《网络安全法》（“**《网安法》**”）的颁布以法律法规形式确定了网络产品和服务的安全审查制度（“**网络安全审查**”），但事实上中国的网络安全审查制度更早可以追溯至2013年《建立信息安全审查制度》的两会提案。[2]从2013年至2016年期间，我国先后颁布了多项政策及立法，对网络安全审查制度的建设给予了高度关注。[3]

而在2017年《网安法》正式生效前，国家互联网信息办公室（“**网信办**”）已于当年5月2日发布了《网络产品和服务安全审查办法（试行）》（“**《试行办法》**”），以期实现网络安全审查制度的初步落地。

随着《网安法》的施行、关键信息基础设施（CII）安全问题的显现和网络安全审查制度经验的不断累积，2019年5月，网信办会同国家发展和改革委员会、工业和信息化部、公安部、国家安全部等12个部门联合发布了《网络安全审查办法（征求意见稿）》（“**《审查办法（征求意见稿）》**”），并最终于近日正式发布该《审查办法》（以下请见我国网络安全审查制度相关法律法规和立法政策梳理）。

[1] 各国网络安全审查制度及案例分析[EB/OL]. http://www.cac.gov.cn/2015-04/17/c_1114990146.htm. 发布日期：2015年4月17日，最后访问日期：2020年4月28日.

[2] 《网安法》第三十五条规定，关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

[3] 马宁. 国家网络安全审查的内涵及其制度扩展[J]. 保密科学技术,2017(02):12-16.

法律法规/立法政策	颁布机构	颁布时间
《建立信息安全审查制度》的立法提案	不适用 两会立法提案	2013
《信息化发展规划》	工业和信息化部	2013.10.24
《关于建立网络安全审查制度的公告》	不适用 国家互联网信息办公室通知	2014.05.22
《关于加强党政部门云计算服务网络安全管理的意见》	国家互联网信息办公室	2015.12.30
《中华人民共和国国家安全法》	全国人民代表大会常务委员会	2015.07.01
《国家信息化发展战略纲要》	中共中央办公厅、国务院办公厅	2016.07
《中华人民共和国网络安全法》	全国人民代表大会常务委员会	2016.11.07
《网络产品和服务安全审查办法（试行）》	国家互联网信息办公室	2017.05.02
《关键信息基础设施安全保护条例（征求意见稿）》	国家互联网信息办公室	2017.07.10
《贯彻落实总体国家安全观 健全完善关键信息基础设施安全保护法律体系》	不适用 国家互联网信息办公室通知	2018.04.19
《网络安全审查办法（征求意见稿）》	国家互联网信息办公室等[4]	2019.05.21
《网络安全审查办法》	国家互联网信息办公室等[5]	2020.04.13

二、网络安全审查的制度框架及制度流程

结合《审查办法》及其他相关法律法规、指导性文件，我们总结网络安全审查制度的框架如下：

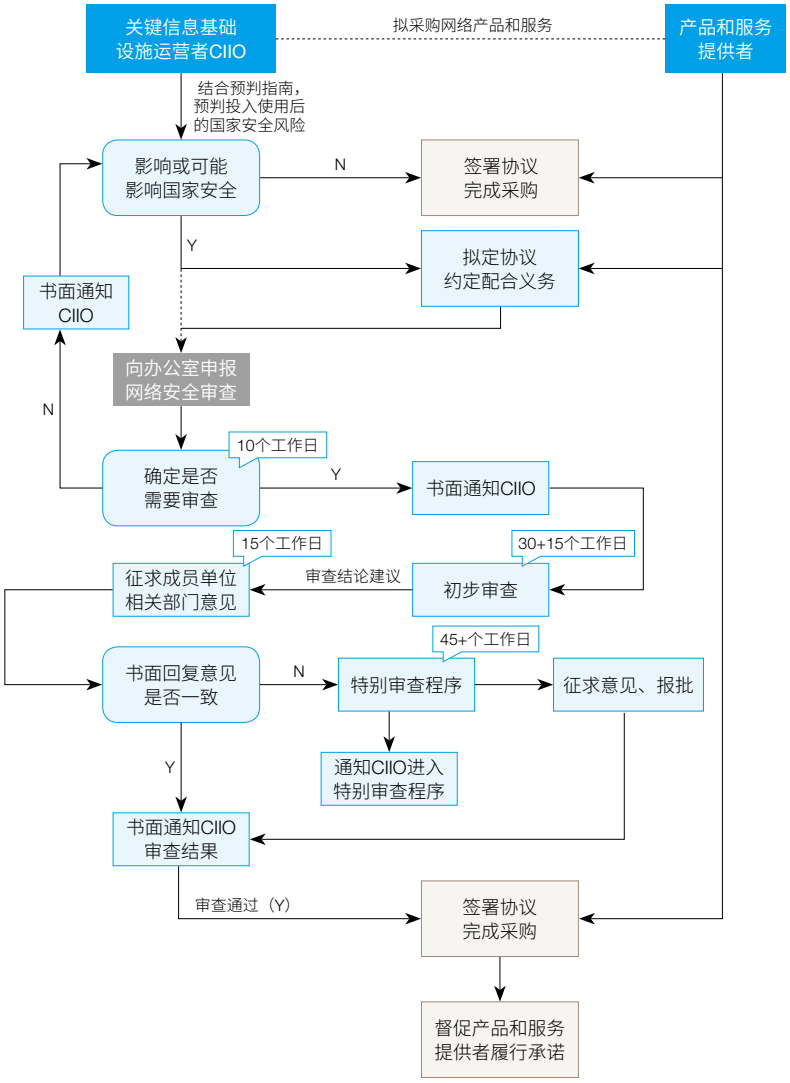
制度框架	
适用范围	- 运营者采购网络产品和服务，影响或可能影响国家安全的（第2条） 电信、广播电视、能源、金融、公路水路运输、铁路、民航、邮政、水利、应急管理、卫生健康、社会保障、国防科技工业等行业领域的重要网络和信息系统运营者在采购网络产品和服务时，应当按照《审查办法》要求考虑申报网络安全审查（《关于关键信息基础设施安全保护工作有关事项的通知》）； - 运营者采购网络产品和服务，经预判该产品和服务投入使用后可能带来国家安全风险、影响或者可能影响国家安全的；或结合本行业、本领域预判指南需要向网络安全审查办公室申报网络安全审查的（第5条）。
审查内容	- 产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏，以及重要数据被窃取、泄露、毁损的风险； - 产品和服务供应中断对关键信息基础设施业务连续性的危害； - 产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险； - 产品和服务提供者遵守中国法律、行政法规、部门规章情况； - 其他可能危害关键信息基础设施安全和国家安全的因素（第9条）。

[4] 国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、国家安全部、商务部、财政部、中国人民银行、国家市场监督管理总局、国家广播电视总局、国家保密局、国家密码管理局。

[5] 同前注。

制度框架	
运营者的权利义务	权利： - 企业商业秘密和知识产权、未公开材料及未公开信息的受保密权（第16条）； - 对未遵守保密义务或有失客观公正的审查活动的举报权（第17条）。 义务： - 通过采购文件、协议等要求产品和服务提供者配合网络安全审查（第6条）； - 督促产品和服务提供者履行网络安全审查中作出的承诺（第18条）。
法律责任	- 运营者违反《审查办法》规定的，由有关部门责令停止使用，处采购金额一倍以上十倍以下罚款； - 直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款（《审查办法》第19条，《网安法》第65条）。

同时，《审查办法》还对2019年《审查办法（征求意见稿）》中所建立的网络安全审查流程进行了优化，我们在此总结新的网络安全审查流程如下：



除了运营者依据上述流程依法申报之外，网络安全审查工作机制成员单位还可以对影响或可能影响国家安全的网络产品和服务发起“主动审查”。[6]

三、《审查办法》重大修改和亮点

相比于19年颁布的《审查办法（征求意见稿）》，此次正式发布版本在运营者的风险预判实践、供应商协议内容合规要求、审查机构和人员保密义务范围等方面均作出了调整，同时在具体审查内容方面，《审查办法》也做了关注要点的方向性调整。

（一）构建多部门联席工作机制，推动安全审查与行业监管衔接

当前，其他国家的安全审查多由通信部门主导工作，但其中，也不乏有多部门联动开展审查的事例，例如，美国国家安全审查由外国投资委员会负责，该委员会由财政部、司法部等九大部门组成，负责组织调查活动。同样的，俄罗斯网络安全审查由工业与贸易部组织，并征询联邦安全局和国家保密委员会的审核评估意见。

[6]《审查办法》第十五条规定，“网络安全审查工作机制成员单位认为影响或可能影响国家安全的网络产品和服务，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照本办法的规定进行审查。”

如上文制度框架所示，《审查办法》确立了以中央网络安全和信息化委员会统一领导，网信办会同公安部、国安部等12个重要国家部委机构组成的国家网络安全审查工作机制：在网络安全审查办公室完成初步审查后，将审查结论建议发送至工作机制各成员单位以及相关关键信息基础设施保护工作部门，在得到相关单位和部门的统一确认意见的前提下形成最终审查结论。由此，在网络安全审查构建多部门联席工作机制的前提下，形成了多部门共同监管运营者的安全审查机制。

对于目前各行业内散见的针对运营者采购网络产品和服务的安全审查要求，以《密码法》为例，运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当通过有关部门组织的国家安全审查。[7]我们理解，其立法逻辑和目的与网络安全审查机制构建的思路基本一致，因而，对于各工作机制成员单位针对其负责行业领域内的运营者的安全评估与网络安全审查存在交叉的情况，多部门联席工作机制将有助于各部门之间就关键信息基础设施保护凝聚共识，同时也能够在一定程度上为运营者的网络安全审查申请及评估提供便捷通道。

（二）运营者可基于行业指南判断是否需启动网络安全审查申报

继承《审查办法（征求意见稿）》中的立法思路，《审查办法》中肯定了网络安全审查申报及审查程序并非无条件地适用于任何运营者的网络产品和服务采购活动。其中第五条规定了运营者在采购网络产品和服务时，应当预判该产品和服务投入使用后可能带来的国家安全风险，在预判结果认为该采购活动会影响或可能影响国家安全时，运营者应当申报网络安全审查。

值得注意的是，第五条第二款中特别指出，关键信息基础设施保护工作部门可以制定本行业、本领域的预判指南。这意味着本行业、本领域的预判指南将对运营者的风险预判具有较强的指引作用，同时特定行业、领域的预判指南的建立也反映出了《审查办法》对行业特殊性与领域特殊性的认可与尊重，该类预判指南将有助于更好地与关键信息基础设施的认定机制相衔接，同时在一定程度上消除此前一度引发的“网络安全审查与行业实践之间存在技术壁垒”，运营者在实践中可能面临两难之境的担忧。

当然，特定行业、领域的预判指南的制定仍然需要时间，在制定后其效力和指引作用以及实践中的效果也有待进一步的观察。

（三）网络安全审查成为采购合同生效的前置条件

此外，《审查办法》中还新增了对于采购合同内容、采购合同签署及履行等的要求。具体而言，《审查办法》及相关问答已经明确指出，网络安全审查的申报应当在运营者与产品和服务提供方签署正式合同前完成；或将网络安全审查通过作为合同生效的条件。此外，运营者在申报网络安全审查的采购合同中，还需要通过采购文件、协议等约定产品和服务提供者配合网络安全审查的义务，[8]网络安全审查申报时需提交采购文件、协议和拟签订的合同。[9]在网络安全审查通过后，运营者还有义务督促产品和服务提供者履行网络安全审查中作出的承诺。[10]

上述规定一方面有助于实质性地发挥网络安全审查在运营者产品和服务采购活动中的安全保障作用，避免因协议约定与网络安全审查之间发生冲突而削弱网络安全审查的实际作用或导致其形同虚设；另一方面，通过对采购合同、协议等文本的审查也有助于运营者与产品和服务提供方之间合理分配网络安全责任与义务，并间接通过合同约束为运营者提供产品和服务的供应方，从各个环节保障关键信息基础设施运营的供应链安全。

（四）审查内容：技术中立，以维护国家安全为核心

各国网络安全审查中一般可能会对技术以外的因素进行考量。比如美国去年发布的《确保信息通信技术与服务供应链安全》的行政令的安全审查对象和重点为“涉及由外国对手拥有、控制或受其管辖或指导的人设计、开发、制造或供应的信息和通信技术或服务”，[11]禁止交易、使用可能对美国国家安全、外交政策和经济构成特殊威胁的外国信息技术和服务，[12]体现了美国政府试图以政治、外交等非技术因素为主要考量基准，对信息通信技术与服务供应链进行安全管控。

《审查办法》在网络安全审查重点评估因素中删除了有关“对国防军工、关键信息基础设施相关技术和产业的影响”、“产品和服务提供者受外国政府资助、控制等情况”[13]等与政治、外交和贸易环境等非技术因素，正如网信办负责人在《审查办法》答记者问中重申我国对外开放的基本国策，[14]修改主要体现了网络安全审查在以维护国家安全为要务的基础上，向实质产品与服务内容等技术因素的偏向转移。

另外，如《审查办法》第九条第（三）项所示，该条列明的

[7]《密码法》第二十七条第二款：关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当按照《中华人民共和国网络安全法》的规定，通过国家网信部门会同国家密码管理部门等有关部门组织的国家安全审查。

[8]《审查办法》第六条。

[9]《审查办法》第七条。

[10]《审查办法》第十八条。

[11]《确保信息通信技术与服务供应链安全》第一条（a）（1）。

[12] 公安三所网络安全法律研究中心. 美国总统行政令《确保信息通信技术与服务供应链安全》全文中文翻译[EB/OL]. https://www.secrss.com/articles/10721. 发布日期：2019年5月16日，最后访问日期：2020年4月28日.

审查因素包括："产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险"。由此可见，供应链安全作为安全审查的重点关注内容，审查拟从产品与服务来源、供应渠道、服务提供方式、服务属性以及其他非技术因素对供应链的影响等方面全方位的进行风险评估与认定。但同时，鉴于审查因素目前均为方向性的要求，缺乏较为明确的细节指引，因此在实践中各审查部门如何平衡各因素在评估过程中的比重以及各因素下的判断标准仍有待观察。

（五）明确审查机构和人员的保密义务的范围

相较19年《审查办法（征求意见稿）》第十五条对参与网络安全审查人员就其于审查工作中获悉的信息承担保密义务，不得用于审查以外的目的的一般性约束，《审查办法》进一步对审查机构和人员的保密义务进行细化与明确，也即，将保密范围限缩至企业商业秘密、知识产权以及审查工作中获悉的运营者、产品和服务提供者提交的非公开资料。[15]同时，在资料公开方面，除了如19年《审查办法（征求意见稿）》里的审查目的限制以外，《审查办法》也增添了有关资料未经提供方同意不得向无关方披露的要求，以尽可能全面地保护企业权益。

（六）更多实施细则有待出台

《审查办法》确定了网络安全审查的基本流程和要求，但在实施过程中还有待其他部门出台有关实施细则。例如，《审查办法》尚未就审查决定设置申诉途径。如果审查未通过，运营者是否可以基于合理理由提出异议？作为利益相关方的网络产品及服务的提供者，是否也有权对审查决定提出申诉？此外，运营者识别、关键信息基础设施保护工作部门有关本行业及领域的预判指南、适用网络产品与服务的具体类别等问题也有待立法者进行进一步的说明与探讨。

四、《审查办法》对相关企业的影响

对于运营者而言，本次《审查办法》构建了多部门联席工作机制，推动了安全审查与行业监管的衔接，减轻了运营者可能需向网信办和行业监管部门多头申报网络安全审查的负担。但另一方面，《审查办法》将是否需要进行网络安全审查申报的预判义务、后续产品和服务提供者履行承诺的监督义务等均施加于运营者，且其需对上述义务的履行承担法律责任，从而可能会增加运营者在生产经营中的负担。尤其在目前有关运营者范围、需申报网络产品与服务采购具体类别等指南尚未发布的情况下，运营者可能难以准确把握申报的启动标准和时机。因此，我们建议从事公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域的经营者：

1. 就自身是否属于运营者与行业监管部门进行密切的沟通和确认；

2. 对于不确定是否要进行网络安全审查申报的产品和服务采购，与网信办和关键信息基础设施保护工作部门进行充分的沟通和确认；

3. 建立公司内部对网络安全和服务采购的审查机制，包括但不限于：（1）对网络产品和服务提供商的安全资质进行事先审查；（2）完善与网络产品和服务提供商的采购协议，约定其对网络安全审查的配合义务和不遵守网络安全审查中所做承诺所需向运营者承担的违约责任；（3）有权针对产品和服务提供者履行网络安全审查中做出承诺的情况进行不定期的抽查和监测，或者要求产品和服务提供者就履行情况向运营者定期提交报告。

对于网络产品和服务的提供者而言，考虑到网络安全审查为运营者产品和服务采购合同签署或生效的前提条件，其可能增加向运营者提供网络产品和服务的不确定性、延长采购合同正式生效履行的时间。对于可能向运营者提供网络产品和服务的供应商而言，建议：

1. 对于可能的客户群体进行分类，针对客户所处的不同行业类型，根据安全审查重点预先做好准备，以便有针对性的与不同行业主管部门进行沟通；

2. 对于可能涉及关键敏感行业的客户，就是否已经被认定为运营者充分沟通，并跟踪认定结果；

3. 对于可能向运营者提供服务比例较大的供应商，内部提前核查网络安全审查可能涉及的考量因素，并形成初步结论；

4. 配合启动网络安全审查，并根据内部核查结果履行对于运营者的承诺，包括不利用提供产品和服务的便利条件非法获取用户数据、非法控制和操纵用户设备，无正当理由不中断产品供应或必要的技术支持服务等。

总体而言，《审查办法》构建了国家网络安全审查体系的总体实施框架，我们相信，随着未来具体实施细则的出台，网络安全审查将深入影响运营者的日常运维与采购活动，因此，我们建议运营者与网络产品及服务提供者切实关注相关立法动态，以审慎判断自身活动受规制和受影响的程度，以便及时响应政策与法规的要求，确保做出在合规基础上的最优商业选择。

（本文发布于2020年04月28日。）

[13]《审查办法（征求意见稿）》第十条。

[14]《网络安全审查办法》答记者问[EB/OL]. https://mp.weixin.qq.com/s/yzhiqTvfi107cir2zpMkdw. 发布日期：2020年4月27日，最后访问日期：2020年4月28日.

[15]《审查办法》第十六条。

叶上初生并蒂莲——最新出台的《电子商务法》与《网络安全法》之比较

在上个世纪九十年代，使用互联网还被称为“上网冲浪”，断电和座机欠费可能是我们能够理解的最大“网络安全”问题。在那个十年，很长的一段时间内亚马逊还是条河，阿里巴巴还在等待四十大盗，京东还在卖光驱，“电子商务”还是镜花水月。但几乎是一瞬间，“电子商务”成为最时髦的词汇，互联网交易风潮无可阻挡，而“千年虫”、“熊猫烧香”等网络病毒随即席卷全球，网络成为最大的逐利场也是众矢之的的风险高地。二十年过去了，“网络安全”已经从网络运行安全，扩展到网络信息安全，并上升到公民的人身财产安全甚至国家安全的层次；“电子商务”也重塑了大家的交易习惯，逐渐成为国民经济的支柱性产业之一。风险与收益并存、安全与发展互促，“网络安全”和“电子商务”似乎从未脱离彼此。

2017年6月1日《中华人民共和国网络安全法》（下称“**《网安法》**”）正式生效，成为我国规范网络运行安全和信息安全的基础性法律。《中华人民共和国电子商务法》（下称“**《电商法》**”）作为管理电子商务经营者、规范电子商务交易秩序的基础性法律，也在昨日正式通过。纵观两部法律，尽管规制的法律关系有所不同，但由于电子商务与网络的天然联系，《网安法》与《电商法》仿佛“叶上初生并蒂莲”，在网络安全领域的法律规则上相得益彰。

一、《电商法》与《网安法》的一脉相承

《网安法》对《电商法》的影响，从立法审议时间线便可看出端倪：2016年12月《电商法》草案第一次提交审议，恰逢《网安法》表决通过不久。[1]而自第一次审议开始，《电商法》就已对电子商务领域网络安全等问题予以高度关注。回顾立法进程，《电商法》最初曾大篇幅反映网络安全立法需求，后续审议稿尽管精简了相关条款，但保留了其中的关键条款，体现出《电商法》对网络安全，特别是电子商务消费者个人信息权益保护的重视。

《电商法》与《网安法》的一致性，充分反映在《电商法》有关网络安全的规则条款中。《网安法》以网络运行安全、网络信息安全为切入点，对各行各业的网络安全制度提出了整体性、综合性的要求。而作为电子商务领域的基础性法律，《电商法》对电子商务经营者的网络安全要求同样也落脚于网络运行安全与信息安全方面的责任与义务。

例如，《电商法》第三十条规定，电子商务平台经营者应当采取技术措施和其他必要措施保证其网络安全、稳定运行，防范网络违法犯罪活动，有效应对网络安全事件，保障电子商务交易安全；同时要求电子商务平台经营者制定网络安全事件应急预案，在发生网络安全事件时应立即启动应急预案，采取相应的补救措施，并向有关主管部门报告。《电商法》的这些要求均与《网安法》下的规则制度要求相同。[2]《电商法》对电子商务平台经营者有关保证网络运行安全，预防网络安全事件的要求是对《网安法》基本规则在电子商务领域的重申和确认。

而在网络信息安全领域，《电商法》与《网安法》也同样呈现出一脉相承的特点。《电商法》第二十三条简明扼要地指出电子商务经营者在收集、使用个人信息时所应遵循的法律规则[3]。而第二十四条有关对电子商务经营者对用户个人信息相关权益的尊重与保护，[4]则是承继了《网安法》中对个人信息主体权益保护的总体思路。

二、《电商法》对《网安法》的具化和延伸

虽然在网络安全基本规则思路上一脉相承，相比于《网安法》对网络运营者的

[1]《网安法》系2016年11月7日由全国人大常委会表决通过。

[2]《网安法》第十条规定，建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。第二十五条规定，网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

[3]《电商法》第二十三条规定，电子商务经营者收集、使用其用户的个人信息，应当遵守法律、行政法规有关个人信息保护的规定。

[4]《电商法》第二十四条规定，电子商务经营者应当明示用户信息查询、更正、删除以及用户注销的方式、程序，不得对用户信息查询、更正、删除以及用户注销设置不合理条件。电子商务经营者收到用户信息查询或者更正、删除的申请的，应当在核实身份后及时提供查询或者更正、删除用户信息。用户注销的，电子商务经营者应当立即删除该用户的信息；依照法律、行政法规的规定或者双方约定保存的，依照其规定。

一般规制，《电商法》结合电子商务领域的特点，一方面对《网安法》下的一般性规则进行了细化，另一方面也针对电子商务领域进一步延伸具体要求，体现了不同法律权益的平衡。

（一）数据存储和安全保障：平台上信息的记录、保存与保护

根据《电商法》第三十一条，电子商务平台经营者应当至少在三年内记录、保存平台上发布的商品和服务信息、交易信息，并确保信息的完整性、保密性、可用性。

而根据《网安法》及其配套措施的相关规定，个人信息的收集、使用等处理活动应当进行记录，且并未对于记录的时间长短进行严格的限制（网络日志留存六个月）；此外，根据《网安法》第十条，网络运营者应采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性；而在2018年5月1日《信息安全技术个人信息安全规范》（下称“《安全规范》”）中第4点（f）项进一步明确了个人信息处理的确保安全原则，要求保护个人信息的保密性、完整性、可用性。

相较而言，《电商法》的规定不仅对记录和保存义务的时间限制进一步明确，同时还就电子商务平台经营者对信息的安全保护义务范围进行了澄清，从“网络数据”具化至“平台上发布的商品和服务信息、交易信息”。这一过程中，数据类型的澄清反映了目前电子商务经营过程中最为主要的信息范围，避免了在电子商务经营者因《网安法》下安全保障义务范围过大而付出过高的合规成本；而时间限制的设定则与《民法总则》第一百八十八条[5]调整后的民事诉讼时效保持了一致，为电子商务领域的诉讼纠纷中的证据保留和收集提供了保障，一定程度上将数据存储义务体系和纠纷解决机制进行了融通。

（二）个人信息的使用：个性化搜索结果展示

《电商法》第十八条第一款规制了电子商务经营者利用大数据分析等技术向用户展示个性化搜索结果的行为。该款规定，电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务的搜索结果的，应当同时向该消费者提供不针对其个人特征的选项，尊重和平等保护消费者合法权益。

对应地，《网安法》第四十一条规定了网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则；而《安全规范》第7.10条规定了当仅依据信息系统的自动决策而做出显著影响个人信息主体权益的决定时，个人信息控制者应向个人信息主体提供申诉方法。

一般认为，《电商法》第十八条的规定主要是防止电子商务经营者利用大数据分析“杀熟”，即电子商务经营者利用大数据算法，通过收集用户画像、支付能力、支付意愿，做到“一人一价”，甚至出现“会员价”高于正常价格的情况。而由于大数据分析过程均在后台完成，具有较高的隐蔽性，消费者在受到歧视待遇时甚至无法察觉。因此，在电子商务经营者利用大数据分析进行个性化搜索结果展示时，要求其提供不针对特定消费者个人特征的产品或服务的选项，有助于保障消费者的知情权以及公平交易的权利，一定程度上避免“歧视”情况发生。对比《网安法》体系下对网络运营者使用个人信息的正当性原则要求以及自动化决策的约束规定，《电商法》针对目前行业中典型问题，将正当性原则解释为消费者平等选择的权利，将约束自动化决策的方式由“提供申诉方法”调整为“提供不针对其个人特征的选项”，一方面反映了电子商务领域的现实实践，同时也是通过对一般体系下非强制性规则（《安全规范》为推荐性国家标准）的适度突破，确保了在平台和消费者力量极端不对等情况下对自动化决策的约束。

（三）个人信息主体权利：访问与注销

《网安法》在第四十三条中要求网络运营者在特定前提下满足个人信息主体的两项权利，删除权及更正权。作为《网安法》的配套国家标准，《安全规范》沿袭该思路对个人信息控制者收集、使用个人信息，对实现个人信息主体合法权益保护等提出了具体的要求，在《网安法》基本规则以及个人权利响应上补充了“访问权”、“注销权”、“可携权”等。但由于《安全规范》作为非强制性的推荐性国家标准，其效力直接影响了上述个人权利响应机制要求的落地。

《电商法》第二十四条不仅进一步确认个人信息主体在《网安法》下的删除权及更正权，在法律层面明确要求电子商务经营者还应当明示用户信息“查询”及“用户注销”的方式、程序，不得对用户信息“查询”以及“用户注销”设置不合理条件，加强了“访问权”及“注销权”的强制力。

但值得注意的是，《电商法》并未采纳《安全规范》7.9条中推荐的“可携权”。根据《安全规范》中“可携权”的要求，根据个人信息主体的请求，个人信息控制者应为个人信息主体提供获取以下类型个人信息副本的方法，或在技术可行的前提下直接将特定个人信息的副本传输给第三方。“可携权”在欧洲《一般数据保护条例》（General Data Protection Regulation，“GDPR”）第二十条中以“Right to Portability”的形式体现，其立法的初衷考虑到可携的前提是数据的格式化和标准化，格式化数据在不同主体间的自由流通，有助于消除形成数据流通的技术壁垒，促进数据经济的发展。从《电商法》角度出发，未采纳“可携权”并不是与数据自由流通的大趋势相背离，而更可能是维护现阶段市场稳定发展的取舍之道。尽管目前数据已成为电子商务领域的重要竞争资源，但数据权属以及各主体对数据主张权利边界等问题并不清晰。在中

[5] 参见《民法总则》第一百八十八条第一款：向人民法院请求保护民事权利的诉讼时效期间为三年。法律另有规定的，依照其规定。

国电子商务领域目前高速发展又激烈竞争的特殊阶段和大背景下，在法律层面强制性推行“可携权”可能会降低企业的竞争积极性，造成电子商务市场的混乱。因此《电商法》有选择性地采纳《安全规范》中个人信息主体的权利，体现了其在市场发展不同阶段，不同法律权益的取舍和平衡。

（四）互联网内容审核：消费者评价的删除

依据《电商法》第三十九条，电子商务平台经营者不得删除消费者的评价。[6]本条规定旗帜鲜明地针对目前电商平台中出现的刷单、篡改评价以影响消费者正常判断平台内经营者信用和服务质量的现状，通过禁止电子商务平台经营者删除消费者评价，杜绝恶意的评价删改行为，确保了电商平台依据第三十九条第一款建立的信用评价体系的有效性。

而从此前的互联网信息内容管理体系来看，根据《网安法》第四十七条，网络运营者发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告；而《互联网信息服务管理办法》第十五条，互联网信息服务提供者不得制作、复制、发布和传播的信息类型包括九类；同时，根据同文第十六条，互联网信息服务提供者在发现前述九类信息内容时，应立即停止传输，保存有关记录，并向国家有关机关报告。

看似《电商法》中的规定可能与现行互联网信息内容管理制度相冲突，导致消费者评价这一信息内容跳出现行管制体系；但实质上看，第三十九条的规定内容对电子商务平台经营者的互联网信息内容管理义务并未减少，仅在义务实现方式上作出了调整。由于《电商法》并未将消费者评价排除于互联网信息以外，而电子商务平台经营者依法不得删除该等信息，则要求其在该等信息发布前采取更为严格、准确、有效的信息筛选机制，由事前防范通过消费者评价的途径发布或传输违法违规信息。为此，《电商法》基于对信用评价体系有效性的保障，将现行互联网内容审核通常的“事前筛选+事后补漏”机制在消费者评价方面进行了适度的调整，使得以《网安法》和《互联网信息服务管理办法》为基础的一般性互联网内容审核体系与信用评价体系融洽共存。

（五）其余存在差异的条款

此外，《电商法》中还存在一些可能与《网安法》中特定规则存在差异的条款，有待日后的执法和司法实践进一步调和不同立法之间的差异，包括但不限于：

1. 《电商法》第二十五条中对电子商务经营者配合有关主管部门、提供电子商务数据提出了相应的义务要求：根据《网安法》的相关规定，并未赋予有关主管部门在非履行网络安全监督管理职能、侦查国家犯罪及国家安全等情形下要求网络运营者未经用户同意提供个人信息的职权，则有关主管部门如行使此职权要求电子商务经营者提供电子商务数据且其中涉及用户个人信息时，电子商务经营者将不可避免地陷入必然违法的两难境地；此外，《网安法》第四十二条一般性规定中，未经被收集者同意，不得向他人提供个人信息，而根据《电商法》中的规定，有关主管部门可依据行政法规级别的授权向电子商务经营者要求提供电子商务数据，如涉及个人信息时，则很可能需要进行在《网安法》和《电商法》的规定之间折中选取合理边界。
2. 《电商法》第七十九条虽将侵害个人信息和不履行网络安全义务的行为责任直接转引至《网安法》等法律和行政法规的罚则规定，而在其余罚则条款中仍有部分内容涉及网络安全相关义务的履行，以第七十六条第三项为例，其中规定的侵害、影响用户信息查询、更正、删除以及用户注销权利的行为，对电子商务经营者而言由市场监督管理部门责令限期改正，可以处一万元以下的罚款；而《网安法》第六十四条[7]规定，处罚方式不仅包括责令改正和罚款，还视情节严重程度可采取责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照等罚则，且罚款计算方式与此项亦有所不同。为此，有关主管部门在进行监督管理和执法处罚时，为确保符合合理、适当的原则，则需更为谨慎地选取法律依据和处罚程度。

三、小结与展望

无论是“网络安全”和“电子商务”的天然联系，还是《网安法》和《电商法》立法进程的紧密衔接，两部法律之间立法宗旨和思路始终一脉相承、根源相通；针对的规制对象和范围虽有差别，但《网安法》和《电商法》均着眼于网络运行和网络信息两个方面，通过强制性义务和权利的分配（如前述制定网络安全事件应急预案的义务、用户个人信息的相关权利等），确保网络安全，实现技术和经济稳步、健康发展。

[6] 参见《电商法》第三十九条：电子商务平台经营者应当建立健全信用评价制度，公示信用评价规则，为消费者提供对平台内销售的商品或者提供的服务进行评价的途径。

电子商务平台经营者不得删除消费者对其平台内销售的商品或者提供的服务的评价。

[7]《网安法》第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。

但同样两部法律也存在着利益权衡取舍上的不同，尤其是《电商法》对《网安法》建立的一般性网络安全合规体系在电子商务领域具化和延伸过程中，《电商法》充分反映了特定领域的特定情况，适度调整了具体的规制规则（如前述消费者评价上起主要作用的互联网信息审核方式），使得《网安法》下的一般体系在电商领域具有了更细致和贴切的展现形式。

总体而言，网络安全为电子商务的发展保驾护航，电子商务又是网络安全的重要实践领域，为此，《网安法》及其配套措施的制定、出台确立了一般性的网络安全保护义务体系，而《电商法》则针对电商领域将关键条款进行了具体适用和延展；值得期待的是，这两朵“并蒂莲花”结合之下，为电商领域的网络安全保护提供更为综合、细致和具有针对性的体系化规制，为电子商务市场的健康发展奠定更为坚实的基础。

附表：《电商法》中涉及网络安全的条款汇总

分类	主要内容	条款规定
与网络运行安全有关的条款	电子商务平台经营者保障网络安全的一般性义务	**第三十条** 电子商务平台经营者应当采取**技术措施**和**其他必要措施**保证其网络安全、稳定运行，防范网络违法犯罪活动，有效应对网络安全事件，保障电子商务交易安全。 电子商务平台经营者应当制定**网络安全事件应急预案**，发生网络安全事件时，应当立即启动应急预案，采取相应的补救措施，并向有关主管部门报告。
与网络信息安全有关的条款	电子商务经营者的推销和广告限制	**第十八条** 电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务的搜索结果的，应当同时向该消费者**提供不针对其个人特征的选项**，尊重和平等保护消费者合法权益。 电子商务经营者向消费者发送广告的，应当遵守《中华人民共和国广告法》的有关规定。
	用户个人信息的收集和使用义务	**第二十三条** 电子商务经营者收集、使用其用户的个人信息，应当遵守法律、行政法规有关**个人信息保护**的规定。
	用户信息权利的实现与保障	**第二十四条** 电子商务经营者应当明示用户信息**查询、更正、删除**以及用户**注销**的方式、程序，不得对用户信息查询、更正、删除以及用户注销设置不合理条件。 电子商务经营者收到用户信息查询或者更正、删除的申请的，应当在核实身份后及时提供查询或者更正、删除用户信息。用户注销的，电子商务经营者应当立即删除该用户的信息；依照法律、行政法规的规定或者双方约定保存的，依照其规定。
	电子商务数据的提供和保护要求	**第二十五条** 有关主管部门依照法律、行政法规的规定要求电子商务经营者提供有关电子商务数据信息的，电子商务经营者**应当提供**。有关主管部门应当采取必要措施保护电子商务经营者提供的数据信息的**安全**，并对其中的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。
	平台上信息的记录、保存与保护	**第三十一条** 电子商务平台经营者应当**记录**、保存平台上发布的商品和服务信息、交易信息，并确保信息的**完整性、保密性、可用性**。商品和服务信息、交易信息保存时间自交易完成之日起不少于**三年**；法律、行政法规另有规定的，依照其规定。
	服务协议和交易规则的内容要求	**第三十二条** 电子商务平台经营者应当遵循公开、公平、公正的原则，制定平台服务协议和交易规则，明确进入和退出平台、商品和服务质量保障、消费者权益保护、**个人信息保护**等方面的权利和义务。
	服务协议和交易规则的公示要求	**第三十三条** 电子商务平台经营者应当在其首页显著位置**持续公示**平台服务协议和交易规则信息或者上述信息的链接标识，并保证经营者和消费者能够便利、完整地阅览和下载。
	服务协议和交易规则的修改要求	**第三十四条** 电子商务平台经营者修改平台服务协议和交易规则，应当在其首页显著位置**公开征求意见**，采取合理措施确保有关各方能够及时充分表达意见。修改内容应当至少在**实施前七日予以公示**。 平台内经营者不接受修改内容，要求退出平台的，电子商务平台经营者不得阻止，并按照修改前的服务协议和交易规则承担相关责任。

分类	主要内容	条款规定
与网络信息安全有关的条款	平台内商品和服务的信用评价制度	**第三十九条** 电子商务平台经营者应当建立健全**信用评价制度**，公示信用评价规则，为消费者提供对平台内销售的商品或者提供的服务进行评价的途径。 电子商务平台经营者**不得删除**消费者对其平台内销售的商品或者提供的服务的评价。
	电子支付对账服务和交易记录的提供	**第五十三条** 电子商务当事人可以约定采用电子支付方式支付价款。 电子支付服务提供者为电子商务提供电子支付服务，应当遵守国家规定，告知用户电子支付服务的功能、使用方法、注意事项、相关风险和收费标准等事项，不得附加不合理交易条件。电子支付服务提供者应当确保电子支付指令的完整性、一致性、可跟踪稽核和不可篡改。 电子支付服务提供者应当向用户**免费提供对账服务以及最近三年的交易记录**。
	争议解决中提供合同与交易记录	**第六十二条** 在电子商务争议处理中，电子商务经营者应当提供**原始合同和交易记录**。因电子商务经营者丢失、伪造、篡改、销毁、隐匿或者拒绝提供前述资料，致使人民法院、仲裁机构或者有关机关无法查明事实的，电子商务经营者应当承担相应的法律责任。
	电子商务数据的流动与共享	**第六十九条** 国家维护电子商务交易安全，保护电子商务用户信息，鼓励电子商务数据开发应用，保障**电子商务数据依法有序自由流动**。 国家采取措施推动建立公共数据共享机制，促进电子商务经营者依法利用公共数据。
	与网络信息安全相关的罚则	**第七十六条** 电子商务经营者违反本法规定，有下列行为之一的，由市场监督管理部门责令限期改正，可以处一万元以下的罚款，对其中的电子商务平台经营者，依照本法第八十一条第一款的规定处罚： （一）未在首页显著位置公示营业执照信息、行政许可信息、属于不需要办理市场主体登记情形等信息，或者上述信息的链接标识的； （二）未在首页显著位置持续公示终止电子商务的有关信息的； （三）未明示用户信息查询、更正、删除以及用户注销的方式、程序，或者对用户信息查询、更正、删除以及用户注销设置不合理条件的。 电子商务平台经营者对违反前款规定的平台内经营者未采取必要措施的，由市场监督管理部门责令限期改正，可以处二万元以上十万元以下的罚款。
		第七十七条 电子商务经营者违反本法第十八条第一款规定提供搜索结果，或者违反本法第十九条规定搭售商品、服务的，由市场监督管理部门责令限期改正，没收违法所得，可以并处五万元以上二十万元以下的罚款；情节严重的，并处二十万元以上五十万元以下的罚款。 **第七十九条** 电子商务经营者违反法律、行政法规有关个人信息保护的规定，或者不履行本法第三十条和有关法律、行政法规规定的网络安全保障义务的，依照《中华人民共和国网络安全法》等法律、行政法规的规定处罚。
		第八十条 电子商务平台经营者有下列行为之一的，由有关主管部门责令限期改正；逾期不改正的，处二万元以上十万元以下的罚款；情节严重的，责令停业整顿，并处十万元以上五十万元以下的罚款： **（一）不履行本法第二十七条规定的核验、登记义务的；** **（二）不按照本法第二十八条规定向市场监督管理部门、税务部门报送有关信息的；** **（三）不按照本法第二十九条规定对违法情形采取必要的处置措施，或者未向有关主管部门报告的；** **（四）不履行本法第三十一条规定的商品和服务信息、交易信息保存义务的。** **法律、行政法规对前款规定的违法行为的处罚另有规定的，依照其规定。**
		第八十一条 电子商务平台经营者违反本法规定，有下列行为之一的，由市场监督管理部门责令限期改正，可以处二万元以上十万元以下的罚款；情节严重的，处十万元以上五十万元以下的罚款： **（一）未在首页显著位置持续公示平台服务协议、交易规则信息或者上述信息的链接标识的；** **（二）修改交易规则未在首页显著位置公开征求意见，未按照规定的时间提前公示修改内容，或者阻止平台内经营者退出的；** **（三）未以显著方式区分标记自营业务和平台内经营者开展的业务的；** **（四）未为消费者提供对平台内销售的商品或者提供的服务进行评价的途径，或者擅自删除消费者的评价的。** **电子商务平台经营者违反本法第四十条规定，对竞价排名的商品或者服务未显著标明“广告”的，依照《中华人民共和国广告法》的规定处罚。**

（本文发布于2018年09月01日。）

“欲穷千里目，更上一层楼”
——国际新形势下的等保2.0

在2007年，好莱坞的“Die Hard”（虎胆龙威）系列第四部电影正式上映，电影中能达到“fire sale”程度的网络攻击会企图分三步通过“交通系统”、“金融和通讯系统”和其他基础设施来攻占整个美国的网络系统。十年后的2017年，“WannaCry”勒索病毒在全球肆虐，直接影响到公共服务、重要业务、基础设施的正常运行，电影中看似荒诞的情节逐渐在真实生活中上演。随后陆续发生的委内瑞拉遭受网络攻击导致大停电、某著名酒店及某社交类互联网平台等公司频频发生上亿数量级的客户数据泄露等事件，也印证了电影中对于“网络安全”的担忧。

在网络安全的新形势下，网络空间已成为大国博弈的制高点，以国家意志来保障网络空间安全与发展，正成为各国国家战略，并成为培育新的国家比较优势的重要方面。[1]而我国**《网络安全法》**（以下简称“《网安法》”）亦在2017年正式施行，旨在提高全社会的网络安全意识和网络安全保障水平，其中专门构建了**“网络安全等级保护制度”**作为保障基本网络、关键信息基础设施与大数据安全的基础。在全球化网络空间主权争夺的大背景下“登高望远”，“网络安全等级保护制度”是作为提升我国网络安全水平，保障国家安全，促进经济发展，迎接国际化挑战的基础制度之一。

一、“再上层楼”，从1.0到2.0

（一）1.0到2.0，十年磨一剑

早在1994年，我国就已经通过《计算机信息系统安全保护条例》确立了适用于“计算机信息系统”的安全等级保护制度，经过多年的发展形成以《信息系统安全等级保护管理办法》（以下简称**“《等保办法》”**）为核心的规范体系，这一规范体系常常被称作**“等保1.0”**体系。2017年，《网安法》将“国家网络安全等级保护制度”提升为法律要求，使得等级保护制度从“信息（系统）安全”层面进一步拓展至“网络安全”层面。以《网安法》为标志，我国网络安全等级保护制度进入**“等保2.0”**时代。

近日正式发布的三项核心国家标准（即GB/T 22239-2019 《信息安全技术 网络安全等级保护基本要求》、GB/T 25070-2019 《信息安全技术 网络安全等级保护安全设计技术要求》与GB/T 28448-2019 《信息安全技术 网络安全等级保护测评要求》）均将于2019年7月1日正式施行，意味着“等保2.0”时代的新里程正式启航。

[1] “推动全球网络空间治理体系变革”，具体参见 http://www.xinhuanet.com/politics/2018-07/07/c_1123091116.htm （访问日期：2019年5月17日）。

（二）全球互联时代的等保2.0体系

为了积极响应和配合落实《网安法》对“网络安全等级保护制度”的要求，2018年6月，公安部会同中央网信办、国家保密局、国家密码管理局等主管部门联合起草、发布了《网络安全等级保护条例（征求意见稿）》（以下简称“**《网络等保条例（征求意见稿）》**”），具体构筑网络运行分级保护和分级管理的制度体系。

除了法律法规，等保制度作为网络运营者落实网络安全保护义务、国家维护信息和网络安全的重要依据与有力抓手，高度依赖国家标准对等级评定、技术建设整改、测评等环节的具体要求和实践指导。相应地，着眼于当前的技术条件和产业发展变化，为体现更好的政策与产业兼容性，等保2.0体系也将云计算、物联网、工业控制系统和大数据等应用纳入防护体系中。

（三）等保2.0的核心变化

	等保1.0	等保2.0
防护理念	遵循“一个中心、三重防御”的理念，即“安全管理中心”+“安全通信网络、安全区域边界、安全计算环境的防御”	
标准命名	“信息系统安全”	“网络安全等级保护”
定级对象	“信息系统”	“基础信息网络、信息系统（含）采用移动互联技术的系统、云计算平台/系统、大数据应用/平台/资源、物联网和工业控制系统”
安全要求结构	不区分“通用要求”和“拓展要求”	区分“通用要求”和“拓展要求” 针对云计算、移动互联网、物联网以及工业控制系统等四大新型应用领域的行业特点，明确提出相应的安全拓展要求
（安全）技术要求结构	“物理安全” “网络安全” “主机安全” “应用安全” “数据安全和备份与恢复”	“安全物理环境” “安全通信网络” “安全区域边界” “安全计算环境” “安全管理中心”
（安全）管理要求结构	“安全管理制度” “安全管理机构” “人员安全管理” “系统建设管理” “系统运维管理”	“安全管理制度” “安全管理机构” “安全管理人员” “安全建设管理” “安全运维管理”

	等保1.0	等保2.0
定级流程	“确定定级对象”→“确定等级”→（“主管部门/专家审核”）→“公安机关备案审查”→“最终确定等级”	“确定定级对象”→“初步确定等级”→“专家评审”→“主管部门审核”→“公安机关备案审查”→“最终确定等级”
测评周期	四级系统每半年进行一次测评	三级（以上）系统每年进行一次测评
内容调整		新增了“个人信息保护”的内容； 强调安全通信网络、安全区域边界和安全计算环境等三重防御的“可信验证”

二、等保2.0的责任和义务

（一）开展等保是履行法律义务的一部分

开展网络安全等级保护工作的主要目的就是要保护国家关键信息基础设施安全、维护国家安全，这是一项事关国家安全、社会稳定、国家利益的重要决策部署。[2]因此，国家机关、企事业单位开展等保工作将有助于从基础和根本层面推进网络安全防护，履行《网安法》所提出的网络安全合规义务，维护企业自身网络安全。

2019年1月，公安部宣布在全国范围内连续第二年开展“**净网**”专项行动，要求“进一步加大互联网安全监管力度，督促企业落实主体责任，依法严厉查处不履行网络安全义务、为网络违法犯罪提供支持帮助等违法违规行为”，[3]并已在全国范围内逐渐取得显著成效。[4]事实上，现实中已出现不落实等保要求而被认定违法并处罚的案例。[5]

（二）等保2.0与《网安法》相关义务的承接

考虑到《网安法》是等保2.0制度的法律依据，原则上如果企业根据等保2.0的相关制度规定和技术要求相应地落实等级保护义务，能够较大程度地履行《网安法》中的相关义务（具体示例请见下表）。然而，我们也注意到，虽然《网安法》义务与等保制度的落实从性质上都属于法律义务，《网安法》义务与等保2.0要求仍然存在一定区别，这将要求企业在合规实践中着重关注二者之间的差异，整合现有的合规体系避免遗漏。

例如《网安法》第二十一条对网络运营者留存网络日志的期限存在六个月的具体要求。相较而言，如某网络运营者的内部办公系统被评定为等保二级系统，按照其相应的安全通用要求“应详细记录运维操作日志，包括日常巡检工作、运行维护记录、参数的设置和修改等内容”，并不存在明确的日志留存期限要求。

此外，等保2.0中的特定要求也可能为澄清《网安法》中的具体规定提供了重要参考。虽然关键信息基础设施通常被要求达到等保三级及其以上的要求，但等保2.0制度中在三级安全通用要求中，并未明确要求企业将数据（如个人信息或重要数据）存储于境内服务器。然而，在云计算安全拓展要求中则存在“应保证云计算基础设施位于中国境内”以及“应确保云服务客户数据、用户个人信息等存储于中国境内，如需出境应遵循国家相关规定”的要求。在等保2.0制度与《网安法》及其配套措施要求保持一致的前提下，该要求将进一步增加云计算基础设施被认定为关键信息基础设施的可能性。

---

[2] “推动全球网络空间治理体系变革”，具体参见 http://www.xinhuanet.com/politics/2018-07/07/c_1123091116.htm （访问日期：2019年5月17日）。

[3] “公安部召开‘净网2018’专项行动总结暨‘净网2019’专项行动部署会 林锐出席并讲话”，具体参见 http://www.mps.gov.cn/n2253534/n2253535/c6372997/content.html （访问日期：2019年5月17日）。

[4] “各地深入开展‘净网2019”专项行动’，具体参加 http://www.mps.gov.cn/n2255079/n4242954/n4841045/n4841055/c6470655/content.html（访问日期：2019年5月17日）。

[5] 据报道，2019年2月，南京某研究院、无锡某图书馆因安全责任意识淡薄、网络安全等级保护制度落实不到位、管理制度和技术防护措施严重缺失，导致网站遭受攻击破坏。南京、无锡警方依据《网络安全法》第21条、第59条规定，对上述单位分别予以5万元罚款，对相关责任人予以5千元、2万元不等罚款，同时责令限期整改安全隐患，落实网络安全等级保护制度。“江苏网警发布‘净网2019’专项行动行政执法典型案例”，具体参见 https://www.secrss.com/articles/9157 （访问日期：2019年5月17日）。

	《网安法》相关条款	《网络安全等级保护基本要求》相关要求项/控制点（摘录）
第二十一条	（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任	（以等保二级要求为例） 7.1.6 安全管理制度 7.1.7 安全管理机构 7.1.8 安全管理人员
	（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施	（以等保二级要求为例） 7.1.3.3 & 4 安全区域边界-入侵防范 & 恶意代码防范 7.1.4.3 & 4 安全计算环境-入侵防范 & 恶意代码防范
	（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月	（以等保二级要求为例） 7.1.3.5 安全区域边界-安全审计 7.1.4.5 安全计算环境-安全审计 7.1.10.6 安全运维管理-网络和系统安全管理 注：未明确要求网络日志留存期限不少于六个月
	（四）采取数据分类、重要数据备份和加密等措施	（以等保二级要求为例） 7.1.4.1 安全计算环境-身份鉴别 7.1.4.7 安全计算环境-数据完整性 7.1.4.8 安全计算环境-数据备份恢复 注：未明确数据分类要求
第二十五条	网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。	（以等保二级要求为例） 7.1.10.12安全运维管理-安全事件处置 7.1.10.13安全运维管理-应急预案管理
第三十四条	（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查	（以等保三级要求为例） 8.1.7 安全管理机构 8.1.8 安全管理人员
	（二）定期对从业人员进行网络安全教育、技术培训和技能考核	（以等保三级要求为例） 8.1.8.3 安全管理人员-安全意识教育和培训
	（三）对重要系统和数据库进行容灾备份	（以等保三级要求为例） 8.1.4.9 安全计算环境-数据备份恢复 注：备份等级未明确要求具备容灾能力
	（四）制定网络安全事件应急预案，并定期进行演练	（以等保三级要求为例） 8.1.10.13安全运维管理-应急预案管理
第三十七条	关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。	（以云计算安全拓展要求为例） 7.2.1.1 安全物理环境-基础设施位置 7.2.4.3 安全计算环境-数据完整性和保密性 注：三级安全通用要求中不存在明确的数据本地化要求
第四十一条	网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。 网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。	（以等保二级要求为例） 7.1.4.11 安全计算环境-个人信息保护
第四十二条	网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。 网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。	

三、企业开展等保工作的具体指南

（一）公司内部需要做等保的网络/信息系统的范围?

根据《网络安全等级保护基本要求》等标准文件的规定，等级保护对象主要包括基础信息网络、云计算平台/系统、大数据应用/平台/资源、物联网（IoT）和工业控制系统和采用移动互联技术的系统等。对于普通企业而言，企业网站、办公系统和管理系统、企业开发的移动应用软件理论上都会落入到上述等级保护对象的范畴内。

值得注意的是，根据《网络等保条例（征求意见稿）》的有关规定，个人及家庭自建自用的网络无需适用《网络等保条例（征求意见稿）》。[6]涉密网络除遵守一般的等保义务之外，还应当依据国家保密规定和标准，结合系统实际进行保密防护和保密监管。[7]

（二）企业开展等保工作的具体流程?

对于企业而言，网络安全等级保护工作大致可以分为定级对象梳理、定级、备案、网络安全建设、等保测评和安全运行与维护六个阶段。企业可以根据自身情况自行或聘用专业咨询机构开展等保工作，以下是我们梳理的等保工作各阶段的具体工作内容和参与方。

[6]《网络等保条例（征求意见稿）》第二条。

[7]《网络等保条例（征求意见稿）》第四条。

（三）企业已经通过ISO 27000系列标准的认证，是否仍需开展等保工作？

ISO2 7000系列标准是目前国际范围内认可度最高的信息安全管理标准体系之一。实践中，很多大型企业已按照ISO 27000系列标准构建了集团内部的信息安全管理组织架构和组织制度，并适用于全球范围内的集团实体。

ISO 27000系列标准和国内等保标准均能指导企业建立适合企业实际要求的信息安全管理体系，二者均结合系统的重要程度，从技术和管理两方面出发提出风险控制要求，如信息安全处理机制、访问控制、安全审计等。即便如此，等保标准关注于底层网络安全的控制，两者对于网络安全等级的分级标准、具体的信息安全要求仍然存在不小的差异。

相应地，即使企业已经通过了ISO 27000系列标准的认证，企业仍应当按照上述工作流程逐步开展等保工作，在确定企业各系统的网络安全等级之后，在网络安全建设阶段，企业可以基于已有的ISO 27000体系制度进行相应的整改和完善。

（四）可能被认定为第二级的网络？

根据《网络等保条例（征求意见稿）》的规定，对拟定为第二级以上的网络，其运营者应当组织专家评审来完成定级工作，并应当在网络的安全保护等级确定后到县级以上公安机关备案。因此，公司的网络是否被认定为二级网络是企业密切关注的问题。

根据规定，一旦受到破坏会对相关公民、法人和其他组织的合法权益造成严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全的一般网络属于第二级网络。参照公安部相关部门的定级原则：第二级信息系统一般适用于县级单位中的重要信息系统，地市级以上国家机关、企事业单位内部一般的信息系统，例如非涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统等。[8]

（五）哪些网络可能被定为第三级网络？

相比于等保1.0，等保2.0对第三级及以上网络提出了更加严格的网络安全保护义务。根据《网络等保条例（征求意见稿）》的规定，第三级以上的网络运营者需要承担更多的网络安全保护义务，包括对网络安全管理负责人和关键岗位的人员进行安全背景审查；建立网络安全等级测评制度；境内实施技术运维的原则要求等。

根据相关规定，一旦受到破坏会对相关公民、法人和其他组织的合法权益造成特别严重损害，或者会对社会秩序和社会公共利益造成严重危害，或者对国家安全造成危害的重要网络。参照公安部相关部门的定级原则，第三级信息系统一般适用于地市级以上国家机关、企业、事业单位内部重要的信息系统，例如涉及工作秘密、商业秘密、敏感信息的办公系统和管理系统；跨省或全国联网运行的用于生产、调度、管理、指挥、作业、控制等方面的重要信息系统以及这类系统在省、地市的分支系统；中央各部委、省（区、市）门户网站和重要网站；跨省连接的网络系统等。[9]

（六）如何看待关键信息基础设施保护与等保的关系？

网络安全等级保护制度是国家网络安全保障工作的基本制度，关键信息基础设施是网络安全等级保护的重点。关键信息基础设施的安全建设应当遵守网络安全等级保护制度的相关要求。

根据此前《信息安全技术 网络安全等级保护定级指南（征求意见稿）》中的建议，对于确定为关键信息基础设施的，原则上其安全保护等级不低于第三级。因此，关键信息基础设施运营者至少应当按照第三级网络安全等级保护的要求开展等保工作。如关键信息基础设施根据其重要性被认定为第五级的网络，则应当遵守特殊的管理模式和安全要求。

（七）企业已完成等保1.0的合规工作，是否还需要开展等保2.0工作？

如前所述，等保2.0在等保1.0的基础上提出了很多新的技术和组织上的安全管理要求。已经完成等保1.0合规工作的企业，同样应当对比等保2.0的要求，进一步加强网络安全建设，以确保通过新的等保测评。对于新上线的网络和信息系统，则应当按照等保2.0的要求进行系统梳理、定级、备案和测评。

（八）企业完成等保工作后，是否已经满足个人信息保护管理要求？

等保2.0在“通用要求”、“安全计算环境”的安全控制点中新增了“个人信息保护”的内容，但仅仅提出了原则性的管理要求。比如，对于第二级的网络仅要求“应仅采集和保存业务必须的用户个人信息；禁止未授权访问和非法使用用户个人信息”。实践中，企业仍需遵守《网安法》的相关规定，并可参照《互联网个人信息安全保护指南》、《GB/T 35273—2017 信息安全技术 个人信息安全规范》等落实个人信息保护安全管理义务。

（本文发布于2019年05月20日。）

[8]“关于重要信息系统安全等级保护定级的几点意见”，具体参见http://www.djbh.net/webdev/web/SafeProductAction.do?p=getBzgfZxbz&id=8a8182565deefd0d015e6ee9603d0078 （访问日期：2019年5月17日）。

[9]“关于重要信息系统安全等级保护定级的几点意见”，具体参见http://www.djbh.net/webdev/web/SafeProductAction.do?p=getBzgfZxbz&id=8a8182565deefd0d015e6ee9603d0078 （访问日期：2019年5月17日）。

“云深不知处”
——企业远程办公的网络安全常见问题及建议

当前是新型冠状病毒防控的关键期，举国上下万众一心抗击疫情。为增强防控，自二月初以来，北京、上海、广州、杭州等各大城市政府公开表态或发布通告，企业通过信息技术开展远程协作办公、居家办公[1]。2月19日，工信部发布《关于运用新一代信息技术支撑服务疫情防控和复工复产工作的通知》，面对疫情对中小企业复工复产的严重影响，支持运用云计算大力推动企业上云，**重点推行远程办公、居家办公、视频会议、网上培训、协同研发和电子商务等在线工作方式**[2]。

面对国家和各地政府的呼吁，全国企业积极响应号召。南方都市报在2月中旬发起的网络调查显示，有47.55%的受访者在家办公或在线上课[3]。面对特殊时期庞大的远程办公需求，远程协作平台也积极承担社会担当，早在1月底，即有17家企业的21款产品宣布对全社会用户或特定机构免费开放其远程写作平台软件[4]。

通过信息技术实现远程办公，无论是网络层、系统层，还是业务数据，都将面临更加复杂的网络安全环境，为平稳有效地实现安全复工复产，降低疫情对企业经营和发展的影响，企业应当结合实际情况，建立或者适当调整相适应的网络与信息安全策略。

一、远程办公系统的类型

随着互联网、云计算和物联网等技术的深入发展，各类企业，尤其是互联网公司、律所等专业服务公司，一直在推动实现企业内部的远程协作办公，尤其是远程会议、文档管理等基础功能应用。从功能类型来看，远程办公系统可分为以下几类：[5]

- 综合协作工具，即提供一套综合性办公解决方案，功能包括即时通信和多方通信会议、文档协作、任务管理、设计管理等，代表软件企包括企业微信、钉钉、飞书等。
- 即时通信（即Instant Messaging或IM）和多方通信会议，允许两人或以上通过网络实时传递文字、文件并进行语音、视频通信的工具，代表软件包括Webex、Zoom、Slack、Skype等。
- 文档协作，可为多人提供文档的云存储和在线共享、修改或审阅功能，代表软件包括腾讯文档、金山文档、印象笔记等。
- 任务管理，可实现任务流程、考勤管理、人事管理、项目管理、合同管理等企业办公自动化（即Office Automation或OA）功能，代表软件包括Trello、Tower、泛微等。

[1] 中国新闻网，“商务密集区如何防控？北京防控发布会：鼓励远程办公”，http://www.chinanews.com/sh/2020/02-03/9077372.shtml；上海市政府，《致全市各企业书》，http://www.shanghai.gov.cn/nw2/nw2314/nw32419/nw48516/nw48545/u26aw63495.html；广州市防控新型冠状病毒感染的肺炎疫情工作指挥部办公室，《关于做好企业安全有序复工复产工作的通知》，http://www.gz.gov.cn/xw/tzgg/content/post_5655587.html；新华网，《关于杭州市企业严格疫情防控有序推进复工的通告》，http://www.zj.xinhuanet.com/2020-02/07/c_1125541724.htm。

[2] 工信部官网，http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757022/c7683415/content.html

[3] 南方都市报，“疫情之下，近半受访者远程办公学习，超七成人一周出门少于三次”，https://www.sohu.com/a/374155614_161795

[4] 亿欧智库，“疫情下‘隔离’办公，哪些远程协作产品免费助攻？”，https://www.iyiou.com/intelligence/insight122758.html

[5] “协同办公会爆发吗？”，https://www.zhitongcaijing.com/content/detail/271209.html

- 设计管理，可根据使用者要求，系统地进行设计方面的研究与开发管理活动，如素材、工具、图库的管理，代表软件包括创客贴、Canvas等。

二、远程办公不同模式下的网络安全责任主体

《网络安全法》（“**《网安法》**”）的主要规制对象是网络运营者，即网络的所有者、管理者和网络服务提供者。网络运营者应当承担《网安法》及其配套法规下的网络运行安全和网络信息安全的责任。

对于远程办公系统而言，不同的系统运营方式下，网络安全责任主体（即网络运营者）存在较大的差异。按照远程办公系统的运营方式划分，企业远程办公系统大致可以分为自有系统、云办公系统和综合型系统三大类。企业应明确区分其与平台运营方的责任界限，以明确判断自身应采取的网络安全措施。

（一）自有系统

此类模式下，企业的远程办公系统部署在自有服务器上，系统由企业自主研发、外包研发或使用第三方企业级软件架构。此类系统开发成本相对较高，但因不存在数据流向第三方服务器，安全风险则较低，常见的企业类型包括国企、银行业等重要行业企业与机构，以及经济能力较强且对安全与隐私有较高要求的大型企业。

无论是否为企业自研系统，由于系统架构完毕后由企业单独所有并自主管理，**因此企业构成相关办公系统的网络运营者，承担相应的网络安全责任。**

（二）云办公系统

此类办公系统通常为SaaS系统或APP，由平台运营方直接在其控制的服务器上向企业提供注册即用的系统远程协作软件平台或APP服务，供企业用户与个人（员工）用户使用。此类系统构建成本相对经济，但往往只能解决企业的特定类型需求，企业通常没有权限对系统进行开发或修改，而且企业数据存储在第三方服务器。该模式的常见企业类型为相对灵活的中小企业。

由于云办公系统（SaaS或APP）的网络、数据库、应用服务器都由平台运营方运营和管理，因此，**云办公系统的运营方构成网络运营者，通常对SaaS和APP的网络运行安全和信息安全负有责任。**

实践中，平台运营方会通过用户协议等法律文本，将部分网络安全监管义务以合同约定方式转移给企业用户，如要求企业用户严格遵守账号使用规则，要求企业用户对其及其员工上传到平台的信息内容负责。

（三）综合型系统

此类系统部署在企业自有服务器和第三方服务器上，综合了自有系统和云办公，系统的运营不完全由企业控制，多用于有多地架设本地服务器需求的跨国企业。

云办公系统的供应商和企业本身都可能构成网络运营者，应当以各自运营、管理的网络系统为边界，对各自运营的网络承担相应的网络安全责任。

对于企业而言，为明确其与平台运营方的责任边界，企业应当首先确认哪些“网络”是企业单独所有或管理的。在远程办公场景下，企业应当考虑多类因素综合认定，分析包括但不限于以下：

- 办公系统的服务器、终端、网络设备是否都由企业及企业员工所有或管理；
- 企业对企业使用的办公系统是否具有最高管理员权限；
- 办公系统运行过程中产生的数据是否存储于企业所有或管理的服务器；
- 企业与平台运营方是否就办公系统或相关数据的权益、管理权有明确的协议约定等。

当然，考虑到系统构建的复杂性与多样性，平台运营方和企业在远程协作办公的综合系统中，可能不免共同管理同一网络系统，双方均就该网络承担作为网络运营者的安全责任。但企业仍应通过合同约定，尽可能固定网络系统中双方各自的管理职责以及网络系统的归属。因此，**对于共同管理、运营远程协作办公服务平台的情况下，企业和平台运营方应在用户协议中明确双方就该系统各自管理运营的系统模块、各自对其管理的系统模块的网络安全责任以及该平台的所有权归属。**

三、远程办公涉及的网络安全问题及应对建议

下文中，我们将回顾近期远程办公相关的一些网络安全热点事件，就涉及的网络安全问题进行简要的风险评估，并为企业提出初步的应对建议。

（一）用户流量激增导致远程办公平台“短时间奔溃”，平台运营方是否需要承担网络运行安全责任？

事件回顾：

2020年2月3日，作为春节假期之后的首个工作日，大部分的企业都要求员工在家办公。尽管各远程办公系统的平台运营方均已经提前做好了应对预案，但是巨量的并发响应需求还是超出了各平台运营商的预期，多类在线办公软件均出现了短时间的“信息发送延迟”、“视频卡顿”、“系统奔溃退出”等故障[6]。在出现故障后，平台运营方迅速采取了网络限流、服务器扩容等措施，提高了平台的运载支撑能力和稳定性，同时故障的出现也产生一定程度的分流。最终，尽管各远程办公平台都在较短的时间内恢复了平台的正常运营，但还是遭到了不少用户的吐槽。

[6] 搜狐网，“企业微信钉钉崩溃，远程办公谁在‘江湖救急’？”，https://www.sohu.com/a/370534054_429401

风险评估：

依据《网络安全法》（以下简称《网安法》）第22条的规定，网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

远程办公平台的运营方，作为平台及相关网络的运营者，应当对网络的运行安全负责。对于短时间的系统故障，**平台运营方是否需要承担相应的法律责任或违约责任，需要结合故障产生的原因、故障产生的危害结果、用户协议中的责任约定等因素来综合判断。**

对于上述事件而言，基于我们从公开渠道了解的信息，尽管多个云办公平台出现了响应故障问题，给用户远程办公带来了不便，但平台本身并未暴露出明显的安全缺陷、漏洞等风险，也没有出现网络数据泄露等实质的危害结果，因此，各平台很可能并不会因此而承担**网络安全的法律责任。**

应对建议：

在疫情的特殊期间，主流的远程办公平台产品均免费开放，因此，各平台都会有大量的新增客户。对于平台运营方而言，良好的应急预案和更好的用户体验，肯定更有利于平台在疫情结束之后留住这些新增的用户群体。

为进一步降低平台运营方的风险，提高用户体验，我们建议平台运营方可以：

- **将用户流量激增作为平台应急事件处理，制定相应的应急预案**，例如，在应急预案中明确流量激增事件的触发条件、服务器扩容的条件、部署临时备用服务器等；
- 对用户流量实现实时的监测，及时调配平台资源；
- **建立用户通知机制和话术模板**，及时告知用户系统响应延迟的原因及预计恢复的时间等；
- **在用户协议或与客户签署的其他法律文本中，尝试明确该等系统延迟或奔溃事件的责任安排。**

（二）在远程办公环境下，以疫情为主题的钓鱼攻击频发，企业如何降低外部网络攻击风险？

事件回顾：

疫情期间，某网络安全公司发现部分境外的黑客组织使用冠状病毒为主题的电子邮件进行恶意软件发送，网络钓鱼和欺诈活动。比如，黑客组织伪装身份（如国家卫健委），以“疫情防控”相关信息为诱饵，发起钓鱼攻击。这些钓鱼邮件攻击冒充可信来源，邮件内容与广大人民群众关注的热点事件密切相关，极具欺骗性。一旦用户点击，可能导致主机被控，重要信息、系统被窃取和破坏[7]。

风险评估：

依据《网安法》第21、25条的规定，网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：（1）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；（2）**采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；（3）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；**（4）采取数据分类、重要数据备份和加密等措施；（5）法律、行政法规规定的其他义务。同时，网络运营者还应当**制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。**

远程办公的实现，意味着企业内网需要响应员工移动终端的外网接入请求。员工所处的网络安全环境不一，无论是接入网络还是移动终端本身，都更容易成为网络攻击的对象。一方面，公用WiFi、网络热点等不可信的网络都可能作为员工的网络接入点，这些网络可能毫无安全防护，存在很多常见的容易被攻击的网络漏洞，容易成为网络犯罪组织侵入企业内网的中转站；另一方面，部分员工的移动终端设备可能会安装设置恶意程序的APP或网络插件，员工在疏忽的情况下也可能点击伪装的钓鱼攻击邮件或勒索邮件，严重威胁企业内部网络的安全。

在计算机病毒或外部网络攻击等网络安全事件下，被攻击的企业尽管也是受害者，但如果企业没有按照《网安法》及相关法律规定的要求提前采取必要的技术防范措施和应急响应预案，导致网络数据泄露或者被窃取、篡改，给企业的用户造成损失的，很可能依旧需要承担相应的法律责任。

应对建议：

对于企业而言，为遵守《网安法》及相关法律规定的网络安全义务，我们建议，企业可以从网络安全事件管理机制、移动终端设备安全、数据传输安全等层面审查和提升办公网络的安全：

（1）企业应当**根据其运营网络或平台的实际情况、员工整体的网络安全意识，制定相适应的网络安全事件管理机制，**包括但不限于：

- **制定包括数据泄露在内的网络安全事件的应急预案；**

[7] Freebuf，“趁火打劫，谨防黑客冒充权威疫情防控机构，利用‘疫情’发起钓鱼攻击”，https://www.freebuf.com/column/226800.html

- **建立应对网络安全事件的组织机构和技术措施；**
- 实时监测最新的钓鱼网站、勒索邮件事件；
- 建立有效的与全体员工的通知机制，包括但不限于邮件、企业微信等通告方式；
- **制定与员工情况相适应的信息安全培训计划；**
- **设置适当的奖惩措施，要求员工严格遵守公司的信息安全策略。**

（2）企业应当根据现有的信息资产情况，采取以下措施，进一步保障移动终端设备安全：

- **根据员工的权限等级，制定不同的移动终端设备安全管理方案**，例如，高级管理人员或具有较高数据库权限的人员仅能使用公司配置的办公专用移动终端设备；
- **制定针对移动终端设备办公的管理制度**，对员工使用自带设备进行办公提出明确的管理要求；
- 定期对办公专用的移动终端设备的系统进行更新、漏洞扫描；
- 在终端设备上，对终端进行身份准入认证和安全防护；
- 重点监测远程接入入口，采用更积极的安全分析策略，发现疑似的网络安全攻击或病毒时，应当及时采取防范措施，并及时联系企业的信息安全团队；
- **就移动办公的信息安全风险，对员工进行专项培训。**

（3）保障数据传输安全，企业可以采取的安全措施包括但不限于：

- 使用HTTPS等加密传输方式，保障数据传输安全。无论是移动终端与内网之间的数据交互，还是移动终端之间的数据交互，都宜对数据通信链路采取HTTPS等加密方式，防止数据在传输中出现泄漏。
- 部署虚拟专用网络（VPN），员工通过VPN实现内网连接。值得注意的是，在中国，VPN服务（尤其是跨境的VPN）是受到电信监管的，仅有具有VPN服务资质的企业才可以提供VPN服务。**外贸企业、跨国企业因办公自用等原因，需要通过专线等方式跨境联网时，应当向持有相应电信业务许可证的基础运营商租用。**

（三）内部员工通过VPN进入公司内网，破坏数据库。企业应当如何预防“内鬼”，保障数据安全？

事件回顾：

2月23日晚间，微信头部服务提供商微盟集团旗下SaaS业务服务突发故障，系统崩溃，生产环境和数据遭受严重破坏，导致上百万的商户的业务无法顺利开展，遭受重大损失。根据微盟25日中午发出的声明，此次事故系人为造成，微盟研发中心运维部核心运维人员贺某，于2月23日晚18点56分通过个人VPN登入公司内网跳板机，因个人精神、生活等原因对微盟线上生产环境进行恶意破坏。目前，贺某被上海市宝山区公安局刑事拘留，并承认了犯罪事实[8]。由于数据库遭到严重破坏，微盟长时间无法向合作商家提供电商支持服务，此处事故必然给合作商户带来直接的经济损失。作为港股上市的企业，微盟的股价也在事故发生之后大幅下跌。

从微盟的公告可以看出，微盟员工删库事件的一个促成条件是**“该员工作为运维部核心运维人员，通过个人VPN登录到了公司内网跳板机，并具有删库的权限”**。该事件无论是对SaaS服务商而言，还是对普通的企业用户而言，都值得反思和自省。

风险评估：

依据《网安法》第21、25条的规定，网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：（1）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；（2）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；（3）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；（4）采取数据分类、重要数据备份和加密等措施；（5）法律、行政法规规定的其他义务。同时，网络运营者还应当**制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。**

内部员工泄密一直是企业数据泄露事故的主要原因之一，也是当前“侵犯公民个人信息犯罪”的典型行为模式。远程办公环境下，企业需要为大部分的员工提供连接内网及相关数据库的访问权限，进一步增大数据泄露甚至被破坏的风险。

与用户流量激增导致的系统“短时间崩溃”不同，“微盟删库”事件的发生可能与企业内部信息安全管理有直接的关系。如果平台内合作商户产生直接经济损失，不排除平台运营者可能需要承担网络安全相关的法律责任。

应对建议：

为有效预防员工恶意破坏、泄露公司数据，保障企业的数据安全，我们建议企业可以采取以下预防措施：

[8] 腾讯网，“微盟系统故障超24小时 SaaS行业客服安全质受疑”，https://new.qq.com/omn/20200228/20200228A00AZQ00.html

- **制定远程办公或移动办公的管理制度，区分办公专用移动设备和员工自有移动设备，进行分类管理**，包括但不限于严格管理办公专用移动设备的读写权限、员工自有移动设备的系统权限，尤其是企业数据库的管理权限；
- **建立数据分级管理制度**，例如，应当根据数据敏感程度，制定相适应的访问、改写权限，对于核心**数据库**的数据，应当禁止员工通过远程登录方式进行操作或处理；
- 根据员工工作需求，依据必要性原则，评估、审核与限制员工的数据访问和处理权限，例如，禁止员工下载数据到任何用户自有的移动终端设备；
- **建立数据泄露的应急管理方案，包括安全事件的监测和上报机制，安全事件的响应预案；**
- 制定远程办公的操作规范，使用文件和材料的管理规范、应用软件安装的审批流程等；
- **组建具备远程安全服务能力的团队**，负责实时监控员工对核心数据库或敏感数据的操作行为、数据库的安全情况；
- **加强对员工远程办公安全意识教育。**

（四）疫情期间，为了公共利益，企业通过系统在线收集员工疫情相关的信息，是否需要取得员工授权？疫情结束之后，应当如何处理收集的员工健康信息？

场景示例：

在远程办公期间，为加强用工管理，确保企业办公场所的健康安全和制定相关疫情防控措施，企业会持续地向员工收集各类疫情相关的信息，包括个人及家庭成员的健康状况、近期所在地区、当前住址、所乘航班或火车班次等信息。收集方式包括邮件、OA系统上报、问卷调查等方式。企业会对收集的信息进行统计和监测，在必要时，向监管部门报告企业员工的整体情况。如发现疑似病例，企业也会及时向相关的疾病预防控制机构或者医疗机构报告。

风险评估：

2020年1月20日，新型冠状病毒感染肺炎被国家卫健委纳入《中华人民共和国传染病防治法》规定的乙类传染病，并采取甲类传染病的预防、控制措施。《中华人民共和国传染病防治法》第三十一条规定，任何单位和个人发现传染病病人或者疑似传染病病人时，应当及时向附近的疾病预防控制机构或者医疗机构报告。

2月9日，中央网信办发布了《关于做好个人信息保护利用大数据支撑联防联控工作的通知》（以下简称**《通知》**），各地方各部门要高度重视个人信息保护工作，**除国务院卫生健康部门依据《中华人民共和国网络安全法》、《中华人民共和国传染病防治法》、《突发公共卫生事件应急条例》授权的机构外，其他任何单位和个人不得以疫情防控、疾病防治为由，未经被收集者同意收集使用个人信息。法律、行政法规另有规定的，按其规定执行。**

各地也陆续出台了针对防疫的规范性文件，以北京为例，根据《北京市人民代表大会常务委员会关于依法防控新型冠状病毒感染肺炎疫情 坚决打赢疫情防控阻击战的决定》，本市行政区域内的机关、**企业事业单位、社会团体和其他组织应当依法做好本单位的疫情防控工作，建立健全防控工作责任制和管理制度，**配备必要的防护物品、设施，**加强对本单位人员的健康监测，**督促从疫情严重地区回京人员按照政府有关规定进行医学观察或者居家观察，**发现异常情况按照要求及时报告并采取相应的防控措施。**按照属地人民政府的要求，积极组织人员参加疫情防控工作。

依据《通知》及上述法律法规和规范性文件的规定，我们理解，在疫情期间，**如果企业依据《中华人民共和国传染病防治法》、《突发公共卫生事件应急条例》获得了国务院卫生健康部门的授权，企业在授权范围内，应当可以收集本单位人员疫情相关的健康信息，而无需取得员工的授权同意。如果不能满足上述例外情形，企业还是应当依照《网安法》的规定，在收集前获得用户的授权同意。**

《通知》明确规定，为疫情防控、疾病防治收集的个人信息，不得用于其他用途。任何单位和个人未经被收集者同意，不得公开姓名、年龄、身份证号码、电话号码、家庭住址等个人信息，但因联防联控工作需要，且经过脱敏处理的除外。收集或掌握个人信息的机构要对个人信息的安全保护负责，采取严格的管理和技术防护措施，防止被窃取、被泄露。具体可参考文章《解读网信办<关于做好个人信息保护利用大数据支撑防疫联控工作的通知>》。

应对建议：

在远程期间，如果企业希望通过远程办公系统收集员工疫情相关的个人信息，我们建议各企业应当：

- **制定隐私声明或用户授权告知文本，在员工初次提交相关信息前，获得员工的授权同意；**
- **遵循最小必要原则，制定信息收集的策略，包括收集的信息类型、频率和颗粒度；**
- **遵循目的限制原则，对收集的疫情防控相关的个人信息进行区分管理，避免与企业此前收集的员工信息进行融合；**
- **在对外展示企业整体的健康情况时或者披露疑似病例时，对员工的相关信息进行脱敏处理；**
- **制定信息删除管理机制，在满足防控目的之后，及时删除相关的员工信息；**
- **制定针对性的信息管理和保护机制，将收集的员工疫情相关的个人信息，作为个人敏感信息进行保护，严格控制员工的访问权限，防止数据泄露。**

（五）远程办公期间，为有效监督和管理员工，企业希望对员工进行适当的监测，如何才能做到合法合规？

场景示例：

远程办公期间，为了有效监督和管理员工，企业根据自身情况制定了定时汇报、签到打卡、视频监控工作状态等措施，要求员工主动配合达到远程办公的监测目的。员工通过系统完成汇报、签到打卡时，很可能会反复提交自己的姓名、电话号码、邮箱、所在城市等个人基本信息用于验证员工的身份。

同时，在使用远程OA系统或App时，办公系统也会自动记录员工的登录日志，记录如IP地址、登录地理位置、用户基本信息、日常沟通信息等数据。此外，如果员工使用企业分配的办公终端设备或远程终端虚拟机软件开展工作，终端设备和虚拟机软件中可能预装了监测插件或软件，在满足特定条件的情况下，会记录员工在终端设备的操作行为记录、上网记录等。

风险评估：

上述场景示例中，企业会通过1）员工主动提供和2）办公软件自动或触发式收集两种方式收集员工的个人信息，构成《网安法》下的个人信息收集行为。企业应当根据《网安法》及相关法律法规的要求，遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并获取员工的同意。

对于视频监控以及系统监测软件或插件的使用，如果操作不当，并且没有事先取得员工的授权同意，很可能还会侵犯到员工的隐私，企业应当尤其注意。

应对建议：

远程办公期间，尤其在当前员工还在适应该等工作模式的情形下，企业根据自身情况采取适当的监督和管理措施，具有正当性。我们建议企业可以采取以下措施，以确保管理和监测行为的合法合规：

- **评估公司原有的员工合同或员工个人信息收集授权书，是否能够满足远程办公的监测要求，如果授权存在瑕疵，应当根据企业的实际情况，设计获取补充授权的方式，包括授权告知文本的弹窗、邮件通告等；**
- **根据收集场景，逐项评估收集员工个人信息的必要性。例如，是否存在重复收集信息的情况，是否有必要通过视频监控工作状态，监控的频率是否恰当；**
- **针对系统监测软件和插件，设计单独的信息收集策略，做好员工隐私保护与公司数据安全的平衡；**
- 遵守目的限制原则，未经员工授权，不得将收集的员工数据用于工作监测以外的其他目的。

结语

此次疫情，以大数据、人工智能、云计算、移动互联网为代表的数字科技在疫情防控中发挥了重要作用，也进一步推动了远程办公、线上运营等业务模式的发展。这既是疫情倒逼加快数字化智能化转型的结果，也代表了未来新的生产力和新的发展方向[9]。此次“突发性的全民远程办公热潮”之后，远程办公、线上运营将愈发普及，线下办公和线上办公也将形成更好的统一，真正达到提升工作效率的目的。

加快数字化智能化升级也是推进国家治理体系和治理能力现代化的迫切需要。党的十九届四中全会对推进国家治理体系和治理能力现代化作出重大部署，强调要推进数字政府建设，加强数据共享，建立健全运用互联网、大数据、人工智能等技术手段进行行政管理的制度规则[10]。

为平稳加速推进数字化智能化发展，契合政府现代化治理的理念，企业务必需要全面梳理并完善现有的网络安全与数据合规策略，为迎接新的智能化管理时代做好准备。

（本文发布于2020年03月05日。）

[9] 新浪网，“国资委副主任翁杰明：国有企业要作推动数字化智能化升级的排头兵”，http://finance.sina.com.cn/china/gncj/2020-03-04/doc-iimxyqvz7787423.shtml

[10] 同上。

博观而约取，厚积而薄发：《密码法》要点评析及企业合规路径

自《网络安全法》实施以来，中国网络安全与数据合规监管日益深入，网络安全与数据合规已经成为企业的基础合规工作，近期也在企业融资并购交易尽调和上市审查中被重点关注。密码作为网络与信息安全的核心保障技术和基础支撑，密码合规是企业网络安全与数据合规工作中不可或缺的部分。

早在1999年，我国就已经针对商用密码产品制定并实施了《商用密码管理条例》（以下简称《管理条例》），此外对于其他类型密码的规制还散见于《中华人民共和国保守国家秘密法》、《含有密码技术的信息产品政府采购规定》等不同的法律法规中。经过二十年的摸索和积累，2019年10月26日，我国经十三届全国人大常委会第十四次会议表决通过，密码管理领域的第一部综合性法律《中华人民共和国密码法》（以下简称《密码法》）终于将在2020年1月1日生效。

本文将基于《密码法》的法律条文以及其与既有监管要求的区别和衔接，对“放管服”的商用密码管理模式和“关键环节”的特殊监管制度进行重点梳理，并就《密码法》在区块链产业的适用问题进行初步探讨，最后针对商用密码产品的生产和销售企业、普通网络运营者和关键信息基础设施运营者，分别提出应对建议。

一、 中国的密码管理法律体系

在《密码法》出台之前，以《管理条例》为中心，国家密码管理局针对科研、生产、销售、进出口等环节制定了包括《商用密码产品生产管理规定》、《商用密码科研管理规定》在内的多个部门规章，对密码行业实行全面的行政许可和专控管理制度。但随着近几年简化行政审批的“放管服”行政制度改革的持续深化，商用密码产品生产单位审批、商用密码产品销售单位许可等一批商用密码行政许可事项逐渐被取消，国家密码管理局也相应地废止和修改了部分管理规定。

《管理条例》及其配套管理规定都只针对商用密码进行管理，不包括对国家秘密内容的信息进行加密保护或者安全认证所使用的密码技术和密码产品。对于涉及国家秘密的密码产品的管理要求，则散见于《中华人民共和国保守国家秘密法》、《含有密码技术的信息产品政府采购规定》等法律法规中。

规范名称	发布机构	法律状态	生效时间
《密码法》	全国人大常委会	待生效	2020.01.01
《网络安全法》	全国人大常委会	现行有效	2017.06.01
《中华人民共和国保守国家秘密法》	全国人大常委会	现行有效	1989.05.01 2010年10月修订
《商用密码管理条例》	国务院	现行有效	1999.10.07
《商用密码产品生产管理规定》	国家密码管理局	现行有效	2006.01.01 2017年12月修订
《商用密码科研管理规定》	国家密码管理局	现行有效	2006.01.01 2017年12月修订
《电子认证服务密码管理办法》	国家密码管理局	现行有效	2009.12.01 2017年12月修订
《含有密码技术的信息产品政府采购规定》	国家密码管理局、国家安全部等	现行有效	2008.03.01

规范名称	发布机构	法律状态	生效时间
《密码产品和含有密码技术的设备进口管理目录》	国家密码管理局	现行有效	2014.01.01
《国家密码管理局关于做好商用密码产品生产单位审批等 4 项行政许可取消后相关管理政策衔接工作的通知》	国家密码管理局	现行有效	2017.10.11
《国家密码管理局关于废止和修改部分管理规定的决定》	国家密码管理局	现行有效	2017.12.01
《信息安全等级保护商用密码管理办法》	国家密码管理局	现行有效	2008.01.01
《商用密码产品销售管理规定》	国家密码管理局	已失效	2006.01.01 2017年12月废止
《商用密码产品使用管理规定》	国家密码管理局	已失效	2007.05.01 2017年12月废止
《境外组织和个人在华使用密码产品管理办法》	国家密码管理局	已失效	2007.05.01 2017年12月废止

二、《密码法》下分类管理制度

《密码法》下的密码指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。该法明确了密码分类管理制度，密码包括核心密码、普通密码和商用密码。

密码分类	保护的信息种类
核心密码	属于国家秘密的信息：绝密级、机密级、秘密级
普通密码	属于国家秘密的信息：机密级、秘密级
商业密码	不属于国家秘密的信息

与《管理条例》明确将商用密码技术认定为国家秘密不同。**《密码法》第七条仅将核心密码、普通密码认定为国家秘密**，要求密码管理部门依照本法和有关法律、行政法规、国家有关规定对核心密码、普通密码实行严格统一管理。

《密码法》首次通过法律规定了核心密码、普通密码使用要求、安全管理制度以及国家加强核心密码、普通密码工作的一系列特殊保障制度和措施。但整体而言，《密码法》主要规范的还是商用密码产品。以下，我们将就“放管服”模式下的商业密码进行重点讨论。

三、“放管服”模式下的商业密码

《密码法》贯彻了“简政放权、放管结合、优化服务”的改革思路和公平竞争的原则，通过重点把控关键环节管理商用密码，“由重事前审批更多地转为事中事后监管，重视发挥标准化和检测认证的支撑作用”[1]。此外，《密码法》重视与现有网络安全制度的衔接，规定商用密码的检测认证、应用安全性评估和国家安全审查等制度均应适用或衔接《网络安全法》的配套法律法规，以避免重复认证、评估，合理降低企业的合规成本。

（一）商业密码管理之简政放权

• 全流程放权，从“管企业”到“重点管产品”

如前所述，《管理条例》及其配套管理规定，在商用密码科研、生产、销售和使用等环节进行全面的行政许可和专控管理制度，设置了较高的行业准入门槛，尤其是对外商投资企业。但近年来，我国贯彻“放管服”的行政改革要求，通过减少行政审批，逐步放宽行业准入市场。具体而言，国务院年分别于2015年颁布《国务院关于取消和调整一批行政审批项目等事项的决定》（国发〔2015〕11号）（以下简称“2015年《决定》”），于2017年颁布《国务院关于取消一批行政许可事项的决定》（国发〔2017〕46号）（以下简称“2017年《决定》”），取消了商用密码科研、生产、销售和使用等方面的多项行政许可和审批。

《密码法》延续“放管服”的改革思路，没有采取《管理条例》对商用密码各个环节逐条规定管制方式的立法思路，而是通过第二十一条在原则上规定商用密码的各环节应用不得损害国家安全、社会公共利益或者他人合法权益，标志着《密码法》以法律的形式确认了近年来行政机关在商用密码领域全流程简政放权的改革成果。

根据《国家密码管理局关于做好商用密码产品生产单位审批等4项行政许可取消后相关管理政策衔接工作的通知》（国密局字〔2017〕336号）（以下简称“**《国密通知》**”）的规定，

[1] “国家密码管理局负责人就《中华人民共和国密码法》答记者问”，http://www.oscca.gov.cn/sca/xwdt/2019-10/27/content_1057218.shtml，最后访问于2019年11月7日。

生产、销售商用密码产品的单位无需再经国家密码管理局批准，但**生产、销售的商用密码产品仍应当依法办理《商用密码产品型号证书》**。外商投资企业使用境外生产的密码产品、境外组织和个人使用密码产品或者含有密码技术的设备，无需再经国家密码管理局批准，但**外商投资企业、境外组织和个人使用的密码产品或者含有密码技术的设备需要从境外进口的，仍应当依法办理《密码产品和含有密码技术的设备进口许可证》**。

同时，密码管理局将继续依法**实施商用密码产品销售登记备案制度，取得《商用密码产品型号证书》的单位应当于每年1月31日前**，向所在地的省、自治区、直辖市密码管理部门**如实报送上一年度商用密码产品销售登记备案数据**。

基于现行适用的法律法规，我们通过下表梳理了既有商用密码行政许可和审批资质的存续情况。

商用密码行政许可和审批资质	2015年《决定》	2017年《决定》	《密码法》
商用密码科研定点单位证书	取消	N/A	N/A
商用密码产品生产定点单位证书	√	取消	N/A
商用密码产品销售许可证	√	取消	N/A
使用境外生产的密码产品准用证	√	取消	N/A
境外组织或个人使用密码产品准用证	√	取消	N/A
商用密码产品出口许可证[2]	√	√	对适用范围作出修订
密码产品和含有密码技术的设备进口许可[3]	√	√	对适用范围作出修订
商用密码产品型号证书[4]	√	√	与《网安法》网络关键设备和网络安全专用产品衔接
商用密码产品质量检测机构审批[5]	√	√	保留检测、认证机构资质，但商用密码产品由全部强制检测制度调整为自愿检测和强制检测相结合的制度
信息安全等级保护商用密码测评机构审批[6]	√	√	与《网安法》相衔接
电子政务电子认证服务机构认定[7]	√	√	明确认定制度
电子认证服务使用密码许可[8]	√	√	未提及
商用密码科研成果审查鉴定[9]	√	√	未提及

此外，我们了解到国家密码管理局目前正在就新法下商用密码事前行政审批的适用问题开展研究。考虑到《密码法》贯彻落实“放管服”行政改革的立法立意，不排除未来会进一步放宽现行有效的商用密码行政审批（如商用密码科研成果审查鉴定、电子认证服务使用密码许可等）的适用，继续降低商用密码产业准入门槛。

[2] 根据《管理条例》第十三条：“进口密码产品以及含有密码技术的设备或者出口商用密码产品，必须报经国家密码管理机构批准。任何单位或者个人不得销售境外的密码产品。”

[3] 同上。

[4] 根据《管理条例》第八条：“商用密码产品指定生产单位生产的商用密码产品的品种和型号，必须经国家密码管理机构批准，并不得超过批准范围生产商用密码产品。”

[5] 根据《管理条例》第九条：“商用密码产品，必须经国家密码管理机构指定的产品质量检测机构检测合格。”

[6] 根据《信息安全等级保护商用密码管理办法》（国密局发〔2007〕11号）第十一条：“信息安全等级保护商用密码测评工作由国家密码管理局指定的测评机构承担。”

[7] 根据《电子政务电子认证服务管理办法（试行）》第十七条：“国家密码管理局组织开展认证服务能力评估，发布《电子政务电子认证服务机构目录》。”

[8] 根据《中华人民共和国电子签名法》第十七条：“提供电子认证服务，应当具备下列条件：……（五）具有国家密码管理机构同意使用密码的证明文件；……”

[9] 根据《管理条例》第六条：“商用密码的科研成果，由国家密码管理机构组织专家按照商用密码技术标准和技术规范审查、鉴定。”

• 非歧视原则

《密码法》规定了外商投资企业和境外主体在商用密码领域的国民待遇。第二十一条规定，“各级人民政府及其有关部门应当遵循非歧视原则，依法平等对待包括外商投资企业在内的商用密码科研、生产、销售、服务、进出口等单位（以下统称商用密码从业单位）。”《密码法》在商用密码具体权利义务的规定中不区分主体是否为外商，亦充分体现了新法下的商用密码准入的“非歧视原则”。

具体而言，《密码法》在下列几个方面为外商在华从事商用密码业务注入强心剂，为贯彻非歧视原则提供制度保障：

首先，国家鼓励在外商投资过程中基于自愿原则和商业规则开展商用密码技术合作。行政机关及其工作人员不得利用行政手段强制转让商用密码技术（第二十一条）。该规定与同样将于2020年1月1日生效的《外商投资法》禁止行政机关利用行政手段强制外商转让技术的规定[10]一脉相承，反映了近年来国家强调平等保护外商在华合法权益、完善公平市场竞争环境的立法趋势。

第二，明确密码管理部门、有关部门及其工作人员不得要求密码从业单位和检测认证机构向其披露源代码等密码相关专有信息，并应对其在履行职责中知悉的商业秘密、个人隐私严格保密。

第三，规定商用密码检测认证机构应在其履行职责中知悉的国家秘密和商业秘密承担保密义务。

（二）商业密码管理之“关键环节”的特殊监管制度

1. 商用密码进出口管制

《密码法》对商用密码进出口管制制度带来了较大革新，具体可概括为两大方面。

• 进出口的密码类型管制革新

《商用密码管理条例》对商用密码产品进出口实施全面的管制，《密码法》第二十八条转变为对特定类型的商用密码实施进出口管制，具体详见下表：

商用密码类型	《密码法》的管制方法
涉及国家安全、社会公共利益且具有加密保护功能的商用密码	实施进口许可
涉及国家安全、社会公共利益或者中国承担国际义务的商用密码	实施出口管制
大众消费类产品所采用的商用密码	不实行进口许可和出口管制

目前，对既不属于“涉及国家安全、社会共同利益或中国承担国际义务”又不属于“大众消费类产品”的商用密码，《密码法》并未规定进出口管制一般规则，有待后续该法具体实施措施的补充以及实务观察。考虑到第二十八条要求执法部门后续公布商用密码进口许可清单和出口管制清单，结合该法“放管服”的立法精神，我们初步判断未来《密码法》及其配套制度可能采取负面清单的进出口管制制度，即商用密码只要不属于进口许可清单和出口管制清单，即不受进出口管制。

• 进出口的主体管制革新

在《密码法》出台前，只有外商投资企业、境外组织和个人可以在申请“密码产品和含有密码技术的设备进口许可”，并在获得许可后方可进口密码产品或含有密码技术的设备以供自用；其他境内主体均不得使用或进口境外生产的密码产品。

值得注意的是，《密码法》第二十八条不再区分外商与内资主体的商用密码进出口管制义务，仅从商用密码的类型上规定进出口管制。未来是否取消商用密码的进出口管制对外商与内资的主体区分，仍有待具体实施措施的出台以及后续实务观察。

2. 关键信息基础设施运营者的安全评估制度和安全审查制度

《密码法》并未对一般的网络运营者采购与使用商用密码做出一般性规定，但对属于关键信息基础设施的运营者提出了特殊要求，体现了“放”与“管”的监管平衡。

• 安全评估制度

《密码法》第二十七条规定，**关键信息基础设施运营者依据相关规定应当使用商用密码进行保护的，必须自行或者委托商用密码检测机构开展商用密码应用安全性评估。**

特别需要指出的是，该条与以国家标准《GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求》为标志的网络安全等级保护制度（以下简称“**等保2.0**”）相衔接，其中根据等保2.0相关国家标准（含征求意见稿）的建议，关键信息基础设施的安全保护等级原则上不应低于三级，应采用密码技术进行加密[11]。**因此，在等保2.0制度下，关键信息基础设施运营者原则上均需按《密码法》开展商用密码应用安全性评估。**

[10] 根据《外商投资法》第二十二条规定，国家保护外国投资者和外商投资企业的知识产权，保护知识产权权利人和相关权利人的合法权益；对知识产权侵权行为，严格依法追究法律责任。国家鼓励在外商投资过程中基于自愿原则和商业规则开展技术合作。技术合作的条件由投资各方遵循公平原则平等协商确定。行政机关及其工作人员不得利用行政手段强制转让技术。

[11] 参考《信息安全技术 网络安全等级保护定级指南（征求意见稿）》第6.5条以及《GB/T 22239-2019信息安全技术 网络安全等级保护基本要求》第8.1条。

• 安全审查制度

《密码法》第二十七条还规定，关键信息基础设施运营者采购涉及商用密码的网络产品和服务，**可能影响国家安全的**，应当按照相关法律法规要求，**由有关部门开展网络安全审查**。

根据今年5月发布的《网络安全审查办法（征求意见稿）》的规定，运营者采购网络产品和服务时，应预判产品和服务上线运行后带来的潜在安全风险，形成安全风险报告。**可能导致以下情况的，应当向网络安全审查办公室申报网络安全审查：（一）关键信息基础设施整体停止运转或主要功能不能正常运行；（二）大量个人信息和重要数据泄露、丢失、毁损或出境；（三）关键信息基础设施运行维护、技术支持、升级更新换代面临供应链安全威胁；（四）其他严重危害关键信息基础设施安全的风险隐患。**关键信息基础设施的运营者应时刻关注《网络安全审查办法》的立法动态，以确保其随时满足安全审查的合规要求。

3. 商用密码检测与认证制度

《管理条例》第九条规定，商用密码产品,必须经国家密码管理机构指定的产品质量检测机构检测合格。《密码法》尽管明确了商用密码检测与认证制度，**但商用密码产品由全部强制检测制度调整为自愿检测认证和强制检测认证相结合的管理制度**。

《密码法》第二十五条规定商用密码从业单位原则上自**愿接受检测与认证**。但第二十六条与《网安法》下网络关键设备和网络安全专用产品相关制度相衔接，规定了两种**强制接受检测与认证的例外**：（1）涉及国家安全、国计民生、社会公共利益的商用密码产品应列入《网络关键设备和网络安全专用产品目录》进行检测、认证；以及（2）使用网络关键设备和网络安全专用产品的商用密码服务应进行认证。

《网安法》生效以来，《网络关键设备和网络安全专用产品目录（第一批）》以及《承担网络关键设备和网络安全专用产品安全认证和安全检测任务机构名录（第一批）》都已经陆续公布，并会适时更新后续批次。

（三） 强化事中事后监管

事前审批的简政放权为商用密码从业企业带来重大利好，但这并不意味着从业企业的合规要求必然减少。《密码法》第三十一条规定，“密码管理部门和有关部门建立日常监管和随机抽查相结合的商用密码事中事后监管制度，建立统一的商用密码监督管理信息平台，推进事中事后监管与社会信用体系相衔接，强化商用密码从业单位自律和社会监督”。

虽然《密码法》仅提出事中事后监管制度的原则性规定，具体监管措施应如何落地仍有待实施细则的补充，但从业企业可以从已发布的《国密通知》中一窥事中事后监管的大体框架。国家密码管理局在《国密通知》中，就取消一批商用密码相关行政许可事项后如何加强事中事后监管的问题提出了具体措施，大致可以概括为以下几点：

- 全面落实“随机抽取检查对象，随机选派执法检查人员，执法结果及时向社会公开”的“双随机，一公开”制度，加大对商用密码产品的随机抽查力度，及时向社会公开抽查情况与结果；
- 充分发挥行业组织自律作用，积极鼓励从业企业加入行业协会并接受其监督；
- 建立信用体系，及时公示行政审批结果和监督检查情况，并将失信企业纳入“黑名单”重点监控，并将从业企业信用信息推送至国家企业信用信息公示系统；
- 健全投诉举报制度，及时处理社会和群众的投诉举报；
- 依法公开查处违法违规行为的处理情况、处罚依据及处罚结果。

综上可见，《密码法》生效后将采取事中事后强监管的思路，并且与国家社会信用体系与信用监管挂钩，对企业提出了更高的合规要求。密码从业企业应高度重视日常合规工作，随时应对应有关部门的执法监督，特别是随机抽查。

四、《密码法》的前沿阵地：区块链产业适用问题

虽然《密码法》的立法和落地并非剑指区块链产业，但因加密技术是区块链的技术根基，《密码法》毫无疑问将成为区块链法律规制体系的关键组成部分。就《密码法》在区块链产业的适用问题，我们做出以下几点观察：

- 适用范围：根据区块链产品所承载信息的不同，区块链提供商很可能被视为商用密码从业单位或核心、普通密码工作机构，承担《密码法》下对应法律义务。另一方面，区块链技术的政务应用日益广泛，利用区块链技术赋能政务数据管理已纳入中央议程[12]，更有河北雄安新区全国首家工程区块链资金管理平台的前沿实践，可见须以核心密码、普通密码保护国家秘密信息的区块链应用将日益普及。
- 商用密码检测认证：对供应使用商用密码的区块链服务（商用密码服务），企业需特别关注其产品所用的商用密码是否属于前述《网络关键设备和网络安全专用产品目录》所列的密码产品，如果属于，应当经商用密码认证机构对该商用密码服务认证合格。
- 关键信息基础设施：区块链的常见应用领域包括金融、医疗、大数据等，这些领域属于《关键信息基础设施安全保护条例（征求意见稿）》第十八条所列举的范围，不排除此类区块链产品将被纳入关键信息基础设施保护范围。如果区块链企业的网络构成关键信息基础，该区块链企业应

[12] http://www.xinhuanet.com/2019-10/30/c_1125172738.htm

当根据法律要求对区块链产品中的商用密码应用开展安全性评估。

- 进出口管制：区块链技术的去中心化、不可篡改和不可伪造的特性，使得其常应用于跨境交易和跨境物流。当前《密码法》尚未出台配套的实施细则，难以界定境内区块链产品向境外主体提供服务以及在境内使用境外区块链产品是否分别属于《密码法》所规制的“出口”与“进口”。我们建议，供应或使用区块链产品的企业若涉及跨境业务，均应密切关注《密码法》实施细则的立法动态，以及国家密码管理局等主管部门发布的在进口许可清单、出口管制清单等相关规章制度文件。

五、《密码法》下企业的合规路径

在《密码法》下，不同性质的企业所需承担的责任义务存在明显的差异。

（一）对于商用密码产品的生产和销售企业

相关企业应当：

- **关注最新的监管要求和《管理条例》及其配套规定的修订情况，尤其是对于《商用密码产品型号证书》等存续的商用密码行政许可和审批资质的管理要求。**
- **对企业生产和销售的商用密码产品的类型进行梳理。**如前所述，《密码法》对涉及国家安全、国计民生、社会公共利益的商用密码产品提出了强制检测认证的要求，对一般的商用密码产品则采用自愿检测的制度。在进出口方面，《密码法》仅对特定类型的商用密码实施进出口管制，对“大众消费类产品所采用的商用密码”不实行进口许可和出口管制制度。
- **对关键信息基础设施运营者客户进行识别。**如前所述，《密码法》对关键信息基础设施运营者采购商用密码产品提出了特殊的安全评估制度和安全审查制度，作为相关密码产品的供应商，企业同样需要配合关键信息基础设施运营者落实安全评估和安全审查责任。

（二）对于普通的网络运营者

依据《网安法》，网络运营者应当对其网络的网络运行安全和网络信息安全负责。普通的网络运营者（尤其是外商投资企业）在采购商用密码产品时，应当：

- **在网络产品和服务采购管理流程中，关注拟采购商用密码产品的类型及其检测认证的合规性**，若使用《网络关键设备和网络安全专用产品目录》所列商用密码服务，应要求密码提供者提供符合资质的机构所出具的检测、认证合格证书。
- **如果需要使用进口商用密码产品的，应当关注最新的监管要求，明确企业所使用的密码产品是否为大众消费类产品**，是否需要遵守进出口行政审批管制要求。如果需要，应当根据最新的监管要求，申请《密码产品和含有密码技术的设备进口许可证》。
- 此外，网络运营者需对国家秘密进行保护时，必须使用有资质的密码工作机构提供的核心密码或普通密码。

（三）对于关键信息基础设施运营者

如前所述，《密码法》对关键信息基础设施运营者提出了特殊的**安全评估制度和安全审查制度**。若企业构成关键信息基础设施的运营者，除关注上述普通网络运营者的合规要点以外，还应当：

- **确保采用商用密码保护其系统，并且根据法律法规要求开展商用密码应用的安全评估。**由于《密码法》第二十七条要求商用密码应用安全性评估应与关键信息基础设施安全检测评估和网络安全等级测评制度相衔接，而考虑到目前关键信息基础设施安全检查评估制度尚未实施落地[13]，运营者应特别关注该制度的相关立法与监管动态，以及后续《密码法》实施细则中就商用密码应用安全性评估如何与各制度衔接的具体规定。
- **若采购涉及商用密码的产品和服务的行为可能影响国家安全**，还需要参照《网络安全审查办法（征求意见稿）》和《网络产品和服务安全审查办法（试行）》申报网络安全审查。

结语

密码是国之重器，直接关系国家安全与经济稳定，具有重要战略资源地位。《密码法》以法律形式建立我国密码领域的监管框架，对我国大力发展密码产业与保障网络安全具有重大意义。《密码法》在立法技术上强调与现有《网络安全法》配套制度的衔接与呼应，在立法精神上追求监管与放权的平衡以及平等对待市场主体的原则，向密码从业企业及网络运营者释放了鼓励产业发展的积极信号，标志着我国在逐渐步入构建自洽的网络安全监管体系的立法成熟期。

（本文发布于2019年11月09日。）

[13] 目前，关键信息基础设施安全检测评估的政策、标准和实施方案仍在研究中。参考网信办新闻“专家建议：关键信息基础设施安全检查评估势在必行”：http://www.cac.gov.cn/2019-09/18/c_1570335108107742.htm

亡羊补牢未为迟：
如何应对网络安全勒索事件

导语

“见兔顾犬未为晚，亡羊补牢未为迟”，我们谨以此文，献给那些希望在下次风暴来临前扎紧篱笆的企业。

2019年5月26日凌晨，某网约车企业发布声明称其服务器遭到连续攻击，攻击导致该网约车企业的核心数据被加密、服务器宕机，为用户使用带来严重影响。攻击者向该网约车企业索要巨额比特币相要挟，该网约车企业在努力抢修的同时，已向北京网警中心就该网络安全勒索事件报案。

以上被勒索事件发生后，有报道称，该网约车企业的官方网站在勒索攻击发生20小时后仍无法打开，其APP也一度反复显示“暂时无法为您提供服务”“无法获取位置信息”。继而，舆论和公众开始对该网约车企业的诚信和未来发展状况产生了质疑。可以看到，因为未能对勒索攻击事件进行及时有效的响应，最终导致某网约车企业的安全保障能力和业务运营能力受到了社会和用户的全面质疑。

我们也注意到，近年来，网络安全事件特别是勒索事件频繁发生，这些网络安全事件往往性质恶劣、影响广泛，严重破坏企业的运营安全，更对企业的名誉和认可度造成不利影响；同时，用户也可能承受财产损失。由此，我们希望从网络安全和数据合规的角度出发，提示企业面对网络安全事件应当承担的法律义务，同时就企业应对网络安全事件所带来的法律风险给出具体建议。

一、企业应对网络安全事件应承担的法律义务汇总

网络安全事件，特别是勒索型网络安全事件往往对社会、企业和个人均造成不利影响。为妥善应对网络安全事件，保障国家安全和社会秩序，保障公民合法权益，我国发布了一系列法律法规，要求企业积极应对网络安全事件，承担相应法律义务。

我们总结了下述表格，简要介绍主要法律法规针对企业应对网络安全事件应承担的法律义务的相关要求：

表1：企业应对网络安全事件应承担的法律义务小结

时间阶段	法律义务	具体内容
事前	制定网络安全事件应急预案及相关安全管理制度	《中华人民共和国网络安全法》（2017年6月）（“**《网安法》**”）第25条：网络运营者**应当制定网络安全事件应急预案**，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险。 《中华人民共和国计算机信息系统安全保护条例》（2011年1月）（“**《计算机安保条例》**”）第13条：计算机信息系统的使用单位应当**建立健全安全管理制度**，负责本单位计算机信息系统的安全保护工作。 《信息安全技术网络安全等级保护基本要求》（“**《等保要求》**”）7.1.10.12安全事件处置 《信息安全技术个人信息安全规范》（“**《个人信息安全规范》**”）第9章安全事件的处置和报告规定个人信息控制者应**制定安全事件应急预案**。

时间阶段	法律义务	具体内容
事前	监测预警	《公共互联网网络安全突发事件应急预案》（2017年11月）（“**《工信部应急预案》**”）： 4.1事件监测：基础电信企业、域名机构、互联网企业应当**对本单位网络和系统的运行状况进行密切监测，一旦发生本预案规定的网络安全突发事件，应当立即通过电话等方式向部应急办和相关省（自治区、直辖市）通信管理局报告**，不得迟报、谎报、瞒报、漏报。报告突发事件信息时，应当说明事件发生时间、初步判定的影响范围和危害、已采取的应急处置措施和有关建议。 4.2预警监测：基础电信企业、域名机构、互联网企业、网络安全专业机构、网络安全企业应当**通过多种途径监测、收集漏洞、病毒、网络攻击最新动向等网络安全隐患和预警信息，对发生突发事件的可能性及其可能造成的影响进行分析评估；认为可能发生特别重大或重大突发事件的，应当立即向部应急办报告；认为可能发生较大或一般突发事件的，应当立即向相关省（自治区、直辖市）通信管理局报告。** 7.1预防保护：基础电信企业、域名机构、互联网企业应当根据有关法律法规和国家、行业标准的规定，**建立健全网络安全管理制度，采取网络安全防护技术措施，建设网络安全技术手段，定期进行网络安全检查和风险评估，及时消除隐患和风险。**电信主管部门依法开展网络安全监督检查，指导督促相关单位消除安全隐患。
	应急演练	《工信部应急预案》：7.2应急演练：电信主管部门应当组织开展公共互联网网络安全突发事件应急演练，提高相关单位网络安全突发事件应对能力。基础电信企业、大型互联网企业、域名机构要**积极参与电信主管部门组织的应急演练，并应每年组织开展一次本单位网络安全应急演练，应急演练情况要向电信主管部门报告。** 《个人信息安全规范》第9章安全事件的处置和报告规定个人信息控制者应进行**应急响应培训**等法律义务。
	宣传培训	《工信部应急预案》：7.3宣传培训：电信主管部门、网络安全专业机构组织开展网络安全应急相关法律法规、应急预案和基本知识的宣传教育和培训，提高相关企业和社会公众的网络安全意识和防护、应急能力。基础电信企业、域名机构、互联网企业要**面向本单位员工加强网络安全应急宣传教育和培训**。鼓励开展各种形式的网络安全竞赛。
事中	调查评估， 采取必要措施	《网安法》第55条：发生网络安全事件，应当立即启动网络安全事件应急预案，对网络安全事件进行**调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大**，并及时向社会发布与公众有关的警示信息。 《工信部应急预案》5.2先行处置：公共互联网网络安全突发事件发生后，事发单位应当立即启动本单位应急预案，**组织本单位应急队伍和工作人员采取应急处置措施，尽最大努力恢复网络和系统运行，尽可能减少对用户和社会的影响，同时注意保存网络攻击、网络入侵或网络病毒的证据。** 《等保要求》7.1.10.12安全事件处置：应在安全事件报告和响应处理过程中，**分析和鉴定事件产生的原因，收集证据、记录处理过程**，总结经验教训。
	报告主管机关	《应急预案》4.1事件报告：网络安全事件发生后，**事发单位应立即启动应急预案，实施处置并及时报送信息。** 《工信部应急预案》5.2先行处置：公共互联网网络安全突发事件发生后，**事发单位应按照本预案规定立即向电信主管部门报告。** 《计算机安保条例》第14条：对计算机信息系统中发生的案件，有关使用单位应当在**24小时内向当地县级以上人民政府公安机关报告。** 《等保要求》7.1.10.12安全事件处置：**应及时向安全管理部门报告所发现的安全弱点和可疑事件。应在安全事件报告和响应处理过程中，分析和鉴定事件产生的原因，收集证据、记录处理过程，总结经验教训。**
	通知用户/相关 个人信息主体	《个人信息安全规范》第9章要求个人信息控制者将安全事件相关情况**告知受影响的个人信息主体。**
事后	整改（如需）	《网安法》第56条省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。**网络运营者应当按照要求采取措施，进行整改，消除隐患。**
	调查原因、 总结经验	《工信部应急预案》6.1调查评估：公共互联网网络安全突发事件应急响应结束后，**事发单位要及时调查突发事件的起因（包括直接原因和间接原因）、经过、责任，评估突发事件造成的影响和损失，总结突发事件防范和应急处置工作的经验教训，提出处理意见和改进措施，在应急响应结束后10个工作日内形成总结报告，报电信主管部门。**电信主管部门汇总并研究后，在应急响应结束后20个工作日内形成报告，按程序上报。

二、企业应对网络安全事件的路线图

如上表所述，《网安法》《应急预案》《工信部应急预案》《计算机安保条例》《等保要求》《个人信息安全规范》等法律法规及国家标准中，均对企业应对网络安全事件时应承担的法律义务进行了规制；可以看到，这些法律要求实际上同气连枝、互补互足，形成了一套网络安全事件应对体系。针对这一体系，我们建议，企业结合自身实际，参照相关法律要求，设计符合自身特点和需要的应对网络安全事件路线图。

为协助企业更好地规划网络安全事件路线图，我们谨提出如下建议：

（一）居安思危，事前做好防备工作

如无远虑，则有近忧。面对频繁发生的以勒索事件为代表的网络安全事件，我们建议企业将目光放长远，居安逸时思困局，提前做好应对安全事件的防备工作。

1. 制度先行：制定网络安全事件应急预案及相关安全制度

结合《网安法》《应急预案》等法律法规的要求，我们建议企业在安全事件未发生时，提前做好预防准备工作，结合公司自身实际，制定针对网络安全事件的应急预案和相关安全制度。

我们理解，为确保网络安全事件应急预案能够发挥应有的效用，其内容至少应当包括：

- 组织体系和职责：结合企业组织架构和部门职能，预案应当明确承担网络安全事件监测预警、应急处理、事后处置等责任的部门和人员，同时也建议在应急预案中明确人力资源部门、公关部门、法务部门等企业支持部门的配合义务；
- 安全事件分级：《应急预案》和《工信部应急预案》等规制了网络安全事件的等级，建议公司参考自身业务内容，结合上述法律规定，对可能遭遇的安全事件分类、分级，从而针对不同类别、等级的安全事件采取不同的应对措施；
- 落实监测预警工作：建议企业建立适合自身实际的监测机制，采取合适的技术手段和工作方式，明确监测人员的职能并将责任落实到具体岗位；
- 建立应急响应机制：明确网络安全事件发生后，企业内部应急响应的流程和报告内容，以及向有关主管部门报告的流程、内容；
- 明确保障措施和奖惩制度：为确保网络安全事件应急预案能够落地实施，建议在预案中明确设备、技术资料、经费、人力支持等保障措施，同时明确奖惩制度。

2. 防患未然：预防预警和宣传培训

有效的预防预警工作能够尽可能规避、降低网络安全事件风险。我们建议公司结合自身业务实际，评估遭遇网络安全事件的可能性，结合相关法律法规，做好预防预警工作。

具体来说，我们仅提供如下建议供企业参考：

- 监测预警：在监测预警工作中，建议企业注意三项要点，即1）对过去几年行业内发生的影响较大的安全事件应当引起特别注意，并在监测机制中有针对性的监测相关要素；2）建议监测机制侧重企业内部核心资产或核心运营机制的安全；3）明确监测到事故发生后的处理流程；
- 宣传培训：为了能够在安全事件发生时及时、有效的应对，在日常运营中树立安全意识是必不可少的，建议企业通过宣传培训，指导相关人员落实预防预警相关工作；
- 舆情监控：知己知彼，百战不殆。根据我们处理安全事件的经营，一些大型安全事件往往呈国际性、区域性的发展态势，因此，建议企业在预防预警工作中关注相关网络安全讯息，例如国际性或区域性网络安全事件及其拓展趋势。

3. 未雨绸缪：安全事件的应急演练

“宜未雨而绸缪，毋临渴而掘井”，实操演练是检验安全事件防备工作是否到位的试金石。根据《工信部应急预案》等法律法规的要求，企业宜根据企业性质和自身实际需要进行针对网络安全事件的应急演练。就此，我们提出如下建议：

- 演练机制：难事作于易，大事作于细。为确保应急演练起到应有的效果，我们建议企业在演练机制中注意相关细节，即明确应急演练的参与人员、明确应急演练的针对对象、明确应急演练的方式；
- 协调机制：磨刀不误砍柴工，应急演练能够培养企业员工的安全意识，并训练员工高效、有序地应对安全事件，因

此，建议企业协调应急演练与企业正常业务运营间的关系，确保应急演练能够顺利实行；

- 演练总结：我们建议企业记录应急演练过程，并就演练中暴露出的问题进行总结，形成相应的报告。一方面，上述安排能够提高企业应急演练的效率；另一方面，企业也可以将之作为对外宣传自身安全理念，以及应对主管机关相应安全检查的实证材料。

（二）临危不乱，妥善应对安全事件

安全事件往往突如其来，严重影响企业正常运营，易造成企业内部和用户群体的恐慌。我们建议按照内部应急预案的规定，有条理、有计划地处理安全事件，从法律义务的角度看，我们提请企业在处理下述事项时加以注意：

1. 及时应对网络安全事件

我们建议企业充分重视网络安全事件，谨慎判断其严重程度和可能造成的不利影响。在评估不利影响时，我们建议企业评估既有影响的同时，评估不利影响进一步加深的可能。

我们谨为公司提供下述一般性评估因素：

- 安全事件已经或可能造成的财产损失；
- 安全事件是否影响企业用户使用产品或服务；
- 安全事件是否涉及数据泄露特别是个人信息泄露；
- 当前阶段是否存在能够有效解决安全事件的补救措施。

进行调查评估后，我们建议企业根据安全事件的性质和严重程度采取应急响应措施，包括但不限于：

- 启动应急预案：立即启动网络安全事件应急预案，尽最大努力先恢复网络和系统运行，尽可能减少对用户和社会的影响。
- 采取技术措施、保留证据：及时处理漏洞、采取补救措施，如判断安全漏洞，断开影响安全的网络设备，断开与安全漏洞相连的网络连接，跟踪并锁定攻击方向，进行数据备份等。在采取技术措施同时，注意保留网络攻击、网络入侵或网络病毒的证据。
- 及时向主管机关及个人信息主体（如需）报送安全事件相关信息（具体分析如下）。

2. 及时向主管机关报告

结合《网安法》《应急预案》等法律法规的要求，我们建议公司结合网络安全事件的性质和影响，及时向主管机关报告，报告内容包括但不限于：

- 事件可能造成的影响；
- 已采取或将要采取的处置措施；
- 个人信息主体的类型、数量、内容、性质等总体情况（如涉及）；
- 事件处置相关人员的联系方式

3. 告知受影响的用户

当网络安全事件发生时，结合《个人信息安全规范》，企业应视情况将安全事件相关信息及时告知受到影响的用户，告知方式包括但不限于邮件、信函、推送通知、短信、电话等。如果难以逐一告知用户，企业也可以采取合理、有效的方式发布与公众有关的警示信息。

我们理解，告知用户的内容可以包括：

- 网络安全事件的内容和影响；
- 已采取或将要采取的处置措施；
- 用户自主防范和降低风险的建议；
- 向用户提供的补救措施；
- 企业处理安全事件的联系人和联系方式。

（三）惩前毖后，吸取经验再出发

事不师古，往往就会重蹈覆辙。处理好网络安全事件后，及时的总结，进一步吸取经验教训，才能将企业锻造出铜墙铁壁，更好地应对未知的风险。

就此，我们对企业在安全事件处理完成后所应当做的工作提出下述建议：

- 调查事件原因并总结经验：及时调查安全事件的起因（包括直接原因和间接原因）、经过、责任，评估安全事件造成的不利影响和损失，总结突发事件防范和应急处置工作的经验教训，形成总结报告，提出处理意见和改进措施；
- 明确奖惩：如安全事件涉及企业内部人员违规操作，应当予以处罚；对安全事件处理过程中表现出色及不合格的工作人员，明确奖惩措施；
- 合理的对外沟通：塞翁失马，焉知非福。安全事件固然会对企业造成一定损失，但如果企业能够合理应对安全事件，对用户和社会展现其重信誉、负责任、有能力的企业形象，那么企业的声誉和知名度也可能不降反升。由此，我们建议企业以对用户、对社会负责任的态度应对安全事件，并在事件后通过合理的对外沟通，梳理企业负责任的社会形象。

以上，是我们根据协助企业应对网络安全事件的既有经验所规划的安全事件应对路线图。在网络安全问题日益突出的情况下，我们注意到，网络安全事件的类型呈多样化趋势，发生的频率日益升高，影响规模日益扩大。针对不同特点的网络安全事件，我们建议企业因时制宜、因地制宜，采用适合企业自身性质和业务特点的应对方案。如果遭遇突发情况，我们设有紧急情况应对通道（如下），将在第一时间协助企业制定应对方案，帮助企业渡过难关。

（本文发布于2019年06月01日。）

“一带一路”背景下中国企业境外并购的网络安全和数据合规问题

随着“一带一路”倡议的推进，据估计，未来5年中国对沿线国家和地区的投资预计将达到1,500亿美元。[1]可以预见，中国企业通过并购境外企业而“走出去”的需求将日益增多。在中国企业海外业务拓展的过程中，境内母公司和被并购的境外公司之间可能因为经营需要或者业务往来而需要进行大量的数据跨境传输，从而引发数据存储和数据传输的网络安全问题。

目前全球大部分国家都已经建立个人数据保护法规，根据澳大利亚著名隐私保护学者Graham Greenleaf的统计，早在2015年2月，全球制定了个人数据保护法规的国家和地区增加到109个。[2]考虑到个人数据保护立法的普遍性，“一带一路”背景下，中国企业的境外并购不免将受到当地政府部门有关网络安全和数据合规方面的审查，尤其是针对于2017年6月1日实施的《中华人民共和国网络安全法》（以下简称“《网安法》”）将对境外被并购企业收集的境外公民个人信息和重要数据安全保护的影响。

另一方面，《网安法》以及配套措施也对网络运营者包括关键信息基础设施运营者的网络建设、运营、维护和使用制定了一系列规则。这些规则可能对中国企业海外并购的目的和交易后的运营成本产生实质性影响。

基于以上，本文将重点分析：（1）《网安法》对于境外政府审查中国企业并购境外实体的影响；（2）《网安法》对于境外并购交易目的实现以及企业运营成本的影响。[3]

一、《网安法》对境外政府审查中国企业境外并购交易的影响

网络安全对于公民、法人和其他组织合法权益的保护具有重要影响，同时数据作为国家、企业具有价值资源的地位也被普遍认可。[4]数据在被越来越多国家认定为“战略资源”的当下，境外政府对于中国企业境外并购主要关注的网络安全和数据合规问题至少包括：

（1）《网安法》下，境外企业收集的境外公民个人信息数据是否被要求在中国境内存储；（2）《网安法》下，境外企业收集的境外公民个人信息数据是否可能被中国政府获得。

（一）有关境外公民个人信息数据的本地化存储问题

为了保护本国公民的合法权益，不少国家均要求网络运营者在本国境内运营中收集和产生的个人信息数据在境内存储，甚至对于成立地在本国以外的机构来说，只要其在提供产品或者服务的过程中处理了本国/本司法辖区个体的个人数据，将需适用本国/本司法辖区的网络安全和数据保护规则。例如，欧盟《一般数据

[1] 新浪财经，大手笔！中国对“一带一路”沿线国家和地区投资将达1500亿美元，发布于2017年05月15日，http://finance.sina.com.cn/roll/2017-05-15/doc-ifyfekhi7777894.shtml。

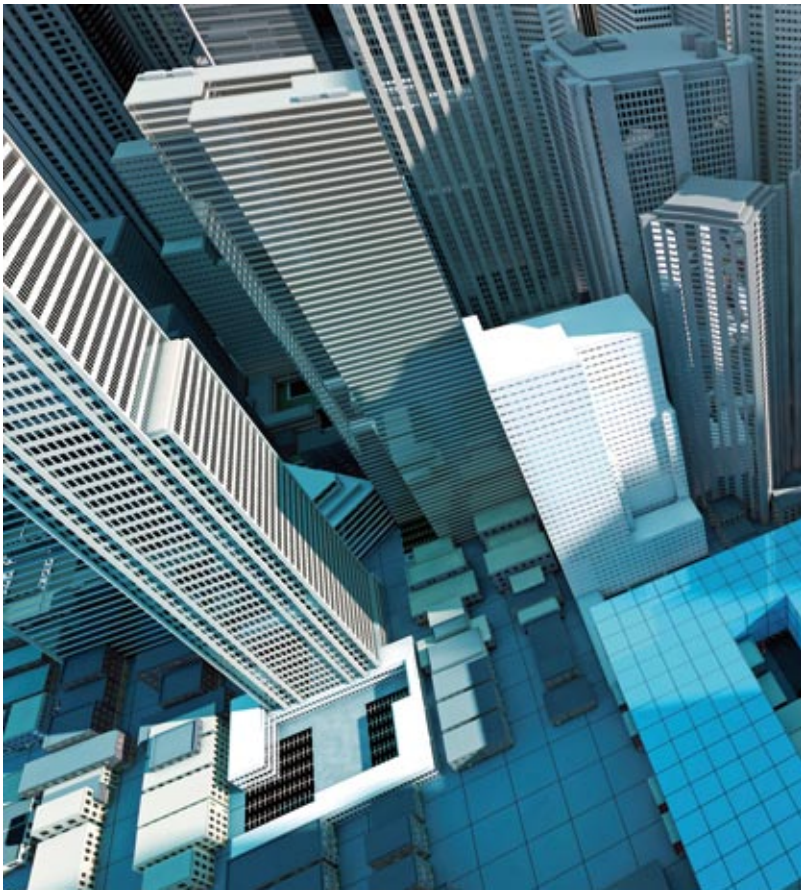
[2] Graham Greenleaf, Global Data Privacy Laws 2015: 109 Countries, with European Laws Now a Minority, (2015) 133, Privacy Laws & Business International Report, February 2015.

[3] 《中华人民共和国网络安全法》于2016年11月7日第十二届全国人民代表大会常务委员会第二十四次会议通过，自2017年6月1日起施行。

[4]有关数据对于企业的价值，请参见：经济学人，当数据成为新时代的石油，2017年5月6日。

保护条例》（General Data Protection Regulation，简称GDPR）最新规定，即使数据控制者在欧盟境内没有设立机构，但其在跨境提供商品或服务的过程中收集处理欧盟公民数据，则也应当适用欧盟数据保护法规。[5]

根据《网安法》第三十七条规定，我国要求关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。我国关于网络安全和数据保护的“属地原则”和以欧盟为代表的 “属人原则”可能存在冲突。依据GDPR的规定，交易后企业若在中国境内存储欧盟公民个人信息，则中国整体以及交易后企业对于数据安全的保护程度需达到足够保护的标准（adequate level of protection）。如果交易双方无法证明符合足够保护标准的要求，交易可能在其他司法辖区受到质疑。



（二）外国公民个人信息可能被中国政府获悉的风险

交易后，如果中国企业通过并购导致外国企业的控制权，境内并购方作为控制人，可以对境外公司的日常运营和战略决策产生决定性的影响，并要求境外企业将收集和产生的外国公民个人信息提供给境内并购方存储或者使用。其次，从运营结构而言，交易后境外被并购方的业务可能面临重组。境外公司收集的外国公民个人信息可能与境内并购方的网络或者关键信息基础设施对接。在上述背景下，国外司法辖区可能会关注，国家网信部门在对于中国境内网络运营者建设、运营、维护和使用网络的监督管理中，是否能获悉外国公民个人信息。

到目前为止，为了配合《网安法》的实施，国家互联网信息办公室（以下简称“**网信办**”）还发布了《个人信息和重要数据出境安全评估办法（征求意见稿）》（以下简称“**《安全评估办法（征求意见稿）》**”）和《网络产品和服务安全审查办法（试行）》（以下简称“**《审查办法》**”）。[6]在目前的《网安法》及配套措施下，可能被中国政府获悉外国公民个人信息情形至少包括以下四种：个人信息和重要数据跨境传输的安全评估、对关键信息基础设施的安全风险抽查和对关系国家安全的网络和信息系统采购的重要网络产品和服务进行的网络安全审查、以及为配合政府部门履行维护网络安全或者其他公职义务的协助和支持。[7]

1. 对网络运营者数据跨境的主管部门评估

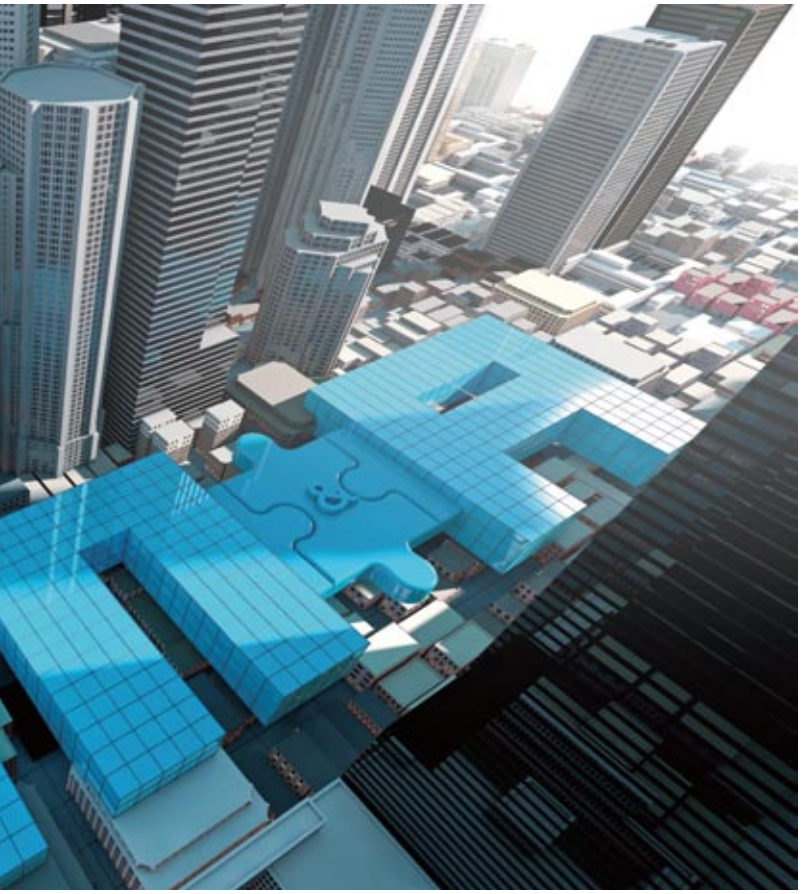
依据《网安法》第三十七条的规定，关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

《安全评估办法（征求意见稿）》进一步将以上《网安法》第三十七条的规制主体从关键信息基础设施的运营者扩大到了网络运营者，甚至要求其他个人和组织参照适用。对于达到《安全评估办法（征求意见稿）》第九条标准的出境数据，网络运营者应报请行业主管或监管部门组织安全评估（即主管部门评估）。在对数据出境的主管部门评估中，应重点评估的内容包括但不限于涉及个人信息和重要数据的情况，包括个人信息和重要数据的

[5] REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)，O.J.L119/1，第三条。

[6] 网信办分别于2017年4月11日发布了《数据跨境安全评估办法》（征求意见稿），2017年5月2日发布《审查办法》并将于2017年6月1日起实施。

[7] 主管部门评估是相对于自行评估而言。《数据跨境安全评估办法（征求意见稿）》第七条要求网络运营者应在数据出境前，自行组织对数据出境进行安全评估。当跨境数据达到一定标准时，网络运营者应报请行业主管或监管部门组织安全评估（即“主管部门评估”）。



数量、范围、类型、敏感程度等。由于《个人信息和重要数据出境安全评估指南》尚未出台，基于以上数据跨境主管部门评估的规定，不能排除被并购主体收集的外国公民或政府的个人信息和重要数据在跨境数据主管部门评估中被中国政府获悉的可能性。

2. 对关键信息基础设施的安全风险抽查

《网安法》第三十九条第一项规定，国家网信部门应当统筹协调有关部门对关键信息基础设施的安全风险进行抽查检测，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估。如果被收购的境外企业由于经营需要或者业务安排与境内网络经营者的系统对接，则可能会被认定为境内网络运营者关键信息基础设施的组成部分，则不能排除其收集的外国公民或政府的个人信息和重要数据在国家网信部门统筹的安全风险抽查中被中国政府获悉。

此外，由于目前关键信息基础设施的定义不明确，增加了对其进行安全风险抽查范围的不确定性。

首先，《网安法》对关键信息基础设施涉及的行业进行了非完全性的列举。

我国在2015年7月公布的《网络安全法（草案）》中，将涉及关键信息基础设施的行业进行了较为详尽的列举，包括：提供公共通信、广播电视传输等服务的基础信息网络，能源、交通、水利、金融等重要行业和供电、供水、供气、医疗卫生、社会保障等公共服务领域的重要信息系统，军事网络，设区的市级以上国家机关等政务网络，用户数量众多的网络服务提供者所有或管理的网络和系统。然而，目前正式颁布的《网安法》，则删除了所列举的关键信息基础设施范围，改为从遭到破坏、丧失功能或者数据泄露的严重后果为导向对关键信息基础设施进行了更为概括性的描述，即“国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。”[8]随后网信办2016年12月27日发布的《国家网络空间安全战略》中有关关键信息基础设施的定义与之类似，但行业列举范围有所扩大。[9]

有关关键信息基础设施的认定步骤，目前仅在网信办2016年6月向其地方执法机构下发的《国家网络安全检查操作指南》有所提及。根据该指南，关键信息基础设施的确定，通常包括三个步骤，一是确定关键业务，二是确定支撑关键业务的信息系统或工业控制系统，三是根据关键业务对信息系统或工业控制系统的依赖程度，以及信息系统发生网络安全事件后可能造成的损失认定关键信息基础设施。[10]同时，指南明确指出关键信息基础设施包括三类：（1）网站类，如党政机关网站、企事业单位网站、新闻网站等；（2）平台类，如即时通信、网上购物、网上支付、搜索引擎、电子邮件、论坛、地图、音视频等网络服务平台；（3）生产业务类，如办公和业务系统、工业控制系统、大型数据中心、云计算平台、电视转播系统等。但是，该指南的发布早于《网安法》的颁布，因此不可能成为《网安法》下的配套细则。另外，根据该指南自身所载说明，其依据是《关于开展关

[8]《网安法》，第三十一条。

[9]依据《国家网络空间安全战略》第四点第（三）项，国家关键信息基础设施是指关系国家安全、国计民生，一旦数据泄露、遭到破坏或者丧失功能可能严重危害国家安全、公共利益的信息设施，包括但不限于提供公共通信、广播电视传输等服务的基础信息网络，能源、金融、交通、教育、科研、水利、工业制造、医疗卫生、社会保障、公用事业等领域和国家机关的重要信息系统，重要互联网应用系统等。

[10]《关于开展关键信息基础设施网络安全检查的通知》，第3.2部分。

键信息基础设施网络安全检查的通知》（中办发2016 第3号），目的是指导关键信息基础设施网络安全检查工作。随着检查工作于2016年12月底结束，配合检查工作发布的指南是否依然有效有待网信办的进一步确认。目前尚不确定，预期正在制定的《关键信息基础设施识别指南》是否会参考《国家网络安全检查操作指南》中有关关键信息基础设施的范围界定和认定步骤的规定。

尽管《网安法》对于关键信息基础设施的范围有不完全列举，关键信息基础设施认定的步骤仍不明确，在《关键信息基础设施识别指南》尚未出台的情况下，识别关键信息基础设施仍有很大的不确定性。有学者认为，大部分行政管理部门受行政教条、“条块”管理的影响，实践中易将本部门所管辖重要行业确定为关键信息基础设施保护范围，[11]从而给关键信息技术设施的管理带来了不确定性。而国外实行关键信息基础设施保护的国家，如美国，则是通过行政法律文件明确保护范围与重点。从克林顿政府时期的八类关键基础设施，到小布什政府时期的十八类，以及奥巴马政府时期的十六类，美国关键基础设施都有明确的法定范畴。[12]

其次，目前《网安法》并未明确与关键信息基础设施的系统对接是否可能会被认定为关键信息基础设施的一部分。

由于《网安法》对于关键信息基础设施范围界定的不确定性，即使境外被并购方在交易后仍然保持独立运营，其与境内并购方的关键信息基础设施可能不可避免的基于运营管理或者业务需要而系统对接，因此不排除有被认定为关键信息基础设施组成部分的可能性。典型的情况是，境内收购方企业在交易后为境外被收购方提供云储存或者计算服务。如果境内收购方企业的云服务平台被认定为关键信息基础设施，将业务系统与云服务平台对接的被收购方的自身业务网络是否被认定为关键信息基础设施组成部分尚待明确。

除了业务平台的对接，实践中，境外被收购方的邮件系统或财务运营网络可能与境内收购方的关键信息基础设施实现对接，从而境外被收购方的邮件系统或财务运营网络是否会被认定为境内收购方的关键信息基础设施组成部分也有待明确。

3. 对重要网络产品和服务进行的网络安全审查

依据《审查办法》的第二条，关系国家安全的网络和信息系统采购的重要网络产品和服务，应当经过网络安全审查。在进行网络安全审查的过程中，将重点审查网络产品和服务的安全性、可控性，其中包括产品和服务提供者利用提供产品和服务的便利条件非法收集、存储、处理、使用用户相关信息的风险。[13]因此，不能排除境外企业收集的外国公民个人信息在传输至境内的过程中被收购主体使用的网络产品和服务提供者收集，并由网信办会同有关部门成立的网络安全审查委员会在组织实施对重要网络产品和服务进行的网络安全审查过程中获悉。

4. 配合政府部门履行网络安全或者其他公职义务的协助和支持

如上所述，境外被收购主体系统中收集的外国公民个人信息数据如果与境内收购方的网络、关键信息基础设施对接，可能依据《网安法》的规定受到一系列的监管。而网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。[14]由于具体监管实施细则尚未发布，不排除网络运营者在监督检查中被要求披露收集的个人信息和重要数据的可能。

此外，根据《网安法》第二十八条，网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。实践中不排除境外被收购主体收集的外国公民个人信息数据在上述活动中向政府披露。

综上所述，由于《网安法》和其他国家关于个人信息和数据保护规定的冲突，以及境外公民个人信息可能依据《网安法》被我国政府知悉，而在《网安法》尚未实施以及其实施细则尚未完全到位的情况下，海外并购可能会因为网络安全和数据保护的合规问题受到其他司法辖区的质疑。

二、《网安法》对于境外并购目的和交易后运营成本的影响

对于中国企业境外并购而言，其目的多为实现境外业务的整合和拓展。为了整合和拓展业务，境外被并购主体收集和产生的数据可能被传回境内总部进行处理和分析，并进一步传回境外被并购主体指导商业行为，因此数据的跨境传输可能成为中国企业“走出国门”后的常态。

然而，《网安法》以及《安全评估办法（征求意见稿）》对网络运营者的数据跨境提出了安全评估的前置条件，可能增加了中国企业境外并购后的经营成本，并且影响境外并购的目的。

第一，对于数据跨境需普遍征得个人信息主体同意的要求

依据《安全评估办法（征求意见稿）》第四条的规定，个人信息出境，应向个人信息主体说明数据出境的目的、范围、内容、接收方及接收方所在的国家或地区，并经其同意。然而，在实际的数据跨境过程中，具体的个人信息主体可能难以被识别且难以被复原。即使在此种情况下，数据出境也需获得相关个人主

[11] 顾伟，美国关键信息基础设施保护与中国等级保护制度的比较研究及启示，电子政务，2015年第7期（总第151期），第97页。

[12] 同上。

[13]《审查办法》，第四条第（三）项。

[14]《网安法》，第四十九条。

体同意，可能对数据跨境造成实质性的障碍。在之后的《数据出境安全评估办法》修改稿中，是否会列举数据跨境征得个人信息主体同意的例外情况值得我们关注。

第二，主管部门评估的适用标准和审查时限

《安全评估办法（征求意见稿）》设定的主管部门评估标准依然存在不确定性。除了以上所述《安全评估办法（征求意见稿）》对于本地数据存储和数据跨境传输规制主体的范围有所扩大，数据跨境主管部门评估的适用标准也可能存在门槛过低的问题。

一方面，依据《安全评估办法（征求意见稿）》要求，出境数据存在以下情况之一的，网络运营者应报请行业主管或监管部门组织安全评估：（一）含有或累计含有50万人以上的个人信息；（二）数据量超过1000GB。对于社交网络行业的数据跨境传输很容易满足第（一）项“含有或累计含有50万人以上的个人信息”的要求，而对于电影数码等行业的数据跨境传输很容易满足第（二）项“数据量超过1000GB”的要求[15]。因此，目前数据跨境主管部门评估的适用标准可能门槛过低，导致网络运营者需投入成本为日常运营的跨境传输申请主管部门评估。

另一方面，《安全评估办法（征求意见稿）》规定了主管部门评估的基本时限，要求行业主管或监管部门组织的安全评估，应当于六十个工作日内完成。由于评估过程中数据跨境传输是否需要停止并未明确规定，尤其是对于数据处理和传输有时效性要求的互联网企业，其日常业务运营可能因为最长可达六十天的主管部门评估而受到阻碍。

第三，每年至少进行一次安全评估和重新进行安全评估的安排

除了安全评估，网络运营者应根据业务发展和网络运营情况，每年对数据出境至少进行一次安全评估，及时将评估情况报行业主管或监管部门。安全评估的硬性要求将增加并购境外企业后的运营成本。

此外，当数据接收方出现变更，数据出境目的、范围、数量、类型等发生较大变化，数据接收方或出境数据发生重大安全事件时，应及时重新进行安全评估。[16]根据要求，未来并购境外企业后，数据传输可能需要采用数据归类，分类统筹，定点管理等方式来避免因为重新评估带来的合规、评估时间等方面的成本。

第四，禁止数据跨境的情形

《安全评估办法（征求意见稿）》规定，存在以下情况之一的，数据不得出境：（一）个人信息出境未经个人信息主体同意，或可能侵害个人利益；（二）数据出境给国家政治、经济、科技、国防等安全带来风险，可能影响国家安全、损害社会公共利益；（三）其他经国家网信部门、公安部门、安全部门等有关部门认定不能出境的。[17]

然而，从文本本身看来，这三类数据的认定标准仍较为宽泛。首先，就“个人信息”而言，在出境环节强调法定的知情同意原则确有必要，但现实中将难以准确判断何种数据出境行为具有或不具有“侵害个人利益”的可能；其次，以“可能影响国家安全、损害社会公共利益”为标准或在兜底条款中引入“有关部门”的自由裁量权，将会在一定程度上增加了判断标准的不确定性，同时也可能影响本条的可操作性，让网络运营者难以合理预期禁止数据跨境的情形。

综上所述，中国境内企业并购境外企业需要考虑到数据跨境传输的要求，评估其可能带来的关于合规、评估时间等方面的成本。此外，由于数据跨境传输的限制，中国境内企业还需要考虑交易后数据跨境的统筹安排。

三、企业合规建议

在《网安法》配套细则尚未完全出台的情况下，对于关键信息基础设施的范围认定等问题尚不确定，为了减少交易来自其他司法辖区审查机构的质疑，也为了准确评估海外并购目的和成本，中国企业一方面需要考虑采取有效措施，例如与被并购的境外企业之间建立防火墙等多种方式，打消其他司法辖区审查机构的疑虑，促使交易顺利进行；同时也需要考虑目前《网安法》的要求对于数据跨境传输等问题可能对交易目的和成本影响，对于企业内部数据流转、平台管理等方面进行提前准备。

《网安法》的配套实施细则包括诸多行业的技术标准会在6月1日前后发布。配套实施细则对于《网安法》的落地具有重要意义，企业需密切关注这些实施细则的发布，并主动与行业监管机构以及细则发布机构沟通，从而了解符合《网安法》规定的最佳行业操作指南。尤其对于可能被认定为关键信息基础设施的运营者，或者将被关键信息基础设施的运营者并购的企业，需关注相关法律法规及政策的发展，尤其是本文中提到的问题在之后的实施细则中是否已得到进一步解决或说明，从而确保交易后企业日常运营中的合规性。

（本文发布于2017年06月06日。）

[15] 据了解，数据量的要求有可能在最终办法中删除。

[16]《数据出境安全评估办法（征求意见稿）》，第十二条。

[17]《网安法》，第十一条。

热点解读：网信办连续颁布三项重磅新规

2017年5月2日，国家互联网信息办公室（“**网信办**”）在其官方网站上连续发布了《网络产品和服务安全审查办法（试行）》、《互联网新闻信息服务管理规定》以及《互联网信息内容管理行政执法程序规定》。

网信办在《网络安全法》（“**《网安法》**”）正式生效前[1]连续发布三项重要规定/办法，体现了国家从战略层面坚决维护国家安全与网络主权的决心和执行力。以上三项规定/办法从实体视角和程序视角分别针对网络产品和服务的安全审查、互联网新闻信息服务管理以及互联网内容信息管理等方面做出细致的规定。下文将对三项重要规定/办法做基本介绍，我们后续将提供更为详尽的解读。

一、《网络产品和服务安全审查办法（试行）》（“《审查办法》”）

根据《网安法》的规定，关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。[2]作为《审查办法》直接的上位法依据，《网安法》的出台就为关键信息基础设施的运营者施加了通过国家安全审查的义务。而《审查办法》更是在引入《国家安全法》（“《国安法》”）作为立法依据的基础上，将安全审查的适用对象拓宽至“关系国家安全的网络和信息系统采购的重要网络信息产品和服务”。

事实上，早在2017年2月4日，网信办就已针对《审查办法》向社会公开征求意见。[3]无论是在征求意见稿阶段还是目前的试行稿阶段，《审查办法》均坚持以第三方评价与政府监管相结合作为审查的基本原则，注重审查网络产品和服务的安全性与可控性。此外，在具体实施层面，根据不同的行业与领域，《审查办法》还要求国家网信主管部门、行业主管部门以及其他有关部门协调分工，负责推进针对不同网络产品和服务供应链（或提供者）的安全审查。值得注意的是，在试行办法中，《审查办法》还针对包括第三方评估机构在内违反相关规定的法律责任进行了概要规定。[4]

二、《互联网新闻信息服务管理规定》（“《管理规定》”）

国务院早在2000年已经制定并颁行了《互联网信息服务管理办法》（2011年修订），并于2005年由国务院新闻办公室专门针对互联网新闻信息服务出台了《互联网新闻信息服务管理规定》。而此次，由网信办负责出台的《管理规定》实质上是对2005年国务院新闻办公室颁行版本的重大修订。

经过向社会公开征求意见[5]以及国家网信办的调研与考察，

[1]《网络安全法》将于2017年6月1日正式生效。

[2]请见《网安法》第三十五条。

[3]“国家互联网信息办公室关于《网络产品和服务安全审查办法（征求意见稿）》公开征求意见的通知”，请见http://www.cac.gov.cn/2017-02/04/c_1120407082.htm。

[4]请见《审查办法》第十四条和第十五条。

[5]“国家互联网信息办公室关于《互联网新闻信息服务管理规定（修订征求意见稿）》公开征求意见的通知”，http://www.cac.gov.cn/2016-01/13/c_1117757912.htm。

《管理规定》的颁行稿主要从准入许可与运行管理等两大方面入手，对互联网新闻信息服务的经营活动进行具体的监管。就准入而言，《管理规定》在其条款中列举了申请许可的条件，[6]并明确了严格限制外资涉足互联网新闻信息服务事业的管理原则。[7]此外，《管理规定》还从人员配备、安管义务以及信息审核备案等方面，对互联网新闻信息服务提供者的经营行为进行具体规范，在各环节切实推进实名制与责任制。此外，《管理规定》还针对违反规定的行为设定了相应的法律责任，以确保互联网新闻信息服务提供者的各项义务得以落实。

三、《互联网信息内容管理行政执法程序规定》（“《程序规定》”）

随着互联网时代的迅猛发展，管理与规范互联网上的信息内容已成为维护网络安全运营的必然要求。然而，监管的有效落实并不仅仅依赖于全面的实体规范，还需要清楚明确的程序规范予以辅助执法。因而除了在实体层面推进《网安法》的全面实施，此次网信办公布的《程序规定》则针对互联网信息内容管理部门的行政执法提出了专门的、具体的规定。我们理解，随着《程序规定》的出台，网信主管部门的执法行为将在实体与程序两个维度实现有法可依、有章可循，一方面能为企业进行自身合规建设或是面临网信执法时提供必要的指引，另一方面更是敦促有关部门依法履职，积极加强网信执法，切实维护国家的网络安全与社会各界的网络权益。

事实上，国家网信办在2016年1月12日就针对《程序规定》的内容向社会各界公开征求意见。[8]经过一年多的调研，《程序规定》最终定稿出台。具体而言，《程序规定》要求各管理部门应当建立行政执法督查制度，由上级部门对下级部门的执法行为进行督查。[9]此外，《程序规定》还要求执法人员应当参加相关培训，经考试或考核后持证上岗，务求在执法队伍建设层面提升执法的规范性。[10]而就具体的执法程序要求而言，《审查办法》从管辖、立案、调查取证、听证与约谈、处罚决定与送达、执行与结案等六大板块，较为全面地规范了国家与地方网信部门的执法行为，为在《网安法》的指导下有效推进互联网信息内容的管理奠定了坚实的程序基础。

（本文发布于2017年07月12日。）

[6] 请见《管理规定》第六条。

[7] 请见《管理规定》第七条。

[8] “国家互联网信息办公室关于《互联网信息内容管理行政执法程序规定（征求意见稿）》公开征求意见的通知”，请见http://www.gov.cn/xinwen/2016-01/12/content_5032320.htm。

[9] 请见《程序规定》第四条。

[10] 请见《程序规定》第五条。

金杜网络安全、数据合规及治理团队简介

金杜网络安全、数据合规及治理团队包括多名合伙人，团队成员均毕业于国内外著名法学院校，拥有硕士以上学历，具备跨学科背景及互联网专业人才，能够多角度多层面为每位客户独特的项目需求提供相应的法律服务。团队所有成员均精通中英文，可以用双语为国内外客户提供便捷、专业的法律服务。团队全体成员将以热情饱满的工作态度、积极进取的工作方式，以中国的实践为基础，以客户需求为导向，为客户提供优质全面的法律咨询和项目服务。

金杜网络安全、数据合规及治理团队也包括金杜海外办公室（即英国/欧洲、美国/日本/中东、澳大利亚办公室）的多名合伙人。金杜海外办公室在数据和隐私保护、网络安全领域拥有丰富的业务经验，提供合规制度设计、隐私声明起草、数据泄露事件应对、数据合规监管机构关系管理等全方位的数据合规法律服务。金杜海外办公室将技术专长和经验深度相结合，与金杜中国境内网络安全与数据团队其他成员一起，为客户提供多司法辖区数据保护、隐私和网络安全等领域的良好建议。

截至目前，金杜网络安全、数据合规及治理团队已经完成近百项境内外网络安全与数据合规的尽调项目或咨询，涉及的行业领域包括但不限于金融、保险、互联网、能源、航空、医疗、智能汽车、智能手机等。服务类型包括依据GDPR或者中国网络安全法的要求进行企业内部数据合规评估及完善、协助客户制定跨境数据传输计划、出具数据处理评估报告、协助客户制定数据商业化合规方案等。

金杜网络安全、数据合规及治理团队积极参与网络安全、数据保护领域的立法、标准制定及研讨活动，对人工智能、区块链等新兴技术的应用和监管有特别关注，是全国信息技术标准化技术委员会大数据标准工作组和全国信息安全标准化技术委员会WG7信息安全管理工作组的成员，以及国家人工智能标准化总体组的通讯成员。

金杜网络安全、数据合规及治理团队在2020、2019年获得《商法》颁发的隐私及数据保护领域卓越律所大奖、LEGALBAND评选的2020、2019年网络安全与数据保护第一梯队律所。团队内宁宣凤律师是2020年、2019年LEGALBAND评选的中国网络安全与数据保护领域BAND 1执业律师，吴涵律师是2018年《环球数据评论》评选的全球“40-under-40 Data Lawyer”中唯一一位来自中国律师事务所的律师。

金杜网络安全与数据团队提供的法律服务主要包括：（1）中国《网络安全法》下网络运行、等级保护、个人信息合规评估（含跨境数据传输分析）及企业合规体系完善；（2）企业数据体系治理；（3）GDPR及其他海外司法辖区数据合规；（4）企业网络信息合规管理体系的建立；（5）内部员工培训；（6）应对网络安全检查；（7）网络安全事件响应规划；（8）云服务的电信监管和网络安全合规；（9）区块链、人工智能、物联网等前沿领域法律咨询。

宁宣凤 | 高级合伙人
合规业务部 | 北京办公室
电话：+86 10 5878 5010
电邮：susan.ning@cn.kwm.com

执业领域

宁宣凤律师是中国最早涉足网络安全与数据合规法律实务的律师之一，拥有一支具备跨学科背景的专业律师团队，其执业方向主要包括：协助客户梳理企业数据（包括个人信息保护）合规体系；协助客户制定修改隐私政策、合规计划；协助客户制定跨境数据传输计划；协助客户制定数据商业化合规方案；协助客户进行网络安全和数据合规自查；协助客户进行内部网络安全和数据合规培训；协助客户应对网络安全检查；协助客户应对网络安全突发事件；协助企业进行云服务的电信监管和网络安全合规；为客户就诉讼、仲裁中证据出境提供审查、咨询服务；有关区块链、人工智能、物联网等前沿领域数据合规咨询等。

宁宣凤律师擅长协助企业建立和完善满足中国、欧盟（GDPR）及美国等多司法辖区要求的网络安全和数据合规体系，为企业数据全球化流动和商业化开发保驾护航。企业所涉行业包括金融、IT、通信、移动支付、智能网联汽车、传媒、能源、航空、化工和制造等多个领域。

为了把握大数据立法的最新动态和监管趋势，宁宣凤律师所在的金杜网络安全与数据合规小组还加入了全国信息安全标准化技术委员会下的信息安全管理标准工作组、全国信息技术标准化技术委员会下的大数据标准工作组以及国家人工智能标准化总体组，积极参与大数据产业标准的制定。

工作经历及教育背景

宁宣凤律师毕业于北京大学，获法学学士学位；后就读于加拿大McGill大学，获法学硕士学位。宁宣凤律师于1988年获得律师资格。

宁宣凤律师于1995年加入金杜律师事务所，现为金杜合伙人，并担任合规业务部负责人。宁律师目前主要的执业领域包括网络安全与数据合规以及反垄断与反不正当竞争。此外，宁律师此前也曾从事国际贸易与投资业务。

吴涵 | 合伙人
合规业务部 | 北京办公室
电话：+86 10 5878 5749
电邮：wuhan@cn.kwm.com

执业领域

吴涵律师的主要执业领域为网络安全和数据合规，反垄断和反不正当竞争法。

吴涵律师在网络安全和数据合规领域的业务内容主要包括：协助客户制定修改隐私政策、合规计划；协助客户制定跨境数据传输计划；协助客户制定数据商业化合规方案；协助客户梳理企业数据（包括个人信息保护）合规体系；协助客户进行网络安全和数据合规自查；协助客户进行欧盟GDPR数据合规评估；协助客户基于上市或交易所需进行数据合规尽职调查；协助客户进行内部网络安全和数据合规培训；协助客户应对网络安全检查；协助客户应对网络安全突发事件。

吴涵律师曾协助多个行业的领先企业就网络安全和数据合规提供法律服务，其处理过的项目涉及金融与保险、支付清算、航空、网约车平台、消费电子、互联网广告、日化、医疗等行业。

吴涵律师是2018年《环球数据评论》评选的“40-under-40 数据领域执业律师”中，唯一来自中国律师事务所的律师。

工作经历及教育背景

吴涵律师是金杜律师事务所合规业务部的合伙人。吴涵律师于2011年加入金杜，在此之前曾先后在北京内资律师事务所和外企工作。吴涵律师曾于2015年在金杜律师事务所伦敦分所任职。

吴涵律师在武汉大学获得地理信息系统（Geographic Information System, GIS）专业工学学士，在北京大学获得中国法硕士学位以及美国法法律博士（Juris Doctor）学位。

吴涵律师具有中国律师职业资格证，其工作语言为英文和中文。

蒋科 | 合伙人
合规业务部 | 北京办公室
电话：+86 10 5878 5112
电邮：jiangke@cn.kwm.com

执业领域

蒋科律师的主要执业领域为科技和电信领域合规、网络安全和数据合规。

※ 科技和电信领域合规

在科技和电信领域合规方面，蒋科律师在过去十余年的执业经历中为各类科技和互联网公司提供了广泛领域内的合规咨询意见，并曾以法务身份为亚马逊云服务在中国市场的运营和产品合规提供法律支持。蒋科律师在此领域处理过的合规问题涵盖数字媒体内容、云服务和其他增值电信服务的市场准入、落地运营和销售，也涵盖硬件产品从生产、进出口、销售、售后到召回和销毁的全生命周期，以及相关的广告营销和消费者保护。相关产品和服务涉及手机和其他智能设备、个人可穿戴设备、商用密码和两用产品以及移动应用、在线图书、音乐、电影和游戏等数字化服务。

※ 网络安全和数据合规

在网络安全和数据合规方面，蒋科律师擅长为跨国企业在中国的分支机构提供网络安全与数据合规意见，并曾在宝马中国担任数字化项目和网络安全合规的主要法务。蒋科律师在此方面为客户提供的服务内容主要包括：协助起草、审阅隐私政策及相关合规计划；评估企业个人信息保护合规体系和各项制度；梳理各种业务场景下的数据跨境传输并协助制定传输合规计划；协助制定和评估数据商业化利用的合规方案；协助进行网络安全和数据合规自查、相关合规培训；协助应对网络安全检查和网络安全突发事件等。

工作经历及教育背景

蒋科律师于2007年首次加入金杜律师事务所，并于2014至2017年担任合伙人。2020年，蒋科律师重新加入金杜律师事务所。2017至2020年再次加入金杜之前，蒋科律师曾分别在宝马中国和亚马逊云服务运营商西云数据从事法务工作。

蒋科律师分别毕业于对外经济贸易大学和美国斯坦福大学法学院，获法学学士和法学硕士学位。

金杜律师事务所被广泛认为是全球最具创新力的律所之一，能够提供与众不同的商业化思维和客户体验。金杜拥有2700多名律师，分布于全球28个城市，借助统一的全球平台，协助客户了解当地的挑战，应对地域性复杂形势，提供具有竞争优势的商业解决方案。

作为总部位于亚洲的国际领先律师事务所，我们为客户发掘和开启机遇，协助客户在亚洲市场释放全部潜能。凭借卓越的专业知识和在核心市场的广泛网络，我们致力于让亚洲走向世界，让世界联通亚洲。

我们始终以伙伴的合作模式为客户提供服务，不止步于满足客户所需，更关注实现客户目标的方式。我们不断突破已取得的成就，在重塑法律市场的同时，打造超越客户预期的律师事务所。

金杜法律研究院是由金杜律师事务所和金杜公益基金会联合发起成立的非营利性研究机构。自设立以来，一直致力于打造具有国际影响力的中国特色新型智库，依托于金杜律师事务所过往二十多年来服务国家经济建设和法治建设过程中所积累的丰富执业经验和专业洞见，对企业“走出去”战略中面临的重要问题进行分析研究，以提供具有建设性和实操性的政策建议和咨询意见。

金杜研究院
KWM_China