国盟信息安全通报

2022 年 3 月 31 日第 249 期

国盟信息安全通报

（第 249 期）

国际信息安全学习联盟

2022 年 03 月 31 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 537 个，其中高危漏洞 180 个、中危漏洞 272 个、低危漏洞 85 个。漏洞平均分值为 5.84。本周收录的漏洞中，涉及 0day 漏洞 299 个（占 56%），其中互联网上出现“Pimcore 跨站脚本漏洞（CNVD-2022-22702）、CuppaCMS SQL 注入漏洞（CNVD-2022-22322）”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 4620 个，与上周（4022 个）环比增加 15%。

主要内容

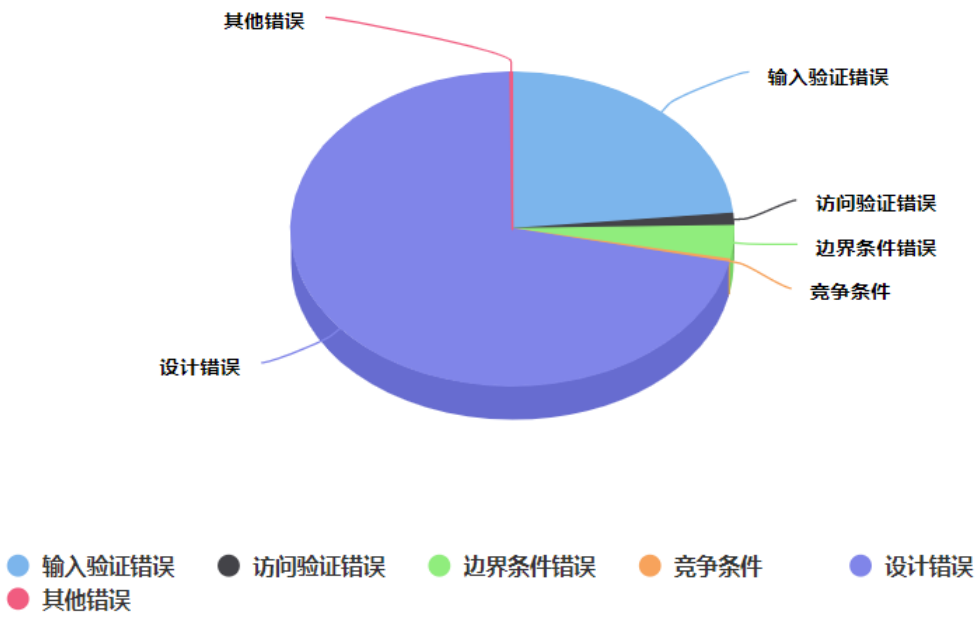
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

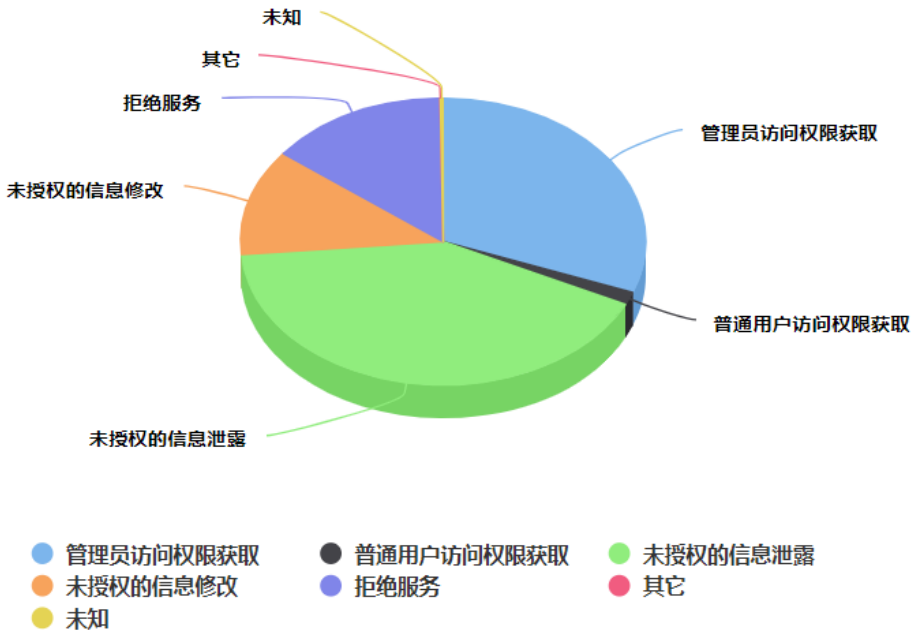
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 537 个，其中高危漏洞 180 个、中危漏洞 272 个、低危漏洞 85 个。漏洞平均分值为 5.84。本周收录的漏洞中，涉及 0day 漏洞 299 个（占 56%），其中互联网上出现“Pimcore 跨站脚本漏洞（CNVD-2022-22702）、CuppaCMS SQL 注入漏洞（CNVD-2022-22322）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 4620 个，与上周（4022 个）环比增加 15%。

二、安全漏洞增长数量及种类分布情况

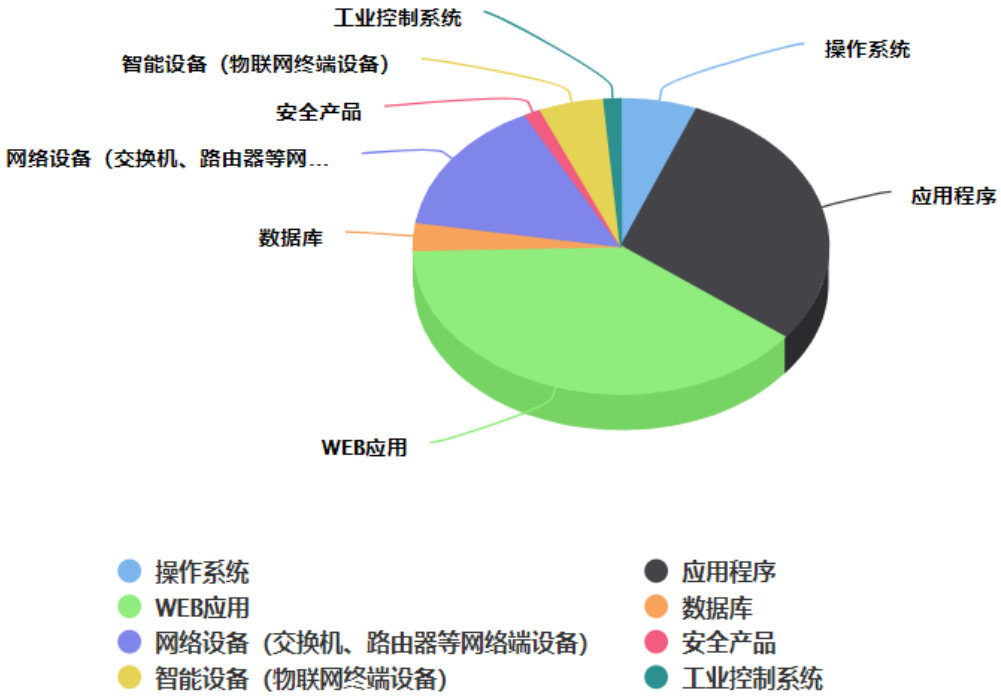
➢ 漏洞产生原因（2022 年 3 月 1 日—2022 年 3 月 31）



➢ 漏洞引发的威胁（2022 年 3 月 1 日—2022 年 3 月 31）



➢ 漏洞影响对象类型（2022 年 3 月 1 日—2022 年 3 月 31）



三、安全产业动态

➢ 织密法网做好互联网平台“守门人”

编者按：数据被称为“信息时代的石油”，作为数据内容之一的个人信息，毫无疑问，因具有巨大的商业价值潜力而被广泛关注。不可否认，数据的信息交流已经完全渗透并覆盖到当今社会人类日常生活中所涉及的各个领域。我国作为人口大国，数据产业带来的经济体量不容小觑，而大多数人可能不注意的是，平时我们在使用手机软件时留下的搜索记录、聊天信息、访问足迹等，都有可能成为用来牟利的信息资源。当下我国正处于全面数字化转型的高质量发展新阶段，在新技术新应用层出不穷的生态语境下，个人信息的处理已经成为社会进步和产业升级新的驱动力，而广大民众对于加大个人信息保护力度也有着空前的关切和期待。2021 年 11 月 1 日，《个人信息保护法》正式施行，标志着我国个人信息保护立法体系更上一个台阶。针对不得过度收集个人信息、“大数据杀熟”、对人脸信息等敏感个人信息的处理等问题作出规制，可以说，这部法律急民之所急，解民之所忧，充分回应了社会关切。《个人信息保护法》实施四个多月来，侵害个人信息权益的违法行为频频发生在我们每一个人身边。进入 2022 年以来，工业和信息化部已经完成两批次 134 款 App 和 SDK 的 200 多个合规问题的通报。不可否认，保护个人信息，拥抱个人信息合法权益受保护、个人信息处理活动受规范、个人信息合理利用受促进的数字治理新时代，任重而道远。由此可见，如何使用好这部法律，发挥其应有作用，还需我们共同努力。

“现在的购物平台太不老实，网页上的广告很奇怪。”网友“张心心”抱怨说，“当天在一个平台上买了东西，广告里就出现了。”家住湖南的牛先生也有同感。用手机搜了狗粮，打开短视频、社交和一些工具软件时，广告里就推送了狗粮，刷短视频也推荐狗粮；搜了一个保温杯，微信公号就推送了保温杯的广告，连款式都一模一样。“甚至只是口头提过一种商品，类似广告就频频出现在手机页面……好像全世界都掌握我的一举一动。”牛先生颇为无奈。你是否也有过这样的经历，某天在和朋友聚餐时提起某个感兴趣的产品，过会儿打开购物网站时就能看到类似产品的推销。抑或是前脚刚看了房价走势，后脚就接到推销楼盘的电话。

这些披着智能算法外衣的广告在为我们带来便利的同时，更让人毛骨悚然。在央视“3·15”晚会上，相关问题被曝光，涉事企业被公开披露后也遭到了严惩。虽然涉事企业被处罚，但是公众就如何保障用户信息权益，防范恶意窃取个人信息的问题仍然充满担忧。我买了什么、搜了什么，全网的购物、短视频、社交平台怎么都知道了？基于大数据算法的精准推送，在服务用户需求的同时，也让人感觉不解和恐慌。不可否认，人们在享受网络技术带来的便利和好处之时也时刻面临着个人信息“裸奔”的风险。

“精准营销”“急刹车”？法律给精准广告划定红线

《中国互联网络发展状况统计报告》显示，截至 2021 年 12 月，我国网民规模达 10.32 亿，互联网普及率达 73.0%。滚滚而来的时代浪潮中，各类网页和软件以其丰富的信息资源和便利的鲜明特点，进入众人的生活。但是，随着相关软件变得更加“贴心”，其背后的信息安全等新型问题逐渐浮出水面。

最常见的便是广告投放问题，在用户不知情的情况下，许多第三方 App 在暗中收集用户的个人数据，包括用户年龄、性别、收入、行业、教育背景、婚姻状态、兴趣爱好等信息，然后对这些数据进行分析。最终根据得出的结论来指导广告的投放，以此来提高产品销售的转化率。

也许在部分人眼中，这种程度的个人信息采集并不打紧，但是其背后的灰色地带却不容小觑。这样的个性化广告“精准营销”往往会衍生出更加严重的犯罪行为，比如诈骗。在知名护肤品珂润商家涉及信息泄露事件中，受害者均为淘宝珂润官方旗舰店消费者。诈骗人员能够准确说出消费记录、订单信息、个人信息等敏感资料，获取消费者的信任后，便以“珂润”产品存在问题为由进行诈骗。遍布全网的受害消费者中，有人被骗了近 10 万元。受害者事后回忆：“本来很警觉，但对方说出那些信息后，自己就放松了防范意识。”

在个人信息的过度采集问题中，App 的违规数据采集的现象不容忽视。2021 年 12 月 20

日，国家计算机网络应急技术处理协调中心点名存在隐私保护不合规行为的 17 款 App，其中包括哈啰出行、和讯财经等在内的 15 款 App“未向用户明示申请的全部隐私权限”。与此同时，在工信部发布的 2022 年第一批侵害用户权益的 App 名单通告中，有 107 款国内知名的 App 应用存在不同程度的违规获取和采集用户数据和权限的情况。

对于此类行为，我国《个人信息保护法》规定：“通过自动化决策方式向个人进行信息推送、商业营销，应当同时提供不针对其个人特征的选项，或者向个人提供便捷的拒绝方式。”简言之，互联网广告商需要向用户提供关闭个性化广告推送的功能。细心的用户可能会发现，微信在《个人信息保护法》实施不久后，给用户推送了改版的服务协议，阿里、京东等大型主流电商平台也都纷纷采取了增加个性推送开关等应对措施。据《App 违法违规收集使用个人信息监测分析报告》(以下简称《报告》)统计，目前全国主流安卓应用商店在架 App 的去重后总数为 112 万款。《个人信息保护法》实施以来，App 强制要求用户打开非必要权限、强制要求用户填写非必要个人信息等典型违规行为明显减少，监测发现仅有 1%的中小应用残留此问题。对此，专家指出，这是因为《个人信息保护法》正式实施后，给精准推送等广告营销模式划定了精准的红线。

为了验证该类情况的整改效果，通过在今日头条、抖音等 App 进行了相关测试，发现这些 App 的设置选项下确实多出了关于个性化广告“关闭/开启”的选项。不过，这些 App 都把“个性化推荐”关闭键“藏得”较为深入，一般在“设置”选项里面的，隐私、广告相关的选项中才找到。

这一“碟中谍”问题也得到了有关部门的重视。今年 1 月，《互联网信息服务算法推荐管理规定》出台，明确了算法推荐服务提供者应当以显著方式，告知用户其提供算法推荐服务的情况；向用户提供不针对其个人特征的选项，或者向用户提供便捷的关闭算法推荐服务的选项。该规定自 3 月 1 日起施行。

此外，《报告》显示，尽管很多 App 不再强制收集个人信息，但仍存在首次启动时弹窗索要多个无关权限的问题，由此产生的投诉举报也比较集中，用户对此较为反感。据国家计算机网络应急技术处理协调中心相关人士介绍，目前量大面广的 App 已将启动时索要权限改为在用户触发特定功能时再索要对应权限，改善了用户体验。监测显示，在华为、小米、vivo、OPPO、腾讯等主流平台的应用商店近 3 个月新上架的应用中，每月平均有近 1000 款应用存在此问题。

“由于 App 数量非常多，推陈出新频率高，而且 App 的个人信息收集行为和方式也在不断变化，监管部门很难做到全覆盖监管，很容易出现覆盖范围过窄的情况。”TalkingData 法

务合规负责人兼数据合规官葛梦莹说，“针对海量 App 收集、使用个人信息的情况，《个人信息保护法》提出了从关键环节入手的监管思路，即首次区分了一般的个人信息处理者和充当‘守门人’角色的操作系统、应用程序分发平台、大型 App 平台等个人信息处理者。这其中就包括了上述应用商店，因为应用商店是众多 App 进行个人信息收集处理的必要通道，从应用商店这个关键环节入手，对其提出增强个人信息保护的要求，例如要求超大平台建立外部监督委员会，主动引入对内部信息处理行为的社会监督，主动承担对平台生态中各方个人信息处理行为的监督，并发布社会责任报告等多种手段来杜绝 App 强制收集非必要个人信息的问题。”

大数据看人下菜碟？更为隐蔽的“二代杀熟”

除了非法收集个人信息等严重违法行为，互联网领域“擦边”行为也在悄然地损害着消费者的权益。

近年来，各地屡有披露，有的楼盘违规收集人脸信息进行大数据分析，对客户类型进行甄别后“精准营销”。多家互联网企业也曾被曝光，利用大数据分析对不同群体进行差别定价，实行“价格歧视”，这一行为被称为“大数据杀熟”。

“大数据杀熟”是指互联网平台依靠数据优势和信息不对称，对用户实施价格歧视，这也并非新鲜话题。来自浙江的胡女士曾经以携程采集了自己非必要个人信息进行“杀熟”，将其告上法庭，此案被称为“大数据杀熟”第一案。法院经审理查明，胡女士一直都通过携程 App 来预订机票、酒店，是该平台享受 8.5 折优惠价的钻石贵宾客户。然而，身为贵宾的胡女士不仅没有享受到优惠，反而多支付了一倍的房价。最后，法院按“退一赔三”标准，对胡女士的诉求予以支持。而彼时，胡女士遇到的还是略显“青涩”的初代杀熟。“初代杀

熟最典型的是，平台对新客展示低价，对熟客显示高价。”上海市消费者保护委员会副秘书长唐健盛解释说。如今，“熟客卖高价”的投诉已越来越少，而基于人工智能、算法迭代以及平台对消费者信息全方位收集的“二代杀熟”则更为普遍，也更为隐蔽。

比如，通过搜集打车、旅游、购物等信息，平台可以为用户进行全方位“画像”，并据此进行精准推送。“如果某一段时间内一直使用某 App 买咖啡，那么购买咖啡将会变贵。但当一段时间不使用后，又会收到平台推送的折扣优惠券。”2021 年 9 月 6 日，北京市民牛先生表达了自己因消费频率不同，在某平台上受到的不同待遇。无独有偶。湖北省武汉市姚女士在一外卖平台小程序下单一份工作简餐时发现，在两个账号上，该商品价格、打包费、配送费都相同，但使用“账号一”开通可领取到 6 张 5 元无门槛优惠券的会员仅需 3.2 元，使用“账号二”开通该会员却需要 15 元。若开通会员购买上述套餐，两者结算价格相差 11.8 元。这已不是姚女士第一次遭遇此类状况。“在同一平台有两个购物账号，很久没用的账号大概率是被判定为非活跃用户，系统自动下发了 15 元无门槛优惠券。”姚女士说，她在某化妆品购物平台注册了两个账号，半年后收到客服的电话称账号已很久未使用，便发放了抵用券希望用户能经常登录平台购买商品。

平台基于用户购物习惯差异，通过系统量身定制出“千人千面”的浏览界面，是“大数据杀熟”的精髓所在。中国传媒大学大数据研究中心沈浩教授认为，多领域存在此类现象，根源于“个性化推荐算法”。“由于现阶段电商、社交媒体都可以获取消费者大量信息，特别是个性化的数据。根据这些行为数据，就能给一个用户贴上成千上万的标签，完成用户数字画像。进而深层次预测用户行为，并在此基础上进行商品推荐。”沈浩教授说。

对此，某电商平台负责人王先生进一步解释道：“用户所在区域、性别，使用的设备型号，浏览商品的类别、价格、停留时间等各种消费行为，都被一套特定的算法所标记。当消费者浏览某一类商品花费较长时间，会产生一定的价格敏感性，那么平台在推荐‘猜你喜欢’时，就倾向于推荐相似度、性价比都较高的产品。”

对于隐蔽性更强的“二代杀熟”，公安部第三研究所网络安全法律研究中心主任黄道丽此前接受媒体采访时表示：“‘大数据杀熟’相对集中在网购、网约车、网络视频和在线票务等领域。尽管‘价格歧视’现象在传统领域依然存在，但‘大数据杀熟’的实施方式非常隐蔽。用户借助电脑或移动端只能看到平台展示给自己的价格，无法像线下‘明码标价’式看到对所有用户公布的价格。”黄道丽指出，对“大数据杀熟”现象执法存在较大困难，因为当用户主张遭遇“大数据杀熟”时，相关企业通常会以季节、数量、区域、捆绑让价、动态定价等因素，强调价格歧视问题的正当性。监管部门基于此，往往无法确认企业是否利用了

个人数据实施“杀熟”。

《个人信息保护法》出台前后，对于“大数据杀熟”乱象，监管部门高度重视并出台相关规定。

2021 年 4 月 13 日，国家市场监管总局会同中央网信办、税务总局召开互联网平台企业行政指导会指出：“实施‘大数据杀熟’等问题必须严肃整治。”2021 年 7 月 2 日，市场监管总局发布的《价格违法行为行政处罚规定(修订征求意见稿)》，亦对电商平台经营者利用“大数据杀熟”等作出规定。《个人信息保护法》强调，不得过度收集个人信息，禁止商家通过自动化决策“大数据杀熟”。2021 年 12 月 31 日，国家互联网信息办公室、工业和信息化部、公安部、国家市场监督管理总局联合发布《互联网信息服务算法推荐管理规定》，这是我国首部关于网络销售平台算法的规定。

平台责任 OR 监管责任？平台经济必须有“守门人”

除了对个人信息的立法保护之外，互联网领域的突出问题也屡屡出现在“两高”工作报告中。在今年全国两会上，最高人民法院工作报告强调：“对侵犯个人信息、煽动网络暴力侮辱诽谤的，依法追究刑事责任。”最高人民检察院工作报告强调：“从严追诉网络诽谤、侮辱、侵犯公民个人信息等严重危害社会秩序、侵犯公民权利犯罪。”网络虚拟空间，依法治理要实，治理网络暴力、清朗网络空间是其中重要内容。

如今，《个人信息保护法》的实施，将与《网络安全法》《数据安全法》构成我国网络空间安全和数据保护的三驾马车，预示着我国个人信息保护法治进程即将翻开新篇章。

“《个人信息保护法》对防范平台通过隐私条例过度收集处理用户个人信息等提供了强有力的法律保障。”中国人民大学国家发展与战略研究院金融科技与互联网安全研究中心主

任杨东撰文提到，针对当前具有市场支配地位的互联网头部企业掌握大量个人信息，对互联网市场稳定及用户数据安全具有支配力的情况，《个人信息保护法》在适用时对大型和小型个人信息处理者进行了区分和细化，明确大型互联网平台是平台经济的“守门人”，需承担更多责任。

对于提供重要互联网平台服务、用户数量巨大、信息量巨大、业务类型复杂的个人信息处理者，杨东举例说明，《个人信息保护法》特别规定了建立健全个人信息保护合规制度体系、定期发布个人信息保护社会责任报告、接受社会监督等义务；对于信息量较少、技术水平较低的小型企业，由国家网信部门为其制定数据处理相关规则。在立法时对适用对象进行区分的目的在于发挥大企业“守门人”的主体责任，并对其加强监管，同时也有利于降低小型企业合规成本，避免其承担过重压力，并弥补事后监管的滞后性。

种种举措并行，足以看出我国政府在公民隐私保护领域的整治力度和决心。“个人数据关乎公民隐私，是每一位公民的基本人权，必须予以保障。”杨东指出，在数字经济蓬勃发展的时代背景下，防止具有市场支配地位的大型平台实施垄断，也是数字经济领域各项法规的立法本意。

自开展 App 侵害用户权益专项整治工作以来，违规收集、使用用户个人信息的多款 App 被要求整改或决定下架，有效打击了侵犯用户隐私的行为。根据工信部官方网站信息，2021 年以来，我国已累计完成 29 万款 App 技术检测，对其中 1862 款违规 App 提出整改要求，并下架了 107 款拒不整改的 App。

近期，国家计算机网络应急技术处理协调中心发布的报告显示，App 无隐私政策问题呈现下降趋势，问题占比由 2019 年最高的 26%下降至 2021 年的 6.7%。平台企业公开收集使用规则的意识显著增强，一些头部企业应用商店今年已加大无隐私政策问题应用的审核力度。在近三个月新上架的 App 中，此问题已基本清零。但是，部分中小体量的应用商店审核机制尚未健全，仍有约 7.8 万款问题 App 需进行下架清理。

此外，针对疫情防控期间突出的个人信息收集和使用问题，全国政协委员、北京国际城市发展研究院院长连玉明在前不久的全国两会上呼吁，需要妥善处理涉疫个人信息“善后”问题。连玉明指出，要明确“谁收集谁负责”“谁使用谁负责”基本原则，细化涉疫个人信息保护主体的责任义务和善后处置的边界。进一步增强对疫情相关个人信息在采集、存储、使用、共享、传输、披露、销毁等生命周期各环节进行风险管控。指定相关机构根据个人信息保密级别、敏感程度划分保存期限，分设处理方式，建立分类分级的存储管理和销毁制度。做到事前可防范、事后可追溯、信息安全可管可控。适时引入“被遗忘权”，阶段性地将前

期公布的个人信息从网络上删除，以消除不良影响。

“以前，个人信息会被无节制地分享和超范围使用。”互联网观察者蒙遗善表示，《个人信息保护法》以及多项相关规定的实施，将彻底改变企业和相关部门不注重保护个人信息的情况，也让用户在主张权利时有法可依，这意味着个人信息处理裸奔的时代或将终结。

与此同时，杨东强调，以透明、平等、智能为核心，以区块链技术为驱动，既对用户数据加密，又实现数据共享的先进技术，也正在为监管机关的治理提供助力。实现数据依法合理有效利用、依法有序自由流动，将促进以数据为关键要素的数字经济发展，让平台和用户共享数字经济发展带来的机遇与便利。

能力越大，责任越大，企业做得越大、平台越活跃，相应的社会责任和道德责任就越大。在数字经济的背景下，可以预见未来互联网领域的商业化应用还会不断地发展和进步，利用大数据进行精准推送、个性化分发的商业模式注定不会被轻易抛弃。这也对企业提出了更加具体的管理责任，要求企业能够准确把握责任，明确工作规范，健全管理制度，完善运行规则。这样，网络平台才能做大做强，网络家园才能风清气正，网络强国才能稳步前行。（来源：《民主与法制》周刊 2022 年第 11 期）

➢ 政府工作报告再提网络安全、数据安全和个人信息保护，推动数字经济发展

2022 年 3 月 5 日，十三届全国人大五次会议在京开幕。政府工作报告中提到，要强化网络安全、数据安全和个人信息保护。这是自 2021 年政府工作报告以来，再次对数据安全和个人信息保护的强调。

此外，数字经济连续多年被写入政府工作报告。今年政府工作报告指出，要促进数字经济发展。加强数字中国建设整体布局。建设数字信息基础设施。同时完善数字经济治理,释放数据要素潜力,更好赋能经济发展、丰富人民生活。数字经济领域，监管治理与促进发展并行。数据要素已成为数字技术进步的助推剂，进而促进生产力的发展。数据的价值只有在有序、规范的流通场景中才能充分发挥，完善公共数据开放共享机制、建立健全数据流通交易规则、拓展规范化数据开发利用场景、加强数据安全保护等方面的布局，已成为未来的发展方向。

强化网络安全、数据安全和个人信息保护

“强化网络安全、数据安全和个人信息保护”已经连续两年在政府工作报告中被强调。

这反映了三个主要趋势：北京师范大学互联网发展研究院院长助理、中国互联网协会研究中心副主任吴沈括在接受 21 世纪经济报道记者采访时表示，首先，网络安全和数据安全监管已成为世界各国共同关注的重大议题，形成了数字化战略当中的焦点议题，具有全球战略高度;其次，网络安全、数据安全与个人信息保护是“十四五”时期，我国进入高质量发展新阶段的重要议题，是国家建设网络强国和数字中国战略的重要组成部分;目前社会各界也高度关注网络安全、网络治理以及数据治理一系列问题，加强网络和数据监管是回应民众利益诉求的一个重要举措。

回顾 2021 年，我国初步搭建完成数据安全的法律架构。《数据安全法》《个人信息保护法》相继于 9 月和 11 月落地施行，与此前生效的《网络安全法》共同形成了数据治理法律领域的“三驾马车”。

相关配套法规纷纷起草或出台：2021 年 8 月， 国务院公布《关键信息基础设施安全保护条例》，对关键信息基础设施的范围认定、各监管部门的职责、运营者责任义务等内容提出具体要求。同年 10 月，国家互联网信息办公室公布《数据出境安全评估办法(征求意见稿)》，对数据出境安全评估重新进行的明确和梳理，提出“风险自评估与安全评估相结合”，在国家网信部门对跨境数据进行评估之前，多加一道企业“自评估”的闸门。

今年 1 月 4 日，国家网信办等十三部门联合修订发布《网络安全审查办法》，将网络平台运营者开展数据处理活动影响或者可能影响国家安全等情形纳入网络安全审查范围，并明确要求掌握超过 100 万用户个人信息的网络平台运营者赴国外上市必须申报网络安全审查

等。

吴沈括认为，在网络安全、数据安全和个人信息保护领域，当前我国需关注和应对的一大挑战为技术支持，尤其是核心技术的安全可控;其次是社会各单位，包括公共部门、私营部门有关网络治理、数据治理的组织管理体系、组织管理架构还有待进一步的普及和落实，从而构筑健康可持续发展的数字生态;此外，社会公众的数字素养有待进一步的提升，在网络空间和数据资源的利用层面，需要进一步提升数字化意识以及必要的数字技能。

从治理的角度出发，也重点指向三个层次、三个方向：在基础设施层面，需进一步强化投入和建设数字基础设施建设;在组织管理层面，全社会合规风控体系尚待公共资源的支持和有力引导;在网络内容、数字内容、数字伦理方面，应有进一步的质量提升和深度建设。”吴沈括说。

今年全国两会期间，数据安全和个人信息保护议题一如既往地受到关注，多位代表委员建言献策。全国政协委员、北京金台律师事务所主任皮剑龙提出了推进人脸识别信息保护的提案，建议加强对人脸识别全流程监管，构建“采集—储存—使用—销毁”一体化的监管体系。全国政协委员、第五空间信息科技研究院院长谈剑锋带来关于升级数据安全管理模式、加强对关键数据管控的提案，强调面向特定领域的基础性数据安全体系建设，尽快设立国家“数据银行”，优先收储个人生物特征、医疗健康数据等具有唯一性、不可再生性的数据，由国家成立专门机构统一管控等。

促进数字经济发展

数字经济已连续多年被写入政府工作报告。从政策演讲过程和政府工作报告中可发现，数字经济的内涵和定义被不断地丰富和具体化，也越来越重视区域布局和特色发展。” 浙江大学国际联合商学院数字经济与金融创新研究中心联席主任、研究员盘和林表示。

今年政府工作报告提出：促进数字经济发展。加强数字中国建设整体布局。建设数字信息基础设施，推进 5G 规模化应用，促进产业数字化转型，发展智慧城市、数字乡村。加快发展工业互联网，培育壮大集成电路、人工智能等数字产业，提升关键软硬件技术创新和供给能力。

在树根互联联合创始人、CEO 贺东东看来，我国工业互联网发展已进入深度应用阶段。下一步应聚焦大数据、工业区块链等共性技术创新，提高工业互联网平台核心通用能力，深化跨行业跨领域应用落地，打造具有国际竞争力的平台型工业互联网操作系统;加强工业互联网赋能职业教育;同时，加强工业互联网数据安全，鼓励具有安全资质的工业互联网领军企业牵头推动安全公共服务平台建设，为数据要素赋能经济发展提供安全保障。

而在建设数字信息基础设施领域，国家层面也已开展行动。日前，国家发改委等联合印发通知，同意在京津冀、长三角、粤港澳大湾区、成渝、内蒙古、贵州、甘肃、宁夏等 8 地启动建设国家算力枢纽节点，并规划了 10 个国家数据中心集群。至此，全国一体化大数据中心体系完成总体布局设计，“东数西算”工程正式全面启动。地方层面，《河南省数字经济促进条例》3 月 1 日起正式施行，立法明确将数字基础设施建设纳入国土空间规划。

盘和林分析，中国经济的深层优势主要体现在具有全局发展的战略定力和超大规模经济体。保持全局发展的战略定力、不受短期波动的冲击和干扰，能够为数字经济的崛起与成长营造一个良好的、稳定的发展环境。但同时，也面临着大数据安全、云安全、供应链安全、区块链安全等一系列全新复杂安全挑战。下一阶段，要研究建设前瞻性的数字安全平台体系，由政府统筹打造城市级数字空间安全基础设施和应急体系，保障经济社会稳定发展。

此外，**“完善数字经济治理，释放数据要素潜力，更好赋能经济发展、丰富人民生活”**也在今年政府工作报告中被提及。

“数据要素是人工智能等数字技术发展的核心关键，而人工智能等数字技术又是未来生产力发展的关键，所以数据要素通过推动数字技术发展的方式，来推动数字技术和数字经济的发展。”盘和林表示。

为释放数据要素潜力，北京、上海等地先后成立数据交易所，政策方面亦不乏创举，如 2020 年 4 月，《中共中央国务院关于构建更加完善的要素市场化配置体制机制的意见》发布，今年 1 月，国务院办公厅印发《要素市场化配置综合改革试点总体方案》，提出数据要素流通规则的多项探索。

“数据的价值只有在流通场景中才能充分发挥，但这种流通必须是有序地、规范地，数据价值才能够自动流向应用。”盘和林建议，未来应努力做好包括完善公共数据开放共享机制、建立健全数据流通交易规则、拓展规范化数据开发利用场景、加强数据安全保护等方面的布局。（来源：商密君）

➢ 《网络安全审查办法》修订后正式施行 织密信息安全“防护网”

由 13 个部门联合修订发布的《网络安全审查办法》（以下简称《办法》）日前开始施行，受到广泛关注。国家网信办有关负责人表示，对《办法》进行修订，主要目的是进一步保障网络安全和数据安全，维护国家安全。

平台出海有“规定动作”

近年来，中国互联网应用加速发展，在通信、支付、购物、视听等领域都涌现出一些体量巨大、全球领先的互联网平台，其中不少已赴国外上市或有相关计划。据了解到，《办法》第七条明确要求：掌握超过 100 万用户个人信息的网络平台运营者赴国外上市，必须申报网络安全审查。这成为各界最为关注的内容。

中国网络安全审查技术与认证中心高级工程师唐旺说，如果互联网平台不遵守国家有关网络安全要求，不落实重要数据和个人信息保护责任义务，上市后在金融力量影响下无序扩张，网络安全风险和威胁将成倍扩大。

业内人士认为，将网络平台运营者赴国外上市纳入网络安全审查，是《办法》修订的一大亮点。从实际情况看，走到出海上市这一步的平台，用户数很少有低于百万级别的。《办法》的修订意味着今后网络安全审查成为平台出海上市的“规定动作”。

“网络安全审查不会限制开放，启动审查后，经研判不影响国家安全的，可继续赴国外上市。”中国信息安全测评中心桂畅旎说，开展网络安全审查是国际通行做法，有利于推进中国网络空间治理体系和治理能力现代化。与此相呼应，《办法》对审查的工作机制、工作流程等进行了适当调整，例如增加了证监会作为网络安全审查工作机制成员单位，以及上市申请文件作为上市审查申报材料的一部分等。中国网络安全审查技术与认证中心工程师齐越认为，总体上看，审查机制和流程沿用了原有审查制度框架，就新纳入赴国外上市审查这一变化进行了有针对性的优化，审查制度在实践中不断得到完善。

为数字经济护航

数字经济时代，数据的重要性愈发凸显。作为国家新型生产要素和基础战略资源的代表，数据安全已成为保障网络强国建设、护航数字经济发展的安全基石。《办法》规定，数据安全也是网络安全审查制度的重要内容，将数据安全风险作为网络安全审查的重要审查因素，并且在供应链安全风险评价的基础上，新增了国家数据安全风险因素评价。

全国信息安全标准化技术委员会委员李雪莹说，修订后的《办法》增加了多项数据安全相关条文，对数据安全的重视程度更高、覆盖对象的范围更广、审查指标更加量化。全国信息安全标准化技术委员会委员黄敏提醒，数据安全已经成为国家安全的重要组成部分，需要重点保护关键信息基础设施、核心数据、重要数据等。

“此次修订以维护数据安全为中心，以做‘加法’的方式，新增了不少亮点。”北京航空航天大学工业和信息化法治研究院研究员雷震文说，推行网络安全审查，加强风险识别和控制，已成为当前世界各主要国家防范网络安全风险的通行做法。《办法》的施行，也将提高全社会对网络安全、数据安全的重视程度。

多方合力依法治网

网络安全审查，是国家安全审查的重要组成部分。中国互联网络信息中心发布的数据显示，2021 年上半年，工业和信息化部网络安全威胁和漏洞信息共享平台总计接报网络安全事件 49605 件。目前，网络产品和服务供应链安全形势依然严峻，数据安全风险在未来将更加突出。

为应对网络安全形势，网络安全审查制度需要与时俱进。从《国家安全法》明确建立国家安全审查与监管制度和机制，到《网络安全法》确立了网络安全审查的主要客体与主体，中国一直在努力保障网络安全和数据安全，维护国家安全。桂畅旎认为，此次《办法》落实对数据安全、网络安全的最新要求，是中国依法治网的具体发展和生动体现。

在中国社科院法学所副研究员周辉看来，《办法》的有效落实需要多方主体共同参与、积极协作，既要有监管部门依法严格履职，也要有关键基础设施提供者、网络平台运营者主动合规，还需要社会公众的舆论参与和监督。（来源：新华网）

➢ 2022 年“3·15”今年曝光的这些问题与信息安全有关

2022 年 3 月 15 日晚，以“公平守正 安心消费”为主题的 “3·15”晚会在央视财经

频道现场直播，引起广泛关注。今年的“3·15”晚会直击数字消费和百姓公共安全领域的热点问题，曝光了一批消费乱象和典型案例。晚会首次设立“3·15 信息安全实验室”，针对消费者日常生活中的信息安全隐患发出风险预警，推动建立安心的市场环境，助力中国经济提质升级，推进高质量发展。

揭露数字经济领域消费乱象，维护市场和行业秩序，促进数字经济健康发展

数字经济迅猛发展，催生出许多新业态，拓展了许多新的消费领域。我国在线直播的用户规模已超过 6 亿，很多用户对自己中意的网络主播，直接用线上支付或是购买虚拟商品进行“打赏”。“3·15”晚会调查发现，美女主播和她们身后的男运营唱“双簧”，设置重重套路，欺骗粉丝情感，诱使用户多多“打赏”，骗取钱财。（3·15 晚会曝光丨“美女主播”实为“抠脚大汉”！联手套路掏空万千粉丝“老公”...直播运营公司套路大起底）

直播电商拉动消费，这两年风头正劲。然而，一些贩卖玉器、翡翠的电商直播间里，主播却假扮工厂主和货主演“对手戏”诱骗消费者。昆明某直播间里，甚至有冒充缅甸矿区现场砍价，不惜编造出走私、偷渡、绑架的“狗血”剧情，把电商直播间变成了欺骗消费者的陷阱。（3·15 晚会曝光丨有演员有剧本！翡翠直播“越境交易”全是演戏！缅甸翡翠代购直播间实为国内写字楼布景）

一些所谓的口碑营销机构，受利益驱使，在搜索引擎、问答平台、口碑网站上，冒充真实用户提问和回答，用“万词霸屏”技术左右搜索结果，还非法篡改、伪造、删除网络信息，妨害网络传播秩序，严重误导了受众，侵蚀了公众的知情权和选择权。（3·15 晚会曝光丨口碑营销公司操纵搜索结果 企业负面给钱就能屏蔽）

捆绑销售软件和频频扰民的骚扰电话都是信息通讯领域严格整治的对象。

垃圾软件、垃圾广告让网络用户不胜其烦。“3·15”晚会通过调查发现，马鞍山百助网络公司专门向软件下载网站提供下载器，他们把下载器伪装成高速下载界面，诱骗用户点击

下载，甚至强制用户安装不需要的捆绑软件，以此获得高额推广收入。（3·15 晚会曝光丨软件下载平台“高速下载”竟是陷阱！200 余家软件下载站都沦陷？）

国家相关部门一直在整顿骚扰电话，但融营通信、容联七陌等个别企业却为电话营销公司非法搭建外呼系统，帮助骚扰电话逃避监管。杭州以渔信息技术公司、郑州绿牵网络科技公司等企业甚至抓取网站用户浏览数据，让骚扰电话变得更加精准。（3·15 晚会曝光丨浏览网页就能泄露手机号 起底骚扰电话背后的秘密）

首次设立“3·15 信息安全实验室”，针对日常信息安全隐患发出风险预警，拓展民生服务功能

今年“3·15”晚会首次设立“3·15 信息安全实验室”，针对消费者日常生活中容易忽视的信息安全隐患，进行专业场景式测试，及时发出风险预警。

如今，不少广告和 App 都打着免费 WIFI 的旗号，吸引消费者连接上网。其实，很多都是伪装的广告链接。一旦用户被诱导点击，链接中的应用程序就会自动安装到手机里，非法搜集用户信息，激活弹窗广告，让弹窗广告不断出现在用户手机上。（3·15 晚会曝光丨“免费 WiFi”App 暗藏陷阱：不仅根本连不上 还致隐私大曝光）

儿童智能手表可以方便家长和孩子联系，让家长随时掌握孩子行踪。但“3·15 信息安全实验室”测试发现，市场一些低配版本的儿童智能手表存在很大安全隐患，可以轻松获取地理定位、人脸图像、录音等权限的授权，导致用户隐私信息很容易被泄露，增加儿童和家庭安全隐患。（3·15 晚会曝光丨家长小心！低配的儿童智能手表成“行走的偷窥器”...）

本届“3·15”晚会由最高人民法院、最高人民检察院、国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、司法部、交通运输部、农业农村部、商务部、国家市场监督管理总局、国家药品监督管理局、中国消费者协会等领导机关、政府部门和机构与中央广播电视总台联合主办。

工信部：立即查处“3·15”晚会曝光的信息通信领域违规行为

2021 年 3 月 16 日，工业和信息化部高度重视用户权益保护工作，针对 3 月 15 日央视播出“3·15”晚会报道的以免费 Wi-Fi 为名诱骗用户下载恶意 APP、应用软件平台强迫捆绑下载、骚扰电话、儿童手表安全防护等问题，立即组织认真核查，依据《个人信息保护法》《网络安全法》《电信条例》《规范互联网信息服务市场秩序若干规定》《电信和互联网用户个人信息保护规定》等有关法律法规要求，进行严厉查处。


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
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 > 工业和信息化部 > 机关司局 > 信息通信管理局 > 工作动态

工业和信息化部立即查处“3•15”晚会曝光的信息通信领域违规行为

发布时间：2022-03-16 11:14 来源：信息通信管理局

工业和信息化部高度重视用户权益保护工作，针对3月15日央视播出“3·15”晚会报道的以免费Wi-Fi为名诱骗用户下载恶意APP、应用软件平台强迫捆绑下载、骚扰电话、儿童手表安全防护等问题，立即组织认真核查，依据《个人信息保护法》《网络安全法》《电信条例》《规范互联网信息服务市场秩序若干规定》《电信和互联网用户个人信息保护规定》等有关法律法规要求，进行严厉查处。

针对以免费Wi-Fi为名诱骗用户下载恶意APP问题。一是对曝光的Wi-Fi破解精灵、雷达Wi-Fi、越豹Wi-Fi助手等3款APP，第一时间下架处理。二是组织相关省通信管理局对3家涉事企业依法进行查处。三是组织第三方检测机构对Wi-Fi连接类APP进行全面技术检测，发现问题严肃处理。

针对应用软件平台强迫捆绑下载问题。一是组织相关省通信管理局对曝光的百助网络公司及PC6、桔梗、ZOL、腾牛网等软件

针对以免费 Wi-Fi 为名诱骗用户下载恶意 APP 问题。一是对曝光的 Wi-Fi 破解精灵、雷达 Wi-Fi、越豹 Wi-Fi 助手等 3 款 APP，第一时间下架处理。二是组织相关省通信管理局对 3 家涉事企业依法进行查处。三是组织第三方检测机构对 Wi-Fi 连接类 APP 进行全面技术检测，发现问题严肃处理。**针对应用软件平台强迫捆绑下载问题。**一是组织相关省通信管理局对曝光的百助网络公司及 PC6、桔梗、ZOL、腾牛网等软件下载平台依法进行查处。二是举一反三，督促主要软件下载平台开展自查自纠，全面整改捆绑欺骗误导用户下载软件等违规行为。**针对骚扰电话问题。**一是责令基础电信企业立即关停涉事企业拨打骚扰电话的语音专线，加强通信资源规范管理。二是组织相关省通信管理局对融营通信、容联七陌等呼叫中心企业进行核查，并依法予以处罚、实施行业信用管理。三是联合有关部门深入整治骚扰电话有关问题，加强源头治理。**针对智能儿童手表安全防护问题。**组织开展全面排查和专项治理，强化技术检测和监督检查，对安全能力不达标的儿童专用移动智能终端，将责令停止销售并依法处置涉事企业，切实保障未成年人权益。

下一步，工业和信息化部坚决贯彻落实党中央、国务院决策部署，积极采取有效措施，持续强化电信和互联网用户个人信息保护，针对侵害用户权益行为开展专项治理，加强技术检测和监督检查，加大处置和曝光力度，积极配合有关部门严厉打击网络黑灰产业等违法犯罪行为，全力营造更安全、更健康的信息通信消费环境。（来源：互联网综合整理）

四、政府之声

➢ 国家网信办发布《互联网弹窗信息推送服务管理规定（征求意见稿）》

2022 年 3 月 2 日，国家互联网信息办公室发布了《互联网弹窗信息推送服务管理规定（征求意见稿）》（以下简称《意见稿》），对互联网弹窗信息推送服务提出十项要求，包括不得恶意对普通用户和会员用户进行差别频次推送；不得以任何形式干扰或者影响用户关闭弹窗；不得设置诱导用户沉迷、过度消费等违反法律法规或者违背伦理道德的算法模型；不得通过弹窗信息推送服务诱导用户点击，实施流量造假、流量劫持等。

根据《意见稿》，互联网弹窗信息推送服务，是指通过操作系统、终端设备、应用软件、网站等，以弹出消息窗口页面形式向互联网用户提供的信息推送服务。互联网弹窗信息推送服务提供者，是指提供互联网弹窗信息推送服务的操作系统、终端设备、应用软件、网站等所有者或者运营者。（来源：中国网信网）

- **《互联网弹窗信息推送服务管理规定（征求意见稿）》**
- **全文：**http://www.cac.gov.cn/2022-03/02/c_1647826956995841.htm

➢ 工信部印发《车联网网络安全和数据安全标准体系建设指南》

2022 年 3 月 7 日，工业和信息化部印发《车联网网络安全和数据安全标准体系建设指

南》，提出到 2025 年，形成较为完善的车联网网络安全和数据安全标准体系。

车联网是新一代网络通信技术与汽车、电子、道路交通运输等领域深度融合的新兴产业形态。随着汽车电动化、网联化、智能化交融发展，车辆运行安全、数据安全和网络安全风险交织叠加，安全形势更加复杂严峻。

工信部提出，到 2023 年底，初步构建起车联网网络安全和数据安全标准体系。重点研究基础共性、终端与设施网络安全、网联通信安全、数据安全、应用服务安全、安全保障与支撑等标准，完成 50 项以上急需标准的研制。到 2025 年，完成 100 项以上标准的研制，形成较为完备的车联网网络安全和数据安全标准体系。（来源：工业和信息化部）

- **《车联网网络安全和数据安全标准体系建设指南的通知》全文：**
- https://www.miit.gov.cn/jgsj/kjs/jscx/bzgf/art/2022/art_0319fb270f634beabd52fbb41c8eb152.html

➢ 中共中央办公厅国务院办公厅印发《关于加强科技伦理治理的意见》

2022 年 3 月 20 日，中共中央办公厅、国务院办公厅印发了《关于加强科技伦理治理的意见》，并发出通知，要求各地区各部门结合实际认真贯彻落实。《意见》指出，科技伦理是开展科学研究、技术开发等科技活动需要遵循的价值理念和行为规范，是促进科技事业健康发展的重要保障。

《意见》提出的治理要求是，伦理先行、依法依规、敏捷治理、立足国情、开放合作。《意见》明确科技伦理原则，包括增进人类福祉、尊重生命权利、坚持公平公正、合理控制风险、保持公开透明。

《意见》要求健全科技伦理治理体制，包括完善政府科技伦理管理体制、压实创新主体科技伦理管理主体责任、发挥科技类社会团体的作用、引导科技人员自觉遵守科技伦理要求。

《意见》强调加强科技伦理治理制度保障，包括制定完善科技伦理规范和标准、建立科技伦理审查和监管制度、提高科技伦理治理法治化水平、加强科技伦理理论研究。

《意见》明确要强化科技伦理审查和监管，包括严格科技伦理审查、加强科技伦理监管、监测预警科技伦理风险、严肃查处科技伦理违法违规行为。

《意见》还对深入开展科技伦理教育和宣传提出要求，包括重视科技伦理教育、推动科技伦理培训机制化、抓好科技伦理宣传。（来源：新华社）

- **《关于加强科技伦理治理的意见》**
- **全文：**http://www.gov.cn/zhengce/2022-03/20/content_5680105.htm

➢ 科技部发布《人类遗传资源管理条例实施细则（征求意见稿）》

2022 年 3 月 22 日，科学技术部发布关于公开征求《人类遗传资源管理条例实施细则

（征求意见稿）》（以下简称《实施细则》）意见的通知。《实施细则》拟规定，不得向境外提供我国人类遗传资源。


中华人民共和国科学技术部
Ministry of Science and Technology of the People's Republic of China

全站 请输入关键字 搜索

首页 组织机构 信息公开

当前位置：科技部门户 > 通知通告

www.most.gov.cn

科学技术部关于公开征求《人类遗传资源管理条例实施细则（征求意见稿）》意见的通知

日期：2022年03月22日 11:12 来源：科技部 【字号：大 中 小】

为贯彻落实好《中华人民共和国人类遗传资源管理条例》，确保各项规定落地落实，进一步提高我国人类遗传资源管理效能，科技部研究起草了《人类遗传资源管理条例实施细则（征求意见稿）》，现向社会公开征求意见。欢迎广大公众提出意见，并通过以下途径和方式反馈：

1.通过电子邮件将意见发至sfs_swyyc@most.cn,邮件名称“实施细则征求意见”。

2.通过信函方式将意见寄至：北京市海淀区复兴路乙15号，科技部社会发展科技司（邮编：100862）,请在信封上注明“实施细则征求意见”字样。

3.通过传真方式，将意见发送至：010-58881471。

意见反馈截止时间为2022年4月21日。

根据《实施细则》，人类遗传资源包括人类遗传资源材料和人类遗传资源信息。人类遗传资源材料是指含有人体基因组、基因等遗传物质的器官、组织、细胞等遗传材料。人类遗传资源信息是指利用人类遗传资源材料产生的人类基因、基因组数据等信息资料。

《实施细则》拟规定，采集、保藏、利用、对外提供我国人类遗传资源应当尊重人类遗传资源提供者的隐私权，事先取得知情同意，确保提供者健康并保护其合法权益，并应当遵守科研活动的相关要求及技术规范，包括但不限于标准、规范、规程等。

《实施细则》拟明确主体资格。在我国境内采集、保藏和对外提供我国人类遗传资源必须由我国科研机构、高等学校、医疗机构和企业开展。境外组织、个人及其设立或者实际控制的机构不得在我国境内采集、保藏我国人类遗传资源，不得向境外提供我国人类遗传资源。

（来源：科技部）

- **《人类遗传资源管理条例实施细则（征求意见稿）》**
- **全文：**http://www.most.gov.cn/tztg/202203/t20220322_179904.html

五、本期重要漏洞实例

➢ Microsoft 发布 2022 年 3 月安全更新

发布日期：2022-3-8

更新日期：2022-3-8

描述：2022 年 3 月 8 日，微软发布了 2022 年 3 月份的月度例行安全公告，修复了多款产品存在的 71 个安全漏洞。受影响的产品包括：Windows 11（27 个）、Windows Server 2022（28 个）、Windows 10 21H2（30 个）、Windows 10 21H1（30 个）、Windows 10 20H2 & Windows Server v20H2（30 个）、Windows 8.1 & Server 2012 R2（22 个）、Windows Server 2012（20 个）、Windows RT 8.1（21 个）和 Microsoft Office-related software（6 个）。利用上述漏洞，攻击者可进行欺骗，绕过安全功能限制，获取敏感信息，提升权限，执行远程代码，或发起拒绝服务攻击等。提醒广大 Microsoft 用户尽快下载补丁更新，避免引发漏洞相关的网络安全事件。

CVE 编号	公告标题	最高严重等级和漏洞影响	受影响的软件
CVE-2022-24508	Windows SMBv3 Client/Server 远程代码执行漏洞	重要 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Windows 10
CVE-2022-21990	Remote Desktop Client 远程代码执行漏洞	重要 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2022-23294	Windows Event Tracing 远程代码执行漏洞	重要 远程代码执行	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016 Server 2012 R2 Server 2012 Windows 8.1
CVE-2022-24459	Windows Fax and Scan Service 权限提升漏洞	重要 特权提升	Windows 11 Server 2022 Server, version 20H2 Server 2019 Windows 10 Server 2016

			Server 2012 R2 Server 2012 Windows 8.1
CVE-2022-24509	Microsoft Office Visio 远程代码执行漏洞	重要 远程代码执行	Office LTSC 2021 365 Apps Enterprise Office 2019

来源：https://msrc.microsoft.com/update-guide/releaseNote/2022-Mar

➢ Spring Cloud Function 存在 SPEL 表达式注入漏洞

发布日期：2022-03-30
更新日期：2022-03-30
受影响系统：
Spring Spring Cloud Function >=3.0.0.RELEASE，<=3.2.2
描述：

CVE(CAN) ID: CNVD-2022-23932
Spring Cloud Function 是基于 Spring Boot 的函数计算框架。Spring Cloud Function 存在 SPEL 表达式注入漏洞，攻击者可利用该漏洞通过 SPEL 表达式注入的方式在远程执行注入攻击。
建议：

厂商已发布了漏洞修复程序，请及时关注更新：

https://github.com/spring-cloud/spring-cloud-function/commit/0e89ee27b2e76138c16bcba6f4bca906c4f3744f

➢ Oracle MySQL Server 拒绝服务漏洞

发布日期：2022-01-19
更新日期：2022-03-30
受影响系统：
Oracle Oracle MySQL Server <= 8.0.27
Oracle Oracle MySQL Server <= 5.7.36
描述：

CVE(CAN) ID: CVE-2022-21304
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 5.7.36 及之前版本和 8.0.27 及之前版本存在拒绝服务漏洞。攻击者可利用该漏洞通过多种协议访问网络破坏 MySQL Server，并在未经授权的情况下导致程序挂起或频繁崩溃（拒绝服务）。

链接：https://www.oracle.com/security-alerts/cpujan2022.html

建议：

厂商补丁：

Oracle

Oracle 已经为此发布了一个安全公告（cpujan2022）以及相应补丁：

cpujan2022：Oracle Critical Patch Update Advisory - January 2022

链接：https://www.oracle.com/security-alerts/cpujan2022.html

➢ IBM Cognos Controller XML 外部实体注入漏洞

发布日期：2022-01-21

更新日期：2022-03-30

受影响系统：

IBM IBM Cognos Controller 10.4.2

IBM IBM Cognos Controller 10.4.1

IBM IBM Cognos Controller 10.4.0

描述：

CVE(CAN) ID: CVE-2020-4875

IBM Cognos Controller 是美国 IBM 公司的一套商业智能与计划解决方案。该产品具有流程自动化、财务审计控制、创建和管理财务报告等功能。

IBM Cognos Controller 10.4.0、10.4.1 和 10.4.2 版本存在 XML 外部实体注入漏洞。远程攻击者可利用该漏洞泄露敏感信息或消耗内存资源。

链接：https://exchange.xforce.ibmcloud.com/vulnerabilities/190838

建议：

厂商补丁：

IBM

IBM 已经为此发布了一个安全公告（190838）以及相应补丁：

190838：IBM Cognos Controller XML external entity injection

链接：https://exchange.xforce.ibmcloud.com/vulnerabilities/190838

六、本期网络安全事件

➢ 因供应商遭受网络攻击 丰田汽车停止日本所有工厂运转

2022 年 2 月 28 日，由于一家主要供应商遭受到网络攻击，丰田汽车将于 3 月 1 日关闭其在日本的所有工厂。据悉，供应商受到网络攻击已经导致零部件供应管理系统停止运行。丰田方面仍在研究 3 月 2 日之后能否恢复正常运营。本次受到网络攻击的供应商是为丰田提供塑料零配件的小岛工业(Kojima Industries)。一名接近小岛工业的人士告诉记者，“我们确实受到了某种网络攻击，目前遭受损失的程度还在统计中，将会尽快做出回应，首要任务是尽快恢复丰田的生产系统。

丰田方面拒绝就此置评：3 月 1 日丰田关闭所有日本国内工厂后，将影响约 1 万辆汽车的生产，约占丰田在日本国内月产量的 5%。据丰田汽车官网，丰田汽车在日本共拥有 16 座工厂。

此前，丰田曾多次因供应链问题而停产。2021 年下半年以来，丰田汽车多次因芯片短缺而宣布减产或停产。2021 年 10 月，丰田停产了日本的 14 家工厂共 27 条生产线;2022 年 1 月，丰田汽车宣布将于今年 2 月暂停日本国内 8 家工厂的 11 条生产线。据丰田汽车 2022 财年第三财季(2021 年 10 月-12 月)财报，丰田汽车 2022 财年第三财季营收为 7.786 万亿日元(约合人民币 4270 亿元)，同比下降 4.5%;营业利润为 7843.7 亿日元(约合人民币 430 亿元)，同比下跌 20.6%。丰田方面在财报中表示，受供应链影响，丰田将 2022 财年的年度产量目

标从此前的 900 万辆削减到了 850 万辆。（来源：澎湃新闻）

➢ 美国芯片巨头英伟达 确认遭黑客入侵致数据泄露

2022 年 3 月 2 日，美国芯片巨头英伟达公司日前证实，公司电脑网络遭到黑客攻击，一些重要信息被盗，目前黑客正在网络上泄露这些盗取的数据。此外，黑客这次攻击的动机十分不寻常。

英伟达通过一份声明表示：根据公司目前了解的情况，外部黑客获取了员工的账号密码信息，进入了系统，他们从公司系统中盗取了一些专有的机密信息，并且在网络上泄露。

英伟达表示，该公司团队正在分析这些被盗走的信息，不过初步估计，这次黑客攻击事件预计不会对公司的业务，以及服务客户的能力造成干扰。该公司表示，他们是在 2 月 23 日第一次发现了这次黑客攻击事件。

在加密移动聊天工具 Telegram 的一个频道中，一个网络黑客犯罪集团已经公开对英伟达提出了勒索。一些网络安全专家介绍，这个名为“LAPSU$”的黑客集团在南美洲和西欧地区都招募了成员。

美国一家财经媒体引述一位知情人士报道称，这次黑客攻击属于所谓的“勒索软件攻击”。在这种攻击类型中，黑客可能会在被攻击的系统中安装加密软件，导致对方无法读取数据，

随后黑客会提出消除加密软件的赎金要求。

不过英伟达方面表示，目前尚未发现内部网络中部署了恶意软件。相反，黑客直接盗走了重要数据，然后威胁公开这些重要信息，他们提出的条件是英伟达取消对一些显卡产品施加的限制，这些限制影响了对方利用显卡“挖掘”加密货币的效率。英伟达拒绝了黑客提出的沟通要求，随后他们开始披露这些被盗数据。（来源：财联社）

➢ 出售环球影城内测票骗取钱财 男子犯诈骗罪获刑！

2022 年 3 月 18 日，在网络发布虚假的北京环球影城内测票出售信息，收到钱款后就拉黑买家，先后骗取 7 名被害人钱财。近日，北京市石景山区人民法院以诈骗罪判处被告人林某某有期徒刑九个月，缓刑一年，并处罚金 1 万元。

2021 年，在北京环球影城试运营期间，许多人愿意在网上花高价“求票”。林某某看到这种情形动了心思，在微博上发布信息，谎称自己有环球影城内测票出售，吸引买家。交易谈拢后，林某某将李某某(另案处理)制作的虚假收款链接发给被害人，被害人通过虚假收款链接支付完钱款后，就被林某某拉黑，被害人并未得到北京环球影城的内测门票。

据了解，林某某通过上述方式共骗取毛某某等人 18996 元。2021 年 9 月 24 日，林某某被民警抓获，后其家属代为赔偿了被害人的全部损失。

石景山法院经审理认为，被告人林某某伙同他人以非法占有为目的，通过网络发布虚假

信息骗取被害人财物，数额较大，其行为已构成诈骗罪，依法应予惩处。鉴于林某某到案后能如实供述犯罪事实，自愿认罪认罚签署具结书，且能积极赔偿被害人经济损失取得谅解，系初犯，故依法可对其从轻处罚，并依法适用缓刑。据此，石景山法院以诈骗罪对林某某作出了如上判决。

法官提示：当前，时常有热门景点、演出等休闲娱乐活动火爆到“一票难求”，社交媒体、二手交易网站等便利了大家“出票”“求票”的迫切需求，有的不法分子把握买家心理，趁机骗取钱财，事情一旦败露，就拉黑了之。

法官提醒：游客在购买景点门票时，务必要选择正规的购票渠道，尤其是热门景点，网络上的转卖信息常常“鱼龙混杂”。如果选择进行二手交易，一定要选择实名认证且依托第三方支付平台的交易网站，并保存好相关的聊天记录、付凭证等。一旦发现被骗，拨打 110 报警求助，用法律武器维护自己的合法权益。一些怀有侥幸心理的卖家，觉得拉黑买家，自己“隐藏”在网络背后，就不会被追究责任，殊不知网络不是法外之地，只要在网络上进行了交易，必定会留痕，终将被追究法律责任。

法条链接：中华人民共和国刑法：第二百六十六条 诈骗公私财物，数额较大的，处三年以下有期徒刑、拘役或者管制，并处或者单处罚金;数额巨大或者有其他严重情节的，处三年以上十年以下有期徒刑，并处罚金;数额特别巨大或者有其他特别严重情节的，处十年以上有期徒刑或者无期徒刑，并处罚金或者没收财产。来源（来源：法制日报）

➢ 三星内部员工窃取数百份商业机密信息文件 被捕

2022 年 3 月 24 日，据多家韩媒报道，三星电子最近发现其 DS 代工部门一名员工涉嫌信息泄露，并对此案展开调查。据悉，这是一名计划离职的员工，在家办公时，疑似访问了公司的机密信息：与半导体相关的电子文件，并对文件内容进行了拍摄。而三星数据库系统是禁止员工使用智能手机拍摄来获取机密信息。

三星电子根据《产业保护技术法》，于 22 日向国家情报院举报了这一事实。目前，该员工已被拘捕。昨天，三星电子已经证实，正在对此案进行调查，但没有提供相关细节。**公司发言人表示：**“此人因违反信息保护规则正在接受调查。但目前尚不清楚被盗信息的类型以及该员工是否将其交给了第三方。”经调查，该员工承认其通过手机拍下了相关敏感信息的行为。

据多家媒体报道，该员工拍摄了数百份商业机密文件，有网友推测这些信息可能是为了提供给竞争对手而被窃取的。这名员工所在的代工部门，隶属于三星电子半导体事业暨装置解决方案(DS)部门下属的，晶圆代工事业部，2021 年 12 月庆桂显出任 DS 部门新领导。庆桂显上任后，就有相关消息报道，他要进行组织变革，在晶圆代工事业部下设立企业企划小组，专门进行统筹控制。南韩业界认为，此次的组织变革，三星已蓄谋已久，这是提升三星系统半导体竞争力的重要一环。三星的目标是在 2030 年成为全球系统半导体龙头，此前，三星一直积极地在半导体领域进行持续地投资。

除了此次内部员工涉嫌泄密，此前，三星电子多次遭到外部网络攻击而导致公司机密数据泄露，对公司造成重大损失。

2022 年 3 月 7 日，三星电子表示，Galaxy 手机源代码遭黑客入侵，导致内部公司数据泄露，包括 Galaxy 智能手机的运行源代码。之后，黑客组织 LAPSUS$声称已取得访问三星电子数据的权限，并在他们的 Telegram 频道上发布了一份 190GB 的种子文件，里面有暴露三星电子设备安全系统的机密源代码，包括三星电子智能手机生物认证算法和绕过部分操作系统控制的 Bootloader 源代码。

2020 年 2 月 5 日， 三星电子证实发生手机用户隐私交叉泄露，多位三星电子智能手机用户对科技媒体报告称，在上周四智能手机上收到了神秘推送通知之后，他们发现手机系统向他们展示了陌生人的个人数据。这个现象导致许多三星电子用户误认为三星的后台系统已经被黑客入侵，他们赶紧登录其网站更改密码。随后，三星承认确实发生了数据泄

露问题。

2018 年 12 月，三星电子因曲面屏技术泄露导致公司在未来 3 年内销售额损失 58 亿美元，利润损失 8.9 亿美元。（来源：集微网）

➢ 意大利铁路系统遭黑客攻击 多地车站受影响

2022 年 3 月 23 日，当地时间意大利铁路系统受到黑客攻击，多地火车站受影响。意大利铁路公司表示，目前没有证据表明攻击来源。

罗马火车站屏幕提示出现故障当地时间 3 月 23 日上午，意大利首都罗马特米尼火车站受到黑客攻击，直到 24 日上午该车站电子信息显示屏仍只能显示部分信息，造成许多旅客因信息不明而出现混乱。火车站安排工作人员使用扩音器为旅客指示方向并提供信息。23 日，米兰市多处火车站售票机也因黑客攻击出现故障，无法售票。

24 日凌晨，威尼斯圣卢西亚和梅斯特雷车站的信息系统出现了故障，且出现显示屏信息与列车实际运行不符的情况。目前该车站售票处关闭、售票机无法正常工作，有旅客称网上购票时也遇到困难。但意大利铁路公司尚未说明此次故障是否与 23 日网络攻击有关。

意大利铁路公司称：正在与意大利国家网络安全机构和警方密切合作，调查此次事故。（来源：央视新闻）

➢ 两成网民遭遇个人信息泄露，如何整治数据安全“重灾区”？

2022 年 3 月 15 日，根据中国信息通信研究院日前发布的《中国信息消费发展态势报告》显示，在消费群体方面，我国网民规模持续扩大突破十亿。《报告》同时也提示警惕数据安全、个人信息泄露等风险。

个人信息保护法实施以来，甘肃、江苏等地公安机关就已破获多起侵犯公民个人信息犯罪的案件。甘肃省灵台县公安局不久前刚刚打掉一个全链条网上购销公民个人信息的犯罪团伙。犯罪嫌疑人闫某某和胡某某利用经营店铺，骗取用户身份信息和手机号，非法注册各类网络账号，这些网络账号最终都落入“网上号商”的犯罪团伙手中。警方发现这两名嫌疑人背后还隐藏着一个犯罪团伙。今年 2 月到 3 月，专案组转战重庆、四川、云南，抓获 7 名侵犯公民个人信息犯罪团伙成员。该团伙从 2019 年起组建微信群非法买卖公民个人信息，他们利用通信业务代理商身份，以赠送礼品、话费等方式为诱饵，骗取用户个人信息后注册各类网络账号，以每个账号 3 元至 20 元价格出售，非法获利近十万元。

江苏警方近日也破获一个贩卖公民个人信息的犯罪团伙。该团伙主要贩卖股民和学生的信息，他们把个人信息称作“料子”。“股民料子”包括炒股者姓名、手机号、交易所等信息；“学生料子”则包含家长姓名、电话、孩子就读学校等。“料子”还分手拨料子和 AI

料子。手拨料子通过人工拨打，确认过真实性和可靠性。AI 料子则是嫌疑人通过软件随机生成的电话号码，没有其他身份信息。经审查，从 2018 年至今，该团伙贩卖公民个人信息 20 余万条，获利 20 余万元。

中国互联网络信息中心《第 49 次中国互联网络发展状况统计报告》显示，截至 2021 年 12 月，有 22.1%的网民遭遇个人信息泄露。公安机关提醒广大群众不要点击、使用来源不明的链接、网站、手机 APP，更不能将短信验证码提供给他人，严防信息泄露。

部分手机 APP 后台监视用户

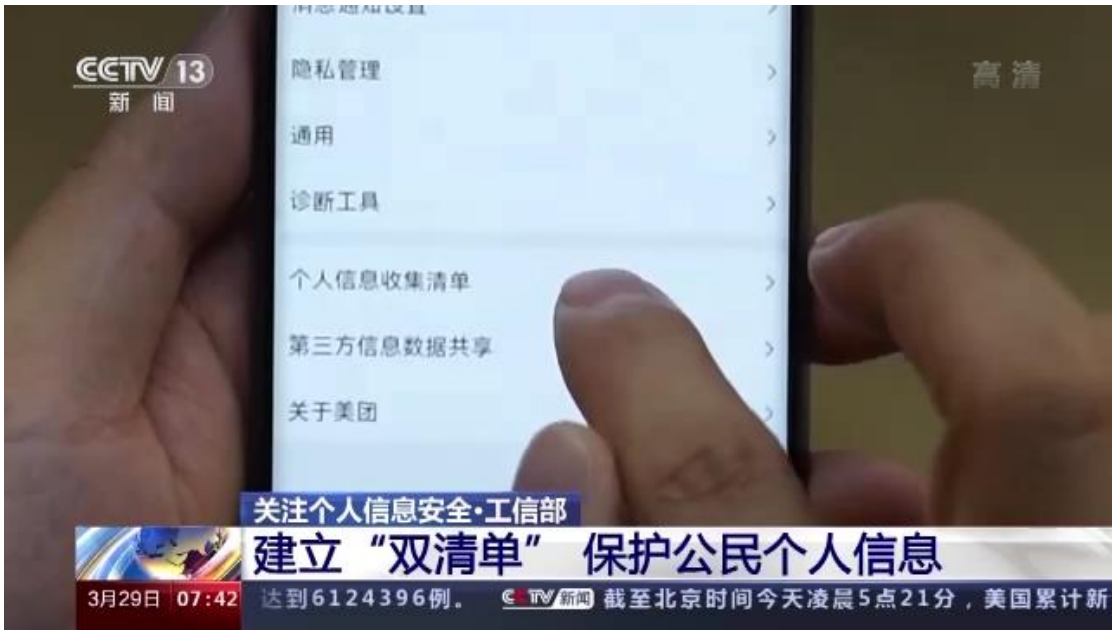
随着个人信息保护法的实施，加强个人信息保护，拒绝个人隐私在互联网上“裸奔”已经有法可依。但仍有不少用户觉得自己处在手机 APP 的监视下。很多网友都有过这种经历，在网上看了某个物品或输入一个关键词，很快就会收到手机 APP 推送的相关广告或信息。这是怎么回事呢？

在一家网络安全机构，技术人员用检测工具对两款手机浏览器收集用户信息行为进行了测试。技术人员复制了一个模拟的银行账号密码，尽管此时并没有使用浏览器，但检测工具却在浏览器调用的一段程序中发现了那个银行账号密码。**网络安全工程师 吕石奎：**这款 APP 读取了我们复制的银行卡号和密码。它拿走的这个过程，实际是明文拿走，并没有做相关的加密处理。

技术人员接着又在手机上选择了测试用的电话号码和短信，并把浏览器转入后台运行，这两次操作的内容同样被浏览器读取，包括在电商平台上浏览的商品信息也被两款被测试浏览器完整记录。其中一款浏览器在进程被关闭的状态下，仍然能够记录用户行为。

建立“双清单” 保护公民个人信息

为了让用户清晰掌握手机 APP 调用和索取个人信息的活动，工信部此前就提出要建立个人信息保护的“双清单” 。专家指出，手机 APP 在正常使用过程中会出现调用个人信息和索取权限的活动，不同手机 APP 之间有时也需要共享位置、通讯录等敏感信息，这增加了个人信息保护的监管难度。为了让用户清晰掌握个人信息在手机 APP 及第三方间共享的情况，工信部提出建立个人信息保护“双清单”，要求相关企业建立已收集个人信息清单和与第三方共享个人信息清单。



中国信息通信研究院泰尔终端实验室信息安全部主任 宁华：要求企业在“二级菜单”中简洁、清晰列出“第三方共享个人信息清单”，包括与第三方共享的个人信息种类、使用目的、使用场景和共享方式等。

多措施整治违规收集使用个人信息等行为

为了治理 APP 违规收集使用个人信息和欺骗诱导用户提供个人信息等问题， 工信部委托中国信息通信研究院联合互联网、手机终端、电信运营商等产业链各环节成立 APP 用户权益保护标准工作组，按照“知情同意”和“最小必要”原则组织制定了《APP 收集使用个人信息最小必要评估规范》《APP 用户权益保护测评规范》等标准，明确了检测要求和方法，为监管提供了更加明确的监管依据。

记者从工信部了解到，首批主要互联网企业已经在去年年底基本完成个人信息保护“双清单”的设置。在某款手机 APP 上，用户点开菜单就可以查看这个 APP 已经收集的用户个人信息种类、使用目的、使用场景以及与第三方共享的个人信息和共享方式等。手机

终端企业也按照工信部要求开发了 APP 权限最小化推荐等功能，主动对手机上的 APP 过度索取权限行为做出规范和限制。

电信运营商则通过区块链技术的防窜改特性来追踪防范个人信息泄露风险。**电信运营商信息安全中心负责人 温暖：**我们会将操作日志的数据特征上区块链，确保它不能被窜改，同时再定期进行校验。如果日志一旦被窜改就说明存在问题。我们就会以风险的方式核查具体的事件。据了解，工信部通过制定标准、技术检验、专项整治、行业自律等措施，大力整治违规收集使用个人信息等侵害用户权益行为。去年累计检测 208 万款 APP，通报 1549 款违规 APP，对 514 款拒不整改的 APP 进行下架处理。（来源：央视新闻）