FANGDA PARTNERS
方達律師事務所

中国年度企业合规蓝皮书

2018-2019

发布方

中国公司法务研究院

中国国际贸易促进委员会商事法律服务中心

方达律师事务所

主笔

方达合规团队

编辑委员会

主任

蔡晨风　中国贸促会商事法律服务中心主任
　　中国贸促会全国企业合规委员会秘书长

辛　红　中国公司法务研究院秘书长

张　顺　中国贸促会商事法律服务中心副主任
　　中国贸促会全国企业合规委员会副秘书长

尹云霞　方达律师事务所合伙人

中国公司法务研究院编辑团队

乔　楠　中国公司法务研究院秘书长助理

荣　悦　中国公司法务研究院外联部主任

中国国际贸易促进委员会编辑团队

张智超　中国贸促会商事法律服务中心业务合作处处长

韩　瑞　中国贸促会商事法律服务中心业务合作处干部

王岱凌　中国贸促会商事法律服务中心业务合作处干部

主笔

方达合规团队

尹云霞	马　锋	庄燕君	杨建媛	赵何璇
张　毅	康英杰	龙明珠	王凯琳	周梦媛
李晓霞	刘　超	张　芳	章娅玮	张文豪
郭庆营	黄燕妮	牛　玥	王嘉华	刘书婷

※ 中国公司法务研究院

中国公司法务研究院是法制日报社设立的、以公司法务研究为核心的平台。法制日报社主办的《法制日报》是中央政法委机关报，是党和国家在民主法治建设领域的重要舆论阵地，是党在政法战线的主要喉舌，是18家中央媒体之一，也是中国目前惟一一家向国内外公开发行的中央级法制类综合性日报。法制日报社下设法治号、法制网、法人杂志等多个子报子刊、网站与客户端等新媒体平台。

中国公司法务研究院旨在搭建中国公司法务界最具影响力的信息交流、服务咨询平台，通过内容产出和系列活动的开展，提升公司法务在企业内部的战略地位，推动公司法务职业群体的成长成熟。同时，充分发挥媒体平台作用，促进企业的稳健发展。

中国公司法务研究院旗下拥有中国公司法务年会、中国公司法务30人论坛、走进企业等多个品牌活动，独家或联合其他机构连续发布了中国合规蓝皮书、中国企业走出去报告、中国企业家犯罪（媒体样本）报告等系列年度报告。

其中，中国公司法务年会是国内首家媒体打造的全国性法务高端交流平台，也是法制日报倾力打造8年的品牌活动。目前中国公司法务年会不仅在国内举办北京、上海、深圳、武汉等会场，同时联合其他机构与日本法务界建立了交替主办的年度沟通平台——中日企业法务论坛。

※ 中国贸促会全国企业合规委员会

中国贸促会全国企业合规委员会由中国贸促会商事法律服务中心、中国企业联合会与北京新世纪跨国公司研究所于2018年1月共同发起成立。合规委员会以国家企业合规政策为指导，联合国内外关注和支持企业合规的组织及个人，借鉴国际合规先进经验，以促进企业合规经营、优化营商环境、弘扬合规文化、推进企业合规职业化建设为己任，着眼于培育具有全球竞争力的世界一流企业，为企业合规经营提供全方位服务。

合规委员会是促进企业合规的工作机制，其组织机构包括：委员会主席、理事会、专家委员会和秘书处。委员会主席由中国贸促会会长担任，副主席、理事长、常务副理事长分别由发起单位相关领导担任。理事会是合规委员会的决策机构，秘书处是委员会的日常工作机构，专家委员会负责为委员会的发展与决策提供专业支持。委员会秘书处设在中国贸促会商事法律服务中心。

截至2019年10月，合规委员会已发展81家企业成员和1家团体成员（其成员单位904家），合计成员企业985家，成员涵盖国有企业、民营企业、外资企 业在内的世界五百强企业，其他多为行业龙头企业或上市公司。行业范围涵盖能源、制造、金融、交通运输、通讯、互联网等各产业及行业领域。

※ 方达律师事务所——全方位、专业的中国律师事务所

长期以来，方达一直作为大中华区为数不多的顶尖律师事务所之一享有盛名。方达创建于1993年，是首批向国内外客户提供全方位服务的中国律师事务所之一，在北京、香港、上海、深圳和广州设有办公室，拥有约700名律师。

方达的律师在监管合规、诉讼、仲裁、投资、资本市场、并购、融资、知识产权、隐私和数据保护以及税务领域拥有数十年从业经验，方达在多个行业也具备丰富经验，可以应对客户全面的业务需求，为客户提供全方位的优质服务，并擅长提供复杂法律问题的解决方案。

方达凭借近年来在中国法律服务市场的卓越表现荣膺行业各类奖项，充分证明了我们在处理相关领域重大法律事务方面的杰出专业技能。从2000年至今，我们的多个业务领域持续被各大法律评级机构和专业媒体，如《钱伯斯亚太》、《中国法律与实践》、《IFLR 1000》、《亚洲法律事务》、《PLC Which Lawyer》、《Dealmakers Monthly》、《ASIAN-MENA COUNSEL》等评为中国顶尖级别律师事务所。

※ 方达合规及政府执法团队——兼具丰富的本土知识与国际标准的专业合规团队

方达合规及政府执法团队具备丰富的本土和国际经验，团队成员拥有中国、美国、英国、香港等多地的律师执照，且很多律师在加入方达前在欧美等地积累了丰富的合规经验。同时，方达合规及政府执法团队在不断扩展，吸引了最优秀的人才，包括前检察官、前执法人员，在刑事调查及诉讼领域、行政审查及诉讼领域经验丰富的高级合伙人，以及知名的公司内部合规律师。

方达合规及政府执法团队一直为跨国公司和中国企业提供全方位的合规服务，业务范围覆盖刑事、民事、行政、劳动等完整法域，尤其在处理反腐败、反垄断或竞争法、网络安全与数据隐私保护、出口管制与制裁、国家秘密、证券监管、反洗钱、雇用和劳动、知识产权、健康和安全及环境法律等。方达合规及政府执法团队同时也为“走出去”的中国企业在全球提供全方位的监管合规服务。方达合规及政府执法团队尤其擅长的领域包括：内部调查、政府调查、定制化合规制度建设、刑事案件等，有卓越的专业知识和丰富的实践经验。

方达合规及政府执法团队同样荣获各大权威评级机构奖项，例如，2017年《钱伯斯亚太》首次评选了中国“公司调查/ 反腐败”业务领域的律师团队，当年以及此后的2018、2019年，方达皆荣列该领域下的第一等律所。《法律500强（亚太区）》于2017至2019年亦评选方达为监管/合规第一梯队律所。2019年，方达也被《中国法律与实践》评为“年度监管与合规律所”。

主笔介绍：

尹云霞

方达合规业务负责合伙人。中国合规方面的领军律师，连年被著名法律评级机构钱伯斯及Legal500评为“ 监管及合规”及“企业调查 / 反腐败”的顶级律师，被《中国法律与实践》评为2019年度最佳合规律师。有深厚的经验代表客户应对复杂的国内外执法、危机处理、内部调查、建立合规体系，如反腐败、反舞弊、数据合规、证券欺诈等。参与过诸多国际知名案件包括西门子FCPA monitorship、GSK 中国商业贿赂案件。尹律师有多年海外职业经验，为美国法学博士，入选白帽协会（美国杰出法律人士学会）。

马锋

方达合伙人。马律师的主要执业领域为知识产权、生命科学和争议解决。 马律师是中国和美国纽约、加州以及哥伦比亚特区的执业律师。马律师处理各类知识产权业务，就知识产权的申请和注册、许可和执行，以及技术转让提供优质服务。马律师也就涉及药品、生物制品、医疗器械、化妆品、特殊食品和其他消费品的监管和合规问题向客户提供法律服务。马律师曾在大型国际律师事务所工作多年，马律师服务过的客户包括跨国公司和中国企业。

庄燕君

方达合伙人。为世界五百强公司、在美国上市的中国顶级互联网公司等多家跨国企业长期提供内部调查、合规尽调、刑事咨询、刑事辩护等服务。被钱伯斯《2019亚太法律指南》评为公司调查/反腐败领域“受认可律师”，现任中律联企业合规研究院顾问。加入方达前，在北京某检察院工作15 年，历任公诉处主办检察官、反贪局主侦检察官，办理房地产、医疗等多个领域的商业贿赂案件上百件，办理普通刑事案件六百余件。

杨建媛

方达合伙人。杨律师的主要执业领域为数据保护、网络安全、监管合规，在涉及跨境法律问题与应对不同执法机构的复杂事务方面具有丰富的实务经验。杨律师持续协助客户建立全球和中国特色的数据保护项目、提供数据跨境的合规解决方案、开展数据商业化使用合规评估、第三方数据合规尽职调查、应对政府针对网络安全与数据保护的突击检查与执法，以及代表客户处理因合规事项引发的行政程序及争议解决事项。

赵何璇

方达合伙人。赵律师在跨国企业及中外律师事务所工作多年，在帮助中国及跨国企业建立、实施及完善合规制度，发现和应对企业合规风险方面积累了丰富的经验。赵律师曾帮助不同行业的跨国公司和本土企业处理各类合规法律事务，如提供法律意见、内部调查、应对政府执法、完善内部合规体系、各类投资及并购交易的合规尽职调查等，以及争端解决与刑事辩护等业务。赵律师执业的领域包括制裁与出口管制、反腐败及商业贿赂、反舞弊、网络安全与数据保护、广告法、国家秘密等。

目录

第一章 2018-2019全球重大合规事件评述 02

一、 2018-2019中国重大合规事件评述 03
1. 本轮机构改革及行政执法体制调整基本完成 04
2. 新《反不正当竞争法》下商业贿赂执法综述 06
3. 中国数据保护立法与执法趋势综述 11
4. 《企业境外经营合规管理指引》解读 16
5. 《中央企业合规管理指引（试行）》解读 20

二、 2018-2019境外重大合规事件评述 25
1. 境外反腐败执法综述 26
2. 境外数据保护执法综述 36
3. 美国经济制裁立法及执法综述 40
4. 世界银行制裁体系介绍及对中国企业的建议 45

第二章 问卷调研 56

第三章 企业应加强数据保护合规 86

1. 全球数据保护立法和执法的趋势、差异及中国企业的对策 87
2. 《个人信息安全规范》修订要点 91
3. 流量的突围：线下流量及新零售中的数据保护问题 95
4. 隐私诉讼在中国：向左走向右走 99
5. 境内外重大数据泄露案件及公司汇报要求解析 105

第四章 美国出口管制与经济制裁制度及对中国企业的影响 110

1. 美国经济制裁法律体系解读 111
2. 美国出口管制法律制度及中国企业风险防范 115
3. 中国科技企业如何避开美国出口管制陷阱 123
4. 美国对华为出口管制最新动态及中国企业如何应对 127

第五章 刑事合规热点分析及如何应对刑事调查 132

1. 2018-2019年度刑事合规热点概览 133
2. 刑事合规热点问题涉及的相关罪名解读 134
3. 企业如何应对刑事调查 161

第一章

2018-2019
全球重大合规事件评述

2018-2019
中国重大合规事件评述

一、本轮机构改革及行政执法体制调整基本完成

2018年3月21日，中共中央印发了《深化党和国家机构改革方案》（下称“《方案》”）。深化党和国家机构改革，是贯彻落实党的十九大决策部署的一个重要举措，是全面深化改革的一个重大动作，是推进国家治理体系和治理能力现代化的一次集中行动。

根据中央统一部署，本轮机构改革在2018年“两会”后全面推开，至2018年底，国家机关机构改革全部落实到位。2018年9月13日,《海南省机构改革方案》印发，成为首个获得中央批准的省级机构改革方案。此后，山东、福建、广东、湖南、云南、浙江、宁夏、北京、上海等省(区、市)机构改革方案陆续公布，均对机构改革作出全面部署。2019年7月，深化党和国家机构改革总结会议在北京召开，标志着经过一年多的时间，本轮机构改革的任务总体完成。

（一）本轮机构改革的特点

改革开放以来中国已经历了多次机构改革，基本上延续“五年一小改、十年一大改”的规律，本轮机构改革在理念、范围和深度上均大大超越了以往历次机构改革，具有以下特点：

1. 机构设置基本上下对口

《方案》特别提出，涉及省市县各级涉及党中央集中统一领导和国家法制统一、政令统一、市场统一的机构职能要基本对应。地方机构设置同中央和国家机关保持总体一致、上下贯通是本轮地方机构改革的鲜明特点。例如，对应国务院机构改革中新组建的自然资源部、生态环境部、应急管理部、市场监管总局等部门，各省市县基本上均成立了对口的部门。

2. 统筹设置党政机构

本次机构改革注重加强党的领导。党的有关机构可以同职能相近、联系紧密的其他部门统筹设置，实行合并设立或合署办公。比如将国家公务员局并入中央组织部，中央组织部对外保留国家公务员局牌子；将国家新闻出版广电总局的新闻出版管理职责划入中央宣传部，中央宣传部对外加挂国家新闻出版署(国家版权局)牌子；将国家新闻出版广电总局的电影管理职责划入中央宣传部，中央宣传部对外加挂国家电影局牌子。

3. 市场监管领域是改革重点

实行统一的市场监管，是建立统一开放竞争有序的现代市场体系的关键环节。然而由于历史原因，中国市场监管一直沿袭“分段监管为主、品种监管为辅”的多部门管理体制，市场监管和综合行政执法职能分散在不同行政部门。本轮机构改革设立市场监管总局，将政府对流通领域的工商监管、生产领域的质量监管、生产和流通领域的食品和药品监管、价格监管、知识产权保护、反垄断等六大市场监管职能归一，统一监管、综合执法。市场监管领域的改革顺应了现代市场经济发展需要统一市场监管的趋势和要求，有利于从体制机制上消除“九龙治水”的弊端。

4. 因地制宜，特色创新

因地制宜是地方机构改革的实践要求。从目前公布的方案来看，各省在保证中央集中统一领导的前提下，突出地方特点和特色，探索了符合自身实际需要的机构设置模式，既体现了全局的统一性，也呈现出局部的灵活性。例如，海南是旅游大省，为了适应建设国际旅游消费中心的建设要求，整合旅游、文化、体育等职能，

海南省组建了省旅游和文化广电体育厅；为适应信息时代发展特点，加强互联网与政府服务的深度融合，多地设置了与大数据相关的机构：浙江组建了大数据发展管理局，山东、福建等地也成立了大数据管理局。

（二）行政执法体制改革

行政执法体制改革是历次机构改革的重点，《方案》提出要按照减少层次、整合队伍、提高效率的原则，大幅减少执法队伍种类，合理配置执法力量。一个部门设有多支执法队伍的，原则上整合为一支队伍。推动整合同一领域或相近领域执法队伍，实行综合设置。完善执法程序，严格执法责任，做到严格规范公正文明执法。

1. 建立五大综合执法队伍

大力推行综合执法是近年来行政执法体制改革的方向，《法治政府建设实施纲要（2015-2020）》明确提出，要重点在食品药品安全、工商质检、公共卫生、安全生产、文化旅游、资源环境、农林水利、交通运输、城乡建设、海洋渔业、商务等领域内推行综合执法，支持有条件的领域推行跨部门综合执法。《方案》提出，要建立市场监管、生态环境保护、文化市场、交通运输、农业5大综合执法队伍，标志着综合执法取得突破性进展。建立五大综合执法队伍，有助于解决饱受诟病的政出多门、执法不规范等问题，实现政令统一、标准一致、口径统一，进而规范执法。

2. 完善行政执法程序

长期以来，行政执法程序问题一直受到社会关注，既是一个重点问题，也是一个难点问题。《深化党和国家机构改革方案》就此提出，完善执法程序，严格执法责任，做到严格规范公正文明执法。伴随着行政执法队伍的整合，相关部门也高度重视执法程序，抓紧制度建设。比如，2019年以来，市场监管总局相继制定了《市场监督管理行政处罚程序暂行规定》、《市场监督管理行政处罚听证暂行办法》、《市场监管总局关于印发<市场监督管理行政处罚文书格式范本>的通知》等部门规章或文件。此外，《市场监管总局关于市场监督管理部门正确行使行政处罚裁量权的指导意见》也已在公开征求意见。

3. 加强执法联动

《方案》提出，继续探索实行跨领域跨部门综合执法，建立健全综合执法主管部门、相关行业管理部门、综合执法队伍间协调配合、信息共享机制和跨部门、跨区域执法协作联动机制。这种联动机制的建构是行政资源合理配置的重要保障，也是行政机构高效运作的重要保障。此外，行政执法和刑事司法的衔接也进一步得到加强。比如，应急管理部联合公安部、最高人民法院、最高人民检察院联合发布了《安全生产行政执法与刑事司法衔接工作办法》，对安全生产领域中日常执法和事故调查中案件移送、证据收集、协作机制等做了明确规定。

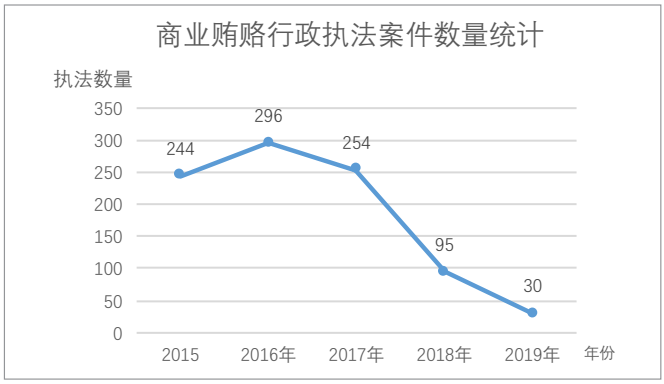
二、新《反不正当竞争法》下商业贿赂执法综述

2017年11月4日，第十二届全国人大常委会第三十次会议审议通过了修订后的《中华人民共和国反不正当竞争法》（下称“新法”），新法已于2018年1月1日起施行。新法公布后，原工商总局发布了《关于积极开展宣传贯彻新<反不正当竞争法>工作的通知》[1]，文件强调，各地要用好用足新法赋予的行政监管职能，以重点领域不正当竞争行为为突破口，以仿冒、商业贿赂、互联网不正当竞争为重点，切实加大监管执法和查办案件力度，依法严厉查处不正当竞争违法行为。当时市场普遍预期，伴随着新法的实施，商业贿赂执法将迎来高潮。但从公开可查询案件情况看，新法实施以来，商业贿赂执法并不活跃。相反，数据显示，与《反不正当竞争法（1993年）》（下称“旧法”）实施时的执法相比，2018-2019商业贿赂执法有较大幅度回落。

（一）新法实施后的执法特点

新法实施以来，我们在公开渠道共查询到125件[2] 商业贿赂执法案例。通过对这些案件的梳理和分析，我们发现，商业贿赂执法呈现以下特点：

1. 总体执法不活跃、地区执法不平衡



我们对近五年公开可查的商业贿赂行政执法案例进行了统计[3]，如上表所示，2015-2017年，商业贿赂执法案件每年稳定在200件以上；2018年新法实施后，当年执法案件数量急剧下降至95件；2019年前8个月，执法案件数量进一步缩减至30件。我们认为，新法实施后，总体执法并不活跃可能基于以下原因：

（1）新法对商业贿赂的认定作出了重大调整。新法聚焦于“信义义务的违反”这一商业贿赂本质特征，明确将交易相对方剔除出商业贿赂的对象，这是对商业贿赂认定的重大调整。因此，新法实施后，一般情况下交易双方之间基于平等协商确立的激励政策（例如折扣、返利）、利润分配、成本分摊等安排将不被认定为商业贿赂，而旧法下交易双方之间的各类赞助、返点等恰恰是商业贿赂的执法重点。

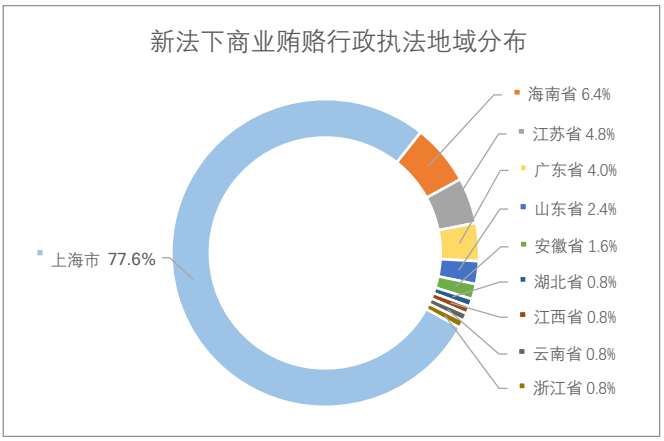
（2）缺乏细化规则的指引。旧法颁布后，原工商总局公布了《关于禁止商业贿赂行为的暂行规定》（下称“《暂行规定》”），《暂行规定》细化了对商业贿赂的认定。此外，原工商总局及其他相关职能部门还出台了一系列文件、答复等，对执法实践中遇到的相关问题予以明确。在新法对商业贿赂作出重大调整的情况下，《暂行规定》是否仍然有效以及如何适用、什么是利用职权或者影响力影响交易、员工责任和单位责任如何划分等一系列问题均有待进一步澄清。由于缺乏明晰的细化规则指引，面对实践中许多有争议的问题，执法机关执法比较谨慎。

（3）中央和地方执法机构处于持续改革和整合过程中。2018年3月21日，中共中央印发了《深化党和国家机构改革方案》（下称“《方案》”），将国家工商行政管理总局、国家质量监督检验检疫总局、国家食品药品监督管理总局的职责整合，组建国家市场监督管理总局。关于执法机构，《方案》明确规定将整合工商、质检、食品、药品、物价、商标、专利等执法职责和队伍，组建市场监管综合执法队伍。此后，中央和省、

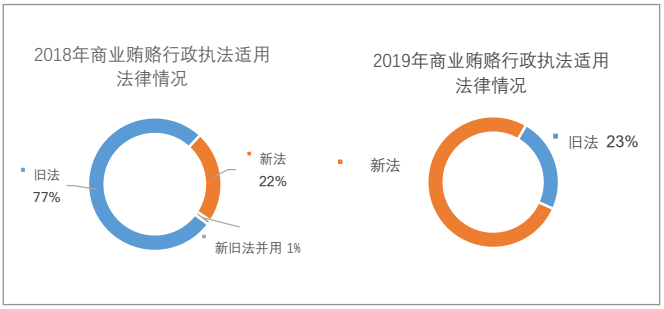
1. 工商竞争字〔2017〕202号
2. 本节所引用案例数据来源于威科先行•法律信息库、上海市市场监督管理局官方网站公布的商业贿赂案件行政处罚决定书，笔者以“商业贿赂”、《反不正当竞争法（1993年）》第八条、第二十二条、《反不正当竞争法》第七条、第十九条的具体内容为检索关键词，汇总截至2019年8月22日，共计135件商业贿赂行政处罚决定书，去掉10件违法事实、具体引用法条等关键内容缺失的案件，本文共分析案例125件。
3. 2015-2017年数据主要源于威科先行•法律信息库公布的商业贿赂案件行政处罚决定书，2018和2019年数据来源于威科先行及上海市场监督管理局官方网站公布的案例。
4. 该结论基于我们在威科先行•法律信息库的案例检索情况，但实践中存在一些地方没有及时将执法信息上网公布的情况。

市、县根据《方案》要求，持续进行机构整合。至2018年底，市场监管部门机构整合基本到位。在机构改革和整合过程中，一定程度上分散执法机关的精力，影响执法活动的开展。

除了总体执法不活跃以外，地区间执法不平衡也是新法实施后商业贿赂执法的鲜明特点。如下图所显示，上海市商业贿赂执法一枝独秀，执法案件数量占比高达77.6%，其他执法活动相对活跃的省份包括海南、江苏、广东，相当多的省份在新法颁布后公开未查到商业贿赂执法案件[4]。

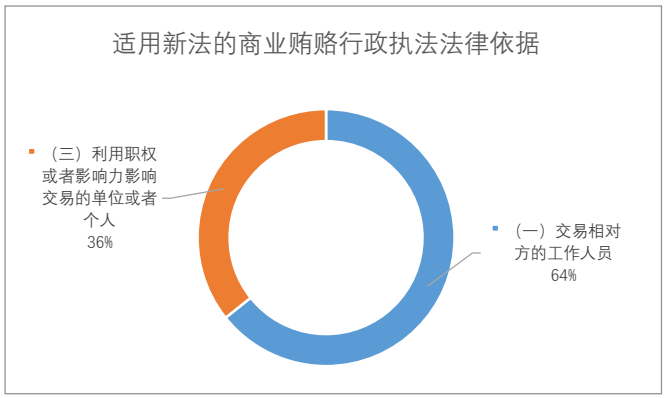


2. 新旧法适用并存



从上图可见，2018年商业贿赂执法案件中，大部分案件适用的是旧法，占比达77%，仅有22%的案件适用新法。我们理解，主要原因是2018年大多数执法案件的违法行为发生在新法实施以前，执法机关原则上应适用违法行为发生时有效的法律（即旧法）。该局面随着旧法下案件不断被消化而发生显著改变，2019年适用旧法的案件占比急剧下降至23%，而适用新法的案件占比上升至77%。

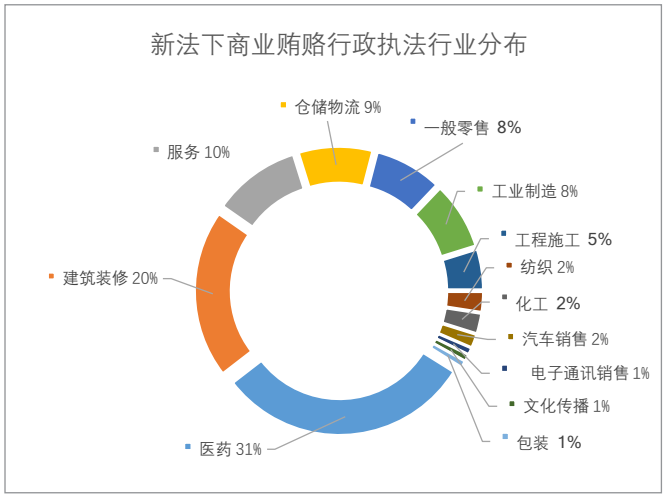
3. 适用新法的商业贿赂执法依据集中于第七条第一款第（一）和（三）项



在适用新法的案件中，64%的案件执法依据是新法第七条第一款第（一）项，即经营者对交易相对方的工作人员进行贿赂，以谋取交易机会或者竞争优势；36%的案件执法依据是新法第七条第一款第（三）项，即经营者对“利用职权或者影响力影响交易的单位或者个人”进行贿赂。被认定为“利用职权或者影响力影响交易的单位和个人”的主要有医院及医生、设计师及建筑装修公司等。新法实施以来，公开渠道尚未检索到依据第七条第一款第（二）项执法的案例。

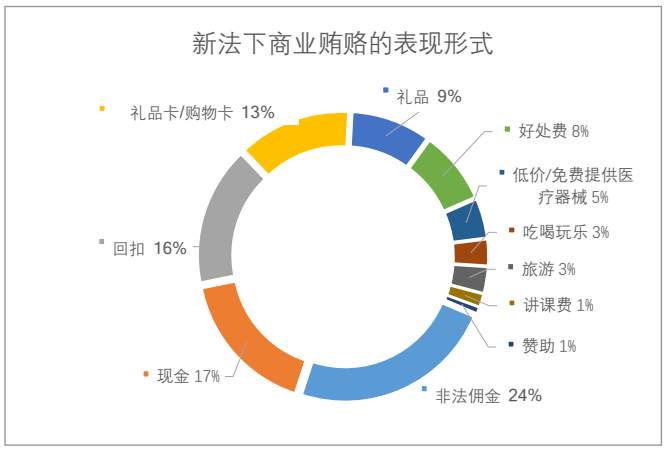
4. 医药及建筑装修成为新法下被重点执法的领域

4. 该结论基于我们在威科先行•法律信息库的案例检索情况，但实践中存在一些地方没有及时将执法信息上网公布的情况。
5. 沪工商检处字〔2019〕第320201810015号
6. 沪监管嘉处字（2018）第142018000158号



从被执法案件的行业分布来看，医药行业仍为重点监管和执法领域，占比达31%，涉案主体包括民营医院、医疗器械公司、药企、医药推广企业、第三方咨询公司等；其次是建筑装修（20%）、服务（10%）、仓储物流（9%）、一般零售（8%）、工业制造（8%）等行业。

5. 商业贿赂的表现形式多样化



从贿赂形式来看，非法佣金、现金、回扣、礼品卡/购物卡、礼品是最常见的行贿方式。有24%的案件给予第三方非法佣金，17%的案件直接给予现金，13%的案件给予礼品卡、购物卡或者消费券，6%的案件涉及按比例给予回扣，还有不少案例通过给予礼品、好处费、低价/免费提供医疗器械、吃喝玩乐、提供旅游经费、发放讲课费、提供赞助的形式进行贿赂。

（二）典型案例分析

1. 设备免费投放仍有较高商业贿赂风险

设备免费投放在旧法下一直是商业贿赂的打击重点，新法对商业贿赂的认定作出了重大调整，将交易相对方排除在受贿主体之外。由此，在新法下，设备免费投放是否仍应被认定为商业贿赂予以打击，引发了广泛争论，至今仍未形成统一认识。但从已公布案例来看，设备免费投放仍存在较高的商业贿赂风险。例如在上海杰智医疗器械有限公司不正当竞争案 中，当事人为获取交易机会，向江苏地区相关医院免费提供爱克发干式胶片打印机10台，并通过上述手段向医院配套销售爱克发胶片。执法机关认为上述行为，排挤了竞争对手，损害了市场公平竞争的秩序，侵害了患者的利益，构成商业贿赂，依照《中华人民共和国反不正当竞争法》第七条第一款第（三）项（贿赂利用职权或影响力影响交易的单位或个人）进行处罚。

也有一些案件，执法机关回避了对医院身份的界定，未明确指出医院属于新法第七条第一款下哪一类主体。例如在上海源洪贸易有限公司商业贿赂案[6]中，当事人以远低于成本价以及合理租赁价格，将两台全自动血液分析仪租赁给上海市嘉定区XX医院，达到了向XX医院销售配套医用耗材的目的。执法机关认为当事人帮助医院绕开设备采购制度、通过这种手段获得医院购买配套耗材的交易机会、并从中获取高额利润的行为，构成商业

贿赂，依照《中华人民共和国反不正当竞争法》第七条第一款进行处罚，但未明确指出依照第七条第一款哪一项。

我们认为，上述两案均存在值得商榷之处。前一案中，执法机关将医院认定为“利用职权或影响力影响交易的单位”，但却未进一步说明医院影响了哪一项具体交易。而在后一案中，执法机关更是未对医院属于哪一项受贿主体予以明确。

2. 执法机关对医生的定性尚不统一

在医药行业中，给予医生各种形式的“好处费”，作为其推荐药品、开具处方等的对价是常见的违法情形。从已公布案例来看，对于该类违法情形，执法机关如何界定医生的身份，存在不同意见。有的倾向于认为医生属于“交易相对方的工作人员”。例如在广州则天医药科技有限公司不正当竞争案中[7]，当事人系药品“艾朴”的广东总代理，其以“学术推广费”的名义向医生支付费用，鼓励该医生多选择使用该药品。执法机关认为当事人假借“学术推广费”的名义支付给医生现金以促进药品销售的行为，构成商业贿赂，依照《中华人民共和国反不正当竞争法》 第七条第一款第（一）项（贿赂交易相对方的工作人员）进行处罚。

也有执法机关认为，医生属于“利用职权或影响力影响交易的个人”。例如在上海泰磐投资管理咨询事务所不正当竞争案[8]中，当事人系从事医药推广的经营单位，执法机关认为当事人“为让相关医院及医生多开其推广的药品，以现金形式向相关自然人[9]支付产品推广费用”，从而构成商业贿赂，依照《中华人民共和国反不正当竞争法》 第七条第一款第（三）项（贿赂利用职权或影响力影响交易的个人）进行处罚。

我们认为，医生基于其专业上的优势，对于患者选用何种药物具有相当大的影响力甚至是决定力，因此，医生收受“好处费”，作为其开具处方、推荐产品的回报，违反医药行业有关规定及医师职业道德，是比较典型的利用影响力受贿的情形，医生宜认定为“利用影响力影响交易的个人”。但是，如果医生为帮助药企的产品“进院”，让医院采购药企的药品，而收受药企给与的好处，则医生应被视为“交易相对方的工作人员”。

3. “讲课费”易构成商业贿赂

我国相关法律法规并未明确禁止医生提供讲课服务并收受讲课费，但讲课费容易被企业滥用，用来掩盖贿赂。实践中很多企业以讲课费名义向医生提供好处，但医生实际并未提供讲课服务。该等模式被认定为商业贿赂的争议不大。例如在阿尔法韦士曼（北京）医药咨询有限公司上海分公司商业贿赂案[10]中，当事人在推广药品过程中，以组织召开相关会议的形式或者直接对临床主治医师以上级别的医生支付所谓的讲课费，从而增加医生的处方量，其中当事人在举办上述会议活动中，医院相关医生六次未作讲课，但却领取讲课费用。执法机关认为，当事人假借不实会议讲课等名义给付医生讲课费，医生利用医疗服务中职务便利，促成患者购买当事人推广的相关药品的行为，违反了《中华人民共和国反不正当竞争法》第七条第一款第（一）项的规定，构成商业贿赂。

4. 公对公的返利安排也可能构成商业贿赂

根据新法，交易双方公对公的返利安排，一般不会被视为商业贿赂。但在某些情况下，如处理不当，该等安排依然存在商业贿赂风险。例如，在上海好胜贸易有限公司商业贿赂案[12]中，当事人在销售酒类产品过程中与上海云迪娱乐有限公司（“上海云迪”）签订促销协议，约定向上海云迪销售600箱雅爵酒，当事人以现金形式，按每瓶人民币15元向上海云迪支付返利共计人民

7. 穗工商处字［2018］177号
8. 沪监管普处字（2019）第072018004595号
9. 判决书中未明确指出该自然人身份。但根据处罚决定书上下文，前述“自然人”有极大可能是医生。

币5.4万元，该返利由上海云迪经理签收，先后交给财务人员和业务经理，业务经理根据销售情况发放给包括业务经理在内的12名曾销售雅爵酒的业务员。执法机关认为，当事人的上述行为，违反了《中华人民共和国反不正当竞争法》第七条第（一）项第（一）款的规定，构成商业贿赂。

该案件的争议点在于，当事人与交易相对方的协议中明确约定了返利安排，但实际执行中，该返利由交易相对方的工作人员（即12名销售员）具体获益，在此情形下，该返利究竟是针对交易相对方还是交易相对方的工作人员？从本案被处罚的情况看，执法机关显然认为该返利由具体的销售人员直接受益，因此虽然合同系公对公签订，但本质上是向交易相对方的工作人员行贿。这种穿透式认定的执法思路值得企业关注。

5. 商业贿赂执法无起罚点

在新法亦或旧法下，商业贿赂执法无起罚点。很多企业因支付小额回扣或小额宴请被行政机关处罚。比如设计师陈某带客户到当事人上海亦晶实业发展有限公司处订购洗碗机，当事人向陈某支付回扣300元，上海市普陀区市场监督管理局认为当事人的行为构成商业贿赂，罚款8万元；[13]同类型案件还有当事人支付400元、580元回扣，被执法机关分别罚款8万元、9万元；[14]当事人为了获得交易机会，宴请了新任该院负责采购业务的医生，花费605元，上海市青浦区市场监督管理局认为当事人的行为构成商业贿赂，罚款2万元[15]等。

以上案例意在提醒企业，刑法下的贿赂犯罪对个人或者单位分别设置有入罪标准，但在《反不正当竞争法》下，任何满足商业贿赂构成要件的商业行为，无论行贿金额高低，均可能被处罚。而一旦受到商业贿赂处罚，可能会有连带后果，例如被列入黑名单、影响参加招投标及政府采购、IPO上市等。因此，企业应对其商业模式和合规内控引起足够重视，以免因小失大。

10. 沪监管静处字〔2019〕第062018004224号
11. 沪监管青处字（2018）第292018000076号
12. 沪监管黄处字（2019）第012018001966号
13. 沪监管普处字（2018）第072018000307号
14. 沪监管普处字（2018）第072018000308号、沪监管普处字（2018）第072018000227号
15. 青市监案处字〔2018〕第290201610081号

三、中国数据保护立法与执法趋势综述

2018至2019年，我国在数据保护领域的立法活动，无论是法律法规的制定还是国家标准的修订，都在紧锣密鼓地开展之中。在执法层面，在全国上下开展了针对App和互联网金融领域违法违规收集使用个人信息的乱象的整治。下文将总结今年中国数据保护立法与执法方面的动态与趋势。

（一）立法趋势综述

1.《数据安全法》、《个人信息保护法》纳入立法计划

在2018年9月公布的“十三届全国人大常委会立法规划”中，《数据安全法》、《个人信息保护法》与其他67部法律被列为“条件比较成熟、任期内拟提请审议的法律草案”。

在2016年发布的《国民经济和社会发展第十三个五年规划纲要》（下称“十三五规划”）中，第二十七章以专章形式提出“实施国家大数据战略”，将大数据列为国家的“基础性战略资源”，在强调加快数据开放共享、促进数据产业发展的同时，又指出要 “加强数据资源安全保护”，保障数据资源的“安全高效可信应用”，体现出安全与发展并重的治理原则。在2019年3月十三届全国人大二次会议新闻发布会上，大会发言人张业遂表示《数据安全法》作为加强国家安全、社会治理领域的立法，将成为2019年重点推进的立法工作。

个人信息保护方面，目前我国总体上呈现分散立法状态，尽管已经有刑法、民法总则、消费者权益保护法、网络安全法、电子商务法等多部法律、法规、规章涉及个人信息保护，但仍然需要根据社会形势的发展，制定有针对性的专门法律来加以规范，形成合力。全国人大常委会已将制定个人信息保护法列入本届立法规划，相关部门正在抓紧研究和起草。

2. 部门规章《数据安全管理办法》公开征求意见

2019年5月28日，国家互联网信息办公室（“网信办”）发布《数据安全管理办法（征求意见稿）》（下称“征求意见稿”），首次以部门规章的形式对重要数据和个人信息安全的保护与监督管理提出较全面的规定，征求意见稿对《网络安全法》确立的各项数据安全规则进行了细化。在个人信息保护方面，征求意见稿很大程度上吸收了《信息安全技术　个人信息安全规范》（下称“《规范》”）的合规要求，将国家标准层级上的部分要求转变为法律义务，进而解决了企业在个人信息合规工作中的困惑。

征求意见稿在《网络安全法》基础上，对人员架构、事中风控、安全措施方面的规则进行了细化，构建起了数据安全治理的框架。人员架构方面，征求意见稿规定了数据安全责任人制度（第17条、第18条）；事中风控方面，针对处理环节的风险，征求意见稿要求网络运营者对所接入的第三方承担安全责任（第30条），并对网络运营者兼并、重组、破产的情况下数据承接方的义务作出规定（第31条）；安全措施方面，征求意见稿要求网络运营者采取数据分类、备份、加密等安全措施（第19条），鼓励安全认证制度（第34条），并进一步细化了数据安全事件的应急处置要求（第35条）。

针对个人信息保护，征求意见稿很大程度上吸收了《规范》的要求与今年 App违法违规收集使用个人信息专项治理工作中的实践经验，将这些实践做法转变为法律义务。具体而言，在收集环节，征求意见稿明确了个人信息的收集使用规则要求（第7-10条）、“同意”机制的适用与具体要求（第11-13条、第22条、第27条）；在处理环节，规定了个人信息的保存期限（第20

条），对个人信息主体的查询、更正、删除个人信息和注销账号请求的响应要求（第21条），以及向他人提供时的安全风险评估要求与同意的例外情形（第27条）；此外，征求意见稿要求个人信息的间接收集方与直接收集方负有同等的保护责任和义务（第14条）。

在重要数据保护方面，征求意见稿对重要数据的保护停留在备案与审批的初步探索阶段。相较于两年前发布的《个人信息和重要数据出境安全评估办法（征求意见稿）》与《信息安全技术 数据出境安全评估指南（征求意见稿）》，征求意见稿中对“重要数据”的定义进行了更新，将重要数据国家安全等因素之间的关系由“密切相关”改为了“直接影响”，同时特别指出一般不包括“企业生产经营和内部管理信息、个人信息”。征求意见稿还对重要数据要求落实备案制度（第15条），落实发布、共享、交易、出境前的安全评估制度（第28条）。然而，如何识别重要数据的问题仍然未得到解决。

除了传统意义上的“数据安全”，征求意见稿此次还将“数据安全”的含义进一步延伸到了对数据滥用行为的规制。具体而言包括对爬虫等自动化手段抓取行为（第16条）、定向推送行为（第23条）的限制，对自动合成内容（第24条）、社交网络转发内容（第25条）要求加标，对假借他人名义发布信息要求立即删除（第26条），对利用数据发布市场预测等信息要求不得影响国家安全、经济运行与社会稳定（第32条），以及配合国务院有关主管部门为职责需要依法要求时提供相应的数据（第36条）。

整体而言，这些规定体现了《数据安全管理办法》乃至未来《数据安全法》的数据安全观已经突破了传统信息安全的“保密性、完整性、可用性”要求，将监管延伸到数据利用过程中的滥用行为，为维护社会稳定与数据资源的“安全高效可信应用”作出大胆的尝试。

3. 针对数据跨境问题的《个人信息出境安全评估办法》公开征求意见

2019年6月13日，网信办发布《个人信息出境安全评估办法（征求意见稿）》（下称“征求意见稿”）。相较于两年前发布的《个人信息和重要数据出境安全评估办法（征求意见稿）》与《信息安全技术 数据出境安全评估指南（征求意见稿）》，此次征求意见稿表明，在出境安全评估方面，将对个人信息与重要数据分而治之。

整体而言，为促进个人信息的依法有序自由流动，征求意见稿确立了个人信息“经安全评估后出境”的规范框架。需要指出的是，征求意见稿规定的适用范围是“网络运营者向境外提供在中国境内运营中收集的个人信息”这一特定场景，并未包括个人访问境外网站的行为。

征求意见稿所规定的安全评估内容反映出对个人信息出境风险在事前、事中与事后的管理处置。征求意见稿关注个人信息出境前网络运营者或接收者的业务模式、网络运营者获得个人信息是否合法正当以及数据传输合同能否得到有效执行，要求网络运营者披露自身和境外接收者的基本状况、个人信息出境计划、风险分析以及安全措施，对网络运营者规定了重新评估义务（第3条）、出境记录保存义务（第8条）、年度报告与安全事件报告义务（第9条）以及定期执法检查要求（第10条）和举报制度（第12条）等。

此次征求意见稿尤其关注“网络运营者与接收者签订的合同”这一合规手段，引导网络运营者主动监督境外数据接收方的安全管理水平，为个人信息主体维权提供切实可行的救济途径，对此规定了该合同的内容要素（第13条）、网络运营者的责任和义务（第14条）、接收者的责任和义务（第15条）以及个人信息出境后转移

的条件（第16条）等。这些规定提升了企业合规风控的可操作性，为企业合规实践产生积极作用。

征求意见稿侧重事先安全评估、辅之以合同约束为保障，反映出主管机关就个人信息出境全面进行风险控制的管理思路。

4. 聚焦儿童保护的《儿童个人信息网络保护规定》发布

2019年8月23日，网信办发布《儿童个人信息网络保护规定》（“《儿童保护规定》”），并将于2019年10月1日起正式实施。《儿童保护规定》系统地规定了儿童个人信息保护的法律要求，在《中华人民共和国网络安全法》（“网安法”）等个人信息保护法律法规的基础上针对儿童这一特殊主体规定了更为具体和更为严格的合规要求。企业需要及时识别该规定对自身的适用性，并尽快做出相应的合规安排及调整。

《儿童保护规定》的适用范围较为广泛。根据《儿童保护规定》第2条和第3条，该规定保护未满14周岁未成年人的个人信息，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”。从条文本身来看，任何企业的业务如果涉及上述活动都将可能适用《儿童保护规定》。尽管《儿童保护规定》最后一条规定，“通过计算机信息系统自动留存处理信息且无法识别所留存处理的信息属于儿童个人信息的，依照其他有关规定执行”，而一些网站或App在通常情况下不涉及或很少涉及儿童用户，能否排除适用该规定还有待监管机关的进一步明确。

《儿童保护规定》第9条再次重申了网安法第41条中个人信息处理的“告知+同意”要求，并进行了一定的细化：（1）“告知”必须通过显著、清晰的方式进行；（2）“同意”应当由儿童监护人作出。《儿童保护规定》最终发布的版本没有采取征求意见稿中“明示同意”的要求，这给企业在实操中如何确认和证明已经取得监护人的有效同意留下了疑问。

《儿童保护规定》第12条规定：“网络运营者存储儿童个人信息，不得超过实现其收集、使用目的所必需的期限”，明确了网络运营者在儿童个人信息保护上的限期删除原则，填补了网安法中对于个人信息保护的基本原则中的空缺（虽然有观点认为限期删除原则可以从数据最小化原则中推倒，但是国际上个人信息基本保护原则中的数据最小化原则是独立于限期删除原则的）。这意味着如果网络运营者适用《儿童保护规定》，则其必须明确需要留存儿童个人信息的期限，并且建立按期删除机制。

《儿童保护规定》第16条规定网络运营者在委托第三方处理儿童个人信息时，应当对受托方及委托行为进行安全评估，并应当与受托方签订协议，明确双方在数据保护方面的责任分配。第17条也要求网络运营者在向第三方转移儿童个人信息时，应当自行或者委托第三方机构进行安全评估，同样补充了网安法未予明确之处。

《儿童保护规定》第8条和第15条均提及了儿童个人信息保护负责人：第8条要求网络运营者指定专人负责儿童个人信息保护，第15条规定企业员工访问儿童个人信息时，应经儿童个人信息保护负责人或者其授权的管理人员审批。

《儿童保护规定》第21条规定数据泄露事件“造成或者可能造成严重后果的，（网络运营者）应当立即向有关主管部门报告，并将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的儿童及其监护人”，调整了网安法第42条第2款中的数据泄露汇报义务的门槛，即明确数据泄露已经或可能产生严重后果时需要向有关主管部门报告。但实践中什么是“严重后

果”，还需要网信办给出更为明确的指引。

相较于网安法第43条，《儿童保护规定》第20条规定扩大了儿童监护人的删除权行使范围。除了在第43条基础之上增加（1）超出目的范围或者必要期限收集、存储、使用、转移、披露儿童个人信息的，和（2）儿童监护人撤回同意两种情形外，还明确监护人可以行使删除权的范围“包括但不限于”该条所列情形。对于已经按照网安法建立用户行权机制的企业来说，可能需要根据《儿童保护规定》的要求调整涉及儿童个人信息行权时的回应方式。

《儿童保护规定》的落地显示了网信办对于推进个人信息保护工作的决心，广泛的适用范围、严格的监护人同意以及覆盖儿童个人信息进入网络运营者的全生命周期的要求都体现了网信办对儿童网络用户保护的重视。

5. 国家标准《信息安全技术 个人信息安全规范》修订

2018年5月1日，推荐性国家标准《信息安全技术 个人信息安全规范》（下称“《个人信息安全规范》”）正式实施，填补了我国个人信息保护在实践标准中的空白，在接下来的一年多时间里对企业开展个人信息安全合规起到了积极的指引作用。

2019年2月1日，全国信息安全标准化技术委员会（下称“信安标委”）发布了《信息安全技术 个人信息安全规范（草案）》（以下简称“《规范（草案）》”）并公开征求意见。之后，信安标委又将草案进行了完善，并先后于2019年6月25日和2019年10月24日再次公开征求意见，最终形成《信息安全技术 个人信息安全规范（征求意见稿）》（以下简称“《规范（征求意见稿）》”）。

本书第三章将对比《个人信息安全规范》、《规范（草案）》及10月最新发布的《规范（征求意见稿）》，详细分析此次修订的要点与趋势。

（二）执法趋势综述

1. 四部委联合开展App违法违规收集使用个人信息专项治理工作

2019年1月25日，中央网信办、工业和信息化部、公安部、市场监管总局在北京举行“App违法违规收集使用个人信息专项治理”新闻发布会，并正式对外发布《关于开展App违法违规收集使用个人信息专项治理的公告》，宣布将在2019年全年范围内开展专项治理工作，并委托相关单位成立专项治理工作组。

专项治理工作重点针对如下行为进行查处：（1）强制、过度收集个人信息；（2）未经消费者同意、违反法律法规规定和双方约定收集、使用个人信息；（3）发生或可能发生信息泄露、丢失而未采取补救措施；以及（4）非法出售、非法向他人提供个人信息等行为。

截至2019年8月31日，专项治理工作组通过微信公众号“App个人信息举报”已收到8000余条民众举报，选取近600款用户数量大、与民众生活密切相关的App进行评估，督促问题严重的200余款App进行整改，涉及整改的问题点达800余个，无隐私政策、强制索权、超范围收集个人信息等问题得到显著改善。

2. 工信部专项整治APP违规收集个人信息、过度索权等八类问题

为巩固和深化专项治理工作的成果，工业和信息化部信息通信管理局于2019年11月4日召开整治工作启动会，宣布开展信息通信领域App侵害用户权益专项整治行动。

此次专项整治行动面向App服务提供者和App分发服务提供者两类主体对象，重点整治违规收集用户个人信息、违规使用用户个人信息、不合理索取用户权限、为用户账号注销设置障碍等四个方面的八类突出问题。整治工作将持续两个月，分为三个阶段，第一阶段是APP服务提供者对照八类问题自查自纠；第二阶段为监督抽查阶段；第三阶段为结果处置阶段，具体措施有组织APP下架、停止APP接入服务、向社会公告等。

3. 公安扫黑除恶行动，打击爬虫业务中的违法收集使用个人信息行为

2018年8月开始，针对网络乱象，公安机关已实行“一案双查”制度：（1）对网络违法犯罪案件开展侦查调查工作；（2）同步启动对涉案网络服务提供者法定网络安全义务履行情况的监督检查。对拒不履行法定网络安全义务、为网络违法犯罪活动提供帮助的网络服务提供者，公安机关将依法对其进行严厉查处，努力从源头遏制网络违法犯罪案件发生。

时至2019年年末，多家现金贷相关的数据源公司被公安机关查处，涉事高管被警方控制，截至目前，多家知名数据风控相关公司都已经主动或被动地停止了与爬虫相关的数据业务。此次行动源于公安机关在全国范围开展的打掉“套路贷”和暴力催收的数据源头扫黑除恶行动，以及银监会、互联网金融风险专项整治、P2P网贷风险专项整治工作领导小组办公室等监管机构主导的现金贷溯源性整肃行动。

下文《刑事执法热点分析》将进一步分析述执法行动的重点与趋势。

4. 其他行业主管监管及执法动态

· 证监会制发《证券基金经营机构信息技术管理办法》

中国证券监督管理委员会制发《证券基金经营机构信息技术管理办法》，自2019年6月1日起施行。《办法》包括如下内容：一是全面覆盖各类主体；二是明确治理、安全、合规三条主线；三是强化信息技术管理的主体责任；四是支持经营机构应用信息技术，提升服务效能；五是督促各类市场主体切实履行自身信息技术管理职责，明确处罚措施。

· 教育部：将与网信部门联合行动治理校园APP

2019年3月1日，教育部表示将与网信部门开展联合行动，治理教育类APP。教育部印发了《2019年教育信息化和网络安全工作要点》，包括研究制定规范校园APP管理的意见，规范第三方校园APP的引入和自主开发校园APP的建设，重点加强学习类APP的规范管理。2019年9月5日，教育部、中央网信办等八部门联合印发《关于引导规范教育移动互联网应用有序健康发展的意见》，建立起教育APP的备案制度，加强事中事后的监管工作。

· 国家卫生健康委办公厅及国家中医药管理局办公室发布《关于落实卫生健康行业网络信息与数据安全责任的通知》

2019年4月，国家卫生健康委办公厅及国家中医药管理局办公室发布《关于落实卫生健康行业网络信息与数据安全责任的通知》，明确医疗卫生机构需履行的网络信息与数据安全保护义务。

其他行业主管也均对数据加强管控，例如测绘部门、人类遗传资源办公室等。

四、《企业境外经营合规管理指引》解读

去年年底，为了更好地为企业开展境外经营提供指引，推动企业持续提升合规管理水平，国家发展改革委、外交部、商务部、人民银行、国资委、外汇局、全国工商联七部委联合发布了《企业境外经营合规管理指引》（“《指引》”）。

为什么七部委对中国企业在境外经营的合规管理如此关注？据商务部、外汇局统计，2018年，我国对外全行业直接投资8591.4亿元人民币，其中，我国境内投资者共对全球161个国家和地区的5735家境外企业进行了非金融类直接投资，累计实现投资7974亿元人民币。我国对外承包工程业务完成营业额已经达到1.12万亿元人民币，新签合同额1.6万亿元人民币。同时，我国对外劳务合作派出各类劳务人员49.2万人。从以上这组数据不难看出，中国企业在境外的投资、对外承包工程和劳务输出都已经达到了不容小觑的规模。随着中国企业在海外的投资、业务扩张，也逐渐开始受到境外合规风险的影响，部分企业还因此吃了亏。近年来，在中美博弈的背景下，国际局势愈发复杂，新的立法与执法情况层出不穷，具有大量跨国业务的中国企业在合规方面面临着前所未有的挑战。

（一）境外经营合规的依据是什么？

这个问题不仅是企业在境外经营合规管理中最首要的问题，在境内合规方面，也困扰着不少企业。根据《指引》，境外经营合规的依据主要是企业及其员工的经营管理行为符合有关法律法规、国际条约、监管规定、行业准则、商业惯例、道德规范和企业依法制定的章程及规章制度等要求。这里对合规依据的范围规定比《央企合规管理指引》（“《央企指引》”）要更宽。

在《央企指引》中，“合规”是指中央企业及其员工的经营管理行为符合法律法规、监管规定、行业准则和企业章程、规章制度以及国际条约、规则等要求。一方面，《指引》的合规依据不再局限于国内的法律法规，也包括企业在境外经营过程中适用的当地法律法规、监管规定以及行业准则等。另一方面，《指引》相较于《央企指引》对合规的定义，增加了符合商业惯例与道德规范的要求。虽然《指引》对于合规的定义非常广泛，但事实上具有一定必要性：大部分在境外运营的企业均需要在一定程度上适用外国法，而且部分国家对于商业管理及道德规范的尊重、认可程度比较高。在这些地区，即使部分违反商业惯例或道德规范的行为不会引起直接的刑事或行政法律后果，也无法排除企业经济、声誉受损的可能性。例如，中国企业在“出海”过程中，频繁遇到棘手的劳工问题，有时即使中国企业的做法没有违反当地法律法规，但由于劳动用工制度或待遇与当地商业惯例或道德规范不符，就会引起长时间的罢工，导致公司业务停摆。

（二）海外合规需要关注哪些领域的合规要求？

《指引》按照我国企业在境外经营的四种最主要形式，即对外贸易、境外投资、对外工程承包以及日常经营，对企业需要关注的合规要求进行了总结。

具体而言，首先，无论是在上述任何一种境外活动中，企业都应该做到合规全覆盖，确保经营活动全流程、全方位合规，要做到这一点，企业必须全面梳理其在境外的业务，了解各个业务环节存在的合规风险，并在全面了解相关海外法律法规及制度要求的基础上，对标公司的合规现状，找到差异并有针对性地制定搭建合规体系的方案。

其次，针对企业在境外的主要经营模式不同，应该关注的合规风险也存在差异。企业应该在全面了解各业务环节的风险基础上，结合自身所在的行业、经营的国

1. 数据来源：《2018年我国对外全行业直接投资简明统计》，中华人民共和国商务部对外投资和经纪合作司，http://www.mofcom.gov.cn/article/tongjiziliao/dgzz/201901/20190102829082.shtml
2. 数据来源：《2018年我国对外承包工程业务简明统计》，中华人民共和国商务部对外投资和经纪合作司，http://www.mofcom.gov.cn/article/tongjiziliao/dgzz/201901/20190102829083.shtml
3. 数据来源：《2018年我国对外劳务合作业务简明统计》，中华人民共和国商务部对外投资和经纪合作司，http://www.mofcom.gov.cn/article/tongjiziliao/dgzz/201901/20190102829084.shtml

家，综合考虑该领域的法律责任、执法活跃程度、是否曾经受到执法等多方面因素，评估各个领域合规风险的等级，并抓住重点领域着重管控。根据《指引》的总结，在对外贸易中，企业应关注的领域至少应包括贸易管制、质量安全与技术标准、知识产权保护等方面的具体要求，关注业务所涉国家（地区）开展的贸易救济调查，包括反倾销、反补贴、保障措施调查等；在境外投资中，企业应关注的领域至少应包括市场准入、贸易管制、国家安全审查、行业监管、外汇管理、反垄断、反洗钱、反恐怖融资等方面的具体要求；在对外承包工程中，企业应关注的领域至少应包括投标管理、合同管理、项目履约、劳工权利保护、环境保护、连带风险管理、债务管理、捐赠与赞助、反腐败、反贿赂等方面的具体要求；在境外日常经营方面，企业应关注的领域至少应包括劳工权利保护、环境保护、数据和隐私保护、知识产权保护、反腐败、反贿赂、反垄断、反洗钱、反恐怖融资、贸易管制、财务税收等方面的具体要求。

根据我们的实践经验，《指引》中指出的这些关键合规风险领域确实是建立在大量实践案例的基础上，通过我国企业在“走出去”过程中遇到的合规问题总结归纳形成的，对具有境外业务或投资的企业而言具有较高的参考价值。

（三）合规治理应该由谁负责?

自从我国企业开始在全球扩展业务，很多企业都在不同程度上搭建了自己的合规管理组织体系，有些公司的合规管理牵头部门是法律事务部门，而有的公司设立了独立的合规管理部门。总体而言，《指引》将合规管理职能分为决策、管理、执行三个层级，并建议企业在此基础上，根据自身组织架构分配具体的合规管理责任。《指引》的建议指出，企业合规决策层的主要职责是以保证企业合规经营为目的，通过原则性顶层设计，解决合规管理工作中的权力配置问题；合规管理高级管理层应分配充足的资源建立、制定、实施、评价、维护和改进合规管理体系；各执行部门及境外分支机构应及时识别归口管理领域的合规要求，改进合规管理措施，执行合规管理制度和程序，收集合规风险信息，落实相关工作要求。至于是否应该设置合规委员会、具体由哪个部门作为合规管理部门以及由谁来担任合规负责人，《指引》并没有给出唯一的答案，企业可以结合自身实际来安排，但专职的合规人员、独立的合规部门以及畅通的汇报线，都是有效的合规管理体系的重要保障。

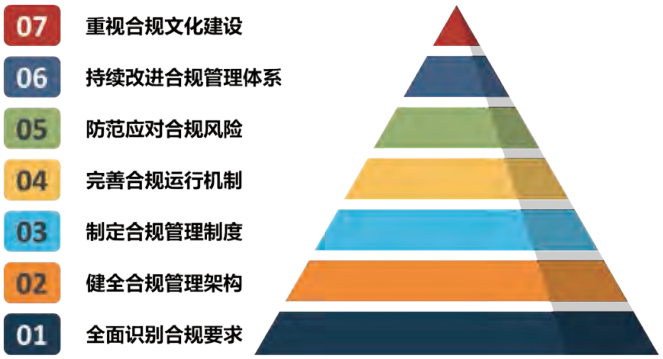
《指引》也指出了合规工作内部协调的重要性。《指引》主要强调了四种合规工作需要协调好的关系：一是合规管理部门与业务部门之间分工协作的关系，双方应密切配合；二是合规管理部门与其他监督部门的关系，例如审计、监察等部门；三是企业与外部监管部门的关系；四是企业与第三方的关系。

其实合规管理不应该是某一个单独的部门的职责，合规部门也不应该只有“管理”这一种职能。合规需要从每一个员工做起，也需要多个层级的不同部门齐抓共管，形成合力。合规主管部门在此过程中，不仅需要承担管理职能，对重大的合规风险进行把控并牵头开展合规管理工作，同时还要发挥服务职能，为公司其他部门以及下属企业的相关部门提供支持，为公司业务发展保驾护航。

很多跨国经营的中国大型企业均存在多线发展的业务，公司内部组织架构也由公司总部及数量众多的下属子公司、分公司组成。在这种情况下，各下属公司不仅应该相应地明确合规决策、管理和执行三个层次的职能部门，还应该与公司总部之间保持密切联系。公司总部如果想要将合规管理体系切实落地，必须对下属企业的合规状况进行监督，保证制度实施。与此同时，公司总部也应当为下属公司提供必要的支持，例如：对识别到的合规风险及时提示下属企业进行防范，遇到重大的合

规风险应该引导下属企业妥善应对。

（四）如何从零开始建立一套完整的境外经营合规体系？



图表1 企业境外合规管理基本框架

《指引》提出了一套比较成熟的合规体系建立框架，对于“从零开始”进行合规体系建设的企业而言，相当于一张路线图，具有很高的参考价值；对于已经开始开展合规体系建设的企业而言，也有助于让企业了解应当如何完善现有体系。

第一步：全面识别合规要求

首先，建立合规体系应该从全面识别合规要求开始。合规管理应该是以合规风险导向。如果不了解企业所面临的合规要求，适当的管理也自然无从谈起。在识别合规要求时，可以参考以上第二部分介绍的，《指引》列举的对外贸易、境外投资、对外工程承包以及日常经营中需要关注的核心合规要求。不过，《指引》指出的只是大部分企业常见的合规要求，并不能代表所有企业所面临的合规要求。因此在此基础上，如果想要真正全面地识别企业面临的合规要求，企业还应该相应地关注所在行业、国家的具体规范。

第二步：健全合规管理架构

明确了企业需要符合的合规要求包括哪些之后，为了开展下一步合规管理工作，首当其冲需要确定的就是合规管理职能应该由哪些部门来承担。在这一步，企业可以参考以上第三部分介绍的内容搭建内部合规管理组织体系。

第三步：制定合规管理制度

很多大型中国企业的内部制度其实已经相对完备，企业在进行合规制度建设之前，应该先进行一定程度的梳理，了解哪些制度存在缺失、哪些制度有待更新、哪些制度适用于国内实践但无法满足境外下属单位的需求。《指引》也为企业列举了应具备的基本制度，主要包括以下几类：

1. 合规行为准则：“合规行为准则是最重要、最基本的合规制度，是其他合规制度的基础和依据，适用于所有境外经营相关部门和员工，以及代表企业从事境外经营活动的第三方。”

2. 合规管理办法：“企业应在合规行为准则的基础上，针对特定主题或特定风险领域制定具体的合规管理办法，包括但不限于礼品及招待、赞助及捐赠、利益冲突管理、举报管理和内部调查、人力资源管理、税务管理、商业伙伴合规管理等内容。企业还应针对特定行业或地区的合规要求，结合企业自身的特点和发展需要，制定相应的合规风险管理办法。”

3. 合规操作流程：“企业可结合境外经营实际，就合规行为准则和管理办法制定相应的合规操作流程，进一步细化标准和要求，便于理解落实。”

第四步：完善合规运行机制

合规运行机制主要是指除了制度之外，能够推动合

规管理体系稳定、持续、有效运行的一系列机制。即使企业已经建立了相对完善的内部制度，但“徒法不足以自行”。合规如果要脱离纸面制度真正融入公司的实践，需要合规运行机制的配合和保障。《指引》指出了六种合规运行机制，从各个机制所发挥的作用来看，大致可以分为事前、事中以及事后三个阶段的机制。

首先，在事前阶段，企业应当确保合规事项上传下达畅通有效。对员工，企业应将合规培训纳入员工培训计划，而且培训内容需随企业内外部环境变化进行动态调整。对公司决策管理层，合规负责人和合规管理部门应享有通畅的合规汇报渠道，保证能够第一时间将合规管理情况、风险评估情况以及重大合规风险汇报给决策层，并采取进一步应对措施。

在事中阶段，企业应该建立合规考核机制，全面覆盖企业的各项管理工作。合规考核结果应作为企业绩效考核的重要依据。同时，由于境外法律复杂多变，企业的境外分支机构难以针对合规问题作出准确的评估以及决策，这就需要境外经营相关部门和境外分支机构及其员工在履职过程中遇到合规风险事项时，及时主动寻求合规咨询或审核支持。这也体现了合规部门“管理”、“服务”的双重职能。

在事后阶段，也就是发生了潜在的违规事件时，企业可以通过畅通的信息举报体系、规范的调查与全面有效的问责机制保障合规管理具有威慑力。关于举报体系，企业可以根据自身特点和实际情况建立和完善，但员工、客户和第三方均应该有权进行举报和投诉，而且企业应充分保护举报人。针对举报事项，企业应该谨慎、及时地开展调查。在调查过程中，注意不要破坏证据，也不能泄露举报人信息。在问责方面，企业应建立全面有效的合规问责制度，明晰合规责任范围，细化违规惩处标准，严格认定和追究违规行为责任。

第五步：防范应对合规风险

依据《指引》，所谓合规风险，是指企业或其员工因违规行为遭受法律制裁、监管处罚、重大财产损失或声誉损失以及其他负面影响的可能性。正如前文所述，境外经营的合规风险会受到经济、政治、科技等多重因素的影响，往往频繁变化，因此除了最初的合规要求识别，企业还需要动态地识别合规风险，并通过风险评估筛选出重点管控的合规风险。

在这一方面，一个典型的案例就是去年美国对伊制裁的恢复。2018年5月份，美国突然宣布退出《伊朗核协定》（“JCPOA”），发布了《国家安全总统备忘录》，并在2018年逐步恢复了对伊朗的全面经济制裁。这一突变对全球很多行业的贸易都产生了不小的影响。对于存在对伊业务的中国企业而言，更是让人措手不及。如何平衡境外合规风险与业务，在降低合规风险的同时尽可能地保护业务，成为了很多企业去年面临的难题。除此之外，其他常见的突发性合规风险还可能包括受到境外反洗钱、反垄断、商业秘密等相关原因的突击执法等。如果不能及时识别、评估并采取措施防范这样的合规风险，企业将可能面临严重的法律责任以及经济与声誉损失，企业高管还有可能被追究个人责任。

为了动态地识别并应对合规风险，企业各境外分支应该聘请专业人员密切关注公司在该国业务所需遵守的法律法规，了解当地执法趋势。在识别风险后，企业可根据企业的规模、目标、市场环境及风险状况确定合规风险评估的标准和合规风险管理的优先级。

第六步：持续改进合规管理体系

正如合规风险复杂多变一样，合规管理体系也不应该是一成不变的。《指引》提出了三种可以促进合规管理体系持续不断改进的方法：

首先，企业可以与审计部门相互配合，通过审计“对企业合规管理的执行情况、合规管理体系的适当性和有效性等进行独立审计”，并共享审计结果。

其次，企业可以通过自查或委托外部专业机构“定期对合规管理体系进行系统全面的评价，发现和纠正合规管理贯彻执行中存在的问题，促进合规体系的不断完善”。在合规管理体系评价过程中，常用的方法包括：在制度层面，可以开展制度与现行法律法规、规范性文件的差异分析；在执行层面，可以通过选取一定的样本进行深入测试，考察合规管理体系是否得到了执行。

第三，“企业应根据合规审计和体系评价情况，进入合规风险再识别和合规制度再制定的持续改进阶段，保障合规管理体系全环节的稳健运行”。

第七步：重视合规文化建设

合规文化建设之所以被放在最后一步，是因为合规文化建设并不是一朝一夕就能够达成的目标，需要在合规管理体系反复执行、不断改进的过程中逐步建立并最终成为员工日常工作的一种习惯。很多企业的决策层都已经意识到了合规的重要性，并通过将合规融入企业文化、公开宣讲以及合规培训等方式，向公司内部员工传达了了解合规、重视合规的观念。此类的宣传教育固然重要，但更重要的是在合规管理体系践行的过程中，不断让企业内部员工乃至外部合作伙伴都能够从中受益，真正感受到在合规的保驾护航下，企业能够更加“行稳致远”。

五、《中央企业合规管理指引（试行）》解读

2018年11月2日，国务院国有资产监督管理委员会正式印发了《中央企业合规管理指引（试行）》（以下简称“《指引》”），自发布之日起生效。这部指导央企合规体系建设的核心制度从起草开始，就受到了不少中央企业、国有企业的广泛关注。《指引》在制定的过程中不仅借鉴了全球先进的合规体系建设经验，更融合了招商局集团、中国石油、中国移动、东方电气、和中国铁路工程总公司五家试点央企3年以来的宝贵实践经验。

（一）《指引》的制定背景

在政策层面，近年来国资委等国家有关部门通过出台一系列的政策，不断推动中央企业加强全面合规管理，加快提升央企依法合规经营管理水平。早在2012年，商务部、中央外宣办、外交部、发展改革委、国资委、预防腐败局等六个部委局和全国工商联就联合下发了《中国境外企业文化建设若干意见》，重点阐明了中国境外企业文化建设的九大内容，其中包括坚持合法合规，做到依法求生存、依法求发展。2015年12月，国资委发布了《关于全面推进法治央企建设的意见》，提出了到2020年，“中央企业依法治理能力进一步增强，依法合规经营水平显著提升，依法规范管理能力不断强化，全员法治素质明显提高，企业法治文化更加浓厚，依法治企能力达到国际同行业先进水平”的总体目标。在2017年初，为了规范中央企业的投资行为，国资委同时颁布了《中央企业投资监督管理办法》和《中央企业境外投资监督管理办法》两部规章。2017年5月，习近平总书记主持中央全面深化改革领导小组会议，审议通过了《关于规范企业海外经营行为的若干意见》。2017年底，《合规管理体系 指南》国家标准正式发布，并已于今年1月开始实施。去年，发改委会同四部委终于出台了

《企业海外经营合规管理指引》，要求企业确保对外贸易、境外投资、海外运营以及海外工程建设中全流程、全方位的合法合规，符合境内外法律法规和监管要求，避免重大合规风险。适逢中美贸易战开始，在执法层面，中国企业已经成为海外执法的重点关注目标之一。这种日趋复杂的国际贸易局势以及愈发复杂的制裁措施，也在督促着中国企业依法合规经营。

（二）《指引》对征求意见稿的重大调整

《指引》分为总则、合规管理职责、合规管理重点、合规管理运行、合规管理保障以及附则六个部分。整体而言，《指引》的规定言简意赅、简单明了，重点突出，也给了企业更多的空间来结合自身情况构建合规体系。具体而言，《指引》的核心内容主要体现在以下几个方面：

1. 合规标准明确化

实践中，央企、国企开展合规体系建设过程中，最常提出的一个问题就是：企业应该按照什么标准来设立合规制度？什么是合规？不解决这一问题，建立合规体系自然无从谈起。《指引》第二条就将颇具争议的合规标准问题加以明确：《指引》所称合规是指“中央企业及其员工的经营管理行为符合法律法规、监管规定、行业准则、和企业章程、规章制度以及国际条约、规则等要求”。

值得注意的是，党规党纪、商业惯例和道德规范虽然在理论上也属于“广义合规”的范畴，但并没有被《指引》明确列举。其中商业惯例与道德规范的范围较广，在不同的行业或文化领域可能存在不同的解读，边界较为模糊，将其纳入合规管理的主要标准，企业恐怕难以落实执行。而党规党纪则应该适用于企业内全体党员，但不一定适用于全体员工。近年来，央企在推进“走出去”和“一带一路”战略中扮演着重要的角色，无论是对境外投资还是境外业务的规模都显著增长，但在此过程中也不乏海外政府执法、多边银行制裁等带来的惨痛的经验与教训。因此，为了避免央企在海外遭受严重的处罚，明确要求企业及员工的行为符合国际条约与相关规则就显得十分必要。这一规定消除了很多企业的困惑，同时也为央企的合规管理奠定了基础，与时俱进地考虑到了央企在海外的合规管理需求。

2. 合规管理职责清晰化

在笔者以往协助央企进行合规建设的过程中，企业还常问到的一个核心问题是合规部门如何设置，合规职能如何划分，这也是构建合规体系最先要解决的问题之一。《指引》明确了“三道防线”：第一道防线是业务部门，一线业务人员是防范合规风险的第一道防线，业务人员及其负责人应当合规开展业务并在发现合规风险时主动向合规管理牵头部门报告；第二道防线是合规管理的牵头部门，往往由企业内部法律事务部门或合规部门担任。这些部门负责组织、监督和管理合规工作，是合规管理体系建设和实施的主要责任单位；第三道防线是内部审计和纪检监察部门，它们在其职责范围内履行合规管理职责，同时也能对公司整体合规管控措施起到监督的、评估作用。在领导层面，企业合规委员会与企业法治建设领导小组或风险控制委员会等合署，承担合规管理的组织领导和统筹协调作用。这样有利于企业内部承担风险管理职责的部门形成合力，齐抓共管，促进合规管理工作的顺利开展。

除此之外，《指引》还强调了合规管理牵头部门的客观独立原则，即合规管理牵头部门独立履行职责，不受其他部门和人员的干涉。这是对合规管理职能独立性的有力保障。

值得注意的是，《指引》虽然将合规管理的核心职

责清晰划分出来，但关于监察、审计、内控、风险管理、安全生产质量环保等相关部门具体如何履职，如何与合规部门相互配合，《指引》并没有做出强制要求，给企业留下了一些依据自身情况自由裁量与协调的空间。

在合规体系架构方面，我们在此前的《2016-2017中国合规及反商业贿赂调研报告》第三章“企业建立合规体系”中也进行了详细介绍，敬请参详。

3. 合规管理重点突出化

在《指引》的第十三条，国资委列举了七个需要企业关注的合规重点领域，其中包括：市场交易、安全环保、产品质量、劳动用工、财务税收、知识产权以及商业伙伴。实践中，对商业伙伴的管理其实至关重要，但很多企业认为第三方既然与公司没有任何关联关系，其不合规行为不会对企业造成影响，所以一直没有引起足够的重视。其实大量的违法违规行为是通过第三方进行的，例如大部分的FCPA执法均涉及第三方。近年来，国内外的执法机构都加强了对企业商业伙伴的审查和关注，例如，在美国司法部对于企业合规制度的指引中，特别强调公司是否结合第三方所在行业以及从事业务评估具体的风险等级并在合作前进行适当的尽职调查，如何应对在第三方尽职调查中发现的高风险信号，与第三方合作的条款是否合理完善，公司采取何种措施确保第三方切实履行合同，公司如何维护与第三方的关系，如何监督并促进第三方行为合规等问题。如今，随着国际局势日趋复杂，海外执法日趋活跃，加强对央企境内外商业伙伴的合规管理对于完善企业的合规管控，形成闭环的风险防范措施尤为重要。

根据《指引》，对商业伙伴领域的合规管理应当对重要商业伙伴开展合规调查，通过签订合规协议、要求对方作出合规承诺等方式促进商业伙伴行为合规。在这个方面，您可以参考《第三方选择阶段的合规管控：如何避免打开潘多拉魔盒》、《第三方合规管理机制：合作中的管控与矫正》以及《2015-2016中国合规及反商业贿赂调研报告》第三章第二部分“建立并完善第三方监督与管理机制”。

4. 海外合规管理全面化

《指引》在不同条款都强调了对海外业务合规管理的要求。

在海外人员管理方面，《指引》明确将“海外人员”也作为需要重点管理的人员。为了做到这一点，央企应“将合规培训作为海外人员任职、上岗的必备条件，确保遵守我国和所在国法律法规等相关规定”。

在海外投资经营方面，《指引》第十六条还要求央企强化海外投资经营行为的合规管理，深入研究投资所在国法律法规及相关国际规则，全面掌握禁止性规定；健全海外合规经营的制度、体系、流程，重视开展项目的合规论证和尽职调查；定期排查梳理海外投资经营业务的风险状况，重点关注重大决策、重大合同、大额资金管控和境外子企业公司治理等方面存在的合规风险，妥善处理、及时报告，防止扩大蔓延。这些要求也与《企业境外经营合规管理指引》的要求相呼应。在这个方面可以参考《2016-2017中国合规及反商业贿赂调研报告》第五章“对外投资中的合规尽职调查”。

5. 合规风险响应及时化

《指引》在合规管理运行一章中明确了保证合规机制顺利运行的几个方面指引。归纳起来，基本上将合规体系建立分为了事前、事中、事后三个阶段，并提出了风险应对的要求。在事前，企业应当建立健全合规管理制度，建立合规风险识别预警机制，加强合规风险应对，针对已发现的风险制定预案；在事中，如果发生了

合规风险，企业要采取及时有效应对措施。在企业的日常经营管理中，要将合规审查机制作为必经程序；在事后，要强化违规问责，同时开展合规管理评估，定期分析合规管理体系的有效性。

在实践中，企业往往普遍存在的一个误区，即企业如果具备了完善的合规管理制度体系，就不会出现重大的合规风险事件。其实，即使企业有着完备的合规体系，也无法完全排除发生合规事件的可能性。但完备的合规管理体系能够帮助企业及时发现风险并妥善应对。在合规管理体系建设过程中，很多企业主要将关注点集中在事前的制度设计方面，但其实正确、及时的合规风险响应机制和事后持续的改进与问责能够帮助企业化解风险、降低损失并且避免类似的风险再次出现。在应对调查和检查时，企业的配合程度和采取的补救措施有时候可能影响处罚的结果。积极的配合、正确的应对方式和及时的补救措施，可以将问题带来的负面影响最小化。因此，企业不仅应该针对合规风险制定相应的应急预案，还应该组织关键员工定期按照预案进行模拟演练，让制度不再停留于纸面。在这个方面可以参考《2015-2016中国合规及反商业贿赂调研报告》第三章第三部分“建立并完善危机应对方案和体系”。

6. 合规管理信息化

《指引》在“合规管理保障”一章中总结了六个重要的合规管理的保障，分别是合规绩效、合规信息化、合规职业人才、合规培训、合规文化、合规报告制度。其中强化合规管理信息化建设的要求是《指引》和征求意见稿都予以强调的、保障合规管理落实的重要措施。根据《指引》要求，央企应当通过信息化手段优化管理流程，记录和保存相关信息。运用大数据等工具，加强对经营管理行为依法合规情况的实时在线监控和风险分析，实现信息集成与共享（第二十四条）。由于现在很多央企的规模庞大、业务多样，若要实现精细化管理，单纯依靠人工进行合规管控往往会造成巨大的工作量，如果能够通过统一的内部审批信息系统处理规律性的具有统一标准的审批事项，则能够减少相当一部分工作量。信息化管理作为合规管理的一个重要保障是保证合规与效率兼顾的一个重要手段。在这个方面可以参考《2016-2017中国合规及反商业贿赂调研报告》第三章第四至七部分。

（三）央企合规体系构建建议

按照《指引》的要求，我们建议央企采取以下几个步骤构建自己的合规体系：建立组织机构、全面风险识别与评估、建立合规体系、合规体系落地执行和合规体系评估。

我们建议企业首先应当按照《指引》关于合规职责的要求，成立公司的合规委员会，确定合规负责人以及合规牵头部门，并明确各自的职责。

其次，由于大部分央企体量庞大，业务多样，员工众多，企业应当采用“以风险为基础”的方法，在开始建立合规体系之前全面排查、识别并评估集团及下属各个行业的子公司以及各业务线所面临的合规风险。在此基础上，综合考虑所在国家、所在行业的一系列风险因素后，对不同的合规风险进行梳理和初步评估，了解公司现有合规体系与外部规范要求的差异，制定总体规划，按重要性和紧迫性循序渐进地开展有针对性的合规体系建设。这些因素包括：合规风险后果的严重程度、该业务是否是公司的支柱性业务、该风险是否是执法热点、公司现有制度的完善程度以及是否曾经出现过此类风险等等。

之后，企业可以在以上基础上对企业的合规体系进行搭建，确保合规体系覆盖：事前预防、事中监督以及事后应对三个方面。比如：在各具体业务操作的规划阶

段，加入合规风险的识别与评估，事先对员工进行合规培训，培养员工的合规风险防范意识；在业务执行过程中，进行合规监督工作，确保相应合规流程得到执行；合规事件出现后应有完善的应对、补救及惩处措施来有效控制合规事件对企业造成的损失和影响，并降低类似事件今后再次发生的可能性。

为了使得公司制定的合规政策及相关操作指引能够被严格执行，公司应当建立健全合规审查机制，并定期就合规政策的执行情况进行检查，强化违规问责机制，让合规体系具备“牙齿”，而不仅是停留在纸面的“纸老虎”。企业可以考虑将合规管控流程纳入企业的信息化系统中。信息化系统能够帮助企业对于不同业务环节可能面临的合规风险点进行有效的管控和记录。与此同时，企业还应不断评估现有合规体系，尽量使其能够与企业的业务保持同步发展。

2018-2019
境外重大合规事件评述

一、境外反腐败执法综述

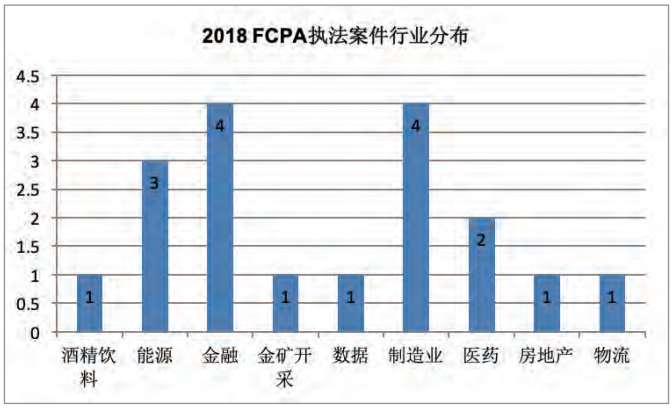
（一）FCPA执法动态

2018年是特朗普上台执政的第二年，FCPA执法势头较2017年也变得更加强劲。总体而言，2018年FCPA执法强度高于过去十年的平均值，但与创下纪录的2016年，其“成绩”并不是特别突出。

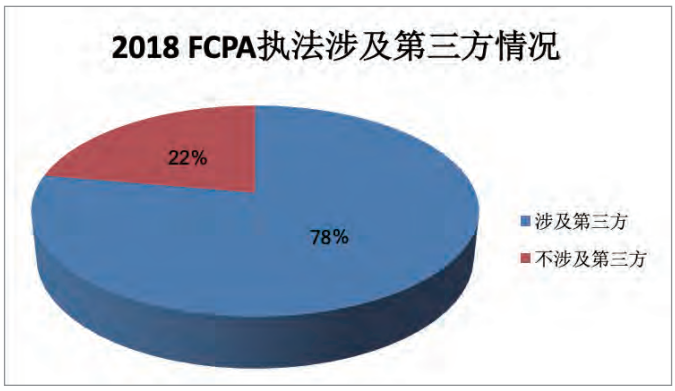
要点概览：FCPA执法势头不减，金融、制造业、能源和医药行业是FCPA 2018执法重点领域；三分之二以上案件涉及通过代理、经销商等第三方行贿，凸显第三方合规管控的重要性；中国成为FCPA最热点的执法区域，中美贸易战带来新挑战；《FCPA公司执法政策》（FCPA Corporate Enforcement Policy）适用范围扩大，凸显了M&A中合规尽调的重要性；多国政府联合执法打破和解记录。

1. FCPA 2018年执法特点

从行业层面来看，2018年被执法最多的行业是金融、制造业、能源和医药。值得一提的是，2018年的执法案件有一起涉及在中国通过贿赂政府官员非法获取企业及个人信息/数据的案例。

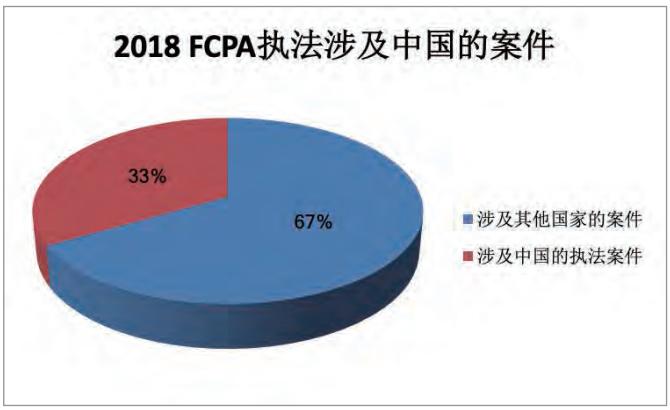


从贿赂的形式来看，有至少78%的案件涉及通过代理商、中介、经销商等第三方进行贿赂。这与FCPA执法历史上至少三分之二案件都涉及通过使用第三方进行贿赂的情况相符。FCPA执法机关建议，企业可通过实施有效的合规机制来降低第三方代理的风险，包括对第三方进行反腐败尽职调查。否则，企业故意通过第三方贿赂或施行鸵鸟政策，第三方的贿赂行为可能被视为企业的行为，企业可能因此承担FCPA下的法律责任。



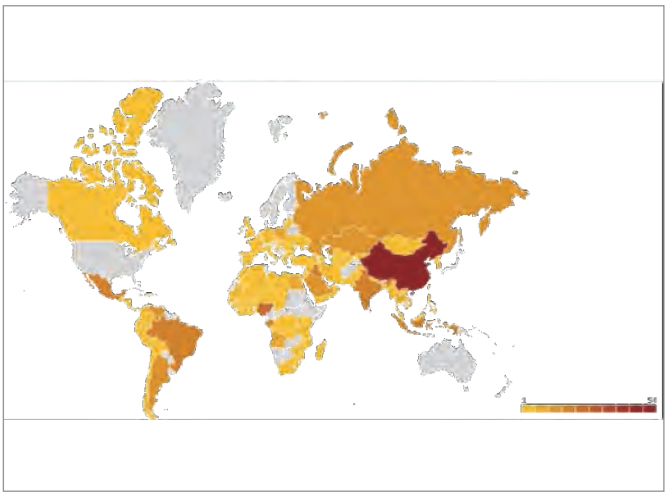
2. 中国成FCPA最热点执法区域，中美贸易战带来新挑战

2018年FCPA执法的企业案件中，其中有约33%的案件涉及在中国的行贿。



案件	主要违法事实	处罚依据
Panasonic Corp. 松下电器	其美国子公司向中国某国有航空公司某管理人员提供退休后年薪20万美金的咨询职位，以向国有航空公司销售其飞行娱乐和通信系统产品	反贿赂条款 会计条款
Stryker Corp. 史赛克公司	其中国子公司使用未经公司政策批准授权的分销商来销售公司产品，公司未实施有效的政策去发现和阻止这些未经授权的分销商，使得销售中支付不当利益的风险提高	会计条款
Credit Suisse Group AG 瑞士信贷银行	雇佣、晋升中国国有企业高管的亲属朋友以利用该高管影响力获得相关投行业务	反贿赂条款 会计条款
United Technologies Corporation 联合技术公司	其子公司向中国政府官员提供现金、礼品、旅游等好处以向国企销售其电梯设备	反贿赂条款 会计条款
Dun & Bradstreet 邓白氏公司	其在中国的2个子公司向中国官员行贿以获得未公开的企业财务状况信息，以及通过第三方获取未公开的个人信息及获得特定业务	会计条款
Polycom, Inc. 宝利通	其中国子公司向中国政府官员、国企客户中的关键人物提供好处以销售音视频会议系统	N/A（不起诉）

在FCPA四十多年的执法史上，中国是FCPA执法案件中发生贿赂行为最多的司法辖区。FCPA历史执法案件总计约260件，其中54起涉及在中国的行贿，远超于其他国家，涉及贿赂较多的其他国家包括尼日利亚（23起）、伊拉克（22起）、印度尼西亚（21起）、墨西哥（20起）、印度（19起）、加蓬（18起）、巴西（18起）、俄罗斯（15起）。[2]



在中美贸易战背景下，美国更是发起中国行动计划（China Initiative），旨在利用FCPA执法打击中国企业。美国时任司法部（DOJ）部长于2018年11月提出中国行动计划，并任命司法部国家安全局局长领导和执行该计划。[3]该计划旨在加强推行特朗普提出的国家安全总体战略，拟借助FCPA等美国法律，针对中国企业实施更广泛的“长臂管辖”，目标之一是查明涉及与美国企业竞争的中国公司的FCPA案件。中国企业需谨慎评估公司是否可能会受到FCPA管辖并采取预防措施。

3. 司法部扩大《执法政策》适用范围，凸显M&A合规尽调的重要性

美国DOJ助理副部长2018年7月25日在美国ACI会议第9届全球反腐败合规会议上宣布，司法部计划将《FCPA公司执法政策》（FCPA Corporate Enforcement Policy）（以下简称“《执法政策》”）适用于承继方（Successor Companies）在M&A中发现不合规行为后主动向司法部披露并积极配合的情况。[4]《执法政策》是DOJ在2017年11月由原试点计划（Pilot Program）衍变而来的一项永久政策，旨在鼓励企业在M&A活动中主动向DOJ报告目标公司可能存在的违法事实、积极配合调查以及整改，并给予企业更加透明的“奖励”（Credit）。

DOJ助理部长强调，如承继方在投前尽调发现可能违反FCPA的事项，DOJ鼓励其通过FCPA Opinion Procedure来询求DOJ意见，之后再决定是否采取进一步并购行动。FCPA Opinion Procedure是1993年DOJ开始实施的一项执法指导，如果企业对于涉嫌可能违反FCPA的事项向DOJ发起咨询，DOJ会将相应回复在官网公布供企业参考。这些指导在过去并未被企业所重视和参考，DOJ助理部长的讲话预示DOJ未来可能加大对该程序的使用力度。

2. Stanford Edu, available at http://fcpa.stanford.edu/statistics-analytics.html.
3. China Initiative Fact, DOJ, 2018-11-1, available at https://www.justice.gov/usao-ndtx/pr/usa-erin-nealy-cox-appointed-ag-s-china-initiative.
4. Deputy Assistant Attorney General Matthew S. Miner Remarks at the American Conference Institute 9th Global Forum on Anti-Corruption Compliance in High Risk Markets, 2018-7-25, available at https://www.justice.gov/opa/pr/deputy-assistant-attorney-general-matthew-s-miner-remarks-american-conference-institute-9th

对于投前未能发现但投后管控发现合规问题的，DOJ鼓励承继方采取《执法政策》里的步骤采取补救措施，并根据该政策对企业进行相应奖励。

DOJ这一计划无疑促使企业在今后的M&A活动，尤其是在腐败高发的国家开展投资活动时，加大对合规尽调的重视。早在2012年DOJ和SEC联合发布的《FCPA指南》(A Resource Guide to the U.S. Foreign Corrupt Practices Act)中，美国政府就鼓励企业投前开展合规尽职调查及投后加强合规机制及内控建设，以降低M&A活动相关的FCPA执法风险。根据《FCPA指南》，很多情形下，对于在M&A情形中可能涉嫌违反FCPA事项但及时主动向执法机关披露并积极配合的企业，最后执法机关都未发起执法活动。[5]

《执法政策》的适用范围扩大到M&A活动，无疑为执法机关提供了更明确的指导，也为企业减少了不确定性。FCPA“胡萝卜与大棒”的政策将激励更多企业重视和开展M&A相关的合规尽调。

4. 国际联合执法创下FCPA新纪录

多国政府联合执法在FCPA领域已并不稀奇，2018的FCPA多国政府联合执法创下新纪录。

2018年9月，Petrobras（巴西国家石油公司）向美国和巴西政府支付总计17.8亿美元以和解其在巴西的系统性贿赂，这一和解金额超过了西门子此前向美国和德国政府支付的16亿美元和解金额，成为FCPA历史总和解金额排名第一的案件。

值得注意的是，如果DOJ并未依据《执法政策》（FCPA Corporate Enforcement Policy）认定Petrobras符合罚金减免条件的话，Petrobras可能要再缴纳至少25%的罚金。显然FCPA执法机关现在更倾向于使用“胡萝卜”而非“大棒”来执法，鼓励更多企业去自我检举、自我调查、自我补救。

一般来说，涉及多国政府联合执法的往往也是大案要案，贿赂涉及的区域广、往往成为系统性贿赂，最后的和解金额也比较高。2018年的FCPA执法共有4个案件涉及多国政府联合执法，仅这4个案件支付给DOJ的刑事方面的罚没总金额就超过10亿美金。[6]美国政府已和英国、新加坡、巴西、法国、德国、瑞典、挪威、奥地利、土耳其等国政府达成了良好的合作关系，并且成功联合破获多起跨国公司腐败贿赂案。

多国政府联合执法已成FCPA执法常态，今后跨国企业发现在一国的潜在贿赂行为后一定要谨慎处理，避免产生蝴蝶效应，受到多国政府联合执法。美国司法部副部长General Rod J. Rosenstein在2018年第35届美国ACI会议上强调，任何想在其他司法辖区掩盖其欺诈行为的企业，都应当知道美国的“长臂管辖”。FCPA的“长臂管辖”及多国政府联合执法是跨国企业在今后经营中不得不重视的重要问题。

5. 美国司法部修改《执法政策》

美国司法部（DOJ）在2019年3月对《反海外腐败法》（FCPA）下的《FCPA公司执法政策》（FCPA Corporate Enforcement Policy）（“《执法政策》”）进行修订，其中一些修订引起业界较大关注。

《执法政策》是DOJ于2017年底公布的一项指导政策，旨在鼓励企业发挥主观能动性，在执法机关发起调查之前就自我检举、全力配合并采取适当和及时补救措施（“三大条件”），DOJ会据此对企业进行评估、嘉奖。只要企业满足前述三大条件且不存在规定的严重情形，DOJ会推定不起诉（Presumption of Declination）。

5. A Resource Guide to the U.S. Foreign Corrupt Practices Act, Joint Release by DOJ and SEC, P. 28.
6. Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the American Conference Institute's 35th International Conference on the Foreign Corrupt Practices Act, Oxon Hill, MD ~ Thursday, 2018-11-29, https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-american-conference-inst
7. Criminal Division Announces Publication of Guidance on Evaluating Corporate Compliance Programs, Department of Justice, 2019-4-30, available at https://www.justice.gov/opa/pr/criminal-division-announces-publication-guidance-evaluating-corporate-compliance-programs.

DOJ对该政策的修订进一步明确了企业获得合作奖励所应满足的条件。其中，DOJ要求企业对即时聊天软件实施适当管控最是引起业界关注。

在2017年公布的《执法政策》中，DOJ对即时聊天软件秉持完全禁止的态度。然而，从该政策实施至今，DOJ并未在公开的FCPA和解案件中援引该项规定对企业的补救措施（第三大条件）进行评价或认可。其中一项重要原因在于，企业在日常业务中依赖即时聊天软件与客户、合作伙伴等进行沟通，完全禁止该等工具的使用是不切实际的。从可操性出发，DOJ从此前的“完全禁止”修改为了“实施适当的指导和管控”（见如下针对本条修改前和修改后的政策对比）。

《执法政策》（2017）	《执法政策》（2019）
Appropriate retention of business records, and prohibiting the improper destruction or deletion of business records, including prohibiting employees from using software that generates but does not appropriately retain business records or communications.	Appropriate retention of business records, and prohibiting the improper destruction or deletion of business records, including implementing appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms that undermine the company's ability to appropriately retain business records or communications or otherwise comply with the company's document retention policies or legal obligations.
适当留存业务记录，并禁止不当销毁或删除业务记录，包括禁止员工使用可以生成但不适当留存业务记录或沟通的软件。	适当留存业务记录，禁止不当销毁或删除业务记录，包括：对私人通讯和“阅后即焚”平台的使用实施适当指导和管控，鉴于该等平台有损公司适当留存业务记录或沟通的能力，或者遵守公司文件留存政策、履行相关法律义务的能力。

其他主要修订还包括：为获得相应奖励，企业只需要披露实质性（Substantial）涉案人员，而非此前规定的全部涉案人员。DOJ在政策最后还做了一些说明，例如，如果企业在并购活动中发现目标公司存在潜在违反FCPA的行为，主动披露并积极采取补救、整合等措施的，DOJ便会根据《执法政策》对企业不起诉。

这一修订给依赖即时聊天软件开展业务的跨国企业带来新的挑战。以中国企业为例，微信是很多企业内部、外部工作和业务沟通普遍使用的工具；类似情况也存在于美国、韩国、日本、印度等国。显然，完全禁止该等工具的使用会极大影响企业开展业务的效率，与当前商业环境和沟通习惯不符。

从起初“完全禁止”到现在“适当管控”，体现了DOJ对该问题的关注，以及其在当前执法环境下对企业合规的期待。正因如此，DOJ正逐步让《执法政策》变得更加实用、更具可操作性。然而，从用语来看，《执法政策》在个案中仍给执法人员留了较大的解释空间，企业在实际执行时依然会有很多疑问。例如，企业具体需采取哪些措施、做到何种程度才为适当的（appropriate）管控？为了尽可能达到合规，企业是否需要完全禁止员工使用微信进行工作相关的沟通？企业是否需要购买专用软件或平台（例如企业版微信或钉钉）并要求员工使用且保存工作相关沟通记录？虽然存在众多疑问，但当前形势表明，DOJ把这个“皮球”踢给了企业，企业如不采取行动，将无法满足DOJ对企业合规的期待。

6. 美国司法部更新《企业合规机制评估指南》

2019年4月30日，美国司法部公布《企业合规机制评估指南》（Evaluation of Corporate Compliance Programs）（“《指南》”），该《指南》是检察官评估企业合规机制的指导性文件。事实上，该《指南》是司法部反欺诈科（Fraud Section）于2017年发布的《企业合规机制评估指南》的更新，旨在统一司法部其他指南和标准。该指南集成了多个部门的意见，包括副部长办公室、反欺诈科以及反洗钱和资产追查办公室（Money Laundering and Asset Recovery Section）。[7]

在发布该指南的公告中，司法部副部长称“有效的合规机制在阻止不合规行为、促进调查和达成公平和解中发

8. HM government, Anti-Corruption Newsletter: Spring 2019, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/796987/AC-newsletter-spring-2019.pdf.
9. SFO, New Joint Principles Published to Compensate Victims of Economic Crime Overseas, 2018-6-1, available at https://www.sfo.gov.uk/2018/06/01/new-joint-principles-published-to-compensate-victims-of-economic-crime-overseas/.
10. 该银行在2015年被我国的中国工商银行收购，目前的公司名称是ICBC Standard Bank PLC。

挥着至关重要的角色。本《指南》……确保检察官更加严格和透明地评估企业合规机制的有效性”。

该《指南》共分为三部分。第一部分主要讲如何认定企业合规机制是设计精良的（well-designed），涉及风险评估、公司政策与流程、培训和沟通、举报和调查流程、第三方管控、投资并购；第二部分是讲如何认定企业合规机制是有效实施的，包括中高管理人员的合规决心、合规部门的独立性与资源、奖惩措施；第三部分讲如何衡量企业合规机制是有效运行的，评估企业合规机制的持续改进、定期检查和审阅、不合规行为的调查及不合规行为的根源分析与补救。

DOJ对《执法政策》和《指南》的修订体现了其在FCPA执法中对企业合规机制的重视。

（二）英国反腐败动态

1. 英国设立一项4500万英镑的反腐败专项计划

英国于2018年10月批准了一项4500万英镑的全球反腐败专项计划（Prosperity Fund Global Anti-corruption Programme）。该计划致力于通过和其他政府之间的合作来打击腐败、推进全球贸易，为企业提供公平的竞争机会。[8]

2. 英国三家执法机构就适用补偿救济（Compensation）达成共识

2018年6月1日，英国的三家执法机构皇家检察署（Crown Prosecution Service）、国家犯罪调查局（National Crime Agency, NCA）、重大欺诈案件调查局（Serious Fraud Office, SFO）达成一项共识：在特定的案件（包括腐败案件）当中可以采取补偿救济（Compensation），将相关的财产退还给受损的国家、公司、个人。三家执法机构同意在之后的每一个案件中考虑补偿救济。据统计，三家机构自2014年以来在五个案件中对海外受害者退还的金额达到4920万英镑。[9]

3. SFO宣布英国第一份延迟起诉协议（Deferred Prosecution Agreement, DPA）执行完毕

标准银行（Standard Bank PLC）[10]因违反2010年《反贿赂法案》（Bribery Act 2010）被SFO调查并与SFO达成了英国历史上第一份延迟起诉协议（DPA）。该DPA要求目标公司支付2600万美元的罚款，向坦桑尼亚政府支付600万美元的损害补偿，并且必须雇佣一名外部顾问负责向SFO汇报在反腐败方面的内控、整改措施。2018年11月30日，SFO宣布该DPA执行完结。[11]

4. 打击经济犯罪联席委员会（Economic Crime Strategic Board）成立

在英国内政大臣（Home Secretary）和财政大臣（Chancellor of the Exchequer）的呼吁之下，英国于2019年1月14日成立打击经济犯罪联席委员会（Economic Crime Strategic Board），委员会的成员来自政府及执法部门的高层官员。该委员会致力于通过协调行动来分配资源、协调目标以打击经济犯罪。[12]

5. 派特法公司（Petrofac）前全球销售总监David Lufkin因海外行贿获刑

派特法公司（Petrofac）是全球知名的为石油和天然气行业提供油田服务的供应商。它在泽西岛注册，主要办事机构位于伦敦，在伦敦证券交易所上市，在全球多个国家从事商业活动。

11. SFO, UK's First Deferred Prosecution Agreement, between the SFO and Standard Bank, Successfully Ends, 2018-11-30, available at https://www.sfo.gov.uk/2019/02/07/former-senior-executive-convicted-in-petrofac-investigation/.
12. HM government, Anti-Corruption Newsletter: Spring 2019, available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/796987/AC-newsletter-spring-2019.pdf.
13. SFO, Former Senior Executive Convicted in Petrofac Investigation, 2019-2-7, available at https://www.sfo.gov.uk/2019/02/07/former-senior-executive-convicted-in-petrofac-investigation/.
14. (7) In subsection (4)(a), "politically exposed person" means a person who is (a) an individual who is, or has been, entrusted with prominent public functions by an international organisation or by a State other than the United Kingdom or another EEA State, (b) a family member of a person within paragraph (a), (c)known to be a close associate of a person within that paragraph, or (d)otherwise connected with a person within that paragraph.

2019年2月6日，派特法公司（Petrofac）前全球销售总监David Lufkin在法庭中承认行贿的事实，他通过行贿来为公司争取重大合同，其中在伊拉克的合同金额超过7.3亿美元，在沙特的合同金额超过35亿美元。他的行为违反了《反贿赂法案》（2010 Bribery Act）。英国SFO正在针对派特法公司（Petrofac）开展集中调查。[13]

6.《刑事金融法案》（Criminal Finances Act）中的不明财产法令（Unexplained Wealth Order）和没收（Forfeiture）措施被执法部门首次使用。

作为2017年《刑事金融法案》（Criminal Finances Act）的一部分内容，不明财产法令（Unexplained Wealth Order）在2018年1月31日生效。这项命令要求财产权主体就特定财产的来源做出解释，主要是一些与其收入情况不相符的财产。有权使用该法令的执法机构有：英国国家犯罪调查局（National Crime Agency，NCA），英国税务及海关总署（Her Majesty's Revenue and Customs，HMRC），英国金融市场行为监管局（Financial Conduct Authority，FCA），英国重大欺诈案件调查局（Serious Fraud Office，SFO）。该法令只能适用于政治公众人物（Politically Exposed Persons，PEP）或者有重大犯罪嫌疑的主体。英国的《犯罪获益法》（Proceeds of Crime Act 2002）第362（B）（7）条将PEP定义为：被国际组织或外国政府授予公职的人。 该法令首次于2018年10月对Zamira Hajiyeva女士适用，她被要求就一处房产做出解释。她的丈夫曾担任阿塞拜疆一家国有银行的高管，因职务犯罪获刑。[15]

2017年通过的《刑事金融法案》（Criminal Finances Act）首次允许执法部门对罪犯在不法活动中获得的或者用于从事不法活动的银行账户内的资产采取冻结（Freeze）、没收（Forfeit）措施。2019年3月15日，SFO决定没收罪犯Nisar Afzal的多达150万英镑的资产，该笔资产是从事不法活动所得。SFO在该案中首次使用《刑事金融法案》（Criminal Finances Act）所确立的该项执法措施。[16]

7. 一些反腐败案件获得新的进展

2019年2月22日，SFO宣布结束劳斯莱斯(Rolls-Royce)案。劳斯莱斯（Rolls-Royce）是一家专业从事涡轮产品生产的英国公司。在劳斯莱斯（Rolls-Royce）案中，目标公司及其子公司涉嫌在印度尼西亚、泰国、印度、俄罗斯、尼日利亚、中国、马来西亚从事长达三十年的贿赂活动。最终SFO与目标公司达成了延迟起诉协议（DPA），目标公司须支付罚金4.97亿英镑。SFO综合考虑证据及公共利益决定将不对目标公司中的个人提起控诉。[17]

阿尔斯通公司（Alstom Power）是一家大型法国公司，总部位于法国巴黎附近，其主要业务为电力及轨道交通基础设施。2018年12月21日，阿尔斯通公司的前全球销售主管因行贿罪被判处4.5年刑期。公司涉嫌在立陶宛对政府官员行贿，涉及的合同金额达到2.4亿欧元。公司被SFO指控的其他腐败行为还有：在突尼斯、印度、波兰等国家的有轨电车及信号设备采购中行贿；在立陶宛的两个发电站项目中行贿；在匈牙利的铁轨车辆采购中行贿。[18]

Unaoil是一家总部位于摩纳哥的公司，由Ahsani家族成立于1991年。据Unaoil称，它为中东，中亚和非洲的能源部门提供“工业解决方案”。这家公司涉嫌在伊拉克从事腐败活动。SFO对目标公司的调查开始于2016年3月。2018年5月22日，SFO宣布对Unaoil公司两名责任人提出指控，这两名员工Basil Al Jarah和Ziad Akle涉嫌向礼顿建筑公司（Leighton Contractors Singapore PTE Ltd）行贿以获得超过7.33亿美元的

15. Hayley Humphries and David Odejayi, Azerbaijani Couple at the Centre of UK's First Unexplained Wealth Order, 2018-10-22, available at https://www.lexology.com/library/detail.aspx?g=48417bd4-34b7-477f-a40a-09a8a5cd81ef.
16. SFO, SFO Nets £1.52m from Convicted Birmingham Fraudster, 2019-3-15, available at https://www.sfo.gov.uk/2019/03/15/sfo-nets-1-52m-from-convicted-birmingham-fraudster/.
17. SFO, SFO Closes Glaxosmithkline Investigation and Investigation into Rolls-Royce Individuals, 2019-2-22, available at https://www.sfo.gov.uk/2019/02/22/sfo-closes-glaxosmithkline-investigation-and-investigation-into-rolls-royce-individuals/.
18. SFO, Former Alstom Power Global Sales Director Sentenced to 4.5 Years for Corruption, 2018-12-21, available at https://www.sfo.gov.uk/2018/12/21/former-alstom-power-global-sales-director-sentenced-to-4-5-years-for-corruption/.

合同，项目内容是在伊拉克南部建立两条石油管线。2018年6月26日，SFO将刑事诉讼的起诉文书送达目标公司。2018年12月21日，员工Stephen Whiteley接到指控。[19]

（三）法国反腐败动态

1. 法国国家金融监察局与美国司法部第一次开展反腐败联合行动

2018年6月4日，法国国家金融监察局（French National Financial Prosecutor's Office, PNF）与美国司法部对一家法国大型金融机构——法国兴业银行作出联合执法处罚。此项行动中，两家机构就罚款问题进行了协调。此项行动意味着美国、法国的联合执法关系有了进一步发展。在过去几年里，就美国对几家法国公司如 Alcatel-Lucent S.A.，Alstom S.A.，Technip S.A.，and Total, S.A. 的执法行动，法国曾拒绝配合并指责美国对外国公司的管辖。[20]

2. 法国根据《萨宾第二法案》公布《合规指引》

2019年2月4日，法国反腐败执法机构根据《萨宾第二法案》（Loi Sapin II）的要求公布新的《合规指引》（Anticorruption Compliance Guide），该指引致力于帮助公司建立合乎要求的合规制度。指引指出，公司应该根据自己的具体情况建立合规系统。指引还建议公司任命一名合规官（Compliance Officer），公司必须为合规官及合规团队提供充足的资源。合规官的职责并不仅限于反腐败，还应该扩展到反洗钱、内部交易等领域。尽管指引的内容大多是建议性的，但是公司对该指引的遵循程度将影响执法机构对该公司检查时的评分。指引明确指出公司的CEO应该对合规工作负责，公司、CEO及合规官应该对反腐败机制的缺失承担责任。[21]

（四）巴西

巴西公布反腐败罚金的确定标准。2019年4月3日，巴西反腐败执法机构国家审计署（Office of the Comptroller General, CGU）公布了更为明确统一的罚金计算标准，各家公司可以在其合规项目中采取有针对性的应对措施。[22]

（五）阿根廷

1. 2018年，阿根廷发生“笔记本事件”（Notebook Scandal），腐败事件波及包括前总统（克里斯蒂娜）在内的多名高级别官员

“笔记本事件”被认为是与巴西“洗车行动”比肩的重大腐败事件。据报道，受雇于前任政府高官的一名私人司机在其8本笔记本中详实记录了2005年至2015年期间他给政府官员运送装在袋子里的大量现金的细节。这段时间正是基什内尔与克里斯蒂娜相继担任阿根廷总统的期间。在他记录的信息中，其中两处地址是阿根廷时任总统克里斯蒂娜的私人住址和总统府。检方称在2005年至2015年前总统（克里斯蒂娜）收到1.6亿美元的贿金。随着该事件持续发酵，阿根廷司法部门开始介入调查，包括前政府总理、多位部长和国务秘书，以及国有和私人大型企业负责人在内的十几人遭到逮捕。阿根廷检察官表示，这些互相关联的刑事案件里，贪污的贿款总额可能高达1.6亿美元（约合10.9亿元人民币），不排除还会有进一步逮捕行动。[23]2017年11月，前副总统Amado Boudou被捕。[24]

2. 阿根廷反腐败局发布合规指引（Compliance Guidance）

根据阿根廷在2017年发布的《公司刑事责任法案》

19. SFO, Further Charge Against Individual in SFO's Unaoil Investigation, 2018-12-21, available at https://www.sfo.gov.uk/2018/12/21/further-charge-against-individual-in-sfos-unaoil-investigation/.
20. Richards Kibbe & Orbe LLP, U.S. and France Ride New Wave of Anti-Corruption Cooperation, 2018-6-15, available at https://www.lexology.com/library/detail.aspx?g=0929003b-1e52-4767-a10f-e9a47d73d9fe.
21. French Anticorruption Agency Sets the Pace: New Anticorruption Compliance Guide Just Published, 2019-3-8, available at https://www.jdsupra.com/legalnews/french-anticorruption-agency-sets-the-66282/.
22. Heloisa Uelze, Alessandro da Cruz, Marcelo Leite and Fernanda Casagrande, Brazil: Manual for Calculation of Fines in Sanctioning Administrative Proceedings is Published, 2019-4-3, available at https://globalcompliancenews.com/brazil-manual-calculation-fines-sanctioning-administrative-proceedings-published-20190318/.
23. 何蔚, 8本笔记本揭开前政府惊天贪腐案 阿根廷前女总统“悬了”, 2018-8-25，http://news.hsw.cn/system/2018/0825/1017791.shtml.

（Law on Corporate Criminal Liability, CCL）第22、23条，参与特定政府项目、政府招标的企业必须建立完善的合规机制。针对此项规定，阿根廷反腐败局（Anti-Corruption Office）于2018年10月6日发布27/2018号法令，对企业的合规机制提出了具体要求。[25]

3. 阿根廷通过2019-2023年反腐败计划（National Anti-Corruption Plan）

2019年4月10日，阿根廷以政府法令Decree No. 258/2019发布新的反腐败五年计划。该计划致力于协调反腐败工作，确立工作重点，遵循国际条约，涉及规制商业贿赂（integrity in private sector）、机构调整、民众参与、反腐败教育。公告中还为每一项内容设置了实施时间。该法令还成立了诚信委员会（“Ad honorem”advisory council），由一些知名专家组成，委员会负责监督反腐败计划的执行。[26]

（六）厄瓜多尔

厄瓜多尔成立国际反腐败委员会（International Anti-Corruption Commission）。2019年2月25日，厄瓜多尔的反腐败大臣（Anti-Corruption Secretary）、财务部长出席了第一次会议。国际反腐败委员会的三个工作目标是：预防腐败、腐败调查、执法。委员会将与联合国、美洲国家合作组织（Organization of American States）、美洲国家发展银行（Inter-American Development Bank）、透明国际（Transparency International）开展合作。委员会的主要职责是配合其他反腐败执法部门的工作。[27]

（七）爱尔兰国际反腐败改革

2018年5月，爱尔兰司法部长向立法机关上议院提交了《刑事司法（腐败违法行为）法案》，该法案是爱尔兰政府2017年打击白领犯罪计划的核心部分，也将使爱尔兰履行其国际反腐败相关承诺。该法案将引入一些新的罪行，并扩大爱尔兰反腐败法的范围。新法案包括“主动和被动腐败”的一般罪行，适用于利用职权、雇佣或业务进行腐败行为的任何主体。该法案适用于爱尔兰的企业和个人，不论其腐败行为发生在世界任何地方，也不论相关腐败行为在行为发生地是否构成犯罪。与英国《反贿赂法案》类似，爱尔兰新法案规定，如果企业可以证明其采取了合理的措施并进行了尽职调查以阻止违法行为，则企业可以提出抗辩。[28]

2018年6月5日，该法案被总统签署并正式纳入国家法律。[29]

（八）阿联酋国际反腐败改革

阿联酋从2018年开始发起了一系列重要举措。第一，发布《反洗钱法案》以打击金融犯罪。电子货币首次被纳入规制范围，允许执法机关使用钓鱼执法（sting operation）。第二，修改刑法当中腐败犯罪的相关规定。对外国公职人员行贿被纳入犯罪行为。阿联酋刑法典第一次规定域外效力：对于给阿联酋造成影响或者涉及阿联酋国民或居民的犯罪行为，阿联酋具有管辖权。这标志着阿联酋的反腐败工作与国际更为接轨。第三，加强与国外执法机构的合作，如美国的财政部。阿联酋和美国联合打击与伊朗相关的货币交易。第四，加强执法机构的权力和责任。阿联酋在金融执法部门——迪拜金融服务局（Dubai Financial Services Authority）和金融服务监管局（Financial Services Regulatory Authority）任命多名重要官员，还修改了一些金融监管法规。[30]

（九）澳大利亚通过《保护告密者法案》（Whistleblowing Bill）

24. BUENOS AIRES, Argentina Congress Passes Law to Fight Corporate Corruption, 2017-11-09, https://news.yahoo.com/argentina-congress-passes-law-fight-corporate-corruption-234306401--finance.html.
25. Fernando Goldaracena, Vanina Caniza and Luis, Argentina, Guidelines for the Implementation of Compliance Programs Issued by the Anti-Corruption Office, available at https://globalcompliancenews.com/argentina-guidelines-for-the-implementation-of-compliance-programs-issued-by-the-anti-corruption-office/.
26. Fernando Goldaracena, Vanina Caniza and Luis, Argentina, Guidelines for the Implementation of Compliance Programs Issued by the Anti-Corruption Office, 2018-10-6, available at https://globalcompliancenews.com/argentina-guidelines-for-the-implementation-of-compliance-programs-issued-by-the-anti-corruption-office/.
27. Cari Stinebower, Rebecca Toro Condori and Alexandra Solórzano, Ecuador Cracking Down on Corruption, 2019-2-25, available at https://www.cmtradelaw.com/2019/02/ecuador-cracking-down-on-corruption/.
28. Irish Anti-Corruption Law Reform Moves One Step Closer, 2018-5-11, available at https://www.out-law.com/en/articles/2018/may/irish-anti-corruption-law-reform-closer/.
29. Criminal Justice (Corruption Offences) Act 2018, the Houses of the Oireachtas, available at https://www.oireachtas.ie/en/bills/bill/2017/122/.

《保护告密者法案》的全称是《2018年财政部法律修正案（加强告密者保护）法案》(Treasury Laws Amendment (Enhancing Whistleblower Protections) Bill 2018)，在2019年2月19日得到国会通过，3月12日获得御准(Royal Assent)，将于2019年7月1日生效。该法案的主要内容有：增加可以获得保护的“保密者”的范围；在特定的紧急情况下，可以向媒体或者国会披露告密信息；增加对告密者的保护措施，允许受到公司迫害的告密者诉求赔偿；要求国有或大型私有公司在法案生效后六个月内建立告密机制。[31]

（十）意大利通过一项反腐败领域修正法案

2019年1月31日，意大利的一项新反腐败修正法案生效，法案全称为：《关于打击违反公共管理相关犯罪及政党活动诉讼时效和透明性的措施》（Measures to Fight Crimes against the Public Administration as well as on the Matter of Statute of Limitations and Transparency of Political Parties and Movements）。

法案对意大利刑法典有多处修改：第一，增加贿赂犯罪的刑期，最低期限从一年提高到三年，最高期限从六年提高到八年。第二，增加新的刑罚方式，例如永久禁止参与政府项目、永久禁止担任公职。第三，对于持续性犯罪，追诉时效从犯罪终止时开始计算。追诉时效在第一次判决生效时中止，在最终判决生效时继续计算。第四，将利用影响力犯罪（Trafficking in Illegal Influence）确定为新的犯罪。第五，触犯侵占罪、对司法人员行贿罪、利用影响力犯罪（Trafficking in Illegal Influence）的，可能被禁止参与政府项目。第六，自首或提供重要信息的，减轻或免除刑罚。

该法案对商业贿赂施加了民事责任，其中最大亮点是增加了禁业惩罚的期限，禁业惩罚的内容有：停止公司营业、禁止参与政府项目、撤销相关证照。[32]

（十一）印度尼西亚法院判决NKE公司承担刑事责任

2019年1月3日，印尼反腐败法庭（The Corruption Court）判决NKE公司（PT Nusa Konstruksi Enjiniring, Tbk）在8个政府项目中构成行贿。

在印尼最高法院2016年12月发布《公司犯罪案件处理手册》（Case Handling Procedures for Corporate Crimes）不久，执法机构反腐败局（Corruption Eradication Commission）对NKE公司开始反腐败调查。NKE公司是印尼一家从事建筑行业的大型上市公司。在法院审理NKE案之前，NKE的前总裁Dudung Purwadi已经因在两项政府工程中从事腐败活动而获刑，刑期为四年零八个月，罚金1.8万美元，返还在两个项目中的非法获益（103.6万美元、263.8万美元）。2019年1月3日，法院判决NKE在多达八个政府项目中构成贿赂罪。

根据印度尼西亚刑法，公司犯罪可能获得的刑罚有：罚款、没收财产、返还非法获益、停止营业。本案NKE受到的处罚是：罚金5万美元、返还非法获益611.7万美元、六个月内禁止参加政府招标。

NKE一案标志着印尼法院在处理公司犯罪案件中就如何计算责任范围走向成熟。公司应该返还其在腐败项目中获得的不法利益。NKE在八个项目中的非法获益是1717.4万美元，法院将此数额减去贿金等费用，最终确定NKE需要返还的利益是611.7万美元。仅仅在2018年，反腐败执法机构已经调查了四起以公司为主体的腐败案件。[33]

30. Borys Dackiw, Matthew Shanahan, Mazen Boustany, Andre Abou Aad and Laya Aoun-Hani, UAE: Strengthening Compliance against Financial Crime: Recent Developments and Enforcement Trends in the UAE, 2019-4-4, available at https://globalcompliancenews.com.
31. Georgie Farrant and Michael Michalandos, Australian Parliament Passes Whistleblowing Bill, 2019-3-26, available at https://globalcompliancenews.com/australian-parliament-passes-whistleblowing-bill-20190219/.
32. Riccardo Ovidi, Italy's New Anti-Corruption Law, 2019-3-15, available at https://globalcompliancenews.com/italys-new-anti-corruption-law-20190228/.
33. Andi Yusuf Kadir, The Cost of Corruption for Corporations in Indonesia: Takeaway from Recent Enforcement of Corporate Criminal Liability, 2019-2-15, available at https://globalcompliancenews.com/cost-corruption-corporations-indonesia-takeaway-recent-enforcement-corporate-criminal-liability-20190122/.

（十二）俄罗斯通过一项反腐败领域修正法案

2018年8月14日，俄罗斯一项反腐败领域修正法案生效。根据该修正法案，触犯国内贿赂犯罪的公司主动配合调查、主动披露信息的，可以减轻或免予处罚。法院在审理腐败案件中可以冻结公司的相关财产，冻结的最大数额可以是公司可能受到的罚款。法院在审查来自检察机关的冻结请求时不必通知目标公司。[34]

（十三）泰国通过《2018反腐败法案》（2018 Anti-Corruption Act）

2018年7月22日，泰国《2018反腐败法案》（2018 Anti-Corruption Act）生效，该法案取代了《1999反腐败法案》。该法案带来的一项重大变革是将在泰国从事商业活动的域外公司纳入管辖。对于公司为责任主体的案件，公司可以举证已经建立合理的防控机制作为抗辩。公司可能受到的最大处罚金额为非法获益或造成损失的两倍。[35]

（十四）马来西亚通过一项反腐败领域修正法案，首次确立“公司责任”

2018年10月10日，马来西亚一项反腐败领域修正法案生效，法案的全称是《2009年马来西亚反腐败委员会修正案》（Amendments to the Malaysian Anti-Corruption Commission Act 2009）。法案的主要内容是将公司作为腐败犯罪的责任主体，通常又被称为是“公司责任条款”（Corporate Liability Provisions）。利益关系人从事腐败活动的，公司（包含本国公司及外国公司）应该承担刑事责任。“利益关系人”可以是公司董事、职员以及第三方服务提供者。法案对公司施加的是严格责任，即便公司宣称对利害关系人的行为不知情也应该承担责任。公司可以将已经建立完善的防控措施（Adequate Procedures）作为免责抗辩。公司触犯腐败犯罪的，其董事、高管被推定犯同样罪行，除非能够证明自身不知情或者已尽到注意义务。作为应对，广大公司应该定期监督自己的员工等利害关系人，定期审查自身的相关制度。[36]

（十五）乌克兰宣布成立反腐败法庭（Anti-Corruption Court）

2019年4月11日，乌克兰总统宣布专门法庭——反腐败法庭成立，致力于加强法官在审理腐败案件时的独立性。当天有28名法官宣誓就职。成立该法庭属于乌克兰与国际货币基金组织之间一个39亿美金合作项目的部分内容。[37]

34. Paul Melling, Anton Subbot, Edward Bekeschenko and Maxim Kalinin: Russia: Important Amendments to the Procedure for Prosecuting Companies for Bribery, 2018-9-3, available at https://globalcompliancenews.com/russia-procedure-prosecuting-companies-bribery-20180903/.
35. Peerapan Tungsuwan and Yuthana Sivaraks, The new Anti-Corruption Act: Clearly Defined to Cover Foreign Juristic Persons Registered Abroad, 2018-8-10, available at https://globalcompliancenews.com/anti-corruption-thailand-20180810/.
36. Brian Chia, Kherk Ying Chew, Eddie Chuah and Adrian Wong, Malaysia Introduces “Corporate Liability” Bill, 2018-4-6, available at https://globalcompliancenews.com/malaysia-corporate-liability-20180406/.
37. Ukraine Launches Long-Awaited Anti-Corruption Court, 2019-4-12, available at https://www.aljazeera.com/news/2019/04/ukraine-launches-long-awaited-anti-corruption-court-190411153101996.html.

二、境外数据保护执法综述

自欧盟《通用数据保护条例》（General Data Protection Regulation, “GDPR”）于2018年5月28日生效以来，经过一年多的积累，欧盟各数据保护监管机构的执法已经逐步步入成熟期。其他国家和地区也纷纷跟随GDPR的步伐加强了在数据保护领域的立法和执法工作。日趋严格的数据保护立法和执法无疑对“走出去”的中国企业提出了新的挑战。本篇将主要梳理过去一年全球主要地区的数据保护执法情况，并就未来的执法趋势进行预测，以期为大家提供参考。

（一）欧盟GDPR执法综述

1. 从“软执法”到“硬执法”

自GDPR生效以来，虽然欧盟各数据保护监管机关均收到了大量的投诉和数据泄露报告，但是实际执法比例并不高。根据欧盟数据保护委员会（European Data Protection Board, “EDPB”）的官方统计，截止2019年5月22日，各成员国接收和处理（中）的GDPR相关案件累计已经超过28万件，但是根据公开的数据，

过去一年真正执法和处罚的案例不足100件，比例相对较低。[1]究其原因，一方面面对刚刚生效的GDPR，各监管机构也尚处于准备阶段，人力和物力不充足，而且还投入了较多的精力用于开展市场调研和制定实践指南；另一方面，鉴于GDPR很多规则仍尚待理清，监管机构在过去一年主要以回应企业咨询和软执法为主，对违反GDPR规定的企业往往会首先给予较长时间的缓冲和整改期。

数据来源：EDPB[2]

但是随着第一年探索期的结束，数据保护监管机构多已经积累了较为充分的执法经验，并且多数监管机构从国家预算层面也获得了人力和物力方面的资源支持，特别是考虑到目前各监管机构仍有大量的案件积压，预计2019年和2020年GDPR相关的处罚案例会趋于活跃，且罚金额度也将会有一定程度提高。从英国数据保护监管机关（Information Commissioner’s Office, “ICO”）近期拟对一家航空公司（£183.39M）和一家酒店（£99.2m）的罚额也可以窥见一斑。

2. 执法基本涵盖GDPR的各方面要求

纵观公开的GDPR执法案例，可以看出各监管机关的执法几乎涵盖了GDPR的各个方面的要求，其中各个监管机构更为关注的是GDPR第5条规定的各项数据保护基本原则。例如：

- 法国CNIL对Google的处罚（€50,000,000）：未向个人信息主体充分告知如何收集和使用其个人信息；未取得用户的有效同意；缺乏法律基础。

1. http://www.enforcementtracker.com/，最后访问时间2019年10月14日。
2. 1 year GDPR-taking stock, https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en，最后访问时间2019年10月14日。

- 葡萄牙数据保护监管机构对一家医院的处罚（€400,000）：账户权限设置不符合最小化原则；未采取适当的技术措施保护数据安全。

- 德国巴登符腾堡州数据保护监管机构对一家社交媒体公司的处罚（€20,000）：未采取适当的技术安全措施（未加密存储用户密码）。

- 德国巴伐利亚州数据保护监管机构对一家企业执法（€50,000）：未与数据处理者签订数据处理协议。

- 希腊数据保护监管机构对电信公司OTE处罚（€400,000）：未及时更新存储的个人数据（违反数据准确性的要求）；未能及时响应数据主体退出商业推广信息的请求；上述行为因企业未采取技术措施和组织措施（违反privacy by design的要求）。

此外，虽然目前数据保护监管机构的执法案例主要是针对数据控制者，但是也不排除将来监管机构对处理者执法。并且，高额的罚金也会驱使控制者提高对处理者的要求，例如提高合同违约责任限额，从而将数据保护的义务转嫁至处理者。

正如英国ICO的信息保护委员（Information Commissioner）Elizabeth Denham在2019年数据保护从业者大会（Data Protection Practitioners' Conference）中提到，GDPR的问责制（Accountability）要求企业进行数据合规“不仅仅是勾选框和数据处理记录”，“GDPR的下一个阶段需要关注全面的数据保护，即在业务运营的各个流程纳入数据治理”。[3]对于可能落入GDPR管辖范围的中国企业来说，需要尽早将GDPR的合规纳入日程，建立全面和可持续的合规项目。

（二）美国数据保护执法综述

1. FTC将可能获得更为广泛的执法权

美国联邦贸易委员会（Federal Trade Commission, “FTC”）是美国最主要的数据保护执法机构。根据美国政府问责局（GAO）的统计，自2008-2018年美国FTC已经就数据保护问题共计进行过逾100次执法，FTC在多项政府报告中也指出隐私保护和数据安全仍是其执法重点领域。但是FTC目前的执法权限有所限制，仅限于对违反《美国联邦贸易委员会法》（FTC Act）、违反与FTC的和解协议以及COPPA等特定领域的不合规行为进行处罚。FTC已经多次在正式的报告中请求扩大其执法权，并且也已经得到多个政府部门的支持。特别是，如果未来美国制定联邦统一的数据保护法后，FTC将有望担任联邦数据保护监管机构，从而获得更广泛的执法权。

2. 儿童个人信息保护不容小觑

《儿童在线隐私保护法》（Children Online Privacy Protection Act, “COPPA”）一直是美国FTC进行执法的重点。2019年，FTC因违反COPPA的规定分别对美国版抖音（Musical.ly）和YouTube处以570万美元和1.7亿美元的处罚。而且需要注意的是，美国COPPA具有域外适用效力，即使未在当地设立公司，也有可能落入到COPPA的管辖范围，例如在Mucical.ly案中FTC即是对Musical.ly Inc（美国公司）和其在开曼的母公司（Musical.ly）共同执法。2019年5月，FTC致函位于乌克兰的约会应用程序提供商Wildec. LLC，要求其删除未经监护人同意收集的13周岁以下儿童的个人信息。 因此，对于已经或者计划在美国市场开展业务的中国企业来说，不管是否涉及在当地设立公司，均需要审慎判断其业务范围是否可能落入到COPPA的适用范围。

3. Elizabeth Denham's speech at the Data Protection Practitioners' Conference on 8 April 2019，
https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/04/data-protection-practitioners-conference-2019/，最后访问时间2019年11月11日。

根据COPPA、美国FTC制定的《COPPA实施规则》以及相关的案例，判断COPPA的适用与否可以参考以下标准：COPPA适用于（1）“针对儿童”（directed to children）提供服务的网站或在线服务的提供者，或（2）“事实上明知”（has actual knowledge）其收集了13周岁以下儿童个人信息的网站或在线服务的提供者。

- 判断是否“针对儿童”（directed to children）可基于以下因素：网站或在线服务的主题、视觉内容、动画形象或其他以儿童为导向的活动、激励、音乐或其他音频内容、模特的年龄、儿童名人或儿童感兴趣的名人、语言或者其他因素。FTC也会参考网站或在线服务的目标群体构成或者有意吸引的目标群体的相关证据。但是，即使网站或者在线服务根据上述因素判断是“针对儿童”提供，而其主要目标用户并非儿童的，即（i）该网站或在线服务在收集年龄信息之前未收集任何访客的个人信息；并且（ii）在其满足法律规定的告知和监护人同意的要求之前，严禁收集、使用或披露经识别为13周岁以下的用户的个人信息，该网站或在线服务一般也不被认定为“针对儿童”。此外，如果网站或者在线服务提供者事实上明知其会直接从另一“针对儿童”的网站或在线服务收集儿童个人信息，该网站或在线服务也会被认定为“针对儿童”。网站或者在线服务只是使用信息定位工具，如索引、超链接等提及或者链接至“针对儿童”的网站或在线服务，该网站或在线服务也不构成“针对儿童”。

- 而对于“事实上明知”（actual knowledge）的判断，FTC在其《COPPA实施规则》也指出，事实上明知即事实上确实知晓，不同于“应当知道”(has a reason to know)。FTC对于“事实上明知”的判断标准之一是如果网络运营者在提供网站或在线服务的过程中明确询问用户的出生日期，则认为该提供者在事实上明知。

3. 以CCPA为代表的州立法带动执法

《加州消费者隐私保护法案》（California Consumer Privacy Act, “CCPA”）将于2020年1月1日生效，加州总检察长也于2019年10月10日公布了根据CCPA提出的实施细则征求意见稿，征求意见于2019年12月6日结束，该实施细则将为CCPA的实施和执法提供更多的支持。加州CCPA作为美国第一个颁布统一数据保护法律的州，代表了美国隐私法发展的趋势，美国其他州，例如华盛顿、马塞诸塞、新墨西哥、纽约州也开始制定类似的法律。这些法律内容虽然各有所重，例如华盛顿州的隐私法案主要借鉴GDPR制定，但是都注重对消费者隐私的全面保护。CCPA在内容和执法范围极广，而且也具有域外适用效力。预计随着CCPA和其他州立法的生效和实施，州层面的数据保护执法会有所增加。对于在美国开展跨州业务的中国企业来说，客观上可能会存在同时需要遵守不同州的数据保护法的情况。

（三）其他国家和地区数据保护执法综述

1. 俄罗斯

俄罗斯属于数据保护领域的强监管国家之一。俄罗斯数据保护机构（Roskomnadzor）会通过自动化方式对俄罗斯境内的企业的数据合规情况展开系统性的监控，并且也会不定期的开展实地检查。自2016年开始，俄罗斯即建立了网站黑名单制度，违反数据保护规定的网站，例如未遵守数据主体权利要求，即可能被列入黑名单，而且俄罗斯数据保护监管机构有权暂停违规网站的运营。根据Roskomnadzor的官方统计，2016年共计有219个网站被列入黑名单，84家被暂停运营；2017年有453家企业的网站被列入了黑名单，其中176个网站被暂停运营。[5]

4. https://www.ftc.gov/system/files/attachments/press-releases/app-stores-remove-three-dating-apps-after-ftc-warns-operator-about-potential-coppa-ftc-act/wildec_letter_redacted.pdf，最后访问时间2019年11月11日。
5. Russia: Main Takeaways from Roskomnadzor's Open Doors Day, https://www.hldataprotection.com/2018/02/articles/international-eu-privacy/russia-main-takeaways-from-roskomnadzors-open-doors-day/#page=1，最后访问时间2019年11月11日。

俄罗斯数据保护监管机构针对外国企业的执法多集中于数据本地化的要求。例如2016年俄罗斯曾因LinkedIn未履行本地化存储义务而关闭LinkedIn在俄罗斯的网站，并且将LinkedIn列入了黑名单，要求其将处理的俄罗斯用户的个人信息在俄罗斯境内的服务器上存储，并且将服务器的位置告知俄罗斯数据保护机构。2019年1月21日，俄罗斯数据保护监管机构宣布启动针对Twitter和Facebook公司的行政诉讼，理由亦是未按要求将其用户个人信息在俄罗斯本地部署，并且未能提供关于其进行本地化部署的整改计划的相关信息。

2. 澳大利亚

澳大利亚的数据保护执法以被动执法为主，同时数据保护监管机构Information Commissioner也有权主动展开调查和执法。目前澳大利亚违反个人信息保护规定的罚金上限为42万澳元（个人）和210万澳元（企业）。2019年3月，澳大利亚政府启动了个人信息网络保护和提高非法处理和使用个人信息处罚的计划，并以此作为澳大利亚数据保护监管机构未来三年的工作重点。

3. 日本

日本《个人信息保护法》（Act on the Protection of Personal Information, “APPI”）于2015年进行了大幅度的修正，修订案于2017年5月30日正式生效。在此之前，日本是由各行业的主管部门负责该行业的数据保护监管和执法。自2017年5月30日起，《个人信息保护法》的实施监管和执法工作便主要由于2016年1月1日正式设立的个人信息保护委员会（Personal Information Protection Committee, “PPC”）负责。自开始执法以来，日本个人信息保护委员会执法主要以要求企业提交说明文件和要求企业进行整改为主，尚未有真正执法的案例，但不排除其已经启动了调查程序。日本《个人信息保护法》每三年审阅一次，并会根据审阅的情况进行修订，下一次的审阅时间在2020年。日本个人信息保护委员会可能会考虑在APPI中引入较为明确的“遗忘权”概念，以及加强对个人信息泄露的要求。此外，日本公平贸易委员会（Japan Fair Trade Commission）于2019年8月29日公开对关于平台经营者在涉及消费者提供个人信息的交易时经营者的支配地位的指南（Guidelines Concerning Abuse of a Superior Bargaining Position under the Antimonopoly Act on the Transactions between Digital Platformer Operators and Consumers that provide Personal Information, etc）征求意见，并指出如果必要时FTC将会和PPC一起处理平台经营者（platform operator）侵犯消费者个人信息的情况，[6]提供电子商务等平台服务的企业也需要关注日本数据保护执法和竞争执法结合的相关动态。

4. 韩国

韩国以2011年颁布的《个人信息保护法》(Personal Information Protection Act)为核心，辅之以其他部门法，逐步形成了一套严格的数据保护制度。

韩国也一直在寻求获得欧盟的数据保护充分性认定，自2018年以来进行了多项修法工作。《促进信息和通信网络利用和数据保护法》（Promotion of Information and Communications Network Utilization and Data Protection, “Network Act”）的一项修正案（2019年3月19日生效）要求满足一定门槛的离岸信息服务提供商在韩国设置本地代表，负责履行隐私保护官的职责，并回应韩国监管机构的问询。另一尚未通过的修订案拟将目前的罚金上限（相关销售额的3%或4亿韩元）提高至相关销售额的3%或10亿韩元，并扩大韩国通信委员会（Korea Communications Commission）的行政执法权。此外，韩国也对儿童个人信息保护相关的法规进行了修订，增加了收集14周岁以下儿童的个人信息

6. Request for Public Comments on “Guidelines Concerning Abuse of a Superior Bargaining Position under the Antimonopoly Act on the Transactions between Digital Platformer Operators and Consumers that provide Personal Information, etc.”, https://www.jftc.go.jp/en/pressreleases/yearly-2019/August/190829.html，最后访问时间2019年11月11日。

需要征得监护人明示同意以及对儿童内容管控方面的要求。

5. 拉丁美洲

过去一年拉丁美洲各国在数据保护立法和执法方面均有较大的发展。

巴西于2018年8月通过了《数据保护法》，主要参考GDPR的相关规定制定，将于2020年8月生效。此外，巴西还于2018年12月设立了专门的数据保护监管机构（National Data Protection Authority）。

受GDPR影响，阿根廷也于2017年发布了其新的《数据保护法（草案）》，其现有《数据保护法》从2000年开始实施，同时阿根廷也是南美洲第一个获得欧盟充分性认定（adequacy decision）的国家。

智利在已有个人信息保护法的基础上，于2017年发布了新的修正案，目前修正案尚在讨论中。

哥伦比亚的Superintendency of Industry and Commerce（SIC）有权对企业个人信息保护的实践进行调查，并且要求企业采取合规措施。SIC于2019年1月24日发布了要求Facebook更好地保护哥伦比亚居民个人信息的决议，因为有约3100万哥伦比亚居民受到Cambridge Analytica事件的影响。

三、美国经济制裁立法及执法综述

2018-2019年间，美国经济制裁立法和执法异常活跃。立法方面，美国公布《合规承诺框架》明确有效合规计划的要素，并明确表示其将在具体执法时考虑企业是否具备有效的合规计划。此外，美国通过颁布一系列行政命令迅速升级针对委内瑞拉的经济制裁、同时增强针对原有制裁国家（伊朗、俄罗斯、朝鲜、古巴）的经济制裁措施并扩大域外效力。执法方面，美国针对中国企业实施的经济制裁行为愈发增多；此外，美国重新聚焦针对金融机构的大资金、高关注的案件。

（一）立法动向

1. OFAC公布并实施《合规承诺框架》

2019年5月2日，美国财政部海外资产控制办公室（"OFAC"）发布《合规承诺框架》（A framework for OFAC Compliance Commitments）（简称“《框架》”），鼓励建议受美国管辖的实体，以及在美国境内、与美国人开展业务或使用美国原产货物或服务的外国实体建立制裁合规计划（Sanctions Compliance Program,简称“SCP”）。

该《框架》概括了有效的制裁合规计划应具备如下五个基本要素：

（1）管理层承诺：管理层必须设置合规部门或专员，并赋予其自主权、定期与管理层沟通的权利、以及充足的资源和技术。

（2）风险评估：企业应考虑与地理位置、产品和服务、供应链和客户有关的风险；企业应当定期进行风险评估，以应对不断变化的风险。

（3）内部控制：企业应当制定并定期更新与风险识别、禁止或报告违规行为相关的书面政策和程序，并保存相关记录。

（4）测试和审计：企业评估当前 SCP 程序的有效性、薄弱环节和缺陷，并依据审计结果改进其合规计划。

（5）培训：企业应当至少每年进行一次针对员工、利益相关方的培训，并定期更新培训资料。

在OFAC执法范围越来越广、打击力度越来越大之际，《框架》的实施无疑具有重要意义。首先，是否存在有效的SCP是OFAC认定违规行为是否“情节严重”（Egregiousness）、以及决定处罚轻重的考量因素之一。其次，作为执法行动和解的一部分，OFAC会要求违规企业参照《框架》的要素做出合规承诺。

2. 美国迅速升级针对委内瑞拉的经济制裁

十数年来，美国政府一直将经济制裁作为一种政策手段，对委内瑞拉政府和个人进行限制。自2017年8月以来，美国接连颁布了5项行政命令，将制裁范围从传统的恐怖主义、贩毒、贩卖人口、反民主行动等领域迅速扩展到金融、石油、黄金领域。目前，美国财政部已经对129名委内瑞拉人以及与委内瑞拉有关联的个人实施了制裁；此外，美国国务院吊销了成百上千张签证。

■ 2017年8月第13808号行政令：禁止美国人士或在美国境内开展某些特定债权或权益类交易、或从委内瑞拉政府大量购买债券及有价证券，并禁止委内瑞拉政府进入美国金融市场（豁免交易除外）。

■ 2018年3月第13827号行政令：禁止为/替/代表委内瑞拉政府数字货币/硬币/代用币的发行提供融资或进行其他相关交易。

■ 2018年5月的第13835号行政令：禁止美国人士或者在美国境内实施与购买委内瑞拉债权（包括应收账款）及将此作为担保相关的交易。

■ 2018年11月1日第13850号行政令：授权OFAC将在委内瑞拉黄金行业和美国财政部长决定的其他任何行业开展经营活动的任何个人和实体列入SDN名单，并进行资产冻结。

■ 2019年8月5日第13884号行政令：宣布冻结委内瑞拉政府的资产，并全面禁止美国人士与委内瑞拉政府或其权益开展交易（获得许可证除外），以及针对帮助或支持马杜罗政府的非美国人士实施二级制裁。

在上述行政令的背书支持下，美国财政部迅速开展了针对委内瑞拉的大规模制裁，主要集中在石油和金融领域：

■ 2019年1月28日，美国财政部宣布制裁委内瑞拉石油公司（PdVSA），并且将范围扩大至其拥有50%以上（含）所有权的实体。因此，受美国司法管辖的所有委内瑞拉石油公司的财产（权益）将被制裁封锁，美国人士被禁止与其进行交易。

■ 2019年3月11日，美国财政部基于帮助委内瑞拉石油公司从石油销售中获取现金流的理由，宣布制裁欧洲金融莫斯科人民银行(Evrofinance Mosnarbank，俄罗斯最大的商业银行之一，俄罗斯和委内瑞拉共同拥有）。

■ 2019年3月19日，美国财政部以利用非法黄金交易资助委内瑞拉政府为由制裁委内瑞拉国有黄金公司（Minerven）。

■ 2019年3月22日，美国财政部宣布制裁委内瑞拉经济与社会发展银行（Venezuelan Economic and Social Development Bank，简称BANDES）及其5家子公司，理由是该银行协助Maduro政权将资金从委内瑞拉转移至境外。

■ 2019年4月，美国财政部以运输委内瑞拉石油为由宣布制裁44艘船舶（共涉及6家船运公司），其中5家船运公司将委内瑞拉石油运往古巴。

■ 2019年4月17日，美国财政部制裁委内瑞拉中央银行，其目的在于切断该银行获得美元的途径、并限制其进行国际金融交易的能力。

毫无疑问，美国对委内瑞拉经济制裁首先会冲击美国人士，但同样会殃及中国企业（作为非美国人士），因此中国企业切不可掉以轻心。前述制裁对中国企业的影响主要为：

■ 禁止交易：中国企业的美国分支机构、美籍/居民员工被禁止与委内瑞拉政府或者SDN名单实体进行交易。

■ 无法通过美国银行结算：中国企业自身与委内瑞拉政府或者SDN名单实体之间的交易无法通过美国银行进行结算。

■ 被列入SDN名单的风险：若中国企业在委内瑞拉从事黄金业、石油业、金融业，或向SDN名单实体提供货物、服务、金融、物质、技术支持以及其他帮助或资助，则其自身将面临被列入SDN名单的风险。

3. 美国增强原有经济制裁措施、扩大域外效力

（1）伊朗

2018年，美国单方面退出“联合全面行动计划(JCPOA)”（又称“伊核计划”）并宣布对伊朗重启全方面制裁。让情况更为复杂的是，欧盟此次并没有与美国步调一致，而是启动了“阻断法令(Blocking Statute)”以应对美国的长臂执法。

根据阻断法令，当欧盟成员国公民或者法人因另一欧盟成员国法人遵循美国制裁措施而遭受损害时，可以向该法人寻求损害赔偿。虽然有“阻断法令”的“保护”，但为了避免企业在美国市场的地位受到威胁，汽车（雷诺；雪铁龙）、银行（德国Allianz银行；法国Wormser银行）、能源（道达尔）、航运（德国Hapag-Lloyd公司和丹麦AP Moller-Maersk公司）、电信（德国电信公司）等行业100多家欧洲公司仍然选择离开伊朗。

2019年，美国又对伊朗的经济命脉行业——石油、钢铁铝铜行业（两项最重要外汇来源）采取更高压的经济制裁措施：

■ 2019年4月22日，美国政府宣布将不再给予中国等八个国家和地区进口伊朗原油的豁免；

■ 2019年5月8日，美国总统签署第13871号行政命令，批准对伊朗的钢铁铝铜行业、以及开展涉及伊朗钢铁铝铜行业交易或为之提供便利的非美国金融机构实施制裁。

（2）俄罗斯

自2014年起，美国开始针对俄罗斯采取经济制裁措施，作为对俄罗斯入侵乌克兰、干扰选举、反人权、使用生化武器、扩散武器、与朝鲜贸易、以及支持叙利亚和委内瑞拉等行为的报复。美国的制裁措施通常包括冻结财产、限制使用美国金融系统、禁止入境美国等。近年来，美国对俄罗斯的制裁措施呈现出向二级制裁发展的趋势。

2018年4月6日，OFAC将近40名俄罗斯个人和实体（包含寡头及其控制的公司、高级政府官员、俄罗斯国有武器贸易公司、以及俄罗斯银行）列入SDN名单。这些个人或实体在许多重要国际公司中拥有控制权，引发了OFAC根据“50%规则”而对某些公司的暂时封锁。因此，这些公司不得不重新评估其面对制裁措施的风险敞口，甚至剥离俄罗斯主体持有的利益/股权。

美国经济制裁（尤其是二级制裁）强大广泛的域外效力以及美国政府近年来激进的执法态度意味着，美国人士和非美国人士都面临着与被制裁国家/主体有关的重大甚至无法预料的制裁风险。

（3）朝鲜

尽管2018年美国和朝鲜的关系有所缓和（以两国元首于2018年6月12日的峰会为标志），但是OFAC仍旧继续关注朝鲜，这与美国政府朝鲜半岛无核化的政策遥相呼应。

2018年，OFAC继续将朝鲜个人和实体列入SDN名单中。2018年一开年（1月24日），OFAC基于“为朝鲜大规模杀伤性武器及其他非法业务提供财政或其他支持”的理由将9个实体、16个人和6艘船只列入SDN名单。此后仅一个月（2月23日），OFAC将与朝鲜有联系的56名个人、实体和船只列入SDN名单。

2018年2月和2019年3月，OFAC会同美国国务院和美国海岸警卫队两次发布指南，着重指出了朝鲜为逃避美国制裁而采取的欺骗性做法，以便包括金融机构在内的公司能够充分实施应对措施。

（4）古巴

一直以来，美国对古巴实施全面的全国禁运措施。虽然奥巴马政府期间某些措施放缓，但是特朗普上台后又加强了制裁措施。

最新变化于2019年6月4日生效，当日OFAC公布了《古巴资产管制条例》修正案，重点内容包括：1）取消对“民间”团体教育旅游的许可；2）结束对搭乘客船、旅游观光船和私人飞机前往古巴的例外许可。

（二）执法案例

1. 越来越多针对/包含中国企业的经济制裁行为

■ 中远集团两家子公司等六家中国公司因涉嫌运输伊朗石油而被制裁。2019年9月25日，OFAC以运输伊朗石油为由对六家中国公司和相关五名高管发起新一轮制裁。这六家公司为：中国远洋海运集团的两家子公司中国大连中远海运油品运输有限公司（COSCO Shipping Tanker (Dalian) Co.）和大连中远海运油运船员船舶管理有限公司(COSCO Shipping Tanker (Dalian) Seaman & Ship Management Co.)、中和石油有限公司(CHINA CONCORD PETROLEUM CO)、昆仑航运有限公司(Kunlun Shipping Company Ltd)、昆仑控股有限公司(Kunlun Holding Company Ltd）、以及飞马88有限公司(Pegasus 88 Limited）。据OFAC官网的信息，制裁对象适用于上述6家公司及被其单独或合并持有50%股份以上的实体，但不包括母公司中国远洋海运集团及其他子公司。

■ 美国斯坦利公司因其中国子公司向伊朗出口设备而被处罚。2019年3月27日，美国斯坦利·布莱克和德克公司（“斯坦利公司”）就其中国子公司江苏国强工具有限公司（“国强公司”）23次明显违反美国《伊朗贸易和制裁条例（ITSR）》，而与OFAC达成1,869,144美元的和解协议。2013年5月，斯坦利公司收购国强公司60%的股权并为国强公司的员工进行了一系列制裁合

规培训。然而，国强公司在2013-2014年仍然继续向伊朗出口设备；此外，国强公司的董事与高管在明知出口行为违反美国针对经济制裁措施的情况下仍然参与了这些活动。

■ 两家中国船运公司因帮助朝鲜运输而被列入SDN名单。2019年3月21日，OFAC以帮助朝鲜规避美国和联合国制裁措施为由，将两家中国船运公司大连海博国际货运有限公司和辽宁丹兴国际货运有限公司列入SDN名单。据OFAC官网报道称，大连海博国际货运有限公司在2018年初将货物从中国大连运往朝鲜南浦白头山，船只悬挂朝鲜国旗；辽宁丹兴国际货运有限公司经常以欺骗性手段，令驻欧盟的朝鲜采购官员能为朝鲜政权购买商品。

■ 中国烟台杰瑞公司因向伊朗出口或转出口产品而被处罚。2018年12月12日，中国烟台杰瑞石油服务集团股份有限公司（“杰瑞公司”）与OFAC达成和解协议，将为其11次违反美国《伊朗交易与制裁条例》缴纳278万美元。据悉，杰瑞公司被指控通过绕道中国，将原产于美国的产品出口或转出口给伊朗的最终用户。此外，杰瑞公司还被指控出口原产地为美国的产品，且明知或应知该等产品是为了生产、混合或掺入中国制造的产品，且这些中国制造产品将被供应，转运或转出口给伊朗的最终用户。

2. OFAC重新聚焦金融机构

■ 法国兴业银行因违反美国经济制裁而支付13.4亿美元天价罚款。2018年11月，法国兴业银行（Société Générale）因涉嫌与受制裁国家（古巴、伊朗、苏丹、利比亚、缅甸和朝鲜）实体发生交易行为而与美国诸多监管和执法机构（美国司法部、美联储、OFAC、纽约州检察官办公室、纽约州金融服务局）达成和解，同意向其支付总计13.4亿美元的罚款，成为仅次于法国巴黎银行（BNP Paribas S.A.）89亿美元的史上第二大制裁合规罚款。这项和解意义重大，一方面其符合非美国金融机构因违反美国制裁而支付巨额罚款的先例，另一方面也体现出OFAC和其他政府机构继续优先处理针对金融机构的大资金、高关注的案件。

■ 意大利UniCredit银行因违反美国经济制裁而支付6亿美元和解金额。2019年4月15日，OFAC宣布与意大利UniCredit银行达成三项和解协议，金额总计6亿美元。2002-2012年，意大利UniCredit银行通过伪造业务凭证或隐瞒交易信息等方式，利用美国金融系统，与位于伊朗等受美国经济制裁地区的实体或者受美国经济制裁的其他实体进行业务往来，并为该等实体提供金融服务并输送资金，严重违反了美国经济制裁规则以及联邦和纽约州多项法律。

四、世界银行制裁体系介绍及对中国企业的建议

（一）引言

世界银行集团由国际复兴开发银行（IBRD）、国际开发协会（IDA）、国际金融公司（IFC）、多边投资担保机构（MIGA）和国际投资争端解决中心（ICSID）五个机构组成，旨在通过向发展中国家提供中长期资金和智力支持，帮助发展中国家实现长期、稳定的经济增长。其中国际复兴开发银行和国际开发协会一般被通称为“世界银行”。

世界银行（World Bank，下文亦称“世行”）自1946年开始运作以来，通过提供和组织长期贷款，在促进各国特别是发展中国家实现经济可持续发展、促进全球减贫、维护世界金融稳定等方面发挥了重要作用。一直以来，中国与世界银行保持着紧密的合作关系。一方面，中国通过向世行申请贷款，支持涉及城建、环保、交通、农业、能源等领域的项目建设；根据《世界银行集团制裁体系2018年度报告》（World Bank Group Sanctions System Annual Report FY18，以下简称“《世行2018年度报告》”），2018财年中国为世界银行第四大借款国，借款金额达17.88亿美元。另一方面，中国企业越来越多地以中标者、供应商、服务商、承包商等多种角色参与世行在中国及其他国家和地区援建的各类项目。

世行成立后很长一段时间内，其在推行贷款项目过程中深受腐败问题困扰，例如，因借贷国的国内政治腐败问题导致项目资金无法依其借贷目的得到有效利用。由于世界银行负有不干涉成员国内政的义务，[1]起初世界银行对借贷国的国内政治腐败问题往往只能“视而不见”。但自上世纪90年代起，世行日益强调腐败问题与造成项目失败、经济发展受限之间的关系，逐步将打击项目中存在的腐败问题纳入其管辖范围之内，并在1996年正式引入反腐败制裁体系，开始参与全球腐败治理。世行将此强调为其对资金利用所负有的信义义务（Fiduciary Duty），以确保世行所提供的资金仅为项目目的使用，与干涉成员国内政无关。

经过二十余年间的数次改革，世行不断扩大反腐败制裁的管辖范围，强化制裁的强制性，相应设立的反腐败制裁体系亦日益成熟。受到世行的制裁，意味着在一定期限内，将无法参与世行资助的项目，对于企业的声誉而言亦是极大的损害。此外，2010年4月，世界银行集团、亚洲发展银行、非洲发展银行集团、欧洲复兴开发银行、美洲开发银行集团签署了《共同实施制裁决议的协议》（Agreement for Mutual Enforcement of Debarment Decisions，以下简称“《交叉制裁协议》”），对腐败、欺诈等应制裁行为进行交叉制裁（亦称“联合制裁”）。根据《交叉制裁协议》，针对超过一年期限的制裁措施，如果一家企业被一家缔约银行制裁，会在同等时间内被禁止参与以上所有缔约银行所资助的项目。因此，尽管当前对于世行施行制裁权力的正当性问题仍存在争议，但毫无疑问在实践中借贷国以及承包世行资助项目的企业及个人对于世行的制裁机制均无法视而不见，对于中国的企业及个人而言更是如此。

尤其是近年来，随着“一带一路”倡议的推进，越来越多的中国企业走出国门，承建海外工程项目，但是由于不熟悉国际合规监管环境及相关政策，中国企业也容易遭受多边开发银行或当地政府的处罚。近年来，中国企业和个人受世行制裁的数量总体呈上升趋势，且自2017年起成倍递增。2017年21个中国企业和个人受到世行制裁，2018年增长至44个；2019年6月因世行对中国铁建股份有限公司（“中国铁建”）施加的制裁措施同时施加于其所控制的700多个公司，使得仅2019年上半年中国企业和个人受世行制裁的数量骤然井喷至823个。根据世行官网数据，截至2019年11月13日，受到世行制裁的中国企

1. 根据《国际复兴开发银行协定》（Articles of Agreement of the International Bank for Reconstruction and Development）规定，世行不得介入会员国的国内政治。第3条第5款（b）项规定：“银行应规定办法，保证使任何贷款的款项只能为提供贷款所规定的目的之用，并使之充分注意节约和效率，但不得计及政治的或其他非经济性的影响或考虑。”第4条第10款规定：“银行及其官员不得干预任何会员国的政治，其一切决定也不应受有关会员国政治性质的影响。一切决定只应与经济方面的考虑有关，权衡此种考虑时应无所偏倚，以期达到第一条所阐明的宗旨。”

业和个人的数量增加至876个。[2]

值得注意的是，在世行的制裁体系中，世行十分强调在企业内部建立“合规计划/合规体系”的重要性，并就此专门制定了《世界银行集团廉政合规指南》（World Bank Group Integrity Compliance Guidelines，以下简称“《世行合规指南》”）。熟悉《世行合规指南》对于企业事前防范制裁风险、争取减轻制裁或免于制裁等均有重要作用。

（二）世界银行制裁体系介绍

1. 制裁范围：制裁对象及应制裁行为

根据世行制定的《关于预防和打击国际复兴开发银行贷款和国际开发协会信贷和赠款资助项目中的欺诈和腐败行为的指南》（Guidelines on Preventing and Combating Fraud and Corruption in Projects Financed by IBRD Loans and IDA Credits and Grants，以下简称“《反腐败指南》”），[3]世行制裁机制适用于所有世行资助项目在使用贷款资金中存在的欺诈和腐败行为（Fraud and Corruption），包括世行全部或部分资助的项目。

《反腐败指南》适用于所有贷款资金接受者（recipients of loan proceeds），主要包括：（1）借款人；[4]（2）所有最终使用贷款资金的个人或实体，实践中可能包括承包商、供应商、服务商等具体项目参与者；（3）负责存放或支付贷款资金的个人或实体，例如财务代理（fiscal agents）；以及（4）可以影响贷款资金的使用或对此作出决策的个人或实体。[5]概括而言，与世行项目贷款资金的使用存在关联的任何个人或实体，均可能受到世行制裁机制的管辖。应注意，上述个人或实体不包括会员国及其政府官员，但是国有企业及机构除外。[6]在会员国或其政府官员发生欺诈或腐败的情况下，一般由世界银行通过政治及外交渠道解决或与会员国一起进行处理。

此外，世界银行的制裁还可能延伸至被制裁方的关联公司。根据《制裁程序》规定，关联公司（Affiliate）是指控制被制裁方、受被制裁方控制或与被制裁方一起被共同控制的任何法律实体或自然人，包括被制裁方所控制的其他公司以及被制裁方的母公司或姐妹公司。

《反腐败指南》中规定的欺诈和腐败行为主要包括以下五类：（1）腐败行为（corrupt practice），指直接或间接地提供、给予、收受或索要任何有价物以不当影响另一方的行为，典型的腐败行为包括行贿受贿、提供或索要回扣。（2）欺诈行为（fraudulent practice），指通过任何作为或不作为（包括虚假陈述（misrepresentation）），故意或肆意误导（或企图误导）其他方，以谋取财务等利益或逃避义务；实践中，欺诈行为包括出具虚假的资质证书，提供虚假的投标保函、履约保函、虚假发票，虚假陈述项目经验以及不披露代理、佣金、分包商等。（3）共谋行为（collusive practice），指双方或多方之间为实现某个不当目的的共谋，包括对其他方的行为产生不当影响；典型的共谋行为包括串通报价、虚假竞标等。（4）胁迫行为（coercive practice），指直接或间接地以危害或损害（或威胁危害或损害）任何一方或该方的财产，以不当影响某一方的行为。（5）妨碍行为（obstructive practice），[7]指（i）为实质性妨碍世行对被指控的腐败、欺诈、胁迫或共谋行为进行调查，故意破坏、伪造、改变或隐瞒调查所需的证据材料或向调查官提供虚假陈述；和/或威胁、骚扰或恐吓任何一方以防止其透露与调查相关的所知信息或协助继续调查，或（ii）对世行行使其审计或获取信息的合同权利构成实质性妨碍的行为。[8]

实践中，世界银行基于“欺诈行为”做出制裁决定的情形占据很大一部分，自2014年至2018年，始终保持

2. http://www.worldbank.org/en/projects-operations/procurement/debarred-firms，最后访问时间2019年11月18日。
3.《反腐败指南》于2006年制定，经2011年1月及2016年7月两次修订，现行最新版本为2016年7月1日修订版。
4. 部分情况下，可能由非会员国政府的其他实体作为借款人，并由会员国政府进行担保。
5.《反腐败指南》第5条。
6. 根据《世界银行投资项目融资借贷者采购规则》（The World Bank Procurement Regulations for IPF Borrowers，以下简称“《采购规则》”）（现行最新版本为2018年8月修订版本）第3.22条，借贷国仅可因履行合同的能力及资源或在发生利益冲突事项的情况下，拒绝某一企业或个人申请投标。因此，一般情况下，国有企业或机构与一般企业具有同等竞标资格。
7. 世界银行为加强调查的有效性及制裁的强制性，将妨碍行为纳入制裁范围之内，但这在理论上及其他多边开发银行的实践中均存在争议。
8.《反腐败指南》第7条。

在占比70%-80%左右。[9]在招投标过程中对企业资质、项目经验等做出虚假陈述而被认定为构成“欺诈行为”，是中国企业遭受世行制裁的重要原因之一。例如，2019年6月12日，东方电子股份有限公司为满足项目要求，在招标过程中伪造两份信件，被世行认定为“欺诈行为”， 从而失去在未来的15个月内参与世界银行资助项目的资格，根据《交叉制裁协议》失去参与其他六家开发银行资助项目的资格，期满后在满足特定条件情况下可恢复资格[10]。2019年9月11日，中国能源建设集团湖南省电力设计院有限公司为满足招投标要求，编制并提交虚假的诉讼历史、合同经验和业务资质，被认定为“欺诈行为”并受到世行制裁，在未来20个月内失去参与世界银行资助项目的资格，同时根据《交叉制裁协议》失去参与其他六家开发银行资助项目的资格[11]。

2. 制裁措施及制裁效果

（1）制裁措施及考量因素

针对以上欺诈和腐败行为的发生，《世行资助项目中的制裁程序及和解》（Sanctions Proceedings and Settlements in Bank Financed Projects，以下简称“《制裁程序》”）[12]中规定了世行可采取的五种制裁措施，分别为斥责（Reprimand）、附条件免于除名（Conditional Non-Debarment）、附条件解除的除名（Debarment with Conditional Release）、除名（Debarment）以及返还得利（Restitution），[13]其中附条件解除的除名为基准制裁方式，是世界银行最常用的制裁方式之一。此外，世行还针对制裁措施的裁量、加重及减轻等专门制定《世界银行制裁指引》（World Bank Sanctioning Guidelines，以下简称“《制裁指引》”）。

具体而言，制裁措施包括：

a. 斥责，是指就被制裁方的应制裁行为向其发出正式的斥责信（Letter of Reprimand）；该制裁措施主要适用于不当行为本身十分轻微、或对不当行为的参与程度很低的情况。

b. 附条件免于除名，是指若被制裁方能够遵守特定的补救性、预防性条件或其他条件，将免于被世行施加除名制裁。该等条件可能包括采取措施以提升合规管理水平（包括采纳或完善及实施廉政合规计划（Integrity compliance program，以下简称“合规计划”））、赔偿损害、针对某些员工采取纪律性措施等。这一制裁措施主要适用于被制裁方已经自愿采取全面性纠正措施，且情况表明现阶段不需要对其进行除名的情况。此外，在被制裁方的关联公司虽未直接参与不当行为，但对所发生的应制裁行为存在系统性监管疏漏的情况下，关联公司亦可能受到附条件免于除名的制裁。

c. 附条件解除的除名，即被制裁方被除名（须先经过一段特定除名期间后）[14]直至满足特定的补救性、预防性条件或其他条件，该等条件同样可能包括采取措施以提升合规管理水平（包括采纳或完善及实施合规计划）、赔偿损害、针对某些员工采取纪律性措施等。该制裁措施的主要目的在于鼓励被制裁方建立或完善内部合规体系，在除名期满后企业再次参与世行所资助活动的情况下，得以控制、减少可能带来的风险。

d. 除名，包括永久性除名和一定期限内除名，系指永久性或在一定期限内取消被制裁方（i）参与或获益于世界银行资助项目合同的资格；（ii）以分包商、顾问、制造商或供应商、或服务提供者的身份参与其他有资格参与者所承接的世行资助项目；以及（iii）获取世界银行的贷款资金或以其他方式参与任何世行资助项目的准备或实施。

施加这两种不附条件直接除名的措施，主要是考虑以

9. 《世行2018年度报告》第39页。
10. 东方电子受世行制裁新闻：https://www.worldbank.org/en/news/press-release/2019/06/12/world-bank-group-debars-dongfang-electronics-co-ltd，最后访问时间2019年11月18日。
11. 中国能源建设集团湖南省电力设计院受制裁新闻：https://www.worldbank.org/en/news/press-release/2019/09/11/world-bank-group-debars-china-energy-engineering-group-hunan-electric-power-design-institute-co-ltd，最后访问时间2019年11月18日。
12. 《制裁程序》于2009年制定，后经多次修订，现行最新版本为2016年7月1日修订版本。
13. 《制裁程序》A部分第9.1条。
14. 根据《制裁指引》第II条A款，附条件解除的除名必须首先经过一段特定期间，在此之前即使被制裁方满足特定条件，除名制裁亦不能直接解除。

下两个方面：其一，若被制裁方原本就设有完善的合规计划，或已经针对涉案员工进行相关处分等，再对其设定条件要求整改或完善的必要性不大，此时考虑直接对其施加一定期限内除名的措施而非附条件解除的除名；其二，施加永久性除名制裁措施，则主要适用于情节严重，但可能无法通过对被制裁方设定条件要求其改善或提升的情况，该制裁措施主要适用于自然人、被该等自然人紧密控制的公司以及壳公司等。

e. 返还得利，即向借贷者以及任何其他方返还所有不正当所得或进行补救。

世界银行在考虑对被制裁方施加何种制裁时，将综合考虑以下因素，例如：不当行为的严重性；不当行为所带来的损害程度；被制裁方对世行调查的配合程度；被制裁方过去曾被世界银行或其他多边发展银行认定存在违法行为的情况（主要指可能被施加除名制裁的案件）；是否存在减轻处罚的考量因素，例如在不当行为中担任次要角色、自愿采取纠正措施或配合调查，包括达成和解等；是否违反制裁程序的保密要求等。[15]根据《制裁指引》，基准制裁措施为附条件解除的除名，为期三年，并在此基础上综合各项加重及减轻因素调整制裁措施的种类及期限。

（2）制裁效果及影响范围

世行所施加的制裁措施，制裁效果显著且影响范围较大。

其一，世行所施加的制裁一般为整体性制裁，对被制裁方所施加的制裁措施可同时施加于被制裁方的任何关联公司以及被制裁方的承继者和受让者（Successors and Assigns）。[16]以中国铁建及其两个全资子公司被世行施加为期9个月的除名制裁为例，该制裁措施同时扩展至中国铁建所控制的730个关联公司。在9个月的制裁期限过后，上述三个公司及730个关联公司还将受制于为期24个月的附条件免于除名的制裁。[17]

其二，除名制裁将自动扩展至世界银行集团其他机构成员，包括IFC和MIGA所资助或担保的项目，以及世界银行担保的项目及碳金融业务（carbon finance operations）。[18]

其三，制裁措施具有交叉制裁效果。2010年4月，世界银行集团、亚洲发展银行、非洲发展银行集团、欧洲复兴开发银行、美洲开发银行集团等签署《交叉制裁协议》，针对腐败、欺诈、共谋、胁迫等应制裁行为，[19]若企业被其中一家缔约银行施加超过一年期限的制裁措施，则将在同等时间内被禁止参与以上所有缔约银行所资助的项目。根据《世行2018年度报告》，2018 财年，世界银行集团确认了其他多边开发银行的73 项交叉制裁。

其四，制裁信息将被公布。2012年，制裁理事会开始将其制裁决定予以公布。根据《制裁程序》第10条，有关被制裁主体及制裁措施的相关信息应当公开发布。[20]制裁信息一经发布将广而告之，这一方面更加杜绝了被制裁主体变相规避制裁措施的可能（借贷国政府、业务合作伙伴均将知悉相关制裁信息），另一方面可能导致其他国家政府启动调查或对相关行为进行处罚，对于被制裁主体的声誉亦大有损害。

3. 制裁程序——三个主要机构、两级制裁体系

世界银行的制裁体系中涉及三个主要机构，即廉政局（Integrity Vice Presidency）、资格暂停和除名办公室（Office of Suspension and Debarment）以及制裁理事会（Sanction Board）。其中，廉政局为调查机构，资格暂停和除名主管（Suspension and Debarment Officer，以下简称“暂停主管”）及制裁

15.《制裁程序》A部分第9.2条。
16.《制裁程序》A部分第9.4条（b）及（c）款。
17. 中国铁建受世行制裁新闻：
https://www.worldbank.org/en/news/press-release/2019/06/05/world-bank-group-debars-china-railway-construction-corporation-ltd-and-two-subsidiaries，最后访问时间2019年11月18日。
18.《制裁程序》A部分第4.2条（d）款。
19.《交叉制裁协议》中认可的应制裁行为不包括妨碍行为。
20. 有关制裁名单及制裁措施的相关信息可在以下网站中获取：www.worldbank.org/en/projects-operations/procurement/debarred-firms

理事会为负责审查及做出制裁决定的两级审理机构，后两者一般称为两级制裁体系。暂停主管负责案件初步审理；制裁理事会负责处理申诉案件并做出最终裁决。

（1）调查机构

实践操作中，首先由廉政局负责案件初步调查、收集证据，调查对公司或个人（以下简称“被调查对象”）的应制裁行为，包括上文所介绍的腐败、欺诈、共谋、胁迫及妨碍行为等。调查完成后，若廉政局认为有充分证据证明被调查对象存在应制裁行为，其将向暂停主管提交“指控声明及证据”（Statement of Accusation and Evidence），该声明应包括对被调查对象的具体违法行为指控、明确被调查对象（包括建议施加制裁措施的每一个关联公司）、案件基本事实概述及制裁依据，并提交相关证据（包括其所掌握的可以争取免于制裁或减轻处罚的证据）。此外，世行于2010年引入制裁协商解决机制（Negotiation Resolution Agreements (settlements)，下称“和解机制”），由廉政局负责与被调查对象进行和解谈判、达成和解协议。

（2）两级制裁体系[21]

a. 第一级——暂停主管

暂停主管主要负责与世界银行资助项目相关的案件，负责对廉政局所提交的案件及证据进行初步审核，世界银行将暂停主管定位为“行政法官”（Administrative Judge）。若认为证据不足，暂停主管可要求廉政局进行补充调查。若认为证据充足，暂停主管将向被调查对象发出“制裁审理通知”（Notice of Sanctions Proceedings，以下简称“通知”），该通知应包括建议的制裁措施，并附上指控声明及证据，暂停主管亦可建议对被调查对象的关联公司施加适当制裁。针对期限为6个月以上的制裁，被调查对象接到通知后，将被自动暂停参与世界银行资助项目的资格，此被称为“临时资格暂停”。接到通知后90天内，若被调查对象未对相关指控或建议的制裁措施提出异议，则建议的制裁措施将在90天后被执行。

b. 第二级——制裁理事会

世行制裁理事会由七名成员组成，其中包括两名替补成员（alternate members）。为加强理事会的独立性和中立性，2009年起世行开始引入外部人员担任理事会成员，至2016年已演变为七名成员均由外部人员担任。制裁理事会的成员由世行行长提名后，由执行董事会（Executive Directors / Board of Directors）任命；执行董事会在听取世行行长的建议后负责选出制裁理事会主席。若被调查对象对指控或建议的制裁措施提出异议，则案件将交由世界银行制裁理事会处理。处理具体案件时，制裁理事会将针对个案选出三名理事会成员组成审理小组（panel），审理小组的成员由理事会主席任命。

若被调查对象在收到通知后90天内，向制裁理事会递交书面答辩（Response），则案件将进入由制裁理事会审理的第二级程序，廉政局可就被调查对象所提出的答辩进行书面回应（Reply）。制裁理事会将审议通知中提出的指控及制裁建议、各方的答辩及回应，并审核案件所有证据。根据被调查对象或廉政局的申请，或制裁理事会的自主决定，可就案件举行听证会，但该听证会为非正式（informal）、不公开（confidential）举行，且听证内容仅限于双方所提交的书面材料中的论点及证据。除制裁理事会自行决定召集一个或多个证人出席听证会外，听证会上不允许证人作证，且不允许进行交叉质询（cross-examination）。此外，在听证会上，若一方拒绝回答或回答不实，将被解释为不利于该方。

值得注意的是，世界银行在其《制裁程序》中明确指

21. 针对世界银行两级制裁体系，世界银行集团撰写并发布了《世界银行集团制裁体系》（World Bank Group Sanctions System）一文进行介绍。

出，制裁程序“不适用任何正式的证据规则”（formal rules of evidence shall not apply）。任何证据均可以提交而不论其形式、性质，并由暂停主管及制裁理事会自行决定所有被提交证据的相关性、实质性、证明力及充分性（relevance, materiality, weight, and sufficiency of all evidence offered）。在证明标准上，世界银行采用民事诉讼中通用的优势证据标准，其做出裁定的标准为“比不可能更有可能”（more likely than not）。该证明标准相对偏低，既不要求证据具有高度盖然性，亦远非刑事诉讼程序中的排除合理怀疑标准。

综上审查，若制裁理事会裁定被调查对象不太可能存在应制裁行为，则制裁程序终止。若制裁理事会裁定被调查对象更有可能存在一项或多项应制裁行为，将对被调查对象施加适当的制裁，并在适当情况下可能对其关联公司施加制裁。制裁理事会的决定为最终决定且即刻生效，无论是廉政局、暂停主管或被调查对象，均无法对其终局决定进行再次申诉。此外，从上述听证会及证据规则中我们亦可看出，暂停主管及制裁理事会对制裁审理程序拥有很大程度上的自由裁量权，消极对待世行发出的相关制裁通知或决定将可能对自身带来非常不利的后果，例如上文所述，在听证会上，若一方拒绝回答或回答不实，将被解释为不利于该方。

（3）临时资格暂停（Temporary Suspension）及先期资格暂停（Temporary Suspension Prior to Sanctions Proceedings）

临时资格暂停是指，在暂停主管发出通知后，若该通知中所建议的除名制裁期限为6个月以上，则自通知发布之日起，直至制裁审理程序结束，被调查对象将自动被暂停参与世行资助项目的资格。针对被建议施加两年以上制裁措施的企业，临时资格暂停的效果还将同时覆盖其关联公司。设置临时资格暂停程序[22]的目的，在于避免被调查对象在制裁程序结束之前仍可继续参与新项目。

先期资格暂停[23]相比临时资格暂停更进一步，是指廉政局在进行案件调查期间，若其认为有充分证据证明被调查对象存在腐败或欺诈行为，且至多一年内案件调查非常有可能（highly likely）成功结束并提交指控声明及证据，则廉政局可以在调查结束或提交书面指控之前，向暂停主管申请提前暂停相关被调查对象参与世行资助项目的资格。先期资格暂停期限为6个月，廉政局可申请延期一次。若在先期资格暂停期限到期之前，廉政局未能提起正式指控，则被调查对象将自动恢复资格。而若在先期资格暂停期限之内，廉政局提起正式指控，则被调查对象的除名期限将自动延期至整个制裁程序结束。

被调查对象可以在收到临时资格暂停或先期资格暂停通知后30日内，提交书面解释及相关证据对该等资格暂停措施提出异议，并由暂停主管进行审查并决定是否修改或撤回资格暂停决定。

以上两种资格暂停程序将除名期间两次提前，尤其是先期资格暂停程序甚至将除名期间提前至案件调查期间，这对于被调查对象所产生的影响是不言而喻的。资格暂停的效果等同于除名，这意味着即使案件结果最终未裁定对被调查对象施加制裁措施，但在整个制裁审理过程中乃至调查期间，被调查对象参与世行资助项目的资格均被取消。

4. 制裁时效限制：十年

在廉政局提交指控声明及证据之时，若（1）与应制裁的欺诈和腐败行为相关的合同已执行完毕达十年以上，或（2）相关欺诈和腐败行为发生在十年以前，该行为将免于被追诉。[24]

22.《制裁程序》A部分第4.2条。
23.《制裁程序》A部分第2条。
24.《制裁程序》A部分第4.1条（d）款。

（三）中国企业应对世界银行制裁的建议

综观实践中受世行制裁的中国企业，主要以工程类公司为主，其中国有企业占据很大一部分。尤其在“一带一路”倡议后，随着走出去的企业越来越多，在遵守项目所在国当地法律法规的同时，中国企业亦应同时了解、熟悉世界银行集团等国际金融机构的相关合规、制裁制度。就应对世界银行制裁而言，了解其所针对的制裁对象、应制裁行为、制裁措施以及整个制裁程序等，方能更好地找到应对方法、及早预防风险，不至于在受到世行制裁的情况下措手不及。

根据上文对世行制裁体系的整体介绍，首先，建议参与世行资助项目的中国企业，尤其是工程建设类企业，应了解并建立符合世行标准的合规计划。其次，在实践中遇到世行制裁相关事项时应做到积极回应及配合，及时了解相应制裁事项所对应的案件事实，争取通过谈判达成更有利的和解条件。

1. 建立并实施合规计划

合规计划一词在上文引言及介绍世行整体制裁体系的过程中反复被提及。实际上，世界银行十分强调在企业内部建立合规计划的重要性，并就此专门制定《世行合规指南》，对合规计划的内容及标准进行具体规定。世界银行鼓励企业建立合规计划的最终目的在于预防和减少廉政合规风险，预防和减少对世行所资助活动可能带来的风险。

一项有效的合规计划，是预防、减轻、甚至免于世行制裁的有效措施之一。世行作为经济全球化的重要推动者和全球腐败治理的重要参与者，在合规领域亦积累了相当丰富的经验，其所制定的《世行合规指南》中对合规计划的设置亦采纳了国际通行或认可的标准。因此，对于企业而言，建立并实施合规计划不仅是应对世行制裁的一项长期有效的机制，对于提升企业的合规管控水平同样行之有效。

（1）建议企业建立并有效实施合规计划的重要性

其一，合规计划是世行制裁措施的重要组成部分。世界银行在《制裁指引》中反复强调“重整”（Rehabilitation）为减少廉政合规风险的核心措施，所谓重整系指通过施加特定条件帮助被制裁方提升廉政文化、防止再犯。这也是世界银行将附条件解除的除名作为基准制裁措施的核心原因之一，其明确强调，施加条件的目的在于鼓励被制裁方的合规建设，以期减少未来对世行所资助活动可能带来的风险。这一理念对于附条件免于除名、除名（包括永久期限及一定期限内的除名）等其他制裁措施亦适用，在施加这些制裁措施之前合规计划均被考虑在内。

其二，合规计划是考量制裁措施的重要减轻因素之一。在《制裁指引》所列举的减轻因素中，“有效的合规计划”（Effective Compliance Program）为明确列举的减轻因素之一。当然，对于是否“有效”的判断将综合合规计划的设置、实际实施效果进行考量，仅为“书面计划”将无法认定其有效性。这便要求企业不仅应对合规计划的设计上心，且应保证其可实施性并融入日常实践中。

其三，合规计划是达成和解协议的重要条件之一。世行的和解机制允许被调查对象和廉政局在制裁程序的任何阶段（包括调查阶段）、制裁委员会最终裁决之前达成和解协议，并由暂停主管进行审查。选择和解谈判，企业将可能以遵守廉政局所提出的特定条件换取更轻程度的制裁措施，例如更短期限的除名制裁。企业同意制定并实施合规计划，是达成和解协议的重要条件之一。

（2）《世行合规指南》及合规计划的主要内容

世界银行集团发布的《世行合规指南》中，对于合规计划的内容进行了系统性规定。《世行合规指南》明确指出，制定并实施合规计划的目的在于防止、发现欺诈和腐败行为，并进行补救。该指南的主体内容吸收了经认可的各项国际标准，包括2009年经济合作与发展组织《关于进一步打击国际商业交易中行贿外国公职人员行为的建议》（Recommendation for Further Combating Bribery of Foreign Public Officials in International Business Transactions）及其附件二《内控、道德与合规最佳实践指南》（Good Practice Guidance on Internal Controls, Ethics, and Compliance）、国际商会《关于打击勒索和贿赂的准则与建议》（Combating Extortion and Bribery: ICC Rules of Conduct and Recommendations）、世界经济论坛合作反腐败倡议《PACI反贿赂原则》（Guidelines for Countering Bribery）以及美国《量刑指南》（Sentencing Guidelines）等。

总体而言，一项有效的合规计划应包括书面政策及程序，并将合规实践融入日常工作中，制定、实施并遵守符合要求的合规计划是企业全体员工及高管的责任所在。一项完整的合规计划通常需要建立与完善公司内部完整的合规体系与工作流程，包括但不限于：（1）公司内部政策和程序；（2）针对业务伙伴的政策；（3）内部控制；（4）培训和宣传；（5）报告机制及补救措施等。

其中，公司内部政策和程序方面应包括关于对员工的尽职调查，限制聘用退休官员，礼品、招待、宴请、旅行及其他支出，慈善捐赠、政治捐献以及好处费等的规定和限制；针对业务伙伴的政策应包括对业务伙伴的尽职调查、告知其合规计划并要求做出合规承诺、记录留存、合理报酬以及监管监督方面的规定；内部控制方面应包括在财务记账、雇佣合同及业务伙伴合同、决策程序等方面做出规制。

2010年9月，世行廉政局任命了第一位廉政合规官（Integrity Compliance Officer，下称“合规官”）。除监督被制裁企业的廉政合规情况（或者个人遵守行为准则的情况）外，合规官还负责决定合规条件、和/或由制裁委员会或暂停主管所确定的作为制裁措施一部分的其他条件是否得到了满足。在以上合规计划的制定和实施过程中，企业应不定期向合规官报告工作进展情况，接受其评估与持续的监督。只有在满足合规官的审查要求后，被制裁主体才能被解除制裁或者免于制裁。

（3）以《世行合规指南》为基准，充分参考国内合规指引

《世行合规指南》为指导性文件，在不违背《世行合规指南》的原则性要求的基础上，企业在建立合规计划时可以根据企业自身的性质及所在国的国情进行具体设计和调整。

2018年，《中央企业合规管理指引（试行）》（“《央企合规指引》”）和《企业境外经营合规管理指引》（“《境外合规指引》”）相继出台，一方面对中央企业的合规管理提出了系统性要求，另一方面对企业提升境外经营管理水平、合规管理水平亦提供了参考。中国企业在建立合规计划时，可以《世行合规指南》为基准，根据企业性质，充分纳入上述两份国内合规指引的相关要求，从而建立起同时符合国内要求、国际标准的全面合规体系。

2. 及时回应、积极配合

在收到任何世行发出的与制裁相关的通知、要求或其

他文件时，建议企业认真对待并及时回应，并在涉及世行对自身进行调查的情况下积极配合。对于被调查对象而言，消极对待或实施妨碍行为将可能带来非常不利的后果。

其一，“妨碍行为”属于世行五类应制裁行为之一。妨碍世行针对欺诈和腐败行为进行调查、破坏或伪造证据等行为，存在触发额外制裁措施的风险。

其二，干扰世行的调查是考量制裁措施的加重因素之一，可能导致制裁期限增加1-3年；[25]相反，积极配合廉政局的调查是考量制裁措施的减轻因素之一，减轻幅度可达33%。配合廉政局进行调查的行为可包括：（1）提供实质性协助与合作，包括自愿披露行为、提供真实、完整、可靠的信息或证言等；（2）开展内部调查，并将内部调查结果及相关证据与廉政局分享；（3）认罪或承担责任，在调查阶段尽早认罪或承担全部责任；（4）自我约束，在调查结束之前自愿主动放弃参与世行资助项目。[26]

其三，根据世行所采纳的证据规则及裁量标准，消极对待世行针对应制裁行为进行的调查或要求，将可能被解释为不利于企业自身。

因此，综合考虑被调查案件的事实及证据，当企业判断最终被世行施加制裁措施的可能性较大的情况下，建议适当考虑尽早承认相关不当行为或承担相应责任。

3. 及时谈判、达成和解

和解机制是可以提前终止世界银行制裁程序、有效解决应制裁事项的方式之一，对于世界银行而言亦可有效节约调查资源、裁判资源。和解谈判可以在制裁程序的任何阶段进行，包括调查阶段。和解机制自引入以来得到越来越频繁的应用，根据《世行2018年度报告》，从2014年至2018年，达成和解的案件从6件上升为26件。2018财年，暂停主管审查案件的数量和审阅廉政局提交和解协议的数量已基本持平，分别为27件和26件。

若和解协议中约定了具体处置方式，则自和解协议生效之日起案件终结（亦可在和解协议中约定具体终结日期）；若和解协议中约定要求延期制裁程序，并要求被制裁方在一定期间内遵循特定条件，则在此段期间内视为制裁程序中止（延迟执行）。在第二种情形中，除非协议另有约定，在延期期满且被制裁方遵守协议中规定的特定条件的情况下，制裁程序应予结束。[27]但若廉政局后续发现被制裁方存在违反和解协议的行为，可以重启案件并从制裁程序中止之点开始继续进行。[28]

在进行和解谈判的过程中，对于企业而言，不妨将《制裁指引》中所列的加重及减轻因素作为参考，可将其中企业所拥有的减轻因素作为谈判筹码，尽可能争取更轻程度的制裁措施或更有利的和解条件。

25.《制裁指引》第IV条C款。
26.《制裁指引》第V条C款。
27.《制裁程序》B部分第3条（a）（b）款。
28.《制裁程序》B部分第4条。

第二章

问卷调研

本次调研问卷的发放时段为2019年8月11日至10月20日，涉及2018-2019年度的国内外立法、执法对企业的影响、企业合规整体建制、企业应对政府突击检查、企业投资合规尽职调查以及企业内部调查、网络安全及个人信息保护、知识产权等方面问题。最终共计回收263份有效问卷。其中本章节所涉及数据比对是与2017-2018年度（“此前年度”）蓝皮书的问卷调研数据进行对比。

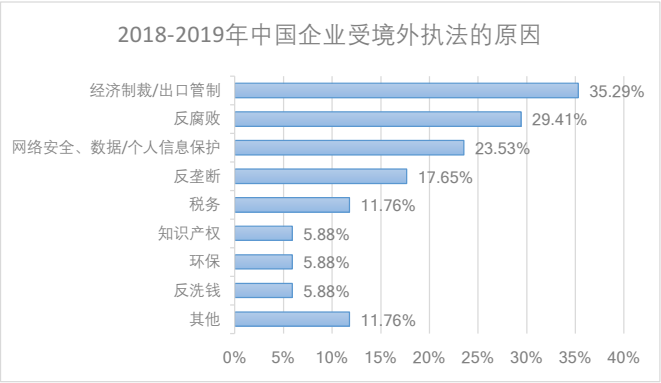
263家参加调研的企业中，按照类型划分，外商独资企业约占23%、内资民企约占36%、国企约占30%、中外合资企业约占6%，另外其他类型的约占5%。按照行业划分，有约20%的企业来自金融与投资行业（“金融投资”），医疗与健康行业（“医疗健康”）占比超过19%，“TMT、信息传输、软件和信息技术服务行业”（统称“TMT”）和汽车制造与销售（含零部件）行业（“汽车”）各自占比约为13%及7%。房地产与建筑行业（“房地产”）、制造业（不含汽车、医药、科技制造）（“制造”）、能源与环保行业（“能源环保”）、科技制造行业、专业服务、交通、运输、仓储和邮政、批发与零售行业（“批发零售”）、餐饮住宿、电子商务、教育与科研、商贸行业、采矿业、文化、体育和娱乐业行业、智能制造等企业也参与了调研。按照规模划分，约63%的企业为500人以上的大型企业（其中大多数超过1000人），101-500人的中型企业以及100人以下的企业各占比约为21%和16%。

一、国外执法变化对企业的影响

（一）企业受境外执法情况

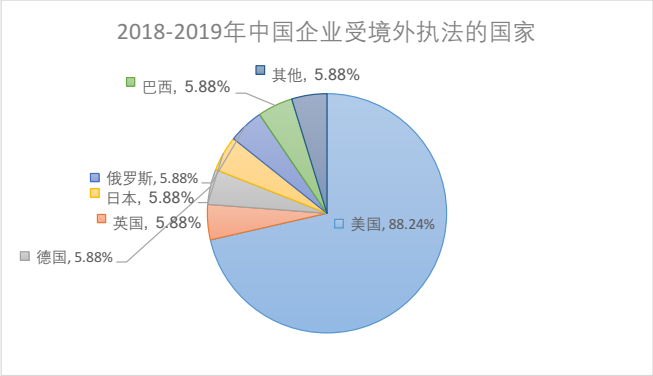
经济制裁/出口管制成为企业遭受境外执法的首要原因，反腐败及网络安全、数据/个人信息保护为重要原因

2018-2019年境外被执法的中国企业（包括国有企业、内资民企、中外合资企业以及外商独资企业）当中，经济制裁/出口管制成为企业遭受境外执法或处罚的首要原因，超过1/3的被执法企业2018-2019年遭受过经济制裁/出口管制执法。除此之外，反腐败及网络安全、数据/个人信息保护也是中国企业遭受境外执法的重要原因，其各自所占比例约为29%和24%。（见图1）

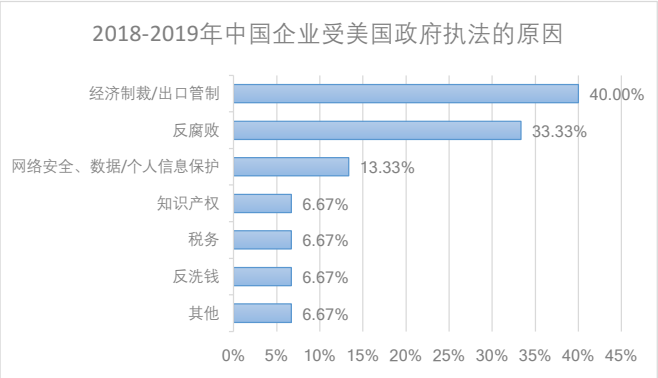


（图1：2018-2019年中国企业（包括国有企业、内资民企、中外合资企业以及外商独资企业）受境外执法的原因）

值得一提的是，2018-2019年境外被执法的中国企业当中，遭受到美国政府执法的企业从55%上升到88%；（见图2）并且，因经济制裁/出口管制遭受美国政府执法的中国企业从8%上升了四倍至40%，而反腐败仍作为除了经济制裁/出口管制之外，美国对中国企业执法的最重要原因。可以见得，中国企业受到美国执法，尤其是经济制裁/出口管制方面的影响增大，并且美国仍对反腐败执法十分重视。（见图3）



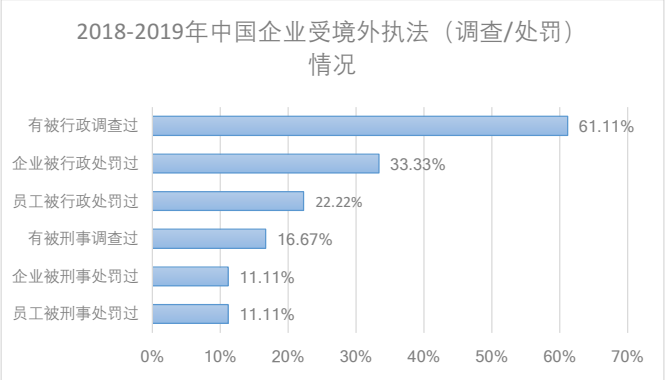
（图2：2018-2019年中国企业受境外执法的国家）



（图3：2018-2019年中国企业受美国政府执法的原因）

行政调查仍为企业遭受境外执法的首要类型，同时企业受刑事调查的比例增高

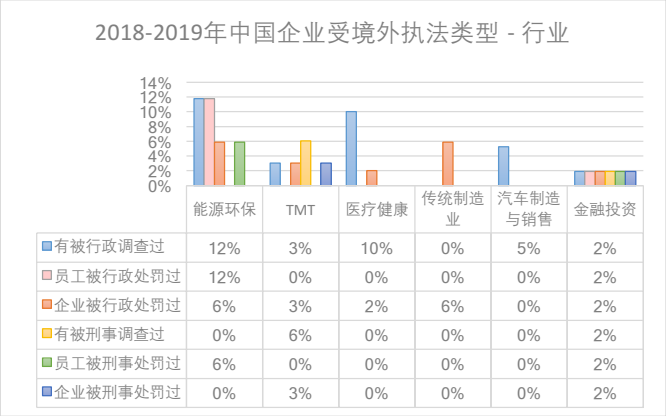
2018-2019年，受到境外执法的企业中约61%所遭受的执法类型为行政调查，为遭受境外执法的首要类型，且较去年比例增高了11%；行政处罚方面，三分之一的企业被处罚，处罚个人的比例由此前年度的14%增长至22%。2018-2019年受到刑事调查的公司比例约为17%；其中，虽然受到刑事处罚的个人的比例下降了2%至11%，但遭受到刑事处罚的公司由此前年度的没有增长至11%。（见图4）



（图4：2018-2019年中国企业受境外执法（调查/处罚）情况）

能源环保行业为2018-2019年度遭遇境外执法的高风险行业

2018-2019年度，能源环保行业有高达12%的企业遭遇境外行政调查，且有12%的员工遭受到行政处罚、6%的员工甚至遭受过刑事处罚，为行业中员工遭受处罚比例最高的。相较此前年度蓝皮书数据，2018-2019年TMT行业的员工受行政、刑事处罚的比例有所下降。（见图5）



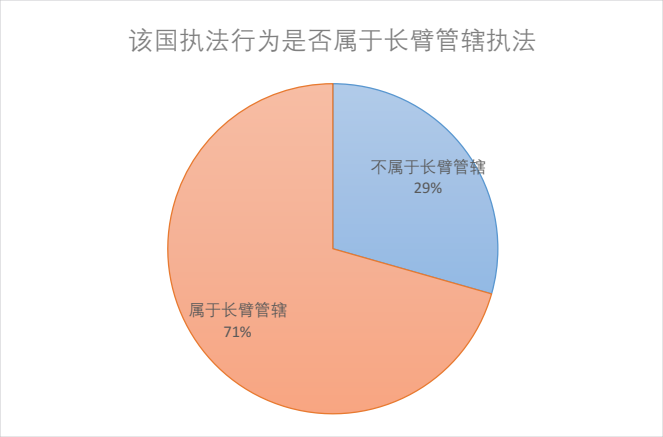
	能源环保	TMT	医疗健康	传统制造业	汽车制造与销售	金融投资
有被行政调查过	12%	3%	10%	0%	5%	2%
员工被行政处罚过	12%	0%	0%	0%	0%	2%
企业被行政处罚过	6%	3%	2%	6%	0%	2%
有被刑事调查过	0%	6%	0%	0%	0%	2%
员工被刑事处罚过	6%	0%	0%	0%	0%	2%
企业被刑事处罚过	0%	3%	0%	0%	0%	2%

（图5：2018-2019年中国企业受境外执法类型－行业）

（二）境外执法的手段及风险

超七成受境外国家执法的企业系受长臂管辖执法

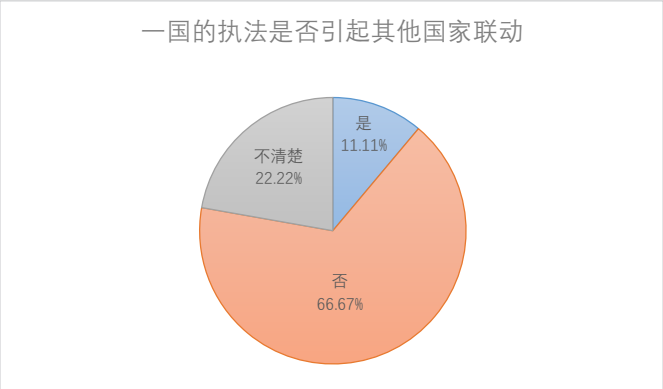
调研发现，超七成受境外国家执法的企业系受境外长臂管辖执法。（见图6）



（图6：该国执法行为是否属于长臂管辖执法）

预防跨境执法的联动风险

调研发现，有11%曾遭受境外执法的企业在受到一个国家执法后又引起其他国家执法的联动。（见图7）



（图7：一国的执法是否引起其他国家联动）

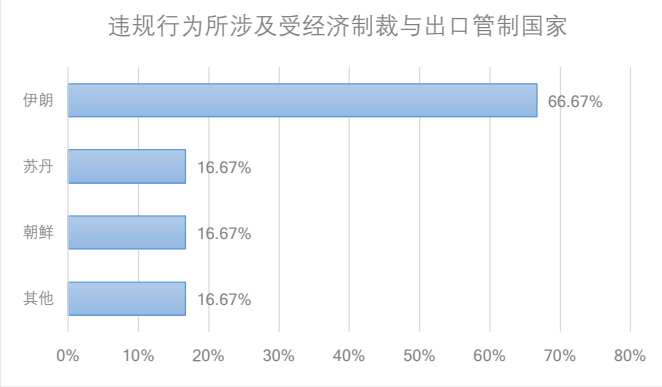
（三）企业受境外经济制裁/出口管制执法的情况

三分之二企业的违规行为涉及伊朗；三分之二企业被执法后业务受限；BIS和OFAC为进行经济制裁/出口管制执法的主要执法部门

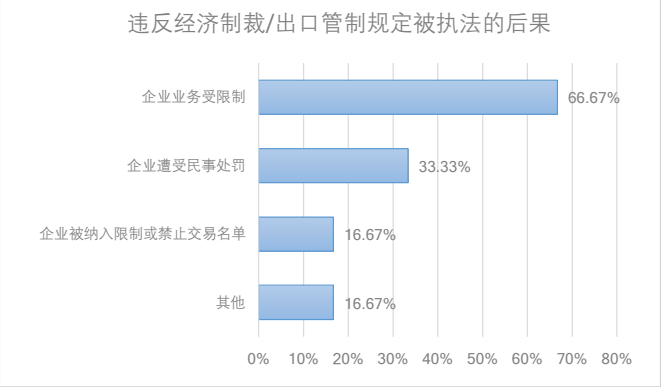
如前所述，2018-2019年境外被执法的中国企业中，经济制裁/出口管制成为企业遭受境外执法或处罚的首要原因，占其中的三分之一。（见图1）

因经济制裁/出口管制被执法的企业中，有三分之二企业的违规行为涉及伊朗，其次是苏丹和朝鲜，均占比六分之一。（见图8）此外，其中有三分之二的企业因受经济制裁/出口管制执法，导致其业务受到限制。还有超三成的企业因此遭受民事处罚。（见图9）

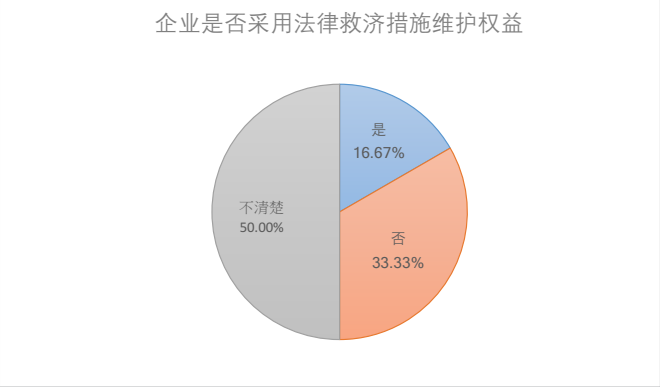
而在作出经济制裁/出口管制执法的执法部门当中，被调研企业受美国商务部工业安全局（BIS）和财政部海外资产办公室（OFAC）执法占比最高，均占比50%，其次是美国司法部（DOJ），占比17%。（见图10）



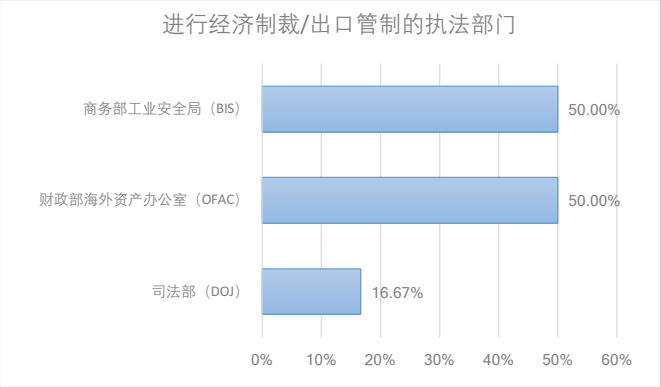
（图8：违规行为所涉及受经济制裁与出口管制国家）



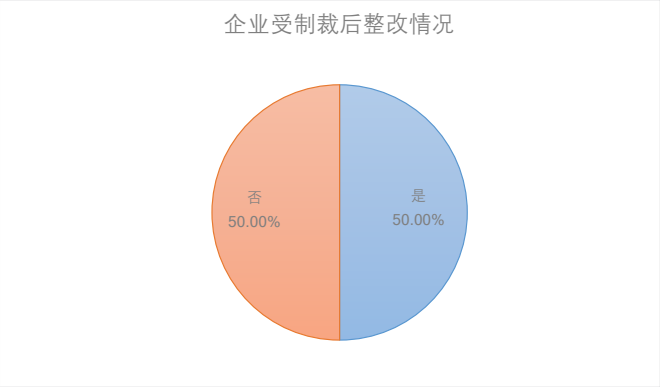
（图9：违反经济制裁/出口管制规定被执法的后果）



（图11：企业是否采用法律救济措施维护权益）



（图10：进行经济制裁/出口管制的执法部门）



（图12：企业受制裁后整改情况）

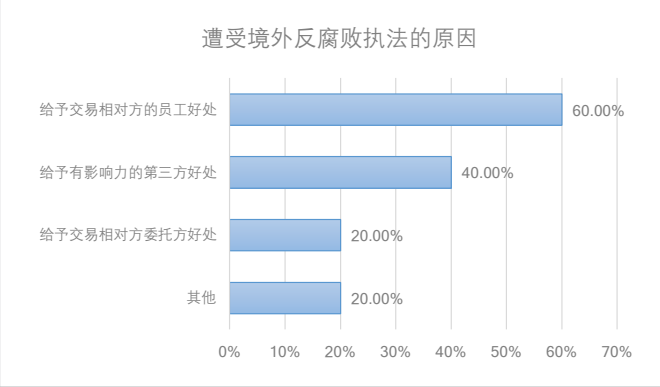
仅17%的企业采取法律救济措施；有一半企业受制裁后进行整改

2018-2019年仅17%被境外经济制裁/出口管制的企业采取法律救济措施维护自身权益。（见图11）有一半的企业受制裁后进行整改。（见图12）

（四）企业受境外反腐败执法的情况

给予交易相对方的员工好处是企业或员工受到境外反商业贿赂执法的首要原因

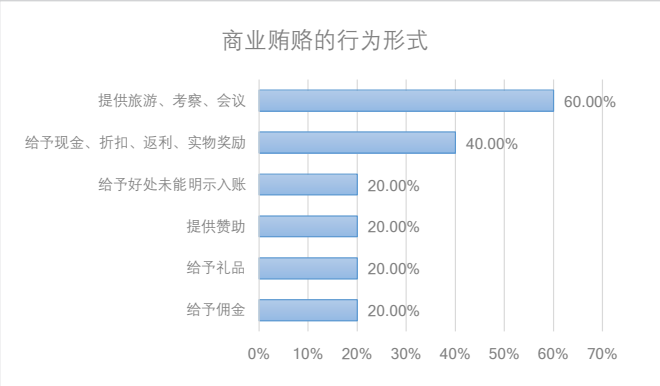
2018-2019年给予交易相对方的员工好处是企业或员工遭受反商业贿赂调查或处罚的首要原因，其比例由此前年度的50%上升至60%。另外，约40%的企业是因为给予有影响力的第三方好处而受到反商业贿赂调查或处罚。除此之外，1/5的企业因为给予交易相对方委托方好处受到调查或处罚。（见图13）



（图13：遭受境外反腐败执法的原因）

提供旅游、考察、会议为受境外反腐败执法的主要查处贿赂形式

在2018-2019年因商业贿赂受到境外执法的企业中，提供旅游、考察、会议为主要查处的商业贿赂形式，从去年的0%上升至50%；给予现金、折扣、返利、实物奖励等，仍为境外反贿赂执法重点查处的商业贿赂形式之一，占四成。（见图14）



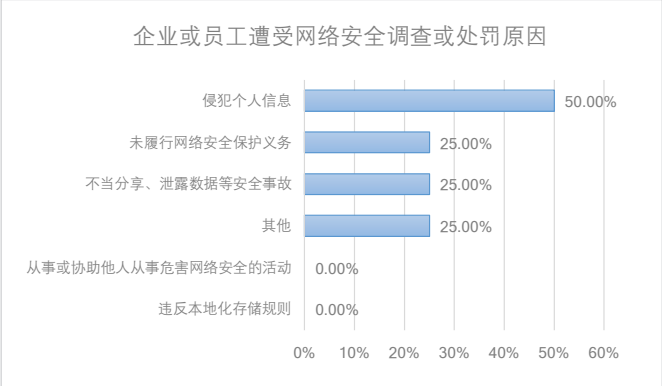
（图14：商业贿赂的行为形式）

（五）企业受境外网络安全执法的情况

侵犯个人信息是企业或员工遭受网络安全调查或者处罚的首要原因

如前所述，2018-2019年境外被执法的中国企业当中，网络安全、数据/个人信息保护在企业遭受境外执法或处罚的原因中位列第三，占比约24%，仅次于经济制裁/出口管制和反腐败。（见图1）

侵犯个人信息是企业或员工遭受网络安全调查或者处罚的首要原因，占比50%，其次是未履行网络安全保护义务和不当分享、泄露数据等安全事故，均占比25%。企业或员工应注重个人信息保护。（见图15）



（图15：企业或员工遭受网络安全调查或处罚原因）

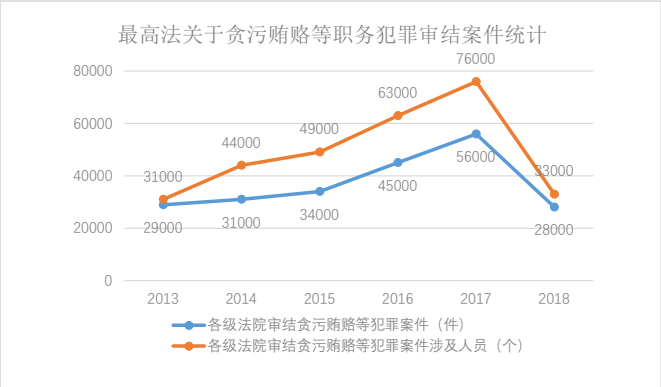
二、国内立法及执法变化对企业的影响

（一）国内立法及执法动态及企业的应对

2018年度职务犯罪立案侦查及贪污贿赂案件审结情况：建立国家监察委员会，保持惩治腐败高压态势

2019年3月12日最高人民法院以及最高人民检察院在第十三届全国人民代表大会第二次会议上提交工作报告。2018年度各级法院审结的贪污贿赂等犯罪案件与涉及人员大幅下降，这是由于16年以来密集的反腐案件于去年进入审判期且进一步结案者多。（见图16）但2018年最高检工作报告显示，最高检积极配合国家监察体制改革，受理各级监委移送职务犯罪16092人，已起诉9802人，不起诉250人，退回补充调查1869人次，不起诉率、退查率同比分别下降9.5%和37%。

2019年1月11日中央纪委国家监委在中国共产党第十九届中央纪律检查委员会第三次全体会议上提交工作报告。2018年建立国家监察体系总体框架立案审查调查中管干部68人，涉嫌犯罪移送司法机关15人，共对52.6万名党员作出党纪处分。坚持无禁区、全覆盖、零容忍，坚持重遏制、强高压、长震慑，坚持受贿行贿一起查，“打虎”、“拍蝇”、“猎狐”多管齐下。

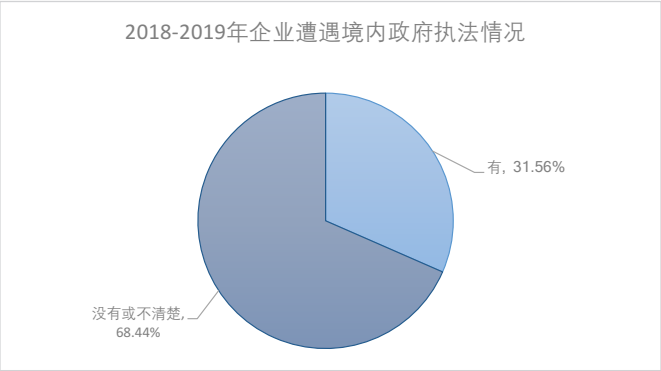


（图16：2018年最高人民法院工作报告）

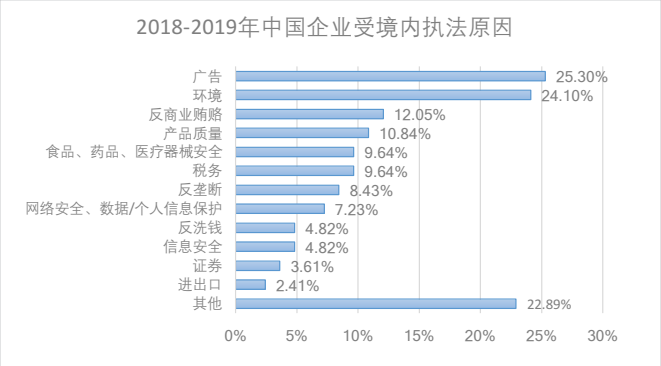
（二）企业受境内执法情况

广告违法为企业遭受境内执法的首要原因、环境违法为重要原因

近1/3参与调研的企业曾在2018-2019年遭受中国政府的调查或执法，与此前年度蓝皮书数据基本持平。（见图17）其中，25%遭受到调查执法的企业是由于广告违法，其次是环境违法，由此前年度的12%翻倍至24%，环境执法强度有明显提高。反商业贿赂与产品质量紧随其后，分别以12%和11%的比例位列2018-2019年度中国企业受境内执法原因第3、4名，其中反商业贿赂执法比例与此前年度数据相比有较大变动，可能与新法对商业贿赂的认定做出了重大调整、新法下缺乏细化规则的指引以及中央和地方执法机构处于持续改革和整合过程中有关。（见图18）



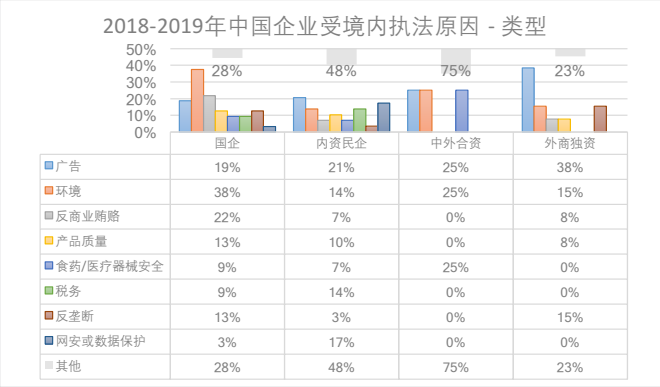
（图17：2018-2019年企业遭遇境内政府执法情况）



（图18：2018-2019年中国企业受境内执法原因）

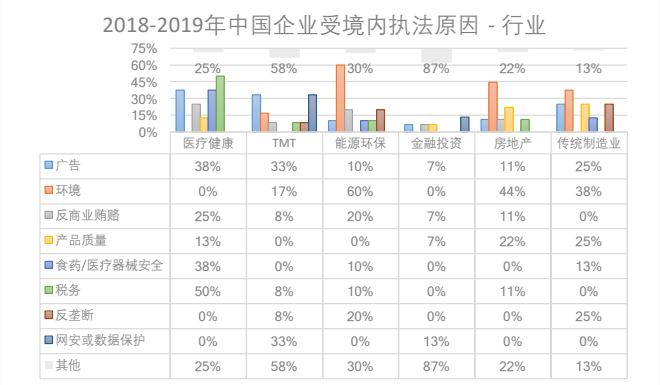
与此前年度数据相比，就企业类型而言，企业遭受境内执法的原因变化较大。广告违法层面，国企受境内广告执法的占比从4%上升至19%，但外商独资企业受广告执法的比例仍然最高，占38%。另外环境执法强度在2018-2019年有明显提高，国企因环境违法受境内执法的占比翻了一番，占比达38%。（见图19）

从行业来看，与此前年度蓝皮书数据相比，2018-2019年企业遭受境内执法的原因变化也较大。医疗健康行业在境内调查执法中受到较高关注，在广告、反商业贿赂、食药/医疗器械安全、税务上从受到执法的比例来看，医疗健康行业均为排名第一的高风险行业，特别是在税务执法中比较突出，50%医疗健康行业企业系由于税务于2018-2019年遭受境内执法。能源环保行业成为了环境违法执法最重要行业。TMT以及传统制造业企业则分别在受到境内网安/数据保护以及反垄断执法中占比最高。（见图20）



	国企	内资民企	中外合资	外商独资
广告	19%	21%	25%	38%
环境	38%	14%	25%	15%
反商业贿赂	22%	7%	0%	8%
产品质量	13%	10%	0%	8%
食药/医疗器械安全	9%	7%	25%	0%
税务	9%	14%	0%	0%
反垄断	13%	3%	0%	15%
网安或数据保护	3%	17%	0%	0%
其他	28%	48%	75%	23%

（图19：2018-2019年中国企业受境内执法原因 – 类型）

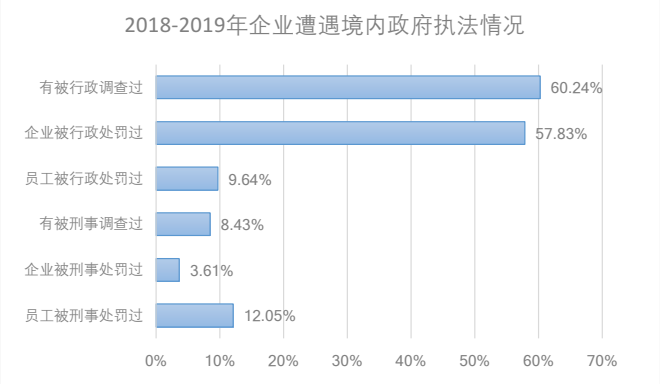


	医疗健康	TMT	能源环保	金融投资	房地产	传统制造业
广告	38%	33%	10%	7%	11%	25%
环境	0%	17%	60%	0%	44%	38%
反商业贿赂	25%	8%	20%	7%	11%	0%
产品质量	13%	0%	0%	7%	22%	25%
食药/医疗器械安全	38%	0%	10%	0%	0%	13%
税务	50%	8%	10%	0%	11%	0%
反垄断	0%	8%	20%	0%	0%	25%
网安或数据保护	0%	33%	0%	13%	0%	0%
其他	25%	58%	30%	87%	22%	13%

（图20：2018-2019年中国企业受境内执法原因 – 行业）

企业遭受境内执法中60%为行政调查，受行政处罚比例持续上升至58%

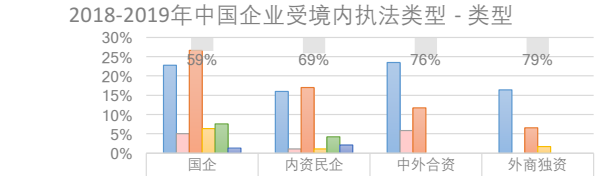
受到境内执法的企业中，超过60%的企业遭受到的执法类型为行政调查，为境内执法的首要类型；此外，企业遭受境内行政处罚的比例逐年上升，由2016年31%、上一年度43%上升至2018-2019年58%。企业遭受刑事调查的比例基本与上一年度持平。（见图21）



（图21：2018-2019年企业遭遇境内政府执法情况）

国企及其员工被行政或者刑事处罚的比例最高

调研结果显示，国企于2018-2019年遭受到行政和刑事调查或处罚的比例均处于较高水平，具体而言其受行政调查比例为23%、员工受行政处罚比例为5%、企业受行政处罚比例为27%、受刑事调查的比例为6%、员工受到刑事处罚的比例也为8%。（见图22）

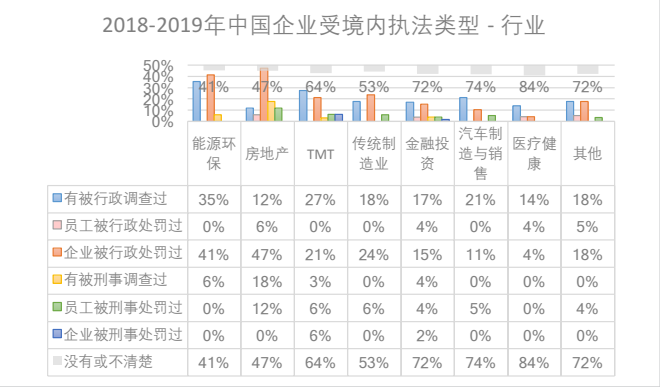


	国企	内资民企	中外合资	外商独资
有被行政调查过	23%	16%	24%	16%
员工被行政处罚过	5%	1%	6%	0%
企业被行政处罚过	27%	17%	12%	7%
有被刑事调查过	6%	1%	0%	2%
员工被刑事处罚过	8%	4%	0%	0%
企业被刑事处罚过	1%	2%	0%	0%
没有或不清楚	59%	69%	76%	79%

（图22：2018-2019年中国企业受境内执法类型 – 类型）

2018-2019年度遭遇境内执法的高风险行业：能源环保、房地产、TMT、传统制造业、金融投资、汽车制造与销售、医疗健康

2018-2019年度，能源环保、TMT、汽车制造与销售行业均有超过20%的企业遭遇境内行政调查。企业行政处罚方面，房地产和能源环保行业受行政处罚的比例高达47%和41%，接着依次是传统制造业24%、TMT 21%。员工行政处罚方面，房地产行业的情况比较突出。相较此前年度数据，2018-2019年房地产行业的企业遭遇境内刑事调查的比例由7%增长至18%，且该行业三分之二被调查企业的员工遭到刑事处罚。总体而言，房地产行业的监管力度持续增强。（见图23）

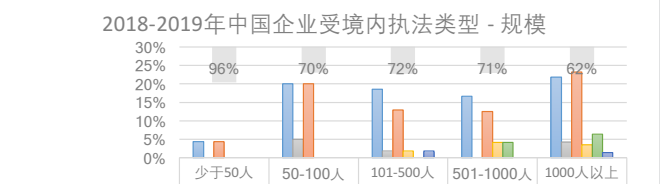


	能源环保	房地产	TMT	传统制造业	金融投资	汽车制造与销售	医疗健康	其他
有被行政调查过	35%	12%	27%	18%	17%	21%	14%	18%
员工被行政处罚过	0%	6%	0%	0%	4%	0%	4%	5%
企业被行政处罚过	41%	47%	21%	24%	15%	11%	4%	18%
有被刑事调查过	6%	18%	3%	0%	4%	0%	0%	0%
员工被刑事处罚过	0%	12%	6%	6%	4%	5%	0%	4%
企业被刑事处罚过	0%	0%	6%	0%	2%	0%	0%	0%
没有或不清楚	41%	47%	64%	53%	72%	74%	84%	72%

（图23：2018-2019年中国企业受境内执法类型 – 行业）

大型公司遭受境内执法强度较大，但中小型企业也存在受境内执法可能性

与此前年度蓝皮书数据相同，大型公司被执法的可能性较高。1000人以上的企业被行政或刑事调查的概率为26%。中小型企业遭受境内政府调查或执法情况也依旧存在，其中遭到行政处罚的比例有所上升。（见图24）



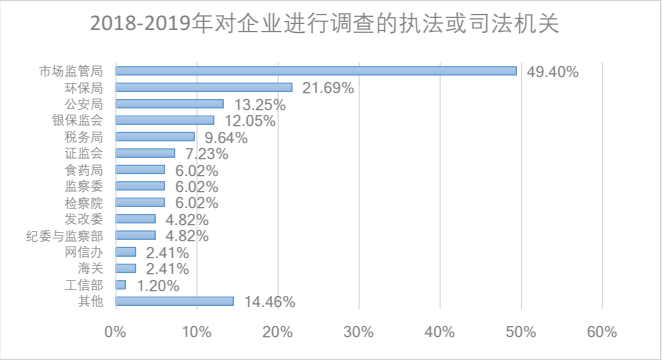
	少于50人	50-100人	101-500人	501-1000人	1000人以上
有被行政调查过	4%	20%	19%	17%	22%
员工被行政处罚过	0%	5%	2%	0%	4%
企业被行政处罚过	4%	20%	13%	13%	23%
有被刑事调查过	0%	0%	2%	4%	4%
员工被刑事处罚过	0%	0%	0%	4%	6%
企业被刑事处罚过	0%	0%	2%	0%	1%
没有或不清楚	96%	70%	72%	71%	62%

（图24：2018-2019年中国企业受境内执法类型 – 规模）

（三）境内执法的主体、手段及变化

市场监管局为最主要的境内执法主体

市场监管局、环保局、公安局以及银保监会为2018-2019年度对企业进行调查和执法的主要机关，其中，对企业进行调查执法的案件49%由市场监管局发起，占将近半数，环保局执法比例由此前年度的10%翻一番至22%，公安局和银保监会的执法比例各自为13%和12%。相较此前年度蓝皮书数据，除工商局，即机构改革后的现市场监管局，近两年一直保持半数以上的执法量以外，环保局、银保监会执法量有明显增长，公安局、税务局和证监会始终维持较高执法活跃度。（见图25）

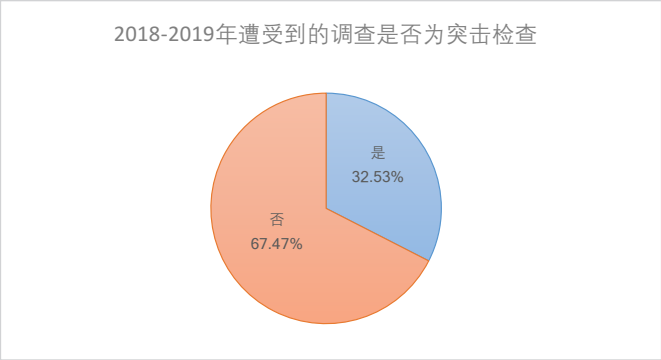


（图25：2018-2019年对企业进行调查的执法或司法机关）

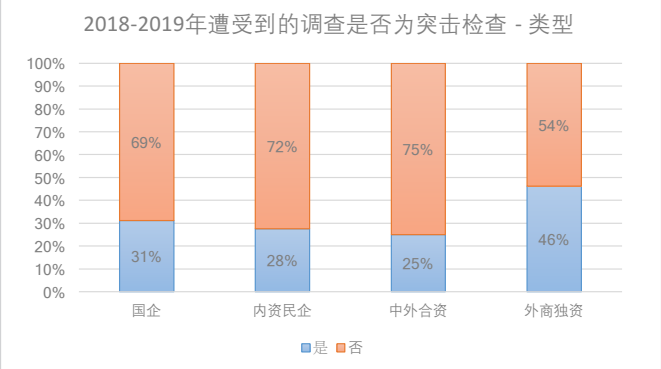
突击检查仍是境内执法的常用手段；但企业就此专门制定政策的比例下降（仅约1/5的企业有针对中国的突击检查政策）

2018-2019年遭受突击检查的企业比例约占33%，从企业类型角度，外商独资企业更易受到突击检查，约占46%，其次是国企约占31%。（见图26、图27）从行业层面分析，针对能源环保、TMT和医疗健康行业的突击检查比较多，分别为60%、50%以及38%。（见图28）

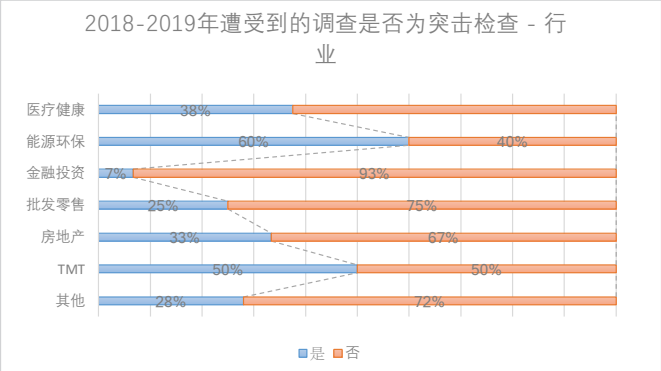
尽管如此，只有约22%的企业制定了针对中国的突击检查政策，不足16%的企业具备全球统一机制，皆相比于去年略微下降3~4%。而短期没有制定突击检查计划的企业达到33%。（见图29）



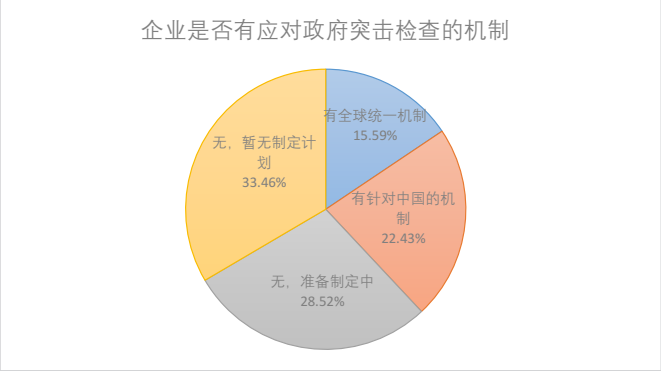
（图26：2018-2019年遭受到的调查是否为突击检查）



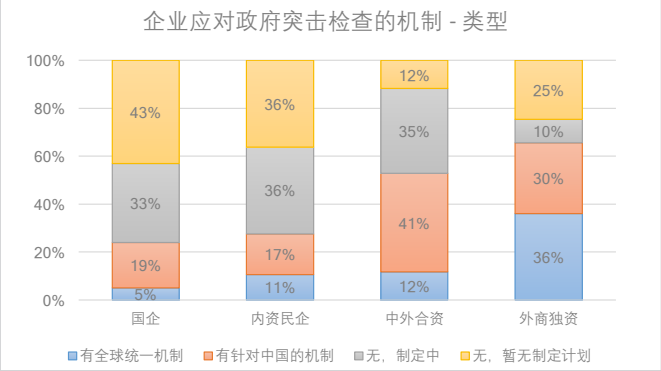
（图27：2018-2019年遭受到的调查是否为突击检查 – 类型）



（图28：2018-2019年遭受到的调查是否为突击检查 – 行业）



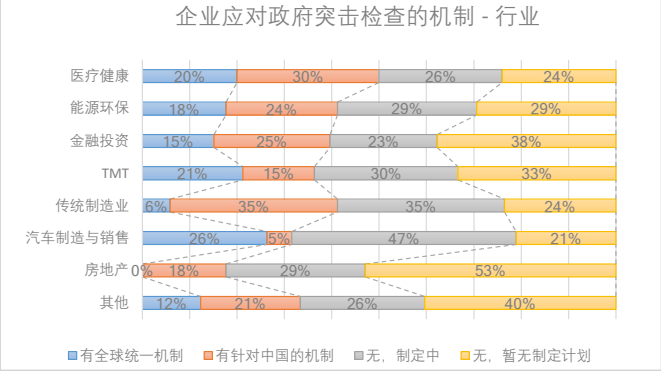
（图29：企业是否有应对政府突击检查的机制）



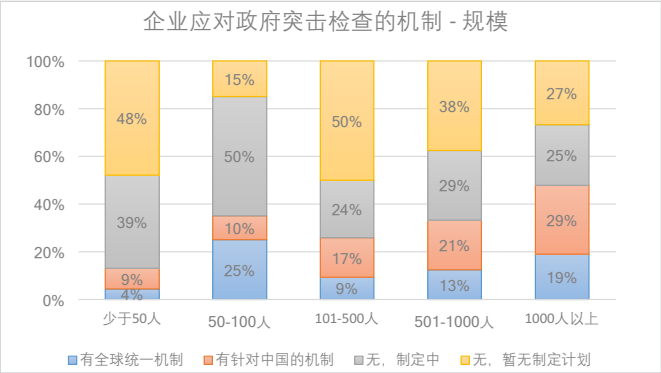
（图30：企业应对政府突击检查的机制 – 类型）

外资企业、医疗健康行业应对政府突击检查机制相对更为完善

与此前年度蓝皮书数据相同，尽管参与调研企业整体应对政府突击检查的机制均不太完善，但相较而言，外资企业（包括中外合资企业以及外商独资企业）具备政府突击检查机制的比例较高，外商独资企业具备政府突击检查机制的比例为66%，且其针对中国的应对政府突击检查机制比例略有上升。（见图30）就行业而言，医疗健康行业有一半的企业目前暂无应对政府突击检查的机制，其他行业中比例最高的房地产有高达82%的企业暂无应对政府突击检查的机制，但相比于去年93%没有突击检查机制已经有所改善。（见图31）从企业规模角度，整体而言规模越大，有应对政府突击检查机制的企业比例越高，但整体应对水平仍然较低，1000人以上的大型企业也不足50%。（见图32）鉴于突击检查是境内执法的常用手段，企业应尽快制定或完善其相应机制。



（图31：企业应对政府突击检查的机制 – 行业）

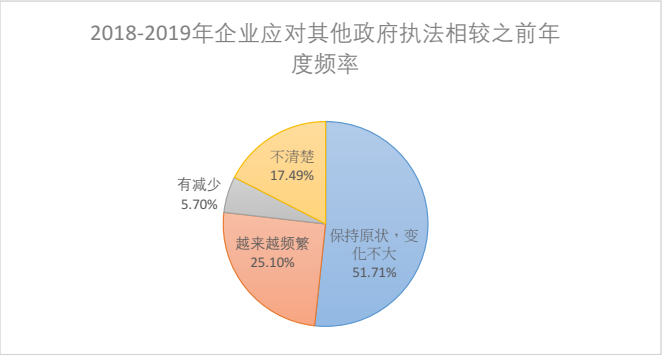


（图32：企业应对政府突击检查的机制 – 规模）

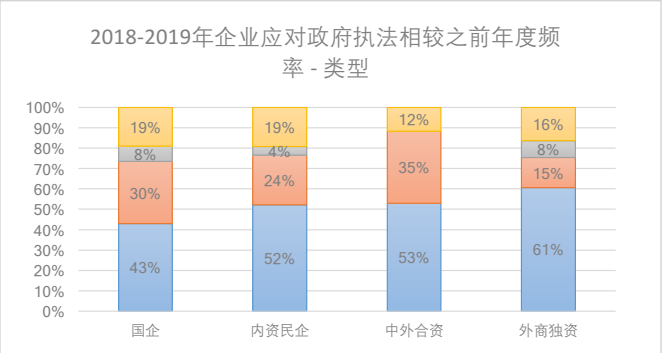
近8成企业认为2018-2019年度境内执法频率变化不大或有所提高

约52%的企业认为2018-2019年度相比于去年，其应对政府执法的频率保持不变，而有1/4的企业认为执法频率有所提高，与此前年度数据相比增加了5%。（见图33）

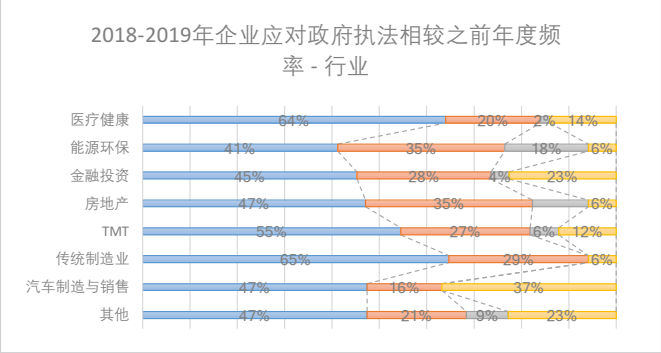
从企业类型角度，相较外商独资企业和民企，更多的国企认为政府执法的频率有所提高，占比30%。（见图34）就行业而言，能源环保行业企业更多的认为政府执法的频率有所提高，占比35%，该感受与前述“环保局执法比例由此前年度的10%翻一番至22%”相符。（见图25及图35）



（图33：2018-2019年企业应对政府执法相较之前年度频率）



（图34：2018-2019年企业应对政府执法相较之前年度频率 – 类型）

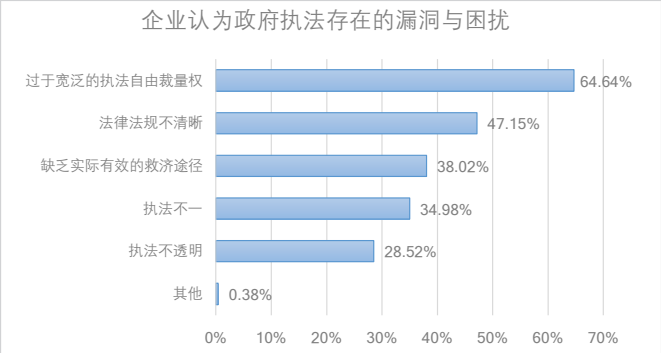


（图35：2018-2019年企业应对政府执法相较之前年度频率 – 行业）

（四）企业对境内政府执法的困惑

政府过于宽泛的执法自由裁量权仍为企业最大的困扰

调研发现，高达约65%的企业认为政府过于宽泛的执法自由裁量权给其带来较大困扰，占比相较去年有小幅提升。此外，认为“法律法规不清晰”的比例由此前年度的40%上升至47%，成为企业对境内政府执法的第二大困惑，紧接着为“缺乏实际有效的救济途径”、“执法不一”、“执法不透明”，相应比例为38%、35%和29%。该结果与此前年度调研数据差异不大，企业整体感受的变化较小。（见图36）

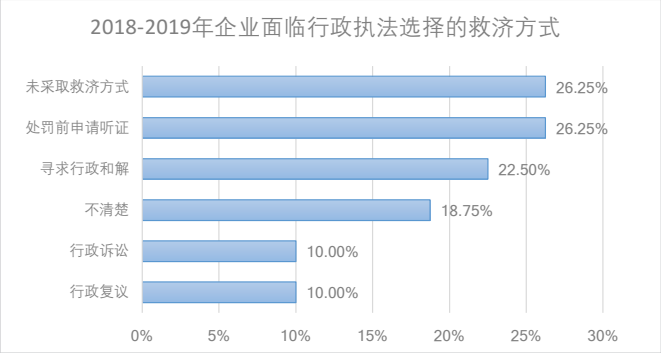


（图36：企业认为政府执法存在的漏洞与困扰）

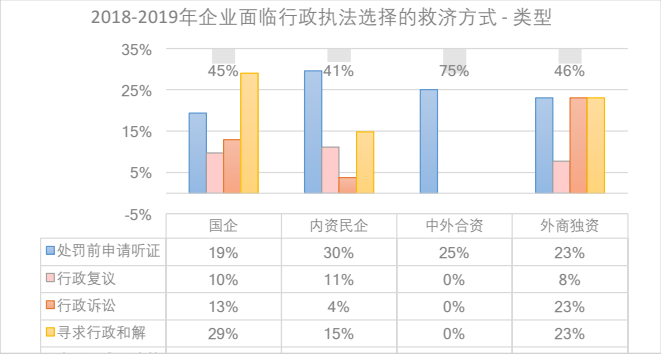
面临行政执法时选择对抗性救济措施的企业较少；房地产行业的企业100%采取救济措施

针对救济途径，调研发现，企业在面临行政执法时，愿意处罚前申请听证和寻求行政和解的占比相对较多，达到26%和23%；选择对抗性措施，如行政复议或行政诉讼的，同比此前年度有小幅增长，但仍然相对较少，均只占10%。（见图37）

就企业类型而言，国企、内资民企以及外商独资企业愿意处罚前申请听证和寻求行政和解的占比均接近50%，相较其他类型企业，外商独资企业愿意选择对抗性措施，如行政复议或行政诉讼的占比最高，约占31%。（见图38）



（图37：2018-2019年企业面临行政执法时选择的救济方式）



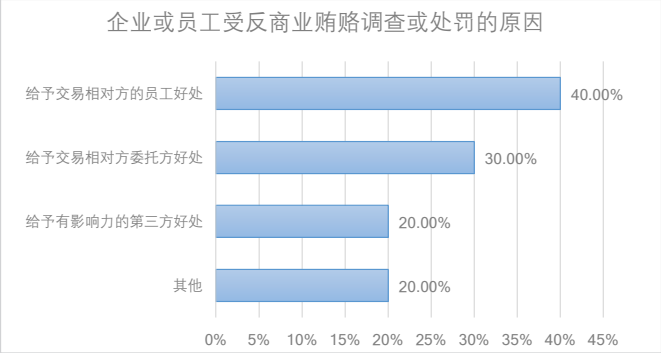
	国企	内资民企	中外合资	外商独资
处罚前申请听证	19%	30%	25%	23%
行政复议	10%	11%	0%	8%
行政诉讼	13%	4%	0%	23%
寻求行政和解	29%	15%	0%	23%

（图38：2018-2019年企业面临行政执法时选择的救济方式 – 类型）

（五）企业受境内反腐败执法情况

给予交易相对方的员工好处是企业或员工受到反商业贿赂执法的首要原因

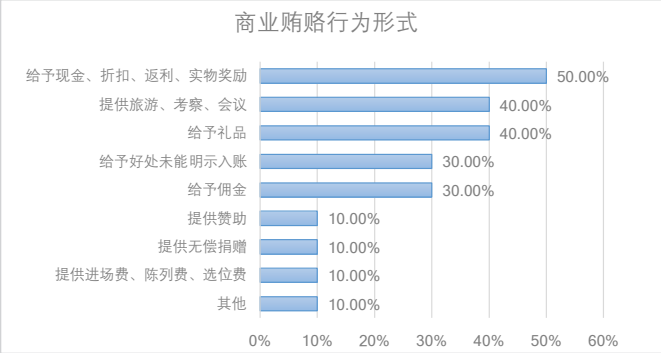
新《反不正当竞争法》自2018年1月1日起实施后，排除了“给予交易相对方好处”作为商业贿赂的形式，故2018-2019年相较于此前年度数据，企业或员工遭受反商业贿赂执法的首要原因由“给予交易相对方好处”变更为“给予交易‘相对方的员工’好处”，其比例达40%。还有约1/3的企业是因为给予交易相对方委托方好处而受到反商业贿赂调查或处罚。除此之外，还有1/5的企业因给予有影响力的第三方好处受到调查或处罚。（见图39）



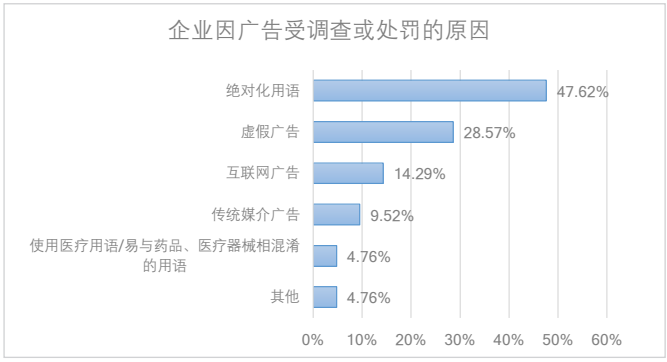
（图39：企业或员工受反商业贿赂调查或处罚的原因）

给与现金、折扣、返利、实物奖励等为受执法企业或员工主要提供的商业贿赂形式

在2018-2019年因商业贿赂受调查或处罚的企业中，给予现金、折扣、返利、实物奖励等为提供商业贿赂的主要形式，相较此前年度的46%进一步提升至50%；其次是提供旅游、考察、会议和给予礼物，均占比40%；再次是给予好处未能明示入账和给予佣金，均占比30%。其余皆在10%。（见图40）



（图40：商业贿赂行为形式）



（图41：企业因广告受调查或处罚的原因）

（六）企业受境内广告执法的情况

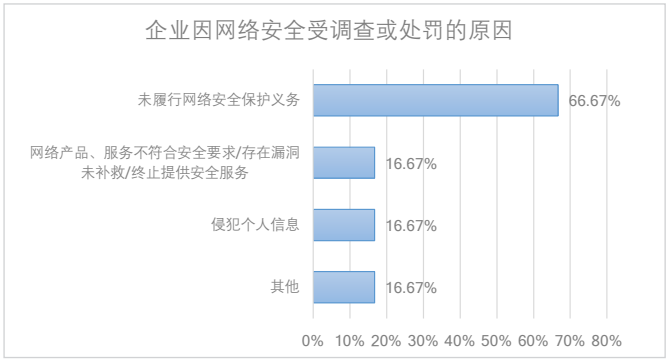
如前所述，广告违法是导致企业遭受境内执法的首要原因，占比约为25%。（见图18）广告执法在各种类型企业中都有所体现，但外商独资企业是广告执法的重点，外商独资企业2018-2019年遭遇调查或处罚的首要原因是广告执法，约占四成，其遭遇广告执法比例高于国企和内资民企。（见图19）因广告遭遇执法的高风险行业有医疗健康、TMT、传统制造业，三者2018-2019年遭遇调查或处罚的原因均有三至四成左右为广告执法，远高于其他行业。（见图20）

与此前年度数据相同，因发布违法广告而受到行政执法的企业中，因为在广告中使用绝对化用语受到调查或处罚的企业占比最高，其次为虚假广告，今年分别占比为48%、29%。从被执法的广告形式上来看，互联网广告遭受调查或处罚的比例仍然高于传统媒介广告，足以见得执法机关对互联网广告管控的重视。（见图41）

（七）企业受境内网络安全执法的情况

如前所述，2017年6月1日中国首部《网络安全法》（下称“《网安法》”）开始施行，执法机关对于网络安全的执法在国企和内资民企中都有所体现，但主要体现在内资民企。有17%的内资民企于2018-2019年遭受过网络安全执法。（见图19）此外，因网络安全遭遇执法的高风险行业有TMT和金融投资行业，两行业2018-2019年遭遇调查或处罚的原因中分别有33%以及13%为网络安全。（见图20）

2018-2019年因网络安全而受到行政执法的企业中，企业因未履行网络安全保护义务受到调查或处罚的比例由17%上升至2/3，可以见得2018-2019年执法机关对于网络安全保护义务的关注急剧上升。（见图42）



（图42：企业因网络安全受调查或处罚的原因）

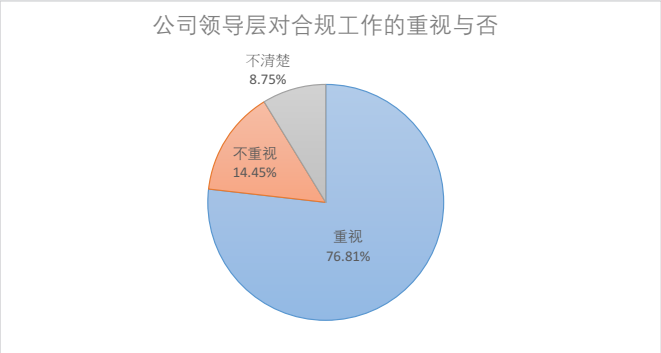
三、企业合规体系建设

（一）企业对合规工作的重视程度

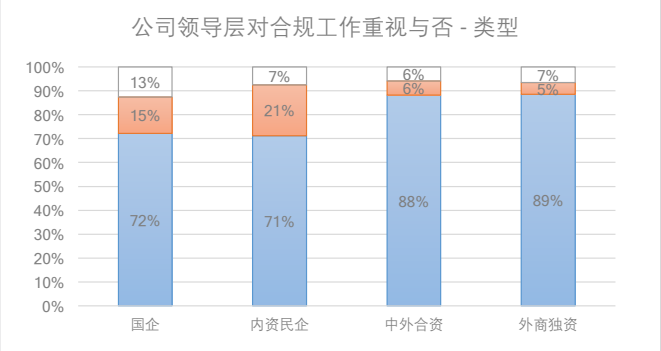
近4/5的公司领导层对重视合规工作；内资企业以及房地产行业对合规工作重视程度仍旧最低

参加调研的企业中有近4/5的领导层重视合规工作。（见图43）从企业类型层面看，外资企业的领导层仍旧比内资企业（包含国企、内资民企）领导层更重视合规工作：与此前年度数据一致，约有9成外资企业领导层重视合规工作，而内资企业领导层仅有七成重视合规工作。（见图44）

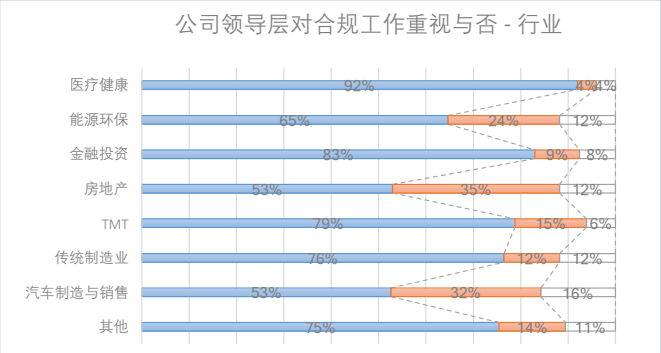
2018-2019年，医疗健康领导层对合规工作最为重视，重视率达到92%，而相较于此前年度数据，医疗健康企业受境内政府执法的比例由31%下降至16%；相反的，房地产行业作为今年仅次于能源环保的境内被执法高风险行业，其企业管理层重视合规工作的比例由此前年度的64%再度降至53%。可以推测领导层对于合规工作的重视程度，与企业受执法风险成反比。（见图23、图45）



（图42：公司领导层对合规工作的重视与否）



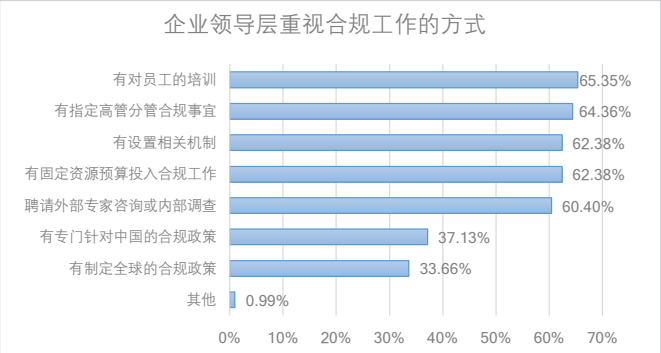
（图44：公司领导层对合规工作重视与否 – 类型）



（图45：公司领导层对合规工作重视与否 – 行业）

企业领导层通过多种方式重视合规工作，但较少采取制定合规政策的方式；国企和能源环保行业企业对合规工作重视程度较低

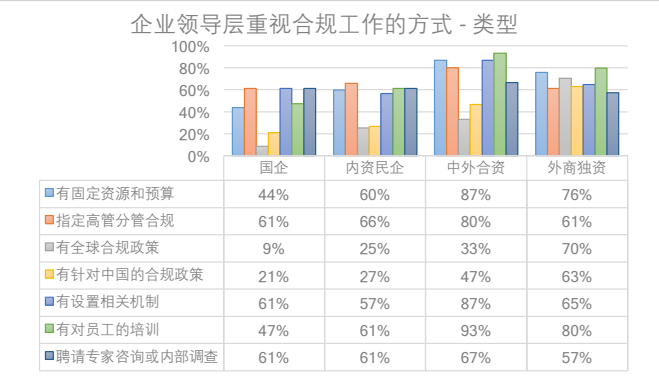
企业领导层通过对员工培训、指定高管分管合规事宜、设置相关机制、固定资源预算投入合规工作和聘请外部专家咨询或内部调查等方式，重视并开展合规工作。在领导层重视合规工作的企业当中，采取上述方式的领导层均占比超过60%，但是有制定全球或专门针对中国合规政策的企业领导层皆只占被调研企业的三分之一左右。（见图46）



（图46：企业领导层重视合规工作的方式）

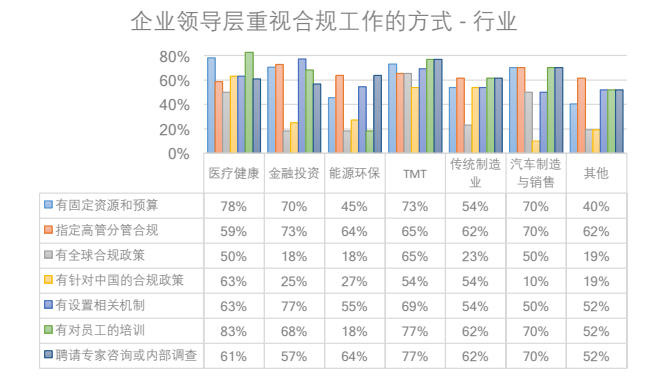
企业类型角度，外资企业领导层会普遍采取更为多样化的方式开展合规工作，同时更加注重对员工的培训和有固定资源预算投入合规工作，比例在75%以上，远高于国企和民企。仅有9%的受调研国企领导层会制定全球合规政策，在中央政府不断出台规范企业海外经营的意见、指引的大背景下，全球合规政策的缺失应引起国企领导层重视。（见图47）

从行业角度，医疗健康和TMT行业的企业管理层会普遍采取更为均衡且多样化的方式开展合规工作，同时相比较其他行业，更加注重对员工培训和制定全球合规政策，能源环保行业在上述两方面均处于行业垫底水平，均占比18%，面对环保局于2018-2019年加强执法，执法比例由此前年度的10%翻一番至22%的执法情况，（见图25）能源环保行业的企业应更加重视并开展合规工作。（见图48）



	国企	内资民企	中外合资	外商独资
有固定资源和预算	44%	60%	87%	76%
指定高管分管合规	61%	66%	80%	61%
有全球合规政策	9%	25%	33%	70%
有针对中国的合规政策	21%	27%	47%	63%
有设置相关机制	61%	57%	87%	65%
有对员工的培训	47%	61%	93%	80%
聘请专家咨询或内部调查	61%	61%	67%	57%

（图47：企业领导层重视合规工作的方式 – 类型）



	医疗健康	金融投资	能源环保	TMT	传统制造业	汽车制造与销售	其他
有固定资源和预算	78%	70%	45%	73%	54%	70%	40%
指定高管分管合规	59%	73%	64%	65%	62%	70%	62%
有全球合规政策	50%	18%	18%	65%	23%	50%	19%
有针对中国的合规政策	63%	25%	27%	54%	54%	10%	19%
有设置相关机制	63%	77%	55%	69%	54%	50%	52%
有对员工的培训	83%	68%	18%	77%	62%	70%	52%
聘请专家咨询或内部调查	61%	57%	64%	77%	62%	70%	52%

（图48：企业领导层重视合规工作的方式 – 行业）

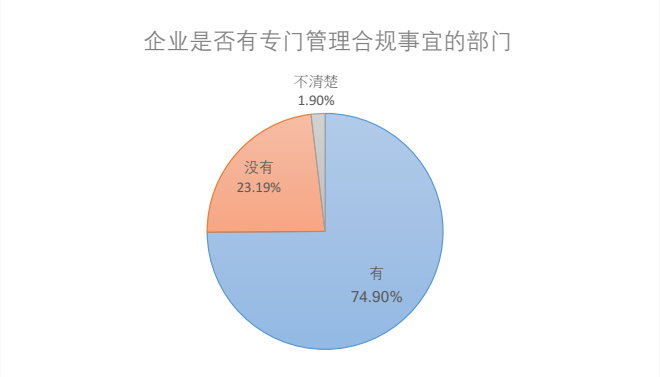
（二）企业合规部门建设

外商独资企业以及医疗健康行业存在合规部门的比例较高；没有专门管理合规事宜部门的主要原因系企业不重视

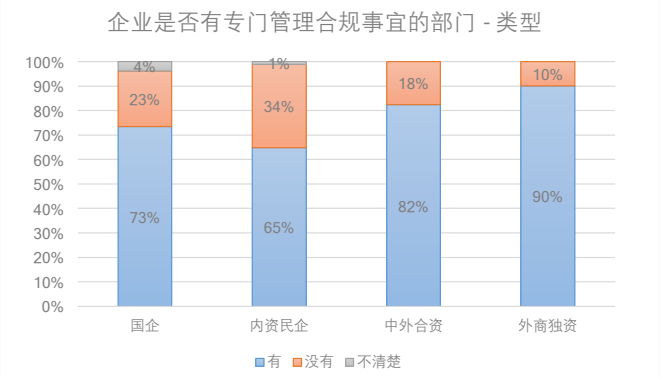
被调研的企业中，有近四分之三的企业存在专门管理合规事宜的部门，比去年上升了约四分之一。（见图49）不同类型的企业，设置专门管理合规事宜的部门比例皆有所增加，尤其与此前年度相比，2018-2019年设有专门管理合规事宜部门的国企从32%上升至73%；外商独资企业仍然相对完善，设置专门管理合规事宜部门的比例由此前年度的82%稳步上升至90%。（见图50）

从行业角度来说，医疗健康行业建立专门管理合规事宜的部门最多，占90%，紧随其后是占89%的金融投资行业。（见图51）就规模角度而言，企业是否有专门的合规管理部门，与企业规模呈较强的正相关性，1000人以上的大型企业建立相关部门的比例最高，约85%，100人以下的小型公司，不足60%。（见图52）

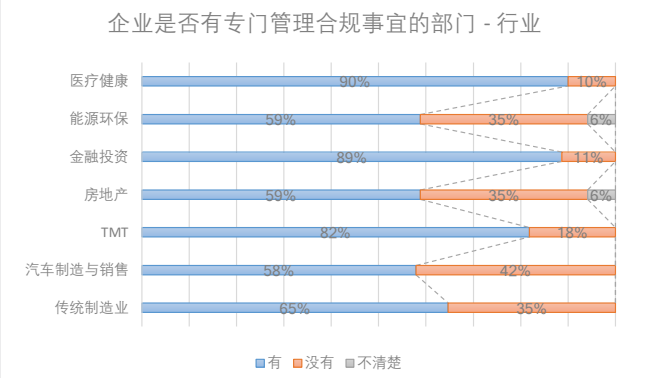
调研显示，46%没有管理合规事宜部门的原因为企业不重视，其次是业务部门自我管理，占比41%。结合前述分析，执法高风险行业应重视合规部门建设。（见图53）



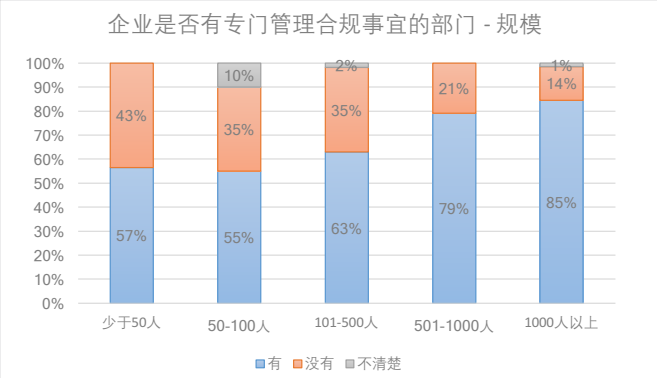
（图49：企业是否有专门管理合规事宜的部门）



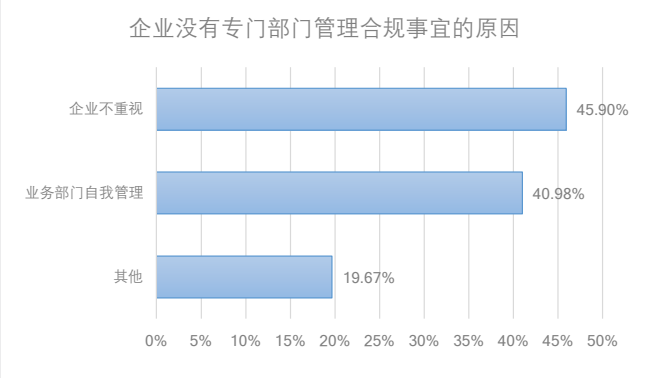
（图50：企业是否有专门管理合规事宜的部门 – 类型）



（图51：企业是否有专门管理合规事宜的部门 – 行业）



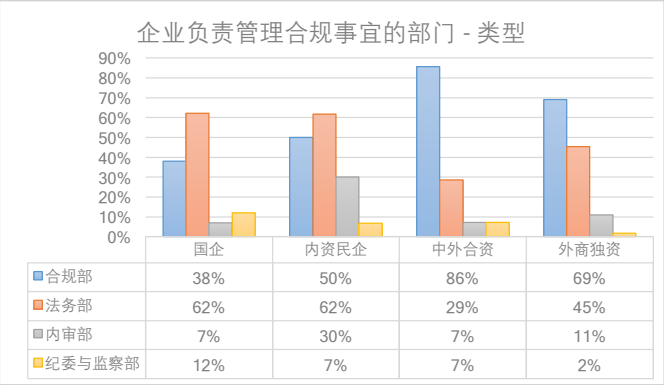
（图52：企业是否有专门管理合规事宜的部门 – 规模）



（图53：企业没有专门部门管理合规事宜的原因）

外企多以合规部管理合规事宜，国企、内资民企中法务部扮演重要角色

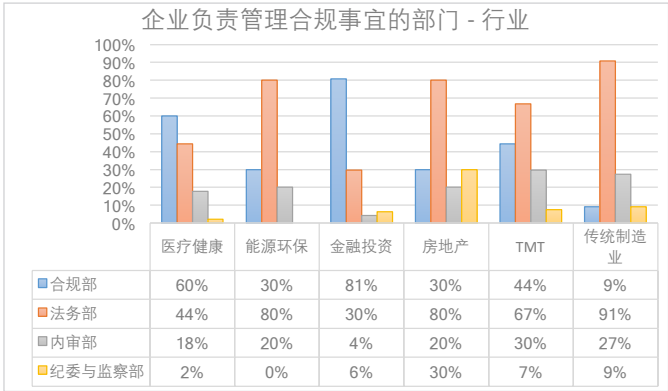
外资企业管理合规事宜的部门仍以合规部为主，合规职能相对独立，与法务部职责划分较明确。国企由法务部管理合规事宜的比例较之此前年度数据有较大幅提高，由40%增长至62%，并取代纪委与监察部扮演主导角色。民企与国企相同，法务部主要管理合规事宜，占62%。（见图54）



（图54：企业负责管理合规事宜的部门 – 类型）

金融投资行业合规部较为独立

81%的金融投资行业企业由合规部负责管理合规事宜，相较此前年度的61%有较大幅度增长，远高于其他行业。其次为医疗健康行业，有60%是通过合规部门负责合规事宜。TMT行业有近一半企业已设立专门负责管理合规事宜的部门。而传统制造业有高达91%的企业由法务部负责管理合规事务，能源环保和房地产行业由法务部负责管理合规事务的企业也高达80%。（见图51及图55）

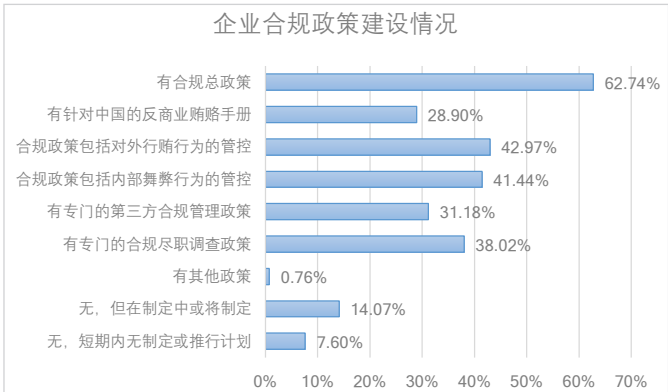


（图55：企业负责管理合规事宜的部门 – 行业）

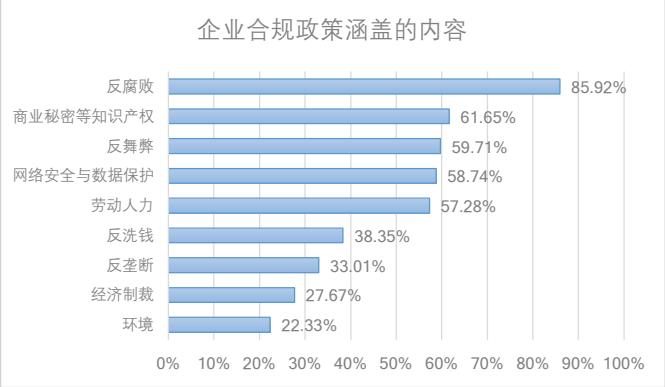
（三）企业的合规政策建设

78%的企业都制定了合规政策

2018-2019年，有78%的被调研企业都制定了合规政策，与此前年度的调研数据基本持平。（见图56）从企业政策涵盖的内容上来看，86%的企业较为关注反腐败，较此前年度进一步增长4个百分点。关注商业秘密等知识产权、反舞弊、网络安全与数据保护及劳动人力的，分别为62%、60%、59%以及57%。（见图57）经济制裁/出口管制、广告、环境是现在境内外执法的高发领域，企业应当对其引起重视并制定相关政策。



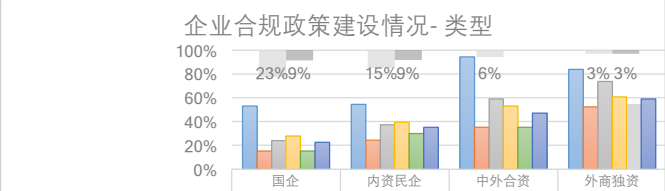
（图56：企业合规政策建设情况）



（图57：企业合规政策涵盖的内容）

外资企业合规政策建设较完备；国企缺少专门的合规尽职调查政策

外资企业有较为全面的合规政策。其中，外商独资企业有52%建设了针对中国的反商业贿赂手册、59%有专门的第三方合规管理政策、54%有专门的合规尽职调查政策，而政策具体管控的行为包含对外行贿行为和内部舞弊行为，分别占比74%和61%，相比于其他类型的受调研企业，建设的最完善。尽管53%的国企已具备合规总政策，但具备合规尽职调查政策、专门的第三方合规管理政策以及合规政策管控对外行贿行为的皆不足25%。（见图58）



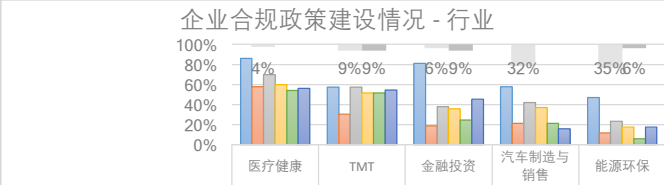
	国企	内资民企	中外合资	外商独资
有合规总政策	53%	54%	94%	84%
有针对于中国反商业贿赂手册	15%	24%	35%	52%
合规政策管控对外行贿行为	24%	37%	59%	74%
合规政策管控内部舞弊行为	28%	39%	53%	61%
有专门的合规尽职调查政策	15%	30%	35%	54%
有专门的第三方合规管理政策	23%	35%	47%	59%
无，制定或推行中	23%	15%	6%	3%

（图58：企业合规政策建设情况 – 类型）

医疗健康行业企业合规政策建设较完备；能源环保行业企业合规政策建设薄弱

就行业而言，医疗健康行业企业合规政策建设较完备，有50%以上的医疗健康行业企业均有合规总政策、第三方合规政策以及合规尽职调查政策。另外，相比于其他行业的企业，医疗健康行业企业格外重视针对中国的反商业贿赂手册以及对对外行贿行为的管控，分别占比58%以及70%。

能源环保行业企业合规政策建设薄弱。在建立合规总政策、专门的合规尽职调查政策、针对中国的反商业贿赂手册、以及对于合规政策针对对外行贿行为以及内部舞弊行为方面的管控在行业中均处于垫底地位，分别占比为47%、6%、12%、24%以及18%。环保局于2018-2019年加强执法，执法比例由此前年度的10%翻一番至22%，（见图25）同时接受调研的能源环保行业企业，被突击检查比例最高，占比60%，（见图28）企业应当对合规政策建设提高重视。（见图59）



	医疗健康	TMT	金融投资	汽车制造与销售	能源环保
有合规总政策	86%	58%	81%	58%	47%
有针对于中国反商业贿赂手册	58%	30%	19%	21%	12%
合规政策管控对外行贿行为	70%	58%	38%	42%	24%
合规政策管控内部舞弊行为	60%	52%	36%	37%	18%
有专门的合规尽职调查政策	54%	52%	25%	21%	6%
有专门的第三方合规管理政策	56%	55%	45%	16%	18%
无，制定或推行中	4%	9%	6%	32%	35%
无，暂无制定或推行计划	0%	9%	9%	0%	6%

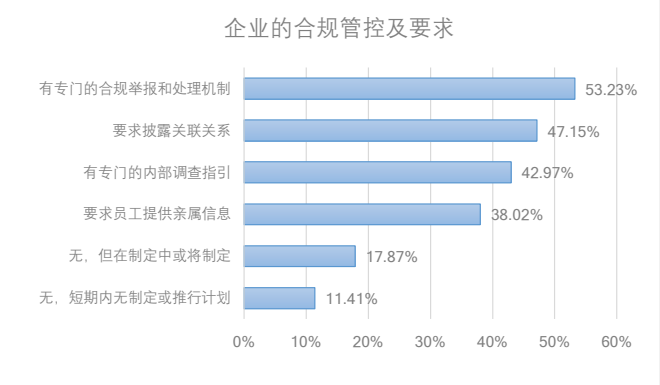
（图59：企业合规政策建设情况 – 行业）

（四）企业的合规管控及要求

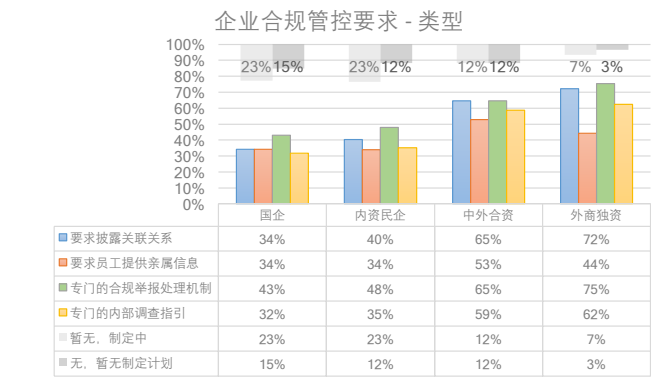
近三成企业暂无合规管控措施；国企、民企的合规管控程度及要求较低；能源环保和房地产行业需要加强采取合规管控措施

接受调研的企业中，过半数企业采取被动型合规管控，有专门的合规举报和处理机制的企业占比53%。采取主动合规管控方式的企业，如要求披露关联关系、有专门的内部调查指引和要求员工提供亲属信息的企业分别占比47%、43%和38%，近三成企业暂无合规管控措施。（见图60）

企业类型的角度来看，外商独资和中外合资企业的整体管控要求相较国企、民企更为严格，暂无合规管控措施的外商独资企业仅占比10%，而暂无合规管控措施的国企则占比38%。（见图61）从行业角度，金融投资和医疗健康行业的整体管控要求相较其他行业更为严格，暂无合规管控措施的企业占比均在20%以下。能源环保和房地产行业需要加强采取合规管控措施，目前均处于行业较低水平。（见图62）从规模来看，企业规模大小与合规管控要求的严格程度呈正相关性。（见图63）

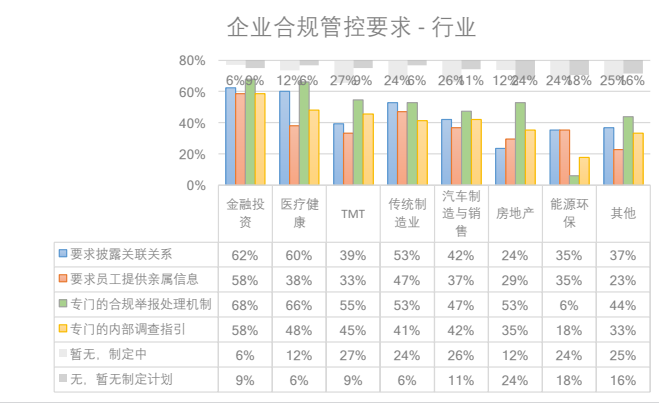


（图60：企业的合规管控及要求）



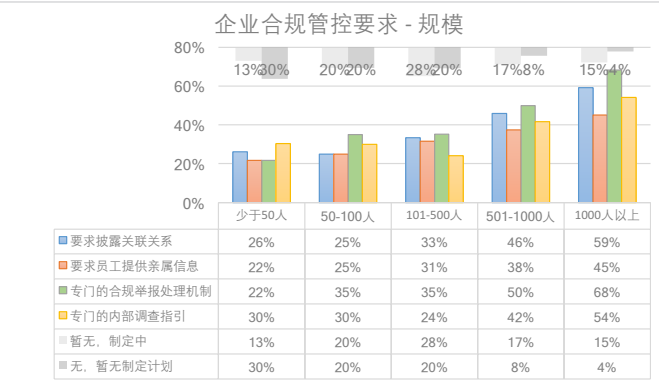
	国企	内资民企	中外合资	外商独资
要求披露关联关系	34%	40%	65%	72%
要求员工提供亲属信息	34%	34%	53%	44%
专门的合规举报处理机制	43%	48%	65%	75%
专门的内部调查指引	32%	35%	59%	62%
暂无，制定中	23%	23%	12%	7%
无，暂无制定计划	15%	12%	12%	3%

（图61：企业的合规管控及要求－类型）



	金融投资	医疗健康	TMT	传统制造业	汽车制造与销售	房地产	能源环保	其他
要求披露关联关系	62%	60%	39%	53%	42%	24%	35%	37%
要求员工提供亲属信息	58%	38%	33%	47%	37%	29%	35%	23%
专门的合规举报处理机制	68%	66%	55%	53%	47%	53%	6%	44%
专门的内部调查指引	58%	48%	45%	41%	42%	35%	18%	33%
暂无，制定中	6%	12%	27%	24%	26%	12%	24%	25%
无，暂无制定计划	9%	6%	9%	6%	11%	24%	18%	16%

（图62：企业的合规管控及要求－行业）



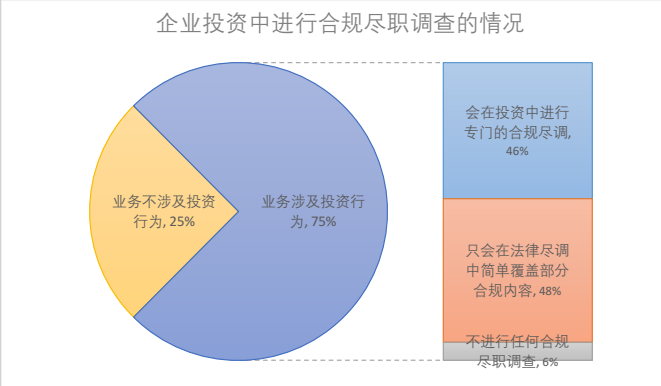
	少于50人	50-100人	101-500人	501-1000人	1000人以上
要求披露关联关系	26%	25%	33%	46%	59%
要求员工提供亲属信息	22%	25%	31%	38%	45%
专门的合规举报处理机制	22%	35%	35%	50%	68%
专门的内部调查指引	30%	30%	24%	42%	54%
暂无，制定中	13%	20%	28%	17%	15%
无，暂无制定计划	30%	20%	20%	8%	4%

（图63：企业的合规管控及要求－规模）

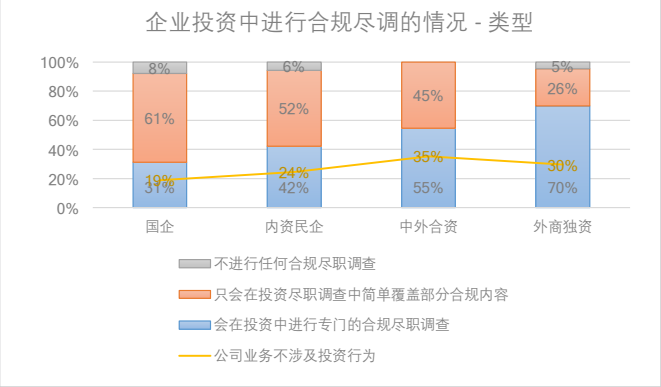
（五）企业进行投资合规尽职调查以及企业内部调查

在对外投资中进行合规尽调比例再度升高；金融投资行业因合规问题停止投资比例高

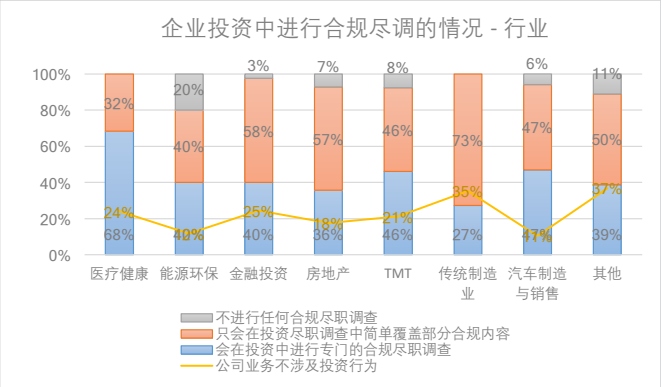
调研显示，75%的企业在业务中都涉及投资行为（见图64）。且2018-2019年合规仍然为企业做出投资决定的重要考量因素之一。投资中，仅有约6%的企业不进行任何合规尽职调查，相比去年11.5%下降了近一半。医疗健康行业在投资中，不存在不进行合规尽职调查的企业，且在投资中进行专门的合规尽职调查的企业占比为68%（见图66）。在涉及投资业务的各类企业中，70%的外商独资企业会进行专门的合规尽职调查，国企多采取在投资尽调中简单涵盖部分合规内容的方式开展合规尽调，占比约60%。（见图65）就尽调结果对企业投资决策的影响而言，近四成的国企和内资民企曾因合规问题停止投资，近六成的金融投资行业企业曾因合规问题停止投资。（见图67、图68）



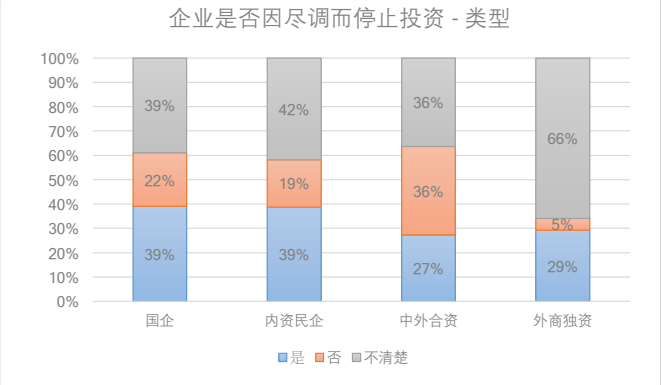
（图64：企业投资中进行合规尽职调查的情况）



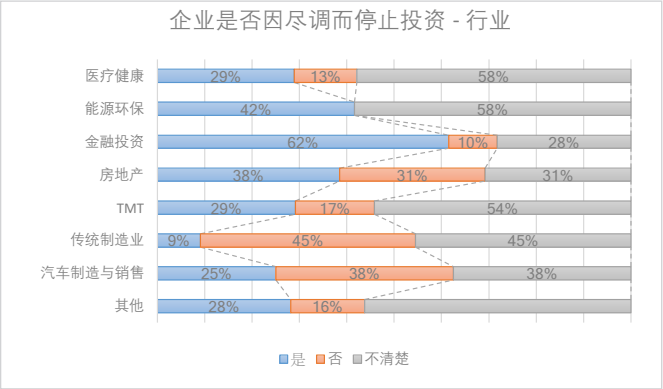
（图65：企业投资中进行合规尽职调查的情况 – 类型）



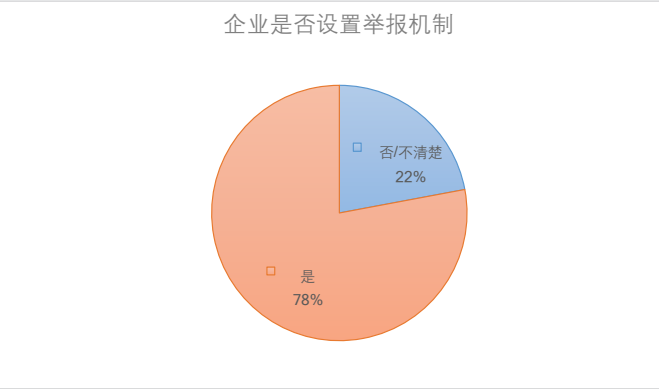
（图66：企业投资中进行合规尽职调查的情况 – 行业）



（图67：企业因尽职调查停止投资情况 – 类型）



（图68：企业因尽职调查停止投资情况 – 行业）

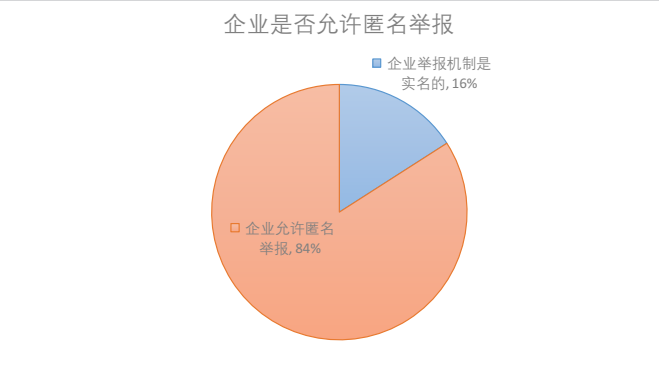


（图69：企业是否设置举报机制）

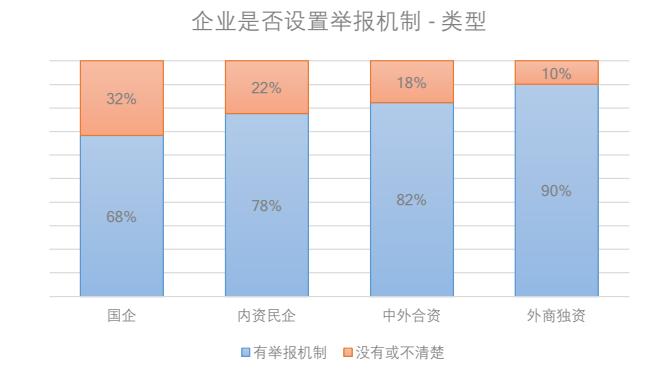
近八成企业设置举报机制，并有近六成企业允许匿名举报；仅约四成国企在发现合规风险后会采取合规措施

企业在开展内部调查时，近八成被调研企业设置举报机制。（见图69）而在设置举报机制的企业中，有84%的企业允许匿名举报。（见图70）从类型角度，仅10%的外商独资企业未设立举报机制，且在设立举报机制的外商独资企业中，有98%都支持匿名举报，远超其他类型企业。（见图71、图72）实践中，支持匿名举报有利于员工或外部第三方及时将公司存在的合规风险披露给公司，外商独资企业在该环节仍然领先于其他类型企业。

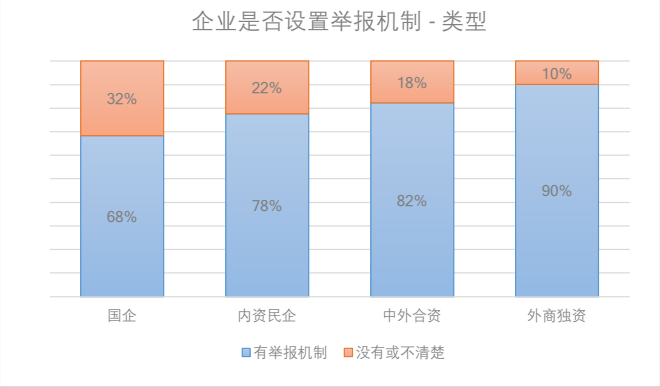
在发现合规风险后，过半数的企业会采取合规措施，超四成企业曾经开除过员工，约两成企业进行过立案，但向执法机关自我检举的企业比例仅约2%。（见图73）其中约七成外商独资企业在发现合规风险后会采取合规措施，相较而言国企则仅约四成。（见图74）



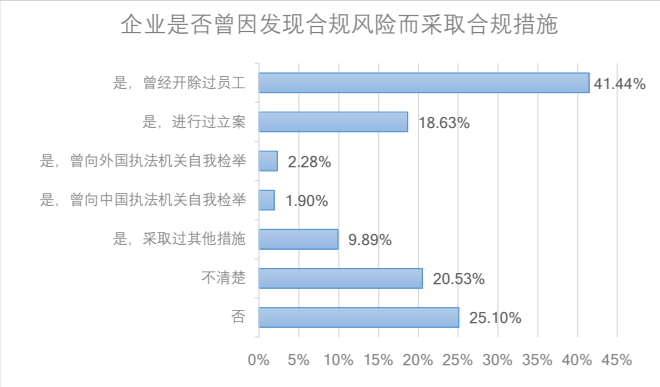
（图70：企业是否允许匿名举报）



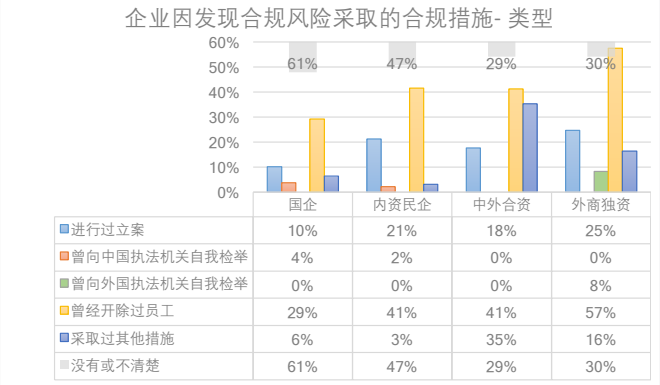
（图71：企业是否设置举报机制 – 类型）



（图72：企业是否允许匿名举报 – 类型）



（图73：企业是否曾因发现合规风险而采取合规措施）



	国企	内资民企	中外合资	外商独资
进行过立案	10%	21%	18%	25%
曾向中国执法机关自我检举	4%	2%	0%	0%
曾向外国执法机关自我检举	0%	0%	0%	8%
曾经开除过员工	29%	41%	41%	57%
采取过其他措施	6%	3%	35%	16%
没有或不清楚	61%	47%	29%	30%

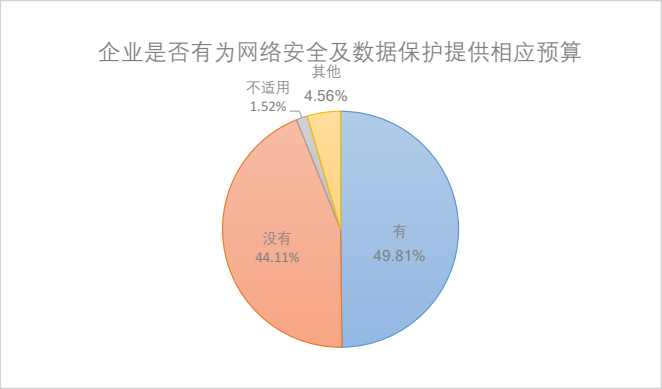
（图74：企业因发现合规风险采取的合规措施 – 类型）

（六）企业网络安全及个人信息保护制度

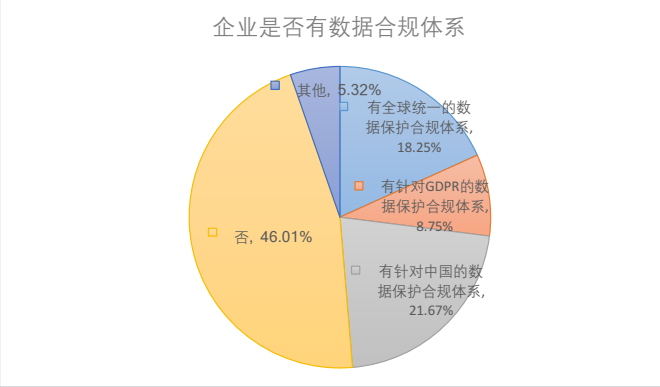
近七成国企没有数据保护合规体系；房地产行业建立数据合规体系的企业不足两成；超七成企业进行过数据合规体系审计

如前所述，78%有合规政策的企业中，59%所建立的合规政策包含了网络安全与数据保护内容。（见图56、图57）约五成企业有为网络安全以及数据保护事宜专门提供相应的预算用于开展公司内部的数据治理、合规以及数据保护工作。（见图75）

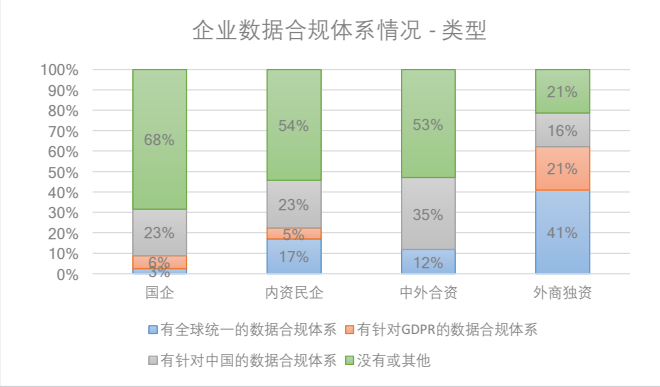
约五成企业有数据保护合规体系，其中超八成被调研外商独资企业有一套数据保护合规体系，但近七成国企没有该合规体系。（见图76、图77）从行业角度，TMT行业近八成企业建立数据合规体系，而房地产企业中建立该体系的不足两成。该现象与执法情况有所关联，中国企业受到网络安全或数据的执法中，TMT行业企业以33%排名第一，而房地产行业为零。（见图78、图20）从规模角度，是否建立数据合规体系与企业规模呈较强的正相关性。（见图79）



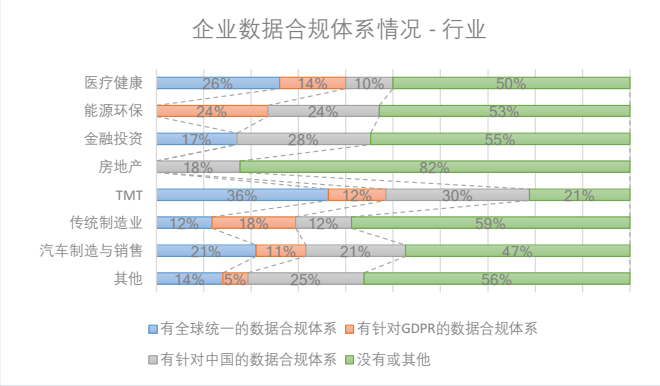
（图75：企业是否有为网络安全以及数据保护提供相应预算）



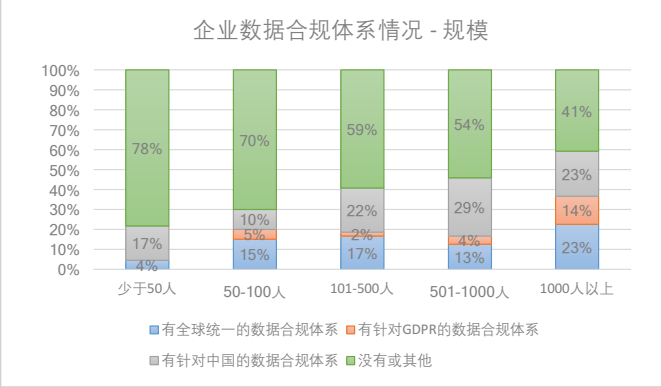
（图76：企业是否有数据合规体系）



（图77：企业数据合规体系情况 – 类型）



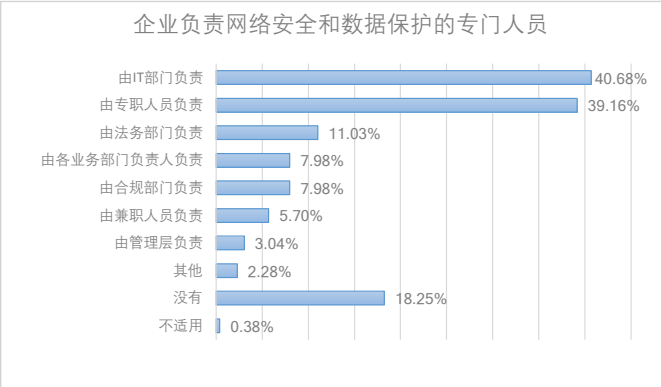
（图78：企业数据合规体系情况 – 行业）



（图79：企业数据合规体系情况 – 规模）

41%的企业由IT部门负责网络安全和数据保护工作

根据调研，在超过八成有负责网络安全和数据保护的专门人员的企业中，41%的企业由IT部门负责，39%的企业由专职人员负责，少数企业由法务部门、各业务部门负责人和合规部门负责。（见图80）

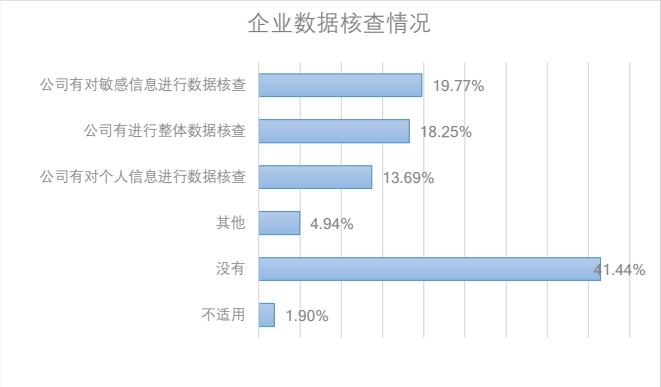


（图80：企业负责网络安全和数据保护的专门人员）

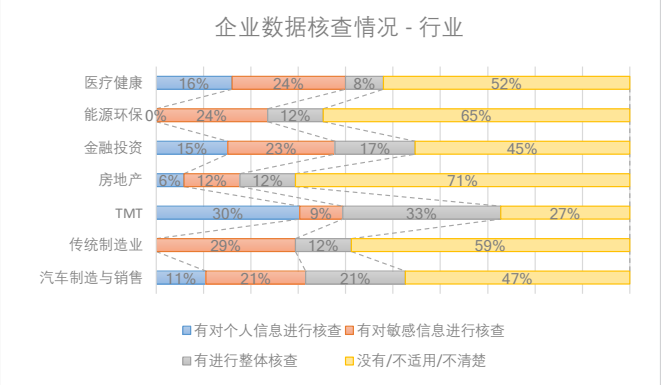
超四成企业没有进行过数据核查；房地产行业不足三成

超四成企业没有进行过数据核查，总体约近三成企业对个人信息或敏感信息进行过数据核查。（见图81）从行业的角度，近八成TMT行业企业进行过数据核查，

房地产行业企业则不足三成，该现象可能与执法情况相关，中国企业受到网络安全或数据的执法中，TMT行业企业以33%排名第一，而房地产行业为零。（见图82、图20）



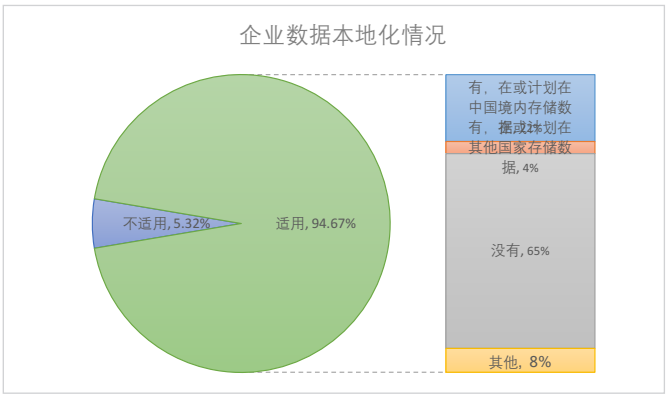
（图81：企业数据核查情况）



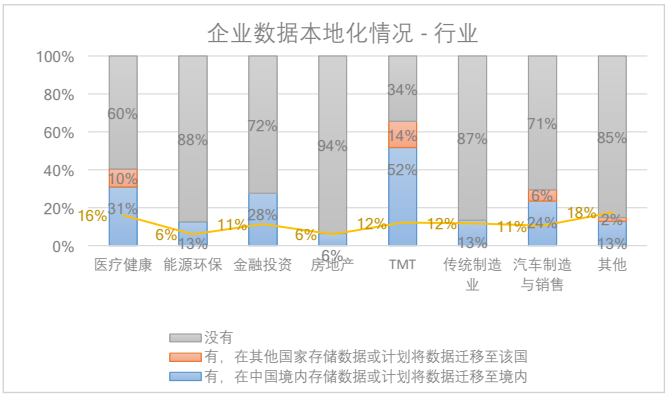
（图82：企业数据核查情况 – 行业）

超六成企业没有进行过数据本地化；六成TMT行业进行过数据本地化，远高于其他行业

调研发现，在适用数据本地化的企业当中，超六成企业没有进行过数据本地化。（见图83）从行业角度来看，TMT行业中66%的企业进行过数据本地化，远高于其他行业，房地产行业仅6%，可能与网安和数据保护执法现状有关。（见图84）



（图83：企业数据本地化情况）



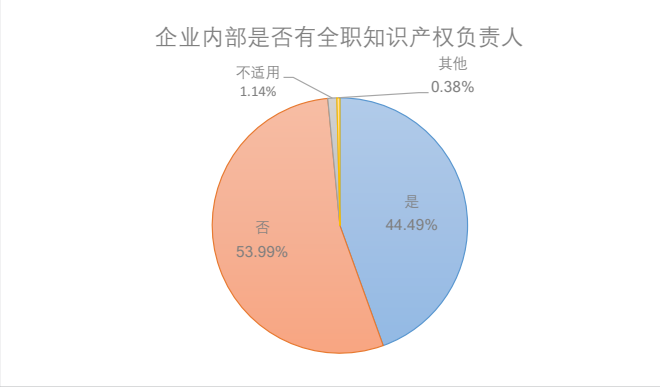
（图84：企业数据本地化情况 – 行业）

四、企业知识产权制度

（一）企业内部的全职知识产权负责人

略低于半数的企业配备了全职知识产权负责人

参加调研的企业中有45%配备了全职知识产权负责人，未配备全职知识产权负责人的企业为54%，仍然超过半数。（见图85）

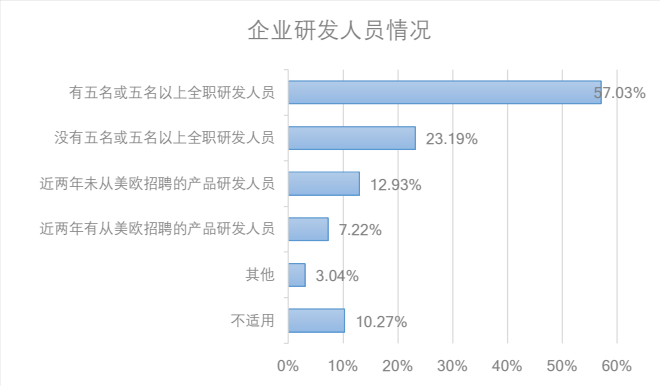


（图85：企业内部是否有全职知识产权负责人）

（二）企业配备的全职研发人员

超过半数的企业配备了五名或五名以上全职研发人员

被调研的企业中，57%的企业配备了五名或五名以上全职研发人员，并且7%的企业在近两年从美欧招聘了产品研发人员。（见图86）

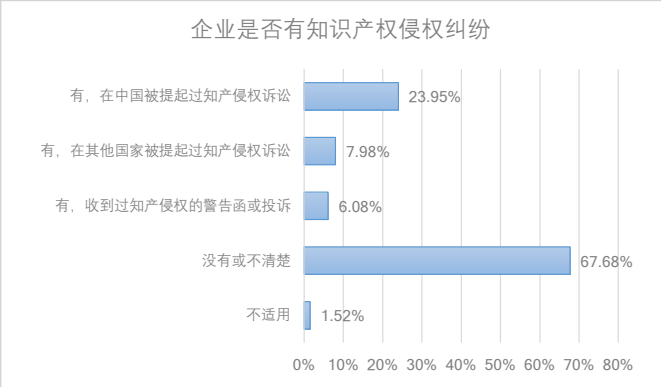


（图86：企业研发人员情况）

（三）企业的知识产权纠纷

68%的企业没有或者不清楚是否有知识产权纠纷

被调研企业中，有68%的企业没有或者不清楚自身是否有知识产权纠纷，有24%的企业在中国被提起过知识产权侵权诉讼，8%的企业在其他国家被提起过知识产权侵权诉讼，6%的企业收到过知识产权侵权的警告函或投诉。（见图87）

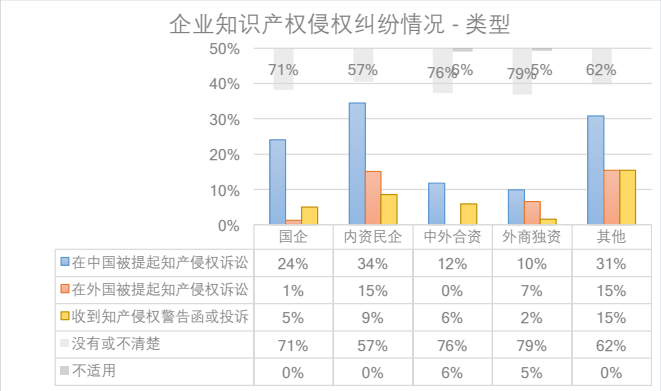


（图87：企业是否有知识产权侵权纠纷）

内资民企涉及国内外知识产权纠纷的比例显著高于国企与外企。就行业而言，能源环保行业涉及知识产权侵权纠纷的比例最低

内资企业较多地涉及知识产权纠纷，有34% 在中国被提起知识产权侵权诉讼，15%在外国被提起知识产权侵权诉讼，有9%收到过知识产权侵权警告函或投诉。国有企业主要涉及在中国被提起知识产权侵权诉讼，占比为24%，在外国被提起知识产权侵权诉讼的只有1%，收到知识产权侵权警告函和投诉的国企也只有5%。

外商独资企业中涉及知识产权纠纷的最少，有10%在中国被提起知识产权侵权诉讼，参与调研的外商独资企业中7%的企业在外国被提起知识产权侵权诉讼，有2%收到过知识产权侵权警告函或投诉。（见图88）

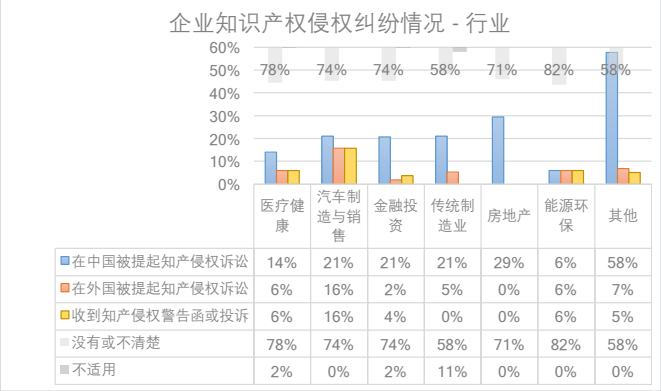


	国企	内资民企	中外合资	外商独资	其他
在中国被提起知产侵权诉讼	24%	34%	12%	10%	31%
在外国被提起知产侵权诉讼	1%	15%	0%	7%	15%
收到知产侵权警告函或投诉	5%	9%	6%	2%	15%
没有或不清楚	71%	57%	76%	79%	62%
不适用	0%	0%	6%	5%	0%

（图88：企业知识产权侵权纠纷情况 – 类型）

就行业而言，能源环保行业涉及知识产权侵权纠纷的比例最低，在中国被提起知识产权侵权诉讼、在外国被提起知识产权侵权诉讼，以及收到过知识产权侵权警告函或投诉，三者各占比6%。

参与调研的房地产企业有29%涉及在中国被提起知识产权侵权诉讼，没有涉及其他类型的知识产权侵权纠纷。相较其他行业，汽车制造商涉及在外国被提起知识产权侵权诉讼的比例较高，为16%，另外有21%涉及在中国被提起知识产权侵权诉讼，有16%收到知识产权侵权警告函或投诉。（见图89）



	医疗健康	汽车制造与销售	金融投资	传统制造业	房地产	能源环保	其他
在中国被提起知产侵权诉讼	14%	21%	21%	21%	29%	6%	58%
在外国被提起知产侵权诉讼	6%	16%	2%	5%	0%	6%	7%
收到知产侵权警告函或投诉	6%	16%	4%	0%	0%	6%	5%
没有或不清楚	78%	74%	74%	58%	71%	82%	58%
不适用	2%	0%	2%	11%	0%	0%	0%

（图89：企业知识产权侵权纠纷情况 – 行业）

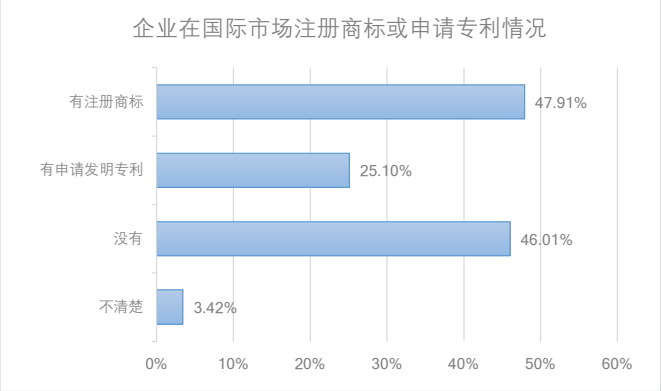
（四）企业在其他法域的知识产权

具有知识产权的内资民企比例明显高于国企；科技制造行业普遍具有域外知识产权

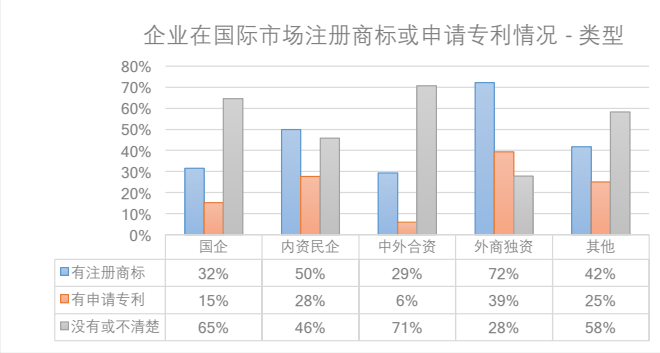
略高于半数的企业在域外具有知识产权，包括48%的企业在域外有注册商标，25%的企业有申请发明专利。（见图90）

就企业类型而言，外商独资企业在域外具有注册商标的占72%，有申请专利的占39%。内资民企在上述两项占比分别是50%与28%，而国企为32%与15%。（见图91）

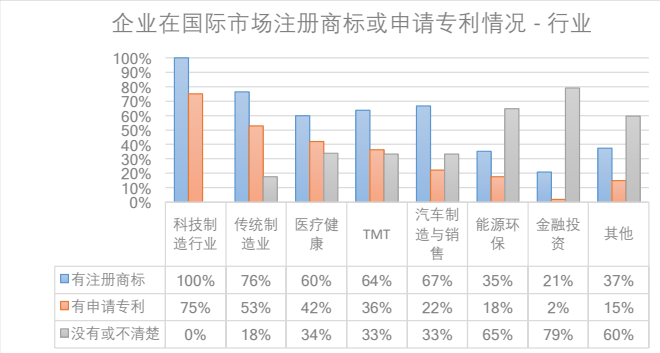
就行业而言，科技制造行业中具有域外注册商标的为100%，具有域外申请专利的为75%，在参与调研企业各行业中所占比例最高。金融投资行业具有域外知识产权的比例最低，上述两项占比分别是21%与2%。（见图92）



（图90：企业在国际市场注册商标或申请专利情况）



（图91：企业在国际市场注册商标或申请专利情况－ 类型）

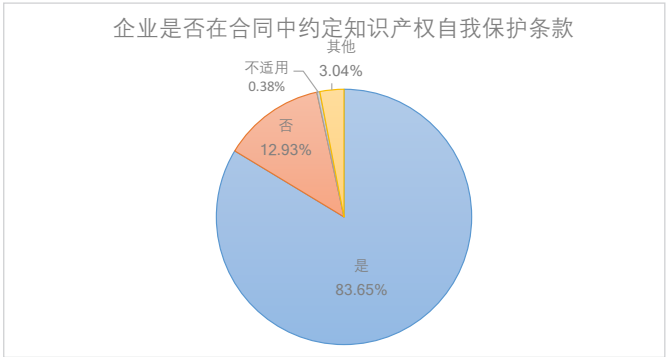


（图92：企业在国际市场注册商标或申请专利情况－ 行业）

（五）企业在合同中约定的自我保护条款

绝大多数企业在与供货商签订的合同中约定了由供应商承诺不侵犯他人知识产权等自我保护条款

84%的企业在与供货商签订的合同中有由供应商承诺不侵犯他人知识产权等自我保护条款，但也有13%的企业与供货商的合同中没有自我保护条款。（见图93）

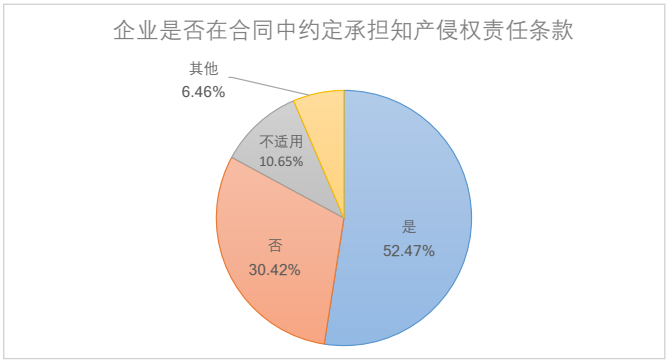


（图93：企业是否在合同中约定知识产权自我保护条款）

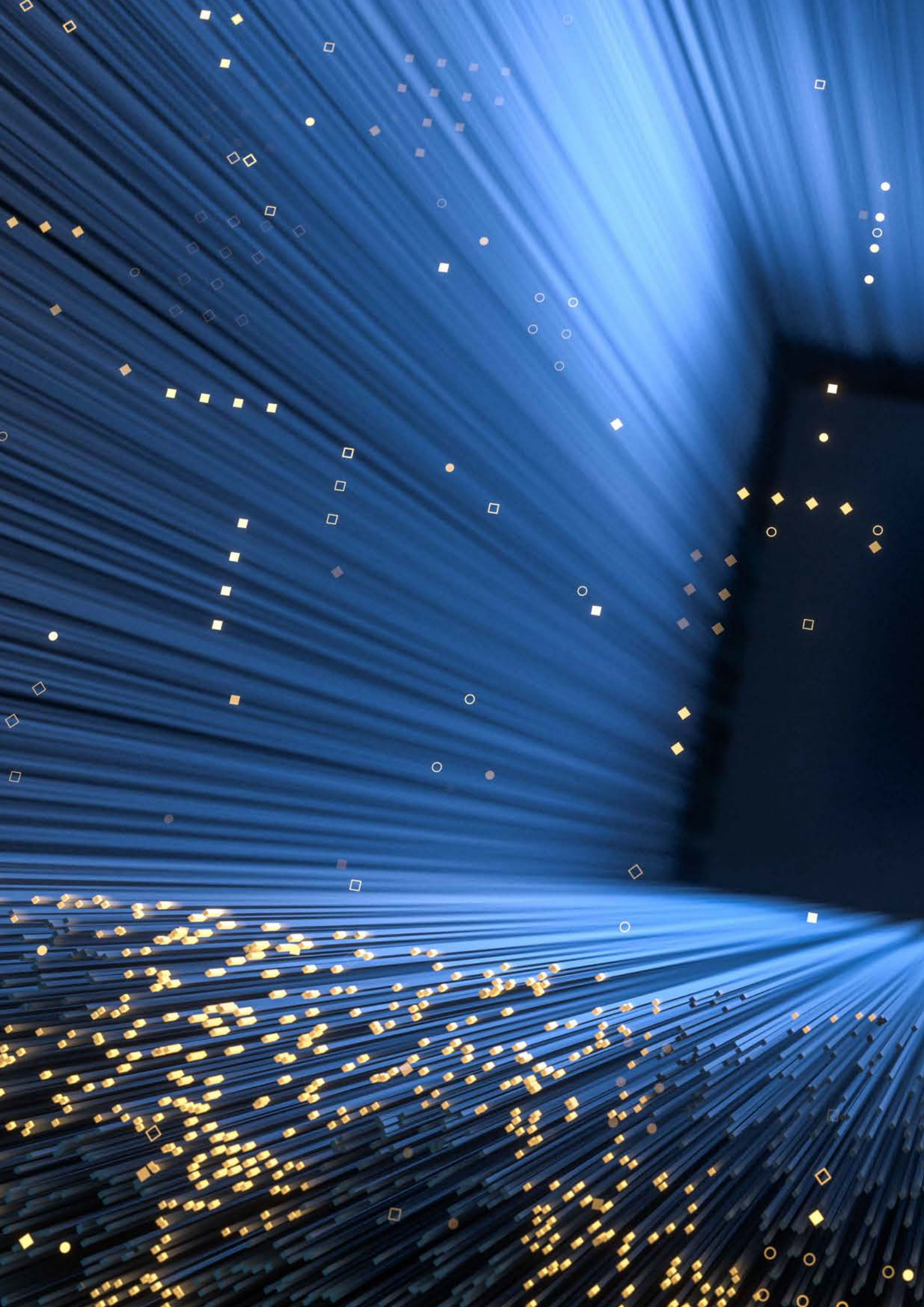
（六）企业在国际市场中签订的合同中的承担知识产权侵权责任条款

略高于半数的企业在与国际市场相关的合同中约定了由企业承担对第三人知识产权侵权责任的条款

53%的企业在与国际市场的经销商或零售商订立供货合同时，其合同包括了由企业承担侵犯第三人知识产权的法律后果的条款。（见图94）



（图94：企业是否在国际市场的供货合同中约定承担知识产权侵权责任条款）



第三章

企业应加强数据保护合规

一、全球数据保护立法和执法的趋势、差异及中国企业的对策

自2016年欧盟《通用数据保护条例》（General Data Protection Regulation, “GDPR”）颁布以来，越来越多的国家开始关注数据保护领域的立法和执法。据统计，现今已有超过132个国家制定了个人信息保护法[1]，各个国家针对知名企业的数据执法案件也屡见不鲜。

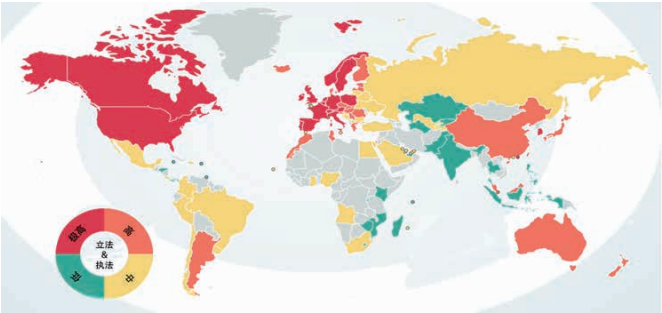
近年来我国的立法、行政及司法机关也在数据保护领域进行了许多的努力以及尝试。我国的数据保护的法律体系也是从2016年《中华人民共和国网络安全法》（“《网安法》”）、《刑法修正案（九）》以及《民法总则》的颁布以来才开始逐步完善的。除了这些上位法，中央网信办、公安部以及工信部等相关部委也均积极进行部门规章和行政法规的制定，并且通过推动各项国家标准的制定和发布来逐步完善，同时也开始在全国范围内对App的非法收集个人信息的情况进行专项整治。

中国企业在“走出去”的过程中，遵守当地的数据保护法律是不可避免的。然而由于在海外市场开拓的初期，考虑到成本的投入以及抢占市场先机的时间等因素，中国企业一般会希望继续沿用国内的系统来支持海外的业务或者沿用中国的业务流程，这意味着当地的数据会被回传到中国进行处理或者按照中国法律建立起来的流程来处理国外的数据主体的数据。这就会涉及到根据中国的法律以及监管机构的要求建立起来的各项流程是否能够满足当地数据保护法律的要求的问题。

在目前数据处理行为日益复杂的今天，是否可以用一套体系满足所有国家的法律要求是每个企业日思夜想的事情，但是这种做法是否实际可行呢？

（一）全球数据立法与执法热潮

由于GDPR是对欧盟的95指令在20多年来数据保护的实践的总结和立法的提升，其经常被许多国家作为立法的蓝本进行对照。横跨大洲与大洋，包括日本、韩国、印度、巴西、新西兰、哥伦比亚、泰国等众多国家与地区，在GDPR出台后均对标GDPR对本国的立法进行完善和制定。Greenleaf教授还把GDPR称为是全球数据保护标准的3.0版本。除在数据保护领域成熟度较高的欧盟及美国之外，其他国家和地区的数据领域执法同样值得关注。例如亚太地区的新加坡、韩国、日本、香港、印度、泰国均积极对标GDPR，日本也已经获得了欧盟委员会的充分性认定，韩国也正在争取充分性认定的过程中。下图展示了全球数据保护立法和执法的程度的分布以及主要国家和地区对标GDPR的情况。



1. Graham Greenleaf, “Global Data Privacy Laws 2019: 132 National Laws & Many Bills”, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3381593, 最后访问时间2019年11月18日。

虽然许多企业从商业成本增加以及阻碍经济技术发展的角度对GDPR规定的标准提出了批评的声音，但是不可否认的是GDPR确实将隐私保护的标准提到了更高的水位。随着民众对于互联网产品的深入理解以及对隐私保护的需求日益增加，许多国家的监管机构也不断以更高的要求审视隐私保护，这两种冲突的理念在许多国家的执法中不断体现，而监管机构最后一般会倾向于保护消费者权益来严格要求企业遵守数据保护法。在欧盟，企业不仅需符合主管部门的监管要求，欧盟的众多社会机构、非政府组织、普通消费者往往具有较强的隐私保护意识，企业还需要受到他们的监督。这导致许多企业在数据领域的违法违规行为很容易被发现传播并且引来监管机关调查和依法处罚。

与传统的合规问题往往具有较强的地缘性不同，企业的数据合规与企业的技术、产品和服务息息相关，在一个国家的不合规往往也可能意味着其他国家的不合规，因此，对于跨国企业来说还需要警惕不同国家监管机构联动执法的风险。如Facebook因Cambridge Analytica事件在欧洲、美国、以至于印度和南美洲等国家和地区均遭受了不同程度的调查和执法。FTC于2019年2月针对美国版抖音TikTok（Musical.Ly）的违规行为处以了5700万美元的罚款，违规的事由为“未能尽合理努力确保儿童家长收到其收集、使用和披露儿童个人信息的通知；未获得家长同意；未能在其用户界面披露收集、使用和披露儿童个人信息的隐私政策；信息保存时间超过合理期限”等违反COPPA（Children's Online Privacy Protection Rule）的行为。其后不久，英国数据保护监管机关ICO（Information Commissioner's Office）也因相似事由启动了对抖音的调查。

此外，数据问题可能衍生出其他的执法风险也值得关注。美国投资委员会（CFIUS）于近期启动了对抖音国际版母公司字节跳动两年前收购Musical.ly的国家安全审查，主要原因是之前的收购没有寻求CFIUS审查，但现在CFIUS认为Tik Tok的用户量和个人数据量巨大，可能涉及美国国家安全的问题。此前，德国联邦反垄断局也曾因Google与旗下关联公司之间的数据交互和数据融合认为Google存在滥用市场支配地位的行为。

除了自身的数据合规外，在投资项目中被投公司的数据合规问题也可能给企业带来执法的风险。例如在2019年7月英国ICO因数据泄露拟对一家国际酒店集团处以高额处罚（逾9920万英镑），英国ICO认为数据泄露的隐患在2016年该国际酒店集团收购另一家酒店集团时已经存在，但是该国际酒店集团在收购过程中未能进行充分的数据合规尽职调查以及时发现该风险，避免更为严重后果的发生，因此也需要承担责任。因此，中国企业在走出去的过程中，需要注意加强对被投资公司数据方面的合规尽调，避免因被投公司在投前的行为承担不必要的风险。

除了美国和欧盟的积极执法以外，亚太许多国家自2016年以来也开始积极地执行当地的个人信息保护法，例如新加坡在2013年《个人信息保护法》生效以来至2016年期间执法案例非常少，直到2016年开始才开始非常频繁地执法。例如，新加坡数据保护监管机构（Personal Data Protection Commission, PDPC）于2019年1月因存储病人数据的系统泄露对SingHealth及其服务提供商IHiS分别处于25万和75万新加坡元的罚款，同一事件共计处罚100万新加坡元，为有史以来最高的罚金。同样，虽然韩国的个人信息保护法已于2011年就出台，但是执法案例一般仅局限在数据泄露后的被动执法，韩国的监管机构也是在近两年需要考虑争取欧盟的充分性认定也才开始频繁地进行主动式执法。而且，为了回应本国企业提出的因韩国个人信息保护相关法规缺乏明确的域外适用效力而导致的对本国企业的反向歧视，韩国于2019年修订了《促进信息和通信网络利用和数据保护法》（Promotion of Information and

Communications Network Utilization and Data Protection, “Network Act”），确立了Network Act的域外适用效力，并要求满足一定条件的境外企业在当地指定一名代表。而且Network Act的主要执法机构Korean Communication Commission（“KCC”）也开始主动接触一些跨国企业（例如Google、Facebook等）督促其履行上述指定本地代表的义务。

我国除网信办及公安部等四部委自2019年起在全国范围内全面开展对App的专项治理活动，约谈、督促整改或下架了大批App外，刑事领域的执法最为活跃。例如新三板上市的大数据公司数据堂因为数据保护的问题而被进行调查，其6名高管受到了刑事追责并被判处有期徒刑等刑罚。近期也有很多大数据企业因为使用爬虫获取数据的违规问题受到公安部门的刑事调查。

（二）不同国家/地区数据保护立法与执法的差异

虽然各国家和地区的态度都是积极的，但不可否认的是，由于实际情况和文化环境的诸多差异，各国数据保护在立法与执法方式仍存在着明显不同。

■ 数据保护法律规定的内容不同

以我国数据保护法律与GDPR的比较为例，在重要的“获得收集个人数据的同意”环节中，我国法律和GDPR就有着不同的规定：

中国法	GDPR
《网络安全法》、《电信和互联网用户个人信息保护规定》、《消费者权益保护法》均未对如何取得被收集者的“同意”做过多的解释和规定，更多是针对披露的内容做出要求，即“明示收集、使用个人信息的目的、方式和范围”。《儿童个人信息网络保护规定》虽然在征求意见稿阶段加入了如何获取同意的要求，即“明示同意应当具体、清楚、明确，基于自愿”，但最终的版本也删除了该条。	GDPR 对于数据主体的同意（Consent）的要求： ➢ 自愿给与（freely given） ➢ 特定目的（specific） ➢ 知情（informed） ➢ 清楚地表述了数据主体的意愿（unambiguous indication of the data subject’s wishes） ➢ 以声明或者清楚的确认行为表示同意（by a statement or by a clear affirmative action）
《个人信息安全规范》（2019 年 6 月征求意见稿）里对收集个人信息和个人敏感信息时获取授权同意有着明确的规定： ➢ 个人信息：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。其中对于同意也没有明确的规定。 ➢ 个人敏感信息：应征得个人信息主体的明示同意，并应确保个人信息主体的明示同意是其在完全知情的基础上自主给出的、具体的、清晰明确的意愿表示。	

除了在获取同意的环节有着不同规定，在数据处理的合法性基础、数据主体的权利等问题上，GDPR与很多国家的法律和中国法均存在着较大的差异。基于国家制度、发展状况、文化环境等多因素的不同，各国家和地区的数据保护立法虽然在原则和部分规定上能够保持基本一致，但在许多环节中仍有着不同的具体规定。例如各地法律在授予法定数据主体权利的考虑存在不同，主要是在公共政策上考虑是否是支持企业的发展还是保护个人的权利优先。

另外一个比较著名的例子就是Google DeepMind与伦敦医院NHS合作的过程中，NHS被英国的数据保护监管机构ICO认定为NHS未遵守数据保护法案，向Google DeepMind部门提供了约160万患者的详细资料进而予以处罚的案例。虽然ICO在其信中表示其支持合理使用个人信息用于临床研究以及发展，但是在这个案件中个人信息保护明显是更为有限的考虑。Google DeepMind在全球很多国家（例如美国）都开展过类似的合作，但未见到公开报道上有对Google DeepMind的类似合作进行处罚的案例。很多国家在平衡个人信息

以及促进科学进步时，一般都会在个人信息保护权上予以限定。在素有高度重视人权及个人数据保护传统的欧洲，往往对企业提出更高的要求。在个人利益和企业利益发生冲突的情景中，主管机关也往往会采取更偏向个人权利应受到更强保护的角度；而在对互联网企业更为“包容”的美国，则会在同样的场景中对类似DeepMind的企业采取更宽容的态度。

（三）应对之策

对于出海的中国企业来说，以一套体系进行合规来应对不同国家的监管虽不能说一个完美的解决方法，但是可以让这些企业尽快从零到有搭建出了个合规体系来应对一些监管的要求。在进行合规工作安排时，这些出海的中国企业可以优先考量如下方面：

1. 找到数据保护规则的“最大公约数”

虽然各国各地区的数据保护立法和执法不尽相同，但在个人信息保护的基本原则上以及一些保护要求上都能够找到相似之处。这些相似之处也并非巧合，因为美国和欧洲最早的数据保护立法也是来源于公平信息处理原则（Fair Information Practices, FIP），随后许多国际条约也是在这个基础上制定的，例如OECD的关于隐私保护以及个人信息跨境的指引。这些类似之处主要集中在个人信息的收集以及分享环节以及个人信息保护的基本原则，例如数据最小化、数据处理的透明度要求、给予数据主体一定的控制权。

除了了解这些规则之间的相似之处来整体决策合规策略，企业还可以通过数据核查的方式来确保数据处理行为的分析是统一的，即同样的数据处理行为在GDPR项下的分析应当与其他的国家的分析类似。这种微观的分析之后能够让企业对其数据处理行为有一定的了解，也可以进而考虑是否可以在不违反当地法律要求的前提下用同一套业务流程以及公司政策进行管理。

虽然寻找最大公约数的做法可以减少合规安排上的重复劳动，但是这种最大公约数的方法不见得满足具体的某一些国家的合规要求，特别是这些有着更为严苛要求的国家。一个典型的例子就是采用ISO/IEC27701的国际标准建立的体系，虽然能够满足一些基本面上的要求，这个国际标准的许多条文也多次强调企业在使用该标准时还需要结合并遵从各国国内立进行的解释和实践。在某个国家的法律更为严格的情况下，不考虑当地法律则非常有可能会违规。因此，寻找最大公约数的做法更多是帮助企业进行第一步的规则的分析，企业不应满足于在这些基本面进行的合规安排。

2. 重点关注立法严格或执法活跃区域

在寻找了最大公约数将数据合规的前期工作确定了之后，企业如何选取哪些合规项目来优先进行？从数据的生命周期来看，常见的容易引发的监管机构执法和被数据主体发现进而投诉或起诉的环节主要是在数据收集和数据分享环节。对于数据的内部留存、保护以及删除环节，这些对于数据主体而言一般可见度比较低，这些内部的管理措施或者技术措施的不足一般只有在出现数据泄露并引发监管机构调查的时候才能被发现。然而对于内部的管理措施，大多数国家一般都是留有一定余地让企业采取最先进的技术以及更有效的管理措施来进行管理。对于个人信息的收集和分享环节，企业必须紧跟当地的监管机构的解释以及执法判例，才能尽早地调整自己在当地的数据收集行为以及业务流程。对于数据分享环节，由于涉及将数据传输给第三方以及第三方是否有能力保护这些数据等问题，对这些第三方进行尽职调查和管理也是非常必要的。

3. 依据相关规定对企业的商业安排做出调整

除了考虑整体合规以外，企业也需要“防患于未然”，应注意对集团企业内的数据处理行为进行区分，并对相应的数据治理体系进行调整，以减少整一个集团的营收被当地的监管机构作为罚金的基数的情形。以GDPR为例，GDPR第83条第4和第5款规定，依据个人或企业违反GDPR规定的不同情形，执法机构分别可“对个人处以1千万欧元罚金，对企业处以1千万欧元或者2%的上一财年全球收入（以较高者为准）罚金”和“对个人处以2千万欧元罚金，对企业处以2千万或者4%的上一财年全球收入（以较高者为准）罚金”。这一条处罚的计算基数中的全球营收是需要判断具体的营收主体为前提，即哪一些主体从事了这些数据处理行为并且由哪些集团主体提供了协助进而来认定完成某些经济活动中的数据处理行为的主体。企业应当尽早对这些结构进行相应的调整，例如内部治理结构中谁负责决策某一个国家的数据保护相关的事宜以及具体发生在当地的数据处理行为的目的、方式、范围。然而这项分析并不简单，因为每个国家针对从竞争法的角度来考虑哪些集团内的实体属于进行同一经济活动的主体都有不同的规定。另外，这些商业安排最好是进行相关的数据处理行为之前就确定下来，否则在后期进行调整就会花费大量的人力物力并且可能会影响业务的延续性。

二、《个人信息安全规范》修订要点

2018年5月1日，推荐性国家标准《信息安全技术 个人信息安全规范》（下称“《规范》”）正式实施，填补了我国个人信息保护在实践标准中的空白，在接下来的一年多时间里对企业开展个人信息安全合规起到了积极的指引作用。

2019年2月1日，全国信息安全标准化技术委员会（下称“信安标委”）发布了《信息安全技术 个人信息安全规范（草案）》（以下简称“《规范（草案）》”）并公开征求意见。之后，信安标委又将草案进行了完善，并先后于2019年6月25日和2019年10月24日再次公开征求意见，最终形成《信息安全技术 个人信息安全规范（征求意见稿）》（以下简称“《规范（征求意见稿）》”）。

对比《规范》、《规范（草案）》及10月最新发布的《规范（征求意见稿）》，可以看到以下修订要点与趋势。

（一）收集环节：明确“业务功能”概念，以此为基础采取折衷方案

现行《规范》将“业务功能”作为判断必要性原则的依据，《规范》要求收集个人信息的类型应与实现业务功能有直接关联；自动采集个人信息的频率应是实现业务功能所必需的最低频率；间接获取个人信息的数量应是实现业务功能所必需的最少数量。然而，作为判断必要性原则的重要依据，《规范》并未对“业务功能”作明确解释。

“业务功能”概念的引入与相关规则的变化贯穿2019年的修订。《规范（草案）》将业务功能区分为“基本业务功能”和“扩展业务功能”，替代了生效版

本在附录中出现的“核心业务功能”与“附加业务功能”。更名试图去除业务功能在企业运营中的主从关系特征：“核心”与“附加”暗含的前提是业务功能之间存在客观而确定的主从关系，而在实践中，业务功能的地位往往因市场因素与企业发展状况而发生变化；改为“基本”与“扩展”则不需要以此为前提，可以由企业自主决定将业务功能定义为“基本”还是“扩展”，更加符合企业的实际状况。就此，修订过程中曾出现多个方案，编制委曾提出在标准主文中对区分“基本”与“扩展”业务功能与获得同意的方式分别作出明确规定。最终,在后续的《规范（草案）》及《规范（征求意见稿）》中被改为放在资料性附录里。

《规范（征求意见稿）》中还明确了对“业务功能”的定义，将其界定为“满足个人信息主体的具体使用需求的服务类型”，并在主文部分新增5.3条，标题由过程稿中的“不得强迫收集个人信息的要求”改为“不得强迫接受多项业务功能”。该条明确规定“（个人信息控制者）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。”

这一变化过程反映出编制委对移动互联网应用程序（下称“App”）功能捆绑、强制授权、过度索权等违法违规收集、使用个人信息现象的关注与解决思路。近年来随着App技术在各行业的广泛应用，App功能捆绑、强制授权、过度索权、超范围收集个人信息的现象大量存在，违法违规使用个人信息的问题十分突出，引发网民热议。因而自2019年1月开始，中央网信办、工业和信息化部、公安部、市场监管总局在全国范围组织开展了App违法违规收集使用个人信息专项治理工作。“强迫接受多项业务功能”是一种典型的突破个人信息收集“合法、正当、必要”原则的现象，《规范（征求意见稿）》针对特定现象作出禁止性规定，有利于为全国范围内的执法机关提供清晰、统一的参考，也为企业合规划清了红线。但业务功能的开关、管理与个人信息收集的关系并不是一一对应的，尤其是在App以外还存在大量以其他形式收集个人信息的产品或服务。前述方案脱胎于App模式所积累的执法与合规经验，以此解释必要性原则并作为一般规则适用于各行业不同的业务模式，还需要更严密的论证。修订正是在这种考量下，建立起了以“业务功能”为基础的折衷方案，通过禁止广泛存在的不合规行为来实现个人信息保护。

（二）使用环节：聚焦个性化展示与汇聚融合

2019年修订的另一大特点是对个性化展示与汇聚融合的关注。

相较于《规范（草案）》，《规范（征求意见稿）》新增了7.4条“用户画像的使用限制”。“用户画像”的概念早在现行版本中就有所定义，在原7.3“个人信息的使用限制”与原7.10“约束信息系统自动决策”中均提出要求，即“除目的所必需外，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”，且“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”。这两项规定背后的逻辑是，个人信用评价类目的可使用直接用户画像但需提供申诉方法，商业广告目的宜使用间接用户画像避免精确定位到个人。当前的修改保留了这两项基本规则，在行文上将其单列出来，并对个人信息控制者增加了两项要求：（1）对个人信息主体的特征描述不应包含暴力黄反毒等内容或表达歧视，（2）在运营或对外合作中的使用环节不得侵权或内容违法[1]。

《规范（征求意见稿）》对于“个性化展示及退出”、“汇聚融合”的部分与之前的《规范（草案）》并无较大的改动，仅去掉了“开展常态化汇聚融合”的规定。

1. 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。

总体而言，数据的“汇聚融合”是有待进一步研究的课题。按照最新版本，对汇聚融合行为的主要约束依然是7.3条“个人信息的使用限制”，但该条也在逻辑上作了更新：7.3a）与b）的顺序调换，原c）项单独放在“用户画像的使用限制”中。因而，在逻辑上首先是不应超范围使用，其次才是处理活动产生的信息如果能够单独或与其他信息结合识别自然人个人身份，应当被认定为是个人信息，并应遵循相应的收集要求。有声音认为，企业内部进行数据的汇聚融合是进行大数据分析的基础，也是信息技术服务创新的起点，通常无法在最初的收集环节就明确处理目的及方式；其处理后的结果及产生的影响也不确定，如果汇聚融合被限制在守法合规的企业内部，危害性通常很小。按照《规范（征求意见稿）》的规定，这种情况应当开展个人信息安全影响评估（DPIA）。就此，也有呼声认为常规的汇聚融合并不需要开展DPIA，否则将大大增加企业的合规成本，阻碍科技产业创新。因而该规定后续将如何变化还有待观察。

此次修订还将原“约束信息系统自动决策”改为“信息系统自动决策机制的使用”，突出了自动化决策机制作为数据使用活动的本质，同时增加和修改了开展DPIA的启动条件、阶段和周期要求。

（三）聚焦注销难：增加对注销机制的要求

如前文所述，今年的修订回应了社会各界对个人信息违法违规收集使用问题的关切。早在2013年发布的《电信和互联网用户个人信息保护规定》（“工信部24号令”）中就指出，“电信业务经营者、互联网信息服务提供者在用户终止使用电信服务或者互联网信息服务后，应当停止对用户个人信息的收集和使用，并为用户提供注销号码或者账号的服务。”《规范》中也明确规定“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”。然而对于什么样的方法属于“简便易操作”业内尚未形成一致观点或做法，目前各类互联网服务中普遍存在的注销难，某些企业基于安全性或其他考虑还会要求用户在注销时去公安局开具证明或手持身份证拍照。

面对这些现象，《规范（征求意见稿）》在第7.12条“个人信息主体注销账户”中增加要求：（1）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；（2）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；（3）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；（4）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；（5）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。《规范（征求意见稿）》还考虑到了一些特殊领域的企业为履行法律义务需长期留存特定种类的个人信息，因而在该条中加注“因法律法规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”，避免了企业以守法为名行不法之实。

（四）其他值得注意的修订要点

1. 提出“信息安全工程”倡议

《规范（征求意见稿）》鼓励个人信息控制者根据国家有关标准在系统工程阶段考虑个人信息保护要求，这一倡议借鉴并回应了GDPR等国际个人信息/数据保护框架中的Privacy by Design制度，相关标准正在制定当中。

2. 强调在委托处理与共享转让中对相关方的管理

《规范（征求意见稿）》在第8.1条和第8.2条新增了个人信息控制者在数据相关合作中的如下义务：在委托处理合作中得知或者发现受委托者未按照委托要求处理个人信息或未能有效履行个人信息安全保护责任的，在共享转让合作中发现数据接收方违反法律法规要求或双方约定处理个人信息的，应立即要求受托者或数据接收方停止相关行为，且采取或要求受委托者采取有效补救措施（例如更改口令、回收权限、断开网络连接等）控制或消除个人信息面临的安全风险。必要时，个人信息控制者应终止与受委托者或数据接收方的业务关系，并要求及时删除从个人信息控制者获得的个人信息。

3. 强调在共同控制中的责任连带

《规范（征求意见稿）》在第8.6条中新增对共同控制者的规定，强调如个人信息控制者未向个人信息主体明确告知第三方（即共同控制者）的身份，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。

4. 强调对第三方接入的管理

依据《规范（征求意见稿）》，除了建立第三方接入管理机制和工作流程、以合同形式明确安全责任、向用户明确标识产品或服务由第三方提供外，企业还应要求第三方向用户征得收集个人信息的授权同意，核验其实现的方式。此外，征求意见稿建议对第三方嵌入或接入的自动化工具开展技术检测和审计，来确保其个人信息收集、使用行为符合约定要求。这一点尤其对通过App使用第三方SDK进行服务的网络运营者提出了更高要求。

5. 细化“组织管理”相关要求

相较《规范》，《规范（征求意见稿）》中规定“应由具有相关管理工作经历和个人信息保护专业知识的人员担任”，同时还对其权责设置作出规定：1）个人信息保护负责人“直接向组织主要负责人报告工作”；2）组织应为个人信息保护负责人和个人信息保护工作机构“提供必要的资源，保障其独立履行职责”。

修订还进一步细化了《网络安全法》第二十二条规定的 “双告知”义务在个人信息保护场景下的适用标准：如个人信息泄露事件可能会给个人带来较大影响，如个人敏感信息的泄露，应当向个人信息主体进行告知；发生超过100万人个人信息或者关系国计民生、公共利益的个人敏感信息泄露、毁损、丢失的安全事件，应将有关情况报告网信部门。这为企业进行安全事件处置提供了切实有效的行动指引，避免实践中因为危害不大的事件频繁告知或报告造成用户恐慌、占用行政资源，也避免企业心存侥幸而不告知、造成损害的扩大。

6. 倡议建立个人信息处理活动的记录

相较《规范》，《规范（征求意见稿）》明确了需要记录的事项，便于企业在实际业务场景中对个人信息的处理情况进行核查。

7. 结构与措辞更加合理

此次修订在行文结构方面上更加合理，措辞也更加严谨。例如，《规范（征求意见稿）》中多处将“不得”改为“不应”，将“如……”改为“……时”，将“访问”改为“查询”，将“用户”改为“个人信息主体”，统一个人信息的英文翻译为“personal information”，将“保障个人信息主体选择同意权”改为“实现个人信息主体自主意愿”等。这些修改一方面立足于标准在执行过程中的法律效力，避免产生具有法律强制力的暗示，另一方面使得标准作为规范性文件具有更严谨的逻辑，减少适用过程中的误解。

8. 附录部分的重要修订

此次在附录部分的修订也值得关注：

（1） 在附录B个人敏感信息判定的示例中，征求意见稿将“系统账号”改为“个人信息主体账号”，并明确密码、口令、口令保护答案、用户个人数字证书等与个人信息主体账号的“组合”，才能构成网络身份标识信息；

（2） 附录C除了前述第一点中介绍的，对基本业务功能和扩展业务功能分别规定了告知和获得同意的义务之外，对交互式功能界面设计示例的适用范围也从“个人敏感信息”扩大到“个人信息”；

（3） 附录D对收集环节的编写要求，将收集和使用个人信息的“目的”改为了“业务功能”，并要求根据不同“业务功能”（原为“目的”）分别列出个人信息类型。如第一点中介绍的，“业务功能”将作为落实合规要求中一个重要基础性概念。

整体而言，《规范（征求意见稿）》总结并吸纳了这一年多来在《规范》适用过程中的经验。社会问题层出不穷，统一立法呼之欲出。面对我国个人信息保护规则散见于多部法律、法规之中的现状，《个人信息保护法》已经被列为“十三届全国人大常委会立法规划”“条件比较成熟、任期内拟提请审议的法律草案”。在这样的时代背景下，《规范（征求意见稿）》切实解决社会现实问题、回应人民群众所盼所需，体现了我国在个人信息保护监管方面的积极探索，在《个人信息保护法》出台之前还将继续发挥着承前启后的重要作用。

三、流量的突围：线下流量及新零售中的数据保护问题

全球零售业经过一百多年的演进，经历了从单一到多元、从线上线下平行（O&O）到线上线下交互（O2O）再到线上线下融合（OMO）的模式转变。随着互联网、大数据、人工智能等技术的不断发展，新零售以及无人商店（例如Amazon Go以及阿里巴巴的无人超市）已然兴起。何为“新零售”？ 2016年，时任阿里巴巴集团董事局主席的马云在阿里云栖大会上第一次提出了“新零售”。在最初作为概念被提出的阶段，“新零售”并没有确切的解释。随着互联网巨头两年多的探索、创新和实践，“新零售”模式逐步清晰化，即以用户为中心，以技术为驱动，依托智能化、可协同的基础设施和新供应链，重构人、货、场，实现“全场景、全客群、全数据、全渠道、全时段、全体验、全品类、全链路”、线上线下深度融合的零售新模式。相比于传统的零售模式，新零售更强调线上服务、线下体验以及现代物流的深度融合。

而要实现新零售模式中的深度融合，企业必须要对线下的数据进行实时收集以及共享。与线上数据收集所不同的是，线下数据收集无法使用网站代码、cookie、在App中SDK埋点等线上收集方式。为了实现线下的数据收集，人脸识别、Wi-Fi探针、可穿戴设备等技术被广泛应用。门店通过此类技术对顾客在门店的行为进行收集和处理，并结合现有的会员体系以及线上的购物浏览行为和偏好来完整地了解顾客的需求，进而在线下门店的服务过程中向顾客提供更为针对性的个性化服务，从而节省顾客在众多商品中的拣选时间。此外，这些线下流量的数据对于商户也具有巨大价值，例如商户向银行进行贷款时，可以通过展示其店铺的真实流量来有效证明其还款能力。银行也能够在对店铺流量有清晰了解的情况下，更好地进行贷后的还款管理。

在我国，个人信息被广泛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或者反映特定自然人活动情况的各种信息，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、行踪轨迹等。企业在收集用户的个人信息前，需要向用户披露收集信息的目的、方式及范围并取得用户的同意。在收集线上流量的场景中，企业一般可以通过在网站、App等交互界面披露隐私政策并要求用户主动点选来符合法律要求。但在收集线下流量的场景中，因为缺乏直观、便捷的用户界面来展示企业的隐私政策，也没有一个能够记录用户同意的机制来证明合规性，满足“告知 + 同意”的法律要求便存在困难。因此，如何符合披露和获取用户同意的法律要求，成为了企业收集线下数据收集的难点之一。此外，在部署人脸识别以及Wi-Fi探针技术之前，需要考虑应用这些技术收集个人信息时的数据保护问题及其他与此相关的问题。

（一）常见的线下数据收集方式及特点

在2002年的科幻片《少数派报告》中，男主角一走进服装店，就立刻被店内的人工智能系统所识别，并在向男主角打招呼后便开始推荐适合男主角购买的商品。在今天，这个场景显然已从科幻片的想象走入了生活的现实。

对线下门店而言，流量可理解为客流量，包括通过率（店铺门前经过了多少顾客）、入店率（进店了多少顾客）、购买率（进店顾客有多少产生购买转化）等指标。为获取这些数据，企业必须在顾客进入门店时获取能够匹配到企业自己的会员数据库中的识别符，这些识别符可能是会员号、手机、身份证、手机的MAC地址、人脸特征等。只有在匹配到这些识别符后，顾客在门店内的行为才能够有效地被利用起来。

1. 人脸识别

线下流量的主要收集场景之一是在线下门店安装摄像头，利用人脸识别技术识别出顾客的年龄、性别甚至具体身份等信息并记录顾客在店内的消费行为，最终统计分析出店面的客流数量、区域人数、顾客停留时长、区域热力图等数据，将顾客进店后的行为进行“数据化”。然而这些具有人脸识别功能的摄像头并非全部需要收集人脸的特征，例如在分析顾客的区域热力图或者客户停留比较长时间的产品摆设区时，技术上只需识别这些人的性别特征或是人数即可。这种收集方式被称为种类化（categorization），与人脸识别后收集人脸的特征（feature）进行匹配的方式不同。

相比使用一般会员卡或使用其他会员的识别符的方式，采用人脸识别方式的优势在于，可以在顾客进店的第一时间进行识别，并收集更多顾客的浏览行为。否则，如果顾客本身不是会员或者本身没有告知店员其识别符或者会员号，则这些行为可能没有办法得到有效记录。

2. 设备识别

Wi-Fi探针是指基于Wi-Fi探测技术，自动识别特定范围内已开启Wi-Fi接收装置的移动终端设备（Android或IOS智能手机、手提电脑、平板等）并获取设备MAC信息的一种硬件。其原理是手机等终端设备只要开启Wi-Fi功能，就会发出探测请求帧寻找可连接的Wi-Fi信号，当该设备进入Wi-Fi探针的侦听范围时，探针就会截获此帧并分析出其MAC层与物理层的信息，获得设备MAC地址、Wi-Fi信号强度、Wi-Fi信号频道、信号帧类型等数据，并通过信号强度和在探针范围内的停留时间分析生成活动轨迹、停留时间等数据信息。

虽然有反对意见表示MAC地址并非像IMEI一样能够直接识别某台设备，但是考虑到MAC地址一般都会

被许多公司自动收集，因此在许多数据库中都已经能够很快地通过MAC地址匹配出更多的个人信息。因此，基于这种可识别性，MAC地址也属于个人信息。

3. 可穿戴设备

通过可穿戴设备记录顾客线下的行为并收集线下数据已经是较为常见的数据收集方式。通过可穿戴设备并且回传到手机或者用户的其他设备，商家可以通过App端获取顾客的行为轨迹，并对该等行为进行分析。

（二）线下数据收集的合规问题

2019年的3.15晚会上爆出了Wi-Fi探针存在的未经同意非法取得个人信息的问题，主要的问题在于，部署Wi-Fi探针以收集用户的MAC地址时，没有向用户明确告知并取得用户的同意。对于人脸识别摄像头的部署，如果商家期望收集人脸的特征来进行匹配会员的信息，需要考虑是否能够进行相应的告知和获取同意的问题，并且进一步考虑如果顾客不同意，则顾客是否能够继续获得相应的产品和/或服务。

1. 如何进行“告知 + 同意”？

根据《网络安全法》第41条和《消费者权益保护法》第29条等规定，企业在收集顾客个人信息前，应当向顾客告知其收集和使用个人信息的目的、方式和范围，并取得顾客的同意，否则可能会面临被有关部门处以警告、没收违法所得、罚款等行政处罚以及被顾客提起侵犯其个人信息保护权利的民事诉讼的风险。无论通过线上渠道还是线下渠道收集顾客的个人信息，企业都需要满足此等要求。

线下缺乏类似线上的可视化的界面可以用来完成“告知 + 同意”的动作。在一般大型的商场或者小型的商店的门口粘贴隐私政策来进行公告，并告知阅读之后走进来商店即代表同意店家使用Wi-Fi探针或者是人脸识别摄像头显然也不是商家所希望采取的方式。但是如果不进行有效地告知并获取同意，商家有可能存在违规的风险。除此之外，如果需要使用人脸这种生物可识别信息（biometric data）用来做识别符，还可能涉及收集个人敏感信息的问题。收集个人敏感信息需要更为明确的告知以及顾客需要给予明确的同意。

2. 如何进行个人信息安全影响评估?

线下流量会收集到大量的个人信息，包括行为数据以及作为识别符的人脸生物特征等。这些用户画像以及个人的生物特征都需要被保护。收集这些个人敏感信息会让这项数据处理行为给个人造成极大的影响，例如利用人脸特征冒名顶替，从而获取更多的信息甚至个人财产。

此外，如果黑客进入到存储这些个人信息的数据库中，则可以准确了解到用户近期的消费情况等信息，使用钓鱼软件对用户进行诈骗或者是网络盗窃的成功率则会大大提高。与该等行为相关的案例在很多国家都屡见不鲜，例如新加坡曾经发生过一起商场的数据库被黑客攻击后，使用数据库内的信息发送钓鱼邮件，进而导致商场被新加坡的数据保护监管机构PDPC处罚的案例 。

考虑到部署这些技术来实现线上线下流量的融合可能会带来更多的数据保护风险，企业一般都需要在部署前考虑进行个人信息安全影响评估。虽然网安法中没有明确哪些情况需要进行个人信息安全影响评估，但是TC260于2019年6月25日发布的最新版《个人信息安全规范》征求意见稿中，可以找到有关个人信息保护安全影响评估的指引。个人信息安全影响评估应主要评估处理活动遵循个人信息安全基本原则的情况，以及个人信息处理活动对个人信息主体合法权益的影响，内容包

括但不限于：

（1）个人信息收集环节是否遵循目的明确、选择同意、最少够用等原则；
（2）个人信息处理是否可能对个人信息主体合法权益造成不利影响，包括是否会危害人身和财产安全、损害个人名誉和身心健康、导致歧视性待遇等；
（3）个人信息安全措施的有效性；
（4）匿名化或去标识化处理后的数据集重新识别出个人信息主体或与其他数据集汇聚后重新识别出个人信息主体的风险；
（5）共享、转让、公开披露个人信息对个人信息主体合法权益可能产生的不利影响；
（6）发生安全事件时，对个人信息主体合法权益可能产生的不利影响。

此外，个人信息安全影响评估中最重要的问题之一为是否能够采用对隐私和个人信息保护影响最小的替代技术，或者是不部署这项技术是否也能够完成这个数据处理行为的目标。如果企业不能提出使人信服的理由，监管机构很可能在事后会对技术的部署及数据处理行为的必要性提出质疑，或者重点关注用户是否能够自由选择不受制于这项数据处理行为（genuine choice of opt-out）。

（三）实践中企业的应对之策

欧盟一些成员国近期都对人脸识别技术的部署方进行了处罚，主要的处罚理由是没有满足个人信息保护的基本原则以及没有进行安全影响评估。有些企业还因为在美国部署人脸识别技术、偷偷收集个人信息而面临集团诉讼。虽然在很多时候，商场或者门店被认为是公共场所，因而民众在公共场所的行为也不被认定为隐私，但是这种没有隐私期待的假定不代表用户对于其个人信息没有保护的期待。

企业在开展新零售之前应当充分想好应对这些合规问题的对策：

1. 在部署这些线下流量数据收集技术之前，企业应做好具体的个人信息安全影响评估，识别可能给个人信息主体造成的风险，设计和采用相应的风险控制措施。在部署之前，企业应当充分考虑如何实现个人信息收集行为的透明化。例如在欧洲，在对自动驾驶汽车进行路测时，测试企业均会在车身上考虑粘贴一个二维码让用户扫描和获取隐私政策。这似乎也给新零售的店家提供了一个思路，即在线下门店通过在门店外张贴海报、告示等方式对其个人信息的收集和使用规则做出说明。但是这种粘贴海报公式的方式如何确保每一个进店的人都确实阅读了这个隐私政策？此外，如果用户不同意收集个人信息就无法进入商场，这是否似乎又违反了数据保护基本原则中的正当和必要原则？

2. 制定内部的管理流程，对用户画像进行精准的管理。TC260于2019年10月22日发布的最新版《个人信息安全规范》征求意见稿中对用户画像的管理对企业提出了新的要求，其中包括：用户画像中对个人信息主体的特征描述，不应包含淫秽、色情、赌博、迷信、恐怖、暴力的内容或表达对民族、种族、宗教、残疾、疾病歧视的内容。在业务运营或对外业务合作中使用用户画像的，不应侵害保护公民、法人和其他组织的合法权益；以及危害国家安全、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。例如，如果奢侈品类门店在使用人脸识别来标注顾客的购买偏好的过程中同时标注了“小三”，则这种用户画像带有一定的歧视意味，企业应当避免使用。

3. 采取充分的技术措施和其他必要措施保护存储的顾客个人信息（尤其是个人敏感信息）的安全，避免发生个人信息泄露或安全事件。如果订单系统与会员系统是单独分开的两个系统，企业可以考虑对两个系统进行同等级别的保护。另外，对于收集作为识别符的人脸特征以及其他敏感的个人信息，企业应当考虑对这些信息进行加密处理。对内也需要加密并且进行权限管控。对于能够向用户进行推送的系统应当严格管理，避免出现同一个账号多人通用或者是任由员工将账号放在不安全的公共云服务上等。

四、隐私诉讼在中国：向左走向右走

近年来，个人信息泄露事件频繁发生，造成的影响巨大，并且个人信息泄露事件在美国及欧洲经常会引发集体诉讼[1]，个人信息安全已经是很多企业最关注的领域之一。隐私诉讼在美国和欧洲的实践是两种不同的方向和模式。目前美国的司法实践呈现出“向左走”趋势，即要求原告必须证明由于个人信息泄露产生了实际损害才能获得相应的赔偿，诉讼成功难度极大。与之相反，《通用数据保护条例》（General Data Protection Regulation, “GDPR”）提供了第82条这个武器，数据主体可以很轻易地依据这条提起诉讼（private action），并且能够很容易求偿物质或者非物质的损失。这种低门槛以及推定数据控制者有过错的隐私诉讼模式则呈现了与美国完全不一样的“向右走”的模式。随着加州的《消费者隐私法案》（California Consumer Privacy Act, “CCPA”）创设的诉权（right to private action），其机制也与GDPR第82条类似，美国的隐私诉讼是否会向欧洲靠拢有待观察。

目前，中国隐私诉讼的发展还处在比较初步的阶段，主要的原因在于个人信息保护权是在2017年《民法总则》颁布后才有的，之前的争议基本上聚焦在隐私权的角度。随着近年来我国数据安全及个人信息保护方面法律法规的完善及公民保护个人信息及隐私意识的逐步提升，实践中已经出现了不少公民因个人信息被泄露而提起侵权诉讼的案例，例如四川航空案[2]、去哪儿网案[3]、京东案[4]、苏宁易购案[5]等。这些代表性案例中，去哪儿网案更是被列入2018年最高人民法院涉互联网典型案例，明确了由于航空公司、网络购票平台疏于防范导致消费者个人信息泄露，应当承担相应的侵权责任[6]。

（一）美国及欧洲的隐私侵权诉讼模式

1. 美国模式：向左走

1. 近年来，美国由于个人信息泄露引发的著名集体诉讼案件包括Equifax案件、Yahoo案件及Anthem Inc.案件等，参见https://www.classaction.com/data-breach/lawsuit/，最后访问日期：2019年10月9日；欧洲由于个人信息泄露引发的集体诉讼案件包括英国Morrisons案件、British Airways案件等，参见“GDPR：数据泄露集体诉讼来到欧洲”，2018年9月26日，https://www.bankinfosecurity.com/interviews/gdpr-data-breach-class-action-lawsuits-come-to-europe-i-4125, 最后访问日期：2019年10月9日。
2. 参见“林念平与四川航空股份有限公司侵权责任纠纷二审民事判决书”，四川省成都市中级人民法院，(2015)成民终字第1634号。
3. 参见“庞理鹏与北京趣拿信息技术有限公司等隐私权纠纷二审民事判决书”，北京市第一中级人民法院，(2017)京01民终509号。
4. 参见“赵亚琼等与北京京东叁佰陆拾度电子商务有限公司隐私权纠纷一审民事判决书”，北京市大兴区人民法院，(2017)京0115民初15827号。
5. 参见“原告李洋与被告江苏苏宁易购电子商务有限公司隐私权纠纷一审民事判决书”，江苏省南京市玄武区人民法院，(2016)苏0102民初1123号。
6. 参见“最高人民法院发布第一批涉互联网典型案例”，2018年8月16日，http://www.court.gov.cn/zixun-xiangqing-112611.html, 最后访问日期：2019年10月9日。
7. Daniel J. Solove & Danielle Keats Citron, “风险与焦虑：数据泄露损害的一种理论”，德克萨斯法律评论，Vol. 96:737 2018。

美国的数据泄露事件后引发的许多集体诉讼中，原告是否受到了实际损害是建立原告的适格诉讼主体（standing）的重要要件之一[7]，而且法院会关注这项实际损害是不是实际或者将要发生（immanency）。很多时候，原告都有证据证明被告确实没有行使相应的注意义务来保护原告的个人信息。但在大部分案件中，法院都没有着眼于被告是否存在过错，而是原告是否产生相应的实际损害，例如信用卡诈骗或身份盗用[8]。此外，损害往往指的是实际损害，而不仅仅是受损害的风险或可能性。在2013年“克拉珀诉大赦国际”一案（Clapper v. Amnesty International）中，美国最高法院认为，对于声称未来可能受到伤害的原告，要在联邦法庭获得诉讼资格，原告必须证明其声称的损害即将到来（requirement of immanency）。 这通常被成功地用来击败原告的控告，因为他们无法指出已经发生的任何特定的身份盗窃或其他损害，只能说明发生这种损害的可能性[9]。当然实践中并非所有法院都认为必须具备即将到来的损害，2015年美国第七巡回法院判决Remijas v. Neiman Marcus Group案件时指出，损害的“实质性风险”可能已经足够[10]。2016年的Spokeo案件中，法院认为原告除了需要证明损害即将到来之外，还需要证明他们遭受了“具体的”（concrete）或“实际的”（de facto）损害[11]。

除了证明数据主体为适格原告上原告需要证明其受到了实际损害，美国法院对于损害赔偿的认定也是比较谨慎的。原告只有在证明其受到了直接经济损失的情况下才能主张损害赔偿，单独针对非经济损失提出的损害赔偿请求无法被法院认定[12]。然而实践中，对于直接经济损失的证明非常困难，使得原告实际上很难获得损害赔偿。例如在银行卡信息泄露案件中，实际损害经常并不存在或很难被量化，因为在发生了数据泄露案件之后，银行卡常常被注销并重新办理，银行也通常会被要求退还消费者未授权消费的费用，使得实际损害难以证明[13]。美国学者对于个人信息和隐私损失（privacy harm）总结为两种形式，一种为实际的损失（objective category of privacy harm），一般表现为财产或者人身损失，这种损失法院一般都会支持；另外一种是尚未发生实际损失，但是主观上存在担心数据被滥用导致的焦虑（subjective category of privacy harm）[14]。这些焦虑等非实际发生的损失基本上没有被美国法院支持过。

目前隐私诉讼在普通法的层面相对困难，但是自从CCPA规定了具体的诉权后，针对数据泄露事件提起民事诉讼更加容易，因为数据主体可以不再需要依据普通法提起诉请，而是直接根据CCPA的规定。此外，使用CCPA的条款直接起诉可以跳过证明实际损失这一环节，但这一条款的适用也是有限制的，例如消费者在提起诉讼之前具有向泄露数据的企业进行通知的义务，且企业在30天内没有补救和解决数据泄露事件或者违规的情况下数据主体才可以起诉。CCPA虽然在严格程度上比肩GDPR，但是CCPA目前看起来并不代表其他州对于数据保护立法的态度，因此CCPA这种创设诉权的方式也不一定最后会发展成美国的主流。

2. 欧洲模式：向右走

相较于美国，欧洲因为其在欧盟层面的许多公约（例如《欧盟基本权利宪章》）倾向于给予消费者更多的保护。GDPR第82条允许数据遭泄露方针对数据控制者及数据处理者直接提起损害赔偿请求，且适用过错推定原则，除非数据控制者或数据处理者能够证明其没有过错，否则将要承担损害赔偿责任。这一规定将举证责任倒置，无疑在很大程度上减轻了原先消费者的举证责任。此外，GDPR下不仅针对经济损失（material damage），针对非经济损失（non-material damage）也能够单独提起损害赔偿请求[15]。

因为GDPR自2018年5月25日才生效，依据GDPR

8. Patrick J. Lorio，“难以实现的数据泄露诉讼，第三条适格诉讼主体及建议的法律解决方案”，哥伦比亚法律及社会问题评论，2017, 51 (1) :79-128。
9. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1142 (2013).
10. Remijas v. Neiman Marcus Grp., LLC, 794 F. 3d 688, 693 (7th Cir. 2015).
11. Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016).
12. 如注9。
13. “CCPA将改变数据泄露诉讼”，2019年8月20日，https://www.jdsupra.com/legalnews/the-ccpa-could-reset-data-breach-14801/, 最后访问日期：2019年10月9日。
14. M. Ryan Calo, “隐私损失的界限”，Vol. 86:1131。
15. 见GDPR第82（1）条。
16. 参见“德国：GDPR下第一个支持非经济损失的法院判决”，2018年12月12日，https://blogs.dlapiper.com/privacymatters/germany-first-court-decision-on-claims-for-immaterial-damages-under-gdpr/, 最后访问日期：2019年10月9日。

第82条的案例还不多，原因之一也是这些诉讼程序一般会比较长，因此可能还没有生效的判决可以分析。2018年11月，德国地方法院Diez根据GDPR第82条（1）针对原告的非经济损失赔偿请求做出了判决。在该案中，原告收到了被告发送的要求其同意接收电邮新闻稿的邮件，这在德国被认为是垃圾邮件且违反了GDPR。原告根据GDPR第82条（1）对其受到的非经济损失向被告提出了500欧元的损害赔偿请求。尽管法院在该案中认可非经济损失可以单独主张损害赔偿，但由于原告已经收到了被告支付的50欧元的赔付，法院认为超过该数额的赔偿并不合理，因此驳回了起诉[16]。

（二）隐私诉讼在中国的发展

1. 诉讼程序

如在中国发生数据泄露事件，数据被泄露方可以寻求以下三种救济方式：提起侵权诉讼、消费者权益保护集体诉讼或消费者协会和检察院公益诉讼。这三种救济方式可能会指向同样的结果，但在所运用的实体法律及救济的程序上却有所不同。例如消费者保护协会或者检察院提起的公益诉讼可能会从消费者权益保护法的角度进行考虑，主要关注企业（即数据控制者）是否在个人信息的收集、处理、使用、分享以及删除上都符合法律法规规定，并非重点关注数据处理行为是否造成了侵权和损失。

目前在侵犯个人信息保护权上的消费者权益保护的集体诉讼尚未有先例，但在检察院公益诉讼方面实践中已有一定程度的发展。在数据泄露事件涉及众多消费者合法权益可能遭受侵害时，消费者可以提起“集体诉讼”。尽管我国并没有美国式的“集体诉讼”制度，但是《民事诉讼法》中共同诉讼的规定一定程度上与集体诉讼接近。根据《民事诉讼法》第53条[17]、第54条[18]，当诉讼标的是共同或同类时，经当事人同意且法院认为可以合并审理的，可以发起共同诉讼，并由当事人推选代表人进行诉讼。然而，虽然中国也曾发生类似的酒店信息大规模泄露事件，但我们暂未查得涉及信息泄露的集体诉讼案件。除了由众多消费者提起共同诉讼，在我国，还可以由消费者协会或检察机关，根据《民事诉讼法》[19]与《消费者权益保护法》[20]的规定，对于侵害众多消费者合法权益的行为，提起消费者公益诉讼。能够提起消费者公益诉讼的只有省级的消费者协会[21]，而在消费者协会不起诉的情况下，可以由检察机关向法院起诉。该领域发展的一大背景为2019年1月25日，中央网信办、工业和信息化部、公安部、市场监管总局共同发布了《关于开展App违法违规收集使用个人信息专项治理的公告》，进一步强化收集使用个人信息的规则，明确重点查处行为。最高人民检察院副检察长张雪樵在“检察公益诉讼工作深入发展，实现办案全覆盖”发布会上也曾指出，除了将法律规定的公益诉讼领域，如食品安全、环境保护等作为重点外，对于群众反映强烈的、媒体报道关注的热点事件，例如个人信息保护、大数据安全、互联网侵权等热点问题，检察机关也会积极探索检察公益诉讼发挥作用的路径[22]。目前各级检察机关就个人信息保护领域的行政公益诉讼问题也展开了研究和试点[23]。尽管个人信息保护并不是《民事诉讼法》和《行政诉讼法》中明确列举的可由检察机关提起行政公益诉讼的领域，[24]但实践中已经出现了检察院因消费者个人信息被侵犯而提起公益诉讼的案例[25]，可见检察院公益诉讼作为个人信息泄露的一种救济方式是不容忽视的。

2. 实体问题

我国《民法总则》第110条规定了自然人享有隐私权[26]，第111条规定了自然人的个人信息受法律保护[27]。这两个权利在内容上是有所区别的，也有重合之处。数据泄露事件可能引发自然人提起隐私权或个人信息权被侵害的侵权诉讼。根据《侵权责任法》第6条[28]，隐私权或个人信息权均为一般人身权，因此在判断侵权责任上适用一

17.《民事诉讼法》第53条：“当事人一方人数众多的共同诉讼，可以由当事人推选代表人进行诉讼。代表人的诉讼行为对其所代表的当事人发生效力，但代表人变更、放弃诉讼请求或者承认对方当事人的诉讼请求，进行和解，必须经被代表的当事人同意。”

18.《民事诉讼法》第54条：“诉讼标的是同一种类、当事人一方人数众多在起诉时人数尚未确定的，人民法院可以发出公告，说明案件情况和诉讼请求，通知权利人在一定期间向人民法院登记。”

29.《民事诉讼法》第55条：“对污染环境、侵害众多消费者合法权益等损害社会公共利益的行为，法律规定的机关和有关组织可以向人民法院提起诉讼。人民检察院在履行职责中发现破坏生态环境和资源保护、食品药品安全领域侵害众多消费者合法权益等损害社会公共利益的行为，在没有前款规定的机关和组织或者前款规定的机关和组织不提起诉讼的情况下，可以向人民法院提起诉讼。前款规定的机关或者组织提起诉讼的，人民检察院可以支持起诉。”

20.《消费者权益保护法》第37条：“消费者协会履行下列公益性职责：（七）就损害消费者合法权益的行为，支持受损害的消费者提起诉讼或者依照本法提起诉讼。”

21.《消费者权益保护法》第47条：“对侵害众多消费者合法权益的行为，中国消费者协会以及在省、自治区、直辖市设立的消费者协会，可以向人民法院提起诉讼。”

般过错原则，需要考虑四个方面：（1）具有侵权行为；（2）侵权行为造成了损害后果；（3）侵权行为与损害后果有因果联系；（4）侵权人存在过错。

司法实践中，数据泄露案件中原告往往很难进行举证，而法院由于其技术能力的限制也很难查明具体事实，因此法院在认定数据泄露的责任归属方面存在一定困难。“去哪儿网”案件中，法院认为“在排除了庞理鹏和鲁超的泄露可能性之后，趣拿公司、东航、中航信都存在泄露信息的可能”[29]。

除了认定责任归属的困难之外，司法实践中法院对于侵权人过错的认定及原被告之间举证责任的分配尚没有一个统一的看法。侵权人过错方面，在“四川航空案”中，法院认定四川航空没有尽到保障个人信息安全等法定义务，主要的原因为“尽管‘没有泄露’作为一个消极事实，四川航空公司很难证明和说明，但可以通过举证证明其履行了采取技术措施和其他必要措施，以确保消费者个人信息安全的义务，来说明林念平信息的泄露并非四川航空公司的过错造成的。”[30]在“京东案”中，针对京东辩称的其已经做到了提示义务，并无过错，及原告被诈骗属于自身疏忽，其自身存在重大过错的观点，法院并没有进行论述和分析，而是以证据规则驳回了原告的诉请[31]。

在原被告的举证责任方面，在“苏宁易购案”和“京东案”中，法院都主张侵权责任构成要件的举证责任应由原告负担，由于原告在两个案件中仅能证明损害事实，无法证明其他的侵权构成要件，因此法院未支持原告的诉讼请求[32]。而在“四川航空案”中，法院以公平为原则采取了举证责任倒置，认为由于消费者举证能力有限，应当由被告企业承担证明责任[33]。2018年8月17日，最高人民法院发布了第一批涉互联网典型案例，其中将去哪儿网案件列为了个人信息保护领域的典型案例。法院在“去哪儿网”案件中并没有突破“谁主张谁举证”这一原则，而是在举证责任分配上将证明信息泄露的责任从弱势的原告一方转移到了需要承担信息安全保障义务的企业一方，认定侵权事实发生“具有高度盖然性”，由此认定原告已经完成了举证[34]。尽管去哪儿网案件中的法律问题并非没有争议，但其作为典型案例一定程度上反映了未来隐私侵权诉讼方面的发展趋势，法院可能会在分配举证责任上采取倾向于保护消费者的态度。

在认定损害赔偿方面，实践中法院往往支持直接的经济损失，而对于无明确证据的精神损害赔偿请求则不予支持。根据《最高人民法院关于确定民事侵权精神损害赔偿责任若干问题的解释》的规定，因侵权致人精神损害，但未造成严重后果，受害人请求赔偿精神损害的，一般不予支持，人民法院可以根据情形判令侵权人停止侵害、恢复名誉、消除影响、赔礼道歉；因侵权致人精神损害，造成严重后果的，人民法院除判令侵权人承担停止侵害、恢复名誉、消除影响、赔礼道歉等民事责任外，可以根据受害人一方的请求判令其赔偿相应的精神损害抚慰金。从这个角度来看，如果不涉及侵犯隐私而仅仅是涉及侵犯个人信息保护权（《民法总则》第111条），可能还难以直接起诉要求精神损害赔偿。这些难点在这几个具体的案例中也可以体现，例如“四川航空”案中，法院支持了原告主张的机票支出、会员积分、机票差价等直接损失及由于诉讼而产生的交通费，但并未支持原告主张的精神损害赔偿金[35]。“去哪儿网”案件中，法院支持了原告的赔礼道歉主张，但认为现有证据无法证明原告因隐私信息被泄露而引发明显的精神痛苦，而对原告的精神损害赔偿请求不予支持[36]。

3. 对企业的建议

虽然我国的个人信息权在民事诉讼的司法实践上相对于侵犯公民个人信息罪以及具体的行政执法而言相对较少，但目前法律项下是有相关救济途径的。目前也有许

22. “最高检通报2018年检察公益诉讼工作情况”http://www.spp.gov.cn/spp/zgrmjcyxwfbh/zgjtbjnjcgyssqk/index.shtml，最后访问时间2019年10月9日。
23. 例如上海市检察院于2019年6月以“检察建议书”的形式要求10家App运营商加强个人信息保护。浙江省诸暨市检察院在处理一起涉及装修公司、房产公司内部员工泄露客户个人信息的刑事案件时，也同时启动了公益诉讼程序，分别向诸暨市市场监督管理局发出诉前检察建议书，以及向诸暨市建设局及装修装饰行业协会发出工作函。之后诸暨市市场监督管理局对涉案的装修公司和房产公司分别作出行政处罚，诸暨市建设局及装修装饰行业协会还组织了协会企业签订个人信息保护承诺书，以加强行业内部整治。
24. 《民事诉讼法》（2017年6月27日修正）第五十五条：“对污染环境、侵害众多消费者合法权益等损害社会公共利益的行为，法律规定的机关和有关组织可以向人民法院提起诉讼。人民检察院在履行职责中发现破坏生态环境和资源保护、食品药品安全领域侵害众多消费者合法权益等损害社会公共利益的行为，在没有前款规定的机关和组织或者前款规定的机关和组织不提起诉讼的情况下，可以向人民法院提起诉讼。前款规定的机关或者组织提起诉讼的，人民检察院可以支持起诉。”《行政诉讼法》（2017年7月1日修正实施）第二十五条：“行政行为的相对人以及其他与行政行为有利害关系的公民、法人或者其他组织，有权提起诉讼。有权提起诉讼的公民死

多学者正在探究如何解决这种司法实践上的难题，例如许多学者专家正在讨论起草《最高人民法院关于审理个人信息纠纷案件适用法律若干问题的解释（学者建议稿）》，希望对许多司法实践中的空白进行厘清。在数据泄露事件发生时，这些大规模的民事诉讼是有可能发生的。虽然目前法律框架上尚未走入类似GDPR第82条的完全过错推定，但东航去哪儿案件一定程度上代表了对于消费者和个人信息权保护的取向。但是东航去哪儿一案并非是完美的先例，因为法院在整个案件的分析论理中均没有对具体是哪个主体出现了数据泄露事件以及两个主体在该项侵权之诉中是否是共同侵权关系进行讨论，而是用“高度盖然性”这个表述暂时搁置这个问题的答案。

对于证明企业在数据保护上没有过错，下面几个角度是可以考虑的，这点可以结合企业的具体数据保护合规工作来落实。

（1）鉴于侵权人具有过错是隐私权或个人信息权的侵权构成要件之一，企业应当在运营过程中严格履行其法定的安全保障义务，确保合规，这在应对隐私诉讼时可以作为企业无过错的抗辩。《网络安全法》第42条规定，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，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。厘清何为法定的“技术措施和其他必要措施”是非常重要的，因为这决定了网络运营者是否在保护个人信息安全上没有履行法定的保护义务因而可能被认为存在过错。该条采取的措辞也旨在给具体的措施留白，以顺应科技的发展，由企业按照企业自身的规模以及风险大小来自行决定采取何种技术措施。除此之外，企业需要考虑按照等级保护的要求来对企业自身的信息系统进行评级定级，然后按照相关的国家标准来采取相应的技术措施。

（2）企业应当及时保存各个阶段、各个版本的合规机制，这些合规机制也是能够在后期的诉讼中证明企业的数据处理行为是合法合规的最好证据。企业应当开展数据保护影响评估（Data Protection Impact Assessment, “DPIA”），及时发现及评估数据安全方面可能的风险和影响，这在企业应对隐私诉讼时也可以成为有效的抗辩之一，因为DPIA能够说明企业已经事前尽到了一定的注意义务来保护个人信息的安全，并且在事前提前识别了处理和减少数据泄露风险的管控措施。如果企业没有在产品的设计上就考虑将个人信息保护纳入其中，那在欧洲可能还会被认为没有符合“data protection by design and by default”的要求，可能会被欧洲监管机构予以处罚[37]。

亡，其近亲属可以提起诉讼。有权提起诉讼的法人或者其他组织终止，承受其权利的法人或者其他组织可以提起诉讼。人民检察院在履行职责中发现生态环境和资源保护、食品药品安全、国有财产保护、国有土地使用权出让等领域负有监督管理职责的行政机关违法行使职权或者不作为，致使国家利益或者社会公共利益受到侵害的，应当向行政机关提出检察建议，督促其依法履行职责。行政机关不依法履行职责的，人民检察院依法向人民法院提起诉讼。”

25. 参见“最高检发布26件公益诉讼典型案例：浙江省诸暨市房地产、装修行业侵犯消费者个人信息公益诉讼案”。在该案件中，2017年9月至12月期间，陈某某、杨某、骆某某等人将非法获取的当地70多个小区近10万余条业主个人信息非法出售、转让，造成消费者个人信息泄露，侵犯公民个人隐私，案件涉及诸暨市多家房地产开发企业和装饰装修企业。该案相关责任人被追究刑事责任，但是作为信息源头的涉案房地产公司和装修装饰公司并未及时受到相应行政处罚。诸暨市人民检察院在办理陈某某等人侵犯公民个人信息案中发现本案线索，认为可能侵害社会公共利益，于2019年1月9日立案调查。经层报浙江省人民检察院批准，诸暨市人民检察院于1月15日向诸暨市市场监督管理局发出督促其依法履职的检察建议，建议该局对涉案企业依法处理，切实履行保护消费者合法权益的职责。诸暨市市场监督管理局对检察建议高度重视，分别于1月18日、3月18日对涉案企业进行立案查处，对涉案装修装饰公司作出罚款3万元的行政处罚，对涉案房地产开发公司作出罚款10万元的行政处罚。

26.《民法总则》第110条："自然人享有生命权、身体权、健康权、姓名权、肖像权、名誉权、荣誉权、隐私权、婚姻自主权等权利。"
27.《民法总则》第111条："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。"
28. 参见脚注5。 29. 参见脚注3。 30. 参见脚注2。 31. 参见脚注4。 32. 参见脚注4及脚注6。
33. 参见脚注2。 34. 参见脚注3。 35. 参见脚注2。 36. 参见脚注3。
37. https://globaldatareview.com/article/1209340/greece-telco-fine-targets-privacy-by-design-failure，最后访问于2019年10月9日。

五、境内外重大数据泄露案件及公司汇报要求解析

随着大数据和人工智能等技术的飞速发展，用户隐私已经成为了越来越重要的话题，自2005年起全球被公开的数据泄露事件已有9,106起[1]。2018以及2019年数据泄露事件频发，掌握众多用户个人信息的社交媒体、金融企业、酒店集团等往往成为数据泄露的重灾区。数据泄露的原因也是多种多样的，既可能由于黑客的网络攻击而泄露，也可能由于公司的第三方合作商或内部员工泄露所致。数据泄露事件往往会给企业带来严重的后果，既可能使企业面临执法机构的调查和处罚，也会给企业带来声誉和用户信任度的损失。

（一）境内外重大数据泄露案件

1. 境外数据泄露案件

Facebook数据泄露案件及Uber数据泄露案件无疑是近年来影响力最大的数据泄露案件。在Facebook案件中，剑桥大学心理学教授亚历山大•科甘与其背后的数据分析公司剑桥分析（Cambridge Analytica）利用Facebook平台数据共享的漏洞，获取了5000万用户的数据，并根据对这些数据的分析，针对特定用户推送竞选广告。Facebook数据泄露丑闻爆发后，在一天内股价大跌7%，市值蒸发360多亿美元。[2]尽管在事件发生之后，Facebook先后采取了在官网上发表声明、由CEO出面进行回应、在报纸上进行公开道歉、宣布终止与多家大数据企业合作、出席国会听证会等措施，[3]但Facebook对于数据泄露事件的回应仍然遭到了广泛的批评。批评者们认为Facebook回应的速度太慢，道歉流于形式，并未真正从中吸取教训。[4]最后Facebook在全球很多地方都引发了当地监管机构的调查以及许多集体诉讼，导致Facebook最后不得不重新审视隐私以及数据保护的价值，并且Facebook也在2019年后期将隐私以及数据保护作为其平台的核心价值。2016年10月，Uber遭到黑客的攻击，造成5700万名客户和司机的个人信息遭到泄露。更严重的是，在数据泄露之后，Uber并没有及时向监管部门通报，也没有发表声明告知用户和司机，而是选择“向黑恶势力低头”，试图缴纳10万美元的费用来让黑客删掉窃取的数据。此次事件发生之后被Uber掩藏了一年多时间，直到2017年11月被媒体曝光后，Uber才不得不承认。[5]此次数据泄露事件对Uber带来了严重的影响。事件发生后，美国FTC对Uber展开调查，并判定由于Uber未对储存的消费者个人数据提供合理有效的保护措施，且隐瞒了数据泄漏事件，对有关个人数据保护的事项做出了不实陈述，而要求Uber严格遵守FTC发布的裁决，实施一系列数据安全的整改措施。[6]此外，2018年9月26日，加州总检察长Xavier Becerra和旧金山地区检察官George Gascon宣布与Uber达成1.48亿美元的和解协议，以解决Uber违反数据泄露报告和数据安全法律的指控。[7]在美国之外，2018年11月，Uber还收到了来自英国和荷兰的巨额罚单，数额共计 117 万美元。其中，英国罚款 38. 5 万英镑（约49. 1 万美元），荷兰罚款 60 万欧元（约67. 9 万美元）。[8]

2. 境内数据泄露事件

2018-2019年也是境内数据泄露事件频发的一年。然而与国外数据泄露事件引起的调查及严格执法的情况相对比，我国数据泄露的执法还有待完善。根据我们的检索，在2018-2019年发生的重大数据泄露事件中，大部分事件中都未检索到有相关部门介入该事件或因该事件对相关公司或责任人执法或处罚的报道，也仅有顺丰快递 、华住酒店 等几家公司对数据泄露事件做出了及时回应和披露。

（二）欧盟、美国及中国对于数据泄露案件的汇报要求

1. 参见https://www.privacyrights.org/data-breaches，最后访问日期：2019年10月9日。
2. “Facebook数据泄露丑闻：备忘单”，2019年5月14日，https://www.techrepublic.com/article/facebook-data-privacy-scandal-a-cheat-sheet/，最后访问日期：2019年10月9日。
3. “数据泄露事件发生之后Facebook是如何回应的”，https://techcrunch.com/2018/04/10/how-facebook-has-reacted-since-the-data-misuse-scandal-broke，最后访问日期：2019年10月9日。
4. “危机应对专家称Facebook未正确处理数据泄露事件”， https://www.apnews.com/cee43df0ef044596a79ecbeea3254cd4，最后访问日期：2019年10月9日。
5. “2016年的Uber数据泄露影响了5700万乘客和司机”，https://techcrunch.com/2017/11/21/uber-data-breach-from-2016-affected-57-million-riders-and-drivers，最后访问日期：2019年10月9日。
6. In the Matter of Uber Technologies, Inc.，美国联邦贸易委员会判决。
7. “Uber将因2016年的数据泄露和隐瞒事件支付1.48亿美元”，2018年9月26日， https://www.cnbc.com/2018/09/26/uber-to-pay-148-mil-

一旦发生数据泄露事件，公司是否应当报告，应该向谁报告，报告什么内容这些问题在不同国家的法律之下有不同的要求：

1. GDPR下的数据泄露报告要求

根据GDPR第33条和第34条，在发生数据泄露事件时，企业具有向监管机构及受影响的个人汇报的义务。[11]根据GDPR规定，如果发生致个人数据遭意外或非法破坏、丢失、篡改、未授权披露或访问的事件，对公民人权及自由造成潜在风险的，[12]涉事公司必须向数据保护机构（DPA，又称为监督机构（SA））报告。[13]如GDPR声明第85条列举的，如果事件可造成个人数据失控或权益受限、歧视、身份盗窃或欺骗、经济损失、未授权逆匿名、声誉伤害、职业性秘密保护下的个人数据机密性丧失，或对涉事自然人造成其他任何重大经济或社会不利情况，公司应报告该事件。[14]未能及时向DPA通报数据泄露事件可致1千万欧元或公司全球年营业额2%的高额罚款。[15]

遭遇数据泄露的公司需在发现事件的72小时之内通报DPA。虽然法律措辞中有“在可能的情况下”这种附加说明，公司仍需对延迟汇报做出解释。如果公司无法立即提供全部所需材料，可以分阶段上报DPA，并在知悉情况后提供更多细节。[16]

公司在向DPA汇报数据泄露事件时，需要涵盖以下一系列问题：

- 数据泄露何时发生；
- 何时以及如何发现的数据泄露；
- 哪类个人数据遭泄露；
- 泄露了多少条记录，影响了多少人；
- 泄露对数据主体有哪些可能影响；
- 公司向用户提供服务的能力受到多大影响；
- 恢复时间；
- 受影响欧盟公民是否收到通知；
- 公司正在采取或将要采取的缓解及预防此类事件的措施有哪些。

除向DPA汇报之外，如果受影响个人的权利和自由面临高风险，公司应立即通知受影响个人。通知受影响个人时，公司需说明个人数据泄露的性质，并给出相关自然人缓解潜在负面影响的建议。[17]

2. 美国法下的数据泄露报告要求

数据泄露汇报在美国是非常常见的。在美国常见的数据泄露种类可以分为信用卡诈骗、黑客行为、内部人员作案、物理存储丢失、未经授权的披露等。

美国联邦法并未对公司的数据泄露报告义务做出规定，但美国50个州都颁布了各自的数据泄露汇报立法。[18]尽管具体的规定各有不同，但各州立法一般都包含以下这些内容：（1）哪些实体必须遵守法律；（2）哪些个人信息受到保护，以及如何定义数据泄露；（3）什么水平的损害程度才可以触发报告义务；（4）报告必须以何种方式和何时送达；（5）是否有例外的情况；（6）执法当局及对受影响个人的补救措施。

美国所有50个州及华盛顿特区所颁布的数据泄露报告法律都要求当泄露的信息涉及更加敏感的个人信息，例如社会保障号码及其他政府身份号码、信用卡及金融账户号码、健康和医疗信息、保险信息、税务信息等时，公司还应通知受影响的个人。在许多州法下，当数据泄露事件影响的人数超过500人时，公司还应通知征信机构。将近一半的州还要求向州检察官及/或数据相关机构的其他官员报告。

---

lion-for-2016-data-breach-and-cover-up.html，最后访问日期：2019年10月9日。

8. “Uber 因2016年的数据泄露和隐瞒事件在欧洲被罚117万美元”，2018年11月27日，https://fortune.com/2018/11/27/uber-eu-data-hack-fines，最后访问日期：2019年10月9日。

9. “顺丰3亿客户数据疑泄露，实测20条中17人为顺丰客户”，2018年9月1日，https://tech.sina.com.cn/i/2018-09-01/doc-ihinpmnr3686375.shtml，最后访问日期：2019年10月9日。

10. “华住酒店用户数据疑被泄露，回应:已报警，无法查证”，2018年8月28日，http://news.163.com/18/0828/15/DQAAT40S0001875P.html，最后访问日期：2019年10月9日。

11. 参见GDPR第33条和第34条。 12. 参见GDPR第4（12）条。 13. 参见GDPR第33条。 14. 参见GDPR声明第85条。

15. Dan Swinhoe，“如何在GDPR下汇报数据泄露”，https://www.csoonline.com/article/3383244/how-to-report-a-data-breach-under-gdpr.html，最后访问日期：2019年10月9日。

16. 参见GDPR第33条。

17. 参见GDPR第34条。

此外，美国联邦法要求在健康信息、金融机构信息、电信服务提供商持有的电信使用信息及政府机构信息泄露时进行报告。

除了向政府部门汇报数据泄露事件之外，在美国法下上市公司还可能被要求向投资者披露数据泄露事件。根据美国证监会发布的上市公司网络安全事件披露指南，如果网络安全风险或安全事件对投资者“有足够的重要性”，公司可能被要求在公司注册、财务声明、10-K表中披露这些信息。[19]

3. 中国法下的数据泄露报告要求

中国的相关法律法规中规定了网络运营者在发生网络安全事件时的报告义务。根据《网络安全法》及《电子商务法》，在发生危害网络安全的事件时，网络运营者及电商平台经营者应采取相应的补救措施，并按照规定向有关主管部门报告。[20]在发生或者可能发生个人信息泄露、毁损、丢失的情况时，除了向主管部门报告，网络运营者还具有及时告知用户的义务。[21]但上述法律法规中并未对报告的方式、报告的时间要求、报告的内容等作出具体规定。

中央网信办于2017年发布的《国家网络安全事件应急预案》（“网络安全事件预案”）对网络安全事件进行了定义[22]和分级[23]，并明确了公司的报告义务。根据网络安全事件预案，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。对于初判为特别重大、重大网络安全事件的，应立即报告国家网络安全应急办公室。[24]网络安全事件预案并未明确规定报告的内容，但《个人信息安全规范》具体阐明了报告内容包括但不限于：涉及个人信息主体的类型、数量、内容、性质等总体情况，事件可能造成的影响，已采取或将要采取的处置措施，事件处置相关人员的联系方式。[25]工信部于2017年发布的《公共互联网网络安全突发事件应急预案》（“突发事件预案”）也规定了需要上报的网络安全事件和具体上报要求。根据突发事件预案，互联网用户信息泄露事件根据泄露人数的不同被划分为特别重大、重大、较大及一般网络安全事件。[26]一旦发生网络安全突发事件，公司应当立即通过电话等方式向工信部网络安全应急办公室和相关省（自治区、直辖市）通信管理局报告，不得迟报、谎报、瞒报、漏报。[27]报告突发事件信息时，公司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。[28]除向有关机构报告之外，《网络安全法》还规定了向个人信息主体的告知义务。当个人信息泄露事件可能会给个人信息主体带来较大影响，如个人敏感信息泄露时，公司应及时将事件相关情况以邮件、信函、电话、推送通知等方式告知受影响的个人信息主体。难以逐一告知个人信息主体时，应采取合理、有效的方式发布与公众有关的警示信息。[29]

综合来看，我国需要汇报的事件的类型主要还是以网络安全事件为主，如果是未经授权的披露这类型的不涉及信息系统或者网络安全事件的数据泄露的情形，需要个案分析是否需要汇报。

（三）公司报告数据泄露事件的考量

数据泄露事件对于公司，尤其是跨国公司无疑会产生严重的影响。公司不仅会面临来自执法机关的调查和执法，还会面临公众的信任危机和舆论压力。公司在面对数据泄露事件时，首先会考虑数据泄露事件可能带来的影响和造成的危害，例如有多少人的信息被泄露了，泄露的信息中是否包含了敏感信息，泄露会对数据主体产生哪些影响等，以此判断是否属于应向监管机构汇报的数据泄露事件。公司可能会担心向监管机构汇报数据泄漏事件会使得公司面临处罚，对公司的运营和业务发展造成不利影响，并会面临公众舆论压力。但如果公司隐瞒数据泄露事件，则不利于公司采取措施减轻数据泄露

18. 参见美国各州的数据泄露报告立法清单，http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx，最后访问日期：2019年10月9日；还可参见美国各州数据泄露报告法规汇总，https://www.dwt.com/gcp/state-data-breach-statutes，最后访问日期：2019年10月9日。
19. 参见“上市公司网络安全披露指南”，美国证监会，17 CFR Parts 229 and 249，2018年2月26日。
20. 参见《网络安全法》第25条，《电子商务法》第30条。
21. 参见《网络安全法》第42条。
22.《国家网络安全事件应急预案》第1.3条：“网络安全事件是指由于人为原因、软硬件缺陷或故障、自然灾害等，对网络和信息系统或者其中的数据造成危害，对社会造成负面影响的事件，可分为有害程序事件、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。”
23.《国家网络安全事件应急预案》第1.4条：网络安全事件分为四级：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。
24. 参见《国家网络安全事件应急预案》第4.1条。
25. 参见《个人信息安全规范》第9.1（3）条。
26. 参见《公共互联网网络安全突发事件应急预案》第3条。
27. 参见《公共互联网网络安全突发事件应急预案》第4.1条。
28. 同上。

事件造成的影响。且一旦数据泄露事件之后被曝光，则公司有可能因为没有及时报告而受到监管机构的处罚，例如Democratic Coalition公司因发生了泄露事件而未履行报告义务而被匈牙利DPA处罚€35,000[30]，UAB Mister Tango因未履行报告义务而被立陶宛DPA处罚€61,500[31]，Uber因未披露数据泄露事件而在英国[32]、荷兰[33]和美国[34]分别被处以£385,000，€600,000和$148,000,000的罚金。

在数据泄露事件发生后，公司及时采取措施，应对危机显得尤其重要。进行数据泄露汇报的主要好处是可以要求政府介入协助调查并且能够借用政府的调查力量来把黑客找出来，否则企业有可能最后成为众矢之的。

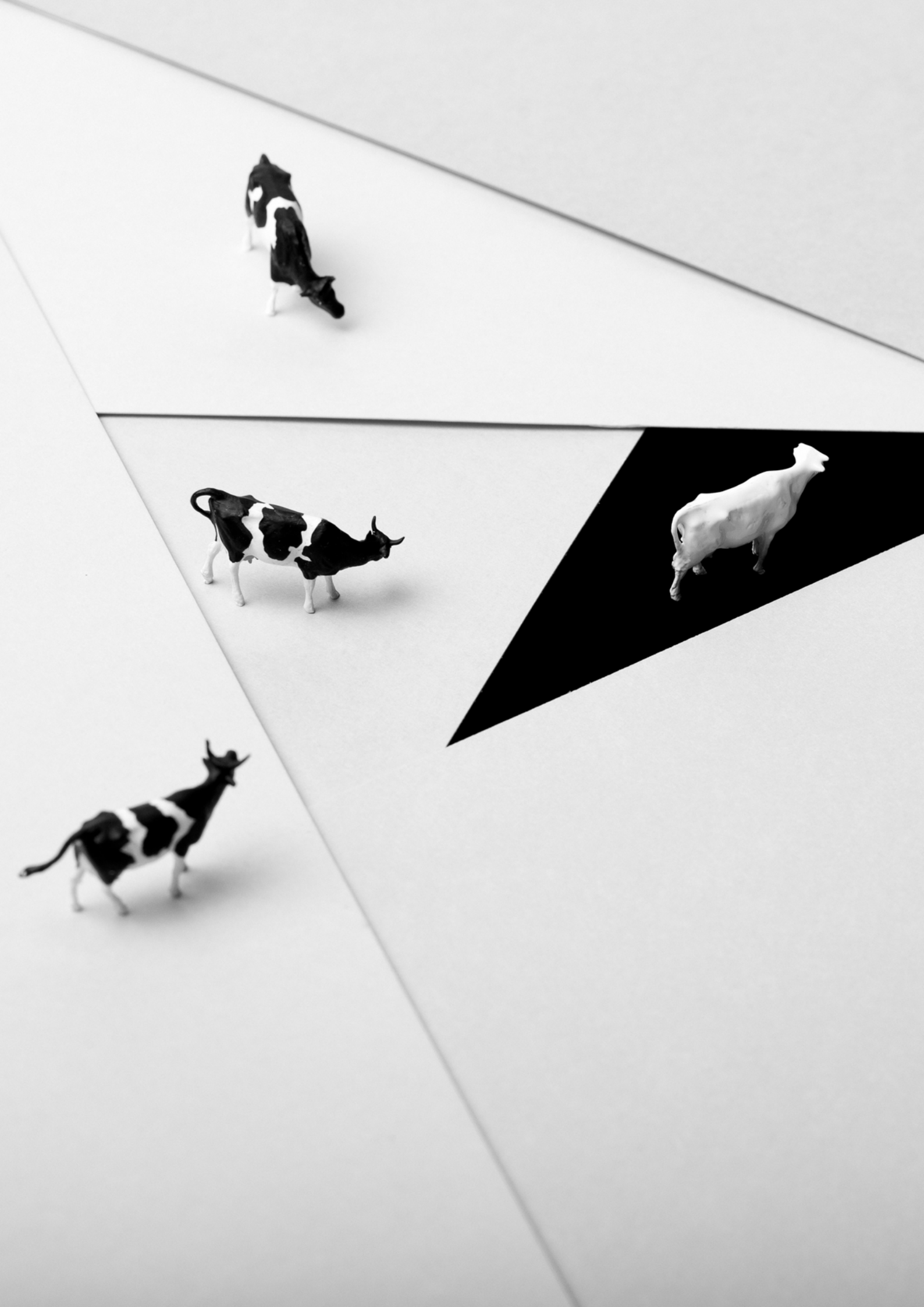
1. 由当地律师与技术咨询机构分析数据泄露是否会对受影响主体造成重大风险，判断是否属于应向监管机构汇报的数据泄露事件，并决定应当在哪些国家、向哪些监管机构进行汇报。律师的尽早介入是十分重要的，因为律师需要判断某个事件是否触发了要汇报的法律义务。然而在报与不报这个当机立断的决定上，许多企业却非常犹豫。2019年的几大数据泄露事件，例如英国航空、万豪等数据泄露案件，虽然企业已经按照法律的要求进行及时的汇报，在企业汇报之后数据泄露案件的调查结果还是招来了大额罚金。虽然有些案子最后的处罚决定尚未做出，目前尚未了解这些欧洲的监管机构例如英国的ICO对数据汇报义务的履行是否在减轻处罚的考虑中起到一定作用，但是这些巨额罚金还是让企业对这种结果感到担心，进而想要尝试凭借自己的运气来考虑是否不要进行数据泄露的汇报。但是，可以确定的是，如果对于数据泄露不进行及时的汇报，监管机构会对不汇报的违规行为进行处罚，可能最后的结果就是在没有保护好个人信息的基础上加重处罚。

2. 在规定的时间内通知数据保护监管机构以及受影响的用户，并采取补救措施，将数据泄露产生的影响降到最小。判断是否需要尽快通知受影响的用户的考虑主要有两个：（1）法律规定的必须通知受影响的用户的情形；（2）是否有些减损的补救措施需要用户自行采取行动完成。例如在系统受到未经授权的访问之后，企业如果能够对现有的用户的账号密码进行哈希或者其他加密处理，防止进一步使用，这种企业需要考虑先前的访问是否达到了数据泄露的汇报要求。如果数据是被未经授权访问之后已经被拷贝走，此时如果涉及到银行卡号等信息，企业无法为全部的用户通知其银行要求银行监控可疑交易或者是挂失，这些就是需要用户即刻进行的。

3. 积极处理好与政府机关的关系，尤其是涉及在多个国家同时展开调查时，因为许多国家之间都有互助的协议，会在调查上提供协助。例如在欧盟如果出现了大规模的数据泄露事件，这些欧盟成员国可能会同时进行调查，同时来确认哪一个国家受到的影响最大来判断主要牵头的调查机构以及协助调查机构（supervisor authorities concerned）。这些调查机构最后会对整体的调查发现进行讨论和进行统一的法律适用的解释，进而得出一个处罚结果。除此之外，欧盟、美国还有其他国家都有一些政府调查上的协助的单项协议。

4. 考虑到集团诉讼往往尾随着数据泄露事件而来，因此公司除了应对监管机构的调查，还应及时固定证据，以应对后续可能发生的集团诉讼。由于数据泄露事件往往伴随着舆论危机，公司应及时披露数据泄露情况并发布公告，表明自身在数据泄露事件中承担的责任，并积极承诺进行补救和整改。企业必须谨慎对待这些在危机中的承诺，因为国外媒体很多时候会过一段时间总结事件发生的时间线以及企业的承诺来看企业是否落实具体的工作，如果仅仅是为了平息舆论而开了大量的“空头支票”，这个时候可能会引来另一波负面的舆论影响。

29. 参见《个人信息安全规范》第9.2条，以2019年10月22日的修订版本征求意见稿为准。
30. “匈牙利SA调查Democratic Coalition的数据泄露事件”，2019年3月21日， https://edpb.europa.eu/news/national-news/2019/hungarian-sa-investigation-regarding-data-breach-democratic-coalition-dk_en，最后访问日期：2019年10月9日。
31. https://www.ada.lt/go.php/lit/Imones-atsakomybes-neisvengs--lietuvoje-skirta-zenkli-bauda-uz-bendrojo-duomenu-apsaugos-reglamento-pazeidimus-/1，最后访问日期：2019年10月9日。
32. https://ico.org.uk/media/action-weve-taken/mpns/2553890/uber-monetary-penalty-notice-26-november-2018.pdf，最后访问日期：2019年10月9日。
33. “荷兰DPA：对Uber数据泄露事件进行罚款”，https://autoriteitpersoonsgegevens.nl/en/news/dutch-dpa-fine-data-breach-uber，最后访问日期：2019年10月9日。
34. “Uber因未报告数据泄露事件而被罚款1.48亿美元”，https://www.theguardian.com/technology/2018/sep/26/uber-hack-fine-driver-data-breach，最后访问日期：2019年10月9日。



第四章

美国出口管制与经济制裁制度及对中国企业的影响

一、美国经济制裁法律体系解读

经济制裁不仅是一个政治问题，也是一个复杂但又十分重要的法律问题。说复杂，是因为这个问题交织了各国的国内法和国际法，规定繁杂，而相关的法律也经常变化更新；说其重要，是因为在过去几年中关于经济制裁的国际执法达到了一个前所未有的高度，受影响的是所有从事跨国投资和贸易的企业，避免违反经济制裁法规成为所有跨国公司，尤其是从事金融服务和贸易服务的公司的一个重大的挑战。

随着贸易战升级，中国企业必须要关注美国经济制裁制度，避免成为美国政府执法的对象。这篇文章将重点介绍美国关于经济制裁的规定，并从实务的角度出发，介绍关于违反经济制裁规定的重要执法案例，以及跨国企业如何做好经济制裁的合规工作。

（一）几个关于经济制裁的基本问题

什么是经济制裁?

经济制裁是一个国际法层面的概念，原指国家通过自助的方式实现国际法的强制性。随着实践的发展，目前经济制裁更多指的是一个国家或国际组织出于外交或是国家安全的目的，停止或限制与制裁对象的贸易和金融往来，具体的手段包括全面中止贸易、禁运特定物资（Embargo）、人员禁入以及冻结制裁对象的资产等。

1. 为什么要进行经济制裁?

最初，经济制裁的主要目的是作为一种替代战争的手段，通过与盟友一起断绝与某个国家经济上的往来，给对方施加压力，期望不通过战争能达成普通外交手段难以取得的效果。从两次世界大战直到冷战期间，这一类的经济制裁都十分普遍。中国在1949年之后也曾是西方经济制裁的对象。

冷战之后的经济制裁，更多了是为了应对世界面临的安全危机和人道主义危机，维护世界和平。例如对苏丹和塞尔维亚的制裁是为了应对当地发生的种族屠杀所引起的人道主义危机；前些年对伊朗制裁的加强是为了阻止伊朗发展核武器。

911事件也深刻的改变了经济制裁的国际格局。美国对从事恐怖主义活动，或对恐怖主义进行资助的个人、组织和国家不遗余力的展开全方位的打击，其中就包括对其实施严格的经济制裁。美国是当今世界所有国家中，对外实施经济制裁最积极、执法最严格的国家，和这也有很大的关系。

2. 美国如何运用经济制裁?

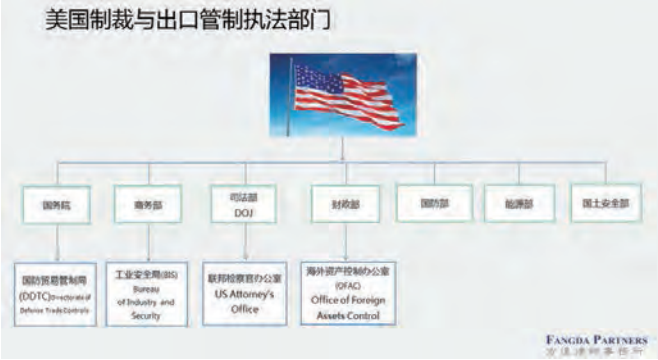
美国经济制裁的两种最主要方式是禁止贸易（Trade Prohibition）和冻结财产（Assets Block）。前者是指，美国人不得与制裁对象发生法律禁止的贸易。后者是指，美国人（主要是金融机构）要履行对制裁对象名下财产的冻结义务（不得转让、支付等）并及时向政府报告。在一些制裁项目里，美国还禁止原本不属于美国管辖的第三国与制裁对象之间的贸易，违反者要受到相应的制裁。

3. 哪些部门主管美国经济制裁?

美国执行经济制裁的主要执法机构是下设于财政部的海外资产控制办公室（Office of Foreign Assets Control，“OFAC”），它成立于朝鲜战争时期的1950年。OFAC的前身是在二战时期发挥重要作用的Office of Foreign Funds Control，该机构对德国等轴心国采取了大量经济制裁。经济制裁是美国外交

政策中的重要一环，国务院（Secretary of State）是OFAC执行经济制裁的合作机关，OFAC的很多决策必须要征求国务院的意见。

除此之外，美国商务部、美国司法部、美国联邦调查局、美国能源局、美国国防部还可能会依据不同的法律依据，对不同的方面进行经济制裁与出口管制的执法。造成这种局面的根本原因是由于美国有关制裁与出口管制的法律法规纷繁复杂，这些法律法规赋予了不同的部门进行执法的权力。但总体来说，OFAC掌管着美国经济制裁的主要职责。



4. 美国经济制裁与出口管制的关系?

简单来说，出口管制是经济制裁诸多手段的一种。出口管制作为美国政府针对特定国家实施经济制裁的手段之一，是指美国政府部门出于国家安全、反恐以及高新技术保护等目的，限制或禁止向某些特定目的地出口含有美国成分产品和技术的制度（并不都针对美国制裁对象）。出口管制主要由美国国务院、商务部工业安全局（Bureau of Industry and Security，“BIS”）具体执行，其中，美国国务院DDTC负责军用产品和技术的出口管制，美国商务部BIS负责军民两用产品和技术的出口管制。

（二）关于美国经济制裁的几个重要法律问题

1. 目前美国都有哪些制裁项目?

目前美国OFAC网站上列举了几十项制裁项目（Programs），其中一大类是以国别命名，比如伊朗制裁，另一大类是以打击目标命名，比如反恐怖主义制裁。这些项目通常被分为两种类别：全面制裁与非全面制裁。

（1）全面制裁（Comprehensive Sanction）

全面制裁是指面向特定国家或地区的全方位的制裁，禁止美国人与该国家或地区的政府、任何行业、个人、实体开展任何贸易，无论是进口、出口还是金融等等，除非获得OFAC的许可证（License）。这类制裁的对象有古巴、伊朗、朝鲜、叙利亚、克里米亚，也是目前最为严格的制裁。通俗来讲，这是一种“地毯式”制裁。

（2）非全面制裁（Non-comprehensive Sanction）

这种制裁又通常被称为选择性制裁或针对性制裁（Targeted Sanction），相对全面制裁，这种制裁更为精确。非全面性制裁可以是针对特定的行业（Sectoral Sanctions），比如俄罗斯入侵克里米亚地区之后，美国对俄罗斯实施的便是这种行业制裁，禁止美国人与俄罗斯在油气领域的贸易。也可以是针对特定的个人、实体，比如禁止美国与特定企业之间的贸易。

在非全面制裁下，不得不提的便是清单式制裁，我们不妨将其理解为一种“点对点”的制裁方式，直接精确到特定个人或实体。在诸多清单里最为重要的便是OFAC定期更新的“特别指定国民名单”或者“SDN名单”（Specially Designed Nationals

and Blocked Persons List, SDN List）。它的重要职能是打击洗钱、恐怖主义、贩毒、大规模杀伤性武器等，名单目前已有6300个左右的个人或实体。美国人不得与清单上的个人或实体开展任何贸易，而且要对他们的资产执行冻结。

值得关注的是，根据著名的“50%规则”，被名单上个人或实体直接或间接控制的企业也要受到财产冻结的处罚。这意味着，即便您的交易对象并非SDN 主体，但被SDN主体直接或间接控制，您也可能受到处罚。

2. 哪些人需要遵守美国经济制裁法律?

美国经济制裁法律适用于美国人这点毋庸置疑，该法律体系中的美国人（U.S. Persons）具体是指：美国公民、永久居民、在美国境内的任何个人或实体、在美国注册的企业及其分支机构。在一些特定的制裁项目里（如伊朗与古巴制裁项目），美国公司在海外的子公司也被视为美国人。

许多中国公司简单地相信，因为它们不是在美国注册的公司或没有美国资本参与，那么美国制裁法律就对它们不适用。这样的理解是错误的。美国的经济制裁法规具有很强的域外效力，在以下情形下，非“美国人”也要遵守美国的制裁法规：

（1）非美国人（Non U.S. person）与美国之间产生了一定的管辖因素

管辖因素也可以理解为与美国的连接点（Contact）。当前美国对非美国人进行管辖的几个常见情形有：

a. 使用了美国的金融系统。例如使用美元进行交易。

b. 违法行为发生在美国领土。

c. 违法行为里涉及美国人。比如参与、帮助、促使美国人违法。

（2）次级制裁（Secondary Sanction）

所谓次级制裁，就是非美国人与美国不存在任何管辖因素的情形下，依然要遵守美国的某些针对特定国家和特定领域的制裁法规。举例而言，特朗普政府宣布退出《伊朗核协定》之后恢复了此前的大量次级制裁，非美国人不得与伊朗的汽车行业、石油行业等发生贸易。同样是在特朗普时期，美国加强了对俄罗斯的次级制裁，禁止非美国人与俄罗斯在军事、能源领域的重要贸易。

受到次级制裁的外国企业可能受到如下处罚：被纳入SDN名单、取消美国的出口许可、禁止使用美国的金融系统（具体包含禁止在美国开设代理账户（Correspondent Account）及支付账户（Payable-through account）、禁止获得美国金融机构的贷款等等）。

3. 所谓的“帮助违反制裁规定”

对美国公司（和特定情形下的外国子公司）来说，除了自己不能从事违反制裁规定的行为，最大的担心来自于被认定为“帮助违反制裁规定”：一个不受美国制裁规定管辖的公司当然可以和美国的制裁对象来往，但这个过程中如果美国公司提供帮助，则该美国公司也会被认定违法。

这一规定的复杂首先体现在美国公司的海外子公司上。虽然在古巴和伊朗之外，美国公司的子公司原则上并不受美国制裁法规的限制，但美国公司本身很容易被OFAC认为是在协助子公司从事违反制裁法规的行为。

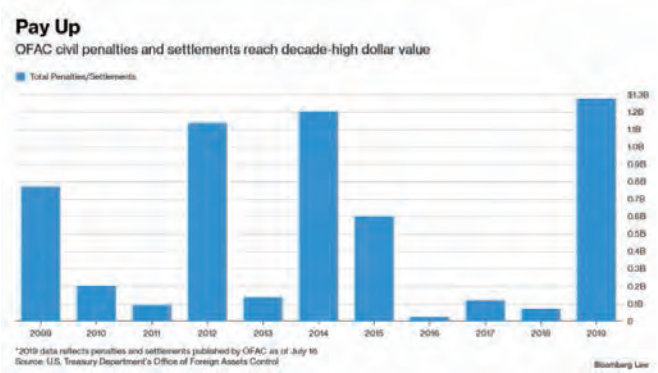
OFAC的目的是要避免母公司把子公司当做幌子，

来从事自己无法从事的交易活动。所以在这个问题上，OFAC要求美国公司的海外子公司必须要完全独立，包括商业计划、决策和具体执行方面。

（三）美国经济制裁的严厉措施

根据《国际紧急状态经济权力法》（50 U.S.C.A. 1705），美国人或者因与美国产生管辖因素的主体违反经济制裁法规的要承担相应的法律后果包括：民事上，最高赔偿金额是25万美金或违法行为涉及交易额的两倍，取更高值。刑事上，故意违反国家经济制裁法规的，判处最高100万美元的罚金，自然人还可能面临不超过20年的刑期（由美国司法部起诉）。

根据美国财政部的统计数据，2009年，OFAC执法案件数量27件，但罚金总额却高达7.7亿美元；2012年，12个执法案件带来了10亿美元的罚金。2014年法国巴黎银行一家就缴纳了89亿美元的罚金。2019年前半年，OFAC已经做出18个和解案件，作出近13亿美元的罚款，罚款金额是2018年全年的17倍。



OFAC罚款金额统计

	Company	Industry	Fine	Year
1	BNP Paribas S.A.	Financial Services	$8.96 Billion	2014
2	HSBC Bank	Financial Services	$2.29 Billion	2012
3	Commzerbank AG	Financial Services	$1.45 Billion	2015
4	ZTE Corporation	Telecommunications	$1.19 Billion	2017
5	Standard Chartered Bank	Financial Services	$967 Million	2012/2014
6	Credit Agricole Corporate and Investment Bank	Financial Services	$787 Million	2015
7	ING Bank N.V.	Financial Services	$619 Million	2012
8	Bank of Tokyo - Mitsubishi UFJ	Financial Services	$574 Million	2013/2014
9	Credit Suisse AG	Financial Services	$536 Million	2009
10	Royal Bank of Scotland (formerly ABN Amro Bank, N.V.)	Financial Services	$500 Million	2010

Includes civil penalties paid by banks to NY regulators (e.g., NYDFS, DANY)

迄今OFAC罚款金额前十名

在这些案例中，OFAC执法重点主要是跨国金融机构，尤其是总部在美国以外的国际银行。但2019年仍有诸多非美国的非金融机构被执法的案例，如德国AppliChem GmbH公司因违反古巴制裁项目而被处以5,512,564美元的罚款；Stanley Black & Decker, Inc.（史丹利百得公司）就其中国子公司江苏国强工具有限公司明显违反伊朗制裁项目被处以1,869,144美元罚款；英国石油天然气行业海底服务提供商Acteon Group Ltd.及其子公司因违反古巴制裁项目被处以227,500美元的罚款。

（四）中国企业应该如何降低美国贸易制裁的风险

与美国制裁项目有关国家开展业务的中国企业对业务的制裁风险及时进行评估，建立客户筛查系统，并通过尽职调查识别交易中直接或间接涉及的高风险客户，尤其是避免与SDN清单（及其子公司）进行交易。如企业进行并购或交易前，需加强交易前尽职调查工作。

同时，面临制裁风险的企业还应考虑建立经济制裁合规体系。2019 年5月2日，OFAC 发布了题为“OFAC合规承诺框架”（A Framework for OFAC Compliance Commitments）的指南（“OFAC框架”），为企业如何建立有效的制裁合规体系提供了指引。

OFAC框架建议所有制裁合规体系应包括五个基本组成部分：1）管理层承诺；2）风险评估；3）内部控制；4）测试和审计；5）培训。OFAC 框架明确确定了OFAC希望公司能建立一套强有力的制裁合规体系。合规体系的建立过程需考虑各种因素，包括公司的规模和复杂程度、产品和服务、客户和交易相对方，以及地理位置等。此外，OFAC重申违规行为发生时如果具有一份强有力的制裁合规体系将被视为重要的减轻情节。

二、美国出口管制法律制度及中国企业风险防范

伴随着中美之间的贸易摩擦，两国的科技博弈一直在持续。而美国通过出口管制制度对中国企业进行的限制，更是为这种博弈增添了最好的注脚。

“中兴事件”第一次让国人领路了美国出口管制制度对中国企业的巨大影响，但现在看来，这只是一个开始。2019年4月，美国商务部将中国37家机构以“不利于美国国家安全或不符合美国外交政策利益”为由加入“未经核实清单”。与清单中所列中国实体有贸易或合作关系的企业和机构将被严格审核。2019年5月，美国总统特朗普签署行政命令，宣布因为国家经济紧急状态，可禁止企业使用被视为对国家安全造成风险的外国电信设备。美国商务部随即将华为及70个附属公司增列入出口管制的“实体清单”，企业若想向华为及附属公司出口被管制的技术必须申请许可证。此禁令一出，华为遭遇空前危机，其他有关的半导体企业也都如履薄冰。2019年8月，美国商务部宣布将8家中国领先的人工智能企业放入实体清单，再一次引起国人对美国出口管制制度对中国企业影响的巨大担心。

（一）美国出口管制法律的历史

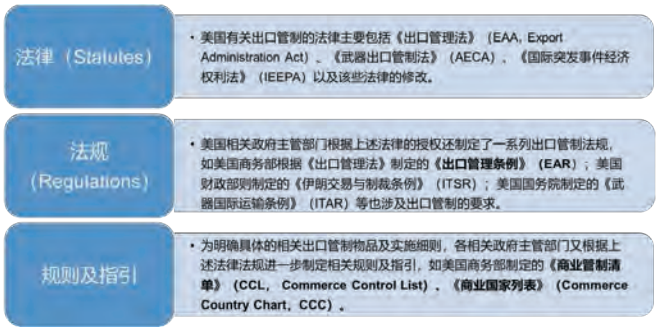
出口管制已在历史长河中存续了很长的时间，二战之后，各国家和地区政府出于政治、经济、军事等多因素的考虑，纷纷制定了出口管制政策，其中以美国的出口管制体系最为复杂且完善。

美国的出口管制制度源起于第二次世界大战之后东西方意识形态的对立，起初的目的在于通过贸易限制的方式使得东方世界无法获得某些当时处于世界领先地位的科学技术或设备，以保证美国的国家安全和世界霸主地位。1949 年 2 月 20 日，美国国会制定了美国战后

的第一部正式出口管制法律——《1949 年出口管制法》(Export Control Act of 1949)。1949年8月，商务部颁布该法令，该法令规定，除了加拿大以外，出口至世界其他国家和地区的美国商品一律需采取出口许可证制度。作为美国重要的外交工具之一，出口管制往往通过鼓励、约束或者制裁的方式来使相关主体达到美国出口管制制度下的条例和美国相关政府部门的预期。而随着世界经济的发展与融合，美国出口管制制度也一直力图在政策的变化中平衡美国经济发展与国家安全的需要。从上个世纪九十年代开始，放宽对于两用品的出口管制成为一种主流和趋势。

（二）美国出口管制法律体系的基本情况介绍

1. 美国出口管制法律体系概览



从1949年美国第一部《出口管制法》颁布以来，美国的出口管制法律体系逐渐发展，并形成了较为成熟的体系。在立法方面，宪法赋予国会制定与外国通商的立法权，总统则凭借否决权和立法倡议权与国会分享立法权。

美国的出口管制法律体系主要由两项基本法律组成：一是 1979 年制定并颁布的《出口管理法》(“EAA”)，主要针对的是两用品(dual-use)的出口管制，另一个 1976 年制定并颁布的《武器出口管制法》(“AECA”)，主要针对军事物项的出口管制。正因如此，在美国出口管制体系中，两用品和军用品会有各自独立的许可审批制度。除此之外，美国出口管制法律体系还包括美国核管制委员会和美国能源部管制核产品所参照的《原子能法》(Atomic Energy Act)和核不扩散法(Nuclear Non-Proliferation Act of 1978)等法律。

《出口管理条例》（“EAR”）是由美国商务部根据EAA制定的一部下位法，属于美国的行政法规，它是BIS的执法依据。EAR是美国有关管制军民两用产品及技术出口的最主要法规，核心内容是限制或禁止任何公司、任何人与“特定国家”或该“特定国家”的公司进行与“管制项目”相关的出口。有关EAR的主要内容，本文将在第三部分阐述。

2. 美国出口管制的最新发展——《出口管制改革法案》（ECRA）

《出口管制改革法案》（Export Control Reform Act of 2018，“ECRA”）生效于2018年8月13日，它的主要目标是进一步通过出口管制的方式限制核心技术流入特定国家，尤其是中国。ECRA最需要关注的是ECRA第1758条，它将“新兴科技（Emerging technology）”和“基础科技”（Foundational Technologies）纳入到出口管制的范畴，并授权BIS对这两项概念做出具体的定义。这一条旨在处理被美国政府认为对国家安全至关重要但未被当下出口管制法律法规所涵盖的技术。

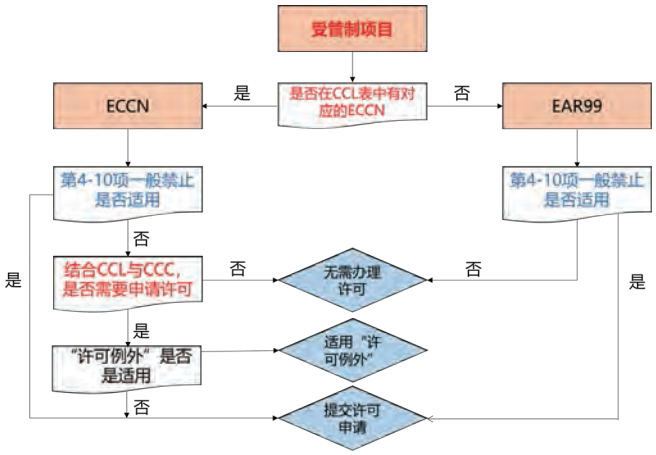
ECRA通过之后，BIS曾在2018年11月19日发布“新兴科技认定草案”并征求社会意见，其认定的新兴科技包含了人工智能（AI）、芯片、量子计算、机器人、面部和声纹技术、脑机接口等时下最为热门的14项技术领域。未来正式通过的新兴科技及基础科技清单将

对现有的CCL做出重大修改，对这些领域的出口将一律需要申请许可。留心观察便可以发些这些领域恰恰是《中国制造2025》中列名的重要行业，美国的态度不言自明。

3. 美国出口管制主管部门

军民两用品出口管制的监管主要由美国商务部下设的产业和工业安全局（Bureau of Industry and Security，“BIS”）负责，它是美国商务部的下级部门。需要注意的是，BIS并非唯一负责管理出口行为的机构， 仅是主管部门中管理范围最广泛的机构。其他出口管制主管部门还有：下设于国务院的国防贸易管制局（Directorate of Defense Trade Controls，DDTC），主要针对一些国防物品的出口管制；下设于财政部的海外资产控制办公室（Office of Foreign Assets Control，OFAC），主要通过贸易制裁的方式执行一些出口管制的事项；下设于能源部的核安全管理局（National Nuclear Security Administration），主要负责核工业的出口限制等。

（三）《美国出口管理条例》（“EAR”）的核心内容解读



1. 哪些项目属于适用EAR的“受管制项目”

作为管理“出口活动”的EAR，受其管辖的项目首先必须是在“出口活动”中被“出口”的项目；其次，在所有被“出口”的项目中，仅有部分项目属于EAR的适用范围。因此，若需了解项目是否适用EAR，需要讨论以下两个问题：（1）哪些活动被EAR认定为“出口”；（2）哪些项目属于EAR的适用范围。

（1）哪些活动被认定为“出口”？

EAR定义的出口活动较之通常意义上的出口范围更为宽泛，它不仅包括了狭义的出口，即管制项目从美国出口到另外一个国家，还包含了转出口、视同出口和转移等概念。

a. 出口（Export）：狭义的出口是指将货物、软件或技术等受管制项目实际运输或转出美国的行为，它既包括有形的实体运输（如将特定货物运输出美国），也包括无形的电子传输（如将受管控的软件与技术传输出美国）。

- 视同出口（Deemed Export）：视同出口是“出口”中的一种情况，是指将技术或软件发布（Release）或以其他方式转移（Transfer）给位于美国境内的外国人，则视为向该个人的国籍所属国的出口。例如，一家美国企业将一项美国技术卖给身在美国境内的一名朝鲜商人，这个过程就是将该美国技术视同出口到了朝鲜。

b. 转出口（Re-export）：转出口是指将受EAR管制的项目从一个外国国家运输或传送至另一个外国国家。如果美国境外的一家公司想出口或转出口原产于美国或与美国有关联的项目，那

么出口或转出口这些项目必须获得BIS的许可。换言之，转出口将美国出口管制措施“附着”在物品上，无论该物品身居何处都会受到BIS的监管。

· 视同转出口（Deemed Re-export）：视同转出口是“转出口”中的一种情况，指即使位于美国境外，将受制于EAR的技术或软件发布或转移给另一个外国国家的国民的行为。无论转移的地点是否位于美国境内，企业或个人向外籍人员发布或转移技术与软件时都应当注意是否发生了视同转出口的行为，此类行为同样受到BIS的规制。

c. 发布（Release）：技术和软件的发布包括以下三种方式：

· 非美国人通过视觉或其他观察方式获取适用EAR的技术资源；

· 非美国人通过口头或书面方式获取适用EAR的技术资源；及

· 其他任何造成适用EAR的技术资源“发布”给非美国人的行为。

d. 转移（Transfer）:是指导致最终使用者和最终用途变化的国内（非美国）转移。例如，中国的一家企业在中国境内将美国技术转让给另一家中国企业，就属于导致该技术的最终使用者和最终用途发生变化的转移活动。

（2）哪些项目属于EAR的适用范围?

对于EAR适用范围的解释，可以根据EAR的规定，从适用EAR的项目类型和不适用EAR的项目类型两方面进行解读。

a. 适用EAR的项目类型

根据EAR的规定，如果企业在从事“出口”活动中，“出口”的系以下四类项目之一的物项，则对该等物项的“出口”需适用EAR的规定，依规定如需要，则需向BIS申请出口许可证：

· 位于美国境内的物项；

· 原产自美国的物项，不论该等项目身处何地；

· 非美国原产，但价值含一定比例以上（根据成分性质和出口目的国的不同分为0%、10%和25%）美国成分的物项。其中，0%主要适用于包括高性能计算机的某些美国原产组件、某些加密软件等成分，或有特殊规定的美国原产“600系列”或“ECCN为9x515的项目”的成分；10%和25%的区别主要取决于出口目的国的不同（具体参见15 CFR § 734.4 DE MINIMIS U.S. CONTENT）；

· 直接依赖美国原产技术或软件生产的非美国制造的“直接产品”；以及在美国境外的工厂生产的产品，但该工厂或该工厂的主要部件是美国技术或软件的“直接产品”。

b. 不适用EAR的项目类型

· 出于美国国家安全及外交政策的目的考虑，由美国政府其他部门或其代理机构排他性管理的项目（如美国国防部依照ITAR管理的军用

品等）；

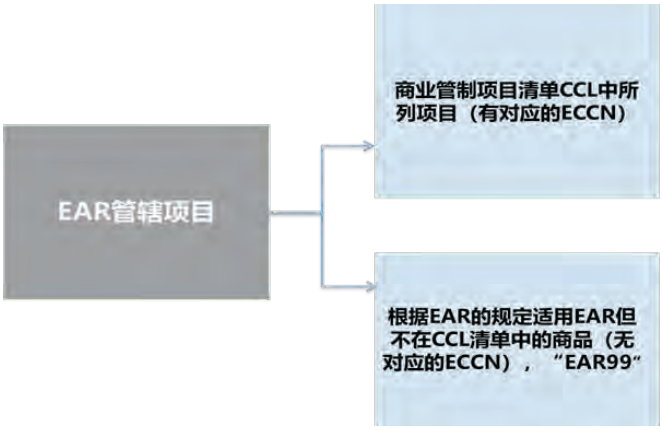
- 已经预录的书籍、报纸、地图等各类出版物；
- 已经公开发表的、或可通过基础研究获得的、或在学术机构的目录课程或相关实验室发布的信息及软件；
- 可从任何专利局获悉的已经公开的专利或者已经公开的专利申（需注意未被分类定级的专利申请拟出口或正修改及补充的专利拟出口事项由PTO (Patent and Trademark Office, 美国专利及商标局)管理）
- 非专有系统描述及部分特定遥测数据

（二）“受管制项目”的内部分类

EAR所管辖的项目可以分为两大类：

（1）ECCN：即出口管制项目分类代码（Export Control Classification Numbers），它适用于《商业管制项目清单》（Commerce Control List，CCL）中所列的项目。ECCN属于特别管制项目，需经过双重审查：在经过一般禁止的审查后，还需要根据CCL和商业国家列表（Commerce Country Chart，CCC）判断是否其受到特殊的管制。

（2）EAR99：EAR99是一个兜底性的代码，它泛指所有受到EAR管辖、但在《商品管制项目清单》没有相应ECCN的商品。EAR99的管制项目只需通过一般禁止项目的审查，一旦通过，产品一般无需许可证即可运往大部分目的地。



ECCN的功能：ECCN的功能在于确定管制项目的受管制原因。ECCN一般由五位数字及字母组成（如下图），具体而言：

- ECCN的第一位数字代表CCL中的项目大类。CCL分为以下10个大类：

（0）核材料、设施和设备及杂项类;
（1）物质、化学品、“微生物”和毒素类;
（2）材料加工类;
（3）电子产品设计开发与生产;
（4）计算机类;
（5）电信和信息安全类;
（6）激光和传感器类;
（7）导航和航空电子类;
（8）海洋类; 及
（9）航空、航天推进类。

· ECCN的第二位字母代表CCL的项目功能组。CCL有五个项目功能组：

A. 系统、设备和组件；
B.测试、检查和生产设备；
C.材料；
D.软件；及
E.技术。

· ECCN的后三位数字系产品代码，代表项目受到管制的原因。例如，000-099代表管制的原因为国家安全，100-199代表导弹技术，200-299表示核不扩散原因等。管制原因一般包括：（1）生化武器；（2）核不扩散；（3）国家安全；（4）导弹技术；（5）地区稳定；（6）武器条约；（7）犯罪控制；（8）反恐等。

3. 一般禁止的审查

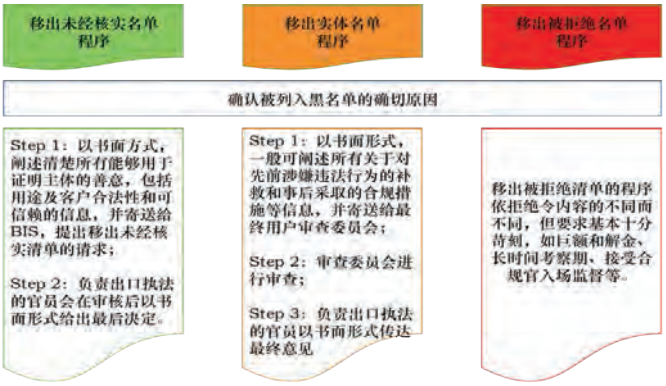
由于美国对出口管制的全面控制原则，无论是ECCN还是EAR99的项目，所有受EAR管制的项目均需先通过一般禁止第4-10项的审查，包括：（1）是否从事拒绝令（Denial Order）禁止的活动；（2）最终用户（End User）及用途（End Use）审查；（3）出口目的国审查；（4）是否支持扩散活动；（5）特定的过境转运；（6）是否违反许可证的条件、指令和条款；（7）是否在明知交易违法或即将违法的情况下仍然从事交易。其中，最为常见的是针对出口目的国、最终用户及用途的审查。

· 出口目的国：主要审查出口目的国是否为受到出口限制的禁运国家，如古巴、伊朗和叙利亚。

· 最终用途：用于特定最终用途的管制项目需申请许可证方能进行出口活动，受限制的最终用途包括：核用途、加密用途、导弹用途、生化武器用途、外国航空器和海洋核动力用途等。

· 最终使用者：除了针对国家的限制之外，美国政府部门在认为某些公司或者个人存在违反出口管制法律的行为时，也会将部分公司和个人列入黑名单。如果最终使用者为黑名单上的实体，则意味着在出口上将受到额外限制。美国财政部、国务院和商务部分别出台了各自执法领域内的出口管制黑名单，如财政部的海外资产管理办公室（OFAC）出台了特别指定国民名单、国务院的国防贸易管制局（DDTC）出台的被取消资格名单等。BIS制定并管理了三份黑名单：被拒绝名单、实体名单和未经核实名单，列入原因、影响及严重程度如下图所示。

由于被拒绝名单、实体名单和未经核实名单的严重程度不同，移出三份黑名单的程序也并不相同（如下图所示）。如果企业被列入以上黑名单，会对其日常经营活动带来不同程度的负面影响。我们建议相关企业尽快与 BIS 进行沟通、积极做好申请移出黑名单的准备工作，以尽快摆脱黑名单的影响。



4. 对于CCC和CCL的使用

对于具有ECCN的受管制项目而言，如果确认不适用第4-10项的一般禁止，那么就通过CCL和CCC两张表格确认对该项目的出口是否具有许可证的要求。而这一步骤也是大部分待出口项目在确认是否需要向BIS申请许可证时的必经之路。

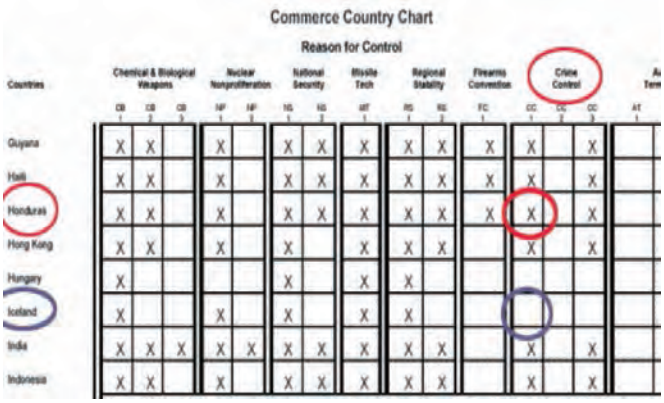
CCL，即商业项目管制清单，其中列明了受管制项目的ECCN（受管制项目分类代码）及每一个受管制项目所对应的项目理由。

Control(s)	*Country Chart (see Supp. No. 1 to part 738)*
NS applies to entire entry except 3A611.y	NS Column 1
RS applies to entire entry except 3A611.y	RS Column 1
AT applies to entire entry	AT Column 1
UN applies to entire entry except 3A611.y	See § 746.1(b) for UN controls

如上图，CCL中的表格左列代表的是受管制项目的ECCN；右边列代表的是受管制原因，如NS（National Security）代表“国家安全”。

在根据CCL明确受管制项目的受管制原因后，我们需要使用CCC确认该等项目是否需要申请办理出口许可证。

CCC，即商业国家列表，列明了出口目的地国家、每个目的地所对应的管制原因和是否需要申请办理出口许可证的结论。



如上图，CCC的横坐标为管制原因，纵坐标为目标国家。使用在CCL表中确认的受管制原因，结合拟出口项目的目的地国家，如果在横纵轴交汇的表格中为“X”，则表示需要办理许可证；如为空白，则表示无需许可证。

5. “许可例外”的适用

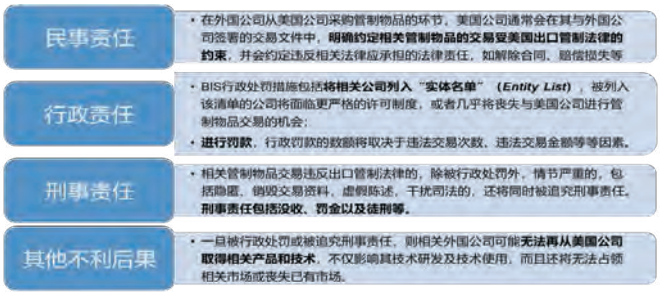
对于在通过CCC和CCL判断，初步确定需要申请出口许可证的出口项目而言，在正式申请之前，仍有一次尝试“豁免”的机会，那就是“许可例外”的适用判断。根据BIS公布的数据，2017年美国出口中国的货物当中，1.88%（24.5亿美元）是在许可证例外授权的情况下出口的。

所谓的“许可例外”，是指美国出口管制条例的一项专门制度，其目的是在不违反出口管制实现目标的情况下尽量减少出口商的负担，即如果满足一些特定条件，某些种类的物项可以不需要申请出口许可证而直接出口。“许

可例外”的种类多样，每一种类均用一个由三个英文字母组成的缩写来代表其含义，如LVS（有限价值装运）、CIV（民事最终用途）、TSR（受控的技术和软件）、ENC（加密货物、软件及技术）、STA（战略贸易授权）等等。需注意的是，缩写虽短，但要符合任何其中一项“许可例外”，都需满足复杂的条件。“出口商”必须经深入的了解和审慎的论证，包括通过向BIS咨询等方式，已确认“许可例外”的适用性。

（四）违反EAR规定的后果

对于中国企业来说，违反EAR规定可能引发民事、行政、刑事责任及其他一系列不利后果（见下图），将可能对企业造成严重的经济利益损失和商誉影响。



（五）中国企业风险防范

对于中国快速发展的科技企业来说，如何在充分利用美国先进产品、技术和软件的同时，能够规避美国出口管制的风险是一个不可回避的话题。中国企业应当：

1. 尽快在企业内部建立出口管制合规体系，涵盖产品设计、采购、生产、销售的全流程。从产品生产/进口、研发、加工、转售等各个可能触发美国出口管制的关键节点出发，增加或强化对产品的出口管制合规审查环节，使企业能够清晰明确地预见到产品在最终出口时可能需要关注的美国出口管制要求；

2. 建立对自身产品和技术中美国成分评估体系，准确识别产品中美国出口管制法下的受管控物项，并对含有受管控物项产品交易的合规风险进行评估，以避免违反美国出口管制法律规定，成为美国政府执法对象；

3. 在遇到比较复杂的问题时，积极与外部专业人士联系，借助专业力量协助企业建立完善的出口管制合规体系、做出对具体项目的风险评估并探讨具有针对性的解决方案；

4. 通过培训和内部宣传，提升关键岗位员工对出口管制法规要求的理解，提升对出口管制合规重要性的认识。

三、中国科技企业如何避开美国出口管制陷阱

2019年10月8日，美国商务部正式决定将包括28家中国实体列入出口管制“实体清单”，其中包括了8家中国顶尖的高科技企业，如大华科技、商汤科技等。这些企业未来在进口美国零硬件产品，以及与美国展开技术合作时将会受到很大的限制。自今年以来，包括华为在内的多家中国企业和研究机构被放入美国出口管制“实体清单”。美国商务部去年就一份针对新兴技术和相关产品的出口管制框架征询公众意见，提出未来对14类新兴技术加强出口管制的计划，其中包括了人工智能等多个中国计划重点发展的行业。可以预见，未来中国的高科技制造及研发企业将越来越多的直面美国出口管制法律所带来的限制和影响。因此，中国的高科技企业一定要重视美国出口管制的法律风险，并提早做好应对准备。

（一）“中国制造”与美国出口管制法

原产于中国的产品，什么时候需要遵守美国的出口管制法?

根据美国《出口管制条例》（“EAR”）的规定，如果中国制造产品中包含了“一定比例以上‘被控制的’美国成分”，那么就有可能受制于美国的出口管制法。

1. 什么是“包含了美国成分”？

根据EAR的规定，在下列情况下，非美国制造的产品/软件/科技（“非美国制造项目”）属于“包含了美国成分”。

2. 在非美国制造的产品中“合并（incorporated）了源于美国的被控制的产品”；或“包含（Bundled）了源于美国的被控制的软件”；

3. 在非美国制造的软件中“混合（Commingled）了源于美国的被控制的软件”；或

4. 在非美国制造的科技中“混合（Commingled）了源于美国的被控制的科技”。

5. 什么是“合并、包含与混和”？

“合并（Incorporate）”通常指的是在非美国制造的产品中包含了源于美国的被控制的产品/软件，且该产品/软件对非美国制造产品的正常运作至关重要，通常和非美国制造产品一同销售，以及与非美国制造产品一同转出口。

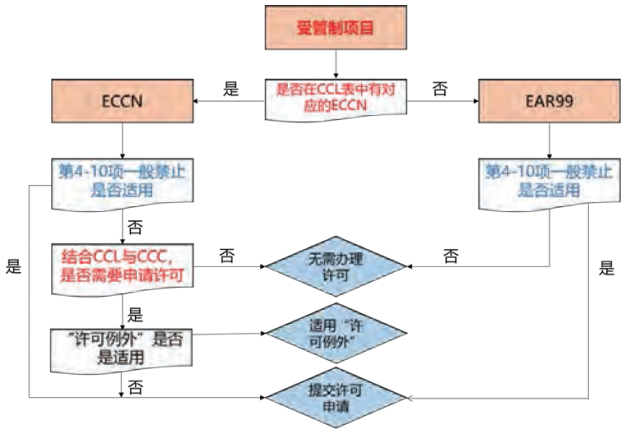
“包含（Bundle）”：是指美国软件专门为非美国制造产品所配置，并与该等产品一起转出口，但并不一定需要在物理上集成到该等产品中。但在设计和生产非美国制造的产品过程中所使用的技术、源代码等无需在“美国成分”的比例计算中被体现。

“混合（Commingle）”的范围较广，包括对美国科技进行重绘（redrawn），使用（used）或参考（consulted），以及任何基于或利用美国科技进行的技术准备和开发。

6. 什么是“被控制（Controlled）的美国成分”？

简单来说，如果一件源于美国的产品、软件或科技被单独销售至非美国制造产品最终销往的国家或地区时，需要获得美国商务部的许可证，那么这类产品、软件或科技即可被视为“被控制的美国成分”。如果中国制造的产品中“合并、包含以及混同”了这种产品、软件或科技，就需要根据其所占比例，考虑申请美国商务部的许可证。

判断一件源于美国的产品、软件或科技是否需要许可证是一个复杂的过程。原则上，是否需要许可证要结合产品的ECCN编码，结合要销售的目的地来综合判断，同时还要结合销售的对象（例如，向实体清单上的企业进行出口需要申请许可证）。限于篇幅我们这里无法完全展开介绍，我们在下面附上一个简要的判断流程图，供读者参考。建议对此有疑问的企业寻求律师的专业咨询。



在实践中，判断“被控制的美国成分”是许多中国企业觉得困惑的问题。要了解“中国制造”是否受到美国出口管制的限制，以及受到何种限制，首先要明白自己的产品中包含的美国成分是否受到限制，以及受到何种限制。一件源于美国的产品、软件或科技，出口中国没有问题，但是将源于美国的产品、软件或科技包含进中国制造的产品中，再出口至其他国家，也许就面临着限制；一件源于美国的产品、软件或科技出口给中国的A公司可能没有问题，但是包含进中国制造中，再转售给中国的B公司（例如在实体清单上的企业），也许就面临着限制。

7. “美国成分”受限制的比例?

如果“中国制造”中包含了受控制的美国成分，那么就要判断该美国成分的比例是否超过了“最低限度”。只有超过了“最低限度”，该中国制造产品才受到EAR的管辖，这就是EAR中的“最低比例规则（DE MINIMIS RULE）”。

根据美国成分的不同类型，最低比例分为0%、10%和25%三档。其中：

- 0%：即指不适用最低比例规则的特殊美国成分，只要中国制造产品中包含着这些“美国成分”，无论比例多小，都应适用EAR的规定；
- 25%：对于其他大多数国家，则一般均适用25%的最低比例。
- 10%：将非“600系列”或非“ECCN为9X515”等项目运输到伊朗、朝鲜、苏丹和叙利亚，或者将EAR99物品（食品和药品除外）运输到朝鲜和叙利亚，适用10%的判断规则。

8. 如何计算美国成分的比例?

简单来说，美国成分的比例是以其“公允市场价值”在最终产品的“公允市场价值”中所占的比例来计算的。

源于美国的“产品、软件、技术”的所谓“公允市场价值”，即其所生产的市场上的公允市场价值。大部分情况下，美国成分的公允市场价值即最终产品生产厂商获得该美国成分所付出的实际代价。最终产品的公允市场价值指在转售时，购入方在其所在市场内为获取该等产品所付出的成本。如果无法用可比较的交易来获得“公允市场价格”，则企业应当自行确定一个合适的计算方法。EAR没有给出一个标准化的计算模型，也不要求企业遵守某种特定的会计准则，而是要求企业使用的计算方法“与实际的业务实践相一致”。换言之，企业必须要确保自己的计算方法是合理且能够自圆其说，并

能够获得美国商务部的认可。

（二）什么样的行为受到美国出口管制法律的规制?

上面我们介绍了什么样的“中国制造”产品会受到美国出口管制法的规制，下面我们来介绍什么样的行为受美国出口管制法规规制。根据EAR，受管制的出口行为有六种，包括出口（Export）、转出口（Reexport）、视同出口（Deemed Export）、视同转出口（Deemed Reexport）、发布（Release）和转移（Transfer）。

出口：即将货物以运输或任何其他方式运送出美国。转出口：是指将一个受美国出口管制法规管控的产品、软件和技术，从一个美国以外的国家转移至另外一个国家的行为。

除此之外，还应当注意“视同出口（Deemed Export）”和“视同转出口（Deemed Reexport）”这两个概念。

视同出口是指，在美国境内向外国人（美国公民、美国绿卡持有者或被授予受保护人身份的人员以外的人员）发布受管制的技术或受管制的软件源代码，这种行为被视同将该管制技术或软件源代码出口到该外国人国籍所在的国或永久居住国。视同转出口：类似的，如果上述行为发生在美国境外，即为“视同转出口。”

发布：主要指的是外国人以视觉或其他查验方式获知受EAR管辖的技术或软件的源代码，以及与外国人进行口头或书面交流受EAR管制的技术或软件源代码。

转移：指的是在美国以外的同一个国家变更产品的最终用途或用户。

中国的高科技企业发展的过程中，不单只是产品“国际化”并卖向全球,越来越多的中国企业采用“全球大脑思维”，在海外设立科研和创新中心，汇聚当地的科研人员和创新资源，以实现“科研创新的全球化”。其中汇聚了顶尖科技人才的美国自然是许多企业的优先选择，例如美国硅谷就吸引了长虹、苏宁、百度等多家中国企业的海外研发中心落户。

在这一情况下，中国企业除了应关注传统的出口和转出口情形下的出口管制问题，还应当关注受管制软件和科技“视同出口”的问题，尤其是在中国企业在美国设立研发基地或实验室、与美国大学共同研发或获取高科技技术或软件源代码、中美技术研发团队进行各种形式的技术交流的过程中，如果涉及将受制于EAR的软件源代码或技术披露、提供给中国公司或中方员工（包括参观美国的实验室、交流技术问题和研发成果等场景），则有可能会引发出口管制的法律风险。有关主体从而需根据EAR的要求判断是否需要在交流活动前申请许可证，否则可能产生违反美国出口管制法的风险。

例如，2016年4月，美国司法部指控美籍公民何某与中国某核能公司在未获得美国商务部有关许可的情况下，何某某在过去十余年间，多次帮助安排美方专家与该核能公司之间进行技术交流，在美国境外非法实施和参与特殊核材料的研发和生产。何某最终因违反美国出口管制法被判入狱24个月；2005年9月，位于美国加州的Maxim Integrated Products, Inc.在未获得美国商务部有关许可的情况下，将ECCN代码为3A001的集成电路元件开发相关技术指示提供给了该公司的中国员工，从而受到了美国政府的调查，并最终支付了192,000美元的罚款达成和解。

（三）中国高科技企业应当如何应对美国出口管制法

中国科技制造企业为应对美国出口管制法律风险，

应当考虑尽快实施以下措施：

1. 如果主要产品中包含了源于美国的产品、软件和技术，则应当尽快对该产品是否受制于美国出口管制法规进行判断。这样的判断应当在专业律师的帮助下，结合产品的特点、构成、成本结构等因素而综合做出。

通过这样的判断，企业应当明确产品是否受到美国出口管制法规的规制，以及受到何种限制，如在何种情况下需要申请许可证，何种情况下不能出口等，并作出正确的应对。同时，应当建立客户筛查机制，筛查交易相对方是否所在被美国政府列入黑名单，并要结合产品和技术的识别结果，对照其最终销售国和最终用户进行风险分析。

需要特别注意的是，企业应当对计算和判断的过程充分的进行记录，并保留文档。日后若面临美国执法机构的询问或调查，如果企业能够提供完整的记录证明其计算和分析过程，且分析结果合理，将大大降低企业被处罚的风险。

2. 在海外设立研发中心，或与海外研发机构有密切合作和交流的中国企业，应当就其研发模式中的出口管制风险进行评估，判断是否可能出现“视同出口”的情形，并根据风险等级制定相应的行为指引，避免违反美国出口管制法规。

3. 更重要的是，中国企业应当考虑尽快制定完善的出口管制合规体系。企业的出口管制合规应当是一个贯穿研发、设计、采购、生产、销售等全流程的一套机制，能够系统性的发现、防范、降低出口管制的风险。

好的出口管制体系，不但是企业在应对美国政府调查执法时一个重要的抗辩，另外，也能使企业各部门、各环节的出口管制合规成为一个有机的整体，极大的降低美国成分比例评估以及客户风险排查等合规工作的操作难度。

例如，就成分评估这一工作而言，相较于上面的介绍，实践中的情况往往较为复杂。许多高科技的“中国制造”产品中既有源于美国的零部件，还使用了源于美国的软件。许多产品所运用的科技有可能是中美研发团队共同开发的结果，产品含有的美国部件、软件和技术是否属于“受控制的美国成分”，还需要向上游厂商追根朔源地了解。因此，如果不在设计和采购阶段就做好产品成分的分析和计算，面对项目压力，企业的法务合规部门很难在短时间内对产品的有效成分进行有效评估。

四、美国对华为出口管制最新动态及中国企业如何应对

2019年8月19日，美国商务部宣布将46家华为关联公司加入商务部的出口管制实体清单（Entity List）中。这是今年5月16日美国宣布将华为及其68家关联公司加入实体清单后，再次大规模的将华为实体纳入限制出口的名单中。与此同时，美国商务部宣布将此前向华为核发有效期限为90日的临时通用许可再延长90天，并对该临时通用许可的许可范围做出了进一步阐述和修改。这一举动在全世界引起了广泛关注，再次牵动了关注中美贸易战的人们敏感的神经。

自美国政府今年5月16日宣布将华为加入实体清单后，美国对华为的出口管制一直是全世界的关注焦点。美国总统特朗普在6月底的G20峰会记者会上曾做出“可以允许美国公司继续向华为供货”的表态，放松对华为的出口管制似乎一度出现希望，但8月19日美国商务部做出的这一最新决定，再次显示了美国对华为出口管制措施的复杂性和长期性。

（一）美国对华为出口管制的大事记

时间	事项
5 月 16 日	美国商务部宣布将 68 家华为实体加入商务部实体清单。所有向华为实体出口、再出口及移转货品交易均需依《出口管理条例》(Export Administration Regulations，“EAR”）向美国商务部申请获得出口许可证。
5 月 20 日	美国商务部向华为实体核发有效期限为 90 日之临时通用许可（Temporary General License，TGL)。临时通用许可在以下范围内向华为出口美国产品： （1）用于继续运营华为现有的网络和设备，包括对软件的更新与维护； （2）对华为现有手机的持续支持，包含软件更新与维护； （3）网络安全研究和漏洞公布；以及 （4）对 5G 标准的发展进行必要的参与。
6 月 29 日	美国总统特朗普在 G20 峰会记者会上做出了可以允许美国公司继续向华为供货的表态。
6 月 29 日	美国参议院民主党党团领袖舒默在特朗普做出最新有关华为的表态后，发出警告称美国不应该在贸易争端的谈判中就华为的问题做出让步。美国共和党参议员鲁比奥也在同一天说，如果特朗普解除了华为的限制，他将犯下大错，美国国会需要通过立法来恢复对华为的限制措施。
6 月 30 日	白宫首席经济顾问库德洛(Larry Kudlow)接受媒体采访时，对于特朗普针对华为的表现出的立场软化进行补充，称这不是大赦，且表示政府十分清楚华为隐藏的安全风险。
7 月 9 日	美国商务部长罗斯称，为了执行两周前总统在 G20 峰会上的指示，美国政府将在不会对国家安全构成威胁的情况下向寻求对华为销售产品的公司发放许可证，但罗斯强调此举并不意味着将华为移除实体清单。对于向华为出口产品的审查仍然使用严格的许可证制度，并采取“推定否认”（presumption denial）的消极态度。
7 月 24 日	根据路透社的报道，美国商务部长罗斯已经收到了 50 多份向华为供货的许可证申请。截至当时，美国商务部未向任何主体颁发许可证。
8 月 7 日	负责政府合同的美国机构发布了一项禁止联邦从包括华为在内的五家中国公司购买电信设备的临时规定，并禁止与华为有业务往来的公司向美国政府提供服务。
8 月 18 日	特朗普重申，他认为华为构成安全风险。他说：“出于国家安全考虑，我们最终不想与华为做生意。”
8 月 19 日	美国商务部宣布将该临时通用许可的生效期延长 90 天并公布官方文件

（二）近期内美国政府放松对华为出口管制的可能性很小

特朗普在G20峰会时释放了放松对华为出口管制的信号，使得许多业务受华为出口禁令影响的企业，以及同样受到美国出口管制措施影响的其他中国企业一度对形势感到乐观，期待美国对华为乃至其他中国科技企业的出口限制会逐渐放松。然而综合来看，我们认为近期内美国政府放松对华为出口管制限制措施的可能性较小。

首先，特朗普在G20峰会时的表态并未实际落实。特朗普在G20峰会上释放出立场软化的信号后在国内受到了广泛批评，随后他本人以及白宫官员在各种场合都在强调对华为的出口限制不会放松。白宫也并没有推出任何实质性的措施来落实特朗普的表态。

其次，美国政府仍然严格限制对向华为出口管制的许可。华为被放入实体清单后，任何人要向华为出口、再出口及移转管制物项的交易，原则上需要根据《美国出口管制条例》向美国商务部申请特定的“许可证”才

能进行交易。如前所述，美国商务部长罗斯表示对华为的出口仍将采用严格的许可证制度，同时对华为销售产品发放许可证将采取一贯的“推定否认”的立场。

结合8月19日又有46家华为关联公司被放入实体清单的事实，美国政府对华为继续高压封锁的态度不言自明。

（三）美国政府对华为的“临时通用许可”：并非手下留情

除了与上述单项交易需申请的许可证以外，美国商务部在5月20日向华为颁布了“临时通用许可”，允许华为在90天内在有限的范围内继续从美国采购部件及向美国客户提供服务而无需额外申请许可，8月19日商务部将此“临时通用许可”再次延长90天。这使得有些人误认为美国对华为的出口限制有所放松，“手下留情”。这一理解是不准确的。

首先，上述临时通用许可的适用范围有限。美国商务部于2019年5月20日核发的临时通用许可（Temporary General License, TGL），其范围仅包含：

- 用于继续运营华为现有的网络和设备，包含软件更新与维护；
- 对华为现有手机的持续支持，包含软件更新与维护；
- 网络安全研究和漏洞公布；以及
- 对5G标准的发展进行必要的参与。

很明显的，上述临时通用许可主要是允许华为购买美国管制物项以维护现有的网络，或给现有的华为手机提供软件更新。但在未获批准的情况下，华为仍被禁止购买美国管制物项来生产新产品。

更重要的是，根据美国商务部的解释，发布及延长临时通用许可的目的主要为保障美国公司与美国消费者的利益，而非为放松对华为的限制。美国政府将继续在临时许可的有效期限内敦促美国主体找到华为的替代品，以尽可能避免技术中断。换言之，这一“临时通用许可”的目的不是为了放松对华为的限制，而是为了最大程度减少出口管制措施对美国使用者造成的影响。

“临时通用许可”的最新修改：

2019年8月19日，美国商务部延长了上述临时通用许可的有效期，并在原临时通用许可的内容上做如下改动和澄清：

- 将临时通用许可有效期延长至2019年11月18日；
- 对于临时通用许可下的许可范围作了进一步说明以提升公众的理解程度，并做出了部分修改，如对第一条中“现有网络和设备之维持”，明确限定终端设备或与维护现有网络和设备无直接联系的设备不在该许可范围中；再如对第二条“对现有手机之支持”中的手机做扩大至“个人消费电子设备”，包括手机、平板电脑、智能手表、移动热点以及类似的个人设备；
- 5月颁发的临时通用许可仅要求与华为进行交易的主体准备“认证声明”。8月19日发布的官方文件对时间点和责任主体做了进一步的明确：规定出口商、再出口商或转让人在依据临时许可开展与华为贸易前，需先从华为处获得“认证声明”。

因此，将“临时通用许可”理解为美国放松或推迟对华为的出口管制是不准确的。在中美贸易谈判长期无重大突破的情形下，可预见美国对华为施加的出口管制措施不会在短期内放松。

（四）中国企业应当如何应对

美国对华为的出口管制措施，不仅极大的限制了华为进口美国产品及使用美国技术，同时对于与华为展开技术合作或有商业往来的其他企业都造成了很大的影响，这里面不仅包括美国企业，也包括许多中国企业。

根据《出口管制条例》的规定，如果一家中国企业向华为再出口、国内转移、转售以下EAR管制物项，都需要向美国商务部申请许可证。如果没有申请许可证而擅自向华为再出口、国内转移、转售，可能会被认定为违规，并面临美国出口管制法律下的严厉处罚：

- 位于美国境内的物项；
- 原产自美国的物项，不论该等项目身处何地；
- 非美国原产，但价值含一定比例以上（根据成分性质和出口目的国的不同分为0%、10%和25%）美国成分的物项。其中，0%主要适用于包括高性能计算机的某些美国原产组件、某些加密软件等成分，或有特殊规定的美国原产“600系列”或“ECCN为9x515的项目”的成分；10%和25%的区别主要取决于出口目的国的不同（具体参见15 CFR § 734.4 DE MINIMIS U.S. CONTENT）；
- 指直接依赖美国原产技术或软件生产的非美国制造的“直接产品”，或是通过直接依赖美国技术或软件所制造的产品或主要产品组件生产的非美国制造的“直接产品”。

基于以上的情形，为了避免违反美国出口管制法规的风险，我们建议中国的科技制造企业，尤其是产品中含有美国技术和成分的企业：

- 建立自身产品和技术的美国成分评估体系，准确识别产品中美国出口管制法下的受管控物项，并对含有受管控物项产品交易的合规风险进行评估，以避免违反美国出口管制法律规定，成为美国政府执法对象。
- 建立出口管制合规体系，建立涵盖产品设计、采购、生产、销售全流程出口管制合规风险的管控体系。
- 通过培训和内部宣传，提升关键岗位员工对出口管制法规要求的理解，提升对出口管制合规重要性的认识。

第五章

刑事合规热点分析及如何应对刑事调查

在企业面临的合规风险中，刑事风险无疑是违法后果最为严重，惩罚力度最强的风险类型，不仅关系到企业能否正常运营，甚至直接关乎企业管理人员及员工的人身自由。刑事合规是一个涉及风险防控、应急处理等多层次内容的系统工程，主要包含一般刑事合规、特定问题合规以及刑事调查应对等方面工作。实践中，不同类型企业面临的刑事合规风险点也会有所不同，企业需要结合自身行业特点，有针对性的开展合规计划制定、合规风险排查、合规调查应对等工作。我们在下文将对2018年-2019年度刑事合规热点问题进行梳理，挖掘热点背后可能涉及的刑事罪名，并就企业应对刑事调查提出一般性的应对方案。

一、2018-2019年度刑事合规热点概览

■ 刑事合规热点一：环保合规

2019年2月，最高人民检察院召开新闻发布会，发布“两高三部”《关于办理环境污染刑事案件有关问题座谈会纪要》。最高人民法院、最高人民检察院先后于2013年、2016年就环境污染犯罪出台专门司法解释，对如何具体把握相关犯罪定罪量刑标准等问题作了全面、系统的规定。此次，最高人民法院、最高人民检察院、公安部、司法部、生态环境部联合发布《关于办理环境污染刑事案件有关问题座谈会纪要》，对办理环境污染刑事案件中的有关问题作出进一步明确，体现了行政、司法机关对环境保护工作高度重视。可以预见，在未来一段时期，各级执法机关将不断加大办理环境污染刑事案件的工作力度，环境污染类刑事案件数量也将持续增多。

■ 刑事合规热点二：网络安全与数据保护合规

2019年各级行政、司法机关在网络安全与数据保护监管领域重拳出击、力度空前。年初，公安部召开“净网2019”专项行动部署会，部署开展“净网2019”专项行动，提出要继续依法严厉打击侵犯公民个人信息、黑客攻击破坏等突出网络违法犯罪。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。2019年9月，网络安全执法力度不断增强，国内多家大数据公司遭公安机关调查，公司管理人员被警方带走协助调查。据悉，部分知名大数据公司主动停止了相关“爬虫”业务，整个大数据行业如履薄冰。2019年10月，为依法惩治拒不履行信息网络安全管理义务、非法利用信息网络、帮助信息网络犯罪活动等犯罪，维护正常网络秩序，两高发布《关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》，进一步明确相关网络犯罪的定罪量刑标准和相关法律适用问题。根据北京市公安局通报的专项行动信息，该局仅在第一季度便破获各类涉网案件2000余起，抓获涉案嫌疑人2200余名，清理网上各类违法信息91万余条，对互联网企业开展监督检查5400余家次，行政查处违法违规企业2300余家次，关停违规账号36万余个，完成安全评估2000余家次，清理下架了移动APP应用商店的未实名应用18.9万余个、下架违法应用2万余个、关停违法应用4800余个，约谈部分移动应用APP平台负责人26人次。[1]

■ 刑事合规热点三：金融外汇合规

2019年,最高人民法院、最高人民检察院联合发布《关于办理非法从事资金支付结算业务、非法买卖外汇刑事案件适用法律若干问题的解释》。《解释》进一步明确了非法从事资金支付结算业务、非法买卖外汇的行为认定依据，以及“情节严重”、“情节特别严重”的认定标准；非法经营罪、洗钱罪、帮助恐怖活动罪的竞合处罚原则；非法经营数额、违法所得数额的认定标准、处罚原则及判处罚金的标准；单位犯罪的定罪量刑标准；从宽处罚的认定条件和标准；非法从事资金支付结算业

1. 北京“净网2019”专项行动取得阶段性成效，http://www.cac.gov.cn/2019-04/24/c_1124409796.htm，最后访问时间2019年11月18日。

务、非法买卖外汇刑事案件犯罪地的认定等一系列问题。在当前对外汇买卖实行严格管制的背景下，企业或个人在国家规定的交易场所以外非法买卖外汇将面临巨大的违规风险。

■ 刑事合规热点四：反商业贿赂合规

2019年1月，中央纪委书记赵乐际在十九届中央纪委三次全会作工作报告时再次强调要“坚持无禁区、全覆盖、零容忍，坚持重遏制、强高压、长震慑，坚持受贿行贿一起查”。早在十九大报告中就出现了‘坚持受贿行贿一起查’的表述，习近平总书记在十九届中央纪委二次全会上再次强调要“坚持受贿行贿一起查”。在过去一段时期内，司法实践中一定程度上存在“重查受贿、轻办行贿”的现象。未来，随着反腐败工作不断推进，对行贿行为同样予以打击或将逐渐成为一种执法常态，防范贿赂违规问题应当引起企业及高级管理人员的高度重视。

■ 刑事合规热点五：证券、期货合规

2019年6月28日，最高人民法院、最高人民检察院发布《关于办理操纵证券、期货市场刑事案件适用法律若干问题的解释》、《关于办理利用未公开信息交易刑事案件适用法律若干问题的解释》，对操纵证券、期货市场、利用未公开信息交易的定罪量刑标准和法律适用等问题做出进一步的规范。随着证券、期货市场的快速发展，内幕交易、泄露内幕信息、利用未公开信息交易、操纵证券、期货市场犯罪不断发生。据最高人民法院相关人员透漏，近四年来人民法院一审受理操纵证券、期货市场、利用未公开信息交易刑事案件112件。特别是2015年股市异常波动以来，重大操纵证券、期货市场犯罪案件以及利用未公开信息交易犯罪案件（俗称“老鼠仓”）不断增加，手段、方式方法更加隐蔽、多样，操纵证券、期货市场犯罪规模化、公司化趋势明显，利用未公开信息交易犯罪案件涉案金额不断增大。《解释》划定了刑法条文中提及的相关概念的认定范围，明确了犯罪立案追诉标准，为执法办案人员提供了清晰的执法依据。未来，行政、司法机关将不断加大对操纵证券、期货市场、利用未公开信息交易犯罪的惩处力度。

二、刑事合规热点问题涉及的相关罪名解读

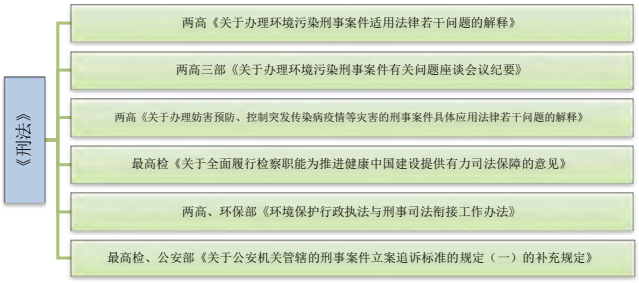
（一）污染环境罪

污染环境罪是企业在环境保护领域违规涉案的“重灾区”,在生产经营中较为频发。如何有效规避环境污染刑事风险已经成为特定类型企业不可忽视的重要问题。据最高人民法院研究室周加海副主任介绍，近年来，人民法院审理的环境污染刑事案件数量大幅增长。以《2013年解释》发布为分界点，之前人民法院审理的污染环境刑事案件年均仅二三十件，而之后的年均案件量达到一千三百余件。特别是，《2016年解释》发布后，人民法院审理的污染环境刑事案件量继续增长，年均超过二千件。据统计，2017年、2018年人民法院新收污染环境刑事案件2344件、2409件，审结2258件、2204件。

1. 法制沿革

2019年2月20日，最高人民检察院召开新闻发布会，发布“两高三部”《关于办理环境污染刑事案件有关问题座谈会纪要》（下称“《纪要》”）。“两高”曾先后于2013年、2016年就环境污染犯罪出台专门司法解

释，对如何具体把握相关犯罪定罪量刑标准等问题作了全面、系统的规定。此次，最高人民法院、最高人民检察院、公安部、司法部、生态环境部联合发布《纪要》，对办理环境污染刑事案件中的疑难问题形成统一的认识。可以预见，在未来一段时期，各级行政、司法机关将不断加大办理环境污染刑事案件的工作力度，企业涉及环境污染类刑事案件数量也将持续增加。与该罪名相关且现有有效的刑事领域法律法规、司法解释等文件归纳整理如下：

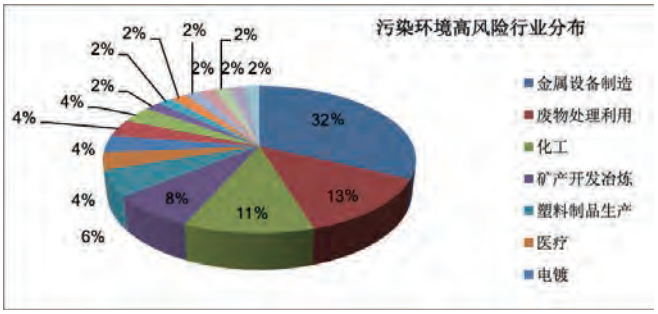


2. 案件特点

我们收集、整理了从2018年1月1日至2019年6月30日已公开的企业触犯污染环境罪的生效判决，共收集到50个单位犯罪的案例，其中，包含2019年2月最高人民检察院等部门召开新闻发布会发布的4起单位涉及污染环境刑事案件典型案例。希望通过分析既往案例，总结企业涉及污染环境犯罪的特点，为相关企业防控环境污染入罪风险提供参考。

■ 金属设备制造、化工、矿产开发等行业属高风险行业

针对搜集的53家涉案企业（部分案件属于多个企业共同涉案，因此统计的企业数目高于案件数）按照所属的行业领域进行分类，发现污染环境犯罪易发、频发的行业相对比较集中。

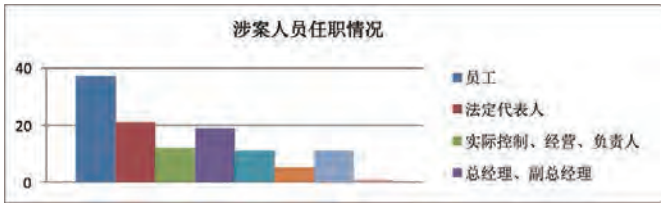


*需要说明的是，对行业领域的分类主要依据企业的营业范围进行划分，部分判决书未明确标注涉案企业的营业范围或者存在一家企业有多个营业项目的，通过查询企业公开信息以及其涉案的主要因素来划定其所属行业

统计结果显示，金属设备制造（占比32%）、废物处理利用（占比13%）、化工（占比11%）、矿产开发冶炼（占比8%）、塑料制品生产（占比6%）等行业是污染环境犯罪的高风险行业。从企业特点上来看，废物处理利用企业由于本身从事废物的回收处理、循环利用业务，在生产实践中单个操作环节出现问题极易导致环境污染问题，进而触犯该罪名，遭受刑罚处理。其他企业则多属于在生产经营过程中可能会产生含铅、汞、铬、铜等重金属元素的废水、废物或者其他类型废物，生产人员在处置过程的不规范操作容易导致严重环境污染问题。

■ 企业管理人员被判刑罚比例高

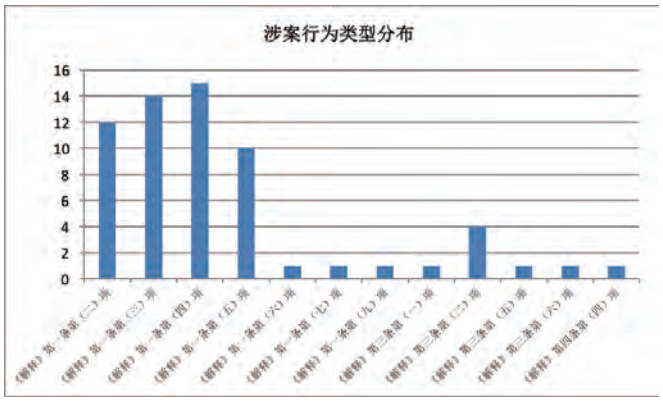
我国刑法对单位犯罪实行双罚制，即对单位判处罚金，对直接负责的主管人员和其他直接责任人员判处刑罚。在统计已生效判例中，共有117名涉案人员被依法追究刑事责任，其中，企业管理人员80名，约占涉案人数的70%，一般员工37名，约占涉案人员的30%。另外，我们针对管理人员的具体任职情况作了细化统计，其中，法定代表人21人，总经理、副总经理19人，企业实际经营、负责人12人，股东11人，厂长、矿长5人，党支部书记1人，中层管理人员、车间主任等11人。



司法实践中，一旦认定涉案企业的行为为单位犯罪，在单位内起到批准、授意、决定、指挥等作用的管理人员往往会被追究刑责。在一些案例中，主管人员的默许行为同样被认定为主观明知，作入罪处理。当然，并不是所有的股东、高级管理人员均会因为企业涉案而被追究刑责，对于并未参与企业实际生产经营的管理人员，由于其无实施犯罪的主观目的及客观行为，因此一般不会将此类人员认定为直接负责的主管人员和其他直接责任人员。

■ 污染环境的违法行为类型多样

《2016年解释》全面系统的规定了污染环境等罪名的定罪量刑标准。近两年法院审理污染环境罪适用的入罪处罚标准基本是依照《2016年解释》的规定来掌握的。我们对单位及其相关人员主要的涉案行为进行了归纳梳理，详见表格。



*需要说明的是，统计中发现有的案件具有数个犯罪行为，也有“典型案例”未能查找到公开判决文书，无法对具体犯罪行为进行统计核实

通过以上统计表格不难看出，企业违反国家规定，排放、倾倒或者处置有放射性的废物、含传染病病原体的废物、有毒物质或者其他有害物质，最常见的被处罚原因为《2016年解释》第一条第（二）至（五）项规定的四种行为：

(二) 非法排放、倾倒、处置危险废物三吨以上的;

(三) 排放、倾倒、处置含铅、汞、镉、铬、砷、铊、锑的污染物,超过国家或者地方污染物排放标准三倍以上的;

(四) 排放、倾倒、处置含镍、铜、锌、银、钒、锰、钴的污染物,超过国家或者地方污染物排放标准十倍以上的;

(五) 通过暗管、渗井、渗坑、裂隙、溶洞、灌注等逃避监管的方式排放、倾倒、处置有放射性的废物、含传染病病原体的废物、有毒物质的;

除此之外，《2016年解释》第三条第（二）项“非法排放、倾倒、处置危险废物一百吨以上的”的情形也较为常见，这是有关“后果特别严重”的规定，所对应的刑期为“三年以上七年以下有期徒刑，并处罚金。”此外，对于具有危险废物经营许可证的企业来说，其实施上述违法行为属于法定的从重处罚情节，需要引起关注。

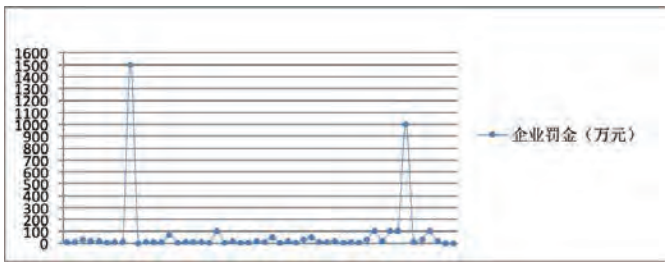
■ 发案线索绝大部分来自于行政执法

除极个别刑事案件立案线索来自于举报之外，绝大多数污染环境刑事案件线索来自于环境行政执法部门的移送，行政执法是刑事立案最主要的线索来源，这也提醒企业重视环保部门日常行政执法工作的重要性。企业重视行政执法工作的意义还不仅限于此，企业2年内曾因违反国家规定,排放、倾倒、处置有放射性的废物、含传染病病原体的废物、有毒物质受过2次以上行政处罚,又实施前列行为的，也将作入罪处理，再次凸显了企业高度重视行政执法工作

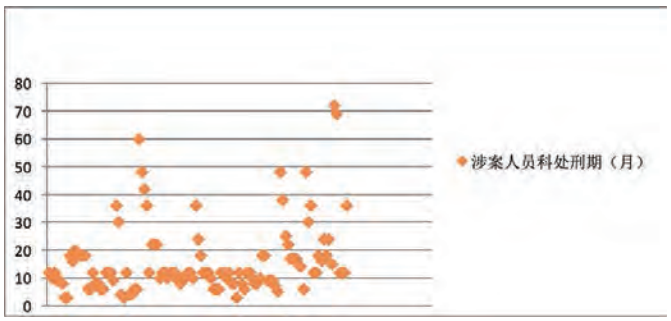
的重要意义。

■ 单位被判处罚金刑跨度大，涉案人员具备适用缓刑的空间

刑法对于污染环境罪没有明确规定罚金数额标准。经统计检索到的已生效判例，针对企业判处的最高罚金为人民币1500万元，最低罚金为4000元，幅度跨度较大，多数判决罚金金额主要集中在人民币10万元至50万元间。法院一般会根据犯罪情节，如违法所得数额、造成损失的大小等，并综合考虑犯罪分子缴纳罚金的能力，依法判处罚金。统计的案例中，被判处最高罚金人民币1500万元的涉案企业，是在生产经营中排放含重金属铊元素的废水至长江上游某重要支流，污染环境，致使下游某城区集中式饮用水水源取水中断十几个小时，后果特别严重。因此，法院在认定时结合犯罪情节确定了相对较高的罚金数额。



针对涉案直接负责的主管人员和其他直接责任人员的刑事处罚同样跨度比较大，其中最高刑期为有期徒刑六年，最低刑期为拘役三个月，平均刑期约为16个月。



刑事案件不尽相同，单个案件在主观恶性、犯罪情节、社会危害等方面均具有特殊性，根据罪责刑相适应原则，法官会针对涉案企业及人员的主客观方面的表现对其科处相应的刑罚。当然，作为同类案件除了具备个体差异外也自然存有一定的共通之处，我们在梳理案件过程中发现该类型案件在科处刑罚时具备适用缓刑的空间。经统计，在涉案的117名人员当中，共有59名涉案人员被宣告适用缓刑，占比约为50%。通过对既往判例的分析总结，一般认为犯罪嫌疑人情节轻微，且在满足以下条件的情形下具有适用缓刑的可能：①如实供述罪行；②赔偿损失，积极开展生态恢复，降低社会危害；③共同犯罪中的从犯；④系初犯，未曾因环境污染违法行为受过行政处罚。人民法院对判处缓刑的被告人，一般还会同时宣告禁止令，禁止在缓刑考验期内从事与排污或者处置危险废物有关的经营活动。生态环境部门根据禁止令，对上述人员担任实际控制人、主要负责人或者高级管理人员的单位，依法不得发放排污许可证或者危险废物经营许可证。

3. 企业经营中容易忽视的风险点

企业涉及污染环境类案件中，往往存在企业经营者的认识与刑事司法认定存有偏差的问题，部分案件属于企业在无意之间涉案进而遭到严重刑事处罚。通过案件梳理，我们统计了以下几个企业运营中容易忽视的风险点。

■ 监管不到位亦有可能构成犯罪

关于污染环境罪主观方面的要求是故意还是过失，目前在司法实践中尚存有一定争议，有人主张故意，有人主张过失，有人主张混合罪过。我们对此不做学术探讨，只是提示相关企业管理人员，实践中疏于管理，监管工作不到位同样有入罪的风险。司法实践中，存在被告单位对其行为可能造成严重环境污染事故、致公私财

产遭受重大损失等后果本应当预见，但由于疏忽大意而没有预见，最终以主观方面存有过失而被认定为构成犯罪的案例。另外，也存在明知对方无危险废物处理资质的情况下仍委托其处理废物，以污染环境罪追究刑责的案例。

■ 长期贮存、搁置危险废物具有入罪的风险

实践中，长期贮存、搁置危险废物有可能被评定为刑法条文规定的“排放”、“倾倒”、“处置”的行为。《纪要》指出，司法实践中认定非法排放、倾倒、处置行为时，应根据《固体废物污染环境防治法》和《环境解释》的有关规定精神，从其行为方式是否违反国家规定或者行业操作规范、污染物是否与外环境接触、是否造成环境污染的危险或者危害等方面进行综合分析判断。对名为运输、贮存、利用，实为排放、倾倒、处置的行为应当认定为非法排放、倾倒、处置行为，可以依法追究刑事责任。比如，未采取相应防范措施将没有利用价值的危险废物长期贮存、搁置，放任危险废物或者其有毒有害成分大量扬散、流失、泄漏、挥发，污染环境的。

■ 企业环评报告等文件中明确的事项，可作为认定犯罪的依据

企业曾因项目运营开展过环境评估、排污许可申请等工作，取得了相应的环评报告、排污许可等文件，未来一旦发生严重污染环境的情形，上述文件中明确记载的事项，可作为刑事案件中判定主观明知、认定危险废物等问题的重要依据。在一则案例中，判决书在事实部分表述称涉案公司于2013年1月通过环评开始投产，其环评和排污许可证均明确规定沥青喷淋废水不外排，存储废水的循环池含有沥青油沉渣，该沉渣属于危险性固体废物。可见，在事实认定过程中，合议庭引用了环评文件、排污许可中明确载明的事项作为刑事案件认定犯罪的重要依据。对于企业来讲，需要了解生产经营中取得的环境评估报告等相关文件记载的信息，尤其是限制、禁止规定，这些信息都有可能成为刑事诉讼中推定企业明知的依据。

4. 犯罪认定中的争议点

查阅判决过程中，我们也重点关注了判决书使用较大篇幅展开论证的争议问题，既然是法庭认定的争议点，那当然也是辩护方比较容易作无罪、罪轻辩护的关键点。其中，《纪要》针对主观过错的认定，有毒物质、危险废物、重金属含量的认定、有害物质的认定等常见争议问题均作了较为详细的界定，我们在此不再赘述，重点探讨的以下几个争议点。

■ 涉案企业行为与环境污染结果是否存在因果关系

认定犯罪要从不法层面考量行为与危害结果之间的因果关系。实践中，导致环境污染危害结果发生的原因较为复杂，容易出现“多因一果”的局面。在具体个案中，企业需要关注自身行为与相关机构认定的危害结果之间是否存在因果联系，如果存在较为确实、充分的证据能够证明涉案企业的行为不可能导致危害结果的发生，或是仅有涉案企业的行为无法导致上述结果发生，则对于免除或减轻企业责任较为有利。例如，自然灾害等介入因素对于危害结果发生的重要影响，在此种情形下，如果涉案企业能证明自身已经尽到了相应的注意义务，采取了必要的防护措施，则属于较为有利的罪轻甚至是无罪辩护点。

■ 监测报告等是否科学准确

案例中诸如重金属元素含量等事项大多是由环境保护主管部门所属的环境监测机构作出。《2016年解释》第十二条规定，环境保护主管部门及其所属监测机构在行政执法过程中收集的监测数据,在刑事诉讼中可以作为

证据使用。《2016年解释》虽认可监测报告的证据地位，但在司法实践中，还需要从监测机构资质、监测程序、监测方法、监测结果等方面对监测报告开展审查。相关部门依照所属行业、污染物等因素的不同出台了相对应的监测技术规范标准。以监测点选择为例，《电镀污染物排放标准》(GB21900-2008)规定，有废水、废气处理设施的，应在该设施后监测。《污水综合排放标准》（GB8978-1996）同样针对不同污染物分别规定了相应的排放口采样点。类似标准为开展监测报告的审查提供了依据，也是判断监测报告准确性的重要抓手。

■ 对鉴定进行形式和实质审查

《纪要》提出对于涉及案件定罪量刑的核心或者关键专门性问题难以确定的,由司法鉴定机构出具鉴定意见。司法实践中有的机构对于案件专门性问题出具的意见会以《鉴别报告》、《检验报告》等形式呈现。关于上述证据是否属于鉴定意见，如何予以参考适用同样是一个案件争议点。根据相关司法解释的规定，对案件中的专门性问题需要鉴定，但没有法定司法鉴定机构，或者法律、司法解释规定可以进行检验的，可以指派、聘请有专门知识的人进行检验，检验报告可以作为定罪量刑的参考。对检验报告的审查与认定，参照适用关于鉴定意见的有关规定。无论是鉴定意见亦或是鉴别、检测报告，均是由相关人员运用自身专业知识、技能和经验对于案件涉及的专业问题出具意见，其作出鉴别的范围不应当超出自身专业领域，更不能代替法官针对法律适用问题出具结论，而且当其证明内容与在案证据材料相矛盾时，不具备优先适用的证明效力。在个案办理过程中，需要从形式和实质两个方面对鉴定意见、鉴别、检测报告等证据予以综合审查。

（二）非法获取计算机信息系统数据罪

随着大数据时代的到来，数据已经渗透到生活和工作的各个领域，成为重要的生产因素，“网络爬虫”作为高效获取海量数据的重要方式在促进数据共享和互联网生态繁荣的同时也引发了一系列涉及利益争端、合规运营方面的突出问题。

1. 网络爬虫的利与弊

网络爬虫（又被称为网页蜘蛛，网络机器人），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。通俗来讲，网络爬虫模仿人工访问操作进行信息读取和收集的工作，只是爬虫爬取信息效率更高，数据量更大。网络爬虫在提升工作效率的同时，也会带来一些负面影响，比如侵占带宽资源，增加网站负荷量甚至会造成网站瘫痪，破坏计算信息系统，侵犯公民个人信息，侵犯商业秘密等。

2.“爬虫”入罪路径选择之一：非法获取计算机信息系统数据罪

非法获取计算机信息系统数据罪是《中华人民共和国刑法修正案（七）》增设的一个罪名，是指违反国家规定，侵入国家事务、国防建设、尖端科学技术领域以外的计算机信息系统或者采用其他技术手段，获取该计算机信息系统中存储、处理或者传输的数据，情节严重的行为。从以往的生效判例来看，涉案人员主要是通过木马、病毒等黑客渗透方式非法获取计算机系统数据。近期，从司法实践来看使用爬虫程序爬取数据的方式亦存在成立此罪的较大风险。

3. 网络爬虫的入罪案例：绕过网站反爬措施获取公开信息入罪

（1）基本案情

2018年，北京市海淀区人民法院对一起利用“爬虫

技术”侵入计算机系统抓取数据案作出判决，该案被“互联网法律大会”列为全国首例利用“爬虫技术”侵入计算机系统抓取数据案。据公开的判决信息显示，被告单位CEO、技术负责人等公司主管人员共谋，采用技术手段抓取被害单位北京某网络技术有限公司服务器中存储的视频数据，并破解被害单位的防抓取措施，使用“tt_spider”文件实施视频数据抓取行为，造成被害单位损失技术服务费人民币2万元。经鉴定，“tt_spider”文件中包含通过分类视频列表、相关视频及评论等接口对被害单位服务器进行数据抓取，并将结果存入到数据库中的逻辑。在数据抓取的过程中使用伪造device_id绕过服务器的身份校验，使用伪造UA及IP绕过服务器的访问频率限制。法院经审理后认为，被告单位违反国家规定，采用技术手段获取计算机信息系统中存储的数据，情节严重，其行为已构成非法获取计算机信息系统数据罪；公司CEO、技术负责人等作为直接负责的主管人员及其他直接责任人员，分别被法院判处有期徒刑九个月至一年不等的刑罚及人民币三万元至五万元不等的罚金。

（2）释法说理

案件的认定在科技和法律界引起了一定争议，数据爬取行为的法律边界在哪？是否需要对其进行刑法规制？据公开的信息可知，被告单位的犯罪行为主要是“破解北京某网络技术有限公司的防抓取措施，使用‘tt_spider’文件实施视频数据抓取行为，造成被害单位北京某网络技术有限公司损失技术服务费人民币2万元”，具体表现在“在数据抓取的过程中使用伪造device_id绕过服务器的身份校验，使用伪造UA及IP绕过服务器的访问频率限制”。主审法官在其撰写的文章中提及，被告单位及被告人在数据抓取过程中，采取了规避或突破被害单位反“爬虫”安防措施的技术手段，未经许可进入被害单位的计算机系统，属于非法获取计算机信息系统数据罪中“侵入”行为，从而构成非法获取计算机信息系统数据罪。[2]

（3）风险评议

计算机信息系统权利人获取数据可能花费了较大成本，数据作为核心资源，其不乐见于他人“不劳而获”。因此，为维护个人利益，网站一般会设置相应的反爬虫的技术保护措施。例如识别User-Agent，运维人员对可疑用户直接拒绝访问；判断同一IP或同一设备在一段时间内访问量异常；通过验证码、滑动解锁的方式，甄别爬虫，封杀IP等。透过上述判决书认定事实及主审法官的著述，我们理解绕过网站反爬虫措施获取数据属于违背权利人意愿读取、收集数据，将有较大可能被认定为对计算机信息系统的‘侵入’，进而以非法获取计算机系统数据罪定罪处罚。

对于“侵入”的理解：在以往判例中，司法机关主要基于以下两种路径判定对计算机信息系统的“侵入”。一是无用户身份的侵入，即通过盗取、破解密码等方式进入系统；二是超权限访问的侵入，即具有合法用户身份，但超越自身授权范围访问信息资源。本案中，涉案人员所实施的行为与前述两种“侵入”方式有所不同，其可以浏览被害单位网站提供视频，但不被允许使用爬虫技术对视频进行爬取，其实施绕过被害单位反爬虫安防措施的行为被评定为对计算机信息系统的“侵入”。此外，还存在一种相对折中的观点，即认为爬取数据行为是否能够认定为“侵入”要看网页设置的防护措施是否复杂严密，如果防护措施较为复杂严密，使用技术手段绕过防护机制的行为可以认定为侵入计算机信息系统，侵入后爬取数据就符合非法获取计算机信息系统数据罪。

对于“公开信息”的理解：由于刑法条文及相关司法解释并未明确规定非法获取计算机信息系统数据罪所称的“数据”是否包含公开信息，理论界及司法实务界对此问题存有争议。有的学者主张对于网页上公开的信息，

2. 游涛、计莉卉：《海淀法院审结全国首例利用“爬虫”技术侵入计算机信息系统抓取数据案》，载微信公众号《北京海淀法院》2018年12月29日。

任何人均可获取，只是权利人对获取方式进行了限制，禁止采取爬虫技术获取。应当理解为网页不排除行为人访问系统，获取信息，只是对访问的方式进行了限定（如对访问频率的限制），要将反爬防护措施与设定访问权限的安全保护措施区别开来，行为人绕开反爬防护措施不宜定性为非法获取计算机信息系统数据罪。本案中，被害单位APP用户或视频APP用户可以观看被害单位网站上的视频信息，从一般意义上讲，我们可以将此类视频信息理解为公开信息，而判决认定采取绕开安全防护措施的方式爬取此类公开的视频信息构成非法获取计算机信息系统数据罪。当然，主审法官在其撰写的文章中认为罪名所称的“数据”与“信息”不同，“数据”是信息化存储、处理和传输的客观表现形式，包含信息数据化后的数据和冗余数据，而非数据本身。[3] 信息公开不等同于数据公开。对于大数据公司来说，并不需要去厘清概念背后的区别与联系，只是在业务开展中需要树立风险防范意识，贸然爬取公开可见的信息存有一定刑事风险。

4. 网络爬虫的出罪案例：采用爬虫获取内部公开数据出罪

（1）基本案情

犯罪嫌疑人于某系某互联网公司网络工程师，该公司内部使用一款企业即时聊天App作为内部人员沟通交流的办公软件，员工通过其个人账号、密码使用手机登陆后，如有工作需要，可与公司内任一员工即时聊天，并可点击查看公司员工备注的姓名、员工号、手机号码、职位职级以及公司组织架构等信息，App后台会将访问记录予以记录，公司内部制度规定非因工作需要不得随意查看其他员工的数据信息。2018年2月，于某对该聊天软件的源代码进行反向编译，查找到该聊天工具传送员工信息数据的服务器接口，后编写了专门的爬虫程序，在其使用其账号密码登陆App后，该程序自动运行，向该接口循环发送访问请求，成功从该隐藏接口爬取到6万余名员工的姓名、员工号、手机号码、职位职级以及公司组织架构等信息。海淀区人民检察院承办检察官认为，于某的行为不构成非法获取计算机信息系统数据罪。[4]

（2）释法说理

本案中，于某对公司聊天即时APP具有访问权限，可以使用点击查看的方式获取APP内数据，而于某通过对聊天软件的源代码进行反向编译，查找到该聊天工具传送员工信息数据的服务器接口，后采取编写爬虫程序方式获取批量数据。其行为从外观上来看，似乎也属违背了权利人的意愿收集数据，但承办检察官认为于某的行为既不符合“侵入+获取”，也不符合“利用其他技术手段+获取”，且其获取的数据属于其职权范围内可以知晓的内容，只是获取数据的表现形式及访问效率与在App内访问有所差别，但无本质不同。于某的行为不构成非法获取计算机信息系统数据罪。

（3）抗辩理由

通过上述不构罪案例，我们理解行为人如果能够主张其并未采取绕开权利人反爬安全措施的技术手段进入计算机系统，且获取的数据未超过权利人明确授权的范围，虽然其获取数据的方式违背了权利人意愿，但构成非法获取计算机信息系统数据罪的风险不高。

需要说明的是，司法人员基于对法律的认识和理解作出的认定并非就是对审理此种类型案件的指导做法，上述几个问题在司法实践中尚存有争议，不同层级、不同地区的法院可能对此问题存有不同认识，当遇到类似案件时还需区别对待，具体问题具体分析。

5. 大数据公司使用爬虫技术时注意事项

3. 游涛、计莉卉：《使用使用网络爬虫获取数据行为的刑事责任认定——以“晟品公司”非法获取计算机信息系统数据罪为视角》，载《法律适用·司法案例》2019年第10期。
4. 纪敬玲、杨程：《对使用爬虫程序获取内部公开数据的刑事责任分析》，载微信公众号《办案指引》2018年11月7日。

虽然各界对于“爬虫入刑”问题尚存有争议，但已生效判决对于处理类似问题具有一定的参考价值。大数据公司在日常经营中要尽量避免因为爬虫技术的使用引发类似的争议问题，以免致使公司及其经营者陷入极为被动的境地。我们也提醒公司在使用爬虫技术时做好以下三点：

（1）尽量避免违背计算机信息系统权利人的意愿爬取数据；

（2）尽量避免给目标服务器带来过大的负荷量，造成损害；

（3）仔细甄别获取数据类型，谨慎处理包含公民个人信息、商业秘密等内容的信息。

此类案件中，除了涉及非法获取计算机信息系统数据罪，还可能涉及到侵犯公民个人信息罪、侵犯商业秘密罪、破坏计算机信息系统罪、侵犯著作权罪等罪名，一般会依照想象竞合原则，择一重处罚。

据了解，此番多家大数据公司遭受调查涉案的多为特殊的数据，即公民个人信息，相应的刑事罪名为【侵犯公民个人信息罪】。关于非法获取、提供公民账号密码、财产状况、行踪轨迹等侵犯公民个人信息的问题，我们将在后续发布的文章中对此作深入分析。

(三) 侵犯公民个人信息罪

1. 罪名概述

根据刑法分则条文对侵犯公民个人信息罪的表述，我们认为应当从四个方面重点理解、把握侵犯公民个人信息罪的认定，即公民个人信息的定义、违法国家有关规定涵义、非法获取公民个人信息认定、非法提供公民个人信息认定。

（1）公民个人信息的定义

我国多部法律文件分别就“公民个人信息”的概念给出相应的定义 ，它们在文字表述和具体含义上略有不同。2017年两高联合发布《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》（下称《解释》），由于《解释》是针对刑事案件办理专门制定的最新法律文件，对于公民个人信息的界定也较为明确具体，我们在刑事风险研判中将以《解释》给出的定义为准。《解释》第一条规定，“公民个人信息”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特定自然人身份或者反映特定自然人活动情况的各种信息，包括姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等。条文明确“公民个人信息”包含了身份识别信息和活动情况信息。不同于我们通常理解的只有身份识别信息属于“公民个人信息”，行踪轨迹等位置信息同样会被认定为“公民个人信息”。

（2）违反国家有关规定的涵义

《解释》第二条对于“违反国家有关规定”作出较为明确的界定。条文将国家有关规定的范围限于法律、行政法规、部门规章等国家层面的规定，从而排除了部门规范性文件、国家标准和一些非国家层面的其他规定的适用。例如，目前对个人信息范围规定最为详细的规定《个人信息安全规范》就是一部推荐性的国家标准，不属于部门规章。相较于之前的规定，《解释》将部门规章添加到规定范围之中，从而扩大对于“公民个人信息”的保护范围。目前，我国有关公民个人信息保护的法律、行政法规、部门规章尚需完善，这就给办案人员留有一定的解读《网络安全法》以及相关法律法规和部门规章中涉及个人信息保护条款的空间，特别是，实践中网络运营者无法按照第四十一条中“告知+同意”的

要求获取公民个人信息时，那么在认定其行为合法性上就存在较大解释空间。

（3）非法提供公民个人信息的认定

《解释》第三条对于“非法提供公民个人信息”行为的认定作出规定，概言之，主要包括三种方式：一是向特定的人提供个人信息；二是通过信息网络或者其他途径发布个人信息；三是未经被收集者同意，将合法收集的公民个人信息向他人提供。

（4）非法获取公民个人信息的认定

窃取或者以其他方法非法获取公民个人信息是侵犯公民个人信息罪的客观行为方式。《解释》第四条对“以其他方法非法获取公民个人信息”的行为进行了进一步明确，违反国家有关规定通过购买、收受、交换等方式获取公民个人信息，或者在履行职责、提供服务过程中收集公民个人信息，属于“以其他方法非法获取公民个人信息”。

2. 司法实践中侵犯公民个人信息罪的具体适用

当前，侵犯公民个人信息犯罪呈高发态势，涉及到日常生活中的各行各业、方方面面。9月份以来，多家互联网金融科技公司涉案，管理人员被警方控制，公司日常经营处于停滞状态，而据媒体报道，上述公司被调查主要因涉嫌抓取公民个人信息，助力“套路贷”暴力催收。鉴于近期密集涉案的大数据科技公司多来自于互联网金融行业，我们就结合互联网金融行业特点梳理一下企业在公民个人信息保护领域可能面临的刑事合规风险，供相关客户参考。

（1）互金行业大数据公司可能涉及的信息类型

侵犯公民个人信息罪的成立以案件存在公民个人信息为前提。在作入罪风险研判之前，首先需要梳理公司可能获取、提供的信息类型。以互金行业为例，该行业大数据公司在业务开展过程中收集的信息种类繁多。其中，《解释》第一条“公民个人信息”定义中明确列举的姓名、身份证件号码、通信通讯联系方式、住址、账号密码、财产状况、行踪轨迹等信息在互金行业大数据公司业务开展中基本均有涉及，也容易被认定为公民个人信息。

此外，互联网金融公司业务开展过程中还可能涉及到《解释》并未明确列举的信息类型主要有：职业信息、学历信息、直系亲属姓名、银行卡号、消费记录、资产情况、通信记录、上网记录、cookie信息等诸多可以用于判定个人信用的信息。对于此类信息是否能够评定为公民个人信息，还需要考量信息本身是否能够直接识别特定自然人或者是否与已经识别的自然人进行关联。其中通过一个识别符（例如IP地址、deviceID、手机号码、邮件等）加上行为数据等这种数据组合一般都能直接识别一个特定自然人及其行为。但是单个数据在不结合其他数据的情况下，例如用户标签本身是否是个人信息这还需要考虑到这些信息本身的颗粒度以及可识别性。这种可识别性在目前的法律法规项下没有明确规定。GDPR（欧盟《一般数据保护条例》）中规定的个人信息的范围与《解释》中的个人信息的范围在内涵上均是非常宽泛的。GDPR对于可识别性的判断标准是一个客观的可识别性，并且需要综合考虑使用该信息的识别成本、耗时以及在该数据处理行为发生当时的技术水平是否能够凭借该信息直接识别个人。这些客观要素来判断“可识别性”也是可以供企业借鉴。

（2）互金行业大数据公司可能涉嫌犯罪的几种行为

由于互金行业大数据公司业务开展过程中需要综合

评定用户的个人信用程度、还款能力等信息，以便于提前预防、有效化解金融风险，因此行业对于准确获取用户个人信息要求比较高。对公民真实个人信息的巨大需求同时也带来了其在信息保护领域的较高风险。我们将从以下三个方面初步分析互金行业大数据公司可能涉及的刑事入罪情形。

■ 作为“套路贷”行为的共犯入罪

“套路贷”，是对以非法占有为目的，假借民间借贷之名，诱使或迫使被害人签订“借贷”或变相“借贷”“抵押”“担保”等相关协议，通过虚增借贷金额、恶意制造违约、肆意认定违约、毁匿还款证据等方式形成虚假债权债务，并借助诉讼、仲裁、公证或者采用暴力、威胁以及其他手段非法占有被害人财物的相关违法犯罪活动的概括性称谓，涉及的具体刑事罪名主要为诈骗、敲诈勒索、非法拘禁、虚假诉讼、寻衅滋事等。当前，各级执法机关不断加大对套路贷违法犯罪行为的打击力度，对此类违法借贷行为呈现持续高压态势。

互金领域的大数据公司与“套路贷”违法犯罪是如何在业务开展中产生交集的呢？我们认为互联网金融领域的大数据公司存在成立“套路贷”犯罪共犯的风险。2019年4月9日最高人民法院、最高人民检察院、公安部、司法部联合发布的《关于办理“套路贷”刑事案件若干问题的意见》（下称“《意见》”）第5条规定，明知他人实施“套路贷”犯罪，具有以下情形之一的，以相关犯罪的共犯论处，但刑法和司法解释等另有规定的除外：

（a）组织发送“贷款”信息、广告，吸引、介绍被害人“借款”的；
（b）提供资金、场所、银行卡、账号、交通工具等帮助的；
（c）出售、提供、帮助获取公民个人信息的；
（d）协助制造走账记录等虚假给付事实的；
（e）协助办理公证的；
（f）协助以虚假事实提起诉讼或者仲裁的；
（g）协助套现、取现、办理动产或不动产过户等，转移犯罪所得及其产生的收益的；
（h）其他符合共同犯罪规定的情形。

通读《意见》第5条规定的几种情形，大数据公司较有可能涉嫌实施“出售、提供、帮助获取公民个人信息”的行为。如前所述，互金行业的大数据公司可能会在用户使用期间收集包括真实姓名、身份证件信息、手机号码、资产状况、通讯录信息等多种信息用于身份识别、信用审核、风险控制管理、逾期账务管理等用途。用户一旦出现逾期还款情形，有些通过大数据公司平台放贷的小贷公司及催收公司等便会采用多种“软暴力”催收行为。例如，有的催收公司会采取拨打电话、发送短信等方式对用户通讯录内亲戚、朋友、家人进行骚扰甚至辱骂，或者在网络平台或是其他公共区域曝光个人信息。小贷公司、催收公司因涉及套路贷被调查，势必会引发警方对通讯录信息以及公民其他个人信息来源的追查。如果用户个人信息是由大数据公司通过自己经营的平台收集后提供给小贷公司、催收公司，尤其是涉及可能超出用户本人授权范围的通讯录内家人、亲戚、朋友等人员的信息，那么大数据公司会有较大可能被认定为明知他人实施“套路贷”犯罪，仍向其“出售、提供、帮助获取公民个人信息”，以“套路贷”共犯论处，进而构成诈骗犯罪等罪名。即便大数据公司对于其合作公司从事“套路贷”行为主观不明知，但其提供用户个人信息的行为一旦达到相应的刑事处罚标准，也将有可能被认定为侵犯公民个人信息罪。如真实情况如此，则可能预示着执法机关逐渐从对“小额贷款公司”、“咨询公司”、“催收公司”等前端犯罪主体的打击开始向数据提供方、中介服务方等方向蔓延。

■ 窃取、收买、交换公民个人信息入罪

司法实践中，窃取公民个人信息有多种表现方式。一种是利用计算机病毒、网络攻击、网络侵入等方式进入计算机系统非法获取公民个人信息，一般来讲，该类行为还会伴有对目标计算机系统设定访问权限的安全保护措施的突破；另一种是通过剽窃、偷取等方式获得他人登录权限，进而进入计算机系统获取公民个人信息，此种方式并非利用科技手段，而且通过采取一般生活概念中的“偷窃”行为实施。我们理解，作为能够发展到一定规模的互金行业大数据公司来讲，采取上述两种明显违规方式获取公民个人信息的情形并不多见。当然，实践中确也存在少数初具规模的大数据公司采取黑客方式侵入竞争对手计算机系统爬取信息的案例。此外，还有一种我们称之为“监守自盗”型窃取，是指信息收集方的内部人员利用职务便利将所掌握的公民个人信息对外售出。严格来讲，该行为应当属于《刑法》条文所规定“将在履行职责或者提供服务过程中获得的公民个人信息出售或者提供给他人”的行为。此种窃取公民个人信息的方式，主要涉及到企业员工的个人犯罪，如果公司对此不知情，则公司因此承担刑事责任的风险较小。当然，在此情况下，涉案公司也可以积极主张企业内部已经制定了具体的公司政策禁止员工实施此类行为，同时采取了一定的技术、管理措施防止“监守自盗”行为的发生，以此来证明公司的主观态度，从而规避公司构成单位犯罪的风险。

收买、交换公民个人信息也可能是此类大数据公司涉案的原因之一。实践中，交换公民个人信息有可能会发生在同业之间互通有无，也有可能发生在不同行业之间各取所需。

■ 未经被收集者同意，将合法收集的公民个人信息向他人提供入罪

大数据公司通过平台授权的方式收集用户的公民个人信息，其中收集到的行踪轨迹、财产信息、征信信息、通信内容等信息与人身安全与财产安全直接相关，属于高度敏感信息。无论是基于评估放贷风险、设置还款提醒的目的还是为了提高客户服务体验，公民个人信息都应在用户授权范围内使用。根据《网络安全法》第四十二条第一款的规定，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。《解释》第三条第二款规定，未经被收集者同意，将合法收集的公民个人信息向他人提供的，属于刑法第二百五十三条之一规定的“提供公民个人信息”。实践中，未经被收集者同意，将被收集人的公民个人信息销售给放贷公司、保险代理、教育培训等行业赚取利润，明显违背、超出了被收集人的授权范围，也会对相关用户的正常生活造成困扰，此种行为违反法律规定，情节严重构成侵犯公民个人信息罪。办理此类刑事案件，准确划定公民个人信息的边界对于认定犯罪较为关键。而且，近年来对于“信息投放只针对终端浏览器而非针对网络用户”的辩解也由于终端设备与特定用户的密切关联愈发受到质疑，需引起重视。

（3）实践中可能存有争议的行为的认定

■ 超范围获取公民个人信息的行为认定

《网络安全法》第四十一条规定，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。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。我们理解，网络运营者收集公民个人信息应当遵循必要原则，不得收集与其提供的服务无关的个人信息，否则将有可能被评定为“非法获取公民个人信息”

的行为。TC260在今年2019年6月1日发布了《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》（下称《规范》）指引企业判断个人信息收集和使用的“必要性原则”，方达律师事务所有幸获邀参与《规范》编写。TC260于2019年8月8日将该指南转为国家标准（信息安全技术移动互联网应用（App）收集个人信息基本规范（草案））并开始公开征求意见。由于这两个都是TC260的一个指南，实践中公安机关是否会以此作为办案参考来判断是否过分采集尚未明确。

■ 仅经用户授权但未经第三方平台授权而获取信息行为的认定

部分大数据公司利用其平台收集用户个人信息时，可能还会要求用户授权公司使用其在第三方购物平台的账号和密码，用于爬取该用户第三方平台内的消费、购物记录等信息。我们理解第三方平台一般会禁止他人爬取平台数据，此种情形下，大数据公司爬取数据的行为如果造成第三方服务器无法正常运行等情形的出现，同样存有涉嫌破坏计算机信息系统等罪名的刑事风险，但实践中是否会作入罪评价还需个案分析。

3. 公民个人信息保护合规运营注意事项

■ 制定、完善企业内部个人信息保护合规政策

企业在日常运营中需高度重视个人信息保护合规政策的制定与完善工作，结合自身运营模式，对于关键环节、关键岗位、关键人员制定相应的合规操作规范、员工行为规范，充分表明企业高度重视个人信息保护的明确态度以及为此设置的实质举措。这也有利于在未来可能出现的刑事诉讼环节厘清企业责任与个人责任。

■ 搭建数据采集的合规体系，做好实时合规管控

企业对外采集数据需根据企业自身需求搭建数据采集合规体系，严格甄别不同数据源以及不同数据类型，制定完善相应的书面流程。按照信息采集的整体步骤，在全流程的关键节点设置风险提示，落实企业内部监管责任，实时开展合规管控。

■ 针对合作方开展合规尽职调查，防范共同犯罪风险

绝大多数企业都有较为强烈的合规经营意愿。但在实践中，企业仅靠主观的合规意愿及罗列的合规条文尚无法有效避免刑事风险。从以往的刑事判例来看，有相当数量的公司是由于上下游合作方涉案进而引发自身涉案,即合作方遭到刑事指控，公司因涉嫌与合作方共同犯罪同样接受刑事调查，公司业务因此陷入停滞，管理人员甚至会失去人身自由。例如，大数据公司遭受调查应当与其下游合作方放贷公司、催收公司遭受刑事指控不无关系，类似情形不仅仅发生在大数据公司行业，在其他行业领域也较为常见。新的执法形势对企业开展投资、合作提出了更高的合规要求。目前，越来越多的企业已经意识到防范来自于合作方刑事风险的重要性，开展合作前会聘请专业律师针对潜在的合作方开展有效的合规尽职调查，尽早发现对方可能涉嫌的犯罪行为，及时研判刑事风险，防患于未然。可以说，合规尽职调查不仅仅是准确识别瑕疵客户的有效手段，同样也是未来抗辩可能面临的刑事指控的强力事由。

■ 向他人提供公民个人信息，需经被收集者同意、授权或作匿名化处理

除了维护国家安全或基于侦查、起诉、审判工作的需要向司法机关提供相关人员的个人信息等特殊情形外，向他人提供合法取得的公民个人信息一般需要被收集者同意、授权。如果能够将公民个人信息作脱敏、变形等匿名化处理，使得通过处理后的信息无法识别特定个人且

不能复原，则可以理解为符合法律规定和监管要求，可以向他人提供。

（四）拒不履行信息网络安全管理义务罪

《中华人民共和国刑法修正案（九）》增设了该罪名。近期，中国裁判文书网公开的一则案例，上海市浦东新区人民法院对胡某一审判决构成“拒不履行信息网络安全管理义务罪”，该案引起业界的广泛关注。

1.罪名概述

拒不履行信息网络安全管理义务罪是指网络服务提供者不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施而拒不改正，有下列情形之一的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金：

(一) 致使违法信息大量传播的；
(二) 致使用户信息泄露，造成严重后果的；
(三) 致使刑事案件证据灭失，情节严重的；
(四) 有其他严重情节的。

单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照前款的规定处罚。

有前两款行为，同时构成其他犯罪的，依照处罚较重的规定定罪处罚。

（1）涉案主体范围

提供下列服务的单位和个人：

■ 网络接入、域名注册解析等信息网络接入、计算、存储、传输服务；

■ 信息发布、搜索引擎、即时通讯、网络支付、网络预约、网络购物、网络游戏、网络直播、网站建设、安全防护、广告推广、应用商店等信息网络应用服务；

■ 利用信息网络提供的电子政务、通信、能源、交通、水利、金融、教育、医疗等公共服务。

（2）监管部门责令采取改正措施

网信、电信、公安等依照法律、行政法规的规定承担信息网络安全监管职责的部门,以责令整改通知书或者其他文书形式,责令网络服务提供者采取改正措施。

（3）涉案主体拒不改正

认定‘经监管部门责令采取改正措施而拒不改正’，综合考虑监管部门责令改正是否具有法律、行政法规依据，改正措施及期限要求是否明确、合理，网络服务提供者是否具有按照要求采取改正措施的能力等因素进行判断。

（4）入罪标准

情形一	致使违法信息大量传播	（一）致使传播违法视频文件二百个以上的； （二）致使传播违法视频文件以外的其他违法信息二千个以上的； （三）致使传播违法信息，数量虽未达到第一项、第二项规定标准，但是按相应比例折算合计达到有关数量标准的； （四）致使向二千个以上用户账号传播违法信息的； （五）致使利用群组成员账号数累计三千以上的通讯群组或者关注人员账号数累计三万以上的社交网络传播违法信息的； （六）致使违法信息实际被点击数达到五万以上的； （七）其他致使违法信息大量传播的情形。

情形二	致使用户信息泄露，造成严重后果	（一）致使泄露行踪轨迹信息、通信内容、征信信息、财产信息五百条以上的； （二）致使泄露住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的用户信息五千条以上的； （三）致使泄露第一项、第二项规定以外的用户信息五万条以上的； （四）数量虽未达到第一项至第三项规定标准，但是按相应比例折算合计达到有关数量标准的； （五）造成他人死亡、重伤、精神失常或者被绑架等严重后果的； （六）造成重大经济损失的； （七）严重扰乱社会秩序的； （八）造成其他严重后果的。
情形三	致使影响定罪量刑的刑事案件证据灭失，情节严重	（一）造成危害国家安全犯罪、恐怖活动犯罪、黑社会性质组织犯罪、贪污贿赂犯罪案件的证据灭失的； （二）造成可能判处五年有期徒刑以上刑罚犯罪案件的证据灭失的； （三）多次造成刑事案件证据灭失的； （四）致使刑事诉讼程序受到严重影响的； （五）其他情节严重的情形。
情形四	其他严重情节	（一）对绝大多数用户日志未留存或者未落实真实身份信息认证义务的； （二）二年内经多次责令改正拒不改正的； （三）致使信息网络服务被主要用于违法犯罪的；

2. 典型案例：胡某拒不履行网络安全管理义务罪

由于拒不履行信息网络安全管理义务罪是新增罪名，而且规定了监管部门责令改正而拒不改正的前置构罪要件，立案标准比较高，目前还鲜少有实务判例，胡某拒不履行信息网络安全管理义务罪是近期一则热点案例。

2015年7月至2016年12月30日间，被告人胡某为非法牟利，租用国内、国外服务器，自行制作并出租“土行孙”、“四十二”翻墙软件，为境内2000余名网络用户非法提供境外互联网接入服务。2016年3月、2016年6月上海市公安局浦东分局先后两次约谈被告人胡某，并要求其停止联网服务。2016年10月20日，上海市公安局浦东分局对被告人胡某利用上海丝洱网络科技有限公司擅自建立其他信道进行国际联网的行为，作出责令停止联网、警告、并处罚款人民币15,000元，没收违法所得人民币40,445.06元的行政处罚。被告人胡某拒不改正，于2016年10月至2016年12月30日，继续出租“土行孙”翻墙软件，违法所得共计人民币236,167元。经鉴定，“土行孙”翻墙软件采用了gotunnel程序，可以实现代理功能，适用本地计算机通过境外代理服务器访问境外网站。法院认为，被告人胡某非法提供国际联网代理服务，拒不履行法律、行政法规规定的信息网络安全管理义务，经监管部门责令采取改正措施后拒不改正，情节严重，其行为已构成拒不履行信息网络安全管理义务罪。

（五）非法经营罪（非法买卖外汇行为）

全国人大常委会于1998年12月29日颁布了《关于惩治骗购外汇、逃汇和非法买卖外汇犯罪的决定》第四条规定，在国家规定的交易场所外非法买卖外汇，扰乱市场秩序，情节严重的，依照非法经营定罪处罚。刑事立法为依法惩治地下钱庄非法买卖外汇犯罪活动提供了法律依据。为依法惩治非法从事资金支付结算业务、非法买卖外汇犯罪活动，维护金融市场秩序，2019年1月31日，最高人民法院、最高人民检察院联合发布《关于办理非法从事资金支付结算业务、非法买卖外汇刑事案件适用法律若干问题的解释》（下称《解释》）。《解释》的出台则进一步解决了司法实践中具体定罪量刑标准不明确，法律适用存有争议的问题。

我国刑法将“在国家规定的交易场所外非法买卖外汇”作为非法经营行为加以规制，情节严重的作入罪处理。不少企业和个人对此存有疑问，只要实施外汇交易行为，达到一定数额就会构成非法经营罪？这个困扰大家的问题在司法实践中确实存有较大的争议。

1. 观点一：实施非法买卖外汇行为，即便是单纯购买，达到法定数额就构成犯罪

我们在办理的相关案件过程中发现，部分执法人员持

有上述观点。他们认为依据法律条文的规定，买卖外汇是指外汇交易的各个环节，是包含‘单纯购买’行为的，至于购买外汇后是自用、投资亦或是出售牟利在此不论，不影响对购买外汇行为作入罪处理，应当认定为非法经营罪。

典型案例；黄某某非法经营案

2010年8月30日，黄某某因涉嫌非法经营罪，内幕交易、泄露内幕信息罪和单位行贿罪获刑14年，据法院查明，其非法经营的事实是黄某某在国家外汇管理局规定的交易场所以外，将人民币8亿元间接或直接通过“地下钱庄”，结算成港币后归还给所欠赌债。

法院认为，黄某某以人民币偿还港币债务的行为，系变相买卖外汇，属于非法买卖外汇的行为，且数额特别巨大，破坏了国家金融市场秩序，根据法律及有关司法解释的规定应以非法经营罪定罪处罚

2. 观点二：不以营利为目的买卖外汇行为，不构成非法经营罪

有的法学专家、实务部门人员则认为，非法经营罪是指自然人或者单位，违反国家规定，故意从事非法经营活动，扰乱市场秩序，情节严重的行为。非法经营罪规制的对象是经营行为，非法买卖外汇构成本罪的前提，是行为具有经营性。从非法经营罪的法条规定来看，《刑法》第225条借助三项具体行为方式的列举和一项兜底条文的规定，采取以空白罪状指引行政法规的立法模式，将数十种非法经营的行为类型纳入到本罪的规制范围之中。但任何一种行为类型，无论违反的是哪项具体的国家规定，其前提都是该行为必须属于“经营行为”。这一点从《刑法》第225条法条文本“违反国家规定，有下列非法经营行为之一……”的表述和本罪的罪名以及它在刑法典中的体系安排上也可以看出。全国人大法工委编著的《中华人民共和国刑法条文说明、立法理由及相关规定》中也指出，第225条第（四）项中所说的非法经营行为，应当“发生在经营活动中，主要是生产、流通领域”。所谓经营行为，指的是以提供商品或服务为行为方式的一种营利性活动。而所谓营利，即指通过交易获得报酬的行为。从非法经营罪的体系安排上看，本罪为“破坏社会主义市场经济秩序罪”一章中“扰乱市场秩序”一节下的罪名，因此，经营行为必须与市场相关，是市场经济领域中的市场交易活动，且这种活动应当能够为市场交易主体带来利益。

典型案例：刘某非法经营案

2014年8月，湖北省高级法院对四川某集团董事局主席刘某等人上诉案依法公开宣判。湖北省高院在二审中认为一审判决认定刘某的非法经营罪不成立，二审宣判称刘某为偿还境外赌债的外币兑换行为，因不具有营利目的，不属于经营行为，不构成非法经营罪。之后，最高人民法院也以裁定的形式指出一审判决中的认定错误，肯定了二审法院正确的法律适用。

典型案例：戴某某非法经营案

2018年3月广州市中级人民法院在审理戴某某非法经营案时认定被告人戴某某作为资金所有者，并非从事非法买卖外汇的经营者，只是将自有港币资金通过私人黑市交易形式兑换成人民币，而非通过非法买进卖出外汇赚取差价牟利，其行为不具有以营利为目的的市场交易性，并非经营行为，故被告人戴某某的行为不构成非法经营罪。

3. 在国家规定的交易场所外买卖外汇存有行政违法和刑事犯罪的双重风险

市场上以自用、投资为目的外汇需求较大，部分企业

及个人在国家规定的交易场所以外，以“对敲”的方式私下兑换外汇的行为屡有发生，此类行为存在行政违法和刑事犯罪的双重风险，应引起足够重视。在前文中我们已经详细介绍此类行为涉嫌刑事犯罪的风险，行政违法的风险则主要体现在违反《中华人民共和国外汇管理条例》的相关规定。根据《中华人民共和国外汇管理条例》第四十五条规定，私自买卖外汇、变相买卖外汇、倒买倒卖外汇或者非法介绍买卖外汇数额较大的，由外汇管理机关给予警告，没收违法所得，处违法金额30%以下的罚款；情节严重的，处违法金额30%以上等值以下的罚款；构成犯罪的，依法追究刑事责任。

（六）单位行贿罪

单位行贿罪作为企业及其高级管理人员非常容易触犯的罪名一直是我们团队关注的重点。在上一期《2017-2018中国年度合规蓝皮书》中，我们从如何区分个人犯罪与单位犯罪的角度对行贿罪、单位行贿罪进行论证分析。过去一年间，由于与罪名相关的刑事政策发生变化，本期我们将重点探讨刑事政策变化对本罪查处、认定的影响。

单位行贿罪是指单位为谋取不正当利益而行贿，或者违反国家规定，给予国家工作人员以回扣、手续费，情节严重的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，处五年以下有期徒刑或者拘役，并处罚金。

1.“受贿行贿一起查”与“保护民营企业发展”间的平衡

反腐败斗争要求要坚持“受贿行贿一起查”。早在十九大报告中就出现了‘坚持受贿行贿一起查’的表述，习近平总书记在十九届中央纪委二次全会上再次强调要“坚持受贿行贿一起查”。2019年1月，中央纪委书记赵乐际在十九届中央纪委三次全会作工作报告，其在报告中再次强调要“坚持无禁区、全覆盖、零容忍，坚持重遏制、强高压、长震慑，坚持受贿行贿一起查”。在过去一段时期内，司法实践中一定程度上存在“重查受贿、轻办行贿”的现象。未来，随着查处腐败工作不断推进，对行贿行为同样予以打击将逐渐成为一种常态。

当前刑事政策同时要求“保护民营企业发展”。2018年11月1日，习近平总书记在民营企业家座谈会上的讲话中指出，要保护企业家人身和财产安全。对一些民营企业历史上曾经有过的一些不规范行为，要以发展的眼光看问题，按照罪刑法定、疑罪从无的原则处理，让企业家卸下思想包袱，轻装前进。

最高决策层针对反腐败工作及保护民营企业发展两个主题所作的表述在思想上是一致的。长期来看，打击行贿、受贿行为的根本目的是要营造一个风清气正、合规有序的政商环境，良性运转、廉洁高效的政商互动关系又能反过来促进民营企业的健康发展，有利于民营企业做大做强。本质上“受贿行贿一起查”与“保护民营企业发展”相辅相成、互相促进的。但从短期来看，在反腐败高压态势下，确实发现了一些企业及其管理人员在经营过程中存在的违法犯罪线索，那在未来一段时期的刑事执法领域，执法部门将会采取何种态度，运用怎样的方式、力度调查单位行贿行为是一个值得关注的刑事热点。

2. 实体上，针对单位行贿犯罪的刑事处罚力度将会加大

在以往的执法实践中普遍存在“重受贿、轻行贿”的问题，受贿案件与行贿案件数量差距悬殊。造成这种情况的主要有两方面原因，一方面由于行、受贿构成要件不同，行贿罪需要具有谋取不正当利益的目的，受贿罪

则无此要求。另一方面，可能在受贿案件查处的过程中，行贿人能够积极配合执法部门的调查，相应的会有一些相对宽松的政策倾向行贿人。近期，决策层多次在重要会议上提出要“受贿行贿一起查”，反映出高层已经关注到在行贿、受贿处理问题上差异不利于从根本上杜绝腐败，营造风清气正的政商环境，就此提出了更为明确的“受贿行贿一起查”的要求。我们可以预见，在司法实践中，各级执法部门将会按照法律规定，严格掌握单位行贿行为的处罚标准，从严惩治行贿犯罪行为。

3. 程序上，针对涉案单位适用调查措施将会更加慎重

在保护民营企业发展的政策背景下，执法部门对企业采取调查、适用强制措施将会更为谨慎，尽量避免出现查办一个案件倒一家企业的不利局面。在具体执法环节，执法部门可能将更加严格适用法律法规有关侦查手段、强制措施的规定，逐步细化区分调查措施的适用对象和范围，进一步提高办案效率、缩减办案期限，依法处置涉案财产，区分不涉案款物、账户、企业生产资料，不超范围查封、扣押、冻结，从社会危险性角度出发，对单位主管人员、直接责任人员审慎采取拘留、逮捕、指定居所监视居住等限制人身自由的强制措施。

（七）内幕交易、泄露内幕信息罪

1. 罪名概述

证券、期货交易内幕信息的知情人员或者非法获取证券、期货交易内幕信息的人员，在涉及证券的发行，证券、期货交易或者其他对证券、期货交易价格有重大影响的信息尚未公开前，买入或者卖出该证券，或者从事与该内幕信息有关的期货交易，或者泄露该信息，或者明示、暗示他人从事上述交易活动，情节严重的，处五年以下有期徒刑或者拘役，并处或者单处违法所得一倍以上五倍以下罚金；情节特别严重的，处五年以上十年以下有期徒刑，并处违法所得一倍以上五倍以下罚金。

2. 入罪及处罚标准

■ 情节严重的，处五年以下有期徒刑或者拘役，并处或者单处违法所得一倍以上五倍以下罚金

在内幕信息敏感期内从事或者明示、暗示他人从事或者泄露内幕信息导致他人从事与该内幕信息有关的证券、期货交易，具有下列情形之一的，应当认定为刑法第一百八十条第一款规定的“情节严重”：

（一）证券交易成交额在五十万元以上的；
（二）期货交易占用保证金数额在三十万元以上的；
（三）获利或者避免损失数额在十五万元以上的；
（四）三次以上的；
（五）具有其他严重情节的。

■ 情节特别严重的，处五年以上十年以下有期徒刑，并处违法所得一倍以上五倍以下罚金

在内幕信息敏感期内从事或者明示、暗示他人从事或者泄露内幕信息导致他人从事与该内幕信息有关的证券、期货交易，具有下列情形之一的，应当认定为刑法第一百八十条第一款规定的“情节特别严重”：

（一）证券交易成交额在二百五十万元以上的；
（二）期货交易占用保证金数额在一百五十万元以上的；
（三）获利或者避免损失数额在七十五万元以上的；
（四）具有其他特别严重情节的。

■ 未经处理部分，累计计算

二次以上实施内幕交易或者泄露内幕信息行为，未经行政处理或者刑事处理的，应当对相关交易数额依法累计计算。

■ 特定情形下的数额认定

同一案件中，成交额、占用保证金额、获利或者避免损失额分别构成情节严重、情节特别严重的，按照处罚较重的数额定罪处罚。

构成共同犯罪的，按照共同犯罪行为人的成交总额、占用保证金总额、获利或者避免损失总额定罪处罚，但判处各被告人罚金的总额应掌握在获利或者避免损失总额的一倍以上五倍以下。

刑法条文所称“违法所得”，是指通过内幕交易行为所获利益或者避免的损失。

内幕信息的泄露人员或者内幕交易的明示、暗示人员未实际从事内幕交易的，其罚金数额按照因泄露而获悉内幕信息人员或者被明示、暗示人员从事内幕交易的违法所得计算。

■ 单位犯罪的处罚

单位犯罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，处五年以下有期徒刑或者拘役。

3.“内幕信息”的范围界定

根据《刑法》第一百八十条第三款的规定，内幕信息的范围依照法律、行政法规的规定确定

（1）《证券法》对“内幕消息”的规定

第七十五条 证券交易活动中，涉及公司的经营、财务或者对该公司证券的市场价格有重大影响的尚未公开的信息，为内幕信息。

下列信息皆属内幕信息：

（一）本法第六十七条第二款[5]所列重大事件；
（二）公司分配股利或者增资的计划；
（三）公司股权结构的重大变化；
（四）公司债务担保的重大变更；
（五）公司营业用主要资产的抵押、出售或者报废一次超过该资产的百分之三十；
（六）公司的董事、监事、高级管理人员的行为可能依法承担重大损害赔偿责任；
（七）上市公司收购的有关方案；
（八）国务院证券监督管理机构认定的对证券交易价格有显著影响的其他重要信息。

（2）《期货交易管理条例》对“内幕消息”的规定

第八十一条第（十一）项 内幕信息，是指可能对期货交易价格产生重大影响的尚未公开的信息，包括：国务院期货监督管理机构以及其他相关部门制定的对期货交易价格可能发生重大影响的政策，期货交易所作出的可能对期货交易价格发生重大影响的决定，期货交易所会员、客户的资金和交易动向以及国务院期货监督管理机构认定的对期货交易价格有显著影响的其他重要信息。

4. 犯罪主体的范围界定

两高《关于办理内幕交易、泄露内幕信息刑事案件具体应用法律若干问题的解释》对“两类主体”的规定

第一条 下列人员应当认定为刑法第一百八十条第一

5.《证券法》第六十七条的规定：发生可能对上市公司股票交易价格产生较大影响的重大事件，投资者尚未得知时，上市公司应当立即将有关该重大事件的情况向国务院证券监督管理机构和证券交易所报送临时报告，并予公告，说明事件的起因、目前的状态和可能产生的法律后果。
下列情况为前款所称重大事件：（一）公司的经营方针和经营范围的重大变化；（二）公司的重大投资行为和重大的购置财产的决定；（三）公司订立重要合同，可能对公司的资产、负债、权益和经营成果产生重要影响；（四）公司发生重大债务和未能清偿到期重大债务的违约情况；（五）公司发生重大亏损或者重大损失；（六）公司生产经营的外部条件发生的重大变化；（七）公司的董事、三分之一以上监事或者经理发生变动；（八）持有公司百分之五以上股份的股东或者实际控制人，其持有股份或者控制公司的情况发生较大变化；（九）公司减资、合并、分立、解散及申请破产的决定；（十）涉及公司的重大诉讼，股东大会、董事会决议被依法撤销或者宣告无效；（十一）公司涉嫌犯罪被司法机关立案调查，公司董事、监事、高级管理人员涉嫌犯罪被司法机关采取强制措施；（十二）国务院证券监督管理机构规定的其他事项。

款规定的“证券、期货交易内幕信息的知情人员”

（一）证券法第七十四条规定的人员[6]；

（二）期货交易管理条例第八十五条第十二项（2016年修订后的条例为第八十一条第十二项）规定的人员[7]。

第二条 具有下列行为的人员应当认定为刑法第一百八十条第一款规定的“非法获取证券、期货交易内幕信息的人员”

（一）利用窃取、骗取、套取、窃听、利诱、刺探或者私下交易等手段获取内幕信息的；

（二）内幕信息知情人员的近亲属或者其他与内幕信息知情人员关系密切的人员，在内幕信息敏感期[8]内，从事或者明示、暗示他人从事，或者泄露内幕信息导致他人从事与该内幕信息有关的证券、期货交易，相关交易行为明显异常[9]，且无正当理由或者正当信息来源的；

（三）在内幕信息敏感期内，与内幕信息知情人员联络、接触，从事或者明示、暗示他人从事，或者泄露内幕信息导致他人从事与该内幕信息有关的证券、期货交易，相关交易行为明显异常，且无正当理由或者正当信息来源的。

5.司法解释认定的“非罪情形”

具有下列情形之一的，不属于刑法第一百八十条第一款规定的从事与内幕信息有关的证券、期货交易：

（一）持有或者通过协议、其他安排与他人共同持有上市公司百分之五以上股份的自然人、法人或者其他组织收购该上市公司股份的；

（二）按照事先订立的书面合同、指令、计划从事相关证券、期货交易的；

（三）依据已被他人披露的信息而交易的；

（四）交易具有其他正当理由或者正当信息来源的。

6.指导案例

■ 案例一：李某某等内幕交易、泄露内幕信息案

裁判要旨：（1）内幕信息敏感期的确定。内幕信息敏感期应自内幕信息形成之时起至内幕信息公开时止，对于影响内幕信息形成的决策者、策划者、推动者或执行者，其决意、策划、推动、或者执行行为往往影响内幕信息的形成，足以影响证券期货交易价格。因此，上述人员决意、决策、动议或执行之时应当认定为内幕信息形成之时。（2）内幕信息知情人员建议他人买卖与内幕信息有关的证券，但没有获利的行为，构成内幕交易罪。

■ 案例二：肖某某内幕交易案

裁判要旨：（1）因获取让壳重组信息而指使他人购买让壳公司股票，后借壳公司改变的，不影响内幕信息的认定。（2）对是基于专业知识的研判还是基于对内幕信息的确信而从事有关证券、期货交易的认定，要准确分析促使行为人作出交易决定的关键因素。（考量交易行为是否明显异常）。对于既利用了专业知识判断，又利用了获取的内幕信息而从事有关的证券、期货交易的行为，只要行为人获取的内幕信息对促使其交易决定有一定影响，即帮助其在一定程度上确信从事相关交易必定获得丰厚回报，就应当认定行为人是利用内幕信息从事内幕交易。具体把握的原则：对于具有专业知识的人员，即使是利用专业知识掌握了内幕信息的内容，只要其进行专业知识判断时依据其利用职务或工作便利获取的信息，也应当认定为内幕信息的知情人员。对于具有专业知识的人员，如果其通过非法手段获取了内幕信息，同时在此过程中也通过其专业知识加强了其判断，或者是先通过专业知识预判出重组对象，后通过获取内幕信息加强了对其预判的确信，原则上只要其从事与内幕信息有关的证券、期货交易，

6.《证券法》第七十四条规定：证券交易内幕信息的知情人包括：（一）发行人的董事、监事、高级管理人员；（二）持有公司百分之五以上股份的股东及其董事、监事、高级管理人员，公司的实际控制人及其董事、监事、高级管理人员；（三）发行人控股的公司及其董事、监事、高级管理人员；（四）由于所任公司职务可以获取公司有关内幕信息的人员；（五）证券监督管理机构工作人员以及由于法定职责对证券的发行、交易进行管理的其他人员；（六）保荐人、承销的证券公司、证券交易所、证券登记结算机构、证券服务机构的有关人员；（七）国务院证券监督管理机构规定的其他人。

7.《期货交易管理条例》第八十一条第十二项规定：内幕信息的知情人员，是指由于其管理地位、监督地位或者职业地位，或者作为雇员、专业顾问履行职务，能够接触或者获得内幕信息的人员，包括：期货交易所的管理人员以及其他由于任职可获取内幕信息的从业人员，国务院期货监督管理机构和其他有关部门的工作人员以及国务院期货监督管理机构规定的其他人员。

8. 两高《解释》第五条 本解释所称“内幕信息敏感期”是指内幕信息自形成至公开的期间。证券法第六十七条第二款所列“重大事件”的发生时间，第七十五条规定的“计划”、“方案”以及期货交易管理条例第八十五条第十一项规定的“政策”、“决定”等的形成时间，应当认定为内幕信息的形成之时。影响内幕信息形成的动议、筹划、决策或者执行人员，其动议、筹划、决策或者执行初始时间，应当认定为内幕信息的形成之时。内幕信息的公开，是指内幕信息在国务院证券、期货监督管理机构指定的报刊、网站等媒体披露。

情节严重的，就应当追究内幕交易的刑事责任。（3）中国证监会应司法机关需要就内幕信息有关问题所作的认定，经审查具有客观性、合法性的，可以作为定案根据（实践中比较倾向的观点是将中国证监会出具的认定意见作为一种准书证予以使用）。

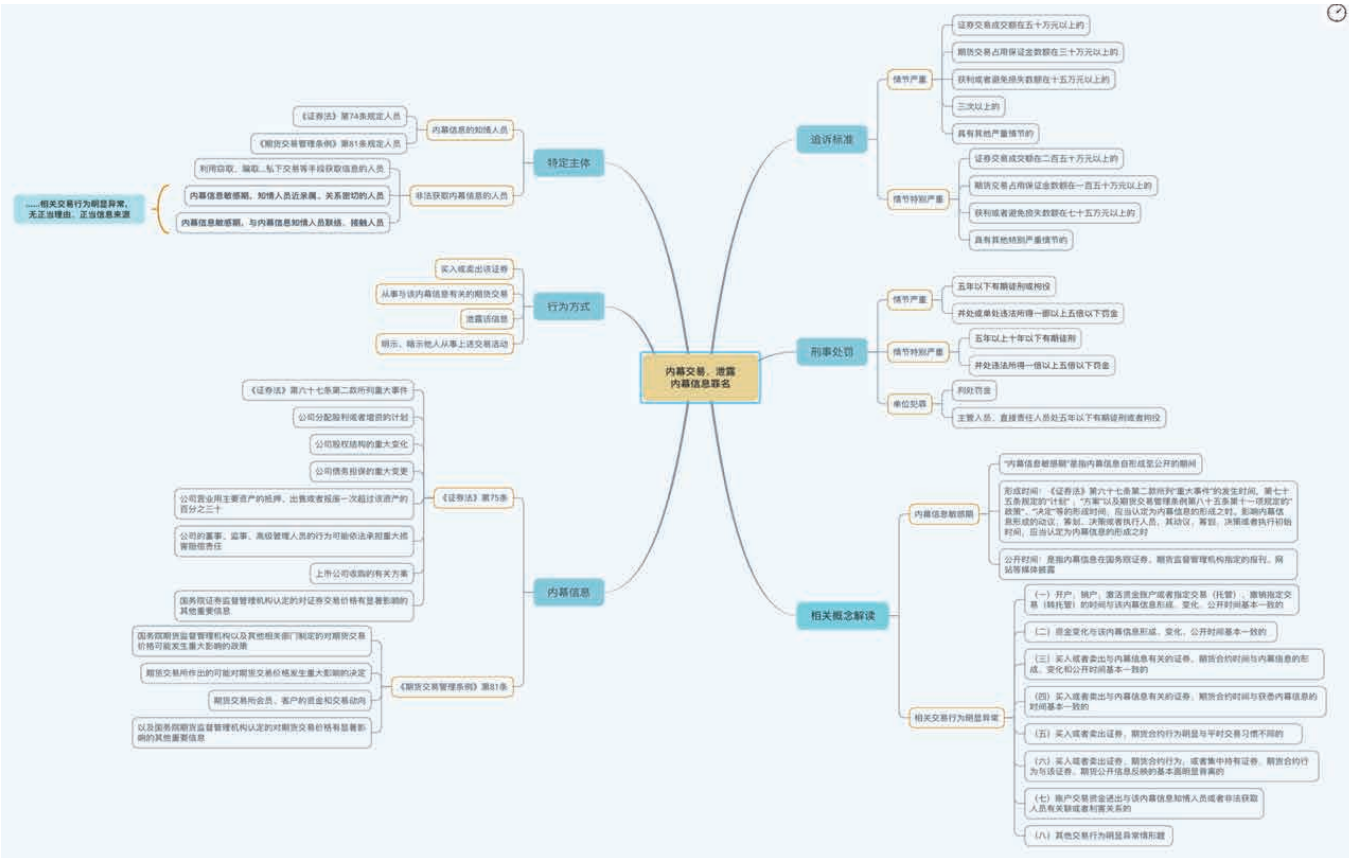
■ 案例三：赵某某等内幕交易案

裁判要旨：内幕信息知情人员的近亲属或者与其关系密切的人被动获悉内幕信息的应当认定为“非法获取证券交易内幕信息的人员”。

■ 案例四：王某某泄露内幕信息、徐双全内幕交易案

裁判要旨：（1）与内幕信息知情人员具有某种经济利益合作的大学同学属于与内幕信息知情人员关系密切的人，其即使是从内幕信息知情人员处被动获悉内幕信息，也应当认定为“非法获取内幕信息人员”。（2）在未获取股票预期价格信息的前提下，对利好型内幕信息公开后继续持股未卖，且公开当日股票价格未出现涨停的，内幕交易的违法所得应当以复牌日收盘价计算违法所得。

附：内幕交易、泄露内幕信息罪结构图



9. 两高《解释》第三条 本解释第二条第二项、第三项规定的“相关交易行为明显异常”，要综合以下情形，从时间吻合程度、交易背离程度和利益关联程度等方面予以认定：
（一）开户、销户、激活资金账户或者指定交易（托管）、撤销指定交易（转托管）的时间与该内幕信息形成、变化、公开时间基本一致的；
（二）资金变化与该内幕信息形成、变化、公开时间基本一致的；
（三）买入或者卖出与内幕信息有关的证券、期货合约时间与内幕信息的形成、变化和公开时间基本一致的；
（四）买入或者卖出与内幕信息有关的证券、期货合约时间与获悉内幕信息的时间基本一致的；
（五）买入或者卖出证券、期货合约行为明显与平时交易习惯不同的；
（六）买入或者卖出证券、期货合约行为，或者集中持有证券、期货合约行为与该证券、期货公开信息反映的基本面明显背离的；
（七）账户交易资金进出与该内幕信息知情人员或者非法获取人员有关联或者利害关系的；
（八）其他交易行为明显异常情形。

（八）利用未公开信息交易罪

1. 罪名概述

证券交易所、期货交易所、证券公司、期货经纪公司、基金管理公司、商业银行、保险公司等金融机构的从业人员以及有关监管部门或者行业协会的工作人员，利用因职务便利获取的内幕信息以外的其他未公开的信息，违反规定，从事与该信息相关的证券、期货交易活动，或者明示、暗示他人从事相关交易活动，情节严重的行为。该罪名依照内幕交易、泄露内幕信息罪的规定处罚，包括关于“情节特别严重”的规定。

（1）入罪及处罚标准

■ 情节严重的情形

（一）违法所得数额在一百万元以上的；
（二）二年内三次以上利用未公开信息交易的；
（三）明示、暗示三人以上从事相关交易活动的。

■ 情节严重的情形

利用未公开信息交易，违法所得数额在五十万元以上，或者证券交易成交额在五百万元以上，或者期货交易占用保证金数额在一百万元以上，具有下列情形之一的：

（一）以出售或者变相出售未公开信息等方式，明示、暗示他人从事相关交易活动的；
（二）因证券、期货犯罪行为受过刑事追究的；
（三）二年内因证券、期货违法行为受过行政处罚的；
（四）造成恶劣社会影响或者其他严重后果的。

■ 情节特别严重的情形

利用未公开信息交易，违法所得数额在一千万元以上的

■ 情节特别严重的情形

违法所得数额在五百万元以上，或者证券交易成交额在五千万元以上，或者期货交易占用保证金数额在一千万元以上，具有下列情形之一的：

（一）以出售或者变相出售未公开信息等方式，明示、暗示他人从事相关交易活动的；
（二）因证券、期货犯罪行为受过刑事追究的；
（三）二年内因证券、期货违法行为受过行政处罚的；
（四）造成恶劣社会影响或者其他严重后果的。

■ 未经处理部分，累计计算

二次以上利用未公开信息交易，依法应予行政处理或者刑事处理而未经处理的，相关交易数额或者违法所得数额累计计算。

■ 特定情形下的数额认定

“违法所得”，是指行为人利用未公开信息从事与该信息相关的证券、期货交易活动所获利益或者避免的损失。

行为人明示、暗示他人利用未公开信息从事相关交易活动，被明示、暗示人员从事相关交易活动所获利益或者避免的损失，应当认定为“违法所得”。

行为人未实际从事与未公开信息相关的证券、期货交易活动的，其罚金数额按照被明示、暗示人员从事相关

交易活动的违法所得计算。

（2）“内幕信息以外的其他未公开的信息”的范围界定

（一）证券、期货的投资决策、交易执行信息；
（二）证券持仓数量及变化、资金数量及变化、交易动向信息；
（三）其他可能影响证券、期货交易活动的信息。

内幕信息以外的其他未公开的信息难以认定的，司法机关可以在有关行政主（监）管部门的认定意见的基础上，根据案件事实和法律规定作出认定。

（3）“违反规定”的认定

“违反规定”，是指违反法律、行政法规、部门规章、全国性行业规范有关证券、期货未公开信息保护的规定，以及行为人所在的金融机构有关信息保密、禁止交易、禁止利益输送等规定。

（4）“明示、暗示他人从事相关交易活动”的综合认定

行为人“明示、暗示他人从事相关交易活动”，应综合以下方面进行认定：

（一）行为人具有获取未公开信息的职务便利；
（二）行为人获取未公开信息的初始时间与他人从事相关交易活动的初始时间具有关联性；
（三）行为人与他人之间具有亲友关系、利益关联、交易终端关联等关联关系；
（四）他人从事相关交易的证券、期货品种、交易时间与未公开信息所涉证券、期货品种、交易时间等方面基本一致；
（五）他人从事的相关交易活动明显不具有符合交易习惯、专业判断等正当理由；
（六）行为人对明示、暗示他人从事相关交易活动没有合理解释。

2. 典型案例

■ 许某某利用未公开信息交易罪案（最高法2012年第10期公报案例）

基本案情：被告人许某某自2006年7月8日起担任光大保德信基金管理有限公司红利股票型证券投资基金(以下简称红利基金)经理，2009年3月4日起兼任均衡精选股票型证券投资基金(以下简称均衡基金)经理，对上述两个基金的资金进行股票投资拥有决定权，直至2010年4月15日离职。2009年2月28日至2010年4月15日期间，在红利基金、均衡基金进行买卖股票情况的信息尚未披露前，被告人许某某利用职务便利，亲自或通过MSN通信、电话等方式指令张某，在史某某、王某某证券账户，先于或同期买入或卖出股票68只，金额达人民币9500余万元，非法获利达人民币209余万元。法院经审理后认为，被告人许某某在担任基金经理期间，违反国家规定，利用掌握的未公开的信息，从事与该信息相关的证券交易活动，先于或同步多次买入、卖出相同个股，情节严重，其行为已构成利用未公开信息交易罪，应依法予以惩处。

裁判要旨：行为人在担任基金经理期间，违反规定，利用掌握的未公开信息，从事与该信息相关的证券交易活动，先于或同步多次买入、卖出相同个股，情节严重，以利用未公开信息交易罪定罪处罚。

（九）操纵证券、期货市场罪

1. 罪名概述

刑法第一百八十二条规定，有下列情形之一，操纵证券、期货市场，情节严重的，处五年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处五年以上十年以下有期徒刑，并处罚金：

（一）单独或者合谋，集中资金优势、持股或者持仓优势或者利用信息优势联合或者连续买卖，操纵证券、期货交易价格或者证券、期货交易量的；

（二）与他人串通，以事先约定的时间、价格和方式相互进行证券、期货交易，影响证券、期货交易价格或者证券、期货交易量的；

（三）在自己实际控制的账户之间进行证券交易，或者以自己为交易对象，自买自卖期货合约，影响证券、期货交易价格或者证券、期货交易量的；

（四）以其他方法操纵证券、期货市场的。

单位犯前款罪的，对单位判处罚金，并对其直接负责的主管人员和其他直接责任人员，依照前款的规定处罚。

2. 条文解读

刑法条文具体列举了四种操纵证券、期货交易市场的行为，只要实施了四种行为之一，情节严重的，就构成操纵证券、期货市场的犯罪。四种行为分别是：

■ 单独或者合谋，集中资金优势、持股或者持仓优势或者利用信息优势联合或者连续买卖，操纵证券、期货交易价格或者证券、期货交易量的。

主要表现为买卖各方单独或者合谋，利用自身持有大量资金、股票、期货合约的优势，或者利用了解某些内幕信息等优势，在某时间段内共同对某种股票或者期货合约进行买卖，或者对同一股票或者期货合约反复进行买进又卖出，操纵证券、期货交易价格或交易量的行为。

■ 与他人串通，以事先约定的时间、价格和方式相互进行证券、期货交易，影响证券、期货交易价格或者证券、期货交易量。

主要表现为各方事先通谋，以约定的时间、价格相互买卖证券或者期货合约，通过反复买进、卖出，虚假造势，误导其他投资者，从而抬高或者打压某种股票或者期货的价格，最终从中获取暴利。

■ 在自己实际控制的账户之间进行证券交易，或者以自己为交易对象，自买自卖期货合约，影响证券、期货交易价格或者证券、期货交易量。

主要表现为自我买卖，即行为人以自己为交易对象，进行不转移证券所有权的自买自卖，或者以自己为交易对象，自买自卖期货合约的行为。通过上述虚假交易行为，影响市场行情，误导其他投资者入市，谋取不法利益。

■ 以其他方法操纵证券、期货市场的。

根据《最高人民法院 最高人民检察院关于办理操纵证券、期货市场刑事案件适用法律若干问题的解释》（下称“解释”）第一条的规定，刑法第一百八十二条第一款第四项规定的“以其他方法操纵证券、期货市场”主要包括：（一）利用虚假或者不确定的重大信息，诱导投资者作出投资决策，影响证券、期货交易价格或者证券、期货交易量，并进行相关交易或者谋取相关利益的；（二）通过对证券及其发行人、上市公司、期货交易标的公开作出评价、预测或者投资建议，误导

投资者作出投资决策，影响证券、期货交易价格或者证券、期货交易量，并进行与其评价、预测、投资建议方向相反的证券交易或者相关期货交易的；（三）通过策划、实施资产收购或者重组、投资新业务、股权转让、上市公司收购等虚假重大事项，误导投资者作出投资决策，影响证券交易价格或者证券交易量，并进行相关交易或者谋取相关利益的；（四）通过控制发行人、上市公司信息的生成或者控制信息披露的内容、时点、节奏，误导投资者作出投资决策，影响证券交易价格或者证券交易量，并进行相关交易或者谋取相关利益的；（五）不以成交为目的，频繁申报、撤单或者大额申报、撤单，误导投资者作出投资决策，影响证券、期货交易价格或者证券、期货交易量，并进行与申报相反的交易或者谋取相关利益的；（六）通过囤积现货，影响特定期货品种市场行情，并进行相关期货交易的；（七）以其他方法操纵证券、期货市场的。

3. 入罪及处罚标准

■ 情节严重的情形

（一）持有或者实际控制证券的流通股份数量达到该证券的实际流通股份总量百分之十以上，实施刑法第一百八十二条第一款第一项操纵证券市场行为，连续十个交易日的累计成交量达到同期该证券总成交量百分之二十以上的；

（二）实施刑法第一百八十二条第一款第二项、第三项操纵证券市场行为，连续十个交易日的累计成交量达到同期该证券总成交量百分之二十以上的；

（三）实施本解释第一条第一项至第四项操纵证券市场行为，证券交易成交额在一千万元以上的；

（四）实施刑法第一百八十二条第一款第一项及本解释第一条第六项操纵期货市场行为，实际控制的账户合并持仓连续十个交易日的最高值超过期货交易所限仓标准的二倍，累计成交量达到同期该期货合约总成交量百分之二十以上，且期货交易占用保证金数额在五百万元以上的；

（五）实施刑法第一百八十二条第一款第二项、第三项及本解释第一条第一项、第二项操纵期货市场行为，实际控制的账户连续十个交易日的累计成交量达到同期该期货合约总成交量百分之二十以上，且期货交易占用保证金数额在五百万元以上的；

（六）实施本解释第一条第五项操纵证券、期货市场行为，当日累计撤回申报量达到同期该证券、期货合约总申报量百分之五十以上，且证券撤回申报额在一千万元以上、撤回申报的期货合约占用保证金数额在五百万元以上的；

（七）实施操纵证券、期货市场行为，违法所得数额在一百万元以上的。

■ 情节严重的情形

操纵证券、期货市场，违法所得数额在五十万元以上，具有下列情形之一的，应当认定为刑法第一百八十二条第一款规定的“情节严重”：

（一）发行人、上市公司及其董事、监事、高级管理人员、控股股东或者实际控制人实施操纵证券、期货市场行为的；

（二）收购人、重大资产重组的交易对方及其董事、监事、高级管理人员、控股股东或者实际控制人实施操纵证券、期货市场行为的；

（三）行为人明知操纵证券、期货市场行为被有关部门调查，仍继续实施的；

（四）因操纵证券、期货市场行为受过刑事追究的；

（五）二年内因操纵证券、期货市场行为受过行政处罚的；

（六）在市场出现重大异常波动等特定时段操纵证券、期货市场的；

（七）造成恶劣社会影响或者其他严重后果的。

■ 情节特别严重的情形

（一）持有或者实际控制证券的流通股份数量达到该证券的实际流通股份总量百分之十以上，实施刑法第一百八十二条第一款第一项操纵证券市场行为，连续十个交易日的累计成交量达到同期该证券总成交量百分之五十以上的；

（二）实施刑法第一百八十二条第一款第二项、第三项操纵证券市场行为，连续十个交易日的累计成交量达到同期该证券总成交量百分之五十以上的；

（三）实施本解释第一条第一项至第四项操纵证券市场行为，证券交易成交额在五千万元以上的；

（四）实施刑法第一百八十二条第一款第一项及本解释第一条第六项操纵期货市场行为，实际控制的账户合并持仓连续十个交易日的最高值超过期货交易所限仓标准的五倍，累计成交量达到同期该期货合约总成交量百分之五十以上，且期货交易占用保证金数额在二千五百万元以上的；

（五）实施刑法第一百八十二条第一款第二项、第三项及本解释第一条第一项、第二项操纵期货市场行为，实际控制的账户连续十个交易日的累计成交量达到同期该期货合约总成交量百分之五十以上，且期货交易占用保证金数额在二千五百万元以上的；

（六）实施操纵证券、期货市场行为，违法所得数额在一千万元以上的。

■ 情节特别严重的情形

实施操纵证券、期货市场行为，违法所得数额在五百万元以上，并具有以下情形之一的，应当认定为“情节特别严重”。

（一）发行人、上市公司及其董事、监事、高级管理人员、控股股东或者实际控制人实施操纵证券、期货市场行为的；

（二）收购人、重大资产重组的交易对方及其董事、监事、高级管理人员、控股股东或者实际控制人实施操纵证券、期货市场行为的；

（三）行为人明知操纵证券、期货市场行为被有关部门调查，仍继续实施的；

（四）因操纵证券、期货市场行为受过刑事追究的；

（五）二年内因操纵证券、期货市场行为受过行政处罚的；

（六）在市场出现重大异常波动等特定时段操纵证券、期货市场的；

（七）造成恶劣社会影响或者其他严重后果的。

■ 未经处理部分，累计计算

二次以上实施操纵证券、期货市场行为，依法应予行政处理或者刑事处理而未经处理的，相关交易数额或者违法所得数额累计计算。

■ 特定情形下的数额认定

“违法所得”是指通过操纵证券、期货市场所获利益或者避免的损失。

“连续十个交易日”，是指证券、期货市场开市交易的连续十个交易日，并非指行为人连续交易的十个交易日。

■ 单位犯罪的处罚

单位实施该罪行为的，依照前述的定罪量刑标准，对其直接负责的主管人员和其他直接责任人员定罪处罚，并对单位判处罚金。

4.“自己实际控制的账户”的认定

（一）行为人以自己名义开户并使用的实名账户；

（二）行为人向账户转入或者从账户转出资金，并承担实际损益的他人账户；

（三）行为人通过第一项、第二项以外的方式管理、支配或者使用的他人账户；

（四）行为人通过投资关系、协议等方式对账户内资产行使交易决策权的他人账户；

（五）其他有证据证明行为人具有交易决策权的账户。

有证据证明行为人对前款第一项至第三项账户内资产没有交易决策权的除外。

5.典型案例

案例一：朱某某操纵证券市场案

基本案情：被告人朱某某，原系国开证券有限责任公司某证券营业部（以下简称国开证券营业部）证券经纪人，上海电视台第一财经频道《谈股论金》节目（以下简称《谈股论金》节目）特邀嘉宾。

2013年2月1日至2014年8月26日，被告人朱某某在任国开证券营业部证券经纪人期间，先后多次在其担任特邀嘉宾的《谈股论金》电视节目播出前，使用实际控制的三个证券账户买入多支股票，于当日或次日在《谈股论金》节目播出中，以特邀嘉宾身份对其先期买入的股票进行公开评价、预测及推介，并于节目首播后一至二个交易日内抛售相关股票，人为地影响前述股票的交易量和交易价格，获取利益。经查，其买入股票交易金额共计人民币2094.22万余元，卖出股票交易金额共计人民币2169.70万余元，非法获利75.48万余元。

裁判要旨：证券公司、证券咨询机构、专业中介机构及其工作人员违背从业禁止规定，买卖或者持有证券，并在对相关证券作出公开评价、预测或者投资建议后，通过预期的市场波动反向操作，谋取利益，情节严重的，以操纵证券市场罪追究其刑事责任。证券公司、证券咨询机构、专业中介机构及其工作人员，违反规定买卖或者持有相关证券后，对该证券或者其发行人、上市公司作出公开评价、预测或者提出投资建议，通过期待的市场波动谋取利益的，构成“抢帽子”交易操纵行为。发布投资咨询意见的机构或者证券从业人员往往具

有一定的社会知名度，他们借助影响力较大的传播平台发布诱导性信息，容易对普通投资者交易决策产生影响。其在发布信息后，又利用证券价格波动实施与投资者反向交易的行为获利，破坏了证券市场管理秩序，违反了证券市场公开、公平、公正原则，具有较大的社会危害性，情节严重的，构成操纵证券市场罪。

三、企业如何应对刑事调查

在上一期《2017-2018中国年度合规蓝皮书》中，我们分享了关于“企业如何有效防范刑事合规风险”的经验、做法。防范刑事合规风险属于刑事合规业务的前期工作，是对企业运营风险的预判、排查。而应对刑事调查活动则是刑事合规业务的后期工作，是对具体合规问题的紧急处置。我们在此探讨的刑事调查活动是指刑事立案之前的初查阶段。刑事立案之后案件进入刑事诉讼程序，严格来讲此阶段已经不属于刑事合规范畴，此时相关涉案人员人身自由有较大可能处于受限状态，企业能够开展的工作较为有限，更多工作还需要依靠专业刑事辩护律师来完成。

（一）刑事调查的法律依据

目前，国内有多部法律法规、司法解释赋予相关执法机关依法开展刑事调查的权力，例如：《中华人民共和国监察法》、《公安机关办理刑事案件程序规定》、《人民检察院刑事诉讼规制（试行）》、《最高人民法院、最高人民检察院、公安部关于办理刑事案件收集提取和审查判断电子数据若干问题的规定》、《最高人民法院、最高人民检察院、公安部、司法部关于办理恐怖活动和极端主义犯罪案件适用法律若干问题的意见》、《最高人民检察院、公安部关于公安机关办理经济犯罪案件的若干规定》等。

（二）刑事调查可查看、调取的证据范围

我们不逐一详释所有法律法规、司法解释对刑事调查的赋权范围，仅在此摘选一条与企业经营联系较为密切的法条展开说明。《最高人民检察院、公安部关于公安机关办理经济犯罪案件的若干规定》第十八条规定，在立案审查中，发现案件事实或者线索不明的，经公安机关办案部门负责人批准，可以依照有关规定采取询问、查询、勘验、鉴定和调取证据材料等不限制被调查对象人身、财产权利的措施。经审查，认为有犯罪事实，需要追究刑事责任的，经县级以上公安机关负责人批准，予以立案。

依照条文规定，公安机关办理经济犯罪案件在立案前可以采取的调查措施有询问、查询、勘验、鉴定和调取证据材料等措施，不能采取限制被调查对象人身、财产权利的措施。通过比对不难发现，公安机关仅在立案前的调查阶段几乎能够查看、收集刑事诉讼法规定的所有证据种类，可以说刑事调查的权限范围是非常大的。

公安机关可以采取的调查方式	可能获取的对应“证据种类”
询问	证人证言 被害人陈述 犯罪嫌疑人、被告人供述和辩解
查询	书证等
勘验	勘验、检查、辨认、侦查实验等笔录 视听资料、电子数据
鉴定	鉴定意见
调取证据材料	物证（或书证等）

（三）企业应对刑事调查的措施

立案前的刑事调查将直接决定案件的最终走向，或者认为无违法犯罪事实不予立案，或者立案侦查进入刑事诉讼程序。从刑事办案的实践来看，案件越在早期作非罪化处理阻力越小、损失越低，而越在刑事诉讼的后期，难度越大，企业面临的损失也会越高。企业能否积

极配合执法、正确应对刑事调查显得尤为关键。

1. 提升应对能力、缓解紧张情绪

在以往的工作中我们发现，相关人员在接受执法机关调查询问时往往会比较紧张，在回答问询环节常出现的情况是刻意回避自身责任，将问题“踢给”他人。例如，“我不负责这块业务”、“我负责全面工作，没具体经手这件事”、“我只负责钱款出入，业务是否真实不归我管”、“我印象中当时应该是XX总具体负责”、“我的签字只是例行公事，决定权在XXX那，具体你应该问他”…，有时甚至会出现所有人员均声称不知情的局面，进而引发执法人员更为深入的新一轮调查。我们理解相关人员面对刑事调查问询的紧张心理，更多源于对刑事调查缺乏了解而产生的莫名恐慌，继而采取将问题推给别人的方式应对问询对其来讲最为踏实、稳妥，但从实际效果来看，这显然不是好的策略。在企业日常的刑事合规培训中，应加强企业管理人员、工作人员能力培养，正确看待刑事调查工作，将配合、应对刑事调查当作自己日常工作的一部分，以合作的心态与执法人员相处，真正化解内心紧张情绪。

2. 配合调查检查，诚实有效互动

在克服紧张情绪的基础上，相关人员应当尽量通过交流与执法人员建立良性互动。回答问询时态度诚恳、依据合理，回答内容前后一致，既要尊重执法，又不刻意迎合，坚持实事求是。对于执法人员提出的调查要求应采取合作态度，不阻挠、破坏甚至抵抗执法行为。通过良性的互动，努力与执法人员建立互信、有效互动关系，并借此获取同执法人员合理讨论问题的机会，了解案件的基本定性，阐述自身抗辩事由。

3. 客观审慎阐述事实，准确提供证据材料

企业要高度重视执法机关的第一次介入调查工作。在一般的办案意识中，相关人员第一次接受问询的笔录，以及第一次调查执法过程中收集到的物证、书证、电子数据等证据都具有较强的证明力，尤其是第一次问询的内容，即便未来相关人员作出其他不同的回答，都较难改变办案人员在先形成的第一判断。基于此，公司及相关人员在阐述事实意见，提供证据材料时要客观审慎。客观审慎不是表现为吞吞吐吐、犹犹豫豫，而是尊重事实，对于不清楚或已遗忘的事实不妄加推测，如实表述，避免提供与案件无关甚至会误导调查方向的证据材料，避免事态扩大。

4. 积极提交证据，充分陈述申辩

面对执法调查、侦查活动，不应一味被动应对，还需要及时收集证据，尽早向执法机关提交，充分陈述申辩。消极应对刑事调查，将会失去澄清事实的宝贵机会，使公司在案件的处理过程中陷于十分不利的境地。企业要及时提交证据，积极开展专业有效的主动申辩，争取执法机关的充分理解和支持。实践中，刑事调查阶段处在立案之前，此时相关人员尚未被采取强制措施，具有一定的人身自由，是企业及管理人员主动收集、提交证据的关键窗口期，也可能是相关人员被限制人身自由之前最好的自证无罪的机会，要充分利用申辩机会，最大化减少不利影响，防止案件进入立案、侦查等后期的刑事诉讼阶段。

5. 及时从外部律师团队处获取专业的法律咨询

企业涉及的刑事法律问题具有较强的专业性，有关职务犯罪、涉计算机网络犯罪、证券期货类犯罪、涉税犯罪、走私犯罪等专业领域的法律适用问题都要求相关人员具有丰富的应对执法调查的经验及扎实的法律专业知识，因此，面对刑事调查活动，涉案公司及人员应第一时间寻求有经验的合规律师的帮助，争取在调查之初尽

早介入，有效防控法律风险。律师作用主要体现在，能够帮助当事人了解涉嫌罪名的构成要件、具体认定及处罚标准；充分讲解诉讼流程、证据收集、采信规则；培训相关人员冷静应对调查。

上述建议仅是针对刑事调查的一般性应对建议。考虑到刑事问题的复杂性和个案之间差异性等因素，企业还需要针对不同案件的执法重点及证据情况就应对策略作相应调整。