国盟信息安全通报

2021 年 02 月 21 日第 234 期

全国售后服务中心

国盟信息安全通报

（第 234 期）

国际信息安全学习联盟

2021 年 2 月 21 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 457 个，其中高危漏洞 163 个、中危漏洞 246 个、低危漏洞 48 个。漏洞平均分值为 5.85。本周收录的漏洞中，涉及 0day 漏洞 238 个（占 52%），其中互联网上出现“WordPress 插件 Easy Contact Form 'Name'跨站脚本漏洞、Nxlog 代码问题漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 6601 个，与上周（5712 个）环比增加 16%。

主要内容

一、概述 4
二、安全漏洞增长数量及种类分布情况 4
➢漏洞产生原因（2021 年 1 月 31 日—2021 年 2 月 21）.....4
➢漏洞引发的威胁（2021 年 1 月 31 日—2021 年 2 月 21）.....5
➢漏洞影响对象类型（2021 年 1 月 31 日—2021 年 2 月 21）.....5
三、安全产业动态 6
➢做好建设网络强国这篇时代大课题.....6
➢深入学习贯彻党十九届五中全会精神大力提升网络强国建设的能力和水平.....8
➢关于第 47 次《中国互联网络发展状况统计报告》，专家这样说.....12
➢2020 年《网络安全法》配套规定和标准综述.....16
四、政府之声 33
➢国家七部门联合发布《关于加强网络直播规范管理工作的指导意见》.....33
➢工信部印发《工业互联网创新发展行动计划（2021-2023 年）》的通知.....34
➢国家网信办启动 2021“清朗·春节网络环境”专项行动.....41
➢工业和信息化部组织召开 APP 个人信息保护监管座谈会.....42
五、本期重要漏洞实例 44
➢关于微软 Windows 操作系统存在 TCP/IP 高危漏洞的安全公告.....44
➢Oracle Business Intelligence Enterprise Edition 信息泄露漏洞.....44
➢Cisco IOS XR 拒绝服务漏洞.....45
➢多款华为产品信息泄露漏洞.....46
六、本期网络安全事件 47
➢Yandex 抓到内鬼:一名员工私下出售用户电子邮件收件箱的访问权限.....47
➢《赛博朋克 2077》开发商 CD Projekt 称遭遇勒索软件攻击.....47
➢以朋友名义向未注册用户发送信息，“脉脉”网站被判侵犯隐私权.....49
➢新加坡最大电信公司文档系统遭入侵，13 万名客户资料外泄.....51
➢央视：开了会员配送费却猛涨 3 倍！“杀熟”又出新招？.....53
➢起亚汽车遭遇勒索软件攻击，赎金高达 2000 万美元.....55

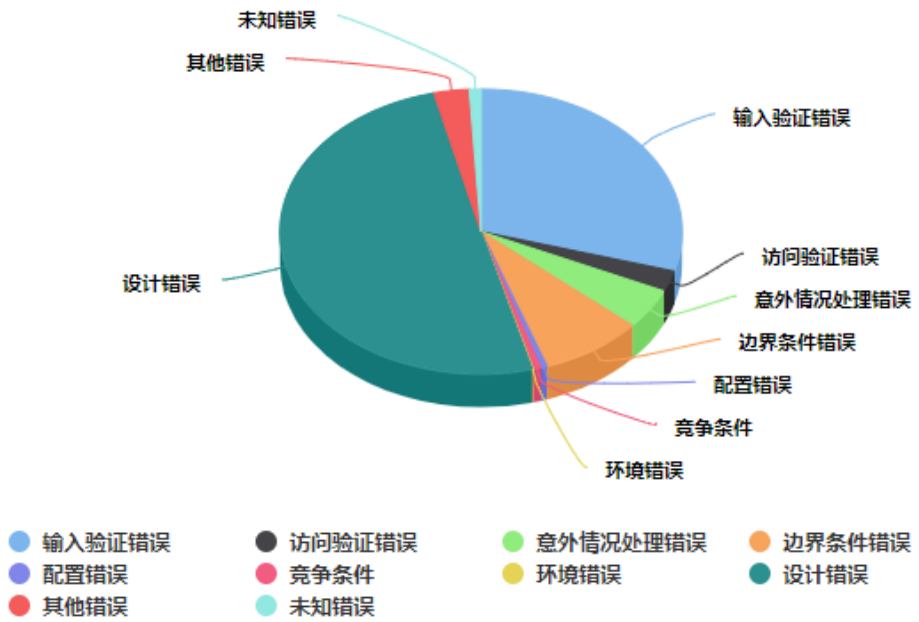
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

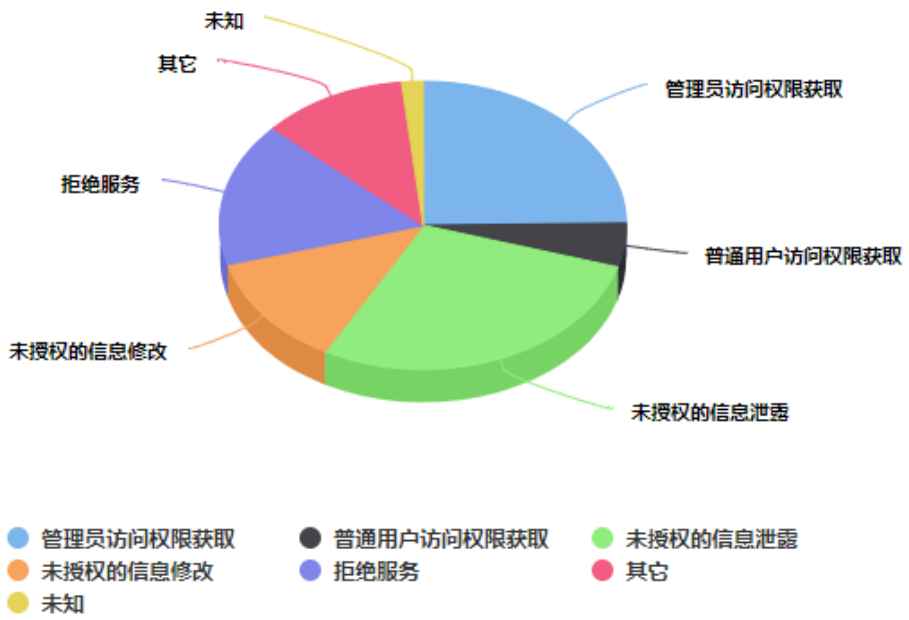
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 457 个，其中高危漏洞 163 个、中危漏洞 246 个、低危漏洞 48 个。漏洞平均分值为 5.85。本周收录的漏洞中，涉及 0day 漏洞 238 个（占 52%），其中互联网上出现“WordPress 插件 Easy Contact Form 'Name'跨站脚本漏洞、Nxlog 代码问题漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 6601 个，与上周（5712 个）环比增加 16%。

二、安全漏洞增长数量及种类分布情况

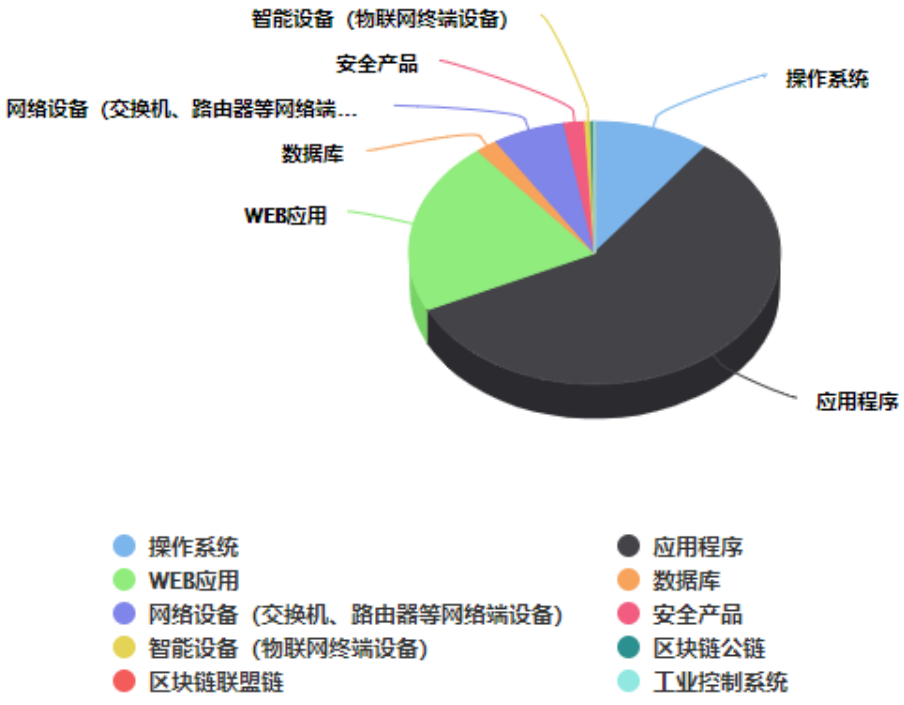
➢ 漏洞产生原因（2021 年 1 月 31 日—2021 年 2 月 21）



➢ 漏洞引发的威胁（2021 年 1 月 31 日—2021 年 2 月 21）



➢ 漏洞影响对象类型（2021 年 1 月 31 日—2021 年 2 月 21）



三、安全产业动态

➢ 做好建设网络强国这篇时代大课题

步入信息时代，谁处于互联网领域的翘楚地位，谁就把握住了时代竞争的主动权。习近平总书记指出，要提高网络综合治理能力，形成党委领导、政府管理、企业履责、社会监督、网民自律等多主体参与，经济、法律、技术等多种手段相结合的综合治网格局。核心目标就是要将我国建设成为新时代的网络强国。党中央高屋建瓴，非常重视互联网及其相关产业发展、致力于互联网相关人才培养、依法治理着互联网行业的健康壮大，积极统筹协调涉及政治、经济、文化、社会、军事等领域网络安全和信息化重大问题，作出了一系列重大决策、实施了一系列重大举措，全力推动网络强国建设。

网络强国建设，人才是关键因素。互联网的本质是信息的互联互通，它为人类生产生活提供诸多便利，广泛造福于我们整个社会。众所周知，信息时代和非信息时代，不是简单的几十年或几百年时间差距，而是信息立体空间与信息平面空间的本质差别。只有真正掌握了先进的信息技术、网络技术，才能将泱泱地球变成一个村，才能在分秒必争的时空抢占经济社会和科技发展的先机。当前致力于建设网络强国，一方面是时代的必然要求，另一方面则是提升国家综合竞争力的必由之路。近年来，我国在互联网技术上确实取得了长足进步，但仍然没有彻底解决部分核心技术被“卡脖子”的制约。为此，我们要建设网络强国，必须从

根本上改变关键技术受制于人的局面，必须要培养一支世界水平的网络科技领军人才，必须造就一个个高水平创新网络团队，必须吸引更多高素质人才参与到信息技术的研究、开发与应用中，真正把网络大国建设成为网络强国。

网络强国建设，要与中华文化紧密结合。互联网对人类社会而言，是一种信息交流的平台，是传播和辐射文化的便捷工具。如今，人们的拇指一动，屏幕一刷，就能传播海量信息，就能遥知千里万里的各种资讯。据有关部门统计，我国已经成为互联网第一大国，国内的网络规模、网民数量、智能手机用户以及利用智能手机上网的人数等，都处于世界遥遥领先的位置。然而，作为一个有着五千年历史文明的国度，在互联网与民族优秀文化的融合上，确实还有很长的一段路需要走。因为只有真正将自己民族的优秀传统文化与互联网有机结合，与人类命运共同体这个时代主题同频共振，才能确保网络强国建设的健行致远，才能达到促进优秀传统文化有效、有序传播的目的。否则，新瓶装老酒，不仅失去了韵味，使得我们的网络建设就会失去灵魂。

网络强国建设，必须与时俱进，不断创新。生活滋润了科技成长，先进科技也快速改变了我们的生活，这是一种螺旋上升的互动。从全球范围看，信息化对经济、政治、文化、社会等各领域的渗透趋势越来越明显，已经成为推动经济社会转型、实现可持续发展、提升国家综合竞争力的强大动力，成为推动高质量发展的核心力量。推进网络创新，走出一条中国特色网络强国建设之路，一方面要把增进人民福祉作为信息化发展的出发点和落脚点，另一方面要让互联网成为了解群众、贴近群众、为群众排忧解难的新途径，这是网络强国建设的核心所在，更是我们网惠万民的关键。各级党委政府要努力推动互联网、大数据、人工智能与群众日益需要和期盼深度融合，引导其健康有序发展，促进互联网企业进一步做大做强，推动我国软硬实力在全球的影响力。

时至今日，互联网已成为继领土、领海、领空之后的“第四空间”，成为大国博弈的战略制高点，成为实践人类命运共同体的利器。只有努力加快网络强国建设，中国梦才会如期实现；只有努力加快网络强国建设，民族复兴才有希望。作为新时代的我们，应该深刻理解网络强国建设的重要意义，坚持从自身做起，充分发挥自身的专业优势，切实结合自己的岗位职责，为建设网络强国的事业贡献自己的一份力量。（来源：人民论坛网）

➢ 深入学习贯彻党十九届五中全会精神大力提升网络强国建设的能力和水平

党的十九届五中全会围绕开启全面建设社会主义现代化国家新征程，明确提出了“十四五”时期我国发展的指导方针、主要目标、重点任务、重大举措。特别是把握信息革命的“时”与“势”，对网络强国建设作出一系列新部署新要求，强调要坚定不移建设网络强国、数字中国，加快数字化发展。站在“两个一百年”奋斗目标的历史交汇点上，全国网信系统要深入学习领会五中全会精神特别是习近平总书记重要讲话精神，增强“四个意识”、坚定“四个自信”、做到“两个维护”，切实把思想和行动统一到以习近平同志为核心的党中央决策部署上来，紧扣准确把握新发展阶段、深入贯彻新发展理念、加快构建新发展格局，扎实做好网络安全和信息化各项工作，为实施“十四五”规划、全面建设社会主义现代化国家开好局、起好步提供有力服务、支撑和保障，以优异成绩庆祝建党 100 周年。

深入学习领会习近平总书记重要讲话精神，准确把握网信工作在全面建设社会主义现代化国家新征程中的职责使命。

习近平总书记从开启全面建设社会主义现代化国家新征程和实现中华民族伟大复兴中国梦的高度，对我国进入新发展阶段、贯彻新发展理念、构建新发展格局进行了深刻阐述。全国网信系统学习贯彻习近平总书记重要讲话精神，关键是要学深悟透这一重要论述的丰富内涵和实践要求，从中明确网络强国建设的时代方位、职责使命、路径选择，做到紧紧围绕大局、主动融入大局、有力服务大局。

要在准确把握新发展阶段中明确网信事业发展的时代方位。新发展阶段是我们党带领人民迎来从站起来、富起来到强起来历史性跨越的新阶段。习近平总书记强调，信息化为中华民族带来了千载难逢的机遇；没有网络安全就没有国家安全，没有信息化就没有现代化。这些重要论述，深刻阐述了网络强国建设与中华民族伟大复兴以及全面建设社会主义现代化国

家的内在关系，明确了网络强国建设在新发展阶段中的历史坐标。当前，信息革命时代潮流与中华民族伟大复兴战略全局和世界百年未有之大变局发生历史性交汇，与党和国家事业发展同步，网信事业发展也在“两个一百年”奋斗目标接续推进中进入了新发展阶段。准确把握新发展阶段，必须立足两个大局，加快推进网络强国建设，抓住战略机遇期，抢占发展制高点，把握时代主动权，切实把信息革命的时代伟力转化为全面建设社会主义现代化国家、实现中华民族伟大复兴的强劲动力。

要在深入贯彻新发展理念中明确网信事业发展的职责使命。新发展理念是一个系统的理论体系，科学回答了关于发展的目的、动力、方式、路径等一系列理论和实践问题。习近平总书记强调，网信事业代表着新的生产力和新的发展方向，应该在践行新发展理念上先行一步，这是习近平总书记在深入思考和把握社会生产力发展规律基础上作出的重大判断。当前，新一轮科技革命和产业变革深入发展，数据资源成为新生产要素，信息技术成为新创新高地，信息网络成为新基础设施，数字经济成为新经济引擎，信息化成为新治理手段，网络安全成为新安全挑战。网信事业在践行新发展理念上先行一步，必须充分发挥信息化驱动引领作用，进一步解放和发展社会生产力；坚持以人民为中心的发展思想，使人民群众在共享互联网发展成果上有更多获得感；坚持以问题为导向，切实解决好网信领域发展不平衡不充分的问题，真正实现网信事业高质量发展；坚持用底线思维谋划发展，统筹发展和安全两件大事，筑牢国家网络安全屏障，及时防范化解网信领域面临和潜在的各种风险。

要在加快构建新发展格局中明确网信事业发展的路径选择。加快构建新发展格局，是以习近平同志为核心的党中央着眼我国发展阶段、发展环境、发展条件新变化作出的一项事关发展全局的重大战略抉择。当前，数字化发展从根本上改变了传统生产方式和发展模式，对于促进各种生产要素的组合在生产、分配、流通、消费各环节有机衔接，推动经济循环的畅通无阻，加快推动形成以国内大循环为主体、国内国际双循环相互促进的新发展格局具有重要意义。加快构建新发展格局，必须着眼实现高水平自立自强、扩大内需、实行高水平对外开放等重大战略任务，加快信息领域核心技术突破，推动数字产业化和产业数字化，促进信息消费，推动网信企业“走出去”，切实把创新主动权、发展主动权牢牢掌握在自己手中。

扎实推进网信事业高质量发展，为全面建设社会主义现代化国家提供有力服务、支撑和保障。

面向全面建设社会主义现代化国家新征程，我们将深入贯彻落实习近平总书记重要讲话精神，坚持政治统领，坚持服务大局，坚持改革创新，坚持问题导向，坚持强化监管，坚持系统推进，全面提升网络安全和信息化工作能力水平，为党和国家事业发展提供强大网上舆

论支持、可靠网络安全保障、有力信息化支撑。

着眼服务“国之大者”，科学规划网信事业发展新蓝图。坚持以习近平总书记重要讲话精神为指导，围绕五中全会提出的一系列战略性、纲领性、引领性的重大任务，提高政治站位、加强研究谋划、做好对接衔接，高水平编制“十四五”网信领域规划，进一步明确发展方向、工作目标和重点任务，努力使规划编制体现时代新变化、符合实践新要求、反映人民新期待。

着眼推动凝心聚力，努力开创网络内容建设管理新局面。坚持正能量是总要求、管得住是硬道理、用得好是真本事，加强和改进网上正面宣传，精心做好党的创新理论网上宣传，统筹做好庆祝建党百年以及开局“十四五”、奋进新征程等重大主题网上宣传，加快建立网络综合治理体系，推动网络文明建设，发展积极健康的网络文化，动员全社会力量加强网络生态治理，切实维护网络意识形态安全和政治安全。强化互联网企业反垄断和防止资本无序扩张，夯实监管责任、创新监管方式、提高监管能力，有效防范和化解风险，走出一条齐抓共管、良性互动、系统协同的互联网发展之路。

着眼高水平自立自强，加快推动信息领域关键核心技术取得新突破。发挥新型举国体制的制度优势和重大工程项目的突破带动作用，加强云计算、人工智能、量子技术、区块链等重点领域的顶层设计和总体布局，加快突破一批关键核心技术，提升供应链关键短板国产化能力，完善激励机制和科技评价机制，落实好攻关任务“揭榜挂帅”等机制，形成创新生态体系和产业自主能力，增强我国在全球产业链供应链创新链中的影响力。

着眼增强发展动能，大力打造经济高质量发展新引擎。充分发挥信息化驱动引领作用，加快推进信息化领域重大政策落实、重点任务突破，加快 5G、大数据中心、人工智能、工业互联网等新一代信息基础设施建设，加快培育数据要素市场，发挥数字经济在国内大循环中的关键节点作用和国内国际双循环中的战略链接作用，大力推动数字经济发展，积极培育新业态新模式新应用，打造具有国际竞争力的数字产业集群，做好国家数字经济创新发展试验区扩围和经验总结，推动网信军民融合深度发展，切实以新动能推动高质量发展。

着眼践行根本宗旨，积极拓展信息惠民为民新成果。坚持以人民为中心的发展思想，加快建设数字政府、数字社会，推动新型智慧城市建设，持续加强关键民生领域信息化建设，着力拓展远程医疗、在线教育、共享平台、协同办公等服务应用，强化数字技术在突发公共事件应对工作中的运用，接续推进网络扶贫和数字乡村建设，加快弥合区域间、城乡间、人群间的数字鸿沟，让人民群众在信息化发展中有更多获得感、幸福感、安全感。

着眼防范化解风险，坚决筑牢国家网络安全新屏障。全面加强网络安全保障体系和能力

建设，深入落实网络安全工作责任制，加强关键信息基础设施安全防护，强化网络安全防御能力建设，加快推进关键信息技术国产化替代进程，强化供应链安全，加大个人信息和重要数据保护力度，加强网络安全产业、人才、学科等建设，切实维护国家网络安全和人民群众切身利益。

着眼高水平对外开放，推动形成网络空间国际合作新格局。深入开展网络空间国际交流合作，大力宣介习近平总书记关于构建网络空间命运共同体的理念主张，办好世界互联网大会，积极参与网信领域全球治理改革完善，加快发展跨境电商等新业态新模式，推进 21 世纪数字丝绸之路建设以及 5G 等信息通信技术合作，为建设网络强国创造更加有利的国际环境。

加强党对网信工作的集中统一领导，确保网信事业始终沿着正确政治方向前进

习近平总书记强调，过不了互联网这一关，就过不了长期执政这一关。要毫不动摇坚持党管互联网，加强党对网信工作的集中统一领导，完善党对网信工作的领导方式、体制机制，不断提高政治判断力、政治领悟力、政治执行力，为网络强国建设提供有力保障。

坚持旗帜鲜明讲政治。始终从政治上观察和处理管网治网中的矛盾问题，进一步站稳政治立场、坚定政治方向、提高政治站位、保持政治定力，始终在思想上政治上行动上同以习近平同志为核心的党中央保持高度一致，自觉在增强“四个意识”、坚定“四个自信”、做到“两个维护”上走在前列、作好表率。

进一步提高政治能力。教育引导广大党员干部从我们党经受执政考验、巩固执政地位、提高执政能力的战略高度来认识互联网、运用互联网、发展互联网，切实提高对互联网规律的把握能力、对网络舆论的引导能力、对信息化发展的驾驭能力、对网络安全的保障能力。

完善互联网管理领导体制。紧盯制约网信事业发展的“瓶颈”问题，进一步健全网信工作体系，充分发挥网信部门的统筹协调作用和各部门的职能作用，各司其职、密切配合，加快健全中央、省、市三级网信工作体系，完善工作机制，加强工作力量，切实形成推进网信工作的整体合力。

强化网信干部人才保障。围绕加强对干部“选育管用”综合施策，进一步树立正确的选人用人导向，激励干部担当作为。推动人才发展体制机制改革，加快建立适应网信工作特点的人事、薪酬、职称等制度，为推动网络强国建设提供更加坚实的干部和人才保障。

加强网信领域党的建设。加强互联网企业党的建设，推动互联网企业不断提高政治能力。加强机关党的建设，突出全面从严治党这个关键，深入实施党建高质量发展行动计划，持之以恒正风肃纪，建设让党中央放心、让人民群众满意的模范机关，着力打造忠诚干净担当的

网信铁军。（来源：学习时报 作者：中共中央宣传部副部长，中央网络安全和信息化委员会办公室、国家互联网信息办公室主任庄荣文）

➢ 关于第 47 次《中国互联网络发展状况统计报告》，专家这样说

2021 年 2 月 3 日，中国互联网络信息中心（CNNIC）在京发布第 47 次《中国互联网络发展状况统计报告》（以下简称《报告》）。《报告》显示，截至 2020 年 12 月，我国网民规模达 9.89 亿，较 2020 年 3 月增长 8540 万，互联网普及率达 70.4%。2020 年，我国互联网行业在抵御新冠肺炎疫情和疫情常态化防控等方面发挥了积极作用，为我国成为全球唯一实现经济正增长的主要经济体，国内生产总值（GDP）首度突破百万亿，圆满完成脱贫攻坚任务做出了重要贡献。

互联网基础资源创新发展，数字经济发展全面繁荣

CNNIC 主任曾宇认为，“十三五”期间，我国数字经济欣欣向荣，互联网应用百花齐放，互联网有力支撑新冠肺炎疫情防控，为我国构建以国内大循环为主体、国内国际双循环相互促进的新发展格局提供了强大支撑。本次《报告》主要体现了以下特点：

在数字经济方面，“十三五”期间，党中央总揽全局、擘画蓝图，先后印发了《国家信息化发展战略纲要》《“十三五”国家信息化规划》等政策文件，全面布局产业发展，精准发

力重点领域，为我国数字经济蓬勃发展起到了举旗定向的关键作用。一是产业数字化转型深入推进。2019 年全国县域数字农业农村发展总体水平达 36.0%，其中农业生产数字化水平达 23.8%。截至 2020 年 6 月，全国应用两化融合管理体系标准企业数量突破 2.8 万家，企业数字化研发设计工具普及率达 71.5%，关键工序数控化率达 51.1%。二是数字产业化水平持续提升。五年间，我国网上零售额突破 10 万亿元，年复合增长率为 24.6%，其中实物网上零售额对社会消费品零售总额增长的贡献率达 45.6%。截至 2020 年 12 月，我国跨境电商进出口额已达 1.69 万亿元。

在互联网应用方面，“十三五”期间，我国互联网应用进入大繁荣、大发展时期，极大满足了人民群众生产生活需要，持续释放数字经济惠民红利。一是商务交易类应用打通线上线下，不断扩大产品渠道、创新营销形式，推动网络购物和网络支付用户规模分别较“十二五”末期增长 89.3%和 105.3%。二是网络娱乐类应用推陈出新，内容工艺显著提升，极大丰富了人民群众的业余生活。其中网络视频用户规模达 9.27 亿，较“十二五”末期增长 83.9%，成为第二大网络应用。三是公共服务类应用如在线教育、在线医疗等不断涌现，不断推动优质公共资源向贫困边远地区延伸，促进全国各地网民协同发展、共享互联网发展成果。

在新冠肺炎疫情防控方面，我国较为完备的互联网基础设施和丰富的互联网应用为打赢疫情防控阻击战起到了关键作用。一是网络应用助力疫情防控。网络新闻与社交平台、搜索引擎等互联网应用形成有效联动，团结鼓舞全国人民共同打好抗疫人民战争，帮助人民群众及时获取抗疫动态，做好个人防护，避免疫情进一步扩散。二是模式创新推动复工复产。远程办公、在线教育等新模式有效满足网民工作、学习等切实需要，为全社会“重启”和经济复苏提供强大助力。截至 2020 年 12 月，远程办公应用用户规模达 3.46 亿，较 2020 年 6 月增长 1.47 亿。

全球最大数字社会初步构建，数字红利惠及各类细分群体

CNNIC 副主任张晓发布《报告》并进行了解读，从网民规模和发展方面总结了 2020 年中国互联网的四个发展亮点：

一是近十亿网民构成全球最大网民群体。截至 2020 年 12 月，我国网民规模达 9.89 亿，占全球网民的五分之一，互联网普及率达 70.4%，高于全球平均水平。随着互联网普及和应用水平的持续提升，更多人民群众得以享受到互联网带来的便利，全球最大网民群体逐步形成。

二是网民人口红利呈现“板块漂移”特征。一方面呈现从“城到乡”迁移特征，数字鸿沟进一步缩小。截至 2020 年 12 月，我国城镇网民规模为 6.80 亿，占网民整体的 68.7%；农

村网民规模为 3.09 亿，占网民整体的 31.3%。我国城乡地区互联网普及率差异为 23.9%，2017 年以来首次缩小到 30%以内。另一方面呈现从“东到西”迁移特征，中西部网民用户增长较快。截至 2020 年 12 月，中西部网民规模较 2016 年增长 40%，增速较东部地区高 12.4 个百分点。

三是“00 后”“银发族”构成多元“数字族群”。CNNIC 数据显示，网民增长的主体从青年群体向未成年和老年群体转化的趋势日趋明显。截至 2020 年 12 月，我国已有近 2.6 亿“银发网民”（50 岁以上），以及 1.6 亿 20 岁以下网民。新增网民中，20 岁以下网民占比较该群体在网民整体中的占比高 17.1 个百分点；60 岁以上网民占比较该群体在网民整体中的占比高 11.0 个百分点。

四是网络扶贫为全面建成小康社会提供有力支撑。党的十八大以来，各级政府部门认真贯彻落实习近平总书记关于实施网络扶贫行动的重要指示精神，加快贫困地区信息化、数字化改造进程，充分发挥互联网在精准脱贫中的作用。在网络覆盖方面，贫困村通光纤比例达 98%；在农村电商方面，电子商务进农村实现对 832 个贫困县全覆盖；在网络扶智方面，学校联网加快实施、在线教育加速推广，全国中小学互联网接入率达 99.7%；在信息服务方面，远程医疗实现国家级贫困县县级医院全覆盖。

数字政府建设持续提速，在线服务水平全球领先

中共中央党校（国家行政学院）电子政务研究中心主任、国家电子政务专家委员会副主任王益民表示，2020 年，我国切实践行以人民为中心的发展理念，充分发挥全国一体化服务体系建设成效，大力推进数字政府建设，为扎实做好“六稳”工作，全面落实“六保”任务提供服务支撑。抗击新冠肺炎疫情的迫切需要，更使得数字政府建设步伐进一步加快。本次《报告》数据显示，截至 2020 年 12 月，我国互联网政务服务用户规模达 8.43 亿，较 2020 年 3 月增长 21.6%，全国一体化政务服务平台实名用户总量达 8.09 亿。

在数字政府建设方面，我国互联网政务服务能力进一步增强。各级政府“一网通办”“异地可办”“跨区通办”渐成趋势，“掌上办”“指尖办”逐步成为政务服务标配，营商环境不断优化。

在一体化政务服务平台建设方面，平台“一张网”整体服务能力持续提升。联合国数据显示，我国电子政务发展指数为 0.7948，排名从 2018 年的第 65 位提升至第 45 位，取得历史新高，特别是作为衡量国家电子政务发展水平核心指标的在线服务指数上升为 0.9059，指数排名大幅提升至全球第 9 位。

新基建助推我国经济由大向强，互联网产业动能持续释放

电子工业出版社总编辑兼华信研究院院长刘九如认为，CNNIC 第 47 次《报告》充分表明：“十三五”期间，我国新基建加快推进，为互联网产业快速发展及新一代信息技术更加广泛应用打下坚实基础。在《报告》中表现为以下两个特点：

首先，新基建全面启动，成功助力互联网产业发展和数字经济繁荣。截至 2020 年 12 月，我国已建成 5G 基站 71.8 万个，推动共建共享 5G 基站 33 万个；连接终端超过 1.8 亿个，已建成全球最大的 5G 网络；工业互联网建设稳步推进，培育形成 100 余个具有一定行业、区域影响力的工业互联网平台，连接工业设备 4000 万台（套），产业规模已达 3 万亿元；空天网络设施加快建设，2020 年 6 月我国成功发射北斗系统第 55 颗导航卫星，提前半年全面完成北斗三号全球卫星导航系统星座部署，基于北斗的导航服务已被电子商务、移动智能终端制造、位置服务等领域广泛应用。

其次，高新技术不断突破，释放产业发展动能。随着量子科技成为信息通信技术演进和产业升级的关注焦点，我国在政策布局、技术发展和产业应用方面均取得显著进展。在区块链领域，2020 年全国已建成 40 个区块链产业园区，区块链相关企业数达 64996 家，2020 年上半年区块链产业市场规模 17.15 亿元，同比增长 246.5%。在大数据领域，2020 年我国大数据产业规模突破万亿元，达到了 10100 亿元，同比增长 26.3%。在人工智能领域，新一代人工智能技术正加速在各行业深度融合和落地应用，推动经济社会各领域从数字化、网络化向智能化加速跃升。

互联网基础资源技术持续创新，跨领域融合发展加速深化

中科院网络中心副主任、中国科学院大学教授谢高岗表示，随着互联网相关产业与应用的持续发展，对互联网基础设施的安全稳定运行、互联网体系结构与基础资源技术的创新突破提出了更高的要求。在《报告》中具体表现在以下几点：

一是技术创新突破推动基础资源安全可靠性不断提升。我国深入开展网络体系结构、互联网基础资源解析、网络安全防护相关技术研发工作，从体系结构基础理论、基础资源感知分析关键技术、安全防护系统等形成了专有自主技术体系，有力维护了我国互联网基础设施安全稳定运行。

二是资源公钥基础设施（RPKI）技术稳步发展。包括 CNNIC 在内的国内相关机构持续开展 RPKI 相关工作，研究实现机制，部署测试系统，形成《资源公钥基础设施（RPKI）发展状况及技术趋势报告》等多种研究成果。

三是跨领域融合发展加速深化。我国互联网基础资源技术与大数据、区块链等技术进一步深度融合，先后孵化出国家互联网基础资源大数据（服务）平台、基于区块链的互联网基

础资源管理服务（实验）平台等技术平台，有力支持了互联网基础资源的管理服务需要。（作者：网信中国）

- **第 47 次《中国互联网络发展状况统计报告》全文：**
- http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/202102/P020210203334633480104.pdf

➢ 2020 年《网络安全法》配套规定和标准综述

《网络安全法》作为我国网络安全的基本法，设置了最基本的网络安全制度框架，包括关键信息基础设施保护制度、网络安全等级保护制度、个人信息保护制度、网络信息内容管理制度、网络产品和服务管理制度、网络安全事件应急响应制度等。这些制度设计相对比较原则和简单，需要出台一系列的配套规定予以支撑和落实。围绕《网络安全法》的基本框架，2020 年，国家网信办、工信部、公安部、市场监管总局、中国人民银行以及国家标准化管理委员会等部门相继发布了《网络安全法》的相关配套规定和标准。

一、《网络信息内容生态治理规定》正式施行

国家互联网信息办公室发布的《网络信息内容生态治理规定》（以下称：《治理规定》），自 2020 年 3 月 1 日起正式施行。《治理规定》集中体现了党的十九届四中全会《决定》中提出的“建立健全网络综合治理体系，加强和创新互联网内容建设，落实互联网企业信息管理

主体责任，全面提高网络治理能力，营造清朗的网络空间。加强网络生态治理，培育积极健康、向上向善的网络文化，有利于建立健全网络综合治理体系”的精神，以网络信息内容为主要治理对象，以营造文明健康的良好生态为目标，突出了“政府、企业、社会、网民”等多元主体参与网络生态治理的主观能动性，重点规范网络信息内容生产者，网络信息内容服务平台，网络信息内容服务使用者以及网络行业组织在网络生态治理中的权利与义务，这是我国网络信息内容生态治理法治领域的一项里程碑事件，而且以“网络信息内容生态”作为网络空间治理立法的目标，这在全球也属首创。

《治理规定》将“网络信息内容生态治理”定义为，指政府、企业、社会、网民等主体，以培育和践行社会主义核心价值观为根本，以网络信息内容为主要治理对象，以建立健全网络综合治理体系、营造清朗的网络空间、建设良好的网络生态为目标，开展的弘扬正能量、处置违法和不良信息等相关活动。

《治理规定》要求网络信息内容生产者应当采取措施，防范和抵制制作、复制、发布含有下列八类内容的不良信息：

1. 使用夸张标题，内容与标题严重不符的信息内容。“标题党“是互联网上利用各种颇具创意的标题吸引网友眼球，以达到各种目的，其主要行为简而言之即发帖的标题严重夸张，帖子内容通常与标题完全无关或联系不大，诸如震惊、惊爆、重磅、罕见、深度好文、轰动全国、绝密偷拍的字眼。笔者在网上搜索了类似“震惊 13 亿中国人”、“感动了中国 13 亿人”、“重磅”、“深度好文”等标题，其内容与标题完全不符，多数以夸张的、曲解的、煽情的甚至无中生有的方式误导网民。

2. 炒作绯闻、丑闻、劣迹等信息内容。当前，娱乐界炒作绯闻、丑闻以及劣迹比比皆是，以明星绯闻八卦为噱头，特别是通过明星和狗仔队的配合来制造绯闻、丑闻、劣迹的热度，这些低俗文化和行为愚弄了大众、污染了网络、触碰了法律，必须依法治理。

3. 不当评述自然灾害、重大事故等灾难的信息内容。我国地域广、人口密集，自然灾害种类多，重大安全事故时有发生。笔者注意到，每当自然灾害和重大安全事故等灾难发生时，总有一些没有事实依据的评述，不仅混淆了是非，而且给社会带来极大的负面影响，必须坚决予以抵制。

4. 带有性暗示、性挑逗等易使人产生性联想的信息内容。为了吸引流量，一些网络平台，以文字、语音、图片、视频等方式进行带有“性挑逗”、“性暗示”的不良行为，比如所谓的“文爱”、“磕炮”等，这些信息内容均带有性暗示或性挑逗的潜淫秽内容，极容易使人产生性联想。

我国《刑法》对淫秽物品的定义是，具体描绘性行为或者露骨宣扬色情的诲淫性的书刊、影片、录像、图片等，但是将有关人体生理、医学知识的科学著作和包含有色情内容的有艺术价值的文学、艺术作品排除在淫秽物品范围之外。

5. 展现血腥、惊悚、残忍等致人身心不适的信息内容。一些网络内容制作者为了骗取用户的点力量，发布和展示血腥、惊悚、残忍的图片和视频，如有的网站发布大量令人不适的惊悚、血腥、虐杀动物、畸形胎儿的图片，同时还兼有“标题党”嫌疑，致人身心感到极大地不适，尤其是对未成年的心理损害极其严重。

6. 煽动人群歧视、地域歧视等的信息内容。煽动是指怂恿、鼓动人做坏事的行为，我们经常在网上看到，一些仅凭自己看到的只言片语就在网上传播并发布地域歧视和人群歧视等过激言论。如有一则“医院多次医疗事故不能给公众解释”的网络帖子，煽动当地人群对医生群体的歧视，该发布者因涉嫌寻衅滋事被公安机关行政拘留 10 日。

7. 宣扬低俗、庸俗、媚俗内容的信息内容。主要是两类信息内容，一是低俗的内容，主要是指低级趣味、庸俗，使人萎靡、颓废的内容；二是媚俗的信息内容，主要是那些迎合于世俗，缺乏自我思想、自我理智，只知随波逐流，芸芸众生等，这些低俗、庸俗、媚俗的信息内容与我国优秀道德文化和时代精神格格不入，必须坚决抵制。

8. 可能引发未成年人模仿不安全行为和违反社会公德行为、诱导未成年人不良嗜好等的信息内容。当前，我国未成年人网民数量近 1.7 亿，智能手机成为未成年人上网的主要工具，未成年人正处于青春躁动期，有很强的求知欲望，他们对网络发布的一些不安全和违反公德的信息内容鉴别力很弱、自控能力较差，很容易在模仿后导致恶性事件的发生，未成年人模仿网络不良行为已经成为威胁青少年网络安全的主要因素。

二、《信息安全技术 个人信息安全规范》正式实施

2020 年 3 月 6 日，国家市场监督管理总局、国家标准化管理委员会发布的中华人民共和国国家标准公告（2020 年第 1 号），全国信息安全标准化技术委员会归口的 GB/T 35273-2020《信息安全技术 个人信息安全规范》正式发布，并将于 2020 年 10 月 1 日实施。

本标准针对个人信息面临的安全问题，根据《中华人民共和国网络安全法》等相关法律，严格规范个人信息在收集、存储、使用、共享、转让与公开披露等信息处理环节中的相关行为，旨在遏制个人信息非法收集、滥用、泄露等乱象，最大程度的保护个人的合法权益和社会公众利益。本标准适用于规范各类组织的个人信息处理活动,也适用于主管监管部门、第三方评估机构等组织对个人信息处理活动进行监督、管理和评估。

本标准按照 GB/T1.1—2009 给出的规则起草，代替 GB/T35273—2017《信息安全技术 个

人信息安全规范》。相比 GB/T35273—2017，此标准除了授权同意、账户注销、实现个人信息主体自主意愿的方法等内容的修改外，还新增了多项业务功能的自主选择、用户画像、个性化展示、个人信息汇聚融合、个人信息安全工程、第三方接入管理等相关要求。

新标准的主要变化如下：

1. 删除了原有的“不得收集法律法规明令禁止收集的个人信息”的要求(见 5.1);

2. 选择同意原则下，新增要求“多项业务功能的自主选择”(见 5.3)；

当产品或服务提供多项需收集个人信息的业务功能时，个人信息控制者不应违背个人信息主体的自主意愿，强迫个人信息主体接受产品或服务所提供的业务功能及相应的个人信息收集请求”。

3. 新增关于收集人生物识别信息的要求，《规范》规定在收集个人生物识别信息前，应单独向个人信息主体告知收集、使用个人生物识别信息的目的、方式和范围，以及存储时间等规则，并征得个人信息主体的明示同意。

对于生物识别信息的存储，《规范》也提出了具体的解决措施。1）个人生物识别信息要与个人身份信息分开存储；2）原则上不应存储原始个人生物识别信息，可采取的措施包括但不限于：仅存储个人生别信息的摘要信息；在采集终端中直接使用个人生物识别信息实现身份识别、认证等功能；在使用面部识别特征、指纹、掌纹、虹膜等实现识别身份、认证等功能后删除可提取个人生物识别信息的原始图像。

4. 在目的明确原则下，新增要求“如产品或服务仅提供一项收集、使用个人信息的业务功能时，个人信息控制者可通过隐私政策的形式，实现向个人信息主体的告知；产品或服务提供多项收集、使用个人信息的业务功能的，除隐私政策外，个人信息控制者宜在实际开始收集特定个人信息时，向个人信息主体提供收集、使用该个人信息的目的、方式和范围，以便个人信息主体在作出具体的授权同意前，能充分考虑对其的具体影响”。

5. 在选择同意原则下，强调了“隐私政策的主要功能为公开个人信息控制者收集、使用个人信息范围和规则，不应将其视为个人信息主体要求签订的合同”。

6. 确保安全原则下，新增多项要求：一是将个人生物识别信息的原始信息和摘要分开存储的技术要求(见 5.4)；二是在信息系统自动决策机制的使用中定期（至少每年一次）开展个人信息安全影响评估，并依评估结果采取有效的保护个人信息主体的措施、向个人信息主体提供针对自动决策结果的申诉渠道，并对自动决策结果进行人工复核；三是明确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。如采用公布投诉、举报方式等信息并及时受理投诉举报、与监督、管理部门保持沟通，通报或报

告个人信息保护和事件处置等情况等；四是要求组织记录的内容包括：所涉及个人信息的类型、数量、来源（例如从个人信息主体直接收集或通过间接获取方式获得）；五是根据业务功能和授权情况区分个人信息的处理目的、使用场景，以及委托处理、共享、转让、公开披露、是否涉及出境等情况。

7. 在最少够用的原则下，新增多项要求：1）要求了用户个人画像的特征描述不能为“淫秽、色情、赌博、迷信、恐怖、暴力”；业务运营或对外业务合作中使用用户画像不能侵害保护公民、法人和其他组织的合法权益，不能危害国家安全、荣誉和利益；2）除为达到主体授权同意的使用目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人；3）在向主体推送新闻信息服务的过程中使用个性化展示时应：显著区分个性化推送服务，如标明“个性化展示”或“定推”等字样，为主体提供简单直观的退出或关闭个性化展示模式的选项；4）电子商务经营者根据消费者的兴趣爱好、消费习惯等特征向其提供商品或者服务搜索结果的个性化展示的，应当同时向该消费者提供不针对其个人特征的选项；5）在向主体提供业务功能的过程中，如使用个性化展示时，建立个人信息主体对个性化展示所依赖的个人信息（如标签、画像维度等）的自主控制机制，保障个人信息主体调控个性化展示相关程度的能力；6）当个人信息主体选择退出个性化展示模式时，应向个人信息主体提供删除或匿名化定向推送活动所基于的个人信息的选项。

8. 在公开透明原则的原则下，新增要求应向主体提供查询方法，能让主体知晓持有的个人信息的类型；上述个人信息的来源、所用于的目的；已经获得上述个人信息的第三方身份或类型；宜直接在产品或服务提供的功能界面中（例如应用程序可设置专门的选项、功能、界面等）设置相应的机制，便于个人信息主体在线行使其访问、更正、删除、撤回授权同意、注销账户等权利。

9. 新增的其他要求包括：应承担第三方接入管理；收集年满 14 周岁未成年人的个人信息前，应征得未成年人或其监护人的明示同意；不满 14 周岁的，应征得其监护人的明示同意等。

三、《网络安全标准实践指南—移动互联网应用程序(App)收集使用个人信息自评估指南(征求意见稿)》公开征求意见

为落实《网络安全法》相关要求，围绕中央网信办、工信部、公安部、市场监管总局联合制定的《App 违法违规收集使用个人信息行为认定方法》，基于 App 专项治理工作组发布的《App 违法违规收集使用个人信息自评估指南》，全国信息安全标准化技术委员会秘书处组织编制了《网络安全标准实践指南—移动互联网应用程序（App）收集使用个人信息自评

估指南》（以下简称《实践指南》），并于 2020 年 7 月 22 日公开征求意见。

《实践指南》归纳总结了 App 收集使用个人信息的六项评估点，供 App 运营者自评估参考使用，小程序、快应用等运营者也可参考其中的适用条款进行自评估。

评估点一：是否公开收集使用个人信息的规则。重点落实《网络安全法》第 41 条规定，网络运营者收集、使用个人信息， 应当公开收集、使用规则。《消费者权益保护法》第 29 条规定，经营者收集、使用消费者 个人信息，“应当公开其收集、使用规则”；

评估点二：是否明示收集使用个人信息的目的、方式和范围。重点落实《网络安全法》第 41 条规定，网络运营者收集、使用个人信息， 应当公开收集、使用规则。《消费者权益保护法》第 29 条规定，经营者收集、使用消费者个人信息，“应当公开其收集、使用规则”；

评估点三：收集使用个人信息是否征得用户同意。重点落实《网络安全法》第 41 条规定网络运营者收集、使用个人信息， 应“经被收集者同意”且“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”。《消费者权益保护法》第 29 条规定经营者收集、使用消费者个 人信息，应“经消费者同意”且“不得违反法律、法规的规定和双方的约定收集、使用信息”，“经营者未经消费者同意或者请求，或者消 费者明确表示拒绝的，不得向其发送商业性信息；

评估点四：是否遵循必要原则，仅收集与其提供的服务直接相关的个人信息，比如是否收集与业务功能无关的个人信息，包括不应收集与业务功能无关的个人信息以及不应申请打开与业务功能无关的可收集个人信息的权限等；

评估点五：是否未经同意向他人提供个人信息，比如向他人提供个人信息前是否征得用户同意，App 是否存在从客户端直接向第三方发送个人信息的情形，包括通过 App 客户端嵌入第三方代码、插件（如 SDK）等方式，应事先征得用户同意，经匿名化处理的除外等；

评估点六：是否按法律规定提供删除或更正个人信息功能，或公布投诉、举报方式等信息 比如是否提供有效的注销用户账号功能，是否提供有效的更正或删除个人信息，是否建立并公布个人信息安全投诉、举报渠道等。

四、全国信安标委发布《信息安全技术 个人信息告知同意指南（征求意见稿）》

2020 年 1 月，全国信息安全标准化技术委员会发布《关于国家标准<信息安全技术 个人信息告知同意指南>征求意见稿征求意见的通知》，就个人信息告知同意国家标准（以下称《告知同意指南》）征求意见。该征求意见稿包括告知同意的适用情形、免于告知同意的情形、告知同意的基本原则、告知、同意等部分，并在附录中详细列举了未成年人、SDK（软件开发工具包）、个性化推荐，以及互联网金融、网上购物等场景下的具体情形。

关于“告知”的基本原则包括公开透明、逐一传达、同步实时、真实准确、具体明确、清晰易懂；根据不同的场景，告知方式可以采用弹窗、文字说明、短信、邮件、电话等。征求意见稿要求，当告知的时间点和收集个人信息的时间点相差很大时，建议个人信息控制者在进一步收集个人信息之前再次告知。《指南》要求，个人信息控制者应当避免告知的频率过高，对个人信息主体造成不必要的打扰。

五、国家网信办等十二部门发布《网络安全审查办法》

2020 年 4 月 13 日，国家互联网信息办公室、国家发改委等 12 个部门联合发布了《网络安全审查办法》（以下简称《办法》），该办法自 2020 年 6 月 1 日起实施。

《办法》明确指出，关键信息基础设施运营者采购网络产品和服务，影响或可能影响国家安全的，应当进行网络安全审查。根据《办法》第九条的规定，网络安全审查重点评估采购网络产品和服务可能带来的国家安全风险，主要考虑以下因素：一是产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏，以及重要数据被窃取、泄露、毁损的风险；三是产品和服务供应中断对关键信息基础设施业务连续性的危害；四是产品和服务提供者遵守中国法律、行政法规、部门规章情况；五是其他可能危害关键信息基础设施安全和国家安全的因素。

《办法》进一步明确了审查内容，包括：产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏，以及重要数据被窃取、泄露、毁损的风险；产品和服务供应中断对关键信息基础设施业务连续性的危害；产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；产品和服务提供者遵守中国法律、行政法规、部门规章情况；其他可能危害关键信息基础设施安全和国家安全的因素。

六、中国人民银行发布《个人金融信息保护技术规范》

2020 年 2 月 13 日，中国人民银行正式发布了《个人金融信息保护技术规范》（JR/T 0171—2020）金融行业标准。《个人金融信息保护技术规范》（以下简称：《规范》）由全国金融标准化技术委员会归口管理，由中国人民科技司提出并负责起草。

个人金融信息是个人信息在金融领域围绕账户信息、鉴别信息、金融交易信息、个人身份信息、财产信息、借贷信息等方面的扩展与细化，是金融业机构在提供金融产品和服务的过程中积累的重要基础数据，也是个人隐私的重要内容。个人金融信息一旦泄露，不但会直接侵害个人金融信息主体的合法权益、影响金融业机构的正常运营，甚至可能会带来系统性金融风险。

《规范》规定了个人金融信息在收集、传输、存储、使用、删除、销毁等生命周期各环节的安全防护要求，从安全技术和安全管理两个方面，对个人金融信息保护提出了规范性要求。

《规范》的发布和实施，有助于规范金融业机构个人金融信息保护工作，提升金融数据风险防控能力，促进我国金融市场的健康发展；有助于提高金融机构个人账户信息、银行卡信息安全管理水平，加大互联网交易风险防控力度，防范各类金融交易风险，切实维护金融稳定，保护金融消费者合法权益。虽然《规范》在性质上属于推荐性标准，但作为第一部专门针对个人金融信息的行业标准，为金融业机构建设个人金融信息保护架构提供了体系化与专业化的参考标准，同时也会成为未来金融领域数据隐私保护立法和执法的重要参考。

七、中国人民银行发布新版《网上银行系统信息安全通用规范》

2020 年 2 月 5 日，新修订的金融行业标准《网上银行系统信息安全通用规范》（JR/T 0068—2020）由中国人民银行正式发布。标准规定了网上银行系统安全技术要求、安全管理要求、业务运营安全要求，为网上银行系统建设、运营及测评提供了依据。标准适用于中华人民共和国境内设立的商业银行等银行业金融机构所运营的网上银行系统，其他金融机构提供网上金融服务的业务系统宜参照本标准执行。

本次标准修订，立足于移动互联和云计算等新技术在网上银行系统不断深入应用、手机银行使用愈加广泛的背景，旨在应对网上银行系统信息安全出现的新形势和新特点，防范新风险。本标准的发布实施，将有效增强现有网上银行系统安全防范能力，促进网上银行规范、健康发展。标准既可作为各单位网上银行系统建设、改造升级以及开展安全检查、内部审计的安全性依据，也可作为行业主管部门、专业检测机构进行检查、检测的依据。

八、《网络安全标准实践指南—移动互联网应用程序（App）个人信息安全防范指引（征求意见稿）》公开征求意见

2020 年 3 月 30 日，全国信息安全标准化技术委员会发布关于《网络安全标准实践指南—移动互联网应用程序（App）个人信息安全防范指引（征求意见稿）》公开征求意见的通知。《移动互联网应用程序（App）个人信息安全防范指引（征求意见稿）》（以下简称《防范指引》）给出了当前 App 个人信息保护合规的常见问题和防范策略，共包含十个常见问题，每个问题下面包含若干情形和若干条防范策略。其中包含超范围收集、申请权限目的不明、强制捆绑授权等等。

《防范指引》给出 App 超范围收集个人信息的问题情形，包括但不限于：

情形一：收集无关信息。收集的个人信息类型或申请的系统权限与 App 提供的业务功

能无关。例如未提供短信相关功能的 App 申请短信权限。

情形二：强制收集非必要信息。因用户不同意收集非必要个人信息或打开非必要权限，App 拒绝提供业务功能。必要个人信息是指保障 App 业务功能正常运行所最少够用的个人信息，包括一旦缺少将导致 App 服务无法实现或无法正常运行的个人信息，以及法律法规要求必须收集的个人信息。例如浏览器 App 强制索要位置权限收集个人位置信息，用户拒绝提供位置权限则无法使用 App 任何功能。

情形三：收集频率不合理。收集个人信息的频率超出 App 业务功能实际需要。例如酒店预订 App 每 1 秒上传一次用户精确定位信息。

该问题的防范策略，包括但不限于：

1．不收集与 App 所提供服务无关的个人信息，不申请与 App 所提供服务无关的系统权限（即使用户可选择拒绝）。

2．遵循最小必要原则，仅收集/申请与 App 业务功能有直接关联的个人信息类型/系统权限。

3．App 收集个人信息前向用户明示收集信息的目的、方式和范围，并征得用户同意，告知同意方式应符合相关法律法规、政策和标准的要求。

4．收集个人信息的频率应在 App 实现业务功能所必需的合理范围内。

5．App 尽量避免收集不可变更的设备唯一标识（如 IMEI 号、MAC 地址等），用于保障网络安全和运营安全的除外。

6．App 收集疫情联防联控所必需的个人信息坚持最小范围原则，收集对象原则上限于确诊者、疑似者、密切接触者等重点人群，一般不针对特定地区的所有人群。

7．针对一些没有高风险的区域、场所或不涉及高风险人群，疫情防控 App 宜尽可能缩小身份登记的个人信息填写范围，达到可追溯的目的即可。例如，收集个人信息可参考“前台匿名，后台实名”等方式，用户可提供手机号，无需填写身份证号或上传身份证图片。

九、公安部发布《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》

2020 年 9 月，公安部网络安全保卫局发布《贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》（以下称：《指导意见》）。

《指导意见》确立了三项基本原则和四大工作目标：

（一）三项基本原则

1. 坚持分等级保护、突出重点。根据网络(包含网络设施、信息系统、数据资源等)在国

家安全、经济建设、社会生活中的重要程度，以及其遭到破坏后的危害程度等因素，科学确定网络的安全保护等级，实施分等级保护、分等级监管，重点保障关键信息基础设施和第三级(含第三级、下同)以上网络的安全。

2. 坚持积极防御、综合防护。按照法律法规和有关国家标准规范，充分利用人工智能、大数据分析等技术，积极落实网络安全管理和技术防范措施，强化网络安全监测、态势感知、通报预警和应急处置等重点工作，综合采取网络安全保护、保卫、保障措施，防范和遏制重大网络安全风险、事件发生，保护云计算、物联网、新型互联网、大数据、智能制造等新技术应用和新业态安全。

3. 坚持依法保护、形成合力。依据《网络安全法》等法律法规规定，公安机关依法履行网络安全保卫和监督管理职责，网络安全行业主管部门(含监管部门，下同)依法履行网络安全主管、监管责任，强化和落实网络运营者主体防护责任，充分发挥和调动社会各方力量，协调配合、群策群力，形成网络安全保护工作合力。

（二）四大工作目标

1. 网络安全等级保护制度深入贯彻实施。网络安全等级保护定级备案、等级测评、安全建设和检查等基础工作深入推进。网络安全保护“实战化、体系化、常态化”和“动态防御、主动防御、纵深防御、精准防护、整体防控、联防联控”的“三化六防”措施得到有效落实，网络安全保护良好生态基本建立，国家网络安全综合防护能力和水平显著提升。

2. 关键信息基础设施安全保护制度建立实施。关键信息基础设施底数清晰，安全保护机构健全、职责明确、保障有力。在贯彻落实网络安全等级保护制度的基础上，关键信息基础设施涉及的关键岗位人员管理、供应链安全、数据安全、应急处置等重点安全保护措施得到有效落实，关键信息基础设施安全防护能力明显增强。

3. 网络安全监测预警和应急处置能力显著提升。跨行业、跨部门、跨地区的立体化网络安全监测体系和网络安全保护平台基本建成，网络安全态势感知、通报预警和事件发现处置能力明显提高。网络安全预案科学齐备，应急处置机制完善，应急演练常态化开展，网络安全重大事件得到有效防范、遏制和处置。

4. 网络安全综合防控体系基本形成。网络安全保护工作机制健全完善，党委统筹领导、各部门分工负责、社会力量多方参与的网络安全工作格局进一步完善。网络安全责任制得到有效落实，网络安全管理防范、监督指导和侦查打击等能力显著提升，“打防管控”一体化的网络安全综合防控体系基本形成。

《指导意见》要求，各单位、各部门应加强关键信息基础设施安全的法律体系、政策体

系、标准体系、保护体系、保卫体系和保障体系建设，建立并实施关键信息基础设施安全保护制度，在落实网络安全等级保护制度基础上，突出保护重点，强化保护措施，切实维护关键信息基础设施安全。

十、全国信安标委发布《信息安全技术 关键信息基础设施边界确定方法（征求意见稿）》

2020 年 8 月，全国信息安全标准化技术委员会发布《信息安全技术 关键信息基础设施边界确定方法》（征求意见稿）。本文件给出了一种基于信息流的关键信息基础设施边界确定方法，为关键信息基础设施运营者开展关键信息基础设施边界识别工作提供参考。

《关键信息基础设施边界确定方法》对关键信息基础设施边界的相关术语和定义做出了定义：

1．关键业务（critical business）电信、广播电视、能源、金融、交通运输、水利、应急管理、卫生健康、社会保障、国防科技等行业和领域中一旦遭到破坏或者丧失功能，会严重危害国家安全、经济安全、社会稳定、公众健康和安全的业务。

2．网络设施（network facilities）连接通信信息网络（例如，互联网、物联网、工控网、专用网等）以及在上述网络中对信息进行设计、采集、整合、处理、呈现、应用、存储、销毁等操作的物理设备。

3．信息系统（information system）由计算机软硬件、网络及其相关配套设备、信息资源等组成的，按照一定规则对信息进行设计、采集、整合、处理、呈现、应用、存储、销毁等操作的人机系统。（来源：GB/T 20986—2007，2.1，有修改）

4．关键信息基础设施（critical information infrastructure）支撑关键业务持续、稳定运行不可或缺的网络设施、信息系统。在形态构成上，可以是单个网络设施、信息系统，也可以是由多个网络设施、信息系统组成的集合。在本质上，属于关键业务的信息化部分，为关键业务提供信息化支撑。

5．关键信息基础设施元素（critical information infrastructure element）对构成关键信息基础设施的网络设施、信息系统的统称，是关键信息基础设施边界识别的最小单元。

6．关键业务信息（critical business information）关键业务持续、稳定运行不可或缺的信息，是关键信息基础设施元素对关键业务提供信息化支撑的桥梁和纽带。关键信息基础设施元素通过对关键业务信息进行设计、采集、整合、处理、呈现、应用、存储、销毁等操作，支撑关键业务自动化、智能化、高效运行。

7．关键业务信息流（critical business information flow）关键业务信息从产生到终止，在整个生存周期内的流动轨迹，处于该流动轨迹上的网络设施、信息系统是关键信息基础设施

候选元素，经关键性评估，一旦遭到攻击、丧失功能或者数据泄露会严重危害关键业务持续、稳定运行的网络设施、信息系统列为关键信息基础设施元素。

8．关键信息基础设施边界（critical information infrastructure boundary）以关键业务为基础，由识别方法和关键信息基础设施元素构成，反映关键信息基础设施元素与关键业务之间的支撑、依赖关系以及关键信息基础设施元素的分布、部署情况，是开展保护、审查、应急处置等工作的重要依据。

《关键信息基础设施边界确定方法》确立了关键信息基础设施边界识别的四项基本原则：

一是业务安全原则：CII 的重要性不是指组成 CII 的网络设施、信息系统很重要，而是因为 CII 所支撑的关键业务非常重要。CII 一旦遭到攻击、丧失功能或者数据泄露会严重危害关键业务正常运行，进而危害国家安全、经济安全、社会稳定、公众健康和安全。因此，CII 边界识别应以保障关键业务安全为基本原则，将关键业务持续、稳定运行不可或缺的网络设施、信息系统识别出来，明确 CII 元素、确定 CII 边界。注：例如，2G 移动通信网络曾是国家重点保护目标，时至今日，支撑 2G 移动通信业务的网络设施、信息系统已失去了重点保护的意义，因为 2G 移动通信业务已被 3G、4G 通信业务所取代。

二是整体性原则：随着经济社会的不断发展，业务规模越来越大，不同业务模块、子业务之间相互依赖、彼此支撑，CII 边界识别应注重关键业务的整体性，确保关键业务的完整性，避免遗漏。此外，跨行业、跨领域已是普遍现象，涉及多个运营者的，应加强信息共享和联动协调，确保 CII 边界识别是从保障整个关键业务安全的角度开展。注：例如，导航业务涉及到卫星、通信链路和直接向用户提供导航服务的三个部分，且每部分由不同的运营者负责经营。每个运营者在开展 CII 边界识别时，首先应确保自身经营业务的完整，还应注重整体协调，从保障整个导航业务持续、稳定的角度考虑。

三是重要性原则：在 CII 运营者所有网络设施、信息系统中，有些网络设施、信息系统对关键业务的持续、稳定运行是至关重要的，有些网络设施、信息系统仅仅是比较重要的，甚至有一些网络设施、信息系统对关键业务是无关紧要的，因此，开展 CII 边界识别应聚焦一旦遭到破坏、丧失功能或者发生数据泄露，会严重危害关键业务持续、稳定运行的网络设施、信息系统，严格控制范围。

四是动态识别原则：CII 与关键业务之间的支撑、依赖关系是动态的，而非静态的。CII 边界识别应采用动态工作方式，及时更新 CII 边界信息。

当 CII 运营者的组织结构、业务架构、从属关系等发生重大调整时，应及时实施边界识

别工作，确保 CII 边界及时调整。

十一、全国信安标委发布《信息安全技术 网络数据处理安全规范（征求意见稿）》

2020 年 8 月，全国信息安全标准化技术委员会秘书处发布《信息安全技术 网络数据处理安全规范》（征求意见稿），《网络数据处理安全规范》规定了网络运营者利用网络开展数据收集、存储、使用、加工、传输、提供、公开等数据处理活动应遵循的规范和安全要求。

本规范适用于网络运营者规范数据处理活动，提高数据安全管理和个人信息保护水平，也适用于主管监管部门对网络运营者数据处理活动进行监督管理，同时还可为第三方评估机构开展相关评估工作提供指导。

《网络数据处理安全规范》对与网络数据处理有关的术语和定义做出了规定：

1. 数据（data）：本文件所称数据是指网络数据，即通过网络处理和产生的各种电子数据，如个人信息、重要数据等。

2. 网络运营者（network operator）：网络的所有者、管理者和网络服务提供者。

3. 个人信息（personal information）：以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息。注：个人信息包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。

4. 个人敏感信息（personal sensitive information）：一旦泄露、非法提供或者滥用可能危害人身和财产安全，极易导致个人名誉、身心健康受到损害或者歧视性待遇等的个人信息。注：个人敏感信息包括自然人的身份证件号码、生物识别信息、银行账号、通信记录和内容、财产信息、征信信息、行踪信息、住址、健康信息、交易信息、14 岁以下（含）儿童的个人信息等。

5. 个人信息主体（personal data subject）：个人信息能够识别或者关联到的自然人。

6. 重要数据（key data）：一旦泄露可能直接影响国家安全、公共安全、经济安全和社会稳定的数据，包括未公开的政府信息，数量达到一定规模的基因、地理、矿产信息等，原则上不包括个人信息、企业内部经营管理信息等。

7. 数据提供方（data provider）：数据处理活动中提供数据的组织或者个人。

8. 数据接收方（data receiver）：数据处理活动中接收数据的组织或者个人。

9. 第三方应用（third party application）：由第三方提供的产品或者服务，以及被接入或者嵌入网络运营者产品或者服务的自动化工具，包括但不限于软件开发工具包（SDK 等）、第三方代码、组件、脚本、接口、算法模型、小程序等。

10. 匿名化（anonymization）：是指对个人信息进行加工，使之无法识别特定个人且不

能复原。

《网络数据处理安全规范》对数据处理提出了四项要求：

一是数据识别：网络运营者应识别数据处理活动中涉及的数据，包括个人信息、重要数据和其他数据，形成数据保；

二是分级分类：网络运营者应按照法律法规、国家标准有关要求，根据业务运营需要，对所掌握的数据进行分级分类管理；采取加密、脱敏、访问控制等措施，对重要数据和个人信息进行重点保护；

三是风险防控：网络运营者开展数据处理活动，应按照有关法律法规的规定履行数据安全保护义务，采取加密、脱敏、备份、访问控制、审计等技术或者其他必要措施，加强数据安全防护，保护数据免受泄露、窃取、篡改、损毁、不正当使用等。建立数据安全管理责任和评价考核制度，制定数据安全保护计划，开展安全风险评估，及时处置安全事件，组织开展教育培训；

四是审计追溯：网络运营者应对数据处理活动的全生命周期进行记录，确保数据处理活动可审计、可追溯。

十二、中国人民银行印发《金融数据安全数据安全分级指南》

2020 年 9 月，中国人民银行正式印发《金融数据安全数据安全分级指南》(JR/T0197—2020)(下称《指南》)，根据金融业机构数据安全性遭受破坏后的影响对象和所造成的影响程度，将数据安全级别由高到低划分为五级。

《指南》列出的影响对象包括国家安全、公众权益、个人隐私、企业合法权益等;影响程度从高到低划分为非常严重、严重、中等和轻微;附录中给出了金融行业典型数据类型及建议划分的最低安全级别。值得注意的是，《指南》特别强调金融业机构应高度重视个人金融信息相关数据，在数据安全定级过程中从高考虑。

其中，个人金融信息中的 C3 类信息(主要为用户鉴别信息，如各类账户密码)属于 4 级数据;C2 类信息(主要包括支付账号、动态口令等)为 3 级数据;C1 类信息(主要包括账户开立时间、开立机构等)为 2 级数据。

金融数据安全分级的大背景是金融数据作为生产要素的价值日益凸显。近年来，随着金融科技和数字经济的发展，金融数据体现出巨大的应用和商业价值。与此同时，数据安全尤其个人隐私保护成为公众关注的焦点。

十三、工信部组织开展 2020 年网络安全技术应用试点示范工作

2020 年 7 月，工业和信息化部办公厅发布《关于开展 2020 年网络安全技术应用试点示

范工作的通知》（以下称：《通知》）。

《通知》了三大重点方向：

（一）新型信息基础设施安全类

1. 5G 网络安全。重点结合增强移动带宽、低时延高可靠、海量大连接三大场景安全需求，针对网络功能虚拟化、网络切片、边缘计算等带来的网络安全需求，在威胁监测、风险识别、安全防御、安全检测、安全恢复、安全模型认证等方面的安全解决方案。

2. 工业互联网安全。围绕装备、电子信息、原材料、消费品、石化、能源等重点生产制造领域，结合工业互联网智能化生产、网络化协同、个性化定制、服务化延伸等典型应用场景网络安全需求，在网络、平台、工控设备、工业 APP、工业数据等方面的安全解决方案。

3. 车联网安全。结合先进驾驶辅助、自动驾驶、车路协同、智慧交通等典型场景，针对智能驾驶系统、车联网平台、无线通信、复杂环境感知、车用高精度时空服务等网络安全需求，在安全认证、安全防护、数据保护、威胁监测、测试验证等方面的安全解决方案。

4. 智慧城市安全。面向智慧政务、智能生活、智能医疗、在线教育、远程办公、智慧环保等典型应用场景网络安全需求，在新型智慧城市设施、建设、运行、服务、管理等方面的安全解决方案。

5. 大数据安全。面向大数据中心、智能计算中心、云计算平台等先进算力设施的网络安全解决方案，以及结合海量网络数据汇聚存储、流动共享等安全需求，在数据资产识别、分类分级防护、数据加密、数据脱敏、泄露追溯等方面的解决方案。

6. 物联网安全。结合智慧家庭、智能抄表、零售服务、智能安防、智慧物流、智慧农业等典型场景网络安全需求，在物联网卡、物联网芯片、联网终端、网关、平台和应用等方面的基础管理、可信接入、威胁监测、态势感知等安全解决方案。

7. 人工智能安全。结合智能机器人、智能语音交互、视频图像身份识别、影像辅助诊断、无人机等典型应用场景网络安全需求，在人工智能数据、算法、平台、应用服务等方面的安全解决方案，以及运用人工智能技术的高级威胁预警、网络资产管理、网络行为溯源分析等安全解决方案。

8. 区块链安全。结合供应链管理、电子交易、数字版权、保险、社会救助等区块链技术典型应用场景网络安全需求，在身份验证、安全存储、存证取证、数据共享流通等方面的安全解决方案，以及区块链基础设施、区块链平台、区块链服务等方面的安全监测、防护、测试验证解决方案。

9. 商用密码应用。针对商用密码在 5G、工业互联网、车联网领域业务应用场景，在密

码算法、密码设备、检测认证服务等方面的解决方案，以及应用商用密码的网络身份认证、设备安全接入认证等解决方案。

10. 电信网络诈骗防范治理。围绕电信网络诈骗技术防范、管理创新、联防联控等安全需求，在涉诈风险实时预警处置、诈骗行为精准分析、远程智能群呼设备监测定位取证、电信网络诈骗协同分析治理等方面的解决方案。

（二）网络安全公共服务类

1. 安全防护。基于云模式提供安全检测、风险评估、流量清洗、域名安全等技术服务的公共服务平台。

2. 安全运营。面向智能制造、智能家居、智慧医疗、智慧交通等重点领域提供网络安全运营服务的公共服务平台。

3. 威胁情报。提供网络安全威胁在线查询、漏洞验证、关联分析、开放共享等信息服务的公共服务平台。

4. 安全培训。提供安全课堂、在线测试、培训认证、攻防模拟等培训服务的公共服务平台。

（三）网络安全“高精尖”技术创新平台类

面向新型信息基础设施安全类、网络安全公共服务类重点方向，以及拟态防御、可信计算、零信任、安全智能编排等前沿性、创新性、先导性的重大网络安全技术理念，汇聚产学研用等创新资源，具备核心技术攻关、产业化应用推广等关键环节协同创新环境和载体的网络安全技术创新或试点示范区。

十四、工信部发布《电信和互联网行业数据安全标准体系建设指南》

为发挥标准对电信和互联网行业数据安全的规范和保障作用，进一步加快制造强国和网络强国建设的步伐，工信部印发《电信和互联网行业数据安全标准体系建设指南》。

2020 年 8 月，工信部公开征求对《电信和互联网行业数据安全标准体系建设指南（征求意见稿）》的意见。征求意见稿表示，在基础共性标准、关键技术标准、安全管理标准的基础上，结合新一代信息通信技术发展情况，重点在 5G、移动互联网、车联网、物联网、工业互联网、云计算、大数据、人工智能、区块链等重点领域进行布局，并结合行业发展情况，逐步覆盖其他重要领域。结合重点领域自身发展情况和数据安全保护需求，制定相关数据安全标准。

当前，我国电信和互联网行业高速发展，汇聚大量数据，在释放数字经济发展潜力、促进数字经济加快成长的同时，面临严峻的安全风险。“安全发展、标准先行”，标准化工作是

保障数据安全的重要基础。

由工业和信息化部组织制定的《电信和互联网行业数据安全标准体系建设指南》，是为了深入落实《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《电信和互联网用户个人信息保护规定》等法律法规要求，以保障电信和互联网行业数据安全为主线，着力增加标准有效供给，不断完善技术标准体系，持续推动标准的制定、实施和国际化，支撑和引领数字经济高质量发展。

《电信和互联网行业数据安全标准体系建设指南》提出，到 2021 年，研制数据安全行业标准 20 项以上，初步建立电信和互联网行业数据安全标准体系，有效落实数据安全管理要求，基本满足行业数据安全保护需要，推动标准在重点领域中的应用。到 2023 年，研制数据安全行业标准 50 项以上，健全完善电信和互联网行业数据安全标准体系，标准的技术水平、应用效果和国际化程度显著提高，有力支撑行业数据安全保护能力提升。

十五、国家网信办发布《常见类型移动互联网应用程序（App）必要个人信息范围》公开征求意见

2020 年 12 月，国家互联网信息办公室发布通知，就《常见类型移动互联网应用程序（App）必要个人信息范围》（下称《App 必要个人信息范围》）公开征求意见。《App 必要个人信息范围》规定了地图导航、网络约车、即时通信、网络支付、网上购物、交通票务、婚恋相亲、问诊挂号、旅游服务、网络游戏、学习教育、用车服务、网络直播等 38 类常见类型 App 必要个人信息范围。

《App 必要个人信息范围》明确，“必要个人信息”：是指保障 App 基本功能正常运行所必须的个人信息，缺少该信息 App 无法提供基本功能服务，即无须个人信息，即可使用基本功能服务。规定指出，只要用户同意收集必要个人信息，App 不得拒绝用户安装使用。（来源：中国信息安全）

四、政府之声

➢ 国家七部门联合发布《关于加强网络直播规范管理工作的指导意见》

2021 年 2 月 9 日，国家互联网信息办公室、全国“扫黄打非”工作小组办公室等七部门联合发布《关于加强网络直播规范管理工作的指导意见》（以下简称《意见》），旨在进一步加强网络直播行业的正面引导和规范管理，重点规范网络打赏行为，推进主播账号分类分级管理，提升直播平台文化品位，促进网络直播行业高质量发展。

一段时间以来，网络直播行业存在传播历史虚无主义、淫秽色情信息，打“擦边球”和危害青少年身心健康等违法违规乱象。同时，暴露出主体责任履行不力、主播良莠不齐、充值打赏失范等问题。为了聚焦解决行业突出问题，净化直播行业生态，国家互联网信息办公室、全国“扫黄打非”工作小组办公室、工业和信息化部、公安部、文化和旅游部、国家市场监督管理总局、国家广播电视总局联合制定实施该《意见》。

国家互联网信息办公室有关负责人指出，出台《意见》的主要目的，是为了督促直播平台对照相关规范，对主播账号实行分级分类管理，规范网络主播行为，防范非理性、激情打赏，遏制商业营销乱象。以强化高品位文化产品供给为目标，推动网络直播平台强化主流价值引领，树牢正确导向意识，大力弘扬社会主义核心价值观，有效提升直播平台“以文化人”的精神气质和文化力量。

《意见》强调，网络直播平台要建立健全直播账号分类分级规范管理制度、直播打赏服

务管理规则和直播带货管理制度，要针对不同类别级别的网络主播账号在单场受赏总额、直播热度等方面合理设限，要对单个虚拟消费品、单次打赏额度合理设置上限，对单日打赏额度累计触发相应阈值的用户进行消费提醒，必要时设置打赏冷静期和延时到账期。

《意见》要求，各地各部门要切实履行职能职责，依法依规加强对网络直播行业相关业务的监督管理，督导企业落实主体责任。网络社会组织要积极发挥桥梁纽带作用，大力倡导行业自律。鼓励社会各界，尤其是网络直播用户广泛参与网络直播行业治理，为广大网民特别是青少年营造积极健康、内容丰富、正能量充沛的网络直播空间。（来源：国家互联网信息办公室）

- **关于印发《关于加强网络直播规范管理工作的指导意见》的通知**
- **全文：**http://www.cac.gov.cn/2021-02/09/c_1614442843753738.htm

➢ 工信部印发《工业互联网创新发展行动计划（2021-2023 年）》的通知

2021 年 2 月 18 日，工业互联网专项工作组针对 2021 年 1 月 13 日印发《工业互联网创新发展行动计划（2021-2023 年）》（工信部信管〔2020〕197 号，以下简称《三年行动计划》）。现就《三年行动计划》有关内容解读如下：


中华人民共和国工业和信息化部
Ministry of Industry and Information Technology of the People's Republic of China

访客预约 | RSS订阅

统一搜索

看新闻 找文件 查办事 提意见 查数据 要投诉

工业和信息化部 新闻动态 政务公开 政务服务 公众参与 工信数据 专题专栏

首页 > 政务公开 > 政策解读

《工业互联网创新发展行动计划（2021-2023年）》解读

发布时间：2021-02-18 08:29 来源：信息通信管理局

近日，工业互联网专项工作组印发《工业互联网创新发展行动计划（2021-2023年）》（工信部信管〔2020〕197号，以下简称《三年行动计划》）。现就《三年行动计划》有关内容解读如下：

1、《三年行动计划》的出台背景是什么？

工业互联网是新一代信息通信技术与工业经济深度融合的全新工业生态、关键基础设施和新型应用模式。它以网络为基础、平台为中枢、数据为要素、安全为保障，通过对人、机、物全面连接，变革传统制造模式、生产组织方式和产业形态，构建起全要素、全产业链、全价值链全面连接的新型工业生产制造和服务体系，对支撑制造强国和网络强国建设，提升产业链现代化水平，推动经济高质量发展和构建新发展格局，都具有十分重要的意义。

1、《三年行动计划》的出台背景是什么？

工业互联网是新一代信息通信技术与工业经济深度融合的全新工业生态、关键基础设施和新型应用模式。它以网络为基础、平台为中枢、数据为要素、安全为保障，通过对人、机、物全面连接，变革传统制造模式、生产组织方式和产业形态，构建起全要素、全产业链、全价值链全面连接的新型工业生产制造和服务体系，对支撑制造强国和网络强国建设，提升产

业链现代化水平，推动经济高质量发展和构建新发展格局，都具有十分重要的意义。

过去三年是工业互联网起步发展期，工业和信息化部会同工业互联网专项工作组各单位，实施《工业互联网发展行动计划（2018-2020 年）》，发布实施十余项落地性文件，不断完善政策体系，实施工业互联网创新发展工程，带动总投资近 700 亿元，遴选 4 个国家级工业互联网产业示范基地和 258 个试点示范项目，打造了一批高水平的公共服务平台，培育了一批龙头企业和解决方案供应商。网络基础、平台中枢、数据要素、安全保障作用进一步显现，工业互联网新型基础设施不断夯实，新模式新业态创新活跃，产业生态不断壮大，各地方、产业各界共识不断凝聚，积极性不断提升，为下一步发展打下坚实基础。

未来三年是工业互联网的快速成长期。为深入贯彻习近平总书记对工业互联网的一系列重要指示精神，落实党中央、国务院决策部署，进一步巩固提升发展成效，更好地谋划推进未来一个阶段发展工作，工业互联网专项工作组制定出台了《工业互联网创新发展行动计划（2021-2023 年）》。

2、《三年行动计划》的主要内容是什么？

《三年行动计划》结合当前产业发展实际和技术产业演进趋势，确立了未来三年我国工业互联网发展目标。到 2023 年，新型基础设施进一步完善，融合应用成效进一步彰显，技术创新能力进一步提升，产业发展生态进一步健全，安全保障能力进一步增强。工业互联网新型基础设施建设量质并进，新模式、新业态大范围推广，产业综合实力显著提升。

《三年行动计划》提出了五方面、11 项重点行动和 10 大重点工程，着力解决工业互联网发展中的深层次难点、痛点问题，推动产业数字化，带动数字产业化。

在基础设施建设方面，一是实施网络体系强基行动，推进工业互联网网络互联互通工程，推动 IT 与 OT 网络深度融合，在 10 个重点行业打造 30 个 5G 全连接工厂。二是实施标识解析增强行动，推进工业互联网标识解析体系增强工程，完善标识体系构建，引导企业建设二级节点不少于 120 个、递归节点不少于 20 个。三是实施平台体系壮大行动，推进工业互联网平台体系化升级工程，推动工业设备和业务系统上云上平台数量比 2020 年翻一番。

在持续深化融合应用方面，一是实施数据汇聚赋能行动，制定工业大数据标准，促进数据互联互通。二是实施新型模式培育行动，推进工业互联网新模式推广工程，培育推广智能化制造、网络化协同、个性化定制、服务化延伸、数字化管理等新模式。三是实施融通应用深化行动，推进工业互联网融通应用工程，持续深化“5G+工业互联网”融合应用。

在强化技术创新能力方面，一是实施关键标准建设行动，推进工业互联网标准化工程，实施标准引领和标准推广计划，完成 60 项以上关键标准研制。二是实施技术能力提升行动，

推进工业互联网技术产品创新工程，加强工业互联网基础支撑技术攻关，加快新型关键技术与产品研发。

在培育壮大产业生态方面，一是实施产业协同发展行动，推进工业互联网产业生态培育工程，培育技术创新企业和运营服务商，再建设 5 个国家级工业互联网产业示范基地，打造 10 个“5G+工业互联网”融合应用先导区。二是实施开放合作深化行动，营造开放、多元、包容的发展环境，推动多边、区域层面政策和规则协调，支持在自贸区等开展新模式新业态先行先试。

在提升安全保障水平方面，实施安全保障强化行动，推进工业互联网安全综合保障能力提升工程，完善网络安全分类分级管理制度。加强技术创新突破，实施保障能力提升计划，推动中小企业“安全上云”，强化公共服务供给，培育网络安全产业生态。

此外，结合重点任务和突出问题，从组织实施、数据管理、资金保障、人才保障四方面明确了支撑要素和政策措施。

3、未来三年，如何进一步夯实工业互联网网络基础？

未来三年，网络领域继续着眼构筑支撑工业全要素、全产业链、全价值链互联互通的网络基础设施，加快企业外网和企业内网建设与改造，提升基础支撑能力。一是推动企业内网由“单环节改造”向“体系化互联”转变。推动工业生产装备和仪器仪表的数字化、网络化改造，让哑设备“活起来”；运用先进适用的网络技术建设 IT-OT 融合网络，把工业全流程的都“连起来”；建立标准化的网络信息模型，让以前难交互、难集成的异构数据都“动起来”。二是推动企业外网由“建网”向“用网”转变。在继续强调提升高质量外网承载能力和互通水平的同时，进一步引导工业企业、工业互联网平台、标识解析节点等接入高质量外网，让企业外网真正“用起来”，提升企业外网应用效能。三是拓展“5G+工业互联网”发展新空间。持续实施“5G+工业互联网”512 工程，深化核心应用，推动应用领域从工业外围环节向生产制造核心环节拓展；优化应用模式，推动应用重心从单点孵化向 5G 全连接工厂拓展；强化产业支撑，加强 5G 工业模组研发、5G 工业互联网专用频率研究、5G 专网建设方案落地。四是探索央地协同发展新模式。充分调动地方积极性，支持各地建设具有地方特色、产业特点的工业互联网园区网络；依托工业互联网产业示范基地遴选和建设工作，引导产业聚集好、带动作用强的地区积极创建“5G+工业互联网”先导区。

4、工业互联网标识解析体系下一步发展重点是什么？

未来三年，我们将通过实施“标识解析增强行动”，从做大规模、做深应用、规范管理三方面进一步提升我国标识解析体系的发展水平。

第一，做大规模。我国标识解析体系建设虽然取得了一定成绩，但与我国制造业门类、体量相比，覆盖范围还不足，因此标识解析体系各级节点的建设还要拓展覆盖范围、完善节点布局。我们将进一步完善国家顶级节点与国际根节点的对接，增强国家顶级节点的服务能力，面向更多行业、更多区域推动建设不少于 120 个二级节点、不少于 20 个递归节点。同时，我们还将探索利用区块链技术构建基于标识的融合型基础设施，支持各地部署不少于 20 个融合节点。

第二，做深应用。建设目的还是应用，不然就成了“烂尾楼”“断头路”，同时与建设相比应用的难度更大，我们将进一步调动各方面积极性，加强标识解析体系的深层次应用。一是深化标识在各行业的推广应用。通过组织开展全国工业互联网标识创新大赛遴选典型案例加强示范推广，特别是应对疫情，我们将拓展标识在冷链物流、应急物资等领域规模化应用。我们还将增强标识资源对接、测试认证等公共服务能力，建立产业链供应链标识数据资源共享机制，促进标识的行业应用推广。二是深化标识在各环节的应用。加强标识解析系统与工业企业信息系统适配，推动标识解析系统与工业互联网平台、工业 APP 等融合发展，深化标识在设计、生产、服务等环节应用，发挥出标识在促进跨企业数据交换、提升产品全生命周期追溯和质量管理水平中的作用。三是大力拓展主动标识。按照标识载体类型，标识应用分为静态标识应用和主动标识应用。静态标识应用以二维码、射频识别码（RFID）、近场通信标识（NFC）等作为载体，借助扫码枪或支付宝“扫一扫”功能等识读软硬件获取信息。主动标识应用通过在芯片、通信模组、终端中嵌入标识，由网络主动向解析节点发送解析请求，无需借助外部设备。这是我们下一步推动的工作重点，未来三年将部署不少于 3000 万枚主动标识载体。

第三，规范管理。去年 12 月，工信部为贯彻落实中央经济工作会议关于加强规制、提升监管能力的相关要求，印发了《工业互联网标识管理办法》，目的就是更好的促进工业互联网标识解析体系建设，更好的规范标识市场主体行为、激发创新发展活力，从制度方面规范各方行为、维护市场秩序。办法将于今年 6 月 1 日实施，我们将组织开展相关宣贯活动，推动各地抓好许可审批，加强监督检查。

5、下一步工业互联网平台工作有哪些具体考虑？

未来，我们将从“建平台、用平台、筑生态”三方面共同推进，加快工业互联网平台体系化升级。

一是“建平台”，构建“综合型+特色型+专业型”工业互联网平台体系。滚动遴选跨行业跨领域综合型工业互联网平台，建立动态评价机制，打造 3-5 个具有国际影响力的工业互

联网平台，深化工业资源要素集聚，加速生产方式和产业形态创新变革。建设面向重点行业和区域的特色型工业互联网平台，推动行业知识经验在平台沉淀集聚，推动平台在“块状经济”产业集聚区落地。发展面向特定技术领域的专业型工业互联网平台。推动前沿技术与工业机理模型融合创新，支撑构建新型制造体系。

二是“用平台”，加快工业设备和业务系统上云上平台。制定工业设备上云实施指南、工业设备数据字典，推动行业龙头企业核心业务系统云化改造，带动产业链上下游企业业务系统云端迁移。鼓励地方政府通过创新券、服务券等形式降低上云门槛和成本、扩大上云范围，创新 “挖掘机指数”“空压机指数”等新型经济运行指标。

三是“筑生态”，持续提升平台应用服务水平。围绕“平台+产品”“平台+模式”“平台+行业/区域”等领域打造一批创新解决方案，加快系统解决方案供应商培育。编制完善工业互联网平台监测评价指标体系，支持建设平台数据监测与运行分析系统，开展平台基础能力、运营服务、产业支撑等运行数据的自动化采集。

6、如何进一步发挥数据在工业互联网创新发展中的重要作用？

数据是平台应用的关键资源，为推动数据汇聚、流转、分析、应用，我们将开展“数据汇聚赋能行动”，主要围绕四方面开展有关工作，综合构建数据驱动新生态。

一是打造数据汇聚的载体，推动工业互联网大数据中心建设。提升数据统筹汇聚能力的同时推动数据高效分级分类，完善国家级中心建设，围绕重点行业建设分中心，针对中小微企业需求搭建个性化公共服务平台，聚焦核心区域建设大数据区域分中心，大幅提升数据汇聚能力、丰富数据资源池，建设数据灾备中心，保障国家网络信息安全。通过研究数据权属确定、价值评估、资源交换、效益共享等机制与接口标准规范，打通国家中心、分中心之间数据链条，健全工业互联网大数据中心数据流通机制。

二是提升数据价值挖掘能力，打造大数据中心综合服务体系。一方面，针对政府监管施政需求，重点打造工业经济和产业运行监测指挥、应急事件预警协调等服务能力，支撑政府提升管理水平。另一方面，针对行业发展需求，打造数据管理能力提升、工业资源共享、解决方案推广、设备与业务系统上云、产融合作、供需对接等服务能力。

三是促进数据流动，推动平台间数据互联互通。建立标准机制，推动平台间数据字典互认，建设统一的工业数据、算法模型、微服务等调用接口。加强平台间合作，联合开展重点问题攻关，实现优势互补，通过统一接口规范，推动机理模型和工业 APP 的跨平台调用与订阅。

四是推动数据知识共享，培育和推广高质量工业 APP。对于共性工业经验知识，打造基

础共性工业 APP 和可适性工业 APP；对于行业工业知识，打造高价值、易推广的行业通用工业 APP；对于特定领域、特定场景的独特工业经验知识，培育企业专用工业 APP。通过构建工业智能解决方案、开源社区、开发者社区、工业 APP 商店等举措，促进工业 APP 交易流转。

7、未来将采取哪些措施推动工业互联网应用创新？

工业互联网融合应用不同于互联网创新应用，工业互联网的主战场在实体经济，特别是工业领域，面向工业、立足工业、服务工业。这要求工业互联网必须与各行业各领域技术、知识、经验、痛点紧密结合，多元性、专业性、复杂性高，这决定了推动工业互联网融合应用需要持续发力，久久为功，重点加强三个方面的工作。

第一，推动形成各方积极参与的团体赛模式。工业互联网是涉及设施建设、融合应用、技术创新、产业生态和安全保障的融合性、系统性工程，企业不能单打独斗。要充分调动工业企业、基础电信企业、工业软件企业、工业控制企业、设备制造企业、解决方案提供商等各方积极性，推动形成主体多元、协同创新的产业生态和“团体赛”模式。进一步发挥工业互联网专项工作组协调机制作用，形成跨部门、跨领域、跨行业合力，完善政策体系和推进措施。鼓励各地工业和信息化主管部门、通信管理局加强协同，形成推动合力。

第二，突出工业细分场景特点。工业互联网面向千行百业，可以说是一米的宽度、五十到一百米的深度，需要与各行业的生产实践、行业特性、知识经验紧密结合，不断突破行业技术壁垒和数据共享障碍。我们将进一步深化工业互联网在各细分领域的应用创新，探索符合行业发展实际需求的智能化制造、网络化协同、规模化定制、服务化延伸、数字化管理等新模式，加强 5G 和工业互联网的融合应用。我们鼓励“跨行业、跨领域”平台的发展，更强调培育聚焦行业特点的专业型、特色型平台，实现精耕细作，产生实效。

第三，推动产业数字化，带动数字产业化。通过发展工业互联网，促进数字经济进一步壮大，不断形成先进生产力，推动工业化与信息化在更广范围、更深程度、更高水平上实现融合发展。一方面，发挥新一代信息技术优势，打造工业全要素、全产业链、全价值链互联互通的新型基础设施、新型应用模式和全新产业生态，激发数据要素作用，促进制造业数字化、网络化、智能化升级。另一方面，为 5G、云计算、边缘计算、人工智能等新一代信息通信技术落地开辟更广阔空间，并带动自动化、软件、网络等产业实现高端化突破，不断培育壮大新技术新产业。

8、开展工业互联网安全工作的总体思路和主要内容是什么？

安全是工业互联网高质量发展的重要前提和保障。近年来，工信部会同相关部门大力推

进工业互联网安全保障体系建设，政府指导、企业主责的安全管理制度初步形成，可感可知的安全技术监测服务体系初步构建，安全产品和服务供给不断增强、监测预警、信息共享、通报处置闭环工作机制初步建立，工业互联网安全相关工作取得阶段性进展。

随着我国工业互联网发展进入新阶段，设备联网、企业上云等情况日益增多，安全风险随之加剧，对网络安全工作提出更高要求。与此同时，工业互联网安全仍面临着工业企业网络安全意识不高、技术防护能力不足、安全监测能力不强、网络安全产业支撑不够等问题。

行动计划坚持问题导向和目标导向，强化前瞻性、创新性、落地性，明确了以落实企业主体责任为导向、以加强安全供给为重点、以培育安全产业为支撑、以强化技术监测服务能力为抓手的工作思路，力争切实建立起制度更加健全、技术更加先进、政企更加协同的安全保障体系。

行动计划安全部分主要包括以下四方面工作。一是落实企业主体责任，实施分类分级管理。针对重要行业的重点企业，实施网络安全分类分级管理制度，明确不同类型企业安全基线要求，进一步推动企业主体责任落实。二是强化产业协同，推进供给侧加快创新。围绕工业互联网产品内嵌安全、企业上云安全等迫切需求，从网络安全技术、安全产品、安全服务等方面引导创新加速，加大安全公共服务能力建设，丰富安全解决方案有效供给。三是加强示范引领，促进安全产业发展壮大。着眼构建网络安全产业良性发展生态体系，优化国家网络安全产业园区布局，培育安全龙头企业和特色企业，开展试点示范，进一步促进安全产业发展壮大。四是坚持专项带动，提升安全技术监测服务能力。进一步提升企业自身防护、区域监测保障、国家协调服务三方面能力，打造多方联动、运行高效的安全技术监测服务体系。

9、《三年行动计划》中提出实施工业互联网企业网络安全分类分级管理制度，具体内容和下一步安排分别是什么？

目前我国联网工业企业数量众多，涉及行业众多，存在信息化发展程度不一、承载业务类型相异、所属行业安全保护规律差异化明显等特点，难以采取“一刀切”的网络安全管理模式。2019 年工信部与国资委等十部门联合印发的《加强工业互联网安全工作指导意见》明确提出要对工业互联网企业实施网络安全分类分级管理，集中力量指导重要行业、重点企业建立安全防护能力，提升安全防护水平。开展分类分级管理，一是进一步贯彻指导意见有关要求，督促企业落实主体责任，健全完善部门协同、政府指导、企业主责的网络安全管理体系；二是指导地方主管部门形成工业互联网企业清单，建立健全定级核查、信息通报、监测预警、安全检查等机制，集中力量指导管理重点企业；三是通过标准规范引领推动企业贯标达标，促进工业互联网企业网络安全防护能力提升。

分类分级管理着力打造“1+4”的制度体系。1 项《工业互联网企业网络安全分类分级管理指南》，明确将工业互联网企业分为联网工业企业、平台企业、标识解析企业等三类，结合企业所属行业的重要性、企业规模、应用工业互联网程度、网络安全风险程度等因素，将企业分成三个级别，同时明确定级流程和安全管理、支持保障等方面的要求。4 项《工业互联网企业网络安全分类分级防护规范》，针对联网工业企业、平台企业、标识解析企业以及工业互联网数据四类对象，分别明确防护要点和不同级别的网络安全防护要求。

今年 1 月 13 日，工信部印发《开展工业互联网企业网络安全分类分级管理试点工作的通知》，启动部署分类分级试点工作。结合各地工业互联网发展实际，目前选定上海、江苏、广东等 15 个省（区、市）232 家重点工业行业的重点企业参与试点。试点工作由各省工业和信息化主管部门与通信管理局共同组织实施，包括自主定级、定级核查、落实安全要求、试点工作总结四个阶段，计划今年 10 月底前完成试点工作。通过试点进一步完善《管理指南》，提升《安全规范》的科学性、有效性和指导性，形成可复制可推广的安全管理模式。

（来源：工业和信息化部）

- **关于印发《工业互联网创新发展行动计划（2021-2023 年）》的通知 全文：**
- https://www.miit.gov.cn/ztzl/rdzt/gyhlw/wjfb/art/2021/art_6706d89a6cbc49cea75e8d47d4787064.html

➢ 国家网信办启动 2021“清朗·春节网络环境”专项行动

2021 年 2 月 4 日，为营造欢乐喜庆、健康祥和的春节网上氛围，国家网信办决定即日起开展为期 1 个月的“清朗·春节网络环境”专项行动。

此次专项行动将围绕改善和保障广大网民上网体验，重点针对门户网站、搜索引擎、浏览导航、弹窗广告等信息入口和资讯推荐、生活服务、社交平台、论坛社区、直播、短视频等应用环节，对色情、暴力、赌博以及低俗、媚俗、庸俗等问题予以坚决治理，对影响群众生产生活的谣言和虚假信息予以坚决打击。重点清理网站平台首页首屏、热搜榜、话题榜、重点推荐板块、弹窗等关键位置的违法和不良信息，防止低俗化炒作；集中整治生活服务类平台推送不良广告行为，特别是为低俗网文引流问题；严格规范直播、短视频类网站平台网红主播行为，引导其言行符合社会主流价值观；严厉打击各类公众账号借春节话题开展恶意营销的行为，清理恶意炒作、断章取义、拼接转载等不实信息；重点整治不良网络社交行为和网络暴力现象，打击诱导未成年人应援打榜、刷量控评行为，整治煽动“粉丝”互撕和进行网络欺凌的行为。

国家网信办有关负责人表示，2021 年是开启全面建设社会主义现代化国家新征程的起步之年，也是中国共产党成立 100 周年的大庆之年，各地网信部门要按照《网络信息内容生态治理规定》相关要求，精心制定工作方案，压实网站平台责任，通过专项行动集中解决群众反映强烈、影响上网观感的网络生态问题，深入开展清理整治，合力净化网络环境，为全国人民凝心聚力开启新征程营造积极良好氛围，为广大群众过一个喜庆祥和的春节营造健康清朗环境。（来源：中国网信网）

➢ 工业和信息化部组织召开 APP 个人信息保护监管座谈会

2021 年 2 月 5 日，APP 个人信息保护监管座谈会在京召开。工业和信息化部党组成员、副部长刘烈宏出席会议并讲话。

会议通报了近期 APP 个人信息保护工作情况。针对 APP 过度索取麦克风、相册、通讯录等权限问题，工业和信息化部专题开展技术检测，对发现存在问题的 179 款 APP 提出了责令限期整改，对其中未按期整改的 26 款 APP 予以公开通报。会议介绍了正在起草的《移动互联网应用程序个人信息保护管理暂行规定》有关情况，与会专家学者和企业负责人进行了研讨交流。电信终端产业协会发布了 9 项《APP 收集使用个人信息最小必要评估规范》系列标准。

刘烈宏指出，党中央、国务院高度重视个人信息保护工作，工业和信息化部强化责任担当，从制度体系建设、标准制定完善、技术手段支撑和企业自律示范四个方面大力开展相关

工作，取得阶段性成效。主要互联网企业、终端企业和安全企业践行承诺，支持平台建设，为 APP 治理作出积极贡献。刘烈宏强调，要继续坚持问题导向，重点解决“麦克风权限滥用”“未经用户同意擅自读写相册”“过度索取通讯录”“隐藏个推关闭选项”等当前用户反映强烈的热点问题。

刘烈宏要求，把握新形势、群策群力，打好综合治理组合拳：一是要稳步增强依法治理能力。进一步完善《移动互联网应用程序个人信息保护管理暂行规定》，加快文件出台进程，推动治理工作制度化、常态化。二是要大幅提高专题治理成效。重点对违规调取语音权限等问题进行深入研究，把问题找准、把根源挖深，对着症结精准发力。三是要持续提升技术治理水平。高效推进全国 APP 技术检测平台建设，形成全年检测 180 万款的覆盖能力。四是要充分发挥舆论监督治理作用。督促企业强化自律，树立高压红线意识，履行法律义务和社会责任。

部信息通信管理局负责同志参加会议。中国信息通信研究院、北京互联网法院、中国消费者协会、北京航空航天大学、中国人民大学等单位的专家学者，百度、腾讯、阿里巴巴、美团、字节跳动、京东、滴滴、新浪微博、快手、小米、OPPO、360、捷兴信源、梆梆等 14 家企业负责人参会研讨。（来源：工业和信息化部）

五、本期重要漏洞实例

➢ 关于微软 Windows 操作系统存在 TCP/IP 高危漏洞的安全公告

发布日期：2021-2-11
更新日期：2021-2-11
受影响系统：
Windows 7 SP1-Windows10 20H2
Windows Server 2008-Windows Server 20H2
描述：

CVE(CAN) ID: CNTA-2021-0005
2021 年 2 月 10 日，微软 Microsoft 在 2 月例行补丁日发布了 2 个 TCP/IP 高危漏洞（CVE-2021-24074/CVE-2021-24086）的补丁，这些漏洞影响绝大部分支持的 Windows 版本中的 TCP/IP 协议栈。CVE-2021-24074 被标记为远程代码执行漏洞，出现此漏洞的原因由于两个数据包分片之间的 IPv4 选项字段错误，导致操作系统 IP 分片重新组装期间出现超出范围的读取和写入。攻击者可以通过构造特殊的 IP 源路由数据包触发漏洞，成功利用此漏洞的攻击者可能获得在目标服务器上执行任意代码的能力。CVE-2021-24086 被标记为拒绝服务类型，攻击者可以通过发送多个精心制作的 IPv6 数据包（多个 IP 包头、无效包头、多个分片头等）触发漏洞，该漏洞利用成功可能导致目标主机发生蓝屏。
CNVD 对上述两个漏洞的综合评级为“高危”。
建议：

厂商补丁：
经综合技术研判，由于上述两个漏洞的威胁程度高，范围广。攻击者如果成功利用，可能导致受害组织内部信息系统瘫痪或失守。微软公司已发布了修复上述两个漏洞的安全补丁，CNVD 建议用户开启 Windows 自动更新程序进行自动修复，或者从微软官方下载补丁进行手动修复。
目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://msrc.microsoft.com/update-guide/zh-cn/vulnerability/CVE-2021-24074
https://msrc.microsoft.com/update-guide/zh-cn/vulnerability/CVE-2021-24086
https://msrc.microsoft.com/update-guide/releaseNote/2021-Feb
附：参考链接：
https://msrc.microsoft.com/update-guide/zh-cn/vulnerability/CVE-2021-24074
https://msrc.microsoft.com/update-guide/zh-cn/vulnerability/CVE-2021-24086
https://msrc.microsoft.com/update-guide/releaseNote/2021-Feb

➢ Oracle Business Intelligence Enterprise Edition 信息泄露漏洞

发布日期：2021-2-1
更新日期：2021-2-1
受影响系统：
Oracle Business Intelligence Enterprise Edition 11.1.1.9.0

Oracle Business Intelligence Enterprise Edition 12.2.1.3.0
Oracle Business Intelligence Enterprise Edition 12.2.1.4.0
Oracle Oracle Business Intelligence Enterprise Edition 5.5.0.0.0
描述：

CVE(CAN) ID: CVE-2021-2003
Oracle Fusion Middleware（Oracle 融合中间件）是美国甲骨文（Oracle）公司的一套面向企业和云环境的业务创新平台。该平台提供了中间件、软件集合等功能。
Oracle Fusion Middleware 的 Oracle Business Intelligence Enterprise Edition 5.5.0.0、11.1.1.9.0、12.2.1.3.0 和 12.2.1.4.0 版本的 Analytics Web Dashboards 组件存在信息泄露漏洞。未经身份认证的攻击者可利用该漏洞通过 HTTP 网络访问破坏 Oracle Business Intelligence Enterprise Edition，对 Oracle Business Intelligence Enterprise Edition 某些可访问数据进行未授权更新、插入和删除，并对其可访问数据的子集进行未授权读取访问。
建议：

厂商补丁：
Oracle
目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://www.oracle.com/security-alerts/cpujan2021.html

➢ Cisco IOS XR 拒绝服务漏洞

发布日期：2021-2-5
更新日期：2021-2-5
受影响系统：
Cisco IOS XR
描述：

CVE(CAN) ID: CVE-2021-1268
Cisco IOS XR 软件是用于服务提供商网络的模块化和完全分布式的网络操作系统。
Cisco IOS XR 的 IPv6 协议处理存在拒绝服务漏洞。该漏洞源于该软件未正确转发具有 IPv6 节点本地多播组地址目标并在管理界面上接收的 IPv6 数据包。攻击者可利用该漏洞导致网络性能下降或拒绝服务。
建议：

厂商补丁：
Cisco
厂商已发布了漏洞修复程序，请及时关注更新：
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-xripv6-spJem78K

➢ 多款华为产品信息泄露漏洞

发布日期：2021-02-02
更新日期：2021-02-05
受影响系统：
Huawei USG9500 V500R005C00SPC200
Huawei USG9500 V500R001C60SPC500
Huawei USG9500 V500R001C30SPC200
Huawei USG9520 V500R005C00
Huawei USG9560 V500R005C00
Huawei USG9580 V500R005C00
描述：

CVE(CAN) ID: CVE-2021-22309
Huawei USG9500 数据中心防火墙，定位于保护云服务提供商、大型数据中心、以及大型企业园区网络业务安全。Huawei USG9500、USG9520、USG9560 和 USG9580 存在信息泄露漏洞。该漏洞源于某模块在一个安全机制中使用弱随机参数作为输入。攻击者可通过暴力破解利用该漏洞获得敏感信息，导致信息泄露。
链接：https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210202-01-fw-en
建议：

厂商补丁：
Huawei
Huawei 已经为此发布了一个安全公告（huawei-sa-20210202-01-fw）以及相应补丁:
huawei-sa-20210202-01-fw：Security Advisory - Information Leakage Vulnerability in Huawei Products
链接：https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210202-01-fw-en

六、本期网络安全事件

➢ Yandex 抓到内鬼:一名员工私下出售用户电子邮件收件箱的访问权限

2021 年 2 月 13 日，俄罗斯搜索引擎和电子邮件提供商 Yandex 今天表示，它抓住了一名员工出售用户电子邮件账户的访问权限以谋取私利。该公司没有透露这名员工的姓名，称此人是其 Yandex.Mail 服务的 "三名拥有必要访问权限的系统管理员之一，负责提供技术支持"。

这家俄罗斯公司表示：目前正在通知被泄露的 4887 个邮箱的所有者，该员工将这些邮箱的访问权限出售给了第三方。

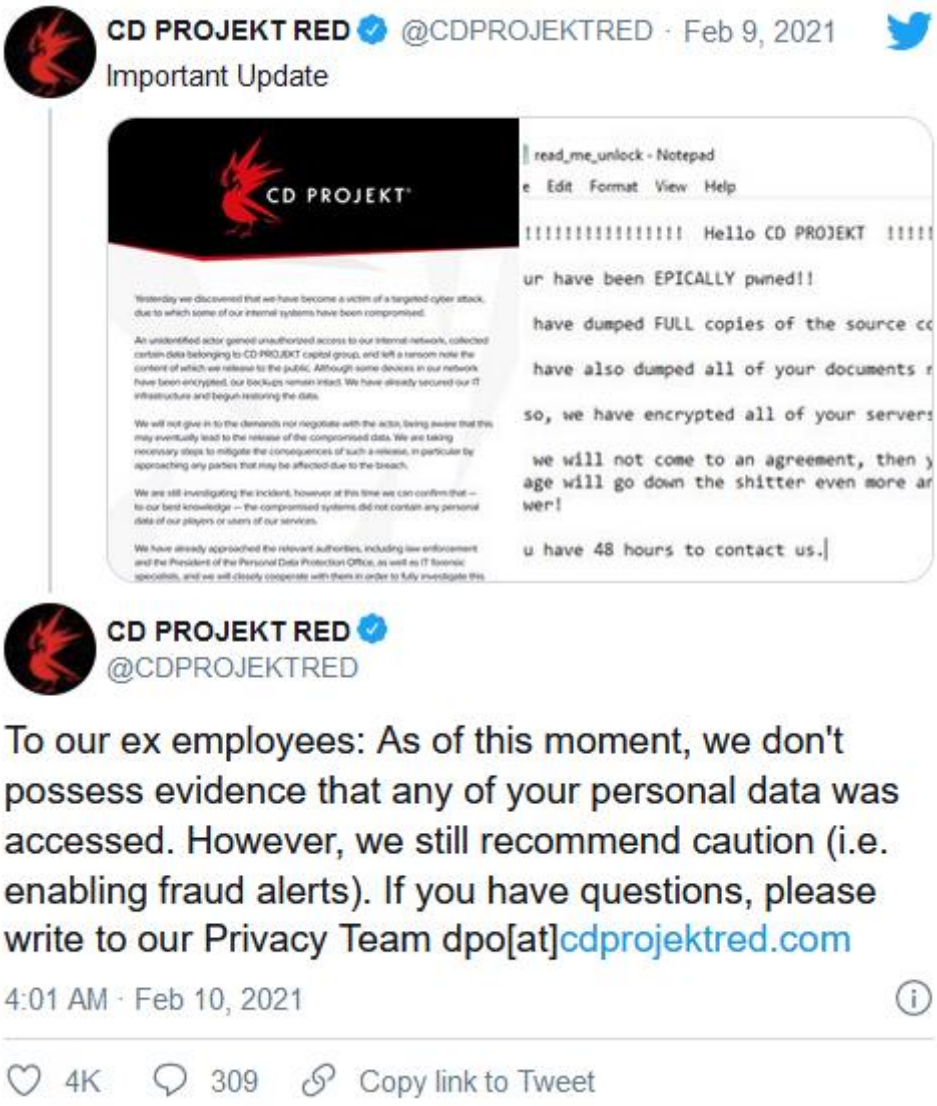
Yandex 官员还表示，他们对被泄露的账户进行了重新安全防护设定，并阻止了看似未经授权的登录，同时要求受影响的账户所有者更改密码。

Yandex 表示，它是在其内部安全团队的一次 "例行检查"中发现这一事件的，但没有详细说明更多细节。这家俄罗斯公司表示，目前正在对该事件进行 "彻底的内部调查"，并计划对其管理员人员访问用户数据的方式进行修改。暂时没有证据表明在最近的事件中访问了用户支付数据。同时，这家俄罗斯科技巨头表示已将该事件提交给当局。（来源：cnBeta）

➢ 《赛博朋克 2077》开发商 CD Projekt 称遭遇勒索软件攻击

2021 年 2 月 10 日，据报道科幻电子游戏《赛博朋克 2077》的开发商 CD Projekt 在周二

表示，该公司遭受了一次网络攻击。这家波兰游戏开发工作室表示，有黑客进入了其内部网络，对服务器进行了加密，并留下了一张赎金纸条，威胁如果不支付赎金，就将公布其游戏的源代码。



CD Projekt 公司在 Twitter 上表示：“虽然我们网络中的一些设备已经被加密，但是我们的备份依然完好无损。我们已经对 IT 基础设施进行了保护，并已经开始了数据恢复工作。我们不会屈服于黑客的要求，也不会与其进行谈判，因为我们知道，这最终可能导致数据被公开。我们正在采取必要的措施，减轻此事造成的后果，特别是通过与任何可能因此次入侵事件而受到影响的各方接触。”**在这条推文中，该公司还公布了黑客留下的赎金纸条，上面写着：**“如果我们不能达成协议，那么你们的源代码将被出售或在网上泄露，你们的文件将被发送给我们在游戏新闻界的联系人。”

网络安全公司 Check Point 的欧洲、中东、非洲和亚太地区事件响应负责人乔恩·尼克斯（Jon Niccolls）表示，所谓的“双重勒索”软件攻击目前正在变得越来越普遍。双重勒索

即黑客窃取数据，并威胁要泄露数据，除非满足他们的要求。尼克斯补充说，几乎一半的勒索软件事件中，黑客都威胁要公布被盗数据。他表扬了 CD Projekt 拒绝与黑客谈判的做法。尼克斯说道："我们呼吁所有组织使用防止攻击和阻止数据泄露的解决方案，来抵御日益增长的勒索软件威胁，并通过培训员工了解钓鱼邮件的风险，因为许多勒索软件漏洞都是这样发起的。我们所进行的研究表明，全球范围内，每 10 秒就有一个组织成为勒索软件的受害者，但是 CD Projekt 拒绝屈服于黑客的要求，这是正确的做法。"

CD Projekt 表示，他们不认为被入侵的系统内包含任何用户的个人数据。该公司表示，他们已经联系了执法部门和波兰个人数据保护办公室（UODO）主席简·诺瓦克（Jan Nowak），以及 IT 取证调查人员。UODO 的发言人周二证实，他们已经收到了 CD Projekt 的数据泄露通知。

最近几个月来，CD Projekt 的日子不太好过。该公司备受期待的《赛博朋克 2077》不久前登陆市场，但是由于存在大量 Bug，并且在老式游戏主机上表现不佳而遭到了大量用户的投诉，该公司不得不回收游戏进行修复，并推迟了发布时间。一直以来，该公司都在试图通过发布修补程序以提升优秀体验。但是，索尼还是因为质量问题从其 PlayStation 商店中撤下了这款游戏，目前尚不清楚该游戏将在何时回归 PlayStation 商店。当时有分析师表示，一款 AAA 游戏因为质量问题被主机厂商的商店下架，这是非常罕见的事情。周二，在遭到黑客攻击的新闻传出之后，CD Projekt 的股价下跌了 5.5%。12 月《赛博朋克 2077》发布以来，该股的跌幅超过 30%。CD Projekt 也是角色扮演游戏《巫师 3》的开发工作室。（来源：新浪科技）

➢ 以朋友名义向未注册用户发送信息，"脉脉"网站被判侵犯隐私权

2021 年 2 月 7 日报道，王某，有前同事标注你为'有两把刷子'并向你推荐了 119 个职业人脉，刘某、戴某、王某等 36 个好友也在脉脉等你，点击链接领取验证码，24 小时有效。"从未注册和使用职场社交平台脉脉，却收到脉脉短信指名道姓称"36 个好友在脉脉等你"，北京市海淀区人民法院近日发布案件快报，披露消费者王某起诉北京淘友天下科技发展有限公司（以下简称"淘友天下"）经营的脉脉网站未经许可，以朋友的名义向其发送短信，侵犯其隐私权的案件。经审理，海淀法院判决脉脉网站停止侵害消费者隐私权的行为，永久删除其个人信息，在《中国消费者报》刊登致歉声明。

我有"36 个好友在脉脉等我"？

据海淀区人民法院发布的案件快报，原告王某诉称，王某未注册和使用淘友天下运营的脉脉职场网站服务，却在 2018 年 3 月 10 日收到淘友天下发送的手机短信，直接称呼其名，并表示有前同事对其作出标注，有多名好友等待其加入。王某点击链接后网页自动跳转至脉脉网站的注册页面。

王某还提交了多份 2017-2018 年间与脉脉网站发送短信行为相关的网络文章及下方回复内容的打印件，均提到该网站的类似行为。王某认为，淘友天下非法获取、保有王某的手机联系方式、朋友信息、职业履历等个人信息，并未经同意向自己发送商业信息，侵犯了自己的隐私权。

脉脉：不违法、未侵权、没数据，但承认发送短信用户“不知情”

案件快报显示，淘友天下坚持称“未非法获取王某的个人信息，相关信息来源合法”，短信由注册用户触发，并表示“大多数应用程序都有获取手机号的行为，包括获取用户通讯录内容”，收集用户信息的行为并不违法，王某没有举证证实获取即造成损害后果。淘友天下坚持辩称，脉脉网站虽有诱导用户发送短信的行为，但并非非法获取。

而当法庭询问淘友天下在 2017 年至 2018 年期间，是否有后台数据记录等证据，证实系用户自己决定和操作向未注册的朋友发送短信时，淘友天下表示时间过去较久，没有留存资料。而王某表示，软件的开发过程均有文档，只是淘友天下不愿提供。

据淘友天下辩称，王某收到的短信应该是当时其朋友对王某点评后触发的。当法庭询问淘友天下，已经注册的用户是否知道其在点评朋友时会导致向被点评人发送短信的行为时，

淘友天下承认，用户“可能不知道点评会导致发送短信”，并“认可涉案短信的文案部分是网站设计的。”

据案件快报，淘友天下表示脉脉网站要求用户在注册时同步上传通讯录。而当法庭询问淘友天下是否将获取通讯录的目的向用户告知，其表示“后期的隐私权通知中有告知内容，之前没有”。值得注意的是，2018 年 5 月，脉脉所属的淘友天下公司因“广告主发布以虚假或者引人误解的内容欺骗、误导消费者的其他情形的虚假广告”被海淀区市场监督管理局行政处罚。

海淀法院：构成侵权，要求脉脉停止侵害行为，永久删除原告个人信息并登刊致歉

据案件快报，法院认为，淘友天下通过其经营的脉脉平台注册会员上传的信息获取了未在该平台注册的王某的电话号码，未经其同意向其发送含有王某本人及朋友姓名的推荐信息，侵扰其私人生活的安宁，构成对其隐私权的侵犯。

海淀法院表示，王某据此要求淘友天下停止侵害行为，永久删除保有的王某所有个人信息的诉讼请求，符合相关法律规定，应予支持。根据淘友天下公司的经营规模、影响力及侵权范围，应该公开致歉。

海淀法院称：本案的特殊性在于，淘友天下并未从原告本人处获得信息，而是通过从他人处收集的信息，编写信息发送，以吸引其注册。上传通讯录或选择给原告点评的关联人，并不知道其上传或点评会触发向原告发送短信的行为。网站的文案故意造成朋友直接邀请注册的假象，与发送无关联内容的普通短信的推荐信息相比，使原告受到较大的打扰和困扰，权益受到侵害，淘友天下应对此承担侵权责任。海淀法院表示，希望网络公司在大量收集和使用用户个人信息时，对范围和边界给予更多注意，避免侵犯公民合法权益。（来源：北京日报）

➢ 新加坡最大电信公司文档系统遭入侵，13 万名客户资料外泄

2021 年 2 月 18 日，当地时间 2 月 17 日晚，新加坡最大的电信公司新电信（Singtel）发布文告，完成 2021 年 1 月 20 日针对文档系统遭入侵的初步调查，披露有近 13 万名客户的个人资料外泄。该公司已开始通知所有受影响的个人与企业，协助他们管理可能的风险。

新电信表示：通过网安专家协助调查和分析，已确定第三方服务供应商 Accellion 的文

档传输应用（File Transfer Appliance，简称 FTA）系统遭非法侵入后被窃取的文档，以及受影响的利益攸关者。泄露的资料包括客户的名字、生日、手机号码和住址的资料组合，以及部分信用卡信息、企业资料。

此外，新电信 28 名前职员的银行户头资料、一家企业客户的 45 名职员的信用卡资料和 23 家供应商、合作伙伴和企业客户的部分资料也被窃取。

新电信指出，这 23 家企业包括供应商、合伙公司和企业客户，大部分被盗取的数据包括新电信内部的非敏感资料，例如数据记录、测试数据、报告和电邮。公司对此数据外泄事件感到抱歉，并表示已紧急通知所有受影响的客户，协助他们管理可能产生的安全风险，以采取适当行动。另外，公司也委任全球数据和信息服务供应商，为受影响客户免费提供监控服务。

新电信于本月 11 日宣布所使用的第三方文档共享系统于今年 1 月 20 日遭黑客袭击，结果客户资料外泄，但表明主要运作不受影响。这起网袭事故与近期影响多国机构组织的文档传输应用违例事件有关，它们包括新西兰储备银行、澳大利亚澳洲证券和投资委员会（ASIC）和美国华盛顿州审计署。（来源：央视新闻）

➢ 央视：开了会员配送费却猛涨 3 倍！“杀熟”又出新招？

2021 年 2 月 1 日，进入大数据时代，很多人都有这样的经历，并不是旅游旺季，机票价格却越搜越高。聊天时随口提到某款商品，一转身就在各大平台上看到相关商品的广告推送。在网络时代，我们能很快地找到自己想要的信息，但自己的信息数据却似乎也更容易被泄露，或在不知情的情况下被商家非法利用。

大数据“杀熟” 会员配送费高于非会员

不久前，一篇质疑某外卖平台运用算法进行“杀熟”的文章引发热议。该平台的一位会员用户指出，同样的订单，他的配送费定价时常比非会员用户的更高。肖先生：经常点同一家的外卖，忽然有一天我开了会员之后，发现配送费价格一下较之前涨出三倍。开了会员之后，反而比非会员价格还要高，那我开会员的意义在哪。文章引发热议后，相关外卖平台联系了肖先生，针对他提出的质疑，平台方给出的回复是：配送费上的价格差异是由于系统缓存而导致的误差。肖先生：我尝试了很多次，在一周之内都是这种情况。缓存的说法肯定说不过去。何来的位置缓存呢？在同一个地方，差异就是存在于会员和非会员之间。

据中消协介绍，消费者对“大数据杀熟”等问题投诉不断增多，问题的核心是互联网平台对算法技术的应用问题，集中体现在推荐算法、价格算法、评价算法、排名算法、概率算法和流量算法等方面。中国消费者协会投诉部主任陈剑：可能经营者对消费者进行精准的个人数据画像。这种画像相关的商品和服务只推荐给了他，所以他所获取的知情权存在很大的缺陷。

平台累积大量个人数据“算”制用户画像

基于大数据的用户画像，能让商家摸清你更爱吃辣还是吃酸，并通过算法把更符合你口

味的餐厅排序靠前。用户数据，往往是通过一个个手机 App 被互联网平台采集的。

在与 App 打交道的过程中，同样也有令大家担忧的问题不断出现，比如“App 偷听”现象，“App 偷听”是否存在呢？来看技术专家做的测试。

App 治理工作组技术专家何延哲：假如发一个语音，当手松开了以后，这个录音事实上还在继续。我们还可以把提示去掉，测试的过程是两分钟。两分钟后，记者看到，在测试程序中生成了一条时长为 120 秒的语音。技术人员将语音数据导出后，经过核对，证实了当测试程序置于前台运行时，“偷听”是可以实现的。此外，经过对比实验，技术人员告诉我们，在测试程序退至后台，或者在手机处于锁屏的情况下，录音依然可以持续进行一段时间，但都会自行终止。只是不同的手机操作系统，锁屏下持续录音的时长略有不同。

在技术上可以实现的“偷听”手段，是否在市面上的 App 中被滥用了呢？

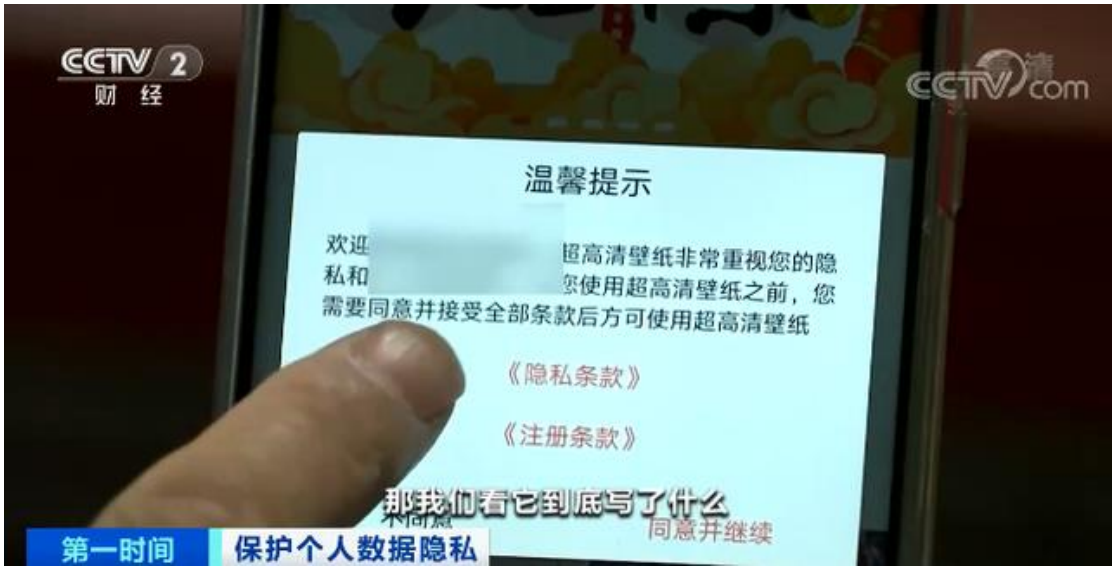
App 治理工作组技术专家 何延哲：目前还没有发现哪款 App 有把语音信息上传之后的偷听行为。那么，平台对用户做出的精准个性化推荐又是如何实现的呢？ 据专家介绍，主要是通过对我们的购买记录、浏览记录、搜索记录，甚至是下载过的应用程序清单等信息进行大数据分析，最终得以实现。

专家提示，用户可以在手机操作系统的权限设置里，找到麦克风权限，检查目前有哪些 App 被授权使用麦克风。根据自己的需要，用户是可以随时关闭对 App 使用麦克风的授权。

部分 App 隐私政策篇幅长账户无法注销

App 治理工作组的专家们在对市面上的 App 进行检测时，还发现很多 App 存在隐私政策篇幅长、用户难以读懂、账户无法注销等诸多问题。在测试的过程中，专家发现一款壁纸 App，隐私政策竟然有一万多字。

专家告诉记者，账号注销难，是目前用户投诉量很大的另一个问题。如今，技术带来的便利和个人信息的保护，正处在一个摇摆天平的两端。专家表示，在这个天平的“配平”过程中，需要监管机构、平台和用户三方在互动中来探寻。



清华大学人工智能国际治理研究院副院长梁正：有一些商业模式的迭代是很快的，这方面不能完全等到法律制定出来。针对每一个问题都有相应的技术解决方案来应对它，不是没解的。关键是要把规则制定清楚。

对 App“越界”行为要严打重罚

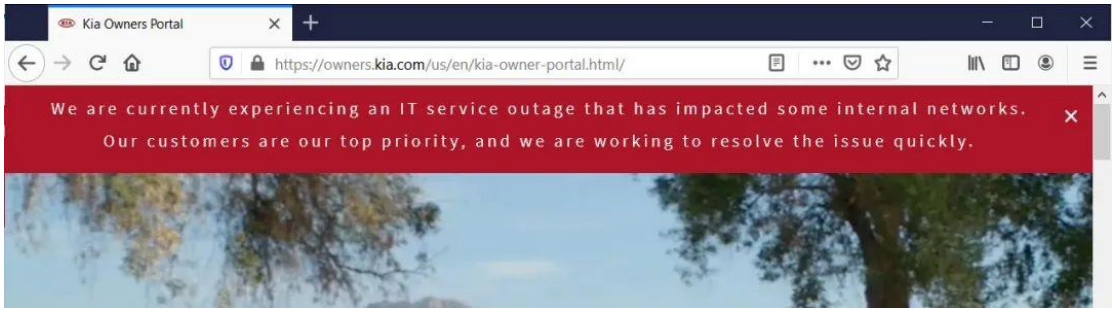
工信部多次在官方网站上通报侵害用户权益的 App，其中不少 App 被通报的原因是违规收集个人信息，强制、频繁、过度索取权限。技术是把“双刃剑”，互联网公司既能给用户推荐更适宜的商品和服务，也能利用技术侵犯用户隐私、损害用户利益。对此，相关监管部门要对 App 的个人信息收集进一步规范和细化，还要强化执法力度，让相关的法律、法规“长出牙齿”，完善惩戒机制，对不顾用户正当权益的 App 运营商予以严惩。（来源：央视财经）

➢ 起亚汽车遭遇勒索软件攻击，赎金高达 2000 万美元

2021 年 2 月 18 日报道，起亚汽车美国分公司遭受 DoopelPaymer 恶意团伙发动的勒索软件攻击，被开出 2000 万美元天价赎金。如果拒绝支付，不仅锁定数据无法还原，失窃的起亚内部信息也将被公之于众。

起亚汽车美国分公司（KMA）总部位于加利福尼亚州尔湾，隶属于韩国起亚汽车公

司。KMA 在全美拥有近 800 家经销商，所有轿车及 SUV 产品都在乔治亚州西点市郊区制造。日前，已经有报告指出起亚汽车美国分公司遭受全面 IT 服务中断影响，包括移动应用 UVO Link、电话服务、支付系统、车主门户网站以及经销商使用的内部站点均受到冲击。在浏览其官方网站时，页面会向用户弹出一条消息，称起亚的“内部网络出现了某些 IT 服务中断问题”。



一位起亚车主在推特上提到，当时他们正打算提车，但当地经销商表示由于勒索软件攻击的影响，官方服务器已经暂时关闭。为此，我们就上述故障与勒索攻击报告联系到起亚美国分公司，对方称正在努力解决问题。

“KMA 已经意识到目前涵盖内部、经销商以及面向客户的系统发生的 IT 中断。对于给客户带来的任何不便，我们深表歉意，也将致力于解决问题并尽快恢复正常运营。”

——起亚汽车美国分公司

我们此次获得了起亚汽车美国分公司在网络攻击期间收到的赎金提示，由此看来攻击是 DoopelPaymer 勒索软件团伙所为。在赎金提示中，攻击方称他们攻击的是起亚汽车母公司：现代汽车的美国分公司。但现代方面似乎没有受到太大影响。这份赎金提示中包含指向 DoppelPaymer Tor 支付站点上的私有受害者页面，其中同样将目标称为“现代汽车美国

分公司”。

受害者页面中提到，他们已经从起亚汽车美国分公司处窃取到“巨量”的数据。如果未能与攻击方达成谈判和解，则数据内容将在未来 2 到 3 周被全面公开。**DoppelPaymer 向来以先窃取未加密文件、再对设备进行全面加密而闻名。**

一旦受害者拒绝支付赎金，则相关信息将很快被公开披露在专门的数据发布站点之上。为了防止数据泄露并获取解密信息，DoppelPaymer 要求起亚方面支付约 404 枚比特币，总价值约 2000 万美元。如果未能在规定时间之内支付完成，则赎金将上涨至 600 枚比特币，约 3000 万美元。DoppelPaymer 方面还没有说明具体窃取了哪种数据类型。但从目前受到影响的起亚服务数量来看，对方很可能已经成功入侵大量服务器。

Emsisoft 方面指出，目前窃取未加密文件并借此逼迫受害者就范已经成为勒索软件中的一种常见策略。迄今为止，全球有超过 1300 家企业受到此类攻击的影响。安全公司 Emsisoft 在《2020 年勒索软件现状》报告中指出，“在全球范围内，已经有 1300 多家企业遭遇知识产权及其他敏感信息丢失，其中多数位于美国本土。请注意，这还仅仅是数据被发布在泄露站点上的公司数量，还没有计入为了防止数据外泄而被迫支付赎金的受害者。”过去曾遭遇 DoppelPaymer 毒手的知名受害机构还包括富士康、仁宝、PEMEX（墨西哥石油公司）、加利福尼亚州托伦斯市、纽卡斯尔大学、乔治亚州霍尔县、Banijay Group SAS 以及不列塔尼电信公司。（来源：安全内参）

信息安全意识产品服务

021-33663299