国家网信办发布近期网络安全、数据安全、个人信息保护相关执法典型案例

近段时间以来，全国网信系统认真贯彻落实《网络安全法》《数据安全法》《个人信息保护法》《网络数据安全管理条例》等法律法规，持续加大网络安全、数据安全、个人信息保护相关执法工作力度，各地网信部门依法查处一批涉网页篡改、数据泄露、违法违规处理个人信息、新技术新应用未经评估上线等违法违规案件。现将典型案例发布如下。

1.广东某科技股份有限公司网页篡改案。网信部门工作发现，该企业用于业务审批等的办公协作平台登录页面被篡改为违法有害内容。经查，该企业涉事系统存在任意文件上传漏洞，遭受勒索软件攻击，该企业当天发现后仅重装系统，未修复系统漏洞。其后，攻击者利用该漏洞上传远程控制木马，将登录页面篡改为违法有害内容。该企业未依法履行网络安全保护义务，未采取必要技术措施保障网络安全，未及时修复系统漏洞，造成网页篡改后果，违反《网络安全法》相关规定。属地网信办已依法责令其改正，并予以警告、罚款处罚。

2.新疆某互联网科技有限公司网页篡改案。网信部门工作发现，该企业门户网站及开发运维的 8 个网站子页面被篡改为涉赌违法信息。经查，该企业上述网站存在安全缺陷和漏洞，相关网页源代码 php 文件被恶意篡改，出现涉赌违法信息。事件发生时，网站管理员休假不在岗，网站处于无人管理状态。该企业作为网络产品、服务提供者，未及时发现其开发的网站存在安全缺陷和漏洞，未立即采取补救措施，未按照规定及时告知用户并向主管部门报告，违反《网络安全法》相关规定，属地网信办已依法责令其改正，并予以警告处罚。

3.山东某医学检验有限公司数据泄露案。网信部门工作发现，该企业某系统相关数据被搜索引擎爬虫爬取。经查，涉事系统开启目录

浏览功能，存在目录遍历和未授权访问漏洞，未正确配置防火墙入侵防护策略，未按照规定留存相关网络日志。相关搜索引擎爬虫通过遍历请求爬取了网站组织架构和文件，导致系统相关数据泄露。该企业未依法履行网络安全、数据安全保护义务，涉事系统未依法留存相关网络日志，未采取技术措施和其他必要措施保障数据安全，造成数据泄露后果，违反《网络安全法》《数据安全法》《网络数据安全管理条例》等法律法规规定。属地网信办已依法责令其改正，并予以警告、罚款处罚。

4.浙江某科技股份有限公司数据被窃取案。网信部门工作发现，该企业 FTP 系统相关数据被窃取。经查，该企业为方便共享、打印系统文件，将涉事系统设置为允许匿名访问，并设置云服务器安全组规则不生效，长期存在未授权访问漏洞，导致涉事系统相关数据被窃取。该企业未依法履行网络安全、数据安全保护义务，涉事系统未采取技术措施和其他必要措施保障数据安全，造成数据被窃取后果，违反《网络安全法》《数据安全法》《网络数据安全管理条例》等法律法规规定。属地网信办已依法责令其改正，并予以警告、罚款处罚。

5.重庆某科技公司数据被窃取案。网信部门工作发现，该企业用于汽车租赁服务的“OA 信息系统”相关数据被窃取。经查，该企业涉事系统 3306 端口开放 MySQL 数据库服务，未设置用户密码，存在弱口令漏洞，导致涉事系统相关数据被先后窃取 159 次。该企业未依法履行网络安全、数据安全保护义务，涉事系统未采取技术措施和其他必要措施保障数据安全，造成数据被窃取后果，违反《网络安全法》《数据安全法》《网络数据安全管理条例》等法律法规规定。属地网信办已依法责令其改正，并予以警告、罚款处罚。

6.广东某保险代理有限公司数据被窃取案。网信部门工作发现，该企业提供保险代理服务的后台系统相关数据被窃取。经查，该企业涉事系统存在越权遍历访问漏洞，攻击者可通过遍历 URL ID 的方式批量获取数据，且该企业购买的云防火墙服务已过期，未按照规定留存相关网络日志，导致涉事系统相关数据被窃取。该企业未依法履行

网络安全、数据安全保护义务，涉事系统未依法留存相关网络日志，未采取技术措施和其他必要措施保障数据安全，造成数据被窃取后果，违反《网络安全法》《数据安全法》《网络数据安全管理条例》等法律法规规定。属地网信办已依法责令其改正，并予以警告、罚款处罚。

7.湖南某科技股份有限公司数据存在泄露安全风险案。网信部门工作发现，该企业内网数据库相关数据存在泄露安全风险。经查，该企业内网数据库存在未授权访问漏洞和弱口令漏洞，某软件研发工程师为工作便利，将合作项目中掌握的大量用户数据拷贝至企业内网数据库，并打开企业内网的公共互联网访问端口，导致内网数据库相关数据暴露在互联网上。该企业未依法履行网络安全、数据安全保护义务，未建立网络安全和数据安全管理制度，涉事系统未采取技术措施和其他必要措施保障数据安全，存在数据泄露安全风险，违反《网络安全法》《数据安全法》《网络数据安全管理条例》等法律法规规定。属地网信办已依法责令其改正，并予以警告、罚款处罚。

8.北京某科技有限公司运营的 App 超范围收集个人信息案。网信部门工作发现，该企业运营的 App 违反必要原则，收集与其提供的服务无关的个人信息。经查，该企业开发的 App 在用户未使用任何功能情况下，后台运行时收集上传用户应用程序安装、卸载信息。用户使用上传 AI 头像等功能时，调用非必要存储权限。相关行为超出了实现个人信息处理目的最小必要范围，违反《网络安全法》《个人信息保护法》《网络数据安全管理条例》等法律法规。属地网信办已依法责令其改正，并予以警告、罚款处罚。

9.上海某科技有限公司违法违规收集人脸信息案。网信部门工作发现，该企业运营的自动售货机存在违法违规收集人脸信息等问题。经查，该企业运营的自动售货机在用户支付环节存在未经同意收集人脸信息等问题，同时该企业存在未建立个人信息保护影响评估制度、相关系统存在 SQL 注入高危漏洞等问题，违反《网络安全法》《个人信息保护法》《网络数据安全管理条例》等法律法规规定。属地网信办已依法责令其改正，并予以警告处罚。

10.浙江某科技有限责任公司运营的 App 提供深度合成服务未按规定进行安全评估案。网信部门工作发现，该企业运营的 App 提供 AI 换脸服务未按规定进行安全评估。经查，该企业运营的 App 是一款深度合成类服务产品，提供视频换脸、图片换脸、照片舞动配音等图片处理功能，用户可对上传图片、视频中的人物进行换脸，但未按规定落实安全评估要求，相关深度合成内容也未作显著标识，存在较大安全风险，违反《互联网信息服务深度合成管理规定》《生成式人工智能服务管理暂行办法》《互联网信息服务算法推荐管理规定》《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》等规定。网信部门已依法责令移动应用程序分发平台依规依约对该 App 予以下架处置。

国家网信办有关负责人表示，网络空间已经成为人们生产生活的新空间，让互联网在法治轨道上健康运行是全社会的共同责任。网信部门将认真贯彻习近平新时代中国特色社会主义思想，特别是习近平法治思想和习近平总书记关于网络强国的重要思想，深入推进依法治网，依法查处相关违法违规行为，切实维护国家网络安全、数据安全，保护人民群众合法权益。

文章来源：“网信中国”微信公众号