CAICT 中国信通院

全球信息通信监管改革趋势报告

（2020 年）

中国信息通信研究院政策与经济研究所

2020 年 10 月

版权声明

本报告版权属于中国信息通信研究院，并受法律保护。转载、摘编或利用其它方式使用本报告文字或者观点的，应注明“来源：中国信息通信研究院”。违反上述声明者，本院将追究其相关法律责任。

前　言

当今世界，科技革命和产业变革日新月异，数字经济蓬勃发展，深刻改变着人类生产生活方式，对经济社会发展、全球治理体系、人类文明进程影响深远。各国都在加快布局数字经济，抢占产业数字化、数字产业化发展先机。在全球新冠疫情冲击下，传统经贸活动受到严重影响，数字经济显现出更强的抗冲击力和发展韧性，“非接触”模式为经济社会稳定运行提供了有力支撑，未来还将承担起进一步培育新动能、促进新消费、推动传统产业转型等重要使命，危与机并存。

面向支撑经济社会数字化转型发展的新使命，国际电信联盟提出数字生态系统下的行业监管转型方向，强调构建综合性、协同化监管模式来促进信息通信技术支撑社会、经济和环境的可持续增长。新冠肺炎疫情发生后，国际电信联盟提出应建立一个适应性强且复原力强的协作监管系统，同时科学使用数字化监管手段，更好地重建和推动数字化转型。顺应这些趋势，全球各个国家和地区的信息通信监管视野逐渐从促进行业本身的健康发展，向推动整个经济社会发展和应对万物互联背景下的各类新挑战转变，加快重塑行业监管体系，积极推行监管改革。

本报告跟踪观察近年来国际组织和重要国家地区在信息通信监管方面的革新历程，总结了在监管目标、职能、方式、手段方面的最新态势，梳理了近两年来各重点领域的主要进展，对下一步全球信息通信监管改革趋势进行了展望。

目 录

一、全球信息通信监管加快转型以适应数字经济发展.....1
（一）监管目标全面升级，为提升各国数字竞争力提供战略支撑.....1
（二）监管职能不断拓展，将新技术新业务新要素纳入监管范畴.....3
（三）监管方式更加灵活，为数字经济创新营造包容审慎的发展环境.....6
（四）监管机制迈向协同，多方共治成为应对融合发展趋势的共同选择.....10
二、全球信息通信监管重点领域改革进展.....13
（一）市场准入管理：放松业务定义限制适应 ICT 跨界发展趋势，云计算等新业务逐渐被纳入准入管理.....14
（二）市场竞争监管：灵活运用竞争监管手段促进网络基础设施投资，数字平台成为反垄断新热点.....16
（三）新技术新业务监管：创新监管方式，着力平衡技术红利释放与未知风险防范.....18
（四）用户权益保护：新技术滥用的新问题备受关注，各国建立长效机制积极应对.....20
（五）宽带网络建设：宽带网络向双千兆网络演进，加大普遍服务投入成为政策重点.....23
（六）频谱资源管理：5G 频谱分配进程持续加速，专网频谱分配取得实质性进展.....26
（七）互操作性管理：OTT 通信与数据互操作性议题进入视野，着力推动多层面的有效互通.....29
（八）网络信息安全管理：网络和数据安全保障热度持续，违法内容管控不断强化.....30
三、 全球信息通信监管改革趋势展望.....34
（一）实现全面的数字连接仍是信息通信监管的首要目标.....34
（二）加快 5G 等新型基础设施建设将是未来一段时期的战略重点.....35
（三）更好适应数字经济发展特点将是监管方式创新的重要方向.....36
（四）释放数据价值和强化数据治理成为各国发展数字经济的关键着力点...37
（五）强化数字平台治理成为信息通信监管的普遍趋势.....37
（六）多方协同的治理机制在应对融合性监管挑战中的作用将进一步凸显...38

一、全球信息通信监管加快转型以适应数字经济发展

数字经济深入发展带来的行业融合挑战原有的监管模式和框架，最大化释放数字经济潜力需要敏捷、创新、协作式的新型监管模式。信息通信行业作为各行各业的关键支撑和连接纽带，更是要求信息通信监管与时俱进、锐意改革、大胆创新，适应数字化转型新形势、新要求。根据 ITU 的最新研究显示，全球目前正在从面向信息通信业的特定行业监管向面向数字化转型的跨部门协同监管转变，监管目标、监管职能、监管方式、监管体制等各个方面正在进行深刻调整。

（一）监管目标全面升级，为提升各国数字竞争力提供战略支撑

信息通信行业的监管目标是跟随技术经济的发展不断进行调整的过程。随着经济社会数字化转型浪潮的到来，国际组织、全球主要经济体纷纷将服务数字经济和社会发展作为信息通信监管目标。同时，在大国竞争和博弈日益加剧的背景下，信息通信行业作为科技竞争的核心领域，监管目标被赋予了不同往日的新内涵。

全球信息通信行业普遍以全面服务经济和社会的综合监管为目标。当前世界正进入数字化全联接的智能时代，万物感知、万物互联，万物智能成为主要特征。以 5G、大数据、人工智能等为代表的新一代信息通信技术开辟了生产生活的新空间，提供了全球发展的新动力。适应发展需要，ICT 行业监管经过几代演进升级，转变为以服务经济社会发展为主导的综合监管目标。国际电信联盟认为，全球信息通信监管经历了五代演进历程。其中，第一代监管目标是鼓励改善国

有垄断电信业务经营的效率和服务，第二代监管目标是以实现部分私有化促进有效竞争，第三代监管目标是保护基础设施投资、服务质量和消费者权益。第四代监管目标，也即各国当前普遍的监管目标是激励跨界融合竞争、促进业务创新、保障网络信息安全、提升消费者福利，在数字生态系统环境下进行融合型监管。此外，部分国家已率先进入第五代监管，愈加重视以跨部门协同监管促进经济社会发展，提升国家竞争力和领导力。2020 年国际电信联盟以“连通目标 2030：利用 ICT 促进可持续发展目标的实现”作为世界电信和信息社会日主题，指出利用 ICT 改善人们生活、促进社会经济发展已成为全球愿景。国际电信联盟第 20 届全球监管机构专题研讨会提出，应建立具有适应性且恢复能力强的协作监管系统，更好地重建和推动数字化转型，应对新冠疫情挑战。

全球数字经济竞争逐步升级，各国将加快下一代信息通信基础设施建设作为其监管目标的重中之重。各国将 5G 等信息通信技术作为引领下一次工业革命的引擎，把建设信息通信基础设施视为掌握全球领导力的关键。美国联邦通信委员会（以下简称“FCC”）近十余年来始终将宽带发展作为重要战略规划目标，《2018-2022 战略》中专门制定发布 5G 加速发展计划，强调释放频谱、促进投资，促进 5G 网络发展；同时美国正加快部署 6G 技术，并计划布局 6G 卫星网络。欧洲电子通信管理机构（以下简称“BEREC”）《5G 雷达指南》[1]将 5G 列为战略优先事项，致力于在统一监管框架下，释放 5G 在创新、

[1] Guide to the BEREC 5G Radar，BEREC 2020 年 6 月发布。

生产和促进增长方面的潜力；BEREC《2021-2025 战略》将促进高容量网络连接、提高竞争和有效投资、推动欧洲内部市场发展、提升欧盟公民利益列入监管目标。此外，为进一步适应数字经济发展态势，欧盟在 2020 年初密集推出《建设欧洲的数字未来》《欧洲数据战略》《人工智能白皮书》等数字经济相关政策文件，提出加快建设云服务中心、数据空间等新型信息通信基础设施，打造数字经济时代具有竞争力的经济体。英国通信管理局（以下简称“Ofcom”）《2020-2021 年度计划》提出将建设世界级的数字基础设施作为首要优先事项。韩国科学技术信息通信部（以下简称“MSIT”）在《2020 年度计划》中提出，创造以数据、网络、人工智能为基础的倡导创新的一流国家。

（二）监管职能不断拓展，将新技术新业务新要素纳入监管范畴

随着信息通信产业对数字化转型的作用不断凸显，为适应数字经济发展新要求、新挑战，信息通信监管机构的职能在以通信网络为核心的传统职能[2]基础上，不断向应用、数据、内容以及物联网、AI 等新领域拓展。一方面，伴随数据要素和新技术新业务发展，信息通信监管职能做出相应扩张或调整；另一方面，监管职能重点逐渐从经济性监管转向社会性监管，即从市场准入、价格管制、互联互通为主，转向以网络安全、内容管理、个人隐私为主，构筑安全、可信、可靠的数字经济生态环境。

物联网等新技术新业务发展促进监管机构职能延伸拓展。服务物

[2] 普遍服务、价格管制、互联互通、码号分配、频谱分配、服务质量、设备认证等。

联网（IoT）等新一代信息通信技术的发展，各国监管机构一方面开展制定战略、推动标准、加大投入等工作，另一方面，调整原有的市场准入、资源管理、设备入网、网络安全等管理职能和增设新职能以适应新技术新业务衍生出的新特征和新要求，并加强与其他机构及主体的协同监管。例如，**在市场准入方面**，欧盟《2018 年电子通信法指令》首次明确将机器对机器(M2M)通信视为电子通信网络和服务的一种，纳入其一般授权体系管理。**在码号资源方面**，日本总务省（以下简称“MIC”）2019 年 5 月宣布计划为 IoT 设备创建约 100 亿个 14 位数字的电话号码，而日本的传统电话号码是 11 位数字。欧盟《2018 年电子通信法指令》建议各成员国通信监管机构在技术可行的情形下，通过空中提供（over-the-air provisioning）的方式，在无需物理访问相关设备的情形下，实现对通信设备标识符的重新编程和通信服务提供商转换，促进物联网等新兴技术的发展。**在设备入网方面**，日本 MIC 计划从 2020 年 4 月开始，通过型号核准方式确保上市的 IoT 终端设备符合可远程接入控制、允许用户修改默认身份和密码设置、可对固件进行升级三项条件。英国政府在 2020 年 1 月宣布将通过立法强制 IoT 设备满足部分强制性要求，例如 IoT 设备密码必须唯一且不能重置为出厂通用设置。**在设备安全方面**，日本 MIC 突破《非授权计算机访问禁止法》限制，从 2019 年 2 月开始与国家信息通信技术研究院、互联网企业共同合作，主动对互联网上的 IoT 设备进行扫描，以识别出未恰当设置密码的 IoT 设备，并通知相关用户完善密码设置。

促进数据资源开放、共享和利用等成为 ICT 监管机构新职能。过去，ICT 监管机构对数据的关注主要集中在个人信息保护上。随着数据成为一种关键生产要素，释放数据资源潜力成为新的监管职能，部分国家 ICT 监管机构开始推动数据的开放、共享和利用，并力图在释放数据潜力和保护个人隐私之间做出平衡。2018 年，**日本**总务省与经济产业省（METI）合作推出“信息库”（information banks）认证机制，确保个人信息以可信的方式被开发利用，平衡个人隐私保护和数据利用之间的冲突。目前，日本信息技术协会被授权开展信息库认证工作，通过认证的信息库行使信息委托功能，替代个人管理并提供数据给第三方利用。其中，认证标准、信息委托示范协议主要事项、信息委托认证方案由总务省和经济产业省通过制定指南来具体规范。**新加坡**信息通信媒体发展局（以下简称“IMDA”）同时兼具个人数据保护（通过下设的个人数据保护委员会（PDPC））和数据创新职能，其在 2019 年 6 月推出“可信数据共享框架”，支持企业探索安全且经济可持续的数据共享机制，促进组织间的可信数据共享。同时还推出数据监管沙箱，使企业通过与 IMDA 和 PDPC 协商，可在一个安全环境中探索数据的创新使用，降低企业合规风险和用户风险。**英国** Ofcom 一方面将通信行业相关数据开放给公众使用，另一方面正在英国政府授权下制定“开放通信计划”，拟使消费者能够简单、安全地与第三方共享其在通信服务中产生的数据。欧洲 BEREC 目前也正在研究探索以数据为中心的监管方法和数据驱动的监管原则，以实现数字经济环境下的监管目标和消费者赋能。

确保 5G 等信息通信设施供应链安全的新要求赋予监管机构更多权力。根据 ITU 的统计，截至 2018 年，在 173 个国家中，有 55%的国家其 ICT 监管机构负有网络安全监管责任，比 2009 年提升了近 10%。随着信息通信基础设施在数字化转型中的支撑作用日益增强以及大国间博弈的不断升级，各国近年来增强了对 5G 等信息通信基础设施的供应链安全管制，信息通信监管机构也相应在 5G 网络运营商和设备供应商管理中被赋予更多监管和执法权力。**欧盟**在 2020 年 1 月发布的《5G 网络安全风险缓解措施工具箱》中建议，强化各国监管机构作用，提升监管机构监管权力，包括可对运营商施加增强型义务（例如关于信令、管理平面的安全义务），同时有权事前限制、禁止 5G 网络设备的供应、部署和运营。**英国**政府在 2019 年 7 月对电信供应链安全进行了评估，并决定建立一个新的、更强大的 5G 和全光纤网络安全框架，打造可持续且多样化的电信供应链。为此，将授权 Ofcom 与相关政府部门一起制定一套新的电信安全要求，提升安全标准,并监督电信运营商的执行。同时还计划通过立法赋予 Ofcom 更多权力开展相关执法工作。**美国 2020 年 3 月**发布《2019 年安全可信通信网络法》，授权 FCC 定期编制、发布构成国家安全威胁的通信设备和服务清单，禁止获得普遍服务基金支持的运营商购买或维护该清单上的设备和服务，并授权 FCC 建立补偿计划来弥补运营商更换设备和服务的损失。目前中兴、华为两家中国企业已经被列入清单。

（三）监管方式更加灵活，为数字经济创新营造包容审慎的发展环境

数字生态系统不断扩张，信息通信监管机构面临着前所未有的冲突和挑战。他们需要在监管的是与否、收与放之间不断权衡，在促进创新和保护市场投资者的长期投资动力之间反复考量，还面临着前所未有的消费者隐私保护、安全保护方面的压力。为此，需要采取更具平衡性、灵活性、包容性和审慎性的监管方式进行应对。

从基于具体规则的监管方式向基于原则和结果的监管方式转变。新一代信息通信技术与社会应用融合所带来的创新多样性和不可预测性，需要更具弹性、适应性和可操作性的监管方式，避免僵化、静态的监管。传统的基于规则的监管被认为过于僵化，难以留出足够的发展空间。因此，近年来 ITU 和部分发达国家提出了在数字化转型过程中使用基于原则的监管方式[3]，以适应快速变化的技术和市场环境。基于原则的监管聚焦于预期结果，而不事先做出过多详细的限制性规定（例如必须遵循特定程序），将细节留给可以更加灵活调整的指南、行为规范、认证规则去规定。例如，欧盟《一般数据保护条例》中规定了数据最小化、目的限制、存储限制等七项个人数据保护原则，而企业具体如何有效遵守还需要依赖后续出台的指南、官方解释以及与监管机构的沟通等。ITU 认为，基于原则的监管更适合在复杂的数字经济环境中找到平衡、有效的解决方案，即使制定详细规则的监管方式不会完全消失，未来的监管也将逐渐转向基于原则的监管。基于此，ITU 提出了前瞻性、整体性、可持续发展、基于证据、市场导向、激

[3] 基于原则的监管（principle-based-regulation）基于原则的监管起源于次贷危机爆发后的金融监管，主要是指以高层次的原则作为手段来实现监管目标，而较少依赖于事先制定的详细规则（即基于规则的监管，rule-based regulation）实施监管。采用基于原则的方法并不意味着完全放弃了规则，而是始终将一般原则与特殊规则（specific rule）相结合（例如指南、行为规范、认证规则），并不断地在两者之间寻找平衡点。同时，在寻找平衡点的过程中更多地依赖于原则，尽量少用具体规则。

励性、促进创新、包容性以及技术中立等九条高层原则供各国制定数字化转型政策时参考。英国上议院在 2019 年发布的《数字世界的监管》报告中同样指出，对数字服务应采取基于原则的监管方式，提出了平等、问责、透明、开放、道德、隐私权等十项数字领域的监管原则。《欧洲数据战略》也提出对构建跨部门的数据治理框架要避免过于详细、严格的事前监管，应采用有利于试验、迭代和差异化的敏捷治理方法，并基于这一原则进行立法。基于原则的监管对监管机构的监管智慧、协调多利益相关方的能力都提出了更高的要求。

强调基于证据的科学审慎监管，避免基于预设风险的事先监管。ITU 以及美国、英国、澳大利亚等主要国家，目前都强调采取基于证据的监管方式，增强监管决策的针对性和有效性，以防因主观预测失准而对数字基础设施和服务的发展做出错误的事先干预。基于证据的监管包含如下几个特征：一是监管决策要依赖于持续收集的数据和事实，以及数据分析和经济分析结果，例如英国 Ofcom 指出，“基于证据的监管者”其决策制定依赖于各类定期或临时性的市场研究。二是要通过公开听证会、公开征询意见、专业研讨会议等方式广泛收集和听取利益相关方意见。三是应采取与风险相称的针对性措施来解决市场中的实际问题，而不是采取宽泛的事前管制措施来防范新技术、新业务可能带来的损害风险。例如韩国在 2018 年出台的《工业融合法》、《信息通信技术融合促进特别法》中，对融合类新产品和新服务确立了“先发展后管制”的原则，明确只有在其使用过程中对人类生命和安全产生了实际威胁，政府才能采取限制措施。欧洲 BEREC

从 2020 年开始启动数字平台对消费者的影响研究，预期在 2021 年完成最终报告，其目的是在基于证据的基础上理解超大型数字平台的相关影响并采取下一步行动。四是积极利用数字技术和数据资源来辅助决策。例如，澳大利亚 ACMA 正在积极推动基于证据的数据驱动型监管，通过采用数据科学、大数据、物联网、AI 和预测分析技术，使其能在强大的证据基础上快速识别和应对威胁，实现精细化监管。

推出监管沙箱建立容错机制包容数字化融合创新业务发展。“监管沙箱”是一种容许新模式新业态突破现有法律法规，进行试验性发展的新型监管制度。“监管沙箱”最早由英国率先在金融科技领域应用实施，目前应用范围已经从金融科技向更广泛的 ICT 融合监管领域应用延伸，应用地区也扩展到美国、澳大利亚、新加坡、日本、韩国、中国等全球 30 多个国家。**韩国**于 2018 年修订《信息通信融合法》《行政监管基本法》等相关法律，率先在 ICT 融合领域系统性实施监管沙箱制度，明确凡是不妨碍国民生命安全的新技术新业务，均可在接受相关监管部门监管、履行相关责任义务的前提下，突破现有法律规定试验性开展，目前已初步取得成效。自 MSIT 从 2019 年推出 ICT 监管沙箱以来，共批准了 40 项申请，有 16 种新技术新业务投放市场，涉及共享经济、行政管理、在线医疗、虚拟现实等多个领域。**日本**政府推出监管沙箱制度，帮助国内外企业在有限时间段和范围内开展新技术新模式的示范项目，打破由上至下的传统监管框架及行业分类对创新的束缚。日本的监管沙箱对技术类型和行业没有限制，尤其是鼓励物联网、人工智能、大数据和区块链的发展，截至 2020 年 2 月，

共有 129 家企业的相关项目在监管沙箱中运营。典型案例包括使用诊断工具在线诊断流感；建立交易平台实现加密货币交易所之间的比特币实时买卖和结算；对集成了高速电力线通信设备的家用电器进行实用性测试等。

（四）监管机制迈向协同，多方共治成为应对融合发展趋势的共同选择

数字经济在加快发展、深化产业融合创新的同时，也给信息通信业监管带来了职责交叉、监管对象激增等新的挑战。要想最大化释放数字经济潜力，就需要建立权责更明确、合作更密切的监管机制，因此跨部门间的协作型监管成为数字经济时代下各国监管部门的必然选择。各国的主要做法包括以下四种模式：

在国家层面建立高规格领导机构，负责数字经济监管顶层设计，统筹和强化跨部门协作。例如，**韩国**在 2018 年成立信息和通信技术战略委员会，由总理担任委员会组长，科学技术信息通信部长担任执行秘书，负责制定促进信息通信技术融合创新发展的相关法律法规，以及对各部门之间尚未明确的监管职责进行协调。**日本**成立创新业务活动评估委员会，其成员由日本首相直接任命，该委员会负责对申请进入监管沙箱的企业进行评估，并协调相关部门承担监管职责。**英国**上议院 2019 年提出，建议成立一个新的机构“数字化局”，负责制定数字经济监管框架，统筹和协调各部门监管职责。

在存在职责交叉的领域，通过签署部门间备忘录等方式划分监管职责，加强跨部门协作，防止监管缺位、越位。根据 ITU2018 年的报

告显示，信息通信监管机构与其他行业监管机构的部门间协作包括正式（如签署备忘录）、半正式（如一次性的联合计划或临时委员会）和非正式（如无制度性合作框架）三种。在竞争监管、用户权益保护、频谱分配三个领域，由于长期以来一直存在职能交叉或者需共同解决的问题，因此跨部门合作在全球各国都较为常见，而在金融、能源等新兴融合领域，部门间协作仍较少见。**从竞争监管来看，美国**的 FCC 与联邦贸易委员会（FTC）、司法部（DOJ）分工合作。FCC 负责电信领域的竞争监管，FTC 负责互联网和计算机等高科技领域的竞争监管。同时，FTC 与司法部签署备忘录，明确各自在信息通信领域反垄断案件调查中的负责领域，并成立融合委员会，每两年进行一次职责划分评估更新。**英国** Ofcom 与竞争和市场管理局（CMA）签署备忘录，双方共同在实际监管工作中确定对具体违法竞争行为的管辖权，并通过信息共享和调查协助的方式实现高效协同。**从隐私保护来看，美国** FCC 与 FTC 签署备忘录，FCC 负责电信运营商的隐私监管，要求电信运营商应遵守“用户专用网络信息（CPNI）”的相关规则。FTC 负责互联网等行业的隐私监管，要求企业制定全面的隐私保护计划，不得非法获取用户信息，并对违反相关法律法规的企业进行处罚。**英国** Ofcom 与隐私保护机构英国信息专员办公室（ICO）签署备忘录，由 ICO 负责涉及用户隐私问题的调查和执法工作，Ofcom 负责对滥用通信网络或服务导致用户隐私泄露的问题进行监管。

对于尚未明确监管部门的新技术新业务，通过组建多方参与的专业研究小组，对其发展趋势及可能带来的监管挑战进行前瞻性研究。

在人工智能、物联网、区块链等新技术新业务领域，大部分国家还未明确具体的监管部门，主要通过成立专门的研究小组或调查委员会的方式，推进监管系统性、前瞻性研究。**在平台监管方面，**2018 年 10 月，**日本** MIC、日本经济省（METI）和公平贸易委员会（JFTC）共同成立研究小组，负责研究数据经济平台运营的基本原则和具体措施。**在物联网方面，**2017 年 3 月，日本经济省和总务省成立联合小组，共同研究制定促进物联网产业发展、保障网络安全、制定技术标准等相关政策。**在人工智能方面，**2016 年 10 月，**日本** MIC 集合来自学术界、产业界和政府机构的成员组成 AI 治理调查委员会，共同制定 AI 使用原则和应用指南，并对相关产业发展的影响和预期风险进行评估。2018 年 5 月，**美国**白宫在美国国家科学技术委员会（NSTC）下设立人工智能特别委员会，聚集美国国家科学基金会和国防高级研究计划局等多个部门官员，共同负责确定人工智能技术对美国的优先级和相应的投资力度。**在区块链方面，**2018 年 3 月，**美国**联邦贸易委员会（FTC），组织其内部人员及业内专家成立区块链工作组，研究区块链技术特别是加密货币对贸易的影响，以及研究不法分子如何利用区块链技术误导或欺骗消费者、扰乱竞争。同时通过资源共享和聘请外部专家的方式，提升该机构关于区块链技术的相关专业知识积累。

除政府主导、跨部门协同以外，监管机构不断加强与行业协会、非营利组织的协同共治。一方面，监管机构将部分职责委托给第三方组织，授权其对相关市场主体进行监管。例如，**英国** Ofcom 委托非

盈利机构 PhonepayPlus 对增值业务进行监管。Ofcom 可派驻代表进入 PhonepayPlus 董事会，并对其制定的监管规则进行审批。**美国**在 2019 年 12 月通过治理非法自动语音电话相关立法，明确 FCC 可以授权私营部门领导的中立第三方组织来负责可疑非法自动语音电话的追溯。**日本** MIC 委托第三方机构“数据交易市场工作组”开展用户个人信息保护工作。该工作组主要负责监督相关企业的相关活动，如是否在商业活动中使用用户个人信息前征求用户同意、是否在用户询问个人信息保护情况时给予明确答复等。**另一方面，行业协会等组织积极参与行业监管，通过制定自律公约，协助政府与监管机构管理市场。**例如，**英国**互联网服务提供商协会（ISPA），主要负责促进互联网行业公平竞争、推动互联网行业发展和自律。ISPA 制定了行业自律公约，约束成员合法经营并遵守 PhonepayPlus 的管理要求。同时 ISPA 还代表互联网服务提供商向英国商业、创新和技能部（BIS）、Ofcom 等政府机构提出监管意见与建议。

二、全球信息通信监管重点领域改革进展

随着信息通信行业的不断转型、融合与演进，各国信息通信监管机构亦根据本国国情和数字化转型要求，通过灵活多样的监管措施来适应信息通信行业发展的新特征、新需求:引入更为灵活包容的许可方式促进 ICT 业务的融合发展；市场竞争管理日渐倾向于服务信息通信基础设施发展的需要，不断放松对电信运营商的限制；努力谋划和创新管理方式以最大化释放新技术新业务发展；通过加强立法、执法和监管来解决数字经济发展过程中衍生的网络欺诈、隐私侵犯、网络

数据安全等问题；将促进高速宽带等基础设施的快速发展和普及作为首要优先事项，着力提升频谱资源使用效能；同时，将一些此前给予较少关注的新兴市场主体（如互联网平台）和新业务(如 OTT 通信、云计算)逐渐纳入监管视野。

（一）市场准入管理：放松业务定义限制适应 ICT 跨界发展趋势，云计算等新业务逐渐被纳入准入管理

自电信市场打破国有垄断之后，各个国家和地区纷纷建立起适应自身情况的市场准入制度，并对进入市场的经营者其权利和义务进行规定。尽管不同国家信息通信市场准入制度存在很大差异，但总体上形成了分级分类管理的模式，即对于稀缺性资源、基于设施的业务、设施规模较大的业务或者对消费者权益和安全影响较大的业务，倾向于采用较严格的个别许可证管理；对于其他业务实施登记、备案、通知等较宽松的许可方式。近年来，这些市场准入制度也随着行业发展新形势和新要求做出了相应调整和改革。

许多监管机构摈弃了以特定技术或业务形态作为业务分类和许可的标准，以更好适应 ICT 融合发展趋势。在许可证类型方面，ITU 的统计数据显示，大约 60%的国家已经推出了统一许可证（unified licences）或一般授权制度，8%的国家推出了多业务融合许可证，但仍有 31%的国家仍使用基于特定业务的许可证[4]。在统一许可证或一般授权体系下，企业只需要获得单一许可证，或者仅需要进行登记或通知，便可以提供任何类型的信息通信网络或服务。**在许可管理方式**

[4] 见 ITU 《GLOBAL ICT REGULATORY OUTLOOK 2018》,第 69 页。

方面，尽管多数国家仍采取较严格的审批方式[5]，但在 5G、物联网技术推动的各行各业融合趋势下，越宽松的许可管理方式越有利于融合新业务的发展。**欧盟**是典型的宽松许可管理方式，根据《2018 年电子通信法指令》，欧盟对所有电子通信网络和服务采用一般授权制度，服务提供者至多需要向监管机构提交通知即可按照规定开展相关活动[6]。获得一般授权的服务提供者享有一系列权利，如互联互通谈判、码号资源使用；他们同时也需要遵守一系列义务，如信息提供、个人隐私保护、合法监听、应急通信、接入义务、网络安全保障、消费者保护、遵守技术标准和规范、非法内容限制等。**韩国**为适应数字经济融合趋势的发展，在 2018 年也对电信业务许可体系进行了改革，将基于设施的电信业务的许可方式由审批制度改为登记制度，并取消了转售业务的登记要求。

各监管机构不断跟踪评估云计算、OTT、物联网等新业务的发展影响，逐渐纳入准入体系进行管理。各国对云计算等新业务总体上保持着先发展后监管的态度，跟随相关业务的发展周期，及其对本国经济、产业和安全的影响，逐渐调整监管方式和要求。**对于云计算，**尽管美国主张将其划分为计算机业务，反对进行许可管理，但越来越多的国家出于促进本国云基础设施发展、确保数据安全目的，逐步将数据中心纳入市场准入管理。**沙特阿拉伯**从 2018 年开始，对在其境内提供云服务，且对境内数据中心或其他关键云基础设施有直接或有效控制的云服务提供商进行登记管理，监管机构有权在不给出理由的情

[5] 国际上一般将审批的许可方式称为“个别许可证”（individual license），即监管机构对每个许可申请进行严格全面的审查，每个许可证的条件、条款、义务、范围可能存在不同，但经营者数量通常不受事先限制。

[6] 一些业务也可以免除通知要求，具体视各成员国监管要求而定。

形下拒绝登记申请[7]。**南非**在 2014 年修订的《电子通信法》中，将数据中心界定为电子通信设施的一种，任何人要拥有、使用、提供、出售或租用电子通信设施来提供电子通信服务，必须经过监管机构批准。**泰国**要求数据中心经营主体需取得第二类电信业务许可证[8]，外资股比不得超过 50%。**印度** 2019 年 10 月发布云服务咨询文件[9]宣布，计划建立在政府监管下的非盈利行业组织来对各类达到规定规模的云服务提供商进行登记管理。**对于 OTT 业务，欧盟**《2018 年电子通信法指令》将对传统通信业务有直接替代作用的 OTT 通信业务（“基于码号的人际交往通信业务”[10]），作为电子通信服纳入一般授权体系管理，需要承担与传统通信服务类似的监管义务[11]。此外，鉴于**物联网**的发展也将涉及码号和频谱资源使用等与公共通信网类似的问题，**欧盟和新加坡**等部分国家和地区开始将机器对机器（M2M）的通信服务纳入准入监管范围。

（二）市场竞争监管：灵活运用竞争监管手段促进网络基础设施投资，数字平台成为反垄断新热点

数字经济下，新一代网络基础设施投资需求不断加大，中小型互联网企业需要更有利于创新的发展环境，各国反垄断监管作出相应调整。总体来看，电信行业反垄断监管趋于放松，互联网行业反垄断监

[7] See https://citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/GuideforCloudServiceProviders_en.pdf

[8] See “Proclamation of the Office of the National Broadcasting and Telecommunications Commission on Criteria and Procedure of Internet Service License Application”.

[9] See https://trai.gov.in/sites/default/files/CP_23102019.pdf

[10]《欧盟电子通信法》 将“基于码号的人际交往通信业务”定义为：与公共码号资源（即国家或国际码号计划中的一个或多个号码）连接的人际通信服务，或允许与国家或国际码号计划中的号码进行通信的业务。

[11] 参见上一段对欧盟一般授权制度的介绍。

管有加强态势。

以产业发展为导向，为加速构建新一代网络基础设施，监管机构对电信主导运营商的管制有所调整。全球大部分国家建立了电信主导运营商概念并加以限制，避免主导运营商过大过强，破坏市场竞争秩序。但是，随着 5G 商用带来前所未有的机遇和挑战，各国为抢占 5G 产业制高点积极准备，对电信主导运营商的竞争管制有所松动。**一是以加大网络投资和建设为条件，批准大型运营商之间的并购申请。**2011 年 AT&T 曾以推动 4G 网络建设为由申请收购 T-Mobile，2014 年 Sprint 也曾提出收购 T-Mobile 的申请，均被美国 FCC 以损害市场竞争为由否决。但是，到 2019 年，FCC 附条件批准了 T-Mobile 与 Sprint 之间的并购，寄希望于合并后的企业推动美国部署强大的 5G 网络。作为并购条件，两家公司承诺将在三年内部署覆盖 97%美国人口、85%农村人口的 5G 服务，六年内为 99%的美国人口提供速率不低于 50Mbps、为 90%美国人提供速率至少达 100Mbps 的移动宽带服务。**韩国**也批准了 SK 电讯收购该国第二大有线运营商 T-broad，批准条件包括，在 2022 年底前在农村地区扩大高速宽带服务等。**二是放松了对主导运营商的批发价格管制，以促进其投资高速宽带网络基础设施建设。**例如，Ofcom 计划通过放松对英国电信（BT）旗下网络基础设施公司 Openreach 的光纤宽带批发价格管制，以使其更快收回光纤宽带网络的投资。

欧美主要国家针对数字平台的监管呈现趋严态势，营造公平有序的竞争秩序成为各国竞争政策改革的重要方向。平台经济在为全球发

展注入巨大活力的同时，由其引发的竞争争议也持续发酵，多个国家和地区开展针对谷歌、脸书、亚马逊、苹果等数字巨头的反垄断调查。**欧盟**继续保持高压态势，欧委会完成谷歌反垄断执法第三案，德、英、法等国也频频主动出击，并尝试将隐私保护、平台规则透明化、数据安全等更多因素纳入反垄断调查考虑范畴。**美国**针对数字平台的反垄断监管态度发生较大转向，从传统上以私人诉讼为主转向行政监管部门主动发起的反垄断行政调查。2019 年 6 月以来，美国众议院、联邦贸易委员会（FTC）、司法部（DOJ）、各州均开启了针对谷歌、脸书、亚马逊、苹果等四大数字平台的反垄断调查。2020 年 10 月，美国众议院反垄断小组委员会公布了长达 16 个月的调查结果[12]，特别强调了的四大平台的市场支配地位及其商业行为所带来的影响和挑战，并建议完善反垄断法律，加强反垄断执法，恢复数字经济的竞争活力。

（三）新技术新业务监管：创新监管方式，着力平衡技术红利释放与未知风险防范

信息通信技术与各行业融合创新引发的法律制度冲突问题，已经成为各国共同面临的监管挑战。如何在鼓励创新和安全有序之间取得平衡成为各国进行法律制度改革和监管创新的重要出发点。监管沙箱制度受到各国的广泛关注，2018 年以来，韩国、日本、新加坡等国通过推出监管沙箱的方式促进 5G、物联网、AI 等数字化融合创新业务的发展，在受控环境内对新技术和业务进行测试，有效收集有关收

[12] 这份题为《数字市场竞争调查：大多数员工的意见和建议》的调查报告是在七场国会听证会、近 130 万份内部文件及邮件、60 位反垄断专家的 38 份意见书、以及对 240 多名市场参与者及被调查平台的前雇员和其他个人的采访的基础上形成的。

益和风险的相关证据，科学评估新技术新业务的经济社会可行性，并并适时改革不相适应的法律法规，在促进创新和风险控制间取得平衡。

各国在监管沙箱的准入范围、流程、监管模式、消费者权益保护等方面逐步形成一整套完整机制，主要有四个关键环节。**一是个案受理审议。**大多数国家就监管沙箱准入范围做原则性规定，对申请项目逐个审议。如，英、法等大部分国家采取“一事一议”方式决定监管沙箱项目是否部分或全部豁免现有法律规定。韩国提出，“法无规定或规定模糊的”可申请“临时许可”，“法有禁止的”可申请“实证监管特例”，获得批准后可在有效期内经营相关业务。日本提出，企业可与政府设立的监管沙箱窗口进行咨询后，向主管机构提交新技术示范申请。此外，为避免审批时间较长，贻误新技术新业务发展机遇，韩国、新加坡等已经开始探索“迅速受理”审批制度。**二是协同监管共治。**各国监管沙箱模式践行了多元共治思路，充分发挥了各类主体在行业治理中的作用。在审批环节，大部分国家监管部门“并行审批、分工联动”，组成包括政府工作人员、民间专家学者在内的审议委员会；在事中事后监管环节，监管部门共同监督项目是否遵守了许可有效期、业务范围等规定，并委托第三方机构进行跟踪监测；同时，企业在整个流程中应根据规定进行信息报告，提供相关数据用于监管改革评估，随时配合相关监管要求。**三是风险防范控制。**监管沙箱的重要一环就是监测可能出现的风险并建立风险预防和损害赔偿方案，在风险出现时暂停相关项目，将可能发生的损害控制在一定范围，确保

风险可控，保障用户权益。韩国强制要求监管沙箱项目必须加入商业保险，确实不能加入的，必须形成监管机构认可的损害赔偿方案，以确保新技术新业务经营者具有损害赔偿履行能力。**四是推动法律修订。**监管沙箱作为一种试验性的准入许可制度，核心价值是通过一段时间的试验，测试可能的风险点，为全面修订现有法律法规提供参考，营造有利于新技术新业务健康发展的市场环境。韩国《信息通信融合法》规定，有关机构应在临时许可有效期到期之前推动修订有关法律法规。

（四）用户权益保护：新技术滥用的新问题备受关注，各国建立长效机制积极应对

近年来，除了传统的资费、合同、服务质量等电信用户权益保护问题以外，全球还面临着网络和电话诈骗、垃圾信息、自动语音骚扰电话等网络技术滥用所引发的新风险，用户个人数据滥用、泄露事件频发，治理难度大、影响范围广。各监管机构不断调整优化相关立法和管理机制，探索建立技术手段等长效机制予以应对。

强化立法执法加大个人信息保护力度。为保护个人信息，各监管机构当前主要着力开展两方面工作。**一是通过专门立法加强个人信息保护。**随着欧盟《通用数据保护条例》（以下简称“GDPR”）在 2016 年出台，美国、日本、韩国、新加坡、巴西、印度等国纷纷制定或修订个人数据保护立法，完善本国数据保护制度。在立法共性上，各国立法将管辖范围适用至境外，进一步明确了数据保护原则，增强数据主体权利，细化了个人数据的分类管理，强化了安全保障等问责措施，

构建或完善了数据跨境流动制度，提高了对违规行为的处罚力度等。另一方面，由于各国国情的不同，在个人数据界定和分类、用户同意要求、责任措施、数据跨境流动等制度的具体设计上体现国别差异。**二是加大个人信息违法行为执法力度。**自 2019 年以来，美欧执法案例和罚款数额不断提升。欧盟方面，截至 2020 年 3 月，GDPR 共产生 230 个罚单，涉及罚金总共约 4.67 亿欧元。其中，2020 年 3 月产生的罚单数量为 32 个[13]，达到 GDPR 实施以来的单月处罚数量最高值。美国在 2019 年实施的隐私执法案件为 11 例（2018 年为 6 例），分别针对 Facebook 和 YouTube 在消费者隐私领域和青少年隐私领域的违规行为，开出了 50 亿美元和 1.7 亿美元的创纪录罚单。2020 年 2 月，美国最大的四家移动运营商因涉嫌违法将消费者地理位置数据的实时访问权出售给第三方聚合商，被美国 FCC 提议处以超过 2 亿美元罚款。**三是加强对违规企业的数据安全整改管理。**美国贸易委员会（FTC）在个人信息保护执法案件中针对违规企业发布的数据安全命令已经使用了 20 年，其可执行性和严格程度已经无法适应新形势的要求。为此，FTC 在 2019 年对数据安全命令进行了三项重大调整，以更好地规范违规企业的数据安全管理行为，提高震慑力，保护消费者利益：第一，提出更具体的数据安全计划。除要求企业实施全面的、基于流程的数据安全计划之外，还要求其实施具体的保障措施（例如年度员工培训、访问控制、数据安全故障监视系统、补丁管理系统和加密）以解决指控中提及的问题，提高命令的可执行性。第二，要求

[13] 数据来源：https://www.enforcementtracker.com/?insights

整改企业将数据安全重要性提升到公司高级管理层。例如，企业必须每年向董事会提交书面信息安全计划，企业高层必须每年就公司信息安全计划的详细信息向 FTC 提供合规证明。第三，提高对第三方评估机构的问责。例如，FTC 每两年批准或重新批准评估机构，要求评估机构提交评估结论的支撑证据，包括独立抽样、员工访谈和文档审查等记录。

多措并举加大新型骚扰电话和诈骗电话治理。随着互联网技术的发展，骚扰电话实施方式由人工向语音机器人转变，骚扰规模大大增加，这成为亟需解决的全球性难题。美欧等国家因其庞大的电信用户市场，成为骚扰电话和诈骗电话的重灾区，近些年来不断通过加强立法、实施行政和技术手段对新型骚扰电话等问题进行监管。**一是从源头和渠道两方面加强骚扰电话整治力度。一方面，**通过高额的罚款增加企业违规成本，从根源上减少骚扰电话。美国在 2019 年底发布《机器人电话滥用犯罪执法威慑法案》，从立法层面严惩机器人拨打骚扰电话违法行为,把处罚使用机器人呼出骚扰电话的罚款金额大幅提高，每通电话的罚款从过去的 1500 美元增至最高 1 万美元，取消了过去单次罚单总罚款不超过 100 万美元的限额。法国在 2020 年 2 月通过了一部打击骚扰电话的法律，将对相关企业和个人涉及骚扰电话的处罚金额总额度分别提高到 37.5 万和 7.5 万欧元。**另一方面，**通过追究提供通信渠道的电信企业的责任来切断传输渠道、有效减少骚扰电话。一些美国本土电信企业通过 IP 语音技术将数亿通海外电话传送到美国电信网络，为骚扰电话提供了便利渠道。根据新发布的法案，

美国司法部即便无法追踪到海外骚扰电话的直接拨打者，也可处罚为机器人电话提供传输渠道的这些电信企业。**二是采取新技术手段提高拦截能力。**为甄别欺骗性较高的电话号码，提高骚扰电话自动识别拦截能力，美国要求电信企业在 2021 年 6 月 30 日前全面使用“呼叫认证”（STIR/SHAKEN）技术实现呼叫者身份的验证。该“呼叫认证”技术此前已被加拿大电信企业全面应用，用于提升骚扰电话拦截效率。**三是加强政府部门与电信企业深度合作。**比如，澳大利亚 ACMA 成立了电信诈骗行动特别工作组，联合电信企业采取设立黑名单、制定白名单、溯源海外电话等试验性措施，打击伪装成权威机构电话实施诈骗或诱导回拨的相关行为。

（五）宽带网络建设：宽带网络向双千兆网络演进，加大普遍服务投入成为政策重点

宽带网络的持续演进升级正不断推进全球数字经济的蓬勃发展，ITU 数据显示，全球有 174 个国家已经出台了国家宽带发展战略规划[14]，尚未通过相关规划的国家中，75%计划近期出台促进宽带发展的政策。多国均将宽带基础设施纳入关键基础设施，并把加强宽带基础设施建设、推进宽带网络演进升级作为主要战略目标。

一是积极推进超高速率固定宽带网络部署，加快实现宽带千兆进程。统计数据显示[15]，已有 61 个国家的运营商相继推出了千兆宽带业务，覆盖全球约 5.8%的人口。欧盟在《塑造欧洲的数字未来》中提出，要加大对数字战略能力的投资，并把加快对欧洲千兆连接的投资、

[14] See ITU,The State of Broadband 2020 :Tackling digital inequalities，A decade of action.
[15] See http://gigabitmonitor.com/-/tPopulation.

修订《宽带成本降低指令》列为关键行动。**英国** Ofcom 在《连接英国报告 2019》提出，将建设全光纤和千兆宽带网络作为优先事项，计划投资 50 亿英镑以进一步扩大全光纤和移动网络的覆盖。2017 年**德国**发布《面向未来的千兆德国》战略，计划分四个阶段[16]，预计总投资 1000 亿欧元，在 2025 年前建设成具有千兆能力的融合基础设施。**韩国**于 2012 年 4 月开始实施 Giga KOREA（千兆韩国）战略，目前已在全国实现了 90%以上家庭的千兆覆盖，另外，韩国 KT 公司正在部署万兆级别宽带网络。

二是高度重视 5G 发展，加快抢筑 5G 竞争新优势。截至 2020 年 3 月底，全球已有 97 个国家和地区的 253 家运营商开展了 5G 试验，其中 75 家运营商宣布提供 5G 商用业务。为推进 5G 的发展，超过 80 个国家和地区出台了 5G 战略行动计划或促进 5G 发展的相关政策，关注重点包括 5G 的发展线路图、技术研发、频谱拍卖/分配、安全和商用服务等。**美国**国家科学基金从 2013 年起就通过专项资金来支持 5G 项目的研发；2017 年《美国国家安全战略》把在全国范围内部署 5G 网络作为首要行动；2018 年发布 5G FAST 计划，提出从增加频谱资源、改进基础设施收费政策、更新联邦法规三方面促进 5G 建设；2020 年 3 月发布《5G 国家安全战略》，明确了保护国内外 5G 基础设施安全的框架。**欧盟**委员会分别于 2014 年、2016 年提出 5G PPP[17] 计划和 5G 行动计划，从 5G 技术研发、测试、商用等方面进行线路

[16] 到 2018 年，所有家庭的带宽达到 50Mbps，并且法律规定新建住宅必须铺设光纤；到 2019 年底，工业园区实现光纤覆盖；到 2020 年底，为 5G 部署完成所有准备工作；到 2025 年，建成具有千兆能力的融合基础设施。

[17] See https://5g-ppp.eu/

部署；2018 年发布《“地平线 2020”2018-2020 年工作计划》，预计投资 17 亿欧元支持 5G、人工智能、物联网等数字技术与其他技术领域创新的融合。2013 年**韩国**未来创造科学部提出 5G 移动通信促进战略，计划总投资 1.6 万亿韩元；2019 年 4 月，韩国 MSIT 发布《实现创新增长 5G+战略》[18]，提出以 5G 商用化为契机，带动上下游产业发展，使韩国成为引领全球 5G 新产业、实现第 4 次工业革命的国家。

三是加大普遍服务投入，进一步弥合数字鸿沟。ITU 数据显示，全球超过 85%的国家出台了普遍服务相关政策[19]，主要关注点集中在加大对农村宽带普遍服务支持力度，加速边远贫困地区和公共服务场所的高速宽带覆盖。2020 年 2 月，**美国**设立“农村数字机遇基金”，计划在未来十年里累计投入 204 亿美元，通过反向拍卖的方式，支持运营商在农村社区等服务不足的高成本地区提供高速宽带服务;3 月，美国发布《宽带部署准确性和技术可用性法案》，要求 FCC 立即修复宽带地图[20]，以确保服务不足地区的消费者能够使用宽带服务；4 月，FCC 宣布将设立“美国农村 5G 基金”[21]，计划提供 90 亿美元以提高偏远地区的 5G 网络覆盖。**英国**《数字经济法案》规定的宽带普遍服务义务从 2020 年 3 月 20 日起正式生效，无法获得“体面的宽带接入”[22]的用户可要求普遍服务提供商[23]在合理的时间范围内为其部署必要的网络基础设施[24]；5 月，Ofcom 公布宽带普遍服务补偿规则，

[18] https://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw11211&artId=1778750.
[19] http://www.itu.int/net4/itu-d/icteye/Topics.aspx?TopicID=13.
[20] 宽带地图反映宽带互联网服务的可用性，收集有关哪些地区可以访问宽带互联网以及哪些地区无法访问宽带的详细信息。
[21] https://www.fcc.gov/5g-fund.
[22] 即 10Mbps/1Mbps 的下行/上行带宽。
[23] 目前，BT 和 Kcom 已被选定为宽带普遍服务义务提供商。
[24] 用户只需承担网络部署费用超过 3400 英镑的部分，且使用新宽带服务的价格与一般用户相同（不超过

计划设立行业基金以补偿普遍服务提供商产生的成本[25]。**加拿大**预计在未来十年内拨出 50 亿至 60 亿加元用于农村宽带投资，承诺在 2026 年以至少 50Mbps/10Mbps 的下行/上行速度为全国 95%的家庭和企业提供互联网接入，到 2030 年达到 100%覆盖率。

（六）频谱资源管理：5G 频谱分配进程持续加速，专网频谱分配取得实质性进展

与 4G 相比， 5G 具备的超高速率、超大连接、超低时延三大特性，将为 eMBB（增强移动宽带）、URLLC（超高可靠低时延通信）、mMTC（大连接物联网）三大应用场景提供有力支撑，从而开启人机交互、万物互联的新时代。当前，全球 5G 进入商用部署的关键阶段，各国纷纷加快推进 5G 公网与专网频谱资源分配。据 GSA 统计，截至今年 2 月，全球已经有 40 个国家完成 5G 公网频谱分配。美、英、德、日等国也陆续出台专网频谱政策，加速推动垂直行业创新发展。

各国纷纷制定 5G 公网频谱分配政策,加速 5G 商用部署进程。一是向电信运营商公开拍卖或直接分配未被占用的频率资源。美国已完成三轮 5G 高频段频谱拍卖。自 2018 年 11 月起，美国已完成 24GHz、28GHz、37GHz、39GHz、47GHz 等高频资源的拍卖，AT&T、Verizon、T-Mobile、US Cellular、Sprint 等多家移动运营商获得频谱资源。**欧洲多国聚焦中低频资源陆续开展 5G 频谱拍卖。**2018 年 3 月，英国将 3.4-3.6GHz 频段中的 150MHz 拍卖给沃达丰、O2、Three 和 EE 四家运营商。2019 年，德国完成 3.4-3.7GHz 频段拍卖，德国电信、沃达

46.1 英镑/月）。

[25] https://www.ofcom.org.uk/__data/assets/pdf_file/0033/195774/statement-uso-funding.pdf.

丰、西班牙电信、联合网络公司旗下 Drillisch 获得相应频段。2020 年 8 月，奥地利开始启动第二批共 27 个 5G 中低频频段的拍卖。**韩国**在 2018 年 6 月完成首批 5G 中频和高频频谱拍卖，SK 电讯、KT Corp、LG U+分别获得 3.5GHz 和 28 GHz 频段频谱。**日本**在 2019 年 4 月完成首批 5G 频谱分配,日本总务省宣布将 3.7GHz、4.5GHz 和 28GHz 频段分配给 NTT DoCoMo、KDDI、软银、乐天移动四家移动运营商。**总体而言，**韩国、日本和欧洲多国目前主要聚焦 3.4-3.8GHz 的中频段资源，纷纷启动拍卖或分配程序。在高频段方面，美、韩、日进展较快，其他多国也正在积极论证或征求公众意见过程中。**二是释放已被占用的频谱资源。**从美国情况看，该国 6GHz 以下频谱主要被广播电视、军用卫星和雷达占用，能够用于发展 5G 的中频段频谱资源极为有限，因此在初期美国主要选择毫米波频谱用于发展 5G。随着频谱资源稀缺性不断凸显以及电信运营商对中频资源需求的日益迫切，**美国**开始大力推进已被占用的 5G 中频资源的重新分配。今年 3 月，美国释放了原来由卫星运营商持有的(3.7-4.2GHz)280M 频谱，移动运营商将支付约 97 亿美元的赔偿金来获取上述频谱。8 月，FCC 宣布，原来由海军保留的 3.55-3.65 GHz 频段由电信运营商 Verizon 与卫星广播服务提供商 Dish Network 等 5G 建设主体拍得。同时，美国白宫和国防部宣布还将释放目前用于军事用途的 3.45-3.55GHz 频段共 100MHz 无线频谱用于 5G 商业服务。今年 7 月，**韩国**在 2020 年 7 月宣布，计划将目前用于卫星通信的 3.7GHz-4GHz 频段，以及即将到期的 2G、3G 和 4G LTE 网络当前使用的 310MHz 频段，重新

分配给 5G 相关移动运营商。

各国持续推动 5G 专网频谱分配，助力 5G+垂直行业创新发展。行业专网作为 5G 赋能垂直领域的主要应用场景和支撑企业数字化转型的关键基础设施，已成为各国关注的重要领域。2019 年以来，美、英、德、日等国相继出台专用频谱政策，为 5G+垂直行业专用网络规划专用频段。**从使用范围来看，**与电信运营商的全国性 5G 公网频谱相比，大部分专网频谱都限定了使用区域范围。**从分配对象来看，**目前专网频谱主要面向工业等垂直行业主体。**从分配方式来看，**主要有以下两种模式：**一是分配未被占用的专用频谱用于 5G 专网部署。**2019 年 3 月，**德国**联邦网络局（“BNetzA”）发布《无线网络接入设备使用 3700-3800MHz 频段的基本框架要求》，成为首个为专网预留 5G 频谱的国家。截止今年 9 月，包括德意志展览公司、巴斯夫化工集团、电信系统集成商 Mugler 等 74 家企业获得了区域 5G 频谱许可。这些频谱主要用于工业园区、博览会场地、农业和林业用地等局部地区的无线接入业务。**日本**总务省于 2019 年 12 月开放 28.2-28.3GHz 的 5G 本地专网频谱牌照申请，今年 2 月日本富士通宣布已获得关东电信局颁发的日本首个 5G 专网频谱牌照。**二是通过监管机构二次授权的方式向企业分配专网频谱。**例如，英国 Ofcom 开放了本地接入许可，对一些本属于公网运营商但尚未规划使用的频谱进行二次授权。在取得公网运营商同意，并提交本地专网不会对公网当前运营以及未来规划造成干扰的证明后，经 Ofcom 许可，企业即可以在人口稀少的农村地区及采矿、海上作业工业场景等特定区域使用这些频谱。

（七）互操作性管理：OTT 通信与数据互操作性议题进入视野，着力推动多层面的有效互通

近年来，对新兴领域跨系统、跨平台互操作性讨论逐步兴起，这些讨论主要集中在两个层面。

第一层面，是通信类 OTT 应用的业务互操作性[26]（业务互通）问题。VOIP、即时通信等通信类 OTT 业务提供与传统通信业务相同或相似服务，随着这类应用对传统话音和短信业务形成替代，不同的 OTT 之间的技术差异可能导致通信服务之间缺乏足够的互操作性，威胁终端用户之间端到端的有效互通，特别是具有较大规模的 OTT 业务如果不支持互通，可能会阻碍新主体进入市场，影响市场活力和创新。因此通信类 OTT 之间的业务互通问题正在进入监管视野。欧盟《2018 年电子通信法指令》指出，欧委会考虑依法通过对欧盟和成员国实际市场形势的评估，决定是否采取强制标准或规范等措施来加强 OTT 之间的互操作性。各成员国将在 2020 年年底前将该部电子通信法条例转化为本国立法，届时针对 OTT 通信服务提供商的管制可能会出台进一步的解释。目前看来，欧盟的互操作性要求将仅对达到一定地理覆盖范围和用户规模的一些 OTT 通信服务商有约束效果。

第二层面，是在更广泛的范围内，探索提出数据的可传输、可编译等互操作性监管要求。数据在推动全球数字化转型中发挥了极其重要的作用，为创新和经济社会发展提供源源不断的动力，如何更好的

[26]互操作性（Interoperability ）又称互用性，是指不同的计算机系统、网络、操作系统和应用程序一起工作并共享信息的能力。

发挥数据要素价值成为全球的共同关注。但目前，数据的收集、利用、流动等环节还存在较多问题：例如少数几家超大型科技企业拥有全球大部分数据，可能会遏制初创公司的创新空间和竞争力；政府公共数据与企业数据、个人数据之间，如何在保障隐私和安全的前提下平衡好数据流通和广泛使用；不同行业领域间和行业内各企业的数据之间，数据标准如何共通，如何更好的发挥数据的集聚效应等等。欧盟在 2020 年 2 月发布《欧盟数据战略》，致力于拓展不同领域之间的数据互通与互操作性，释放数据价值潜力。**一是建立数据交换标准。**欧盟提出要制定《信息和通信技术标准化滚动计划》，进一步完善《欧洲互用性框架》，推动欧盟采用标准化和共享的兼容数据格式及协议，以可互操作的方式来收集和处理不同来源的数据。**二是形成数据共享机制。**欧盟将制定相关机制，如启动《开放数据指令》《高质量数据集实施法案》等文件编写，明确公共部门数据、企业数据开放的顺序、原则和程序，平衡与个人信息保护的要求，满足中小企业在数据方面的特殊需求等。**三是建设数据互通技术平台。**欧盟正在研究开放数据工具、建设下一代数据处理基础设施，促进数据共享互通。如，建立高能效的可信边缘计算处理能力，开发数据存储和处理的通用云平台，构建 9 大领域数据空间，提升数据的可用性、质量和互操作性，有效整合欧盟的数据资源。

（八）网络信息安全管理：网络和数据安全保障热度持续，违法内容管控不断强化

各监管机构仍在持续采取各种措施，健全网络信息安全防护体

系，重点保障网络、数据和内容安全，在 5G、数据跨境流动等新领域提前布局，在内容安全审查方面强化社交媒体等渠道的内容管控。

网络安全方面，随着全球 5G 的发展提速、竞争加剧，5G 安全风险逐渐显现，受到国际高度重视。2020 年 1 月，**欧盟**委员会出台了《欧盟 5G 安全工具箱》[27]，倡议统筹协调成员国制定统一的 5G 安全标准和认证机制，确保所有欧盟国家达到足够的 5G 网络安全水平：如要求 5G 网络运营商通过严格控制访问权限、制定安全操作和监控规则、限制特定功能外包等做法提高安全性；要求监管机构评估供应商的风险情况，通过外国投资审查、贸易防御及反不正当竞争等政策工具在欧盟认定的重要敏感资产上对“高风险”供应商进行设限；还要求确保每个运营商都采取多供应商策略，避免过于依赖或者绑定单一供应商。2020 年 3 月，**美国**签署了《保障 5G 及未来技术的法案》《5G 安全和超越法案 2020》并发布《5G 安全国家战略》，强调在进一步激发 5G 基础设施市场竞争力和多样性的同时，要有效评估 5G 本身的网络安全风险并确定其核心安全原则，继续推动以美国私营部门主导的国内 5G 部署，确保 5G 基础设施的安全性；还要与盟友一道参与全球 5G 安全标准制定，推动安全可靠的 5G 设备及服务的供应，防范因使用 5G 带来的经济发展和国家安全风险，尤其是供应链风险。

数据跨境流动方面，主要国家和地区形成了“在确保安全前提下促进数据跨境流动”的普遍共识。出于保护公民隐私、保障国家安全、扶持产业发展等因素考虑，各国对数据跨境流动实施不同程度的管

[27] 原报告名为：EU Toolbox for 5G Security 2020。

理。全球主要形成了三类监管制度。**一是**以美国为代表的、围绕重要数据实施的负面清单模式，美国政府依托其强大的互联网产业实力，对外倡导数据自由流动，宣扬 APEC“跨境隐私保护规则”（CBPR）机制，拉拢各方加入“低水平保护”体系。对内，美国制定了受控非秘信息（CUI）清单，界定了“重要数据”范围，严格限制关键基础设施数据、新兴和关键技术数据、敏感个人数据出境。**二是**以欧盟为代表的、围绕个人数据实施的白名单模式，欧盟《通用数据保护条例》确立了“充分性认定”的数据跨境流动管理制度，仅允许其公民个人数据流向数据保护水平达到欧盟标准的其他国家或地区。当前共有 12 个国家或地区符合欧盟的要求[28]。**三是**以印度、俄罗斯为代表的数据本地化模式，俄罗斯在“棱镜门”事件后出于对国家安全的考虑，规定所有国内外公司必须在俄境内存储和处理俄公民的个人数据，但同时允许个人数据按照《个人数据保护法》的要求出境。印度要求关键个人数据、物联网数据、支付数据等只能本地化存储，不允许跨境流动，但一般个人数据和敏感个人数据在印度境内存储副本后可以跨境流动。

内容安全方面，更多国家由互联网内容自律管理向强化行业监管转变。根据 ITU 统计，2009 年全球 190 个国家中对互联网内容实施监管的比例为 8%，到 2017 年底这一比例已经上升为 22%。近两年来，由于社交媒体上的网络恐怖主义、网络暴力、儿童虐待等负面事件高

[28] 当前进入欧盟数据跨境流动白名单的包括：安道尔、阿根廷、加拿大（限于商业组织）、法罗群岛、根西岛、以色列、马恩岛、日本、泽西岛、新西兰、瑞士、乌拉圭。

发，包括西方国家在内的全球各国逐渐放弃以互联网企业自我管制为主的管理方式，转而加强政府干预。2020 年 7 月，**欧盟**委员会发布《视听媒体服务指令》修正案指导方针，帮助成员国进一步净化欧盟网络环境。根据修正案，社交媒体首次被纳入监管范围。**英国**政府在 2020 年 2 月宣布，为营造安全可信的数字经济环境，将任命英国 Ofcom 对互联网内容进行监管。此前，Ofcom 只负责电视、广播相关的有害内容监管。**澳大利亚**于 2015 年在澳大利亚通信和媒体管理局（ACMA）下设电子安全专员办公室，2019 年通过《分享重大暴力内容》刑法典修正案，将其监管范围从调查和解决与儿童相关的有害互联网内容投诉扩大至网络暴力内容。**新加坡**于 2019 年通过了《防止网络假信息和网络操纵法》，在新加坡 IMDA 内设了一个专门执行该法案的办公室（POFMA），负责具体发布各部门有关更正或删除网络虚假信息的相关指示，并拥有监督和执法权。**另一方面，在政府倡导下，企业也加大了对在线内容的自主审查力度。**2019 年 5 月，谷歌、微软、亚马逊等 8 家互联网平台企业与法国、新西兰、澳大利亚等 17 个国家共同签署“克赖斯特彻奇倡议”，承诺将尽一切努力“抵制暴力恐怖主义和极端主义”，遵守相关法律、及时删除互联网上的恐怖主义内容。2020 年 6 月，脸书、谷歌、微软、推特等组成的技术联盟（Technology Coalition）宣布将建立一个研究和创新基金，以防止网络成为在线的儿童性虐待工具。2020 年 8 月，脸书、谷歌、微软等 9 家科技巨头就如何在大选前后防止虚假信息传播发布了一

份联合声明，表示会与负责保护选举公正性的美国政府机构定期举行会议，确保美国大选的安全性。

三、全球信息通信监管改革趋势展望

作为带动科技创新的重要引擎和推动经济社会数字化转型的关键支撑，信息通信行业保持健康发展具有更加重要的意义。2020 年 GSR 大会指出，在新冠疫情威胁和全球经济衰退的阴影下，信息通信行业监管可提升经济社会面对突发事件和紧急情况的就绪水平，在出现不利因素的情况下有效满足人们的期待。以 5G 为代表的信息通信技术应用机遇与挑战并存，行业监管面临许多新的改革要求。观察全球各个国家和主要经济体的下一步战略和规划可以看出，未来，各个行业监管机构将进一步坚定地促进行业与经济社会的可持续发展，抢抓新型基础设施发展机遇，创新面向数字平台、数字生态系统的监管方式和手段，探索数据新要素的有效治理，完善新型协同监管体系，积极应对疫情后的数字化转型挑战。

（一）实现全面的数字连接仍是信息通信监管的首要目标

在新冠肺炎疫情的影响冲击下，国际社会普遍认识到，宽带普遍接入是推动经济复苏、实现联合国 2030 可持续发展目标的重要催化剂。但由于信息通信技术的获取和使用存在巨大差距，全球将有数十亿成年人和儿童无法从远程工作、教育、医疗和公共服务中受益，数字鸿沟进一步加剧了贫困人群的困境。例如，联合国预计，全球有 190 多个国家近 16 亿学生因疫情原因中断学校学习，其中低收入和

中低收入国家高达 99%的学生受到影响。[29]另外，互联网用户普及率较低的国家也将落后于全球数字经济发展浪潮，错失数字化转型机遇。**短期来看，**加强网络基础设施建设、确保普遍公平接入，不仅可以应对当前新冠疫情大流行带来的挑战，还可以为恢复经济社会秩序做好支撑，各国将采取更大力度扩大宽带接入以解决当前的突出问题。**长期来看，**高水平的宽带接入也是应对未来灾难、推动数字经济可持续发展的重要保障。国际电信联盟号召各国以努力实现联合国 2030 年可持续发展议程宏伟目标为愿景，从宽带覆盖水平、宽带用户价格、数字技能培养、中小企业服务等方面制定具体目标，创新思维、积极尝试、开放学习、广泛开展合作，有效提升宽带普及率。

（二）加快 5G 等新型基础设施建设将是未来一段时期的战略重点

各国将不断加大对以 5G 为代表的新型网络基础设施的投资部署，把提高网络能力建设作为战略优先事项。预计 2020 年至 2025 年间，全球将在移动网络上投入 1.1 万亿美元，其中 5G 投资将占 80%以上。其中，全球所有投资的一半将来自美国、中国和日本[30]。到 2025 年底，全球 5G 签约用户将达到 28 亿，覆盖全球近 65%的人口，45%的数据流量将由 5G 网络承载[31]。为充分发挥 5G 潜力，实现数字化转型并进一步支撑经济增长，各国政府及监管机构将重点聚焦行业可持续发展，出台相关扶持政策，推动建成安全、可靠、有竞争力的 5G

[29] See: ITU, The State of Broadband 2020 :Tackling digital inequalities，A decade of action.

[30] 数据来源：GSMA《2025 年资本支出展望》。

[31] 数据来源：爱立信《移动市场报告》。

网络，**包括**：制定清晰的国家宽带战略，促进 5G 发展；降低运营商获取和持有 5G 专有频谱的成本；减免行业特定税收，刺激 5G 投资；降低部署成本，强化多部门协调配合，如开放公共建筑和街道基础设施（公交车站、路灯杆等）供 5G 部署使用等等。

（三）更好适应数字经济发展特点将是监管方式创新的重要方向

数字化转型对信息通信监管机构适应市场、技术和应用快速变化的能力提出了空前的高要求，为此，监管机构需要加快改革和调整原有监管方式，进行更为灵活、包容、科学、审慎的监管。以高层原则为指导、以证据和数据为基础、以激励和结果为导向的政策制定和监管方法，正成为 ITU 和美欧等国家推崇的新型监管方式。从具体监管实践看，**一是**监管沙箱作为一种更动态、更基于证据、“边干边学”、全周期管理的新型监管方式，将被越来越多的国家应用于促进信息通信领域和其他行业的融合新兴业态的发展。**二是**在数字化转型的复杂环境下，为确保监管干预的正确性、有效性和科学性，在收集多维度事实和数据的基础上，对监管政策的制定、实施、修订进行全生命周期的影响评估，这种监管影响评估（RIA）工具将进一步在全球普及。**三是**从事前、事中事后监管环节来看，在事前准入环节，统一许可证、多业务许可证由于具有简化许可流程、提升资源使用效率以及更适应技术融合的发展等优点，已成为许可方式的国际最佳实践。在事中事后环节，持续的市场监督、市场分析以及监管影响评估，对及时掌握

市场趋势并预测风险至关重要，越来越多的国家将完善相关的机制推动这种更加灵活的监管方式落地。

（四）释放数据价值和强化数据治理成为各国发展数字经济的关键着力点

数据作为数字经济时代的关键生产要素，对于推动经济社会创新发展具有重要意义。当前，世界主要国家通过完善数据立法、出台数据战略、加强数据国际合作等多种方式完善数据治理机制，力图在保障数据安全的同时，促进数据价值的最大化释放。未来，各国将持续大力培育发展数据要素市场，发挥多元主体作用，构建覆盖社会各层面的数据治理体系，重点从四个方面突破。**一是**促进数据开放共享，将数据资源释放出来，为数据开放应用提供源头供给。**二是**加强数据质量管理，确保数据完整性、一致性、精确性和及时性，不断提升数据资源价值。**三是**实现数据交易流通，促进不同来源数据的聚集、整合，活跃数据市场供需两端。**四是**强化数据风险规制，解决数据相关的风险和问题，为数据价值释放提供安全保障。

（五）强化数字平台治理成为信息通信监管的普遍趋势

数字平台在经济社会数字化转型发展中正扮演着日益重要的角色，少数大型平台企业成为信息内容、数字市场事实上的“守门人”，平台的规则、算法设计对经济社会的影响已越来越无法忽视，并已引起各国监管机构的高度重视。未来，各国将紧紧抓住平台这一关键主体，强化对平台企业的监管，营造更加健康、公平、可持续的数字发

展环境。**一方面**，监管机构将要求平台在内容监督方面承担更大责任，包括对虚假信息、儿童有害内容等的打击。例如，美国司法部已向美国国会提交关于修改 1996 年《通信规范法案》第 230 条的立法草案，对平台无需为用户内容承担责任的条款进行改革，以激励平台更积极地治理网上有害内容。**另一方面**，监管机构将加强对大型数字平台的监管力度，以确保数字市场的公平有效竞争、保护创新。例如，欧盟即将推出《数字服务法案》，引入额外措施，如防止大型平台滥用规模优势伤害竞争对手，禁止大型平台强加不公平条款等，保护数字市场竞争活力。

（六）多方协同的治理机制在应对融合性监管挑战中的作用将进一步凸显

当前，采取第五代协作式信息通信监管已成为国际组织和世界主要国家的共同选择。未来，从制度、机制等多个方面推动协作式监管落地将是下一阶段的重点。**一是**凸显信息通信监管部门在协作机制中的关键地位，进一步发挥在疫情防控等紧急情况下，对互联网带宽、设备部署和基础设施共享等资源的统筹作用，强化在数字经济运行基础上，与卫生、政府、教育和金融等部门之间的核心协调角色。**二是**健全包括协作进程、机构框架等在内的一套制度体系，以跨部门备忘录、联席机制等形式，保证协作的规范化和实操性。**三是**加强多方信息共享和对话平台建设。推动与整个行业主体、第三方组织及相关监管机构之间的信息共享。探索高效透明的国际对话机制，在区域和全球层面共同促进数字市场的繁荣发展。

中国信息通信研究院 政策与经济研究所
地　　址：北京市海淀区花园北路 52 号
邮政编码：100191
联系电话：010-62302662
传　　真：010-62302476
网　　址：www.caict.ac.cn