国盟信息安全通报

2020 年 8 月 02 日第 221 期

全国售后服务中心

国盟信息安全通报

（第 221 期）

国际信息安全学习联盟

2020 年 08 月 02 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 481 个，其中高危漏洞 147 个、中危漏洞 290 个、低危漏洞 44 个。漏洞平均分值为 5.75。本周收录的漏洞中，涉及 0day 漏洞 204 个（占 42%），其中互联网上出现“Open eClass SQL 注入漏洞、Exhibitor 命令注入漏洞”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 3433 个，与上周（3700 个）环比减少 7%。

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（2020 年 07 月 19 日—2020 年 08 月 02）.....4
➢漏洞引发的威胁（2020 年 07 月 19 日—2020 年 08 月 02）.....5
➢漏洞影响对象类型（2020 年 07 月 19 日—2020 年 08 月 02）.....5
三、安全产业动态 6
➢让互联网从“最大变量”变成事业发展“最大增量”.....6
➢从最新发布的《 App 收集使用个人信息自评估指南》看个人信息保护着力点.....11
➢做好“新安全” 保障“新基建”.....15
➢网络安全视野下金融业数字化转型的机遇和挑战.....18
四、政府之声 28
➢工信部发布关于开展纵深推进 APP 侵害用户权益专项整治行动的通知.....28
➢国家网信办全面部署加强“自媒体”规范管理工作.....29
➢市场监管总局关于公开征求《关于加强网络直播营销活动监管的指导意见》.....30
➢公安部集中打击治理电信网络诈骗犯罪取得阶段性成效.....31
五、本期重要漏洞实例 33
➢Microsoft Visual Studio Code ESLint Extention 命令注入漏洞.....33
➢Cisco SD-WAN vManage Software XML 外部实体注入漏洞.....33
➢Adobe Magento php 对象注入漏洞.....34
➢IBM Data Risk Manager 安全限制绕过漏洞.....34
六、本期网络安全事件 36
➢阿根廷电信被黑客勒索软件攻击 并要求支付 750 万美元.....36
➢韩国棋手利用 AI 工具作弊 被判处有期徒刑 1 年.....37
➢上海某“代发工资”公司账户密码是“123456”,730 万被黑客转走!.....38
➢佳明官方确认遭网络攻击：系统正积极恢复中用户数据未丢失或被盗用.....40
➢化妆品巨头雅芳泄漏 1900 万条数据记录.....41
➢现实版谍战大戏：大众汽车特别项目组竟被窃听长达 1 年.....43

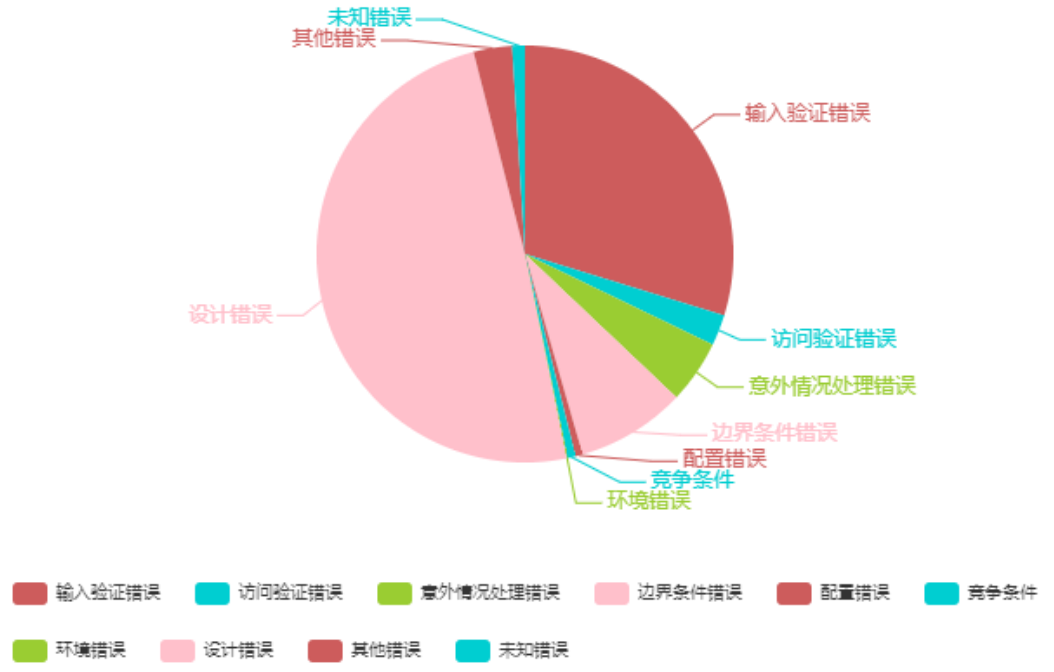
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

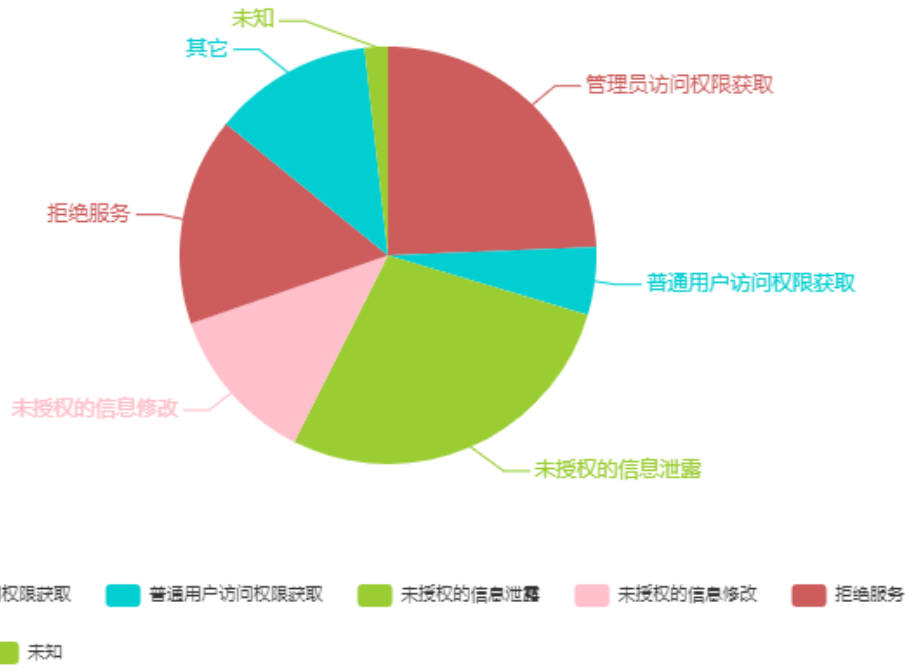
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 481 个，其中高危漏洞 147 个、中危漏洞 290 个、低危漏洞 44 个。漏洞平均分值为 5.75。本周收录的漏洞中，涉及 0day 漏洞 204 个（占 42%），其中互联网上出现“Open eClass SQL 注入漏洞、Exhibitor 命令注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3433 个，与上周（3700 个）环比减少 7%。

二、安全漏洞增长数量及种类分布情况

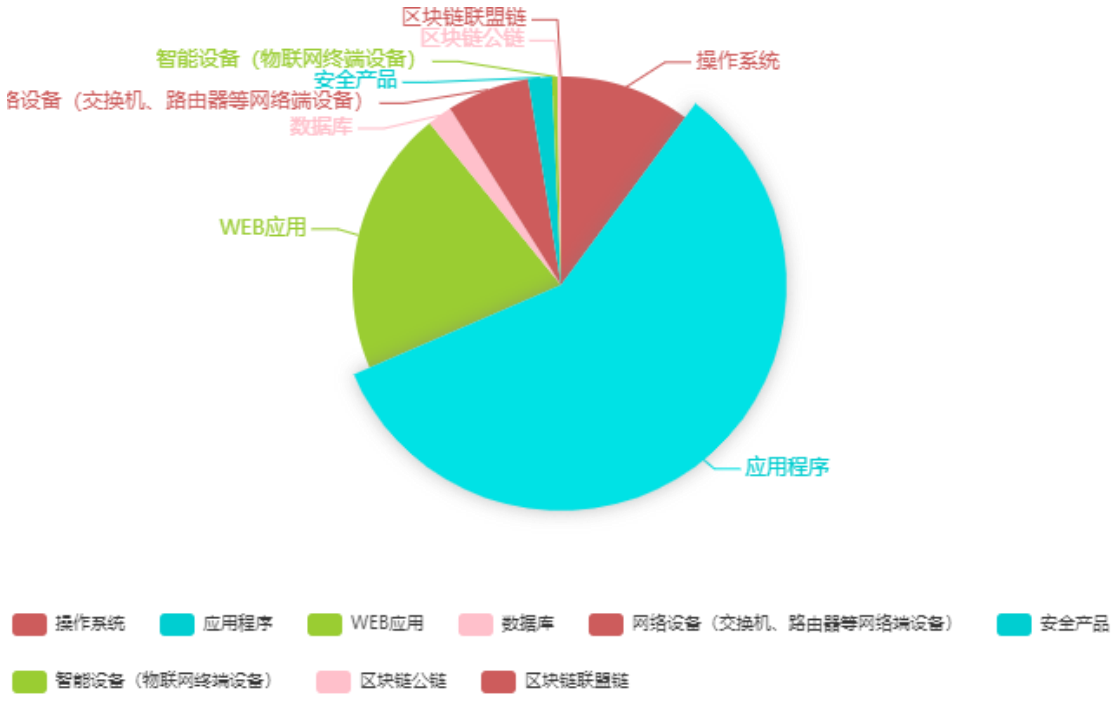
➢ 漏洞产生原因（2020 年 07 月 19 日—2020 年 08 月 02）



➢ 漏洞引发的威胁（2020 年 07 月 19 日—2020 年 08 月 02）



➢ 漏洞影响对象类型（2020 年 07 月 19 日—2020 年 08 月 02）



三、安全产业动态

➢ 让互联网从“最大变量”变成事业发展“最大增量”

日前，中央宣传部副部长，中央网络安全和信息化委员会办公室主任、国家互联网信息办公室主任庄荣文在《中国党政干部论坛》发表署名文章，**要求深刻分析网上舆论新形势，准确判断网络传播格局新变化，科学把握网络传播规律，不断推进工作理念、方法手段、载体渠道、制度机制创新，全面提高用网治网水平，使互联网这个最大变量变成事业发展的最大增量。具体而言，庄荣文提出了三点要求**。

一、因势而谋，科学认识网络传播格局和舆论生态的新变化

互联网作为 20 世纪人类最伟大的发明之一，自 1969 年诞生以来，在世界范围内不断发展、快速普及，已经全面融入并深刻改变着人类社会发展进程。目前，我国作为互联网大国，网民总数已达 9.04 亿、网站数量接近 500 万、各类 APP 达 367 万，使用网络新闻、社交、音乐、文学、视频、直播等已经成为亿万网民日常活动中不可或缺的重要组成部分。总的看，传统传播格局正处于深刻变革之中，网络传播格局和舆论生态正在发生整体重塑。

在理论传播方面，当前我国经济社会的快速发展给人们的思想观念带来深刻影响，网上各种社会思想多样杂陈，多元多样多变的社会思潮通过互联网快速传播扩散，“普世价值”、西方“宪政民主”、历史虚无主义等错误思潮对思想理论传播格局和主流意识形态形成冲击和干扰，党的意识形态部门统一领导思想理论传播的难度加大，落实“两个巩固”的任务更加艰巨。

在正面宣传方面，新媒体迅速崛起，日益成为信息传播的主渠道主平台，新闻客户端和各类社交媒体越来越成为人民群众特别是年轻人的第一信息源，对传统主流媒体传播力影响力的冲击难以避免。据统计，我国排名前十的新闻客户端聚集了 90%以上的信息量和网民流量，信息阅读量以数十亿计，如何用好新媒体做大做强正面宣传成为重大课题。

在新闻报道方面，随着互联网、智能终端广泛普及，新媒体新技术新应用迭代升级，“人人都有麦克风，个个都是自媒体”的现实颠覆了以采编权为中心的媒体管理方式，各类信息爆炸式增长、裂变式传播，提高新闻报道的传播力引导力影响力公信力任务十分艰巨。

在社会舆论方面，网上舆论摆脱现实时间、空间限制，对社会的影响力空前展现，各种力量在网上竞相发声，呈现突发性、多元性、交互性、冲突性、匿名性等特点，舆情风险极易扩大蔓延、形成声势。当前，网络应用平台加快开放融合，使信息能在瞬间实现跨平台全网传播，传播能力呈指数级增长，产生左右社会舆论的强大效果。

在知识普及方面，互联网让信息以数字形式在全球范围内广泛汇集、自由流动，搜索引擎、网络百科、知识付费、问答社区等新模式超越人际传授、印刷品流通等，成为新的知识传播方式，但大量错误信息、低俗信息、虚假信息等也夹杂其中、扩散蔓延。

在网络文化方面，互联网有力激发了文化创造活力，网络文学、网络音乐、网络影视、网络游戏加快发展，网络直播、短视频等迅速崛起，网上文化产品琳琅满目、精彩纷呈，极大丰富了网民的精神文化生活。但与此同时，网络文化产品水平参差不齐、鱼龙混杂，其中包含的个人主义、拜金主义、消费主义、享乐主义等观念，一定程度上对社会主义核心价值观带来了消极影响。

在网络社交方面，目前我国即时通信用户规模达 8.96 亿，网上聊天、网络交友、网络分享等成为人们日常交流交往的重要途径，书信、固话、电报等传统方式日益式微，网络社交平台掌握海量用户信息，链接线上线下多种场景，不仅具有很强的公共舆论议题设置能力，而且社会动员功能不断增强。

在网络生态方面，网络空间已经成为亿万民众共同的生活空间，我国网民人均每日上网时长为 4.4 个小时，通过手机接入互联网的比例超过 99%。如何发挥网络特色、网络优势传播社会主义核心价值观，为广大网民特别是青少年网民构筑良好网络生态、营造清朗网络空间，成为摆在我们面前重大而紧迫的任务。

二、应势而动，有效应对网上正面宣传和舆论引导工作面临的新挑战

习近平总书记强调，宣传思想工作要胸怀大局、把握大势、着眼大事，找准工作切入点和着力点。近年来，在全党全社会的共同努力下，网上正面宣传和舆论引导工作深入开展，

网络内容建设持续推进，网络综合治理体系加快建立，主流思想舆论的传播力引导力影响力公信力不断增强，网上正能量更加强劲、主旋律更加高昂、网络空间日益清朗。一是网上正面宣传有声有色。精心做好习近平新时代中国特色社会主义思想网上宣传，围绕学习宣传党的十九大和十九届二中、三中、四中全会精神以及庆祝新中国成立 70 周年等重大主题，持续创新宣传语态、强化网上互动引导，做到全渠道参与、全平台覆盖，在网络空间唱响了礼赞新中国、奋斗新时代的昂扬旋律，党的声音成为网络空间最强音。二是网上舆论引导及时有效。组织开展重大主题网评引导，建立有关网上舆情引导工作机制，做好经济形势正面引导，围绕“六稳”加强重大政策措施宣介阐释，主动设置议题，回应社会关切，网上舆论引导实效不断增强。三是网络意识形态斗争坚决有力。面对严峻复杂的网络意识形态斗争形势，在管网治网上出重拳、亮利剑，连续打好网络意识形态关键战役，有效遏制各类有害信息传播扩散，及时批驳历史虚无主义等网上错误思潮和观点，网络意识形态安全得到有力维护。四是网络综合治理能力明显提升。加快建立网络综合治理体系，制定出台《网络信息内容生态治理规定》，推动网络生态治理工作进一步科学化、制度化、规范化，深入开展网络生态治理，开展“清朗”系列专项行动，持续推进自媒体乱象和短视频专项整治行动，集中清理负面有害信息、违法违规账号与移动应用程序等，加大青少年网络保护力度，深入推进实施“争做中国好网民”工程，管网治网水平进一步提升。总的看，与党和国家各项事业发展同步，网上正面宣传和舆论引导工作有力有效，呈现出持续健康发展的良好态势。

同时也要清醒认识到，网络宣传舆论工作面临着许多新形势新挑战新课题，维护网络意识形态安全的任务仍然十分艰巨。

网络意识形态斗争形势严峻复杂。西方敌对势力一直把我国发展进步视为对西方价值观和制度模式的威胁，想方设法对我国进行意识形态渗透颠覆，近年来更加倚重将互联网作为意识形态输出最直接最便利的工具，不断升级对我国的网络攻势。境内外敌对势力大肆散布恶性政治谣言，混淆视听、扰乱人心、刻意抹黑党和国家形象，恶意炮制有害思想观点，利用社交媒体进行网上串联结社、煽动“街头政治”，企图侵蚀党的执政基础，破坏我国社会政治大局稳定。面对新冠肺炎疫情的蔓延，一些西方政客将病毒“标签化”、将疫情政治化，炮制炒作所谓的“中国源头论”“中国隐瞒论”“中国责任论”等荒谬论调，对中国刻意污名化，抹黑中国的抗疫措施，网上舆论环境错综复杂。

网络新技术新应用新业态加快迭代。当前，云计算、大数据、人工智能、算法推荐等新技术大规模应用，无网络社交、匿名社交、加密社区、网络直播等新应用层出不穷，网上信息传播呈现出海量聚集、加密传输、差异推送等特点，引发网络传播秩序深刻变革，带来一

系列新课题新挑战。基于大数据的用户画像、算法推荐等新技术正在网络传播领域加速应用，人工智能基于海量数据计算分析用户的兴趣爱好和变化规律，直接生产和精准推送更有针对性的内容，“深度伪造”等技术很容易被用于制作虚假图像、音频、视频等，5G 网络商用将驱动网上信息爆发式增长，更多信息传播将以超清视频、超高清全角度直播为主的多媒体信息流形式呈现，给互联网管理带来新课题。

各类社会风险向网络空间传导趋势明显。当前，我国改革进入攻坚期和深水区，发展面临的风险挑战前所未有，一些热点问题和突发事件发生后，信息在网上扩散发酵，网上舆论又可能反过来激化网下问题，互联网日益成为各类风险的传导器和放大器。新冠肺炎疫情发生以来，网上舆论异常复杂，涉新冠肺炎疫情等网上舆情热度持续保持高位，一些别有用心的人借机胡评妄议，对党的方针政策进行诋毁歪曲，煽动偏激情绪和极端心态，给疫情防控工作、社会大局稳定造成干扰。

网络生态治理仍然任务艰巨。网络空间是亿万网民共同的精神家园。当前，网络空间各种乱象仍然存在，网络暴力高发频发，成为网络空间的“毒瘤”，个人信息过度收集、滥用、泄露等问题日益严峻，网络淫秽色情、网络诈骗、非法网络集资、恶意营销、网络攻击和侵权盗版等行为屡禁不止。这些网上乱象危害良好社会风气，严重侵犯人民群众合法权益，严重污染网络生态环境，对主流意识形态形成干扰和冲击。

三、顺势而为，以建立网络综合治理体系为重点提高用网治网工作水平

习近平总书记强调，中国特色社会主义进入新时代，必须把统一思想、凝聚力量作为宣传思想工作的中心环节。网上正面宣传和舆论引导工作是宣传思想工作的重要组成部分，必须走在前、作表率，自觉从党和国家事业发展大局中深刻认识和把握职责使命，为实现“两个一百年”奋斗目标和中华民族伟大复兴的中国梦提供有力服务、支撑和保障。

坚持高举旗帜，以习近平新时代中国特色社会主义思想统领全局。习近平总书记强调，要高举马克思主义、中国特色社会主义的旗帜，坚持不懈用新时代中国特色社会主义思想武装全党、教育人民、推动工作，在学懂弄通做实上下功夫，推动当代中国马克思主义、21 世纪马克思主义深入人心、落地生根。贯彻落实习近平总书记要求，要聚焦铸魂立心，始终把学习宣传贯彻习近平新时代中国特色社会主义思想作为重中之重，充分发挥互联网的思想引领作用，精心做好宣传阐释，广泛凝聚全党全国各族人民实现“两个一百年”奋斗目标的思想共识和智慧力量。要突出入脑入心，阐释好习近平新时代中国特色社会主义思想蕴含的深刻道理学理哲理，把科学的理论讲透彻，把深刻的思想讲鲜活，让党的创新理论通过互联网“飞入寻常百姓家”。要坚决维护核心，教育引导广大党员干部增强“四个意识”，坚定“四

个自信”，做到“两个维护”，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，真正做到忠诚核心、拥戴核心、维护核心、紧跟核心。

坚持守正创新，不断提高网上正面宣传和舆论引导的传播力引导力影响力公信力。社会主义意识形态的凝聚力和引领力，既取决于富有说服力、感召力的内容，也取决于广泛有效的传播。要坚持正确方向，坚持用马克思主义占领网上阵地，做大做强网上正面宣传和舆论引导，做好网上形势宣传、政策宣传、成就宣传、典型宣传，积极培育和践行社会主义核心价值观，培育积极健康、向上向善的网络文化。要坚持创新思维，推进网上宣传理念、内容、形式、方法、手段等创新，特别是运用好大数据、人工智能、算法推荐等新技术新应用，探索“去中心化”生产方式，建设网上“正能量稿池”，开展分众化传播、差异化传播、个性化传播，做到春风化雨、润物无声。要坚持效果导向，紧密结合知识分子、普通群众、青少年等各类网民群体特点，积极组织开展跟帖评论，及时回应社会关切、群众诉求；善于运用网民视角，深耕信息内容，使广大网民愿听愿看、爱听爱看，不断提升网络宣传引导的针对性和有效性。

坚持立破并举，坚决打赢网络意识形态斗争。能不能牢牢掌握意识形态工作领导权，关键要看能不能占领网上阵地，能不能赢得网上主导权。要以高度的思想自觉、政治自觉、行动自觉坚守网上阵地，既要旗帜鲜明支持正确思想言论，发改革奋进时代之强音、立主流思想舆论之强势，又要在管网治网上出重拳、亮利剑、见实效。要把握网上斗争特点，建立健全网上风险防范机制，坚决粉碎敌对势力网上煽动“街头政治”“颜色革命”等图谋，坚决管控各类有害信息，及时批驳历史虚无主义等错误思潮，有力维护网络意识形态安全。要坚持疏堵结合，对于网民正常表达的意见建议甚至尖锐批评，不能简单化处理，要有针对性地分析、研判和引导，对建设性意见要及时采纳，对困难要及时帮助，对不了解情况的要及时宣介，对模糊认识要及时廓清，对怨气怨言要及时化解，对错误看法要及时引导和纠正。

坚持综合治理，不断提高综合治网能力。建立网络综合治理体系，是党的十九大明确提出的一项重要任务，也是管网治网的治本之策。要加快建立健全网络综合治理体系，努力形成党委领导、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，推动互联网实现由“管”到“治”的深刻转变。要深化依法治网，加快构建系统完备、科学规范、运行有效的管网治网法规制度体系，进一步完善网络综合执法协调机制，全面提高网络空间法治化水平。要强化技术治网，充分利用大数据、人工智能等新技术新手段，探索建设和完善高水平互联网舆情预警分析系统，持续提升对新技术新应用的管控能力。要发挥网民作用，坚持积极服务网民、广泛动员网民、紧紧依靠网

民，真正使广大网民成为正能量的生产者、传播者、引领者，让网民影响网民、让网民教育网民，引导网民自觉规范网络行为、净化网络环境。

坚持党管互联网，进一步落实网络意识形态工作责任制。网络意识形态工作责任制是贯彻落实党管互联网原则、做好新形势下网络意识形态工作的有力抓手。要以党的政治建设为统领，始终推动各级党委（党组）把坚决做到“两个维护”作为网络意识形态工作的头等大事和重中之重，不断增强落实网络意识形态工作责任制的政治责任感和使命感，全面落实各项工作任务，管好导向、管好阵地、管好队伍。健全责任体系，细化责任清单，明晰责任边界，完善责任链条，健全考评指标体系，提升考核刚性标准，进一步构建分工合理、衔接有序、齐抓共管的网络意识形态工作整体格局，全面提升工作的整体性协同性实效性。（来源：人民网）

➢ 从最新发布的《 App 收集使用个人信息自评估指南》看个人信息保护着力点

为指导 App 运营者对其收集使用个人信息的情况进行自查自纠，2019 年 3 月 App 专项治理工作组发布了《App 违法违规收集使用个人信息自评估指南》。随着 App 违法违规收集使用个人信息评估工作的开展和深入，以及《App 违法违规收集使用个人信息行为认定方法》（以下简称“《认定方法》”）发布，国标 GB/T 35273-2020《信息安全技术 个人信息安全规范》（以下简称“《规范》”）的修订，编制组结合各方经验及反馈，及时对指南进行了修订。在 2020 年 3 月对外发布《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，并于 **7 月发布了最新版《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“新版《指南》”）**。

围绕《App 违法违规收集使用个人信息行为认定方法》（以下简称“《认定方法》”）中六

类违法违规行为，新版《指南》进行逐条解读、细化。从结构而言，删减了《征求意见稿》中每个评估点的法律依据，行文更简洁实用；在内容上，更广泛的引入了相关法律法规、标准规范的要求，将六个评估点细化为 71 个条款，且多处以注的形式补充了 App 个人信息保护合规路径及其违法违规典型问题，有助于 App 运营者透过表象深入理解法律法规、标准规范要求，便于其在自评估时有的放矢查找问题；从细节改动来看，文字更简练准确，要求更贴近实际应用，充分体现了个人信息保护与用户良好体验相结合的编制思路。

一、以法律法规标准规范为依据，关注一致性

2019 年国家多部门在开展针对违法违规收集使用个人信息的治理行动中，为规范个人信息的收集使用，发布了多份个人信息保护的技术文件。新版《指南》根据新发布和修订的法律法规及标准规范进行了内容增修。

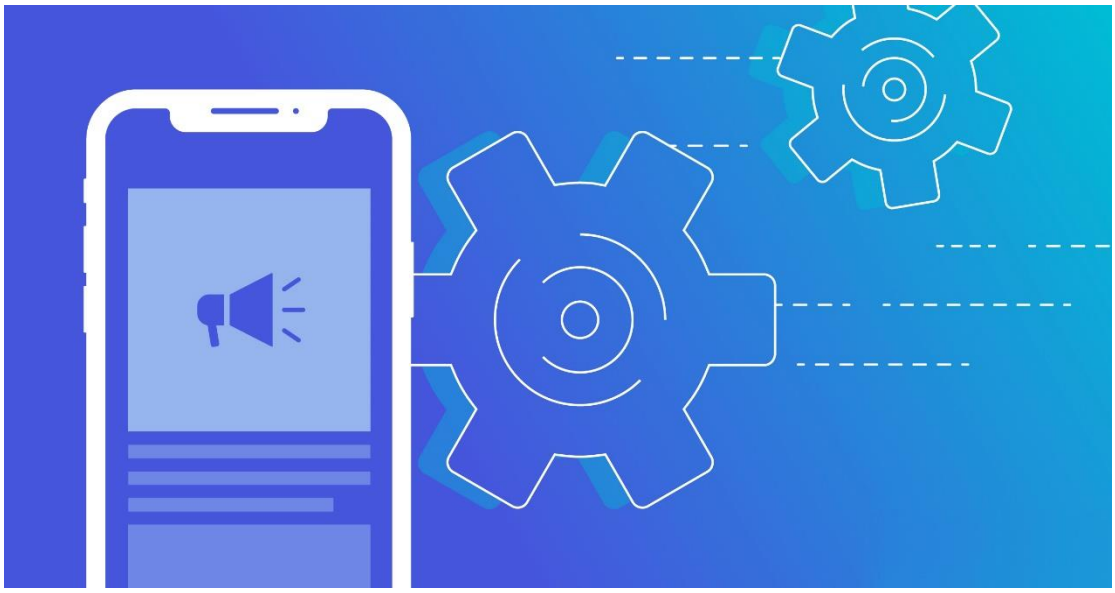
随着数字经济的发展，儿童个人信息正遭遇多种泄露风险。欧盟《通用数据保护条例》也明确提出儿童的个人数据应该受到特殊保护。我国 2019 年 8 月发布首部未成年人数据保护专门法《儿童个人信息网络保护规定》。对应其第八条“网络运营者应当设置专门的儿童个人信息保护规则和用户协议”的规定，新版《指南》对存在涉及收集使用儿童个人信息相关业务功能的 App 增加 1.1d）“制定针对儿童的个人信息保护规则”的要求。

针对 App 中嵌入的第三方应用等收集个人信息的情况，对应于《规范》9.7 中增加的第三方接入管理要求，评估点五将向他人提供个人信息情形细分为 App 直接向第三方发送、后台向第三方发送和接入的第三方应用收集个人信息几种方式，明确 App 运营者需向用户明示产品或服务嵌入的第三方应用，且第三方应用收集行为需获得用户授权的要求。

对于不同文件对同一评估点存在差异的情形，新版《指南》有针对性地提出了自评估建议。如 4.3c）对非正当方式强迫收集用户个人信息的场景中结合《认定》方法第四类行为第五款中“定向推送信息”和《规范》5.3f）中“增强安全性”的要求，建议此二场景下均不强制要求用户同意收集个人信息；再如对于上述两个文件对响应用户查询、更正、删除个人信息和受理用户个人信息安全投诉、举报时限不一致，6.2b）、6.3b）采用了《认定方法》的要求，即响应和处理的时限不得超过 15 个工作日。可见在《规范》提出的个人信息保护基线要求之上，App 作为更加注重与用户交互的服务方式，适合进一步选择更加有利于用户体验的响应机制。

此外，新版《指南》直接引用《规范》中相关要求作为参考，既避免重复又将二者紧密的结合起来。6.1c）中删除“提供额外的个人敏感信息用于身份验证注销过程”为不合理注销账号条件的描述，既是对《规范》的 8.5 c）、e）关于注销身份核验时收集个人信息条件的

呼应，也体现了对于注销账户这类对用户权益影响较大的操作，在要求企业满足用户行使个人信息权利的同时考虑到企业为保障用户权益、避免纠纷等合理诉求的编制思路。



二、引入标注举例，加深运营者对本质要求的理解

《指南》的可以看做是细化和解读法律法规和标准规范的要求，以供 App 运营者自评估参考使用。此版本重点对之前版本添加了扩展说明，同时以“注”的方式引入运营者在个人信息保护上的最佳实践及 App 典型违规应用场景描述，增加了《指南》的实用性。

对需在“常规交互界面”展示隐私政策链接的要求，存在范围不明容易引起歧义的问题，新版《指南》1.3b）将“常规交互界面”改为“固定路径”，并注明固定路径即是指“我--设置--关于”或者“我的--设置--隐私”等用户熟悉的页面跳转路径，精确表达了隐私政策易于查找的含义。

2019 年专项治理工作中发现多款 App 有“频繁征求用户同意、干扰用户正常使用”的违规行为，运营者常常困惑于如何理解此要求的具体频次和应用场景，新版《指南》3.3 a）、b）描述了 App 频繁征求用户意见的具体表现，同时通过标注举例说明“为支持 App 正常运行”等情形下，用户主动选择使用的某一具体功能触发征得同意的动作，不属于频繁干扰行为。

为进一步明确收集个人信息前告知同意的合规要求，在 3.1b）注中增加“用户作出同意前”这一场景描述，更准确地阐释了《认定方法》第三类行为第一款的含义，即 App 收集个人信息的前提不仅需要履行目的告知的义务，还要征得用户授权同意。此外鉴于 App 频繁更新的现状，新版《指南》通过 3.5 b）注的补充说明，App 更新时在何种情况下无需再次征求用户同意，揭示了个人信息保护的实质应真正从用户角度出发，做到应披露尽披露，该简

单就简单，不搞形式主义，不做无用功。

三、调整评估点，突出个人信息保护和良好用户体验相结合

除新增评估点和引用实例外，新版《指南》还对部分评估点的要求和实例进行调整，一方面回应了用户诉求，兼顾使用的便利性，另一方面关注产业发展，增强了企业实践的可操作性。

《网络安全法》第四十一条确定了网络运营者有“公开收集、使用规则”的义务，但未对具体的形式和要求作出规定，因此独立的隐私政策是否为合规化的必然要求，一直为业界争论的焦点，也受到运营者广泛的关注。1.3c)将原来“隐私政策以单独成文的形式发布”的要求，调整为“如果因展示条件等特殊原因使用用户协议、用户须知等文件描述个人信息收集使用规则，则尽可能显著标识并以连续篇幅呈现”，即隐私政策是否单独制定发布可由运营者根据实际情况来决定。这一要求的弱化，增强了用户个性化展示隐私政策的自由度，回应了用户因文本协议过多带来的不良用户体验的诉求。

为确保运营者实践的可操作性和指南的普适性，6.2d)不再强调“同步”响应用户更正删除个人信息，而用后台“及时”执行操作即可。这种细节的修订既结合产业现状，降低了技术难度，又从实践角度提出了保障用户权益可行要求；同时 3.1a）要求在收集个人信息前提供同意不同意选项时，以“自主作出”代替“主动选择”的用户授权行为描述，使得 App 在具体设置相应功能时有更多的灵活度和创新空间，提升了用户的使用体验。

四、回应媒体热议，以问题为导向，向运营者提出建议

个人信息安全相关事件频发，受到媒体和公众强烈关注，监管部门高度重视。App 专项治理工作着重要解决广大网民反应强烈的违法违规使用个人信息的问题，新版《指南》在分析媒体热议问题违规行为本质基础上，对应《认定方法》六类行为提出评估点，为运营者收集使用个人信息合规化提出更全面的建议。针对近期媒体热议，用户关注的 App 自启动和高频次访问用户通讯录、相册等问题，4.4b）中明确在用户主动关闭 App 后，未经用户同意不采用自启动、关联启动方式收集个人信息。这一补充，相较之前 App 专项治理工作组通报的“收集用户个人信息的频度超出业务功能实际需要”问题上更进一步明确了超出合理频率收集个人信息的典型场景；同时，2019 年 3·15 晚会上曝光的某款 App 私自截留用户个人信息的典型违规行为吸纳到 4.4c）中。

新版《指南》体现了法律法规、标准规范对收集使用个人信息的新要求，与《认定方法》文件进行了严格对照统一，将为推动 App 违法违规使用个人信息行为的相关认定标准渐趋一致提供参考。同时，引入典型案例，深入浅出说明个人信息保护的关键点，对出现的新问

题及时地作出回应，结合产业实践和用户诉求提出了建议。总的来看，作为《认定方法》的细化解读，新版《指南》紧密围绕当下 App 个人信息保护领域各方最迫切的需求，将为 App 运营者落实《网络安全法》等法律法规中关于个人信息保护的要求提供进一步的思路和参考。

（来源：中国网络安全审查技术与认证中心）

- **《移动互联网应用程序（App）收集使用个人信息自评估指南》2.0**
- **阅读全文：**https://www.tc260.org.cn/upload/2020-07-22/1595396892533085831.pdf

➢ 做好“新安全” 保障“新基建”

2020 年无疑是“新基建”的元年，3 月 4 日中央政治局常务委员会会议提出“要加快 5G 网络、数据中心等新型基础设施建设进度”，“新基建”犹如一夜春风，席卷了神州大地，各行各业都围绕“新基建”战略，紧锣密鼓地进行布局。

但“新基建”的概念的提出不止于此时，2018 年 12 月 19 日，中央经济工作会议就首次提出“新型基础设施建设”的概念，强调加快发展“5G 商用步伐、推动发展人工智能、工业互联网、物联网等”。近两年来，国家不断出台相关产业政策，“新基建”战略日渐完善，在今年经济受到疫情影响，亟待复苏的背景下，“新基建”的崛起，已然成为让国民经济重新风驰电掣的新动能。

“新基建”的“新”在何处？

与以往的传统基础设施建设相比，“新基建”最大的“新”，是我国为促进信息化社会进

一步发展升级的数字化全面转型，是我国基础设施建设从现实空间拓展到虚拟空间的重大升维。2020 年 2 月 14 日，中央全面深化改革委员会第十二次会议上指出了“新基建”与传统基建的相互关系：“基础设施是经济社会发展的重要支撑，要以整体优化、协同融合为导向，统筹存量和增量、传统和新型基础设施发展，打造集约高效、经济适用、智能绿色、安全可靠的现代化基础设施体系”。

3 月 4 日的中央政治局常务委员会会议，则是给“新基建”的发展划出了重点部分，紧接着，2020 年 4 月 1 日，习近平总书记在浙江考察时强调：“要抓住产业数字化、数字产业化赋予的机遇，加快 5G 网络、数据中心等新型基础设施建设，抓紧布局数字经济、生命健康、新材料等战略性新兴产业、未来产业，大力推进科技创新，着力壮大新增长点、形成发展新动能。”深刻地阐明了“新基建”和数字经济相互促进、共同发展的紧密关系。

2020 年 4 月 20 日，对于“新基建”究竟包含哪些领域，国家发改委给出了权威说法。新型基础设施主要包括三大板块：一是信息基础设施，包括以 5G、物联网、工业互联网、卫星互联网为代表的通信网络基础设施，以人工智能、云计算、区块链等为代表的新技术基础设施，以数据中心、智能计算中心为代表的算力基础设施等。二是融合基础设施，主要指深度应用互联网、大数据、人工智能等技术，支撑传统基础设施转型升级，进而形成的融合基础设施，例如智能交通基础设施、智慧能源基础设施等。三是创新基础设施。主要指支撑科学研究、技术开发、产品研制的具有公益属性的基础设施，例如重大科技基础设施、科教基础设施、产业技术创新基础设施等。

显然，经过这两年的完善，国家对数字经济的发展战略日益清晰，相比传统基建，“新基建”的关键路径是数字化、信息网络、科技创新，这些都和信息化建设密切相关。习近平总书记早就指出：“网络安全和信息化是一体之两翼、驱动之双轮,必须统一谋划、统一部署、统一推进、统一实施。”发展“新基建”，做好网络安全工作至关重要。

发展“新基建”，安全要同步

“新基建”会带来哪些新的安全风险？纵观“新基建”的主要领域，其中不仅有已经发展得如火如荼的新技术，如云计算、物联网、大数据，有升级换代、迈入更广阔应用场景的新型技术，如 5G、工业互联网、区块链、人工智能，还有如卫星互联网、量子通信等最前沿科技。这些技术推动了大量新业务新场景的诞生，也给网络安全带来了新的挑战。可以预见的是，随着“新基建”的深入推进，会有更多的漏洞、更模糊的网络边界、更广的攻击层面、更新的攻击性手段，安全的形势只会越来越严峻，攻防博弈只会越来越激烈。

在今年的“两会”上，代表委员们的提案建言都已经开始关注到“新基建”下的安全挑

战，指出要把握“新基建”发展机遇，但同时必须做好相应的安全保障工作。中国工程院院士倪光南强调，“新基建”一开始就要考虑跟网信相关，采用我国安全可控的信息技术体系，保证基础设施的安全。全国政协常委、民建中央副主席周汉民建议，要把在不同领域、不同行业领先的安全能力变成国家网络安全能力体系的重要组成部分，提高各行各业的“安全基建”能力。全国政协委员、中国科学院信息工程研究所所长孟丹和全国政协委员、安天首席架构师肖新光有着共同的观点，认为数字基建在建设伊始就要考虑安全体系的同步构建，从被动防控向主动防御转变，新型基础设施的网络安全必须同步规划、同步建设、同步运维，实现全生命周期安全。全国政协委员、360 集团董事长兼 CEO 周鸿祎则建议，运用整体思维，规划“新基建”网络安全防护体系顶层设计，同步建设“新基建”的安全基础设施如网络安全大脑，守好“新基建”的每一块砖。还有代表委员建议参照疫情防控经验，构建网络安全应急响应体系，做好“新基建”下安全体系的未雨绸缪工作。

早在 2018 年的全国网络安全和信息化工作会议上，习近平总书记就明确指出要构建“关口前移，防患于未然”的网络安全管理体系。所以，“新基建”网络安全体系的建设，必须严格落实关口前移、同步推进的思想，不能再做“亡羊补牢”的事后工作，不能再将安全作为信息化一个可有可无的部分，而是要牢牢把握“新基建”的发展脉搏，将安全作为“新基建”的一个重要基因，提前做好安全规划，同步推进安全体系建设，真正发挥网络安全的作用和价值，护航“新基建”健康发展。

借力“新基建” 发展“新安全”

“新基建”涉及大量新技术和新场景，这不仅给网络安全带来全新的挑战，也给网络安全产业带来了一个前所未有的发展契机，传统的网络安全也将面临深刻变革，走向“新安全”时代。

“新安全”，一方面指围绕诸多新技术领域所带来的新场景新业务，会催生更多更丰富的安全需求，推动网络安全技术创新，给产业发展注入新的活力。另一方面，网络安全本身也受益于新技术的发展，云计算、大数据、人工智能、区块链、量子通信等技术已经广泛应用于网络安全领域，与传统网络安全技术融合应用，使得网络安全更加智能和高效，推动我国网络安全保障能力和水平迈向新的高度。所以，“新基建”不仅是各行各业的信息网络基建和数字基建，也是网络安全和各行各业全面融合应用的“新安全”基建。安全业界应充分做好准备，提升自身关键技术能力，加强产业生态协同，加快专业人才培养，尽早对“新基建”进行布局。

“新基建”的号角已经吹响，2020 年开年以来，北京、广东、吉林、湖南等 25 个省市

的政府工作报告提及“新基建”。据媒体不完全统计，截至 2020 年 4 月中旬，全国已有 13 个省区市发布了 2020 年“新基建”相关重点项目投资计划，其中 8 个省份的计划总投资额近 34 万亿元。从中央到各地，对“新基建”的政策和资金利好不断，以工信部、交通运输部、科技部为代表的部委，相继发布相关产业政策，大力推动“新基建”的发展。

要确保数字经济行稳致远，安全须成为“新基建”的基建。为此，我们要加快完善相关法规和标准，为“新基建”的网络安全建设夯实根基、明确规范；要加强对“新基建”各领域的研究，为网络安全体系建设提供参考；更要将安全意识融入“新基建”的各行各业，做到安全和发展同步，切实保障我国信息化发展和数字化转型的顺利推进。（来源：《中国信息安全》杂志 2020 年第 7 期）

➢ 网络安全视野下金融业数字化转型的机遇和挑战

在今日中国，随着以云计算、区块链、5G 以及人工智能等为代表的新一代信息技术的普及应用，人际社交、社会治理乃至经济商业等都呈现快速数字化转型的态势。金融机构也已纷纷升级各自科技能力和技术储备布局线上，广泛应用各类新型金融科技赋能数字化转型，寻求在全球数字化浪潮之中及时实现与实体经济的深度融合，促进数字经济场景中业务模式与业务水平的升级蝶变。

着眼监管的维度，金融业数字化转型可能伴生各种涉及技术元素、业务组织以及数据信息等多方面的安全新风险，对相关的制度安排设计、风险管理防范以及监管执法机制等也提出了更高的要求。与此同时，中国的监管机关也正加快数字化步伐，适应行业转型节律，强

调鼓励和规范、引导创新，从政策战略、法律规范以及其他规则等多个层次及时介入和适时革新金融业数字化转型过程中的网络安全治理。

（一）金融业数字化转型的机遇和挑战：网络安全维度的分析

在当下的中国市场，一方面，新一代信息技术普及并逐步走上大规模商用的快车道，从而引领并驱动金融业的供给样态、金融市场的运行架构的升级与创新；另一方面，金融业通过充分挖掘新一代信息技术的价值潜力能更好地实现智能化决策支撑、自动化业务流程、动态化风险管理以及精准化资源配置，进而提高金融业相对实体经济繁荣需求的业务弹性与适应水平，使得数字化金融重在服务和满足实体经济之发展以及普惠金融需要。

这使得目前数字化金融业呈现出专业化和精细化分工的特点，各利益相关方立足自身寻找市场定位和比较优势。其产业链和价值链的持续延申也逐渐形成竞争、互补和包容的生态社群，在这一过程中生成的机遇和挑战形成了广泛的转型期网络安全关切。

1.1 金融业数字化转型与技术要素层面的网络安全关切

金融业关键信息基础设施是各类金融机构广泛链接的基础介质，也是防范各类风险交叉渗透的第一道防火墙。各类金融业务数字化转型以实现数字化、线上化操作流程和服务提供的过程中，与之伴生的是确保支付清算、信用信息共享、身份认证等关键信息基础设施的良性运行，其安全性、高效性和可控性具有根本性意义。着眼技术要素安全的维度，金融业数字化转型与关键信息基础设施安全有着紧密的基础-条件关系。

今年来孟加拉银行失窃事件、汇丰银行信息泄露事件到俄罗斯央行基金损失案件等无不体现了金融业数字化转型中错综复杂的安全形势和泛在的安全关切。侵害金融关键基础设施的各类攻击已成为关键基础设施的重要风险。

于此，中国人民银行、发展和改革委员会等六部门于 2020 年 3 月份联合印发《统筹监管金融基础设施工作方案》（以下简称：《方案》），进一步加强对我国金融基础设施的统筹监管与建设规划，以适应金融科技等新技术新应用兴起所带来的诸多新变化，为数字化金融的未来发展打造有效、合理和规范的制度环境。

《方案》首先指出，中国已逐步形成货币、证券等各类较为齐全、整体稳定的提供金融市场交易活动支持的基础设施体系。但仍应在法制建设、管理统筹、规划建设等方面加强建设，提高其效率，进一步加强对中国金融基础设施的统筹监管与建设。

其次，《方案》指出，加强金融基础设施建设，统筹监管重要金融基础设施，提高服务实体经济水平和防控金融风险能力是核心指向。金融基础设施是金融市场稳健高效运行的基础性保障，也是实施宏观审慎管理和风险防控的重要抓手，具有枢纽意义。对此，《方案》

明确划定金融基础设施统筹监管范围包括金融资产登记托管系统等六类设施及其运营机构。并要求中国人民银行与各部门、地方密切配合，统一监管标准，健全准入管理，优化设施布局，健全治理结构，推动形成布局合理、治理有效、先进可靠、富有弹性的金融基础设施体系。

1.2 金融业数字化转型与组织管理层面的网络安全关切

面对开放、互动和全连接的数字化金融场景，各类业务、技术、网络与数据等多重风险因素的叠加效应日趋放大。在该语境下的金融业数字化转型应革新和重构包括法律约束、行政监管、行业自律、机构内控、社会监督在内的全社会相关方参与的多层次治理体系，以实现风险的全覆盖动态防控。作为转型过程的重要驱动力和关键支撑，金融科技安全水平与之密不可分。

因此，中国人民银行于 2019 年发布了《金融科技发展规划（2019-2021 年）》(以下简称《规划》)，旨在引导金融业秉持守正创新、安全可控、普惠民生、开放共赢的原则，推动金融和科技深度融合协调发展，为商业银行的数字化转型指明方向。并积极探索构建监管科技的应用框架，建立健全金融科技监管基本规则体系，打造中国版的监管沙箱，为数字化转型营造良好的正环境。

具言之，《规划》强调了金融科技的多重积极价值，指出金融科技正成为推动金融转型升级的新引擎、金融服务实体经济的新途径、促进普惠金融发展的新机遇和防范化解金融风险的新利器。

第二，《规划》为金融科技的发展和监管指明目标：应实现金融科技应用的先进可控、增强金融服务能力、提高金融风控水平、提升金融监管效能和合规水平、完善金融科技的支撑作用并推动金融科技产业繁荣发展。

第三，《规划》还明确了金融科技研发应用和安全保障的各项重点任务：其一，要加强金融科技战略部署，加大科技投入，重塑其业务价值链，补齐传统短板。加强体制结构优化，打破部门间的壁垒，提高跨部门协同能力，并利用人才需求目录、人才激励计划等加强人才队伍建设；其二，要强化金融科技的合理应用，如整合各行业各部门的金融大数据、布局并搭建云计算平台、稳步应用算法模型等人工智能技术、加强分布式数据库的规划与研发应用、健全网络身份认证体系等；其三，要为金融服务提质增效，进言之：拓宽金融服务渠道，形成线上下一体的服务方案、利用自然语言处理技术等人工智能实现产品需求分析研发、利用新技术提升网点效率、突破金融服务“最后一公里”限制，为贫困边区提供专业有特色的服务、优化针对小微企业等重点领域企业的信贷流程和评价模型，优化其信贷融资服务，还应

利用移动支付技术实现金融账户统一标记、手机客户端软件规范接口、交易集中路由；其四，增强金融风险技防，加强金融网络安全和应用风险的统筹管控并加大金融信息保护力度；其五，审慎监管力度，建立金融科技监管基本规则体系、加强监管各行业部门协调、提升监管的穿透能力，利用自动化技术采集数据并实时分析，并建立健全创新管理机制实现公开、共同监督的柔性监管方式。还应强调夯实金融科技支撑这一重点任务，要加强金融科技联合攻关、推动法律法规建设、增强和完善信用服务体系、完善行业工作标准并强化金融消费者权益保护。

最后，《规划》明确要以加强组织统筹、加大政策支持、完善金融科技示范区等配套服务、利用“一带一路”倡议，输出和引进金融科技强化国际交流并贯彻好宣传任务的形式保障金融科技的发展。

1.3 金融业数字化转型与数据信息层面的网络安全关切

数据作为一种国家基础性战略资源，对其的充分挖掘是数字化金融领域研发应用各类新型信息技术的物质条件与重要保障。金融业数字化转型离不开数据安全工作的保障以及对消费者数据权益的保护。

个人金融信息一旦遭到泄露，既侵害个人金融信息主体之权益，又影响金融机构的运营，甚至还可能造成系统性金融风险。立足提升金融数据信息安全的维度，2020 年中国人民银行正式发布由多家单位负责与起草的《个人金融信息保护技术规范》（JR/T 0171—2020）（以下简称“《规范》”），完善了相关制度建设。

首先，《规范》相较之于 2011 年中国人民银行发布的《关于银行业金融机构做好个人金融信息保护工作的通知》所定义的个人金融信息（个人身份信息、个人财产信息、个人账户信息、个人信用信息、个人金融交易信息、衍生信息等），采用了一种更广泛的定义，增加了鉴别信息（包括但不限于银行卡密码、预付卡支付密码、 动态口令、短信验证码等）与个人生物识别信息（指纹、人脸、虹膜等）。并根据信息遭到未经授权的查看或未经授权的变更后所产生的影响和危害，将个人金融信息按敏感程度从高到低分为 C3、C2、C1 三个类别，并依据此分类实施针对性的保护措施。

其次，《规范》就个人金融信息提出了基于收集、传输、存储、使用、删除和销毁等各个环节的生命周期技术要求，以及从网络安全、Web 应用安全、客户端应用软件安全、密码技术与密码产品等四个方面提出了与个人金融信息相关的安全运行技术要求。

最后，《规范》从安全准则、安全策略、访问控制、安全监控和风险评估、安全事件处置五方面进行了安全管理要求。点包括对个人金融信息收集、存储、使用的安全管理要求，

对个人金融信息安全管理的制度、组织、人员、访问控制、安全事件的安全管理要求。

（二）金融业数字化转型的安全保障：从云计算到人工智能

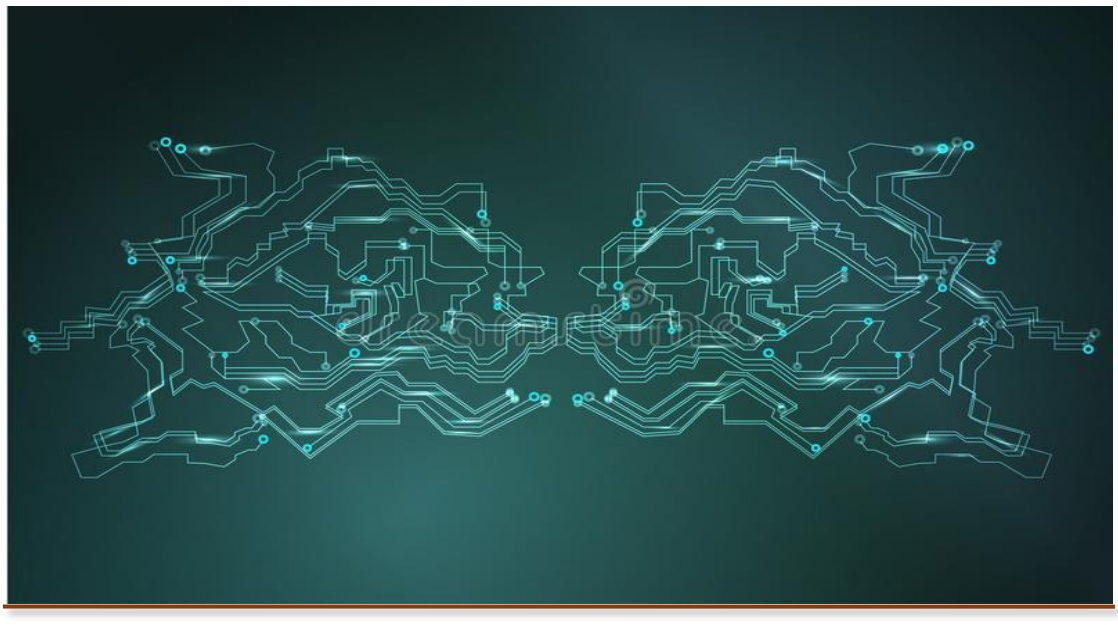
2.1 金融业数字化转型安全保障的域外路径：最佳实践

目前在金融业全行业数字化转型过程中的安全保障方面，从银行、证券到保险等资本市场等各个生态，各市场利益相关方之间有着广泛且密切的互动合作关系。龙头网络科技企业凭借自身在云计算、人工智能、大数据等先进数字化技术领域的智力积累和业务积累，以创新数字化技术为价值驱动，积极参与服务实体经济的金融科技创新，与各大金融机构在智能金融、场景金融和开放数字金融生态等领域深度交互，形成了面向云与智能转型的安全保障最佳实践，具有显著的参考借鉴意义，举例如下：

在云计算方面，瑞士银行通过云计算领域的全面推广合作，在过去几年逐步将风险管理、数据分析与业务应用等关键系统迁移到云平台，基于该云平台云提供的高性能计算平台支撑日均百万次的风险模型计算，成本节约 40%，也使员工的客户对象决策更为快捷。类似的实践还由汇丰银行、伯克希尔哈撒韦公司等实现。

在区块链方面，摩根大通基于网络科技公司的云服务为基于以太坊的区块链平台 Quorum 提供支撑，构建符合监管的摩根币体系。同时基于网络科技公司的云服务组件提供区块链节点监控以及分析能力，实现的低成本、简化的部署和内置的治理。

在云平台方面，友邦公司将原有多个数据库应用及 Web 前端应用迁移到了云环境中，实现弹性业务和成本缩减，同时也确保了容灾备份与关键数据保护等安全架构。还为两万名员工提供了 SaaS 化协同办公平台环境，提升远程会议、移动办公、安全合规的商业内容分享等，确保符合金融监管合规要求。



2.2 金融业数字化转型安全保障的域外路径：监管态势

（1）美国

美国作为金融科技的领先者，其规制模式具有前瞻性，形成了相对严密的监管制度和监管逻辑。在鼓励金融科技创新方面，2017 年美国国家经济委员会发布了《金融科技监管框架》白皮书，全面系统地阐述了金融科技政策设计和监管策略的政策目标和基本原则，并提出六大政策目标。在健全金融法律监管体系和建设完善征信系统方面，美国通过立法和市场竞争的方式实现金融数字化转型的制度建设，如美国国会通过的旨在详细规定征信机构权责的《公平信用报告法》，以及通过竞争形成的法治征信市场。

美国在金融科技监管的顶层设计方面追求统一协调，以避免监管套利、竞次和真空等问题。如《金融科技法案 2019》要求在美国财政部内设“金融科技委员会”，明确每个联邦金融监管机构应设立金融创新办公室等，以形成全国统一的监管体系。

在包容式监管方面，美国倾向于使用“监管沙箱”机制，即允许初创型金融科技公司在享受一定豁免权的、受限但安全的环境中从事科技创新试验。同时美国也注重对新现象的立法与监管，如可能被用于洗钱、非法融资等目的的虚拟货币。美国国会议员先后提交《虚拟货币恐怖主义用途国土安全评估法案》和《金融科技保护法案》，强调优先调查并打击恐怖分子非法使用包括虚拟货币在内的新型金融技术。

（2）欧盟

欧盟在鼓励金融科技创新、推动金融科技和银行业协作、控制风险等方面不断推陈出新，形成了一系列较为成功的科技监管举措。为进一步统筹欧洲对金融科技活动的监管，欧盟委员会于 2016 年成立了金融技术工作组。并于同年，以最基础的支付业作为突破口，通过 PSD2（Payment Service Directive 2）法令推行“开放银行业”计划，规定欧盟所有的银行必须将相关的客户数据和支付服务对第三方服务商进行开放。

其次，欧盟对个人数据的保护也从未松懈。欧盟推出《通用数据保护条例》（GDPR），并与 PSD2 相配套，为“开放银行业”计划推进提供完善的法规体系。最后，在创新方面，欧盟鼓励和支持人工智能与金融业的融合发展，鼓励区块链创新融资方式。支持金融业为人工智能产业融资，并参与到行业发展之中的同时，也支持 ICO 项目方通过使用发售加密货币方法来筹集资金，然后再由项目方启动资金实现项目由概念设计向现实转化，实现利益公开分配和信息的公开披露。

（3）英国

有别于具有全球领先的技术（如美国）和具有庞大规模的市场（如中国）的国家，英国

金融业历史悠久，金融体系成熟繁荣，因此采取具有基于现有金融监管框架实施归口监管、行业自律先行和鼓励创新的监管模式三大特征的主动型监管模式。在四个领域上，英国的监管模式也体现出创新监管的特点：其一为监管沙盒，允许在可控的测试环境中对金融科技的新产品或新服务进行真实或虚拟测试；其二为创新中心制度，支持企业进行金融创新并辅导企业申请监管沙箱资格，支持和引导机构理解金融监管框架，识别创新中的监管、政策和法律事项；其三为创新加速器即监管部门或政府部门与业界建立合作机制，通过提供资金扶持或政策扶持等方式，加快金融科技创新的发展和运用；最后，以科技手段降低合规成本，发展监管科技。

（4）新加坡

新加坡金融管理局（MAS）作为该国的金融监管机构，为实现“激发金融创新活力”与“维护金融体系安全”的双重目标，对金融科技采取了一系列富有创新性的监管举措。

第一，在其内部设立了一个金融技术和创新小组（FTIG）作为专门机构负责制定与金融创新相关的监管政策和发展战略。第二，与国内外银行和其他政府机构合作，为金融服务开发行业客户身份识别应用程序。第三，与新加坡金融科技行业合作开展“概念验证”项目（Ubin），旨在探索分布式分类账技术在支付和证券结算及交收中的运用，并将探索跨境的货银对付和同步交收机制。第四，与新加坡金融行业联合制定并发布了 《新加坡金融业使用人工智能和数据分析“促进公平、道德、负责任和透明”的原则》，规定企业在评估现有的内部框架或者开发新的内部框架时应当遵守的原则，用以规范人工智能和数据分析在金融业的使用。第五，通过金融业科技与创新“概念验证”等计划向新加坡金融机构以及与其合作的技术或解决方案供应商，提供资金支持。最后，新加坡在金融科技监管上还积极寻求与其他国家和地区的合作，如与东盟银行家协会、世界银行、国际金融公司成立东盟金融创新网络。

2.3 金融业数字化转型安全保障的中国路径：实务探索

从目前的最佳实践来看，中国的数字化转型安全保障问题最突出的方向，是构建多方共治机制就重点领域和重点问题实现从传统型“管理”到生态型“治理”的模式转变。如何引导银行金融业发展数据查询和存储之外的功效，并提高数据的保护质量是引导银行金融机构转型的重要抓手。

中国银行保险监督管理委员会于 2018 年 5 月 1 日印发《银行业金融机构数据治理指引》(以下简称《指引》)，开启公私合作数据治理的实务探索。《指引》的总则部分提出了银行业金融机构数据治理的总体要求，要求其治理遵循全覆盖原则、匹配性原则、持续性原则以及

有效性四个原则开展治理。

在数据治理架构方面，《指引》要求建立起组织健全（将数据治理职责上升到董事会，且董事会对数据治理承担最终责任）、职责边界清晰明确的数据治理体系，同时应当建立良好的数据文化。本章第十一条还特别引入了首席数据官的规定，廓清权限。

在数据管理部分，《指引》明确银行业金融机构应结合自身发展需要，制定相应的数据战略和数据管理制度，并有效地执行和修订更新。同时，要依法依规采集、保护客户个人信息安全、划分数据安全等级、完善数据安全技术并定期审计数据安全。此外，银行还应建立数据应急预案和问责机制。

对于数据质量控制的问题，《指引》要求金融机构建立数据质量控制机制、数据质量监控体系、数据质量现场检查等制度，加强数据源头管理。

《指引》还强调数据价值实现中风险控制的重要性，银行业金融机构应当在业务经营、风险管理和内部控制的全流程加强数据应用，以数据为驱动力促进银行业金融机构的健康发展。《指引》最后指出，要通过非现场监管和现场检查两种方式进行持续监管，加强监督管理机制，提升监管水平。

2.4 金融业数字化转型安全保障的中国路径：监管态势

在目前经济下行压力和各种不确定条件下，理解市场心态、把握保增长与防风险的有效平衡、提高金融监管与金融机构治理机制的有效性、确保风险应对要走在市场曲线前面，是重要的内在逻辑与核心指向，包含以下重点工作部署：

其一，强调稳健的货币政策更加灵活适度。其二，要求金融服务实体经济，深化供给侧改革。其三，“建制度、不干预、零容忍”，加快发展资本市场。其四，深化改革开放，将坚定不移深化改革、扩大开放，加快出台和落实金融改革开放举措，保护在华外资企业合法权益。

在此基础上，2020 年颁布的《网络安全审查办法》（以下简称：《办法》）具有重要意义，是相关企业准备贯彻落实工作的逻辑起点。关键信息基础设施运营者的核心网络设备、高性能计算机和服务器、大容量存储设备、大型数据库和应用软件等产品和服务应注意该《办法》所设定的权责：第一，作为关键信息基础设施运营者的企业需要建立采购业务安全风险预判机制，实现安全关口前移，在关键信息基础设施保护工作部门指导下通力合作、强化风险识别与其他能力建设；第二，作为关键信息基础设施运营者的企业在设计采购业务安全风险预判清单、采用各种辅助研判工具时需要重点考虑《办法》提示的主要国家安全风险因素；第三，作为关键信息基础设施运营者的企业需要立足商业生态以及业务场景等自身条件建立覆

盖网络产品和服务采购全流程的供应商协议管理机制。

《办法》秉持坚持防范网络安全风险与促进先进技术应用相结合、过程公正透明与知识产权保护相结合、事前审查与持续监管相结合、企业承诺与社会监督相结合的原则，赋予关键信息基础设施运营者新的安全担当，也为其合理配置了全面的权益保障与责任机制：一方面，《办法》明确规定了网络安全审查程序包括特别审查程序各自的时限要求，作为关键信息基础设施运营者的企业可以据此合理安排自身的业务流程；另一方面，作为关键信息基础设施运营者的企业应当重视《办法》，对违反网络安全审查制度的法律责任应援引《网络安全法》第六十五条规定确立的双罚责任机制。

（三）金融业数字化转型的合规风控路径：谋求全球竞争力的选择

3.1 金融业数字化转型的风控合规：从风险管理到“安全设计”

金融业数字化转型的事实决定了在此形势下需要顺势革新监管执法与合规风控理念，推动从传统的风险管理模式过渡到更注重安全关口前移和全流程风险动态治理的“安全设计”逻辑，强调通过各类数字技术的创新应用融入金融产品和服务的研发及运营全生命周期，并以此满足金融业数字化转型过程中的网络安全需求并实现各项金融监管要求在业务操作层面的全面内嵌。如何包容鼓励技术创新，并引导和提升监管质量亦具有重大意义。

2019 年，中国人民银行发布《中国人民银行启动金融科技创新监管试点工作》，在北京市率先开展金融科技创新监管试点，探索设计包容审慎、富有弹性的创新试错容错机制，划定刚性底线、设置柔性边界、预留充足发展空间，开启了中国版“监管沙盒”的新阶段。2020 年，中国人民银行发布《关于开展金融科技应用风险专项摸排工作的通知》，并组织开展金融科技应用风险专项摸排工作，以贯彻同年人民银行工作会议精神，落实《金融科技发展规划（2019-2021 年）》，加强金融科技应用风险防控，从另一侧进一步凸出了监管机关日益重视的风险关口前移、业务流程内嵌的“安全设计”理念。与此同时，北京、上海等地也在积极推进国家科技创新中心建设、金融科技创新监管工具试点等计划，从而有助于中国金融业数字化转型的加速推进以及监管合规安全理念的升级迭代、有助于提升中国金融市场和各类市场主体的全球竞争力，同时也催生更广泛包容的创新应用和监管治理新生态。

3.2 金融业数字化转型的安全保障与云计算的正向效益

金融业的数字化转型以云计算应用为强力支撑，正如中国人民银行在《中国金融业信息技术“十三五”发展规划》中明确指出的那样，要促进金融业合理利用新技术，建设云计算基础平台，在四个方面实现新技术对金融业务创新有力支撑和持续驱动：第一，为金融业转型提供跟上数字化步伐的新进安全技术保障，更新安全策略；第二，利用云计算提高大数据

处理能力，并提升系统整体的稳定与安全性，为转型提供核心系统；第三，发挥云平台资源的数据存储挖掘和安全保障优势，为数字化转型提供安全保障；第四，发挥云平台算法与计算能力的大数据预警作用，增强金融机构风险预警和控制能力，为转型提供动态风控。可以预见，未来以云计算为依托，通过金融云生态的建设，金融业必将在基础架构、运营模式、服务场景等领域创造出更优质、更便捷的金融产品和服务，驱动数字化转型向更纵深的方向拓展。

3.3 金融业数字化转型的安全保障与人工智能的正向效益

在充斥各类风险的“风险社会”中，金融行业作为巨额资金的集散中心，具有高风险这一基本属性。任何决策失误都可能导致“多米诺骨牌”效应。金融业必须引入包括人工智能技术在内的现代技术进行风险防控，并提供安全保障。

具言之，人工智能技术的安全保障正向效应体现在以下三个方面。首先，人工智能技术通过与网络信息技术、大数据系统、云存储等相结合，可以对企业的信息系统运行进行全方位监控，并有效抵挡网络攻击、维护系统稳定，实现其清查系统漏洞，维护信息系统的安全环境的效用。其次，通过算法设计与算力利用，人工智能技术能实现决策方案的自动化实现，减少了程序紊乱、系统瘫痪的可能，实现了保障程序运行，促进金融业务的高效运转的特质。最后，面对金融业务的复杂性，以及伴生的多元风险，金融业务的运转往往面临复杂的法律合规问题。传统顾问模式已经难以应对复杂的合规需求，应通过人工智能技术融合多方知识，构建全面可靠的合规体系纳入到数字金融业的日常运转过程中，达成最佳实践。

综上，人工智能技术的引入为解决金融业数字化转型过程中所面临的诸多困境提供了良好思路与技术支持，对今后促进数字金融的未来发展、提高安全保障水平具有不可替代的重要意义。（来源：数字经济与社会）

四、政府之声

➢ 工信部发布关于开展纵深推进 APP 侵害用户权益专项整治行动的通知

2020 年 7 月 24 日，工信部印发《关于开展纵深推进 APP 侵害用户权益专项整治行动的通知》，要求今年 8 月底前上线运行全国 APP 技术检测平台管理系统，12 月 10 日前完成覆盖 40 万款主流 APP 检测工作。据介绍，专项整治行动将督促相关企业强化 APP 个人信息保护，及时整改消除违规收集、使用用户个人信息和骚扰用户、欺骗误导用户、应用分发平台管理责任落实不到位等突出问题，净化 APP 应用空间。整治对象包括 APP 服务提供者、软件工具开发包（SDK）提供者、应用分发平台。

四类整治任务正全面展开： APP、SDK 违规处理用户个人信息；设置障碍、频繁骚扰用户；欺骗误导用户；应用分发平台责任落实不到位。

在 APP、SDK 违规处理用户个人信息方面，将重点整治 APP、SDK 未以显著方式标示且未经用户同意，将收集到的用户搜索、浏览记录、使用习惯等个人信息，用于定向推送或广告精准营销，且未提供关闭该功能选项的行为。

此前，中央网信办、工业和信息化部、公安部、国家市场监管总局四部门启动 2020 年 APP 违法违规收集使用个人信息治理工作，受理网民有效举报信息 1.2 万余条，针对 2300 余款 APP 开展深度评估、问题核查，对用户规模大、问题突出的 260 款 APP，有关部门采取了公开曝光、约谈、下架等处罚措施。

通过专项治理工作，公众常用 APP 存在的无隐私政策、捆绑授权和强制索权、超范围收集使用个人信息等典型问题得到明显改善，这些运营者履行个人信息保护责任义务的能力和水平得到有效提升。据媒体问卷调查显示，76%的网民感到 APP 个人信息收集使用问题得到

改善，APP 个人信息收集使用行为规范向好。

在设置障碍、频繁骚扰用户方面，专项行动将重点整治 APP 安装、运行和使用相关功能时，非服务所必需或无合理应用场景下，用户拒绝相关授权申请后，应用自动退出或关闭的行为。

在欺骗误导用户方面，《通知》明确将重点整治通过“偷梁换柱”“移花接木”等方式欺骗误导用户下载 APP，特别是具有分发功能的移动应用程序欺骗误导用户下载非用户所自愿下载 APP 的行为；同时，专项行动也将整治欺骗误导用户提供个人信息，重点整治非服务所必需或无合理场景，通过积分、奖励、优惠等方式欺骗误导用户提供身份证号码以及个人生物特征信息的行为。

在应用分发平台责任落实不到位方面，《通知》指出，将重点整治 APP 上架审核不严格、违法违规软件处理不及时和 APP 提供者、运营者、开发者身份信息不真实、联系方式虚假失效等问题。

《通知》表示，工信部将于即日起组织第三方检测机构对 APP、SDK 进行技术检测，对应用分发平台的主体责任落实情况进行监督检查。对第一次检查发现存在问题的企业，将责令 5 个工作日内完成整改，对整改不彻底仍然存在问题的，将采取向社会公告、组织下架、行政处罚以及将受到行政处罚的违规主体纳入电信业务经营不良名单或失信名单等措施；对在 APP 不同版本中反复出现问题的企业，将向社会公告，并依法依规开展后续处置工作。

（来源：中华人民共和国工业和信息化部）

- **工业和信息化部关于开展纵深推进 APP 侵害用户权益专项整治行动的通知 工信部信管函〔2020〕164 号全文：**
- http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757020/c8027735/content.html

➢ 国家网信办全面部署加强“自媒体”规范管理工作

2020 年 7 月 28 日，国家网信办召开专项部署会，全面部署加强“自媒体”规范管理工作，决定自 7 月 29 日起，在全国范围内开展为期 3 个月的进一步加强“自媒体”基础管理专项治理行动，夯实管理基础，促进“自媒体”健康有序发展。

国家网信办负责人表示，近年来，国家网信办会同有关部门坚持依法治网，大力开展“自媒体”专项整治行动，依法处置违法违规账号和信息，严格内容生态治理，行业生态得到初

步改善，“自媒体”乱象得到初步遏制。但“自媒体”散布虚假信息、歪曲党史国史、宣扬错误价值观、恶意营销、敲诈勒索等现象屡禁不止，公众账号信息服务质量距离广大网民期盼还有不小差距，“自媒体”平台基础管理能力亟待进一步提高。针对突出问题，必须从基础管理这一关键环节入手，坚持依法治理、标本兼治、管建并举，动员各方力量，有效根治“自媒体”领域的痼疾顽症。

国家网信办负责人强调，要抓住关键环节，狠抓任务落实，以全面排查清理问题账号为基础，以推进分级分类管理为重点，进一步压紧压实平台、用户、属地管理责任；要重点推进微信、微博等 13 家主要平台的公众账号分级分类，为“自媒体”账号的属地管理、精准管理、信用管理打下坚实基础，提升“自媒体”规范管理水平；要深入推进相关法规修订工作，重点完善“自媒体”账号内容生产和运营的行为规范，优化平台运行规则；要强化技术治网能力建设，为实施规范管理提供支撑；要建立健全正向激励机制，引导鼓励“自媒体”运营主体生产高质量信息内容；要在网络综合治理体系框架内，建立健全“自媒体”治理体系，形成多部门协调监管、社会各方共同参与的治理格局，全面推进“自媒体”依法管理、规范管理、综合治理。（来源：中国网信网）

➢ 市场监管总局关于公开征求《关于加强网络直播营销活动监管的指导意见》

2020 年 7 月 29 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，市场监管总局起草了《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（征求意见稿）》（简称《征求意见稿》），现向社会公开征求意见。

《征求意见稿》严格规范商品或服务营销。包括：不得通过网络直播销售法律、法规规定禁止生产、销售的商品或服务；不得通过网络直播销售烟草制品等法律、法规规定禁止进行商业推销、宣传的商品或服务；不得通过网络直播销售特定全营养配方食品等法律、法规、规章规定禁止进行网络交易的商品或服务。

《征求意见稿》严格规范广告审查发布。其中，不得以网络直播形式发布医疗、药品、医疗器械、农药、兽药、保健食品和特殊医学用途配方食品等法律、法规规定应当进行发布前审查的广告。

《征求意见稿》依法查处价格违法行为。其中，针对网络直播营销中价格欺诈等问题，根据《价格法》，重点查处捏造或散布涨价信息、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（征求意见稿）**
- **全文：**http://www.samr.gov.cn/hd/zjdc/202007/P020200729511007378894.doc

➢ 公安部集中打击治理电信网络诈骗犯罪取得阶段性成效

2020 年 7 月 28 日，公安部在京召开新闻发布会，通报今年以来公安机关打击治理电信网络诈骗犯罪工作有关情况。

公安部刑事侦查局局长刘忠义通报，今年以来，在党中央的坚强领导下，公安部深入贯彻落实全国打击治理电信网络新型违法犯罪工作电视电话会议精神，组织开展“云剑—2020”、“长城 2 号”、“510”等专项打击行动，坚持立足境内，集中打击高发类案，全力铲除诈骗窝点，重拳整治黑灰产业，全面加强预警防范，取得阶段性成效。上半年，全国共破获电信

网络诈骗案件 10.1 万起，抓获犯罪嫌疑人 9.2 万名，同比分别上升 73.7%、78.4%。


中华人民共和国公安部
The Ministry of Public Security of the People's Republic of China

返回首页 | 信息公开 | 办事服务 | 警民互动

公安部集中打击治理电信网络诈骗犯罪取得阶段性成效

时间：2020年07月28日　　字体：【大 中 小】 分享到：

公安部7月28日在京召开新闻发布会，通报今年以来公安机关打击治理电信网络诈骗犯罪工作有关情况。

公安部刑事侦查局局长刘忠义通报，今年以来，在党中央的坚强领导下，公安部深入贯彻落实全国打击治理电信网络新型违法犯罪工作电视电话会议精神，组织开展“云剑—2020”、“长城2号”、“510”等专项打击行动，坚持立足境内，集中打击高发类案，全力铲除诈骗窝点，重拳整治黑灰产业，全面加强预警防范，取得阶段性成效。上半年，全国共破获电信网络诈骗案件10.1万起，抓获犯罪嫌疑人9.2万名，同比分别上升73.7%、78.4%。从严从重从快打击涉疫情诈骗犯罪，共破案1.6万起，抓获犯罪嫌疑人7506名，有力服务全国疫情防控大局；集中打击网络贷款、网络刷单、杀猪盘、冒充客服等4类电信网络诈骗高发类犯罪，共捣毁窝点2460个，抓获嫌疑人1.9万名，破获案件2.3万起，高发类案得到有效遏制，网络贷款类案件占比由年初的40%下降至20%，网络刷单诈骗日均发案下降30%，杀猪盘案件造成的损失数环比下降25%，冒充客服类案件连续两个月发案环比下降；严厉打击为电信网络诈骗提供服务的黑灰产犯罪，共捣毁黑灰产犯罪窝点7200余个，查处黑灰产犯罪嫌疑人3.2万名，斩断犯罪链条，堵塞监管漏洞；对诈骗窝点集中、黑灰产泛滥、行业问题突出的重点地域实施红黄牌警告和挂牌整治制度，压实地方主体责任，铲除犯罪土壤，重点地域面貌大为改观；强化技术反制和资金拦截，累计拦截诈骗电话1.2亿

从严从重从快打击涉疫情诈骗犯罪，共破案 1.6 万起，抓获犯罪嫌疑人 7506 名，有力服务全国疫情防控大局；集中打击网络贷款、网络刷单、杀猪盘、冒充客服等 4 类电信网络诈骗高发类犯罪，共捣毁窝点 2460 个，抓获嫌疑人 1.9 万名，破获案件 2.3 万起，高发类案得到有效遏制，网络贷款类案件占比由年初的 40%下降至 20%，网络刷单诈骗日均发案下降 30%，杀猪盘案件造成的损失数环比下降 25%，冒充客服类案件连续两个月发案环比下降；严厉打击为电信网络诈骗提供服务的黑灰产犯罪，共捣毁黑灰产犯罪窝点 7200 余个，查处黑灰产犯罪嫌疑人 3.2 万名，斩断犯罪链条，堵塞监管漏洞；对诈骗窝点集中、黑灰产泛滥、行业问题突出的重点地域实施红黄牌警告和挂牌整治制度，压实地方主体责任，铲除犯罪土壤，重点地域面貌大为改观；强化技术反制和资金拦截，累计拦截诈骗电话 1.2 亿个、封堵诈骗域名网址 21 万个，为群众直接避免经济损失 666 亿元；全力落实预警劝阻措施，开通 96110 反诈预警专号，进一步提高预警劝阻效率和成功率，累计防止 561 万名群众被骗；全面加强宣传防范，在全国公安机关“百万民警进千万家”活动中专题部署反诈宣传工作，将宣传的触角延伸至居委会、村委会，切实提升群众的识骗防骗能力。（来源：中华人民共和国公安部）

五、本期重要漏洞实例

➢ Microsoft Visual Studio Code ESLint Extention 命令注入漏洞

发布日期：2020-07-22
更新日期：2020-07-22
受影响系统：
Microsoft Visual Studio Code ESLint extension
描述：

CVE(CAN) ID: CVE-2020-1481
Microsoft Visual Studio Code 是美国微软（Microsoft）公司的一款开源的代码编辑器。
Microsoft Visual Studio Code ESLint Extention 中存在命令注入漏洞。攻击者可利用该漏洞在当前用户的上下文中运行任意代码。
建议：

厂商补丁：
Microsoft
目前厂商已发布升级补丁以修复漏洞，补丁获取链接：
https://portal.msrc.microsoft.com/zh-CN/security-guidance/advisory/CVE-2020-1481

➢ Cisco SD-WAN vManage Software XML 外部实体注入漏洞

发布日期：2020-07-21
更新日期：2020-07-21
受影响系统：
Cisco SD-WAN vManage Software <= 19.2.2
描述：

CVE(CAN) ID: CVE-2020-3405
Cisco SD-WAN vManage Software 是美国思科（Cisco）公司的一款用于 SD-WAN（软件定义广域网络）解决方案的管理软件。
Cisco SD-WAN vManage Software 19.2.2 及之前版本中的 Web UI 存在 XML 外部实体注入漏洞，该漏洞源于程序未能正确解析 XML 外部实体条目，远程攻击者可借助特制 XML 文件利用该漏洞在受影响的应用程序中读写文件。

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-vmanxml-Aj4GFEKd

➢ Adobe Magento php 对象注入漏洞

发布日期：2020-07-22
更新日期：2020-07-30
受影响系统：
Adobe Magento Commerce 1 <=1.14.4.5
Adobe Magento Open Source 1 <=1.9.4.5
描述：

CVE(CAN) ID: CVE-2020-9664
Adobe Magento 是美国奥多比（Adobe）公司的一套开源的 PHP 电子商务系统。该系统提供权限管理、搜索引擎和支付网关等功能。
Magento Commerce 1 1.14.4.5 及之前版本和 Magento Open Source 1 1.9.4.5 及之前版本存在 php 对象注入漏洞。攻击者可利用该漏洞导致任意代码执行。

<*来源：Luke Rodgers
链接：https://helpx.adobe.com/security/products/magento/apsb20-41.html
*>
建议：

厂商补丁：
Adobe
Adobe 已经为此发布了一个安全公告（APSB20-41）以及相应补丁：
APSB20-41：Security Updates Available for Magento
链接：https://helpx.adobe.com/security/products/magento/apsb20-41.html

➢ IBM Data Risk Manager 安全限制绕过漏洞

发布日期：2020-05-07
更新日期：2020-07-27
受影响系统：
IBM Data Risk Manger 2.0.6
IBM Data Risk Manger 2.0.5

IBM Data Risk Manger 2.0.4
IBM Data Risk Manger 2.0.3
IBM Data Risk Manger 2.0.2
IBM Data Risk Manger 2.0.1

描述：

CVE(CAN) ID: CVE-2020-4427

IBM Data Risk Manager 是美国 IBM 公司的一款数据风险管理器。该产品支持发现、分析和可视化业务风险数据等。

IBM Data Risk Manager 2.0.1、2.0.2、2.0.3、2.0.4、2.0.5 和 2.0.6 配置了 SAML 认证时存在安全限制绕过漏洞。攻击者可利用该漏洞绕过认证过程获得系统的完全管理权限。

<*来源：Pedro Ribeiro

链接：https://www.ibm.com/support/pages/node/6206875

*>

建议：

厂商补丁：

IBM

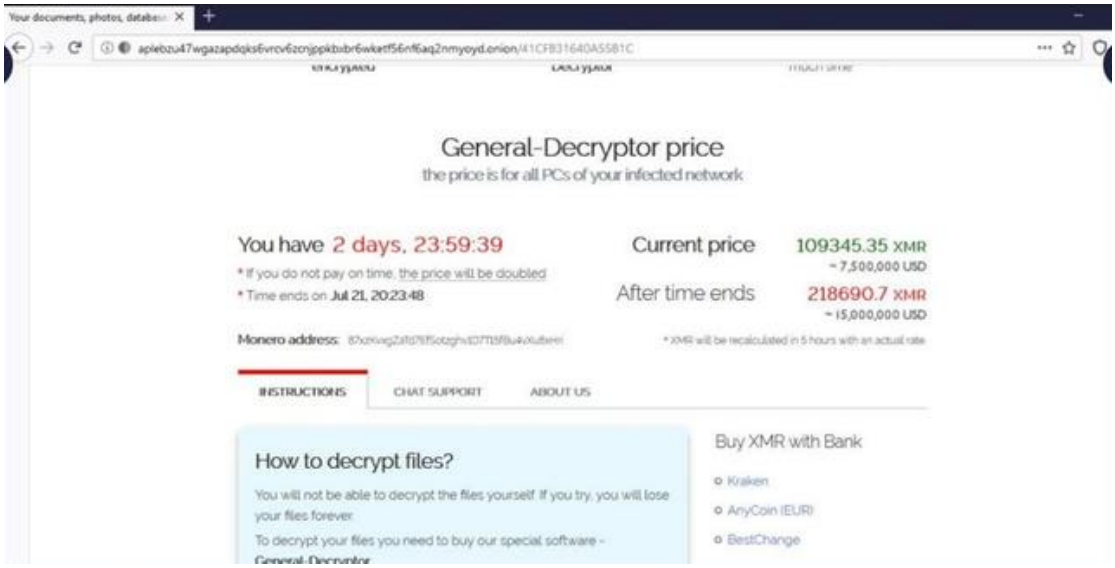
IBM 已经为此发布了一个安全公告（6206875）以及相应补丁:

链接：https://www.ibm.com/support/pages/node/6206875

六、本期网络安全事件

➢ 阿根廷电信被黑客勒索软件攻击 并要求支付 750 万美元

2020 年 7 月 22 日据报道，近日，阿根廷电信公司遭到 REVil 勒索软件攻击，短短一个周末，就造成约 1.8 万台计算机被感染。阿根廷电信是阿根廷最大的互联网服务提供商之一。上周末，某不明身份的勒索软件运营商感染了该公司约 18,000 台计算机。据了解，这次勒索方要求阿根廷电信提供 750 万美元的赎金。



本次攻击事件对阿根廷电信公司运营造成了严重影响。经过调查，本次攻击事件的原理已经明了。一开始，攻击者通过私密手段获得了对公司网络的访问权限。然后，他们控制了公司内部的 Domain Admin 系统，并使用这一访问权限感染了上万台计算机。截至目前为止，阿根廷电信运营的许多网站都因为此次勒索攻击事件而导致脱机。

幸运的是，该事件并未导致电信公司客户的连接问题。固定电话和有线电视服务也没有受到影响。阿根廷电信公司也因此提升了公司内部的网络安全防控。在公司内部的 IT 人员检测到攻击后，他们立即发布通知，警告员工不要连接公司内部 VPN 网络，并对带有存档附件的电子邮件多加注意。

REvil 勒索软件要价 750 万

德国安全研究员 Fernandez 推测，本次攻击事件，REvil 勒索软件或有参与。很快，REvil（Sodinokibi）勒索软件就在其暗网络支付门户上发布了有关阿根廷电信公司信息售卖的页面。其网站显示，若要赎回信息，需支付 109345.35 枚 Monero 代币（约 753 万美元）。截至

发稿时，勒索软件团伙并未在其暗网上将阿根廷电信列入受害者名单，信息也未曾出售。但他们威胁说，如果阿根廷电信公司在三天后不支付赎金，赎金将会翻倍。

这已经不是 REvil 勒索软件运营商将目标锁定在电信公司了。早前，REVil 运营商的惯常做法是以 Pulse Secure、Citrix VPN 和企业网关系统作为入口点，入侵企业电脑，盗取信息。今年 5 月，该组织还入侵了斯里兰卡的一家电信公司。

REvil 勒索软件平均赎金高达 26 万？

在当今的勒索软件领域，REvil（Sodinokibi）勒索软件占据着统治地位。其中，REvil（Sodinokibi）以勒索软件的形式，将其勒索软件病毒出租给其他犯罪集团。而 REvil Affaliates 则是自己寻找渠道，将勒索软件按照到目标公司，然后根据在 其企业内部网络上感染的电脑数量索要赎金。由于 REvil 公司内部这种多重角色设置，想要追踪 REvil 旗下所有的勒索软件动态非常复杂，需要大量的人力和时间。

荷兰电信服务商 KPN 的研究人员表示，根据他们的调查结果显示，今年以来，REvil 在索要的赎金总额已超过 3800 万美元，每家受感染的公司平均需支付 26 万美元的赎金。

而在针对个人和家庭用户的感染案例中，平均赎金数量为 4.8 万美元，远远高于普通勒索软件的 赎金标准。然而，如果像在西班牙电信公司这一案例中，REvil 旗下的子公司成功将其勒索软件扩展到整个公司内网时，企业需支付的赎金量就要大的多。据统计，截至目前为止，每家内网被入侵的公司平均需支付赎金 47 万美元，需要支付 100 万美元以上的企业也不计其数。（来源：SOWORD）

➢ 韩国棋手利用 AI 工具作弊 被判处有期徒刑 1 年

2020 年 7 月 20 日，自 4 年前 AlphaGo 首次登场以来，AI 第一次以作弊工具的身份出现在了围棋赛场上。据外媒消息，近日，韩国地方法院受理了一起围棋锦标赛 AI 作弊案件，相关涉事人员被判处有期徒刑 1 年。今年 1 月 14 日，在韩国围棋定段赛上，一位棋手的异样行为引起了裁判注意，随后检查发现，这名选手身上藏了无线耳机、微型相机等多个违规电子产品。

韩国棋手用 AI 作弊被判刑

原来棋手正通过这些电子产品与外界同伙沟通，试图利用 AI 作弊。其衣扣上的微型相机实时拍摄棋局信息，负责接收的同伙利用 AI 技术分析棋盘局势，并将反馈结果传递到棋

手的无线耳机中。

据了解，棋手所使用的 AI 技术正是由比利时程序员 Gian-Carlo Pascutto(GCP)开发的 AI 项目 Leela Zero，它是围棋领域为数不多的开源项目之一，所有人在 Github 上都可以下载使用。（Leela Zero 是 GCP 根据谷歌最强开源项目 Alpha Zero 扩展而来。如同 Alpha Zero 的发展路径，它不借助任何人类知识，完全从零开始训练。同时，它采用分布式计算，通过他人电脑生成的自对弈棋谱传送到服务器上进行训练，以此借助全球志愿者的力量为 Leela Zero 项目提供算力支持。）

由于裁判发现及时，棋手及同伙的作弊行为并未成功。不过，韩国棋院认为二人行为影响恶劣，触犯了“业务妨碍罪”，交由警察处理后，还委托律师拟定起诉书，对二人提起了刑事诉讼。

近日，韩国东部地方法院作出最终判决：嫌疑人 A 以职业定段为目的，与同伙 B 经过周密计划，利用智能技术违规比赛规则，严重破坏了比赛的公平、公正，性质非常恶劣。经认定，判处嫌疑人 A 一年有期徒刑，其同伙 B 一年有期徒刑，缓期一年执行，并提供 120 小时社会服务。（来源：雷锋网）

➢ 上海某“代发工资”公司账户密码是“123456”,730 万被黑客转走!

2020 年 7 月 17 日，企业付款账户直接沿用系统默认账户密码，“admin“作为账户号，密码“123456”，这样的设置在黑客看来宛若“裸奔”。近日，上海浦东新区小陆家嘴地区发生一起入侵公司网络系统实施盗窃的案件，损失高达 730 万余元。接报后，浦东警方经缜密侦查，迅速锁定嫌犯行踪，组织警力分赴全国多地开展集中收网行动，通过 72 小时连续奋战，成功抓获非法侵入受害公司网站的刘某某、龙某某、金某某等 15 名犯罪嫌疑人，冻结资金 476 万余元，缴获现金 180 万余元。

代付系统遭入侵向 7 个账户汇款

2020 年 6 月 1 日 14 时，浦东警方接到陆家嘴环路上一家公司报案称，5 月 30 日至 31 日期间，该公司自主研发的“代付系统”遭到非法入侵，并向该公司所属银行账户发出汇款指令，先后向 7 个银行账户汇款共计人民币 730 万余元。

案发后，警方高度重视，浦东公安分局反诈打击专班即会网安支队、陆家嘴公安处等相关单位成立专案组，开展案件侦查工作。初步梳理受害公司情况后，警方发现该公司虽然支付操作需与手机号绑定接收验证码，但并没有采用有字母、数字、符号相互交叉的相对复杂和难于破解的强密码，而直接沿用了系统默认的账户密码。鉴于该公司过于简陋的防护措施，警方认为极有可能是外部入侵导致该案发生。

在该公司服务器系统后台日志中，警方发现了外来入侵痕迹，通过数据梳理确认共有国内外三个 IP 地址对“代付系统”进行入侵。对方通过破译管理平台用户名及密码、下载客户数据、破解“代付系统”客户端平台、修改用于验证支付的手机号码及支付密码等操作掌控了资金流转权限，随后发送代付指令，从账户中盗走 730 万余元钱款。

从取款“卡农”深挖犯罪链条

鉴于曾有人于全国多地从收款账号内取现总计 190 余万元，警方判断涉案人员极有可能就在这些取现地点活动。之后，警方通过比对数据分析以及收款账号开户人关系网络，确

认金某某等 4 人与案件有紧密关联，是专门负责提供账户并实施转款、取现的同伙。6 月 2 日，专案组兵分 6 路赶赴全国多地，对上述人员进行侧面排摸，顺利锁定实施“黑客”入侵的龙某某以及张某、周某等负责网上洗钱的团伙成员身份判明行踪。6 月 5 日，专案组果断开展集中收网行动，先后抓获龙某某、金某某、张某、周某等 10 名犯罪嫌疑人。到案后，龙某某交代自己系无业人员，但平日喜好网络技术。5 月 31 日凌晨，龙某某在网上收到一个名叫“张飞”提供的受害公司的账号密码，便对该公司后台进行窥探并尝试上传木马病毒控制网站。在成功登陆该公司“代付系统”后，龙某某向“张飞”提供了登陆系统客户端的“后门”。

犯罪嫌疑人金某某等人交代，有一个叫做“阿强”的人联系金某某，并索要多个私人银行账号供自己使用，承诺给予一定好处。5 月 31 日，金某某在取现后，抽取 5 万余元“好处费”后，将余下的 185 万元现金藏匿等待下一步指令。而犯罪嫌疑人张某、周某则表示，按照“阿强”的指令，将收到的钱款用于购买虚拟币，并通过网络转给了“阿强”。随后警方根据掌握的信息，再一次开展大规模对比排摸，最终锁定“阿强”“张飞”及其他相关人员信息，于 6 月 19 日将主犯刘某某等 4 名犯罪嫌疑人一举擒获。14 天抓获了 15 名犯罪嫌疑人。“上海警察来得太快了，我都来不及反应。”黑客龙某某面对“神兵天降”措手不及。目前，警方已在犯罪嫌疑人金某某父亲处缴获现金 155 万元，并冻结 400 余万赃款，上述 14 人及金某某父亲共 15 名犯罪嫌疑人已被浦东警方抓获，案件正在进一步侦查中。

企业网站不报备一直在“裸奔”

反思该起黑客入侵盗窃案件，浦东公安分局网安支队中队长申屠柳焱指出，企业本身存在重大安全漏洞，并且未完成报备登记的义务。“根据法律法规，企业重要网站上线 30 内要完成报备，进行等级保护测评。”申屠柳焱介绍，而该企业为了降低转账手续费自建网站平台，还没有进行报备“体检”，公安机关无法对此进行监测。上海浦东分局网络与信息安全支队称，该公司自 2019 年五月份成立，近一年时间内几乎未购买任何网络安全保护措施。换句话说，该公司一直处于“裸奔”状态。浦东警方表示，后续将对企业自身存在的违法行为进行处罚。（来源：澎湃新闻）

➢ 佳明官方确认遭网络攻击：系统正积极恢复中用户数据未丢失或被盗用

2020 年 7 月 28 日，佳明 Garmin 官方确认，2020 年 7 月 23 日，受到了网络攻击，导

致许多在线服务受到了影响，包括网站功能、客户服务支持、终端应用程序和公司通讯等。据悉，目前暂停运作的 Garmin 系统和服务，包括 Garmin Connect 国际服务器相关服务等，已陆续恢复运行。“由于目前我们仍在处理部分数据资料，因此某些功能暂时仍然不可用。我们真诚地感谢所有用户的耐心配合与理解！”

佳明强调，目前没有任何迹象显示任何用户数据（包括 Garmin Pay 的付款资料）被非法访问、丢失或被盗用。此外，除了在线服务功能之外，Garmin 产品的功能并未受影响。受到影响的系统正在积极恢复中，我们将致力于在接下来的几天内恢复系统正常运行。官方表示，由于大量的资料正在处理中，预计全面恢复仍需一段时间。

据悉，Garmin Connect 中国大陆服务器并未受到此次事件的影响，中国大陆服务器用户仍可正常使用 Garmin Connect 的相关服务。有用户反馈，中国区用户表示一切正常，同步数据没有问题。

此前，IDC 发布的《中国可穿戴设备市场季度跟踪报告，2020 年第一季度》数据显示，中国成人手表市场前五大可穿戴设备厂商中，佳明排名第四，第一季度出货量 11 万台，市场份额 5%。前三名分别为华为、苹果、小米。

资料显示，Garmin 成立于 1989 年，注册地为瑞士沙夫豪森，研发总部位在美国。最早 Garmin 以航空 GPS 导航产品进入市场，而后在航空、航海、车用市场都有完整的产品。目前其产品覆盖航空、航海、车用、运动健身产品等市场。（来源：快科技）

➢ 化妆品巨头雅芳泄漏 1900 万条数据记录

2020 年 7 月 30 日，全球化妆品巨头雅芳（Avon）最近因云服务器配置错误泄漏了 1900

万条记录，其中包括个人信息和技术日志。

SafetyDetectives 的研究人员发现雅芳在 Azure 服务器上的 Elasticsearch 数据库公开暴露，且没有密码保护或加密。SafetyDetectives 在随后的一份报告中解释说：“该漏洞实际上意味着拥有服务器 IP 地址的任何人都可以访问公司的开放数据库。”

总部位于伦敦的雅芳公司在全球范围内的年销售额超过 55 亿美元，此次暴露的 7GB 数据于 6 月 12 日被安全公司发现之前已经暴露了 9 天。暴露的数据库包含有关客户和员工的个人身份信息（PII），包括全名、电话号码、生日、电子邮件和家庭住址以及 GPS 坐标。此外包括 40,000 多个安全令牌、OAuth 令牌、内部日志、账户设置和技术服务器信息。

根据 SafetyDetectives 的说法，虽然可以利用 PII 进行各种各样的身份欺诈和后续的网络钓鱼诈骗，但暴露的技术细节也给雅芳自身带来了风险。

“鉴于提供的敏感信息的类型和数量，黑客将能够掌握完全的服务器控制权并实施严重破坏性的行动，这些行动能永久性地损害雅芳品牌，暴露勒索软件攻击并使公司的支付基础设施瘫痪。”

有趣的是，6 月 9 日向美国证券交易委员会提交的文件显示，雅芳提及“在其信息技术环境中发生了网络事件，该事件中断了某些系统并部分影响了运营”。雅芳在 6 月 12 日的第二次申明中指出，该公司正计划重启系统。

SafetyDetectives 透露：“雅芳正在继续调查以确定事件的程度，包括潜在的泄露的个人数据。”“尽管如此，由于它的主要电子商务网站未存储该信息，因此目前尚无法预料信用卡详细信息会受到影响。”（来源：网易）

➢ 现实版谍战大戏：大众汽车特别项目组竟被窃听长达 1 年

2020 年 7 月 28 日，原本只是在电影中才能看到的“窃听”戏份，没想到却在现实中上演了。日前，据外媒报道，大众集团内部特别项目小组 Project 1 被“窃听”了 1 年，超过 50 小时的会议录音已经被泄露。目前，大众集团已经开始在内部寻找“内鬼”，调查是哪位员工在 2017-2018 年配合外人窃听集团内部的机密。

据了解，大众该特殊项目小组是为了和波斯尼亚供应商 Prevent 终止合作而建，该小组的任务是评估大众与 Prevent 终止合作的可能性和操作性。两年前，大众解除与 Prevent 的合同，并涉嫌利用反竞争策略阻止 Prevent 收购其它小型供应商。为此，Prevent 在美国提起了一项 7.5 亿美元(合 6.4 亿欧元)的损害赔偿诉讼，指控大众违反了竞争法。因此，外界纷纷猜测此次窃听事件就是 Prevent 指使的，但该公司发言人表示 Prevent 对窃听事件毫不知情。

据悉，被曝光的窃听内容显示大众集团曾与戴姆勒、宝马合作，密谋阻止 Prevent 收购零部件供应商格拉默。

不过，对于以上内容，大众集团发言人表示“并未与戴姆勒、宝马采取一致行动，也并未干预供应商之间的收购行为。”公开资料显示，Prevent 工厂主要位于德国，在下萨克森州、北莱茵-威斯特法伦州、萨克森州、萨克森-安哈尔特州、萨尔州等建有八家工厂，雇佣了多达 3,400 名员工，超过全球员工总数(30,000 人)的 10%，在过去 25 年里为大众提供座椅组装服务，为变速箱、发动机、刹车盘、座椅套供应零件。（来源：快科技）

信息安全意识产品服务

021-33663299