国盟信息安全通报

2020 年 11 月 08 日第 228 期

全国售后服务中心

国盟信息安全通报

（第 228 期）

国际信息安全学习联盟

2020 年 11 月 08 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 418 个，其中高危漏洞 137 个、中危漏洞 226 个、低危漏洞 55 个。漏洞平均分值为 5.79。本周收录的漏洞中，涉及 0day 漏洞 205 个（占 49%），其中互联网上出现“Nagios XI 'Contact Templates'跨站脚本漏洞、Small CRM 'email' SQL 注入漏洞”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 9867 个，与上周（12085 个）环比减少 18%。

主要内容

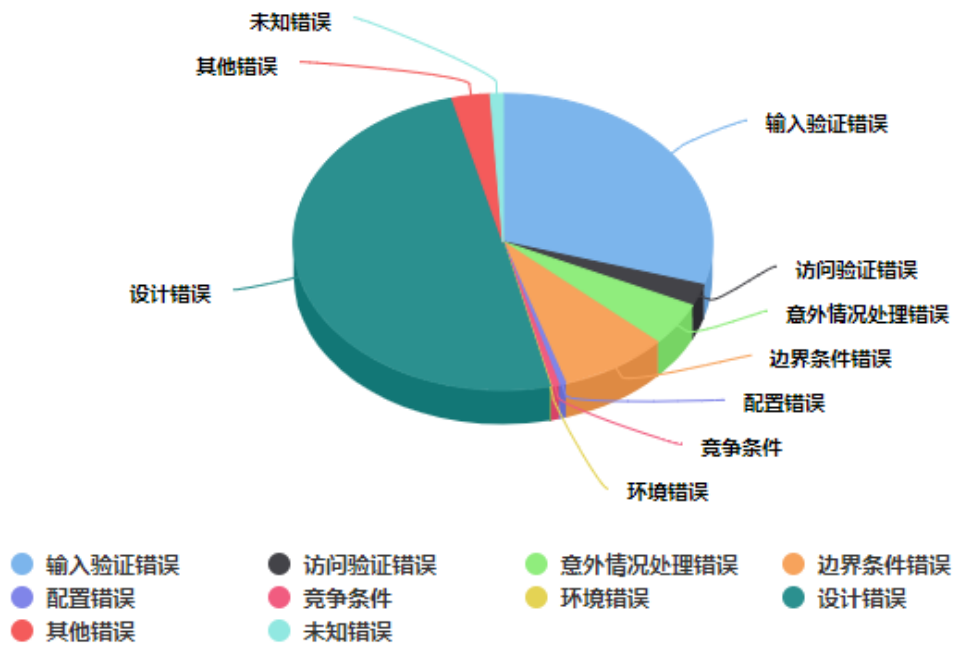
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

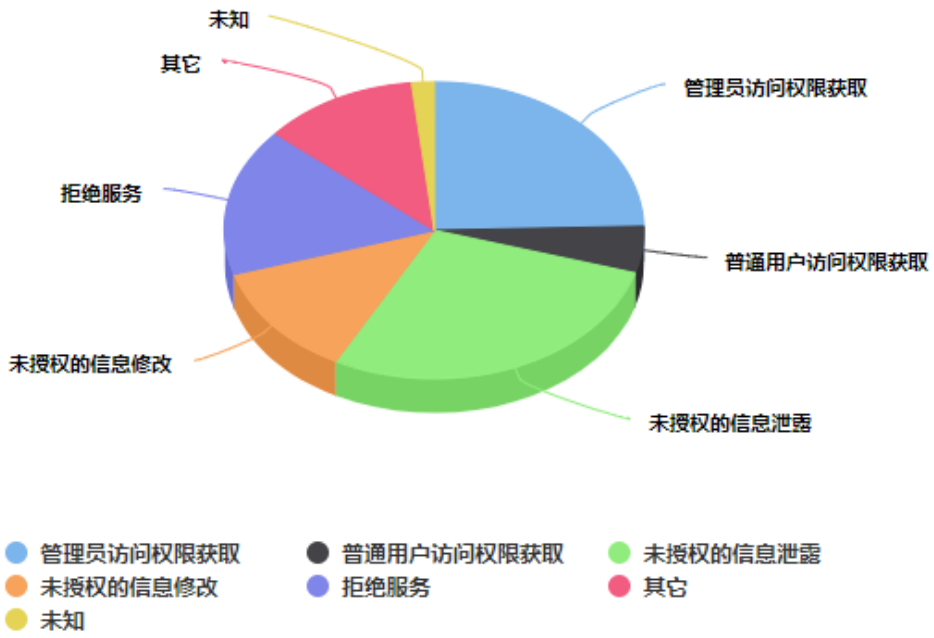
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 418 个，其中高危漏洞 137 个、中危漏洞 226 个、低危漏洞 55 个。漏洞平均分值为 5.79。本周收录的漏洞中，涉及 0day 漏洞 205 个（占 49%），其中互联网上出现“Nagios XI 'Contact Templates'跨站脚本漏洞、Small CRM 'email' SQL 注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 9867 个，与上周（12085 个）环比减少 18%。

二、安全漏洞增长数量及种类分布情况

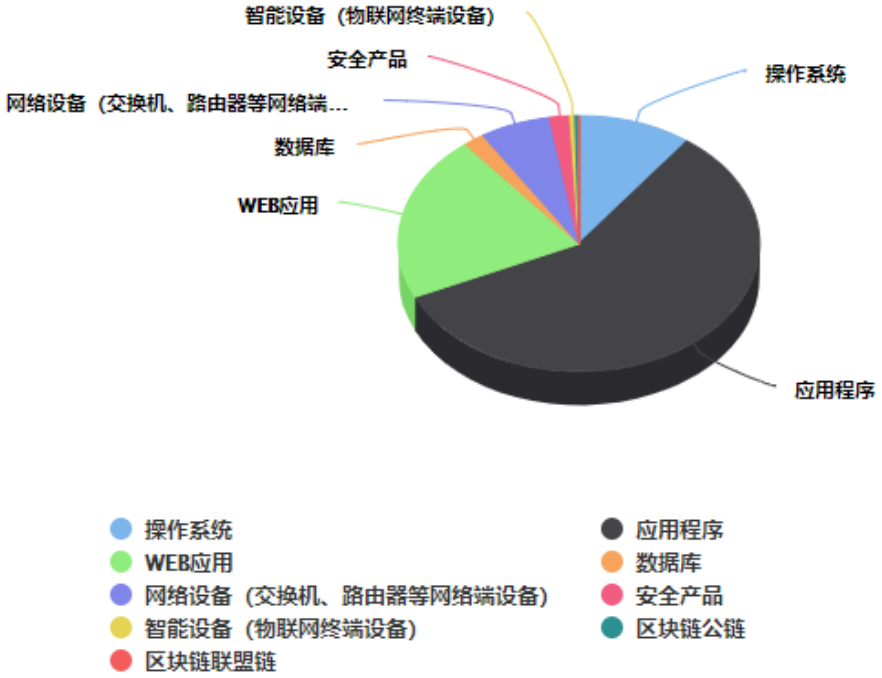
➢ 漏洞产生原因（2020 年 10 月 25 日—2020 年 11 月 08）



➢ 漏洞引发的威胁（2020 年 10 月 25 日—2020 年 11 月 08）



➢ 漏洞影响对象类型（2020 年 10 月 25 日—2020 年 11 月 08）



三、安全产业动态

➢ “十四五”规划建议提及哪些网信工作？

2020 年 11 月 3 日，新华社授权发布党的十九届五中全会审议通过的《中共中央关于制定国民经济和社会发展第十四个五年规划和二〇三五年远景目标的建议》。建议中多次提及**网信工作**，一起来看看。

决胜全面建成小康社会取得决定性成就

经济实力、科技实力、综合国力跃上新的大台阶，经济运行总体平稳，经济结构持续优化，预计二〇二〇年国内生产总值突破一百万亿元。

我国发展环境面临深刻复杂变化

当今世界正经历百年未有之大变局，新一轮科技革命和产业变革深入发展，国际力量对比深刻调整，和平与发展仍然是时代主题，人类命运共同体理念深入人心，同时国际环境日趋复杂，不稳定性不确定性明显增加，新冠肺炎疫情影响广泛深远，经济全球化遭遇逆流，世界进入动荡变革期，单边主义、保护主义、霸权主义对世界和平与发展构成威胁。

到二〇三五年基本实现社会主义现代化远景目标

展望二〇三五年，我国经济实力、科技实力、综合国力将大幅跃升，经济总量和城乡居民人均收入将再迈上新的大台阶，关键核心技术实现重大突破，进入创新型国家前列；基本

实现新型工业化、信息化、城镇化、农业现代化，建成现代化经济体系。

坚持创新驱动发展，全面塑造发展新优势

坚持创新在我国现代化建设全局中的核心地位，把科技自立自强作为国家发展的战略支撑，面向世界科技前沿、面向经济主战场、面向国家重大需求、面向人民生命健康，深入实施科教兴国战略、人才强国战略、创新驱动发展战略，完善国家创新体系，加快建设科技强国。

强化国家战略科技力量

制定科技强国行动纲要，健全社会主义市场经济条件下新型举国体制，打好关键核心技术攻坚战，提高创新链整体效能。加强基础研究、注重原始创新，优化学科布局和研发布局，推进学科交叉融合，完善共性基础技术供给体系。瞄准人工智能、量子信息、集成电路、生命健康、脑科学、生物育种、空天科技、深地深海等前沿领域，实施一批具有前瞻性、战略性的国家重大科技项目。制定实施战略性科学计划和科学工程，推进科研院所、高校、企业科研力量优化配置和资源共享。推进国家实验室建设，重组国家重点实验室体系。布局建设综合性国家科学中心和区域性创新高地，支持北京、上海、粤港澳大湾区形成国际科技创新中心。构建国家科研论文和科技信息高端交流平台。

提升企业技术创新能力

强化企业创新主体地位，促进各类创新要素向企业集聚。推进产学研深度融合，支持企业牵头组建创新联合体，承担国家重大科技项目。发挥企业家在技术创新中的重要作用，鼓励企业加大研发投入，对企业投入基础研究实行税收优惠。发挥大企业引领支撑作用，支持创新型中小微企业成长为创新重要发源地，加强共性技术平台建设，推动产业链上中下游、大中小企业融通创新。

激发人才创新活力

贯彻尊重劳动、尊重知识、尊重人才、尊重创造方针，深化人才发展体制机制改革，全方位培养、引进、用好人才，造就更多国际一流的科技领军人才和创新团队，培养具有国际竞争力的青年科技人才后备军。健全以创新能力、质量、实效、贡献为导向的科技人才评价体系。加强学风建设，坚守学术诚信。深化院士制度改革。健全创新激励和保障机制，构建充分体现知识、技术等创新要素价值的收益分配机制，完善科研人员职务发明成果权益分享机制。加强创新型、应用型、技能型人才培养，实施知识更新工程、技能提升行动，壮大高水平工程师和高技能人才队伍。支持发展高水平研究型大学，加强基础研究人才培养。实行更加开放的人才政策，构筑集聚国内外优秀人才的科研创新高地。

完善科技创新体制机制

深入推进科技体制改革，完善国家科技治理体系，优化国家科技规划体系和运行机制，推动重点领域项目、基地、人才、资金一体化配置。改进科技项目组织管理方式，实行“揭榜挂帅”等制度。完善科技评价机制，优化科技奖励项目。加快科研院所改革，扩大科研自主权。加强知识产权保护，大幅提高科技成果转移转化成效。加大研发投入，健全政府投入为主、社会多渠道投入机制，加大对基础前沿研究支持。完善金融支持创新体系，促进新技术产业化规模化应用。弘扬科学精神和工匠精神，加强科普工作，营造崇尚创新的社会氛围。健全科技伦理体系。促进科技开放合作，研究设立面向全球的科学研究基金。

加快发展现代产业体系，推动经济体系优化升级

坚持把发展经济着力点放在实体经济上，坚定不移建设制造强国、质量强国、网络强国、数字中国，推进产业基础高级化、产业链现代化，提高经济质量效益和核心竞争力。

提升产业链供应链现代化水平

锻造产业链供应链长板，立足我国产业规模优势、配套优势和部分领域先发优势，打造新兴产业链，推动传统产业高端化、智能化、绿色化，发展服务型制造。补齐产业链供应链短板，实施产业基础再造工程，加大重要产品和关键核心技术攻关力度，发展先进适用技术，推动产业链供应链多元化。

发展战略性新兴产业

加快壮大新一代信息技术、生物技术、新能源、新材料、高端装备、新能源汽车、绿色环保以及航空航天、海洋装备等产业。推动互联网、大数据、人工智能等同各产业深度融合，推动先进制造业集群发展，构建一批各具特色、优势互补、结构合理的战略性新兴产业增长引擎，培育新技术、新产品、新业态、新模式。促进平台经济、共享经济健康发展。鼓励企业兼并重组，防止低水平重复建设。

加快发展现代服务业

推动生产性服务业向专业化和价值链高端延伸，推动各类市场主体参与服务供给，加快发展研发设计、现代物流、法律服务等服务业，推动现代服务业同先进制造业、现代农业深度融合，加快推进服务业数字化。

统筹推进基础设施建设

构建系统完备、高效实用、智能绿色、安全可靠的现代化基础设施体系。系统布局新型基础设施，加快第五代移动通信、工业互联网、大数据中心等建设。加快建设交通强国，完善综合运输大通道、综合交通枢纽和物流网络，加快城市群和都市圈轨道交通网络化，提高

农村和边境地区交通通达深度。推进能源革命，完善能源产供储销体系，加强国内油气勘探开发，加快油气储备设施建设，加快全国干线油气管道建设，建设智慧能源系统，优化电力生产和输送通道布局，提升新能源消纳和存储能力，提升向边远地区输配电能力。

加快数字化发展

发展数字经济，推进数字产业化和产业数字化，推动数字经济和实体经济深度融合，打造具有国际竞争力的数字产业集群。加强数字社会、数字政府建设，提升公共服务、社会治理等数字化智能化水平。建立数据资源产权、交易流通、跨境传输和安全保护等基础制度和标准规范，推动数据资源开发利用。扩大基础公共信息数据有序开放，建设国家数据统一共享开放平台。保障国家数据安全，加强个人信息保护。提升全民数字技能，实现信息服务全覆盖。积极参与数字领域国际规则和标准制定。

拓展投资空间

推进新型基础设施、新型城镇化、交通水利等重大工程建设，支持有利于城乡区域协调发展的重大项目建设。实施川藏铁路、西部陆海新通道、国家水网、雅鲁藏布江下游水电开发、星际探测、北斗产业化等重大工程，推进重大科研设施、重大生态系统保护修复、公共卫生应急保障、重大引调水、防洪减灾、送电输气、沿边沿江沿海交通等一批强基础、增功能、利长远的重大项目建设。

完善宏观经济治理

加强宏观经济治理数据库等建设，提升大数据等现代技术手段辅助治理能力。

建立现代财税金融体制

构建金融有效支持实体经济的体制机制，提升金融科技水平，增强金融普惠性。

建设高标准市场体系

推进土地、劳动力、资本、技术、数据等要素市场化改革。

提高农业质量效益和竞争力

坚持最严格的耕地保护制度，深入实施藏粮于地、藏粮于技战略，加大农业水利设施建设力度，实施高标准农田建设工程，强化农业科技和装备支撑，提高农业良种化水平，健全动物防疫和农作物病虫害防治体系，建设智慧农业。

实施乡村建设行动

提高农民科技文化素质，推动乡村人才振兴。

提高社会文明程度

加强网络文明建设，发展积极健康的网络文化。

提升公共文化服务水平

推进媒体深度融合，实施全媒体传播工程，做强新型主流媒体，建强用好县级融媒体中心。推进城乡公共文化服务体系一体建设，创新实施文化惠民工程，广泛开展群众性文化活动，推动公共文化数字化建设。

健全现代文化产业体系

实施文化产业数字化战略，加快发展新型文化企业、文化业态、文化消费模式。

推动共建“一带一路”高质量发展

推进基础设施互联互通，拓展第三方市场合作。深化公共卫生、数字经济、绿色发展、科技教育合作，促进人文交流。

建设高质量教育体系

发挥在线教育优势，完善终身学习体系，建设学习型社会。

全面推进健康中国建设

完善突发公共卫生事件监测预警处置机制，健全医疗救治、科技支撑、物资保障体系，提高应对突发公共卫生事件能力。支持社会办医，推广远程医疗。

加强和创新社会治理

推动社会治理重心向基层下移，向基层放权赋能，加强城乡社区治理和服务体系建设，减轻基层特别是村级组织负担，加强基层社会治理队伍建设，构建网格化管理、精细化服务、信息化支撑、开放共享的基层管理服务平台。

加强国家安全体系和能力建设

坚定维护国家政权安全、制度安全、意识形态安全，全面加强网络安全保障体系和能力建设。

确保国家经济安全

加强经济安全风险预警、防控机制和能力建设，实现重要产业、基础设施、战略资源、重大科技等关键领域安全可控。维护水利、电力、供水、油气、交通、通信、网络、金融等重要基础设施安全，提高水资源集约安全利用水平。

维护社会稳定和安全

坚持专群结合、群防群治，加强社会治安防控体系建设，坚决防范和打击暴力恐怖、黑恶势力、新型网络犯罪和跨国犯罪，保持社会和谐稳定。

加快国防和军队现代化，实现富国和强军相统一

贯彻习近平强军思想，贯彻新时代军事战略方针，坚持党对人民军队的绝对领导，坚持

政治建军、改革强军、科技强军、人才强军、依法治军，加快机械化信息化智能化融合发展，全面加强练兵备战，提高捍卫国家主权、安全、发展利益的战略能力，确保二〇二七年实现建军百年奋斗目标。

提高国防和军队现代化质量效益

加快武器装备现代化，聚力国防科技自主创新、原始创新，加速战略性前沿性颠覆性技术发展，加速武器装备升级换代和智能化武器装备发展。

促进国防实力和经济实力同步提升

优化国防科技工业布局，加快标准化通用化进程。

保持香港、澳门长期繁荣稳定

支持特别行政区巩固提升竞争优势，建设国际创新科技中心，打造“一带一路”功能平台，实现经济多元可持续发展。

积极营造良好外部环境

高举和平、发展、合作、共赢旗帜，坚持独立自主的和平外交政策，推进各领域各层级对外交往，推动构建新型国际关系和人类命运共同体。（来源：网络传播杂志）

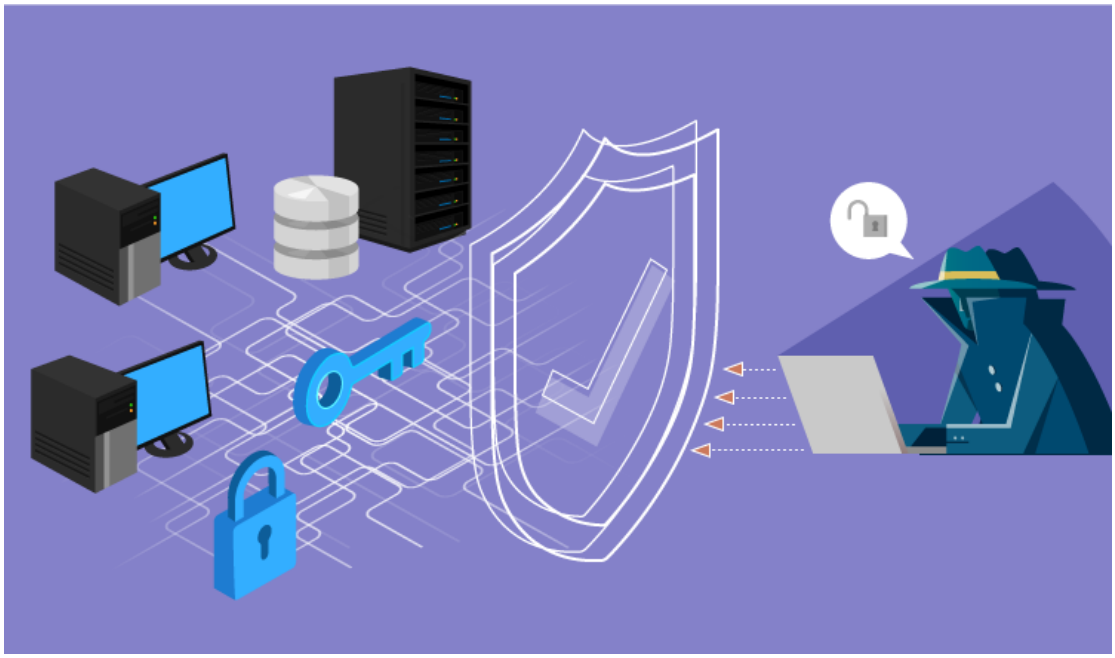
➢ 国家网信办：做好顶层规划 加强网络安全保障体系

2020 年 11 月 2 日，在举行的国务院新闻办公室新闻发布会上，国家互联网信息办公室副主任赵泽良表示，将贯彻落实十九届五中全会提出的网络强国建设任务，做好顶层规划，从顶层上设计我国网络安全工作、信息化工作、网络空间国际合作，进一步加强网络安全保障体系，同时推进互联网对信息技术的运用，将卫星互联网、量子计算、高端芯片、人工智能等技术更多地应用到社会生活、经济建设各个方面。

作为网络强国建设的重要内容，工业互联网也迎来更多支持举措。以浙江为例，浙江省委常委、宣传部部长朱国贤透露，预计到年底，浙江全省“1+N”工业互联网平台体系将连接工业设备 5000 万台，服务工业企业将超过 10 万家，开发集成工业 APP 超 3 万款，尤其是基于浙江中小企业众多、产业集群发达的特点，探索形成的“平台赋能服务商、服务商服务中小企业”的业务模式，成倍放大了工业互联网平台的服务能力，大规模推动中小企业数字化转型。

“下一步浙江将充分发挥杭州技术创新应用活跃、宁波制造业发达的优势，努力推动形

成杭甬双核机制、全省协同共进的工业互联网发展格局，拓展工业互联网融合应用的深度和广度，力争建设成为工业互联网的国家示范区。”朱国贤说。



当天会上还透露，以“数字赋能 共创未来——携手构建网络空间命运共同体”为主题的“世界互联网大会·互联网发展论坛”将于 11 月 23 日至 24 日在浙江乌镇举行。同期，还将举办世界互联网领先科技成果发布活动、“互联网之光”博览会、“直通乌镇”全球互联网大赛等活动。

“今年以来，疫情在全球蔓延，国际形势深刻变革，在这样的背景下，秉持网络空间命运共同体理念，努力推动全球网络空间向更加包容、平衡、共赢方向发展，显得尤为重要。”赵泽良表示，论坛将持续搭建中国与世界互联互通的国际平台和国际互联网共享共治的中国平台，秉持开放、平等、互信、共赢理念，促进全球数字赋能与经济复苏，携手各方让网络空间命运共同体更具生机活力。（来源：人民日报）

➢ 《个人信息保护法（草案）》亮点浅析与建议

2020 年 10 月 21 日，《个人信息保护法（草案）》（下称“《草案》”）由十三届全国人大常委会第二十二次会议审议后公布并公开征求社会公众意见，征求意见截止日期为 2020 年 11 月 19 日。针对这次亮相的草案。笔者在研究了《个人信息保护法（草案）》的历史沿革和发展之后，结合本次《草案》的亮点简要评述，并结合实践，对《草案》提出建议。

一、《个人信息保护法（草案）》出台背景

2020 年 10 月 21 日《个人信息保护法（草案）》出台引起各界广泛关注。早在 2000 年初，我国就提出将个人信息保护成文法化。当时许多学者纷纷提出自己的方案，但由于当时互联网刚刚兴起，法典化的条件不成熟。2017 年 12 月 29 日，全国信息安全标准化技术委员会发布的《信息安全技术：个人信息安全规范》（GB/T 35273-2017），以技术文件的形式明确了个人信息保护领域的法律术语，确立了个人信息处理活动中应遵循的原则性的安全要求。2018 年 9 月 10 日，《个人信息保护法》被列入十三届全国人大常委会立法规划。2018 年 11 月 30 日，公安部发布《互联网个人信息安全保护指引（征求意见稿）》，指导互联网企业建立健全公民个人信息安全保护管理制度和技术措施，有效防范侵犯公民个人信息违法行为，保障网络数据安全和公民合法权益。2020 年 5 月 28 日发布的《民法典》也设定了专章，对隐私权和个人信息进行保护，本次草案的出台留下上位法的法律依据。

随着互联网、通讯技术以及产业数字化，近年来，各国纷纷出台对信息数据安全的成文法律。2018 年 5 月 25 日，欧盟的《通用数据保护条例》（GDPR）正式实施。2018 年 6 月 28 日美国加州通过了《加州消费者隐私法案》（CCPA），2020 年 1 月 1 日正式实施。2018 年 8 月 14 日，巴西《通用数据保护法》（LGPD）也正式通过，2020 年 2 月 15 日正式实施。

亚洲各国也在如火如荼地推进个人信息保护立法。2011 年 3 月，韩国实施《个人信息保护法》。同年 9 月 30 日，《个人信息保护法施行令》和《个人信息保护法施行规则》作为

《个人信息保护法》的配套措施一并开始施行。2017 年 5 月 30 日，日本新修订的《个人信息保护法》（PIPA）也开始实施。印度也于 2019 年 12 月 11 日发布了《2019 个人数据保护法案（草案）》。

《草案》的出台，一方面响应数字化变革导致全球数据立法浪潮，另一方面也凸显我国无论是立法部门、学界、实务界一直对个人信息权利护的重视。《草案》的出台必将进一步完善补充关于个人信息权的相关法律法规，在充分保护个人信息权益方面也将踏出一大步。

二、亮点综述

《中华人民共和国个人信息保护法（草案）》的体系明确，从总则中立法目的（第一条）、保护原则（第二条）（第五条）（第六条）（第七条）、管辖范围（第三条）、个人信息定义（第四条）、国际衔接（第十二条）等到分则部分设立专章，对不同主体如何处理和管理个人信息作出明确的规定和安排。本文总结《草案》有以下七部分的亮点。

亮点 1: 确定以“属地主义”为主，“信息活动路径”为辅的管辖方式。（第三条）

亮点 2：与《民法典》相比，个人信息的定义更为概括，以“原则+例外”的方式对该条进行规定，同时增加了个人信息处理的范围。（第四条）

亮点 3: 多元化个人信息处理方获得授权路径。（第十三条）

按照个人信息处理的方式，《草案》根据优先性分别列出了个人同意、合同约定、法定义务或职责、公共利益、新闻和舆论监督。就公共利益和新闻报道等，虽然此条可能将牺牲个人的部分利益，即不需要个人同意获得授权。但是，法律对此的规定是严格和明确规定的，即存在生命健康和财产安全的必须时才能纳入；只有新闻报道和舆论监督才能成为例外。同时《草案》的第十九条与此条形成良好的呼应。

亮点 4: 对两个以上的信息处理者的义务划分明确化，将连带责任纳入共同处理个人信息的侵权行为，建立明确的法律责任承担方式。（第二十一条）

亮点 5: 对第三方受托人的地位和权利义务进行明确的界定，强调了第三方受托人的合法授权必须单独去的个人信息处理者的同意。同时严厉禁止了第三方利用技术手段破解个人身份。（第二十二条到二十四条）

亮点 6: 具体罗列个人敏感信息，确定敏感信息的外延。尤其是对个人生物特征、医疗健康、金融账户、个人行踪的确定。

亮点 7：明确法律责任，即确定量化了罚款数额，从相关企业、机构到企业、机构负责人，确定到“责任人”。

综上，可看到,从立法的的技术以及自身的特点，我国的《草案》由原则到细节，考量到

各方的利益，建立了具有我国特色的《个人信息保护法》。

三、建议部分

目前《草案》正在征求意见阶段，结合实践中可能会遇到需要进一步明确的问题和方向，拟提出以下建议。

（1）建议进一步明确是否适用于政府部门以及政府部门处理的个人信息

《草案》第三条规定“组织、个人在中华人民共和国境内处理自然人个人信息的活动，适用本法”。并未规定《个人信息保护法》适用于政府部门以及政府部门境内处理个人信息的行为。《草案》第十一条规定，“国家建立健全个人信息保护制度，预防和惩治侵害个人信息权益的行为，加强个人信息保护宣传教育，推动行成政府、企业、相关行业组织、社会公众共同参与个人信息保护的良好环境”。《草案》第三十三条规定，“国家机关处理个人信息的活动适用本法；本节有特别规定的，适用本节规定”。

在《草案》第三条的法律适用范围中,并未明确将政府部门、具有公共职能的企业单位以及受委托代理部分公共职能的企事业单位及其数据处理行为作为本法约束和管辖的主体,建议进一步明确。

（2）建议个人信息的分类与范围进一步明确

按照《草案》第四条的规定，“个人信息是以电子或者其他方式记录的已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。”《草案》中对于个人信息定义的内涵虽明确，但对于“已识别”或者“可识别”的外延规定则相对模糊。

个人信息作为一个相对抽象的概念，立法者有必要列举个人信息的种类、类型以及表现形式，进而进一步界定和确定个人信息的具体范围。笔者认为,仅仅从信息可能存在的路径，即收集、储存、使用、加工、传输、提供、公开等活动，来确定个人信息的范围过于宽泛,希望在正式发布的条文对此有更详细的规定。

（3）建议对目前被消费者广泛投诉非法利用个人信息进行直接营销、电话营销的行为做专章规定并进行处罚

电话营销、垃圾营销短信及垃圾营销短信是历年来被消费者广泛投诉的个人信息被滥用的老问题。相比较其他亚洲国家和地区对直接营销（电话、短信、电子邮件）做出严格规定，本次《草案》并未涉及到利用个人信息进行直接营销的问题。以香港地区为例，如收集个人信息用于直接营销，需要在收集之前以简单明确的书面语言通知被收集个人信息的主体并应获得被收集者的明确同意。并且，个人信息的处理者应提供方式方法，便利于个人随时撤回同意。违法利用个人信息直接营销规则的公司、企业、政府部门需要承担相应处罚甚至刑事

处罚。

（4）建议明确《草案》的执行细则即个人信息权被侵权滥用的具体救济机制和步骤

《草案》第六章规定“履行个人信息保护职责的部门”为国家网信部门、国务院有关部门在各自职责范围内负责个人信息保护和监督管理工作；县级以上地方人民政府有关部门的个人信息保护和监督管理职责，按照国家有关规定确定。

《草案》第七章规定违法行为、处罚形式，处罚金额以及具体法律责任的定性。

在《草案》的第六章、第七章之间欠缺个人发现个人信息被滥用、被侵权之后的具体投诉、救济、复议机制和步骤,建议进一步明确,从而能够使一旦个人发现个人信息被侵权、滥用、盗用,则可以遵循具体的救济步骤获得救济包括获得专家意见、法律意见的权利。

（5）建议增加国家网信办及县级以上的网信部门为推动个人信息保护工作的社会公益职责

由于个人信息保护在国内尚处于萌芽阶段，建议网信办增加相关社会公益职责。具体包括教育公众、企事业单位、其他组织在多种场景下如何做个人信息保护。例如公共场所的监控细则、工作场所的员工隐私保护、电话营销利用个人信息的相关指引等。此外，在个人信息保护的初期，网信办或县级以上网信部门编纂指引性文件,将对提高公众个人信息保护的法律意识有很大助益。

四、结语

数字化变革对各大行业都产生深刻影响。全球范围对个人信息保护立法已形成风潮。一方面，从便利贸易的角度，我国需要提高个人信息保护水平，便于与海外趋严的个人信息安全立法监管要求对接；另一方面，《个人信息保护法》的立法也回应国内消费者对个人信息保护的呼声。以法律形式避免个人信息被滥用、盗用，切实保护个人信息权。我们认为，《个人信息保护法》从《草案》到正式立法，必将会对中国社会、企事业单位以及政府部门产生深远的影响。（来源：中国信息安全）

➢ 5G 时代的网络安全挑战与服务

随着移动通信进入 5G 时代，与前几代移动通信系统相比，5G 依靠大规模天线和超密集组网等显著提升了移动接入技术，带动核心网技术的换代，赋能增强移动宽带、超可靠低时延和广覆盖大连接特性，成为紧密联结物联网、大数据、云计算、人工智能（AI）、区块链和

工业互联网的纽带。同时，5G 还将促进 IT 与 OT（生产技术）的融合，贯通数据从采集、汇聚、处理、分析和决策全过程，发挥数据的生产要素作用。

5G 给网络安全带来的新挑战

5G 推动了新一代信息技术的发展，5G 时代不仅是移动通信的新时代，也是 IT 技术发展的新时代。由于网络安全与信息技术产品总是相伴而生、博弈同行，5G 时代在解决原有一些网络安全风险的同时，又将面对新的安全挑战，对网络系统和网络服务提出了新的要求，这也是网络安全服务发展的新时代。

1. 虚拟化的挑战

互联网初期网络不够稳定，所有业务都以 IP 包方式独立选路。对视频类的长 IP 流也切成小包选路，效率太低。5G 引入 NFV（网络功能虚拟化），通过硬件通用化（白盒化）和软件定义网元功能，可以根据业务流的需要灵活采用 1.5 层、2 层或 3 层转发，增加了网元功能动态变化的能力，提高了转发效率并显著降低时延。NFV 实现同一网元在同一时间对不同的应用业务提供不同的转发功能，例如以路由器模式转发传感器的 IP 包，以交换机模式交换话音 MAC 帧，以交叉连接模式来中继以太网码块，不过各种应用间仅是逻辑隔离而非硬件隔离，存在不安全因素，而且软硬件解耦增加了对外接口，虽然提供了对设备软硬件供应商的可选择性，但多供应商的互操作解决方案增加了互联互通的测试认证以及故障时责任认定的难度。另外开放接口易受外部攻击,需强化硬件锚定（认证）可信机理，维护应用与底层硬件间信任链。

由于数据中心虚拟化的网络、计算与存储资源及 5G 网络虚拟化模糊了网络的物理边界，基于逻辑拓扑定义的虚拟安全域将随虚拟机的迁移状况动态变化，传统依赖网络安全硬件外挂方式的安全机制难以奏效。另外，我国有很强的电信设备定制化产品优势，但 NFV 的白盒化仍依赖国外的通用芯片，存在不可控风险。

2. 切片化的挑战

5G 需要支持从 Kbps 的传感器数据到高达 Gbps 的虚拟现实（VR），需要支持从静止状态下的话音到行进中高铁的通信，需要支持远程医疗和车联网等高可靠业务，但大量的应用对可靠性要求不高。

为了在同一物理设施上支持业务需求各异的应用，按照业务流的带宽、时延、可靠性等需求，在集中的网络运维支撑系统（OSS）管理下组织网络资源，以信令方式自动生成网元的编排与服务的编排，实现端到端切片的产生、终止、指配拓扑和协议等生命周期管理，为各业务流提供与其属性对应的逻辑上的 VPN 通道。现在 5G 的网络切片面临 VPN 海量规模、实时性、端到端通道组织等难题。虽然 VPN 的服务在电信网中早就有，但过去都是预约建立而非实时的，而且仅对极少数业务流开通 VPN 服务。跨运营商网络建立 VPN 连接更是难以想象的任务，前提是运营商间必须相互开放网络资源与业务数据，这基本没有可操作性，而且也会引入网络安全管理上的复杂性。通常集中控制系统易成网络攻击的对象，而底层网络资源共享将挑战切片间安全隔离。5G 在功能上还考虑支持将切片开放给客户来组织、生成和管理，并提供按需实时动态调整权限，虽然增加了对垂直客户的吸引力，但网络资源有被恶意的第三方控制的可能。另外，网络切片是按用户需求提供资源分配优先权，如果用户不可信或需求不准确则滥用网络资源。

3. 开放化的挑战

相对 4G 专用协议，5G 采用通用互联网协议，可直接承载现有网上各种业务，但也为互联网上的病毒打开了方便之门。

5G 采用基于服务的网络体系（SBA），SBA 构建一个业务开放平台，承接各种业务智能单元以 App 方式按需添加，通过模块化的智能单元组合产生相应的智能，便于灵活调用网络服务和组织网络切片。用户身份管理、认证鉴权、密钥管理、安全上下文管理等功能也可以服务化方式调用和开放，提升业务生成能力，适应新业态的不可预见性。SBA 以开放接口承接外部生成的 App 时，存在恶意 App 进入的风险。另外，5G 还具有业务外包能力，开放移动性、会话、QoS 和计费等功能的接口，垂直行业企业可租用这些服务自定义与调配业务，但也面临被误用和滥用的可能，而且恶意第三方容易通过获得的网络操控能力对网络发起攻

击。为此 5G 在网络安全与信息安全的防护方面要比 4G 下更大的功夫。

4. 开源化的挑战

5G 使用的深度学习等软件很多都来自开源软件，开源软件优点是可移植性，可以在操作系统上也可以在专有硬件上运行软件，硬件和软件生态系统的脱钩有利于创新，还增加了对其进行恶意攻击的难度。但开源软件的开发通常落后于商业软件开发，漏洞多、版本升级频繁，执行未知来源程序面临安全威胁，软件测试与漏洞分析检查工作量太大。此外值得注意的是，5G、云计算、大数据和人工智能大量使用的开源软件及其开源社区多为国外主导，而且开源软件并非自由软件，存在受到开源社区管理者限制的可能。

5. 大连接的挑战

5G 将物联网从窄带物联网（NB-IoT）扩展到可支持 100Mbps 业务的宽带物联网和可支持每平方公里百万传感器接入的大规模机器类通信的物联网（mMTC）。5G 物联网还具有接入移动物联网的终端能力，根据需要可提供与物联网终端的人机对话功能，还可以利用一体化接入回传（IAB）技术支持物联网终端间数据接力。物联网所感知的数据可通过 5G 低时延直接上云，相当于云端能力虚拟到终端，可以说 5G 将 AI 与 IoT 无缝融合成为智联网（AI+IoT=AIoT）。更进一步可将 AI 芯片及其操作系统直接嵌入 IoT 模块组成 AIoT 终端，相当于边缘计算能力下沉。还可进一步嵌入区块链能力到 AIoT 终端，保障物联网设备接入认证、数据加密及设备控制授权安全。

但是 IoT 类型很多，需有多种身份管理机制，而不仅是常规移动终端使用的对称密钥，海量 IoT 连接需使用分层管理与群组认证或多节点分布认证，以免信令风暴。IoT 还需要具有多对多的端到端联合加密功能，既要简化密钥但又要有足够强度。IoT 终端由于功耗的限制而难有较强的安全防御能力，而且大连接和永远在线，易被木马入侵成为拒绝服务攻击（DDoS）的跳板。车联网点到多点和广播式及绕过网络的车辆间直接通信（V2V）也带来新的安全问题。

6. 智能化的挑战

5G 会借助 AI 技术来优化网络的运营管理，但 AI 目前水平还是“大数据大算力小任务”，不确定性的概率计算模型需要巨量的空间和时间来训练，而且 AI 结果还不可解释。神经网络目前实质是分类器，依赖大量正确标注的数据，但很多场景仅有小数据。当一些事件和图像处于 AI 模型的辨识分界线时，或者受到样本攻击时会使 AI 误判。攻击者也会利用 AI 技术来发现网络基础设施的漏洞，高级持续性威胁（APT）攻击将会更多出现。

7. 数据私密性的挑战

传统的基于外挂的防火墙、防病毒和入侵检测的安全措施，因网络和算力设施的虚拟化而作用有限。但它无需对被保护系统详细了解，不涉及被保护系统内部的数据。

依赖免疫能力的内生防御方式需要对被保护系统有较深入了解，会跟踪系统的数据，且仍需与外部网络交互安全威胁情报，数据存在外泄风险。数字孪生数据可能会通过外网传输，仅靠加密仍难避免数据被劫持，会映射误导或遭遇外界勒索。数据跨境流动因云化而难定位最终落地点，增加对网络安全事件追溯的困难。在跨企业数据融合时如何保证数据能共享且敏感数据不外泄，也是很大的挑战。清华大学姚期智院士提出 MPC（多方计算）概念来应对这一难题，MPC 协议是一种分布式协议，使用秘密分享、同态加密、混淆电路、不经意传送四大技术，按照明文数据及计算工作没有离开本地的原则，允许各参与方只提交密文分片，通过既定逻辑共同计算出结果，但 MPC 计算量很大，性能还有待改进。

8. 数据资产化的挑战

数据是生产要素，通过将数据分布存储和加密可以防备数据被盗窃或被篡改。但通常对加密的数据难以进行安全扫描检测，而且即便是加密的数据流，也会被劫持成为 DDoS 攻击的炮弹。需要注意的是，一些外部攻击并不以窃取数据为目的而是以勒索为目的，强行将数据再加密使原有数据的拥有方也无法读取数据。因此需要实时对数据进行审计与版本核对，防止因数据（不论是否已加密数据）被恶意再加密，防范的关键是堵塞网络被入侵的漏洞。

9. 应用行业化的挑战

能源、交通等融合基础设施的信息系统与生产系统紧耦合，对网络信息安全的管理比对通信网络系统更为困难，即便是内网也会因管理不慎，例如通过 U 盘而内外勾连，一旦发生网络安全事件将危害国家重要基础设施。

工业互联网底层 PLC、MCU、SCADA 等数据采集与监控系统很多为国外产品，原来因在企业内网对其安全隐患知之甚少。企业的工控软件也有类似情况，一旦与外网关联则有被利用的安全风险。企业会大量应用边缘计算，而边缘计算的安全能力不及中心云，也有被劫持的可能。IPv6 海量的地址有利于实名制，但攻击者可以大量利用 IPv6 地址而掩盖真实攻击源身份，而且基于 IPv6 的分段路由（SR）丰富了路由的选择，为攻击者同时使用多路由或随机使用路由带来方便，同时增加了溯源攻击者路由的困难。

10. 网络安全生态化的挑战

网络安全是涉及业务、管理、流程、团队等各方面的系统工程，不仅是技术更是管理，在企业内要覆盖业务全环节，实现 IT 与 OT 团队融合，还要与外部（生产装备供应商、供应链、网络安全服务商、电信运营商、政府、客户等）实现网络安全威胁情报共享和协同联动。

网络安全需要有法律法规保障，需要国际合作，但基础是建立我国自主可控的网络安全技术、产品和服务的完整体系。

网络安全服务的思考

当今社会，每一个企事业单位、政府、学校、医院等都可能是网络安全攻击的对象，每一个单位都应成为网络安全责任的主体，需要从网络安全的制度建立、组织管理、队伍建设、资金投入等方面全面部署。据 IDC 公司报告，我国在信息安全投入占 IT 投入之比在 2017 年为 1.84%，而全球平均为 3.74%，在信息安全投入的结构中，全球平均硬件、软件和服务分别为 19.3%、36.3%和 44.4%，我国为 55.3%、18.6%和 26.1%，我国在网络安全投入方面不足并且重硬轻软和弱服务，在 5G 时代如果继续这种状况则后果更加严重。5G 时代由于网络安全事件越来越复杂，仅靠本单位的努力往往不够，需要借助第三方网络安全服务机构的支持。

1. 网络安全是产业更是服务

产业讲究通用性，而网络安全服务通常具有个性化及永恒性。为降低网络服务的成本，需要将网络安全能力做成模块化可扩展，前提是需要有很好的总体架构设计和接口的标准化。由于安全配置和管理复杂化，需要自动化管理安全功能部署、编排、配置、调用等以提高效率。

网络安全服务机构不仅要把客户当成服务对象，更要把客户当成合作对象，让安全和业务深度融合，实现从销售硬件为主向安全服务为主的转变，服务中还应包括网络安全人才的培训。

2. 网络安全服务需要在企业制定网络建设方案的阶段介入

企业网络建设方案的制定需要从网络安全角度来审议，网络基础结构应具有灵活改变的能力，以钝化恶意攻击。要假定网元不可信情况下设计网络架构，即零信任机制，但前提是涉及网元的每一操作都需要有信任认证，需要为网络设备生成并签名可信赖代码，例如为 SDN 交换机生成并签名可信代码、完整或部分验证 NFV 中虚拟网络功能（VNF）的代码，在验证和执行之间保持代码的完整性。很多安全挑战是内生的，需要增强内生免疫能力，但一些内生安全防御方案仍难以对抗 DDoS 攻击。企业制定的网络部署方案需要进行网络安全评估，最好邀请专业的网络安全机构来协助进行，或事前听取网络安全服务机构的咨询建议。

3. 网络安全部署需与基础设施同步建设

网络建设全过程需要有可依据的安全标准体系、制度规范和法律法规，网络安全软硬件应与基础设施一同部署，不应作为补丁事后再加入。对于已有的基础设施，也需要定期进行网络安全检测。政府应该支持第三方的应用服务安全检测环境和生命周期的安全风险评估平台的建立和开展服务，包括定期发布网络安全态势，在政府指导下委托企业开展网络安全风险评估，提出网络安全改进的建议。

4. 网络安全需要有大数据支撑

SDN、NFV、网络切片、智能化运维和网络安全保障都需要精准获得全网业务流与网络资源的实时大数据，工业互联网的安全运行也需要获得企业生产系统与网络安全有关的完整数据，在制度上需要保证网络安全实施主体能集中管理网络安全有关数据，而且数据标注与清洗能按标准进行。由于企业担心商业秘密的安全而不可能向其委托的网络安全服务机构提供较全面的数据，网络安全服务机构需要使用数据增强技术从有限的数据样本中进行模型训练，以便优化模型，发现安全隐患。

5. 开发并应用软件代码可信赖检测技术

鉴于从开源软件中发现安全漏洞的工作量很大，网络安全服务机构需要开发通过使用自然语言标准文档的机器翻译来快速提取开源软件信息的方法，所提取的信息用作自动化遵从性测试、正确性证明、协议执行完整性检查等，确保网络内代码值得信赖。

网络安全是个大系统工程，网络安全总是魔高一尺道高一丈。在数字经济时代，网络安全的影响愈加严峻，网络安全的重要性前所未有。随着 5G 等新一代信息技术应用的进一步深入与普及，网络安全新挑战层出不穷，网络安全技术与产业及服务也将得到更大的发展，网络安全的技术与管理创新永远在路上。（作者：邬贺铨）

四、政府之声

➢ 教育部：网络安全等 16 个领域纳入国家安全教育大中小学全覆盖

2020 年 10 月 20 日，教育部关于印发《大中小学国家安全教育指导纲要》的通知[教材〔2020〕5 号]。通知要求，为深入学习贯彻习近平总书记总体国家安全观，结合教育系统实际，教育部 2020 年 9 月印发了《大中小学国家安全教育指导纲要》（以下简称指导纲要）。指导纲要指出，国家安全教育要实现全领域、全学段覆盖，相关内容纳入不同阶段学生学业评价范畴，且纳入大中小学生综合素质档案。

指导纲要明确了国家安全教育主要内容：包括政治、国土、军事、经济、文化、社会、科技、网络、生态、资源、核、海外利益等 12 个领域安全，以及太空、深海、极地、生物等 4 个不断拓展的新型领域安全，围绕各领域安全的重要性、基本内涵、面临的威胁与挑战、维护的途径与方法等方面提出学习要求。（来源：教育部）

- **教育部关于印发《大中小学国家安全教育指导纲要》的通知 教材〔2020〕5 号**
- **全文：**http://www.moe.gov.cn/srcsite/A26/s8001/202010/t20201027_496805.html

➢ 工信部、卫健委部署进一步加强远程医疗网络能力建设

2020 年 11 月 2 日，为深入贯彻落实《国务院办公厅关于促进“互联网+医疗健康”发展的意见》，推进“互联网+”在医疗健康领域的应用发展，增强基层卫生防疫能力，工业和信息化部、国家卫生健康委发布工业和信息化部办公厅 国家卫生健康委办公厅关于进一步加强远程医疗网络能力建设的通知【工信厅联通信函〔2020〕251 号】，提出扩大网络覆盖、提高网络能力、推广网络应用、加强组织保障等四方面十六项举措。

《通知》明确要推进“互联网+”在医疗健康领域的应用发展，增强基层卫生防疫能力，进一步加强远程医疗网络能力建设。在扩大网络覆盖方面，《通知》除了要求基础电信企业持续推进偏远和贫困地区光纤宽带和 4G 网络建设以外，还要求推进 5G 网络覆盖医疗卫生机构，面向有条件的地区和应用需求明确的医疗卫生机构，加快推进 5G 网络建设，充分发挥 5G 网络低时延、大连接、高带宽的特点，应用 5G 切片、边缘计算等先进技术，为远程医疗提供更优网络能力。

同时，推动专线网络资源覆盖二级及以上医院。加快高质量互联网专线、数据专线及虚拟专线（VPN）网络建设，实现专线网络资源覆盖所有二级及以上医院（含妇幼保健院），具备提供优质专线服务能力。此外，《通知》还提出要提升各级医疗卫生机构网络接入率，2022 年实现 98%以上基层医疗卫生机构接入互联网。

在提高网络能力方面，《通知》要求推动医疗卫生机构网络普遍提速。为采用公众互联网接入的医疗卫生机构提速至 100Mb/s 以上，采用互联网专线接入的医疗卫生机构提速至 20Mb/s 以上。

在推广网络应用方面，文件要求探索 5G 网络在远程医疗中的创新应用。鼓励有条件的医疗卫生机构与基础电信企业合作，建设 5G 智慧医疗健康联合实验室或应用示范基地，推动基于 5G 网络的应用创新和服务创新。鼓励医疗设备厂商开展 5G 网络制式的研发和适配工作，提升专业设备的 5G 接入能力，充分发挥 5G 的技术优势。

同时，建设医疗云计算和大数据应用服务体系。充分利用大数据、云计算、人工智能等新一代信息技术，构建医疗专属云服务，结合区域全民健康信息平台建设，推动各级医疗卫生机构间数据共享互认和业务协同。

此外，《通知》还提出鼓励基础电信企业面向医疗卫生机构，特别是贫困地区基层医疗卫生机构，推出互联网宽带和专线接入资费优惠，资费水平不高于其他企业宽带和专线平均资费水平，减轻医疗卫生机构网络使用负担。（来源：工业和信息化部办公厅）

- **《两部门关于进一步加强远程医疗网络能力建设的通知》全文：**
- https://www.miit.gov.cn/zwgk/zcwj/wjfb/txy/art/2020/art_7ded5b88748d405faeccaa71a55ad1c9.html

➢ 国家网信办对手机浏览器扰乱网络传播秩序突出问题开展专项集中整治

2020 年 10 月 26 日，为有效解决网民反映强烈的手机浏览器网络传播乱象，国家网信办即日起对手机浏览器进行专项集中整治，重点聚焦行业突出问题实施“靶向治疗”，通过督导整改立起“带电的高压线”，推动手机浏览器传播秩序短期内实现实质性好转，回应社会关切。

一段时间以来，手机浏览器野蛮生长，违规从事互联网新闻信息服务，成为“自媒体”

传播乱象的聚集地和放大器。据介绍，此次专项集中整治和督导整改，把影响力较大的 8 款手机浏览器纳入首批名单进行重点集中整治，即 UC、QQ、华为、360、搜狗、小米、vivo、OPPO 等。集中整治将多措并举、标本兼治，着力解决三大突出问题：一是发布“自媒体”违规采编的各类互联网新闻信息，如歪曲解读经济民生政策、散布“小道消息”、传播谣言信息、翻炒旧闻编造“新闻”等；二是发布“标题党”文章，如恶意浮夸、“唱衰”“卖惨”、冒名炒作等；三是发布违背社会主义核心价值观的不良信息，如传播低俗图文视频、炒作明星绯闻隐私和娱乐八卦等。

此次集中整治和专项督导对手机浏览器提出了明确整改要求和具体标准，其中包括，不得发布“自媒体”违规采编的互联网新闻信息，不得 PUSH 弹窗“自媒体”发布的各类信息，不得使用断章取义、虚假夸大、攻击侮辱、耸人听闻等噱头式标题炒作热点敏感话题，不得发布无中生有、旧闻翻炒、拼凑剪接、捕风捉影等不实信息，不得发布低俗、血腥等不良信息，等等。

国家网信办有关负责人强调：10 月 27 日至 11 月 9 日，各手机浏览器要对照问题清单深入开展自查整改，举一反三全面清理违规信息、严管“自媒体”账号。同时，建立完善总编辑负责制、内容审核管理规范，从制度层面采取有力有效措施，切实防止扰乱网络传播秩序问题的发生。整改期间，8 款手机浏览器要切实做好“一公告、两审核”：“一公告”即 10 月 27 日 8 时，各手机浏览器要在首屏显著位置发布自查整改公告并 PUSH 推送全量用户，自觉接受社会监督。“两审核”即 10 月 28 日 15 时前，各手机浏览器要按照整改要求向属地网信部门提交细化整改工作安排，经审核同意后开展自查整改；自查整改结束之日，即 11 月 9 日 17 时前，各手机浏览器向网信部门提交自查整改报告和内容运营制度规范并接受审核。

自查整改结束后，网信部门将对自查整改情况进行检查评估，对整改后问题依然突出的手机浏览器，将依法依规进行严肃处置，直至取缔相关业务。此外，各地网信部门还将对属地手机浏览器进行全面摸底排查，一并按要求纳入专项整治和督导整改。

集中整治和督导整改期间，网信部门欢迎社会各界监督（国家网信办违法和不良信息举报中心网址：www.12377.cn）。国家网信办将依法依规对网民举报线索进行核查处置。（来源：网信中国）

➢ 国家市场监管总局关于加强网络直播营销活动监管的指导意见

2020 年 11 月 6 日，为加强网络直播营销活动监管，保护消费者合法权益，促进直播营销新业态健康发展。国家市场监管总局网站发布关于加强网络直播营销活动监管的指导意见，依法查处网络直播营销活动中侵犯消费者合法权益、侵犯知识产权、破坏市场秩序等违法行为，促进网络直播营销健康发展，营造公平有序的竞争环境、安全放心的消费环境。

指导意见要求，压实网络平台法律责任，压实商品经营者法律责任，压实网络直播者法律责任。同时，严格规范网络直播营销行为。规范商品或服务营销范围，规范广告审查发布，保障消费者知情权和选择权。

指导意见要求，依法查处网络直播营销违法行为。包括依法查处电子商务违法行为。依据《电子商务法》，重点查处擅自删除消费者评价、对平台内经营者侵害消费者合法权益行为未采取必要措施、未尽到资质资格审核义务、对消费者未尽到安全保障义务等违法行为。

依法查处侵犯消费者合法权益违法行为。针对网络直播营销中售后服务保障不力等问题，依据《消费者权益保护法》，重点查处对消费者依法提出的修理、重作、更换、退货、补足商品数量、退还货款和服务费用或者赔偿损失的要求，故意拖延或者无理拒绝等违法行为。

依法查处不正当竞争违法行为。针对网络直播营销中虚构交易或评价、网络直播者欺骗和误导消费者等不正当竞争问题，依据《反不正当竞争法》，重点查处实施虚假或者引人误解的商业宣传、帮助其他经营者进行虚假或者引人误解的商业宣传、仿冒混淆、商业诋毁和

违法有奖销售等违法行为。

依法查处产品质量违法行为。针对网络直播营销中售卖假冒伪劣产品等问题，依据《产品质量法》，重点查处在产品中掺杂掺假、以假充真、以次充好、以不合格产品冒充合格产品、伪造产品的产地和伪造或冒用他人厂名厂址等违法行为。

依法查处侵犯知识产权违法行为。针对网络直播营销中售卖侵犯知识产权产品等问题，依据《商标法》《专利法》，重点查处侵犯注册商标专用权、假冒专利等违法行为。

依法查处食品安全违法行为。针对网络直播营销中的食品安全问题，依据《食品安全法》，重点查处无经营资质销售食品、销售不符合食品安全标准的食品、销售标注虚假生产日期或超过保质期的食品等违法行为。

依法查处广告违法行为。针对网络直播营销中发布虚假违法广告问题，依据《广告法》，重点查处发布虚假广告、发布违背社会良好风尚的违法广告和违规广告代言等违法行为。

依法查处价格违法行为。针对网络直播营销中价格违法问题，依据《价格法》，重点查处哄抬价格、利用虚假的或者使人误解的价格手段诱骗消费者进行交易等违法行为。（来源：国家市场监督管理总局）

- **市场监管总局关于加强网络直播营销活动监管的指导意见**
- **全文：**http://gkml.samr.gov.cn/nsjg/ggjgs/202011/t20201106_323092.html

五、本期重要漏洞实例

➢ IBM Security Access Manager 安全绕过漏洞

发布日期：2020-10-27
更新日期：2020-10-27
受影响系统：
IBM Security Access Manager 9.0.7
描述：

CVE(CAN) ID: CVE-2020-4395
IBM Security Access Manager 是美国 IBM 公司的一款应用于信息安全管理的产品。该产品通过面向 Web、移动和云计算的集成设备来实现访问管理控制。
IBM Security Access Manager 9.0.7 版本存在安全绕过漏洞，该漏洞源于在注销后未能使会话失效，攻击者可利用该漏洞模拟系统上的另一个用户。
建议：

厂商补丁：

IBM
目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://www.ibm.com/support/pages/node/6347592

➢ Oracle MySQL Server 存在未明漏洞

发布日期：2020-10-28
更新日期：2020-10-28
受影响系统：
Oracle MySQL Server <=8.0.21
描述：

CVE(CAN) ID: CVE-2020-14838
Oracle MySQL 是美国甲骨文（Oracle）公司的一套开源的关系数据库管理系统。MySQL Server 是其中的一个数据库服务器组件。
Oracle MySQL Server 8.0.21 及更早版本中的 Server: Security: Privileges 组件存在未明漏洞。攻击者可利用该漏洞未经授权读访问一部分 MySQL Server 可访问的数据。
建议：

厂商补丁：

Oracle
厂商已发布了漏洞修复程序，请及时关注更新：
https://www.oracle.com/security-alerts/cpuoct2020.html

➢ 多款 Cisco 产品安全启动绕过漏洞

发布日期：2020-10-21
更新日期：2020-11-05
受影响系统：
Cisco Firepower 2100 Series
Cisco Firepower 1000 Series firewalls
描述：

CVE(CAN) ID: CVE-2020-3458
Cisco Firepower Threat Defense 是一套提供下一代防火墙服务的统一软件。Cisco Adaptive Security Appliances Software 是一套防火墙和网络安全平台。该平台提供了对数据和网络资源的高度安全的访问等功能。
Cisco Adaptive Security Appliance (ASA)和 Firepower Threat Defense (FTD)存在安全启动绕过漏洞。该漏洞源于程序未对安全引导进程进行充分保护。攻击者可通过将代码注入到特定的文件利用该漏洞打破信任链绕过安全启动机制。
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxos-sbbyp-KqP6NgrE
建议：

厂商补丁：
Cisco
Cisco 已经为此发布了一个安全公告（cisco-sa-fxos-sbbyp-KqP6NgrE）以及相应补丁：
cisco-sa-fxos-sbbyp-KqP6NgrE：Cisco Adaptive Security Appliance Software and Firepower Threat Defense Software for Firepower 1000/2100 Series Appliances Secure Boot Bypass Vulnerabilities
链接：https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-fxos-sbbyp-KqP6NgrE

➢ 多款 Mozilla 产品内存破坏漏洞

发布日期：2020-10-01
更新日期：2020-11-05
受影响系统：
Mozilla Firefox < 81

Mozilla Thunderbird < 78.3
Mozilla Firefox ESR < 78.3

描述：

CVE(CAN) ID: CVE-2020-15673

Mozilla Firefox 等都是美国 Mozilla 基金会的产品。Mozilla Firefox 是一款开源 Web 浏览器。Mozilla Firefox ESR 是 Firefox(Web 浏览器)的一个延长支持版本。Mozilla Thunderbird 是一套从 Mozilla Application Suite 独立出来的电子邮件客户端软件。

Firefox 81 之前版本、Thunderbird 78.3 之前版本和 Firefox ESR 78.3 之前版本存在内存破坏漏洞。攻击者可利用该漏洞执行任意代码。

<*来源：Jason Kratzer

链接：https://www.mozilla.org/en-US/security/advisories/mfsa2020-42/

建议：

厂商补丁：

Mozilla

Mozilla 已经为此发布了一个安全公告（mfsa2020-42）以及相应补丁:

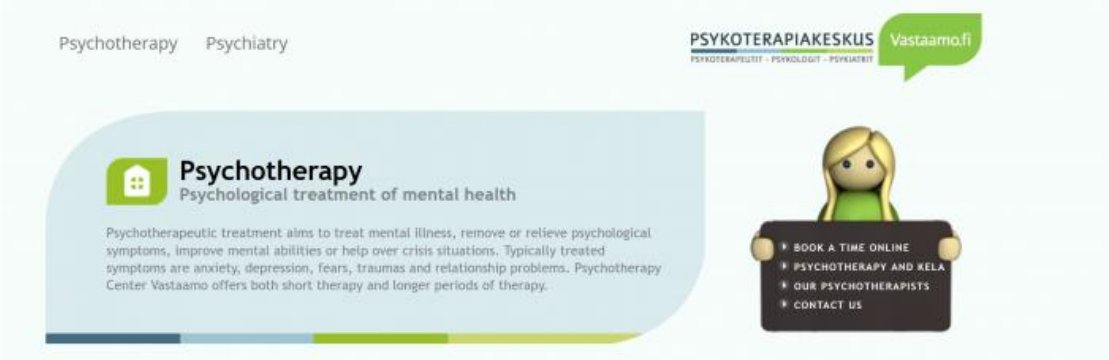
mfsa2020-42：Mozilla Foundation Security Advisory

链接：https://www.mozilla.org/en-US/security/advisories/mfsa2020-42/

六、本期网络安全事件

➢ 黑客攻破芬兰心理治疗公司 Vastaamo 并公布数百人健康数据

2020 年 10 月 26 日报道，据外媒报道，当地时间上周五，有关一群黑客勒索一家为公共卫生系统提供心理治疗服务的私人公司的丑闻结果令芬兰人震惊。在一个号称在数字化和数据安全方面处于领先地位的国家，犯罪分子在检测到 Vastaamo 公司系统中的漏洞后成功访问了该公司数千名客户的数据库。



尽管根据 Vastaamo 网站介绍，该公司为抑郁症和焦虑症患者提供心理和精神治疗。许多客户来自由 Finnish Social Security (Kela)支付的公共服务部门。

据悉，勒索者索要约 45 万欧元（以比特币形式支付）以换取不公布数千人的临床和心理健康数据。而在两日前，犯罪分子开始在加密网络 Tor 上发布数据，每天发布 100 个人。他们声称除非收到钱否则不会罢休。由于该公司拒绝接受黑客的要求，于是包括未成年人在内的 200 多人的个人数据被公布在网上。被公布的信息非常敏感，包括患者的姓名、个人身份证号码、电话号码、电子邮件地址和居住地址以及治疗过程的内容。

据 Vastaamo 在新闻稿中披露，一位不知名的敌对方联系了他们并声称从该公司的客户那里获取了机密信息，对此，芬兰中央刑事警察已经展开刑事调查，另外他们还立即通知了芬兰网络安全中心、Valvira 和数据保护专员。此外，Vastamo 还立即采取了措施，跟外部独立安全专家合作来解释清楚这件事情。

据了解，有 100 人的数据于周四晚被公布。但在周五早上，发布数据的页面被删除，这引发了人们对 Vastamo 可能向敲诈者支付报酬的传言。不过截止到目前，该公司既没有承认也没有否认这笔付款。Vastaamo 董事会主席 Tuomas Kahri 告诉报纸 Ilta Sanomat，他不会对赎金的指控发表评论。

关于勒索者的身份或国籍目前则都不清楚，他们似乎并不担心当局可能会逮捕他们。周

四，Ilta Sanomat 跟他们交换了几条信息。这些罪犯表示，他们不知道公布的信息中有未成年人的数据。不过他们保证这不会停止他们的行动。

据披露，勒索者还向患者个人提供了一种可能，即用价值 540 欧元的比特币删除他们自己的数据。

芬兰国家调查局(KRP)正在调查这次攻击，该机构认为这是一起严重侵犯和传播私人信息的案件。警方要求那些注意到自己私人信息被传播的人提交一份电子犯罪报告。在这起勒索案中，该公司因未能提前通知客户数据被泄露而受到批评。一些人抱怨称，他们是在公众知道这件事之后才被联系上的。（来源：cnBeta）

➢ 女子获取 300 万条公民个人信息推销“男士会所”，获刑三年

2020 年 10 月 28 日报道，向他人推销男士会所业务，王某开设四个办公点，雇佣数十名电话推销员进行电话销售。而员工拿到的公民个人信息，均是王某通过收受等方式获取的，民警在王某自用手机及办公点电脑上查获公民个人信息 300 余万条。记者从北京法院审判信息网获悉，王某因犯侵犯公民个人信息罪，被顺义法院判处有期徒刑 3 年。

2019 年 3 月，王某以他人名义注册成立北京梦创宏伟网络科技有限公司，王某为公司实际经营人。同年 3 月至 10 月，王某又陆续使用北京华艺众合网络技术有限公司、北京飞唐锦荣网络技术艺术有限公司的营业执照，在顺义区开设办公点三处。

作为四处办公点的总负责人，王某管理数十名电话销售人员，从事推销外省市男士会所业务。其间，王某违反国家规定，通过收受等方式获取大量公民个人信息，并提供给下属用于拨打电话推销会所。民警从上述四处办公点扣押的电脑四台、王某个人使用的手机中，查获公民个人信息 300 余万条。

顺义检察院以王某涉嫌犯侵犯公民个人信息罪，对其提起公诉，王某表示自愿认罪认罚。王某的辩护人认为，王某具有坦白情节，认罪认罚，主观恶性低，获利少，建议对其从轻处罚并判处缓刑。

经审理，顺义法院认为，被告人王某违反国家有关规定，非法获取公民个人信息，情节特别严重，其行为已构成侵犯公民个人信息罪。根据王某的犯罪事实、犯罪性质、情节和对社会的危害程度，不宜对其适用缓刑。综合全案证据，法院一审以王某犯侵犯公民个人信息罪，判处其有期徒刑 3 年，并处罚金 3 万元。（来源：北京日报）

➢ 阿里旗下电商平台 Lazada 110 万账户信息被黑客入侵

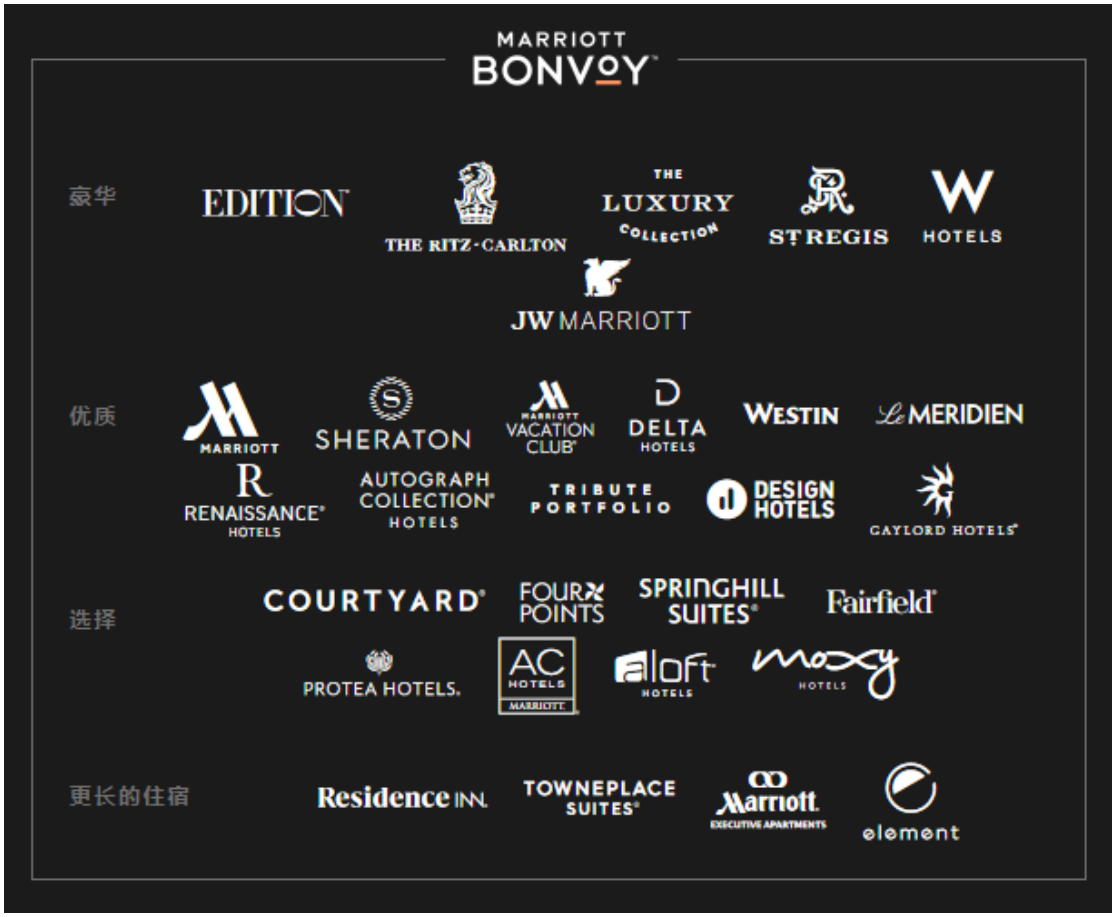
2020 年 10 月 31 日，阿里巴巴旗下电商平台、新加坡电子商务公司 Lazada 今日宣布，其 110 万账号信息被黑客入侵。在这个拥有 570 万人口的国家（新加坡），这显然是一次重大的黑客入侵事件。这些账号信息包括用户的家庭住址和部分信用卡号码等。Lazada 在一封电子邮件中称，这些信息是从其杂货子公司 RedMart 的数据库中窃取的，属于 18 个月前的数据。

Redmart 成立于 2011 年，在新加坡提供生鲜及其他杂货网购服务，平台覆盖了 8000 余种商品。其最大的特色是自建仓储和物流，2016 年被 Lazada 收购。

Lazada 的一位发言人称：“被非法获取的用户信息包括姓名、电话号码、电子邮件和邮寄地址、加密密码和部分信用卡号码。”Lazada 表示，该公司已立即采取行动阻止对数据库的访问，其当前的用户数据不受影响。2017 年 6 月，阿里巴巴宣布再次对 Lazada 投资 10 亿美元，将其所持 Lazada 股份从 51%提高到 83%。（来源：新浪科技）

➢ 因未能确保客户个人数据安全 万豪国际被罚 1840 万英镑

2020 年 11 月 1 日，英国隐私监管机构表示，已就喜达屋酒店及度假酒店国际集团(Starwood Hotels & Resorts Worldwide Inc.，简称：喜达屋)遭受网络攻击对万豪国际集团(Marriott International Inc., MAR)处以 1840 万英镑(2380 万美元)的罚款。



英国信息委员办公室(ICO)表示：一项调查发现万豪未能实施适当的技术或组织措施来保护其系统上处理的个人数据，该机构对该公司未能确保客户个人数据的安全而实施处罚。今年 3 月 31 日，万豪国际集团发布公告，称约 520 万名客人的信息可能被泄露，包括姓名、

地址、联系方式、偏好等。

这已经不是万豪首次大规模泄露客人的个人隐私。

早在 2018 年 11 月，万豪国际集团官方发布声明称，喜达屋旗下酒店的客房预订数据库被黑客入侵，在 2018 年 9 月 10 日或之前曾在该酒店预定的最多约 5 亿名客人的信息或被泄露。这些客人中约有 3.27 亿人的信息包括：姓名、邮寄地址、电话号码、电子邮件地址、护照号码、SPG 俱乐部账户信息、出生日期、性别、到达与离开信息、预定日期和通信偏好。对于某些客人而言，泄露的信息还包括支付卡号和支付卡有效期，但支付卡号已通过高级加密标准(AES-128)加密。

上述消息公布后，万豪国际股价大跌 5.75%。当时万豪国际集团并表示已向相关执法部门报告此事件，并配合调查。资料显示，2016 年美国连锁酒店运营商万豪国际集团以超 120 亿美金收购喜达屋酒店及度假村全球公司。（来源：NBC 新闻网）

➢ 山寨版上海迪士尼 App 被工信部点名，正版回应：已着手调查

2020 年 10 月 27 日，工信部官网通报 2020 年第五批存在侵害用户权益行为的 App 名单，一款名为“上海迪士尼乐园（版本 3.3.7）”的 App 在列。随后，“上海迪士尼等 131 款 APP 侵害用户权益”的话题登上微博热搜。下午 7 时许，**上海迪士尼度假区官方回应**，上述 App 并非官方应用程序。

31	上海迪士尼乐园	霍尔果斯驴迹软件科技有限公司	华为应用市场	3.3.7	违规收集个人信息

据通报，上海迪士尼乐园 App 为霍尔果斯驴迹软件科技有限公司开发，应用来源是华为应用市场，存在的主要问题是“违规收集个人信息”。

上海迪士尼度假区官方微博回应，“上海迪士尼乐园”App 是未经上海迪士尼度假区授权开发的假冒 App，并非上海迪士尼度假区的官方应用程序，与上海迪士尼度假区无任何关联。而且，上海迪士尼度假区已就此与工信部进行了沟通。**记者注意到，目前“上海迪士尼乐园”App 已从华为应用市场下架**。

据悉，上海迪士尼度假区的官方应用程序为“上海迪士尼度假区官方 App”，由度假区团队自行开发和管理。上海迪士尼度假区表示，游客可通过苹果应用程序商店或腾讯应用宝

下载上海迪士尼度假区官方 App。目前，上海迪士尼度假区已就该假冒应用程序着手调查。

“蹭热度”的高仿 App 现象一直屡禁不止

由中央网信办、工信部、公安部、市场监管总局委托成立的 App 专项治理工作组曾撰文表示，“高仿/山寨”App 一方面在用户使用时可能带来安全隐患，另一方面给公平竞争环境、创新活力带来挑战，在持续治理完善移动互联网生态过程中，是始终绕不开的难题之一。

为什么会屡禁不止？应用商店能否进行公正把关？

App 专项治理工作组表示，首先，界定什么是“高仿/山寨”App 一直是个难题。如果是从名称、功能、图标、界面、宣传方式等角度发现 App 之间是否存在相似性来看，恐怕很难给出一个相对固定的标准；如果从商标、产权等角度去衡量，问题的复杂性可能更高，因为大量 App 的功能、服务模式等本身就是高度同质化的状态。

从应用商店把关角度，App 专项治理工作组还谈到，虽然应用商店会根据国家有关法律法规以及相关监管要求，对 App 进行审核和管理。但同时，出于应用商店之间的市场竞争机制，不断充实、丰富应用市场中 App 的类型、数量，吸引更多用户使用往往成为其核心经营思路。

究其内在原因，App 专项治理工作组认为，一旦从“是否为高仿/山寨”角度进行审核：一则审核机制谁来定，谁来审，其过程很难保证公正性，操作不当很有可能会被沦为竞争对手互相打压的工具；二则是否因为审核等原因会导致原有的市场竞争机制被破坏？会对鼓励创新等的氛围和环境造成影响？缺乏了新鲜血液循环，是否会导致应用市场活力、竞争力等下降等都是个未知数，利弊很难评判。（来源：南方都市报）

➢ 瑞典最大保险公司泄露近百万客户个人信息

2020 年 10 月 16 日，当地时间 11 月 3 日，瑞典最大的保险公司 Folksam 在新闻稿中证实，近 100 万客户的个人信息已泄露给 Facebook 和 Google 等社交媒体。Folksam 表示歉意，并已要求公司删除该信息。

在一次内部审计中，Folksam 发现与数字合作伙伴共享了大约 100 万人的个人数据，其中一些被认为是敏感的。Folksam 已要求合作伙伴公司删除该信息。

“我们知道这会引起客户的关注，我们认真对待发生的事情。我们已立即停止共享个人信息，并要求将其删除。”Folksam 营销和销售主管表示，“我们这样做的目的是分析并为客户提供定制的报价，但是不幸的是，我们没有以正确的方式做到这一点。”

Folksam 分享了可能被视为敏感的个人数据，例如，某人购买了工会保险或怀孕保险，以及特别值得保护的个人数据——个人社会保险号。Folksam 已要求已收到个人信息的合作伙伴将其删除。当前，没有信息表明该信息已被第三方以任何不当方式使用。从 Folksam 接收个人数据的公司有 Facebook，Google，Microsoft，Linkedin 和 Adobe。（来源：央视网）

信息安全意识产品服务

021-33663299