

**2019年3月04日第187期**

**国盟信息安全通报**

（**第187期**）

**国际信息安全学习联盟**

**2019年3月04日**

国家信息安全漏洞共享平台（以下简称CNVD）本周共收集、整理信息安全漏洞194个，其中高危漏洞48个、中危漏洞127个、低危漏洞19个。漏洞平均分值为5.60。本周收录的漏洞中，涉及0day漏洞37个（占19%），其中互联网上出现“HotelDruid跨站脚本漏洞、LibRaw'copy\_bayer'函数空指针逆向引用漏洞”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2374个，与上周（1058个）环比增长1.24倍。

**主要内容**

[一、概述 4](#_Toc2345116)

[二、安全漏洞增长数量及种类分布情况 4](#_Toc2345117)

[漏洞产生原因（2019年2月18日—2019年3月04日） 4](#_Toc2345118)

[漏洞引发的威胁（2019年2月18日—2019年2月04日） 5](#_Toc2345119)

[漏洞影响对象类型（2019年2月18日—2019年3月04日） 5](#_Toc2345120)

[三、安全产业动态 6](#_Toc2345121)

[全国开展APP专项治理的背后审议 6](#_Toc2345122)

[2018年中国网络安全大事件 8](#_Toc2345123)

[2019国家数据治理方法前瞻 12](#_Toc2345124)

[把握新一代信息技术的聚焦点 18](#_Toc2345125)

[四、政府之声 22](#_Toc2345126)

[CNNIC发布第43次《中国互联网络发展状况统计报告》 22](#_Toc2345127)

[扫黄打非办公室部署开展“净网2019”“护苗2019”“秋风2019”专项行动 24](#_Toc2345128)

[工信部：多家互联网企业因用户信息问题被督促整改 25](#_Toc2345129)

[2018年上海市网络安全态势分析年度报告发布 25](#_Toc2345130)

[五、本期重要漏洞实例 27](#_Toc2345131)

[关于WinRAR存在系列远程代码执行漏洞的安全公告 27](#_Toc2345132)

[多款IBM产品任意文件下载漏洞 27](#_Toc2345133)

[Cisco SPA112/SPA525/SPA5X5 Series信息泄露漏洞 28](#_Toc2345134)

[Adobe Acrobat/Reader信息泄露漏洞 29](#_Toc2345135)

[六、本期网络安全事件 30](#_Toc2345136)

[瑞典医疗热线泄露270万条通话记录：涉及诸多敏感信息 30](#_Toc2345137)

[国内某人脸识别公司数据泄露 超250万人数据可被获取 31](#_Toc2345138)

[买黑客软件侵入快递公司窃取1.5G个人信息，作案者被判三年 32](#_Toc2345139)

[违规搜集儿童隐私，抖音国际版在美被罚570万美元 33](#_Toc2345140)

[自如员工被控窃取公司信息七万条涉侵犯公民信息罪受审 35](#_Toc2345141)

[倒卖明星隐私链条被曝光 律师:造成严重后果或被追责 36](#_Toc2345142)

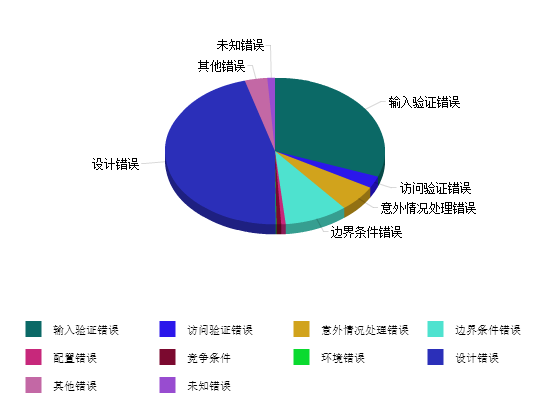
**注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。**

# 概述

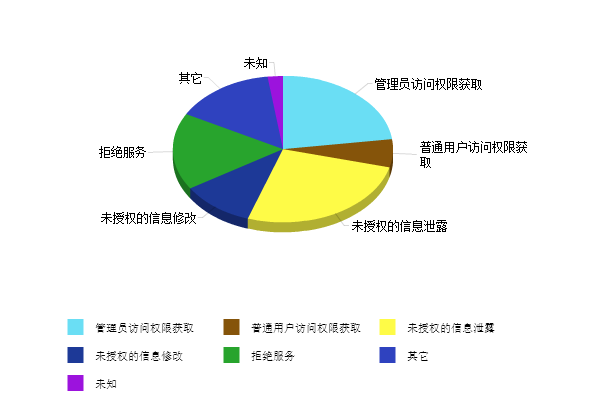
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称CNVD）本周共收集、整理信息安全漏洞194个，其中高危漏洞48个、中危漏洞127个、低危漏洞19个。漏洞平均分值为5.60。本周收录的漏洞中，涉及0day漏洞37个（占19%），其中互联网上出现“HotelDruid跨站脚本漏洞、LibRaw'copy\_bayer'函数空指针逆向引用漏洞”等零日代码攻击漏洞。本周CNVD接到的涉及党政机关和企事业单位的事件型漏洞总数2374个，与上周（1058个）环比增长1.24倍。

# 安全漏洞增长数量及种类分布情况

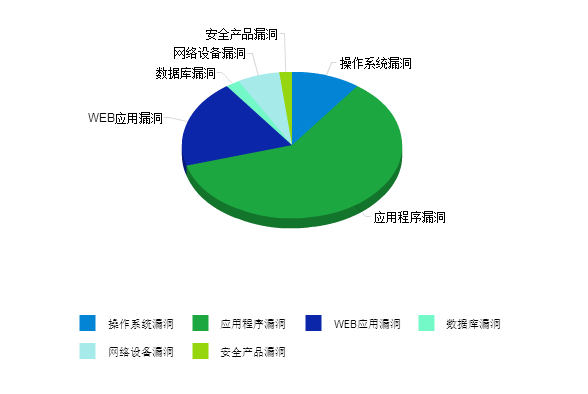
## 漏洞产生原因（2019年2月18日—2019年3月04日）



## 漏洞引发的威胁（2019年2月18日—2019年2月04日）



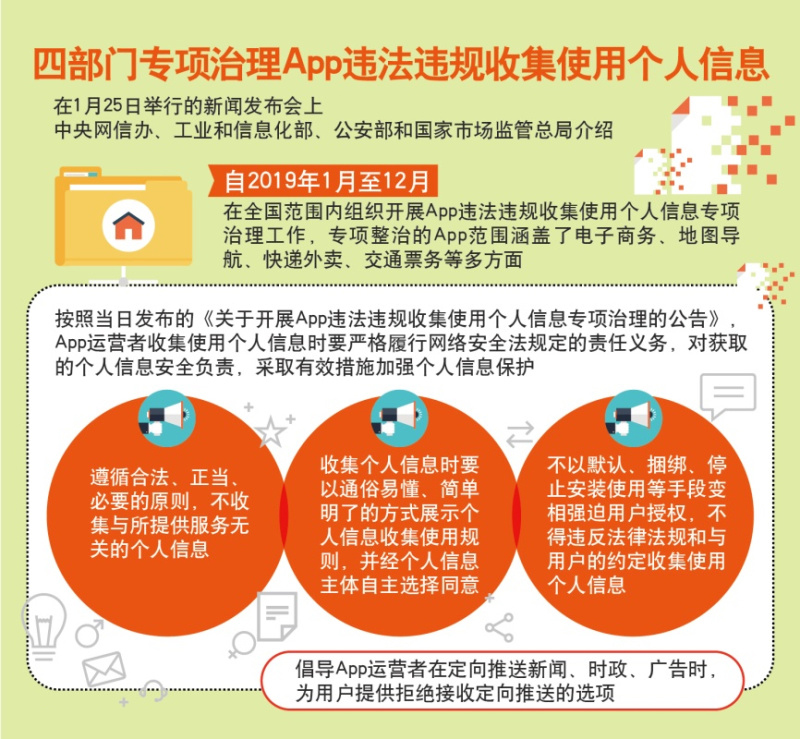
## 漏洞影响对象类型（2019年2月18日—2019年3月04日）



# 安全产业动态

## 全国开展APP专项治理的背后审议

近日，中央网信办、工业和信息化部、公安部、国家市场监管总局联合发布了《关于开展APP违法违规收集使用个人信息专项治理的公告》（以下简称《公告》），将在全国范围内组织开展APP（应用程序）违法违规收集使用个人信息专项治理行动。专家指出，调用多部门力量的专项行动，彰显出政府部门向APP手机客户端违法违规收集个人信息“亮剑”的决心。



**响应呼声，个人信息有保障**

对很多手机用户来说，APP早已成为生活中难以替代的一部分，衣食住行都可囊括其中，APP也在助力社会发展、服务民生等方面发挥了重要作用。对于APP来说，的确需要获取一些用户的基本数据才能正常运行，比如地图类APP需要开启位置权限、摄影类APP需要开启相机权限，但是除此之外，哪些信息不应被采集，需要有一条规范而明确的边界。

四部门此次发布的公告，明确了APP信息收集的边界在哪里，并建立起了严格的约束机制，相当于APP的“紧箍咒”，为用户的利益和安全保驾护航。中央网信办网络安全协调局副局长杨春艳表示，希望通过此次专项治理，对个人信息保护建立长效的监管机制，并持续加大个人信息保护力度。

《公告》要求，APP运营者收集使用个人信息时，不得收集与所提供服务无关的个人信息；“收集个人信息时要以通俗易懂、简单明了的方式展示个人信息收集使用规则，并经个人信息主体自主选择同意；不以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得违反法律法规和与用户的约定收集使用个人信息。”这意味着，在此之前令不少用户无可奈何的“不多开权限不给用”等违规条款必须立刻整改，APP市场也会得到有效净化。

**专业评估，涉及千款APP**

在这次专项治理之中，全国信息安全标准化技术委员会、中国消费者协会、中国互联网协会、中国网络空间安全协会也被安排了一份重点工作：依据法律法规和国家相关标准，编制大众化应用基本业务功能及必要信息规范和APP违规收集使用个人信息治理评估要点。组织相关专业机构，对用户数量大、与民众生活密切相关的APP隐私政策和个人信息收集使用情况进行评估。今年年底前，此次专项治理将完成千款用户规模大、社会关注度高的APP评估工作。



与百姓生活息息相关、用户意见反映强烈的APP，是此次评估工作的重点，涵盖了地图导航、即时通讯、网络支付、网上购物等常用软件。据全国信息安全标准化技术委员会秘书长杨建军介绍，APP选取范围不限操作系统的类型、不限应用商店的平台、不限行业领域、也不限APP运营者的性质。

据了解，四组织将委托专业的测试评估机构，依据规范对APP进行评估，重点对APP超范围收集个人信息、过度索权、强制捆绑授权和违法违规使用个人信息等进行评估，对评估结果确认存在重大问题的，将报送相关部门，为相关部门依据《网络安全法》、《消费者权益保护法》等法律法规开展监管执法等提供参考。

**划下红线，用户使用更安心**

这个时代，手机很可能比用户自己还要“了解”自己，保护用户隐私刻不容缓。这次的专项治理行动就划下了一条区分“可以”和“不可以”的红线，旨在帮助存在不足的APP完成改进，将严重违规的APP清理出市场，让用户使用起来更安心。

《公告》强调，要加强对违法违规收集使用个人信息行为的监管和处罚，“情节严重的，依法暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。”红线之下，也是为了引导行业实现自律，这要求APP运营者将用户的利益摆在心头，维护消费者的合法权益。

与此同时，在互联网用户信息安全越来越引发广泛关注的今天，对APP进行个人信息安全认证具有重要意义。《公告》指出，“开展APP个人信息安全认证，鼓励APP运营者自愿通过APP个人信息安全认证，鼓励搜索引擎、应用商店等明确标识并优先推荐通过认证的APP。”

据介绍，建立APP个人信息安全认证制度，将按照APP运营商自愿申请的原则，由具备资质的认证机构依据相关国家标准对APP收集、存储、传输、处理、使用个人信息等活动进行评价，符合要求的产品将被颁发安全认证证书，准许其使用相关认证标识。此举也是为了促进APP运营者进一步提升个人信息安全保护意识和保护能力，使APP消费市场得到净化。（来源：人民日报海外版）

## 2018年中国网络安全大事件

2019年2月20日，由中国计算机学会主办、中国计算机学会计算机安全专业委员会承办的2018年中国网络安全大事发布会在公安部一所举行。本次会议发布了结合专家组评选和线上投票遴选出的2018年中国网络安全大事。

**1. “净网2018”专项行动打击整治网络违法犯罪**

2018年2月7日，公安部部署全国公安机关从即日起至12月底，深入开展打击整治网络违法犯罪“净网2018”专项行动。专项行动要求强化清理整治，全面规范网络安全秩序，督促指导重点网站、网络服务商、信息服务商和联网单位严格落实信息安全管理责任，严格落实网络实名制等管理制度，依法查处一批“黑产”“黑市”，整治一批违法违规企业，清除一批违规有害应用服务，解决一批危害网络安全、滋生违法犯罪的基础性问题。



**2. 勒索软件持续入侵大型系统，造成严重后果**

2018年3月，湖北某医院内网遭到勒索病毒攻击，导致该医院大量的自助挂号、缴费、报告查询打印等设备无法正常工作;8月，台湾积体电路制造三大厂区出现电脑大规模勒索病毒事件，造成大量经济损失;9月，GlobeImposter勒索病毒入侵山东省10市不动产登记系统，造成系统暂定运行。在2018年国家网络安全宣传周期间，腾讯智慧安全正式发布《医疗行业勒索病毒专题报告》，报告指出在全国三甲医院中，有247家医院检出了勒索病毒，以广东、湖北、江苏等地区检出勒索病毒最多。

**3. 全国网络安全和信息化工作会议在京召开**

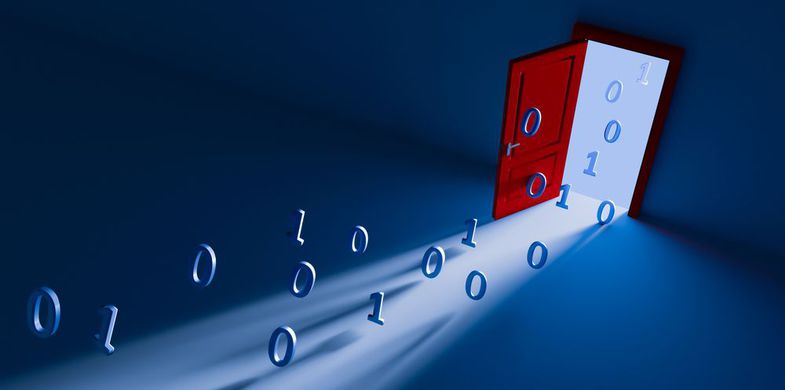
2018年4月20日，全国网络安全和信息化工作会议召开，习近平总书记出席作重要讲话。习近平总书记强调，信息化为中华民族带来了千载难逢的机遇。我们必须敏锐抓住信息化发展的历史机遇，加强网上正面宣传，维护网络安全，推动信息领域核心技术突破，发挥信息化对经济社会发展的引领作用，加强网信领域军民融合，主动参与网络空间国际治理进程，自主创新推进网络强国建设，为决胜全面建成小康社会、夺取新时代中国特色社会主义伟大胜利、实现中华民族伟大复兴的中国梦做出新的贡献。

**4. 国家标准《信息安全技术 个人信息安全规范》正式实施**

2018年5月1日，国家标准《信息安全技术 个人信息安全规范》(GB/T 35273-2017)正式实施。《规范》以国家标准的形式，明确开展收集、保存、使用、共享、转让、公开披露等个人信息处理活动应遵循的原则和安全要求，可以为互联网企业处理用户个人信息提供指导和规范。

**5. 网上公民个人信息泄露频频发生**

2018年以来，国内多家机构疑似发生个人信息泄露事件。6月13日，知名视频播放网站A站(AcFun)遭遇黑客攻击，数据库近千万条用户数据发生泄露；6月14日，前程无忧数据库195万余条用户数据疑似泄露，但遭该公司声明否认；8月1日，浙江省1000万条学籍数据疑似泄露，样本数据经核实与真实信息基本一致;8月28日，华住旗下酒店5亿条用户信息泄露；9月7日，江苏一高校学生信息泄露，疑被企业用于偷逃税款；12月31日，北京警方破获一起侵犯公民个人信息案，网上贩卖470余万条疑似12306铁路订票网站用户数据的犯罪嫌疑人陈某被刑拘。



**6. 公安部发布《网络安全等级保护条例(征求意见稿)》**

2018年6月27日，公安部发布了会同有关部门起草的《网络安全等级保护条例(征求意见稿)》。此条例征求意见稿要求网络安全等级保护工作应当按照突出重点、主动防御、综合防控的原则，建立健全网络安全防护体系，重点保护涉及国家安全、国计民生、社会公共利益的网络的基础设施安全、运行安全和数据安全。征求意见稿拟将网络分为五个安全保护等级，要求网络运营者依法开展网络定级备案、安全建设整改、等级测评和自查等工作，采取管理和技术措施，保障网络基础设施安全、网络运行安全、数据安全和信息安全，有效应对网络安全事件，防范网络违法犯罪活动。

**7. 首届网民网络安全感满意度调查活动在全国开展**

2018年8月27日，2018全国网民网络安全感满意度调查活动正式启动。本次调查活动由80多家网络安全社会组织共同发起，主题为“网络安全为人民，网络安全靠人民”，调查结果在2018年国家网络安全宣传周法治日活动上首次发布。本次调查动员了全国各省的信息安全协会参与组织实施，范围覆盖全国所有省、市、自治区，是国内首次对网络安全满意度进行如此大规模的公开调查，本次调查活动参与人数量多，组织类型全面。活动着眼于反映广大民众对于网络安全态势的感受，积极宣传网络安全，提高网络治理成效，成绩可喜。

**8. 《公安机关互联网安全监督检查规定》正式施行**

2018年11月1日，《公安机关互联网安全监督检查规定》正式实施。根据规定，公安机关将根据网络安全防范需要和网络安全风险隐患的具体情况，对互联网服务提供者和联网使用单位履行法律、行政法规规定的网络安全义务情况开展监督检查。

**9. 国家网信办发布具有舆论属性的信息服务安全评估规定**

2018年11月15日，中国国家互联网信息办公室发布《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》，要求互联网信息服务提供者在特定情况下，按规定自行开展安全评估，并对评估结果负责。该规定自2018年11月30日起施行。对存在较大安全风险、可能影响国家安全、社会秩序和公共利益的互联网信息服务，省级以上网信部门和公安机关应当组织专家进行评审，必要时可以会同属地相关部门开展现场检查。

**10.《互联网个人信息安全保护指引(征求意见稿)》向社会征求意见**

2018年11月30日，公安部网络安全保卫局发布《互联网个人信息安全保护指引》(征求意见稿)，旨在深入贯彻落实《网络安全法》，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。

**11.多项国家重大会议和国际活动网络安保顺利完成**

2018年，全国两会、上合组织峰会、博鳌亚洲论坛、中非合作论坛北京峰会、第五届世界互联网大会、上海进口博览会等国家重大会议和国际活动顺利举办。期间，国内众多网络安全公司作为技术支持单位付出了巨大努力，保障了会议与赛事网络安全平稳运行，网络安全零事故发生。（来源：经济参考）

## 2019国家数据治理方法前瞻

诚如德国著名社会学家克里斯多夫·库克里克提出的“微粒社会”一般，数字化进程的加速，令我们进入人机互动、精细解析的时代，各国均面临数字化治理难题。技术的凸显令数据收集和处理变得极为高效，政治、经济以及社会关系等都以比之前更加精细、透彻的方式被获取、解析和评价，国家数据治理在政府规制和网络自由的平衡中，需探索一种由法律、规则以及代码协同的治理机制。



**一、数据治理的政策问题并非依赖“数据管控”单一手段**

2018年以来，以美国和欧盟为代表的数字经济体，纷纷在国家战略规划及行动中强调数据管控政策地位。美国于3月23日出台“澄清合法获取海外数据法”（CLOUD Act），并在9月份由总统特朗普签署的《国家网络战略》中明确提出“促进数据跨境自由流动战略”；欧盟则主导建立“欧洲单一数字市场战略”并于5月25日正式颁布实施 “通用数据保护条例”（GDPR）。美欧迥异的数据管控政策，令美国在欧4000多家企业特别是以谷歌、脸书等为代表的数字巨头受到欧洲监管机构数十亿美元的天价罚单。欧盟认为，在数字经济大潮中，欧盟28个成员国拥有5亿人的市场，没有理由再缺位，欧盟委员会测算称，“如果有利的政策和立法就位，欧洲数字经济将增长18倍”。然而欧盟单一的法律监管引发美国互联网巨头强烈反弹，2018年7月谷歌称“为符合欧盟今年推出的反垄断政策要求，当欧盟的安卓手机设备制造商要在手机上安装Gmail、Google Maps或其他受欢迎的谷歌系应用软件时，谷歌将对其收费”，另据纽约时报报道，“自2019年2月起，谷歌将对欧洲境内的安卓系统以及使用相关软件的公司进行收费，每台设备征收的费用为40美元”。

**（一）欧洲、亚太等地区数字经济体将强化“数字主权”**

数据作为社会主体“数字双胞胎”的载体，其生成、存储、复制、分发及交互的过程构成人类社会活动在网络空间的“镜像”。随着数据跨境流动，国际规则正从国家主体边域到数字主体国籍边域延伸，数据跨境流动存在“主权”和“安全”隐患。2018年美欧先后推出CLOUD Act和GDPR，加剧数据资源全球化竞争态势，从立法层面看，由于当前国际法缺乏洞见法律域外管辖问题的具体规则，美欧均对国际法域外管辖的“保护”原则进行扩张形成“长臂管辖”，数据主权呼声日渐。

伴随着第四次工业革命的到来，数据作为重要生产资料已成为广泛共识，目前全球有120个国家制定了数据保护政策，形成了六类较具代表性的数据跨境保护方案，数据主权全球轮廓日渐清晰。其一，明确要求数据必须存储在本地服务器的“强要求”国家，中俄是典型代表，同时包括文莱、印度尼西亚、尼日利亚和越南；其二，法律对数据传输的要求相当于数据本地化，即“事实要求”的地区以欧盟于2018年5月25日正式实施GDPR为标志；其三，诸多措施要求在跨境传输之前需征得数据主体同意形成的“部分要求”国家包括白俄罗斯、印度、哈萨克斯坦、马来西亚和韩国，印度储备银行于2018年10月15日要求印度产生的支付数据必须且仅能存储于印度本地，进一步凸显其对本地数据的管控力度；其四，在某些条件下限制跨境传输即“轻微要求”的国家有阿根廷、巴西、哥伦比亚、秘鲁、乌拉圭；其五，仅在特定领域如医疗、电信、金融及国家安全领域限制的“特定领域要求”国家和地区有澳大利亚、加拿大、新西兰、土耳其、委内瑞拉和中国台湾；其六，没有已知的数据本地化法律要求即“无要求”国家，以美国2018年3月23日出台的“澄清合法获取海外数据法” （CLOUD Act）为标志，其不但强调数据跨境流动的自由，并认为限制自由流动将影响数字经济发展，极力淡化“数字主权”概念。

**（二）数字市场呈现“强者愈强”，技术加速“两极分化”**

在数字领域，同样遵循“赢者通吃”的规则，只有少数玩家能够在这个行业中生存并占据主导地位，作为数字化强国的美国，谷歌、脸书、苹果、亚马逊等在全球搜索引擎、社交媒体以及人工智能等垂直领域主导架构并定义发展，如谷歌和亚马逊,通过从成千上万的远程客户端以及应用程序中吸收大规模数据流,获得更加专业的知识、更好的算法，并通过溢出效应获得无与伦比的人工智能能力。欧盟在全球数字经济排名并不靠前（落后于美国、中国、日本等），对欧洲而言，一方面其开放的互联网政策促进了全球互联网巨头的成长，而欧洲本土互联网电商OTTO、Zalando、搜索引擎nomade.tiscali等服务提供商仅获剩余市场的残羹冷炙，一旦欧洲实施监管，却旋即遭到美国巨头的报复性反击；另一方面，数字技术的大规模应用，使得高素质劳动者的效率明显提高 “强者愈强”，而处于低端领域如工业化领域的熟练操作工作以及简单的行政工作等终将被机器以及算法所取代。在经济发展缓慢的高福利社会环境下，此种分化更加明显，欧洲民众的不安情绪引发英国脱欧、“反建制”意大利五星运动党崛起、法国黄背心运动等继续加剧欧洲社会分裂，因而欧盟委员会意识到，绝对不能在第四次工业革命中缺位，欧洲建立“单一数字市场战略”势在必行。正如尤瓦尔·赫拉利在其《未来简史》中所提到的，我们拥有越多的数据，对历史了解越深入，历史的轨迹就改变得越快。

**（三）防控数据泄漏将成全球个人数据保护的立法规制重点**

随着数字化进程的加速，研究者提出“旨在防范公权力或他人打扰生活的‘隐私’概念在数字智能时代面临迭代更替，实现从个人隐私到个人数据的转变显得十分必要”，强调数据主体有效控制权的“个人数据”概念应运而生，环顾全球，各个国家的个人数据保护亦均建立在个人数据权利这一思想基础之上。研究人员通过分析发现，只要数据足够多，对个人的识别就是轻而易举之事，例如研究人员通过在苹果商店里下载的250亿个应用程序其中1/3都附带有地址数据，只要通过4条随机挑选的关于一天之内一个人在何处逗留的信息，就有95%的几率将个人识别出来。因而数字时代，人人都成“透明人”，并深陷巨大的“社会黑箱”之中，“黑箱”就如飞机上的黑匣子，可以将所有重要信息记录清楚，但我们只是信息的生产者，却不知道这些信息将被用于何处，会产生什么样的后果，特别对于由于数据泄漏行为而引发的数据滥用问题更显得力有不逮。过去五年，全球企业、政府乃至军方发生的数据泄露事件逐年上升、态势严峻，据Gemalto发布的《数据泄露水平指数(Breach Level Index）》统计，仅2018年全球就发生了1000多起较大规模的数据泄露事件，共计导致不少于70亿条个人数据泄露，相当于全球每位网民个人信息至少被泄漏1.5次。从成因来看，造成用户个人数据泄露的主要原因存在于三个方面，一是系统、软件、终端、平台等客观存在的各类漏洞，二是个人及企业的数据安全防护网络体系不完善、黑客的攻击技术手段日益多样，三是第三方未经授权的大量访问以及暗网黑市对数据市场的 “旺盛需求”。

**二、网络技术和第三方监督将持续推动个人数据保护能力提升**

斯坦福大学的劳伦斯·莱斯格教授在他的《代码2.0》一书中反复强调一个概念：代码即法律。“即有什么样的代码，就会有什么样的网络社会，决定权在代码手中；当现实社会的法律开始作用于网络空间，代码就越来越不是法律，反而法律开始影响网络的构架，开始影响一行行的代码。”

**（一）重启网络空间技术，强化平台对个人数据保护的责任**

一份调查报告指出，用户仅点击某一热门新闻网站的动作就会触发并激活350多个网络服务器，数字时代的“黑箱”无处不在。互联网的缔造者美国一贯主张，既要在国际范围内保护个人隐私，又不应阻碍个人数据的跨境流动，为此20世纪美国就涌现出许多自律组织，国际互联网联盟（W3C）即是其中一个。1994年10月，由万维网发明者蒂姆·伯纳斯·李（Tim Berners Lee）在麻省理工学院计算机科学实验室成立W3C，W3C开发、设计了“个人隐私选择平台”（P3P，Platform for Privacy Preferences）成为个人隐私权保护策略的一项推荐性技术标准，其能够使网络用户选择在浏览网页时，是否被第三方收集并利用自己的个人信息，如果一个站点不遵守P3P标准，那么有关它的Cookies将被自动拒绝，同时P3P还能够自动识别多种Cookies的嵌入方式。但遗憾的是，自2002年4月P3P被正式推荐以来，仅微软公司的IE浏览器一家选择采用该项技术，相对美国庞大的互联网市场，这一数据简直可以忽略不计。相信随着隐私强化技术（PETs）的不断推陈出新和个人信息保护法律的不断完善，互联网平台将大量采用开放的、可解释的算法决策工具来代替算法黑箱，为此方能加速数字社会变成显式社会。

**（二）第三方机构对个人数据保护的监督力度将不断加强**

对于个人信息将被用于何处，产生何种后果的问题，追本溯源需要从三类数据诉求进行分析。首先，政府层面关注的核心问题是利用大数据了解公民是否“违法犯罪”，因而公民个人行为应是政府层面关注的重点；再者，对商业公司或商业平台而言，他们更希望了解公民的上网数据，这样就能更加有效地进行定向产品推广或广告投放，因而公民的消费信息、浏览喜好例如cookie等信息是商业平台收集个人信息的目的所在；再者，从民众自身来讲，更加注重享有数据主体的权利，研究表明，只要诱使民众以为他们已经掌握了数据，那么他们就会以慷慨的多的方式处理数据。个人数据权益的保护可以说是在互联网公司与用户等各方的博弈中不断前进，由于个人信息保护的很多不确定因素，若有第三方评估机构对互联网企业个人信息保护等行为进行评测，将会带给政府、企业和个人带来持续的警示作用。

**三、我国数据治理与展望**

当前我国个人信息保护法及跨境流动实施细则的出台备受关注，协同法律、规则和技术织就一张疏而不漏、密而不紧的规制之网，将持续为我国家主权利益和数字化发展保驾护航。

**（一）我国数据跨境流动将坚持主权和安全利益至上**

自美国1998年提出“数字地球”计划至今历时20年，美国数字全球化布局奠定其拥有世界范围的数据控制权。然而根据2018年美国《国家贸易评估报告》，美国认为2018年美国数字贸易的主要障碍来自中国、欧盟、印度尼西亚、韩国、尼日利亚、俄罗斯、泰国、土耳其、越南等9个国家和地区，共15项障碍。其中中国最多，共有4项障碍，具体包括：1.对跨境数据流动的限制、对数据本地化要求; 2.对专线和VPN的限制; 3.对云计算限制;4.网络过滤和屏蔽。2018年10月30日互联网协会(Internet Association)为美国贸易代表办公室（USTR）2019年美国《国家贸易评估报告》提交的报告中称，印度、欧盟、印度尼西亚、中国和越南是数字贸易领域五个壁垒最为严重的国家或联盟，报告指出美国商界通过互联网服务可以接触到世界上95%的消费者的能力已不再稳固，报告建议USTR必须持续将向海外推行开放的互联网政策作为一个首要处理的经贸问题。

虽然我国数字经济发展迅速，已成为全球最大的网络市场，拥有世界数量最大的网民群体，但当前形势对我而言存在两方面挑战，一是美国希望通过贸易的流动性强制撬动网络主权、数据主权保护，二是我国具有相当体量的数据跨境传输需求，目前产生的数据合规成本造成企业较大负担和风险。对此，一方面，我国在对境内网络运营者建设、运营、维护和使用网络的监督管理中，从维护主权和安全角度主要采取四方面的评估检查机制： 1.个人信息和重要数据跨境传输的安全评估;2.对关系国家安全的网络和信息系统采购的重要网络产品和服务进行的网络安全审查；3.对关键信息基础设施的安全风险抽查；4.为配合政府部门履行维护网络安全义务的协助和支持，我国“数字海关”的设置有效降低了数据跨境流动的安全风险和隐患。另一方面，针对当前美国逆全球化趋势明显，我国可分三部实施数据跨境传输计划：一是东盟（CAFTA）、金砖国家（BRICS）以及一带一路沿线国家中有我国多个经贸合作伙伴出现在美国“黑名单”中，如印度、俄罗斯、印度尼西亚、韩国、尼日利亚、泰国、土耳其、越南等相关国家，我应积极争取该类国家，在现有经贸基础上构建中国数据跨境传输“朋友圈”；二是鉴于中欧数据主权的利益交汇，我应积极协商争取加入欧盟“数据安全流通区”，既符合中欧双方在全球数据主权方面的共同利益又保障中国在欧企业的共同权益；三是与短期不能建立跨境传输机制的国家，可以采取与相关境外企业之间建立“防火墙”等多种方式，打消其他司法辖区审查机构的疑虑，促使交易顺利进行。

**（二）个人数据保护法宜宽严相济充分发挥平台责任**

随着数据安全风险日益凸显，保护数据安全特别是个人信息安全，成为世界各国共同面对的重要课题。我国的个人信息保护法已于2018年9月正式列入全国人大常委会立法规程。回顾立法之路，从2017年6月1日《中华人民共和国网络安全法》（简称《网安法》）正式施行以来，一系列部门规章、司法解释、国家标准相继出台。一是国家标准化委员会制定的《信息安全技术个人信息安全规范》（GB/T35273-2017）简称“《个人信息安全规范》”），其参考了经合组织（OECD）隐私框架“隐私保护及跨境合作执行建议”、亚太经合组织（APEC）隐私框架（跨境隐私规则体系CBPR）等国际规则，以及通用数据保护GDPR、欧美《隐私盾框架》、美国《消费者隐私权法案》等欧美个人信息保护方面的立法，与这些国家通行的个人信息保护规则具有很多相似之处；二是与《网安法》同时出台的《中华人民共和国电子商务法》（简称《电商法》），承继了《网安法》中对个人信息主体权益保护的总体思路，电商法一方面对《网安法》下的一般性规则进行了细化，另一方面也针对电子商务领域进一步延伸具体要求，体现了不同法律权益的平衡。三是于2018年10月26日颁布实施的《国际刑事司法协助法》，强调中华人民共和国境内机构、组织和个人不得向外国提供证据材料和本法规定的协助，为跨境执法提供了数据管辖主张，对域外的“长臂管辖”进行了回应。

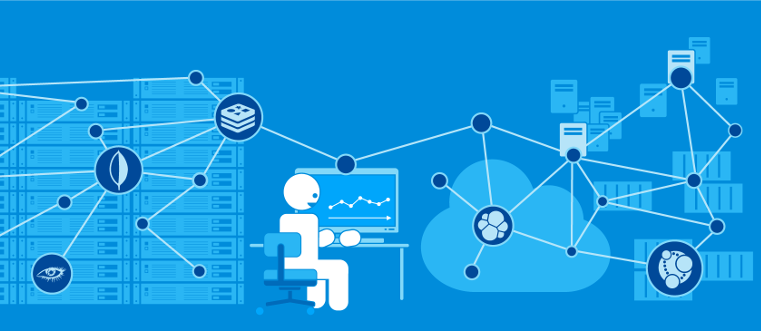


回顾2018,既是数据泄露的灰色之年,也是数据保护开启元年，世界各国已纷纷开始为个人数据“赋权”。在我国，2018年年底社交媒体巨头腾讯公司成为互联网行业中的先行者,于12月27日召开的2018大数据合作与合规峰会上率先发布了《腾讯隐私保护白皮书》，通过技术努力和平台责任为2019年打开了新的希望之门。对于我国的立法者而言，我国个人数据保护法宜秉持宽严相济的“中国特色”，通过法律规制、平台自律以及第三方监督，充分发扬科技向善理念。（来源：《中国信息安全》杂志2019年第1期）

## 把握新一代信息技术的聚焦点

数字化、网络化、智能化是新一轮科技革命的突出特征，也是新一代信息技术的核心。数字化为社会信息化奠定基础，其发展趋势是社会的全面数据化。数据化强调对数据的收集、聚合、分析与应用。网络化为信息传播提供物理载体，其发展趋势是信息物理系统（CPS）的广泛采用。信息物理系统不仅会催生出新的工业，甚至会重塑现有产业布局。智能化体现信息应用的层次与水平，其发展趋势是新一代人工智能。目前，新一代人工智能的热潮已经来临。

习近平同志在2018年两院院士大会上的重要讲话指出：“世界正在进入以信息产业为主导的经济发展时期。我们要把握数字化、网络化、智能化融合发展的契机，以信息化、智能化为杠杆培育新动能。”这一重要论述是对当今世界信息技术的主导作用、发展态势的准确把握，是对利用信息技术推动国家创新发展的重要部署。



人类社会、物理世界、信息空间构成了当今世界的三元。这三元世界之间的关联与交互，决定了社会信息化的特征和程度。感知人类社会和物理世界的基本方式是数字化，联结人类社会与物理世界（通过信息空间）的基本方式是网络化，信息空间作用于物理世界与人类社会的方式是智能化。数字化、网络化、智能化是新一轮科技革命的突出特征，也是新一代信息技术的聚焦点。数字化为社会信息化奠定基础，其发展趋势是社会的全面数据化；网络化为信息传播提供物理载体，其发展趋势是信息物理系统（CPS）的广泛采用；智能化体现信息应用的层次与水平，其发展趋势是新一代人工智能。

**数字化：从计算机化到数据化**

数字化是指将信息载体（文字、图片、图像、信号等）以数字编码形式（通常是二进制）进行储存、传输、加工、处理和应用的技术途径。数字化本身指的是信息表示方式与处理方式，但本质上强调的是信息应用的计算机化和自动化。数据化（数据是以编码形式存在的信息载体，所有数据都是数字化的）除包括数字化外，更强调对数据的收集、聚合、分析与应用，强化数据的生产要素与生产力功能。数字化正从计算机化向数据化发展，这是当前社会信息化最重要的趋势之一。

数据化的核心内涵是对信息技术革命与经济社会活动交融生成的大数据的深刻认识与深层利用。大数据是社会经济、现实世界、管理决策等的片段记录，蕴含着碎片化信息。随着分析技术与计算技术的突破，解读这些碎片化信息成为可能，这使大数据成为一项新的高新技术、一类新的科研范式、一种新的决策方式。大数据深刻改变了人类的思维方式和生产生活方式，给管理创新、产业发展、科学发现等多个领域带来前所未有的机遇。

大数据的价值生成有其内在规律（服从大数据原理）。只有深刻认识并掌握这些规律，才能提高自觉运用、科学运用大数据的意识与能力（大数据思维）。大数据的价值主要通过大数据技术来实现。大数据技术是统计学方法、计算机技术、人工智能技术的延伸与发展，是正在发展中的技术，当前的热点方向包括：区块链技术、互操作技术、存算一体化存储与管理技术、大数据操作系统、大数据编程语言与执行环境、大数据基础与核心算法、大数据机器学习技术、大数据智能技术、可视化与人机交互分析技术、真伪判定与安全技术等。大数据技术的发展依赖一些重大基础问题的解决，这些重大基础问题包括：大数据的统计学基础与计算理论基础、大数据计算的软硬件基础与计算方法、大数据推断的真伪性判定等。

实施国家大数据战略是推进数据化革命的重要途径。自2015年我国提出实施国家大数据战略以来，我国大数据快速发展的格局已初步形成，但也存在一些亟待解决的问题：数据开放共享滞后，数据资源红利仍未得到充分释放；企业赢利模式不稳定，产业链完整性不足；核心技术尚未取得重大突破，相关应用的技术水平不高；安全管理与隐私保护还存在漏洞，相关制度建设仍不够完善；等等。当前，应采取有效举措解决制约我国大数据发展的瓶颈问题。

**网络化：从互联网到信息物理系统**

作为信息化的公共基础设施，互联网已经成为人们获取信息、交换信息、消费信息的主要方式。但是，互联网关注的只是人与人之间的互联互通以及由此带来的服务与服务的互联。

物联网是互联网的自然延伸和拓展，它通过信息技术将各种物体与网络相连，帮助人们获取所需物体的相关信息。物联网通过使用射频识别、传感器、红外感应器、视频监控、全球定位系统、激光扫描器等信息采集设备，通过无线传感网络、无线通信网络把物体与互联网连接起来，实现物与物、人与物之间实时的信息交换和通信，以达到智能化识别、定位、跟踪、监控和管理的目的。互联网实现了人与人、服务与服务之间的互联， 而物联网实现了人、物、服务之间的交叉互联。物联网的核心技术包括：传感器技术、无线传输技术、海量数据分析处理技术、上层业务解决方案、安全技术等。物联网的发展将经历相对漫长的时期，但可能会在特定领域的应用中率先取得突破，车联网、工业互联网、无人系统、智能家居等都是当前物联网大显身手的领域。

物联网主要解决人对物理世界的感知问题，而要解决对物理对象的操控问题则必须进一步发展信息物理系统（CPS）。信息物理系统是一个综合计算、网络和物理环境的多维复杂系统，它通过3C（Computer、Communication、Control）技术的有机融合与深度协作，实现对大型工程系统的实时感知、动态控制和信息服务。通过人机交互接口，信息物理系统实现计算进程与物理进程的交互，利用网络化空间以远程、可靠、实时、安全、协作的方式操控一个物理实体。从本质上说，信息物理系统是一个具有控制属性的网络。



不同于提供信息交互与应用的公用基础设施，信息物理系统发展的聚焦点在于研发深度融合感知、计算、通信和控制能力的网络化物理设备系统。从产业角度看，信息物理系统的涵盖范围小到智能家庭网络、大到工业控制系统乃至智能交通系统等国家级甚至世界级的应用。更为重要的是，这种涵盖并不仅仅是将现有的设备简单地连在一起，而是会催生出众多具有计算、通信、控制、协同和自治性能的设备，下一代工业将建立在信息物理系统之上。随着信息物理系统技术的发展和普及，使用计算机和网络实现功能扩展的物理设备将无处不在，并推动工业产品和技术的升级换代，极大地提高汽车、航空航天、国防、工业自动化、健康医疗设备、重大基础设施等主要工业领域的竞争力。信息物理系统不仅会催生出新的工业，甚至会重塑现有产业布局。

**智能化：从专家系统到元学习**

智能化反映信息产品的质量属性。我们说一个信息产品是智能的，通常是指这个产品能完成有智慧的人才能完成的事情，或者已经达到人类才能达到的水平。智能一般包括感知能力、记忆与思维能力、学习与自适应能力、行为决策能力等。所以，智能化通常也可定义为：使对象具备灵敏准确的感知功能、正确的思维与判断功能、自适应的学习功能、行之有效的执行功能等。

智能化是信息技术发展的永恒追求，实现这一追求的主要途径是发展人工智能技术。人工智能技术诞生60多年来，虽历经三起两落，但还是取得了巨大成就。1959—1976年是基于人工表示知识和符号处理的阶段，产生了在一些领域具有重要应用价值的专家系统；1976—2007年是基于统计学习和知识自表示的阶段，产生了各种各样的神经网络系统；近几年开始的基于环境自适应、自博弈、自进化、自学习的研究，正在形成一个人工智能发展的新阶段——元学习或方法论学习阶段，这构成新一代人工智能。新一代人工智能主要包括大数据智能、群体智能、跨媒体智能、人机混合增强智能和类脑智能等。

深度学习是新一代人工智能技术的卓越代表。由于在人脸识别、机器翻译、棋类竞赛等众多领域超越人类的表现，深度学习在今天几乎已成为人工智能的代名词。然而，深度学习拓扑设计难、效果预期难、机理解释难是重大挑战，还没有一套坚实的数学理论来支撑解决这三大难题。解决这些难题是深度学习未来研究的主要关注点。此外，深度学习是典型的大数据智能，它的可应用性是以存在大量训练样本为基础的。小样本学习将是深度学习的发展趋势。

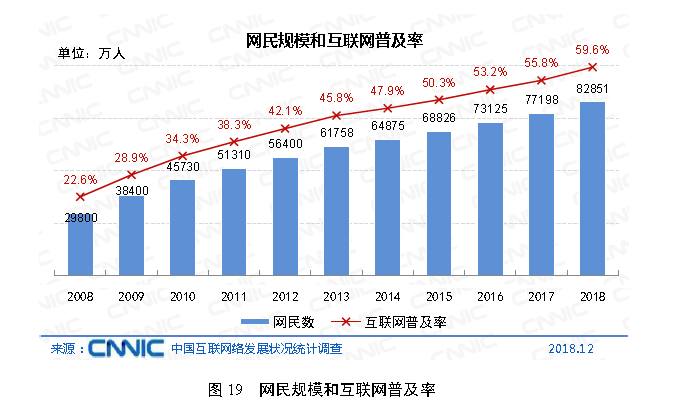
元学习有望成为人工智能发展的下一个突破口。学会学习、学会教学、学会优化、学会搜索、学会推理等新近发展的元学习方法以及“AlphaGo Zero”在围棋方面的出色表现，展现了这类新技术的诱人前景。然而，元学习研究还仅仅是开始，其发展还面临一系列挑战。

新一代人工智能的热潮已经来临，可以预见的发展趋势是以大数据为基础、以模型与算法创新为核心、以强大的计算能力为支撑。新一代人工智能技术的突破依赖其他各类信息技术的综合发展，也依赖脑科学与认知科学的实质性进步与发展。（来源：人民日报 中国科学院院士、西安交通大学教授 徐宗本）

# 政府之声

## CNNIC发布第43次《中国互联网络发展状况统计报告》

2019年2月28日，中国互联网络信息中心（CNNIC）在京发布第43次《中国互联网络发展状况统计报告》（以下简称《报告》）。《报告》从互联网基础建设、互联网应用发展、政务应用发展、产业与技术发展及互联网安全等多个方面展示了2018年我国互联网发展状况。



2018年是贯彻党的十九大精神的开局之年，是改革开放40周年，是决胜全面建成小康社会、实施“十三五”规划承上启下的关键一年，中国互联网络发展迅速，呈现出七个特点。

**一是互联网普及率接近六成，入网门槛进一步降低。**截至2018年12月，我国网民规模达8.29亿，普及率达59.6%，较2017年底提升3.8个百分点，全年新增网民5653万。我国手机网民规模达8.17亿，网民通过手机接入互联网的比例高达98.6%。2018年，互联网覆盖范围进一步扩大，贫困地区网络基础设施“最后一公里”逐步打通，“数字鸿沟”加快弥合；移动流量资费大幅下降，跨省“漫游”成为历史，居民入网门槛进一步降低，信息交流效率得到提升。

**二是基础资源保有量稳步提升，IPv6应用前景广阔。**截至2018年12月，我国IPv6地址数量为41079块/32，年增长率为75.3%；域名总数为3792.8万个，其中“.CN”域名总数为2124.3万个，占域名总数的56.0%。在IPv6方面，我国正在持续推动IPv6大规模部署，进一步规范IPv6地址分配与追溯机制，有效提升IPv6安全保障能力，从而推动IPv6的全面应用；在域名方面，2018年我国域名高性能解析技术不断发展，自主知识产权软件研发取得新突破，域名服务安全策略本地化定制能力进一步增强，从而显著提升了我国域名服务系统的服务能力和安全保障能力。

**三是电子商务领域首部法律出台，行业加速动能转换。**截至2018年12月，我国网络购物用户规模达6.10亿，年增长率为14.4%，网民使用率为73.6%。电子商务领域首部法律《电子商务法》正式出台，对促进行业持续健康发展具有重大意义。在经历多年高速发展后，网络消费市场逐步进入提质升级的发展阶段，供需两端“双升级”正成为行业增长新一轮驱动力。在供给侧，线上线下资源加速整合，社交电商、品质电商等新模式不断丰富消费场景，带动零售业转型升级；大数据、区块链等技术深入应用，有效提升了运营效率。在需求侧，消费升级趋势保持不变，消费分层特征日渐凸显，进一步推动市场多元化。

**四是线下支付习惯持续巩固，国际支付市场加速开拓。**截至2018年12月，我国手机网络支付用户规模达5.83亿，年增长率为10.7%，手机网民使用率达71.4%。线下网络支付使用习惯持续巩固，网民在线下消费时使用手机网络支付的比例由2017年底的65.5%提升至67.2%。在跨境支付方面，支付宝和微信支付已分别在40个以上国家和地区合规接入；在境外本土化支付方面，我国企业已在亚洲9个国家和地区运营本土化数字钱包产品。

**五是互联网娱乐进入规范发展轨道，短视频用户使用率近八成。**截至2018年12月，网络视频、网络音乐和网络游戏的用户规模分别为6.12亿、5.76亿和4.84亿，使用率分别为73.9%、69.5%和58.4%。各大网络视频平台注重节目内容质量提升，自制内容走向精品化。网络音乐企业版权合作不断加深，数字音乐版权的正版化进程显著加快。越来越多的游戏公司开始侧重海外业务，国产游戏在海外市场的影响力进一步扩大。短视频用户规模达6.48亿，用户使用率为78.2%，随着众多互联网企业布局短视频，市场成熟度逐渐提高，内容生产的专业度与垂直度不断加深，优质内容成为各平台的核心竞争力。

**六是在线政务服务效能得到提升，践行以民为本的发展理念。**截至2018年12月，我国在线政务服务用户规模达3.94亿，占整体网民的47.5%。2018年，我国“互联网+政务服务”深化发展，各级政府依托网上政务服务平台，推动线上线下集成融合，实时汇入网上申报、排队预约、审批审查结果等信息，加强建设全国统一、多级互联的数据共享交换平台，通过“数据多跑路”，实现“群众少跑腿”。同时，各地相继开展县级融媒体中心建设，将县广播电视台、县党报、县属网站等媒体单位全部纳入，负责全县所有信息发布服务，实现资源集中、统一管理、信息优质、服务规范，更好地传递政务信息，为当地群众服务。

**七是新兴技术领域保持良好发展势头，开拓网络强国建设新局面。**2018年，我国在基础资源、5G、量子信息、人工智能、云计算、大数据、区块链、虚拟现实、物联网标识、超级计算等领域发展势头向好。在5G领域，核心技术研发取得突破性进展，政企合力推动产业稳步发展；在人工智能领域，科技创新能力得到加强，各地规划及政策相继颁布，有效推动人工智能与经济社会发展深度融合；在云计算领域，我国政府高度重视以其为代表的新一代信息产业发展，企业积极推动战略布局，云计算服务已逐渐被国内市场认可和接受。（来源：中国互联网络信息中心）

* **第43次《中国互联网络发展状况统计报告》全文：**
* http://cnnic.cn/gywm/xwzx/rdxw/20172017\_7056/201902/W020190228474508417254.pdf

## 扫黄打非办公室部署开展“净网2019”“护苗2019”“秋风2019”专项行动

2019年2月27日，为贯彻落实2019年“扫黄打非”行动方案和第三十二次全国“扫黄打非”工作电视电话会议精神，近日，全国“扫黄打非”办公室作出专门部署，要求各地各部门紧紧围绕庆祝新中国成立70周年主线，于3月至11间大力组织开展“净网2019”“护苗2019”“秋风2019”等专项行动，持续净化社会文化环境。

全国“扫黄打非”办公室强调，开展“净网2019”专项行动，将聚焦整治网络色情和低俗问题，通过强化司法打击、行政管理、行业规范、道德约束等多种手段综合施策，综合治理。着重整治网络文学领域，加强对文学网站的监管，规范网站编辑和作者管理，严打利用微信公众号、微博、贴吧、论坛等渠道引流低俗内容的行为。严查淫秽视频打赏平台，坚决打击建立平台、发布链接人员及参与传播的下线代理。继续严厉打击非法网络直播平台，严惩通过直播平台传播淫秽物品、组织淫秽表演的犯罪分子，坚决关停违法直播及聚合软件。

开展“护苗2019”专项行动，着重强化网上网下两项整治，坚决查办涉未成年人的“黄”“非”案件。强化中小学周边文化环境整治，重点查处无证销售出版物和销售非法出版物的违法行为，大力查缴有损未成年人身心健康的不良出版物、“口袋本”图书、卡通漫画、游戏卡片、色情低俗视频等有害信息。强化对未成年人接触较多的互联网应用的整治，特别对网络短视频、游戏、漫画、学习类APP等领域加强清理，坚决遏制色情、低俗、暴力、恐怖、残酷等有害信息传播。同时，组织开展“护苗”正面教育引导工作。

开展“秋风2019”专项行动，重点打击假媒体假记者站假记者及新闻敲诈行为，切实维护新闻出版传播秩序。一是集中整治自媒体违法违规采编、传播有害信息、炒作敏感问题、敲诈勒索等活动。二是坚决打击非法网络期刊，严查利用非法学术期刊实施诈骗行为。三是重点整治电商平台销售非法出版物问题，建立网上出版物证照核验体系，规范网上出版物购销行为。

全国“扫黄打非”办公室负责同志表示，此次专项行动部署，聚焦突出庆祝新中国成立70周年主线，积极回应人民群众高度关注的问题，立足于早，务求实效。“扫黄打非”部门要坚持问题导向，推动行动抓实、抓细、抓到位，以优异成绩向新中国成立70周年大庆献礼！。（来源：全国"扫黄打非"工作小组办公室）

## 工信部：多家互联网企业因用户信息问题被督促整改

2019年2月27日，工业和信息化部信息通信管理局发布《工业和信息化部关于电信服务质量的通告(2019年第1号)》-信部信管函〔2019〕48号文件；(以下简称“通告”)。通告公布了的2018年四季度用户个人信息保护检查发现问题的互联网企业名单。其中，包括猿题库、途家、暴风金融、新浪新闻、网易新闻等。

四季度，工业和信息化部组织对47家手机应用商店的应用软件进行技术检测，发现违规软件43款，涉及违规收集使用用户个人信息、恶意消耗用户相关账户积分、强行捆绑推广其他应用软件等问题，已责令下架。

组织对39家互联网企业44项互联网服务进行抽查，发现14家互联网企业存在未公示用户个人信息收集使用规则、未告知查询更新信息的渠道、未提供账号注销服务的问题，已督促整改。

此外，在组织对三家基础电信企业和50家增值电信企业的136项业务进行抽查中，发现3项业务存在客服电话不正确、无法提供服务等问题，已督促整改。（来源：工业和信息化部）

* **工业和信息化部关于电信服务质量的通告（2019年第1号）全文：**
* <http://www.miit.gov.cn/n1146295/n1652858/n1652930/n4509627/c6656154/content.html>

## 2018年上海市网络安全态势分析年度报告发布

2019年2月18日，上海市委网信办正式发布2018年上海市网络安全态势分析年度报告。报告显示，市委网信办2018年对全市2323家单位的2796个网站开展监测，对网站漏洞、网页篡改、网页仿冒、存在恶意软件、遭受拒绝服务攻击等8类网络安全问题发出告警，向431家事发单位发出网络安全通报523份。与此同时，市委网信办处置多起网络安全事件，并根据《网络安全法》对发生严重网络安全事件的涉事单位进行约谈，全年共计约谈29家单位。

报告显示，上海市委网信办全年共发出通报523份，涉及431家单位，占所有被监测单位的18.6%。其中，网络安全事件通报66份，占总通报数的12.6%；网络安全高危漏洞通报338份，占总通报数的64.6%；网络安全隐患告知书119份，占总通报数的22.8%。

从反馈情况来看，各单位均较为重视。截至目前，66份网络安全事件通报收到反馈66份，已整改66份，反馈率和整改率均为100%；338份网络安全高危漏洞通报收到反馈337份，已整改335份，反馈率为99.7%，整改率为99.1%。

综合全年网络安全通报情况发现，当前全市关键信息基础设施面临的主要安全威胁不仅有可用性风险，更多见的情况是网站被攻击者利用成为牟利工具。主要表现形式有域名劫持和暗链等，域名被劫持解析为色情、赌博网站，或者网站被写入暗链成为提高违规网站搜索排名和流量的工具。2018年上海市委网信办处置多起网络安全事件，主要涉及关键信息基础设施服务中断、敏感信息泄露、大规模拒绝服务攻击、网页篡改等类型。

报告显示，首届中国国际进口博览会网络安全保障工作是2018年全市网络安全工作的重中之重。市委网信办制定专项保障方案，积极协调有关部门共同开展网络安全监测及检测、网络安全渗透测试、网络安全应急响应等重点保障工作。组织技术力量针对重点网站、系统和相关APP共开展网络安全渗透测试工作2批次，共发现并组织修复安全漏洞76处。进博会期间开展现场联合值守工作，迅速响应并成功处置相关网络安全事件，确保进博会期间全市各单位网站或信息系统稳定运行，安全可控。此外，市委网信办牵头开展了2018年全市关键信息基础设施网络安全检查工作，历时四个月，收到1352家单位上报的2099个关键信息基础设施数据，对30家重点单位的45个系统进行了现场抽查，共发现安全问题359个，相关问题都已通报受检单位及时整改并反馈。

为提升全市网络安全意识，促进形成人人参与网络安全，人人共享网络安全的良好氛围，上海市委网信办创新网络安全宣传周的举办模式，联合杨浦区委、复旦大学及全市有关部门共同主办2018国家网络安全宣传周。宣传周期间，各类活动总计超过400场，直接参与活动人数超480万人次，共发送公益短信3915万条，张贴网络安全宣传海报4.35万张，发放宣传手册2.7万册，宣传单页13万份，原创稿件100余篇，总点击量860万次，有效提升了全市居民网络安全意识。（来源：上海市委网信办）

# 本期重要漏洞实例

## 关于WinRAR存在系列远程代码执行漏洞的安全公告

**发布日期：**2019-02-21  
**更新日期：**2019-02-21  
**受影响系统：**

发布时间早于5.70 Beta 1版本的WinRAR软件；

使用unacev2.dll动态共享库的解压、文件管理类工具软件。

**描述：**

WinRAR 是一款功能强大的压缩包管理器，作为档案工具RAR在 Windows环境下的图形界面，可用于备份数据、压缩文件、解压RAR/ZIP等格式的文件、创建 RAR/ZIP 等格式的压缩文件，得到了较为广泛的应用。

近日，Check Point的安全研究团队检测发现WinRAR的四个安全漏洞，分别为ACE文件验证逻辑绕过漏洞（CVE-2018-20250）、ACE文件名逻辑验证绕过漏洞（CVE-2018-20251）、ACE/RAR文件越界写入漏洞（CVE-2018-20252）以及LHA/LZH文件越界写入漏洞（CVE-2018-20253。漏洞攻击者利用上述漏洞，通过诱使用户使用WinRAR打开恶意构造的压缩包文件，将恶意代码写入系统启动目录或者写入恶意dll劫持其他软件进行执行，实现对用户主机的任意代码执行攻击。

CNVD对上述漏洞的综合评级为“高危”。  
<\*来源：CNVD  
链接：http://www.cnvd.org.cn/webinfo/show/4903  
\*>  
**建议：**

1、使用WinRAR软件的用户：WinRAR厂商已发布新版本修复此漏洞，CNVD建议立即升级至最新版本：https://www.win-rar.com/download.html。

2、其他解压、文件管理类软件是否受影响的判断方法：用户可通过检查软件安装目录下是否存在unacev2.dll文件进行判断。

3、建议用户不要打开来历不明的压缩文件。

附：参考链接：

<https://www.win-rar.com/download.html>

<https://research.checkpoint.com/extracting-code-execution-from-winrar/>

## 多款IBM产品任意文件下载漏洞

**发布日期：**2019-02-26  
**更新日期：**2019-02-27  
**受影响系统：**

IBM SAN Volume Controller

IBM Storwize V7000

IBM Storwize V5000

IBM Storwize V3700

IBM Storwize V3500

IBM FlashSystem V9000

IBM FlashSystem 9100

**描述：**

CVE(CAN) ID: [CVE-2018-1775](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1775)  
IBM主要生产并销售计算机硬件及软件，并且为系统架构和网络托管提供咨询服务。  
多款IBM产品中的Service Assistant存在安全漏洞。攻击者可利用该漏洞从操作系统中下载任意文件。  
<\*来源：IBM （[ncsupp@ca.ibm.com](mailto:ncsupp@ca.ibm.com)）  
  \*>  
**建议：**

厂商补丁：  
IBM  
---  
目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：  
<https://www-01.ibm.com/support/docview.wss?uid=ibm10872486>

## Cisco SPA112/SPA525/SPA5X5 Series信息泄露漏洞

**发布日期：**2019-02-21  
**更新日期：**2019-02-25  
**受影响系统：**

Cisco SPA112

Cisco SPA525

Cisco SPA5x5

**描述：**

CVE(CAN) ID: [CVE-2019-1683](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-1683)  
Cisco SPA112/SPA525/SPA5X5 Series都是系列IP电话产品。  
Cisco SPA112、SPA525和SPA5X5 Series在证书处理组件中存在安全漏洞，该漏洞源于程序没有正确验证服务器证书。远程攻击者通过恶意的服务器证书，利用该漏洞可监听或控制部分TLS加密的会话初始协议（SIP）通话。  
<\*来源：Cisco  
链接：<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-ipphone-cert>  
\*>  
**建议：**

厂商补丁：  
Cisco  
-----  
Cisco已经为此发布了一个安全公告（cisco-sa-20190220-ipphone-certs）以及相应补丁:  
cisco-sa-20190220-ipphone-certs：Cisco SPA112, SPA525, and SPA5x5 Series IP Phones Certificate Validation Vulnerability  
链接：<https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190220-ipphone-cert>

## Adobe Acrobat/Reader信息泄露漏洞

**发布日期：**2019-02-21  
**更新日期：**2019-02-25  
**受影响系统：**

Adobe Acrobat Reader DC <= 2019.010.20091

Adobe Acrobat Reader DC <= 2015.006.30475

Adobe Acrobat DC <= 2019.010.20091

Adobe Acrobat DC <= 2015.006.30475

Adobe Acrobat 2017 <= 2017.011.30120

Adobe Acrobat Reader 2017 <= 2017.011.30120

**描述：**

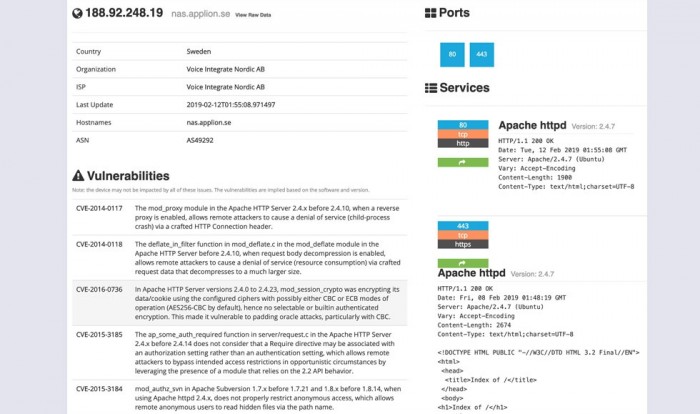
BUGTRAQ  ID: [107114](http://www.securityfocus.com/bid/107114)  
CVE(CAN) ID: [CVE-2019-7815](http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-7815)  
Acrobat是一套PDF文件编辑和转换工具。Reader是一套PDF文档阅读软件。  
Adobe Acrobat和Reader某些版本在实现中存在信息泄露漏洞。远程攻击者可利用该漏洞获取敏感信息。  
  
<\*来源：Alex Infuhr  
链接：<https://helpx.adobe.com/security/products/acrobat/apsb19-13.html>  
\*>  
  
**建议：**

厂商补丁：  
Adobe  
-----  
Adobe已经为此发布了一个安全公告（APSB19-13）以及相应补丁:  
APSB19-13：Security Updates available for Adobe Acrobat and Reader | APSB19-13  
链接：<https://helpx.adobe.com/security/products/acrobat/apsb19-13.html>

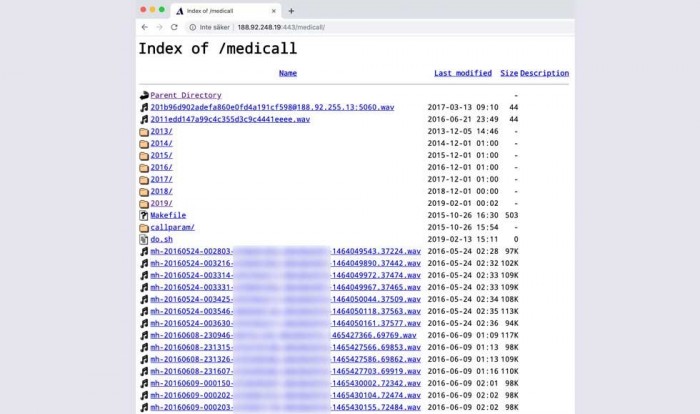
# 本期网络安全事件

## 瑞典医疗热线泄露270万条通话记录：涉及诸多敏感信息

2019年2月19日，援引瑞典科技媒体Computer Sweden报道，拨打给瑞典医疗保健热线1177 Vårdguiden的270万条通话录音信息在网络上曝光。长达17万小时、包含极其敏感信息的呼叫音频存储在开放的Web服务器上，并且没有经过任何的加密和身份认证，意味着互联网上的任意用户都可以通过Web浏览器完全访问这些个人信息。



外媒Computer Sweden表示曾聆听了部分录音信息，其中包括患者的疾病、目前服用的药物以及相关病史等敏感信息。甚至在部分通话中要求描述孩子的症状并要求提供他们的社会安全号码。

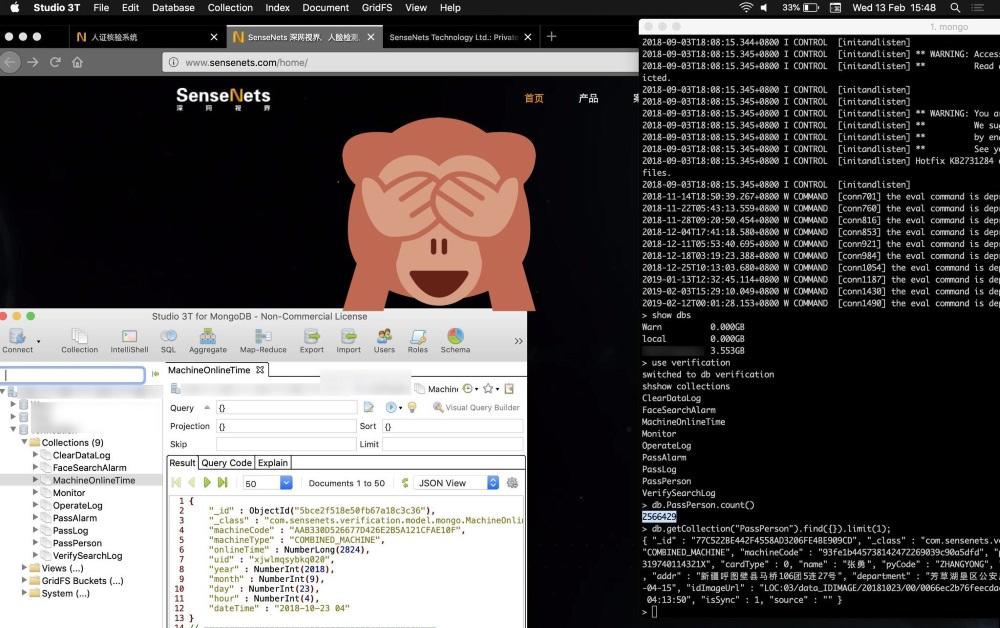


部分文件中还包括这些通话的个人电话号码。数据库中出现了大约57,000个号码，其中许多是呼叫者的个人号码，因此可以轻松地将信息与特定人员匹配。目前还不清楚这些电话可用多长时间，谁应该为违规行为负责，以及是否有任何不良恶意成员已经访问过这些信息。

不过似乎这些泄露的通话都发给1177Vårdguiden的分包商Medicall，后者是一家总部位于泰国，由瑞典人创办的公司。当被问及违规行为时，尽管存在压倒性的相互矛盾的证据，但医疗保健首席执行官大卫·尼布洛姆否认了这一情况。芬兰安全技术公司F-Secure的首席风险官Mikko Hypponen在推文中表示：“拨打给MEDICALL服务热线的通话记录以WAV音频格式存储在不安全的服务器上。”(来源：cnBeta)

## 国内某人脸识别公司数据泄露 超250万人数据可被获取

2019年2月15日，根据微博安全应急响应中心消息，国内某人脸识别公司发生大规模数据泄露事件。超过250万人的数据可被获取，680万条记录泄露，其中包括身份证信息，人脸识别图像及捕捉地点等。



这家公司的对外简介是将深度学习等前沿先进技术用于监控视频分析，实际上就是提供面部识别技术和人群分析技术，并提供公开数据库可在线查找。监控记录的地点包括警察局，酒店，旅游景点，公园，网吧和清真寺等。

举个例子，穿过街道的人可能会被摄像头拍到，这家公司可以通过摄像头画面分析出你是谁，而任何人都可以根据这家公司的实时面部识别来查看某人的位置记录并进行跟踪。可以猜想，如果攻击者掌握了某人的位置信息，就可以轻而易举实施各种犯罪。

发现这事的是GDI基金会的荷兰安全研究员Victor Gevers，小哥称从去年7月起他们就曾试图联系该公司，并对其数据库公开问题进行了警告，但这家公司并未作出回应。(来源：雷锋网)

## 买黑客软件侵入快递公司窃取1.5G个人信息，作案者被判三年

2018年7月，某快递公司IT部门工作人员通过公司技术日志发现，公司所属触屏官网自2018年4月以来被人利用系统漏洞侵入计算机服务器系统内，通过订单查询接口非法获取大量客户数据，至案发时已被非法获取6万余条客户信息。报案后，警方通过技术手段成功锁定一名涉嫌侵犯公民个人信息的犯罪嫌疑人龚某。

日前，经上海市青浦区检察院提起公诉，法院以侵犯公民个人信息罪判处被告人龚某有期徒刑三年，并处罚金人民币六千元。



去年上半年，龚某在某网上聊天群里看到，有人在叫卖一款可以获取某快递公司客户数据信息的黑客软件。他听说贩卖公民个人信息可以赚到钱，于是便联系了对方，花费了500元购买了这种软件。

龚某按照卖家的提示，先是用他人的身份信息注册了云服务器，又购买了一个新手机号，通过短信验证登录进去后，将这款黑客软件程序安装在云服务器上。在激活软件运行程序后，出现了一个滚动显示数据的窗口。不一会儿，便生成了一个内有多个文档的文件夹。龚某打开文档，发现里面全是该快递公司面单信息数据，包含快递订单号、产品名称、收件人姓名、联系方式、收货地址等。

短短三四个月，龚某通过这种方法共非法获取了数以万计条面单信息，他将盗取来的数据信息全都储存在云服务器中。警方调取了龚某使用他人身份注册的云服务器镜像数据，经司法鉴定，去年4月至7月期间，龚某所使用的云服务器IP地址向该快递公司网站发起请求200万余次，非法获得快递运单信息10万余条，进行去除重复后得到记录数6万余条。在对龚某所使用的云服务器内的数据分析发现，涉及该快递公司运单涉案文档900余个，共1.56GB。

快递物流企业掌握的客户个人信息内容丰富且数量巨大，据承办检察官介绍，该院近年来办理的涉嫌侵犯公民个人信息案件多发生在快递物流领域，案件范围涉及全国多地快递子网点，具有明显的行业性特征。犯罪方式除企业内部员工从快递公司内部系统盗取外，近年来还出现了诸如此案中利用高科技手段作案的趋势。“该类犯罪成本低但危害不容小觑，我们曾在办案中发现，有客户遭遇到冒充网购卖家的不法分子联系，导致钱财被骗，原因系客户在还未收到网购快递时，自己的信息已被盗取并在网络上出售，被诈骗分子利用。”(来源：上观)

## 违规搜集儿童隐私，抖音国际版在美被罚570万美元

2019年2月28日消息，据TechCrunch报道，美国联邦贸易委员会（FTC）今天发布了一项重要裁决，短视频应用抖音国际版（TikTok）因违反美国《儿童隐私法》，将被处以570万美元罚款，并将影响该应用在13岁以下儿童中的使用方式。

不过抖音方面称，2017年11月，字节跳动收购musical.ly，2018年8月，TikTok和musical.ly正式合并。由此，TikTok意外卷入了musical.ly历史上的这桩调查，并因此导致在北美的商业化探索受阻，TikTok并没有接入个性化广告。在今天发布的应用更新中，抖音国际版的所有用户都需要验证自己的年龄，13岁以下的用户将被引导到单独的、受更多限制的应用内体验，该体验可以保护他们的个人信息，并阻止他们向TikTok发布视频。

对于这款颇受欢迎的视频应用来说，这一裁决来得有些不太凑巧。就在同一天，抖音国际版开始推广其新的安全设计，旨在帮助社区了解其隐私和安全工具。而早在抖音被称为Musical.ly的时候，FTC就开始调查它。



TikTok发言人表示，随着与FTC和解的达成，公司将在美国更大范围地推进商业化探索。

TikTok北美的相关负责人表示：我们一直积极与FTC进行沟通。随着此次和解，TikTok原来受限于此案的业务可以更大范围展开。

2018年春天，行业监管组织CARU向FTC投诉，宣称抖音国际版违反了美国《儿童隐私法》，未经父母同意就收集13岁以下用户的个人信息。

FTC称，抖音国际版要求用户提供电子邮件地址、电话号码、用户名、姓名、个人简介和头像等资料。该应用还允许用户通过评论视频和发送直接信息与他人互动。此外，用户帐号默认是公开的，这意味着孩子的个人资料、用户名、照片和视频可以被其他用户看到。

FTC主席乔·西蒙斯（Joe Simons）在一份声明中说:“我们知道很多孩子在使用抖音国际版，但他们在收集13岁以下用户的姓名、电子邮件地址和其他个人信息之前，却未征得家长同意。这一创纪录的处罚应该提醒所有针对儿童的在线服务和网站：我们非常重视《儿童隐私法》的执行，我们不会容忍公然无视法律的行为。”

当然，对于抖音国际版这样的应用程序来说，美国《儿童隐私法》实施起来有点复杂，因为它们处于面向成年人和儿童的灰色地带。青少年喜欢这款应用，它经常受到13岁以下儿童的追捧，家长们也往往会默认支持。（来源：网易科技）

## ﻿自如员工被控窃取公司信息七万条涉侵犯公民信息罪受审

2019年2月20日上午，利用职务之便，北京自如生活资产管理有限公司(以下简称自如公司)员工李某下载大量顾客信息，在离职后被举报。通州法院以涉侵犯公民个人信息罪受审，李某被指控侵犯公民个人信息量达80余万条。



**公司发现内部信息被窃**

2018年5月，北京自如生活资产管理有限公司员工发现公司服务器内部客户资料被非法下载，造成7万条客户资料外泄。公安机关调查发现，公司前员工李某有作案嫌疑。

根据公诉机关的指控，2017年4月至2018年6月29日间，被告人李某在公司任职期间，利用技术手段违规从公司内网系统秘密下载大量客户信息并通过网上购买和交换等方式非法获取公民个人信息，还向他人提供所获得的公民个人信息。2018年6月29日，被告人李某被民警查获，涉案苹果手机1部、U盘1个、苹果笔记本电脑1台被起获，经鉴定，上述起获物品中属公民个人信息的总条数为814369条。

公诉机关认为，被告人李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，其行为触犯了《中华人民共和国刑法》第二百五十三条之一，犯罪事实清楚，证据确实、充分，应当以侵犯公民个人信息罪追究其刑事责任。

**超权限下载客户资料**

李某2014年毕业于天津一所理工类大学，2017年4月在自如公司担任管家。她交代称，从公司下载的这些资料是通州区的业主资料，拿到后给了当时的经理，由经理发给新入职的员工，让他们打电话回访老业主，维护关系，并让老业主推荐新房源，这样就有业绩了。

李某承认自己的行为没有经过报批，她的权限是可以浏览全北京成交信息，但没有下载的权限。“公司发现我浏览超越我权限的客户信息，不知道我下载了，技术人员警告过我不准再看超越我权限的信息，我才知道技术后台能检测出来，我就没敢再下载。”

李某说，对于电脑中存的公民信息，有些是公司内部下载的，有些是从互联网上互换的。下载是通过一个软件，公民个人信息包括合同编号、业主姓名电话和房屋地址。

**在竞争公司任职区域经理**

2018年3月，李某因违反公司规定离职，但离职时没有上交这些资料。随后她任职另一家资产管理有限公司，从事业务领域和在老单位相同，并成为了后者公司的通州区区域经理。李某否认把资料提供给新公司。一位自如公司前员工证人称，他之前跟李某要过信息，发现她掌握的个人信息有几万条，很是震惊。在李某违反公司规定离职后，在另一家竞争对手职位攀升，我怀疑跟这些信息有关系，于是上报公司。公司发现信息被窃后报警。庭审中，因李某只认可部分指控，该案未当庭宣判。（来源：新京报）

## 倒卖明星隐私链条被曝光 律师:造成严重后果或被追责

2019年3月1日，据中国之声《新闻纵横》报道：sfz、hz、sjh，这几个缩写您知道是什么意思吗？在网络平台上，它们是倒卖明星隐私和个人信息“行业”的通用语言，分别是身份证、护照和手机号的拼音首字母。

近日，有不少明星通过网络反映自己因隐私泄露而遭到骚扰。在这些问题的背后，是一整条以明星为中心的机场追星利益链条——不仅明星私人信息被明码标价，还有卖家为粉丝提供“刷关”服务：也就是违规帮助粉丝进入机场禁区追星。在微博、贴吧等社交平台上，有不少声称可以提供明星身份证号、手机号的卖家。这些明星信息的可信度如何？隐私信息到底是如何被泄露的？

**身份证号、手机号50元一位，“可以直接打电话给爱豆们”**

在微博、贴吧等社交平台，以明星航班、手机、身份证或者“刷关”等关键词搜索，可以找到很多相关卖家。在名为“明星航班吧”的百度贴吧中，大量明星身份贩子和机票商家聚集于此。

一位卖家告诉记者，当红明星的身份证号、手机号他那里都有，50元一位，如果是港台明星他们就提供台胞证或通行证号码。可以直接打电话给偶像：

“你说的这些明星我都有他们的手机号。你可以打电话给爱豆们，但是查询航班的时候不能用他们的手机查。因为他们的行程都是隐私的，我们去查的时候他就收到短信验证码了，我们就收不到了。查询的时候是用他们的身份证号外加我们自己的手机号去查明星行程的。明星身份证如果要的多，我就给你们按照50元一个。”



**制造机场偶遇：“刷关”陪明星一起候机，只需少量退票费**

之后，粉丝如果想和偶像亲密接触，有了对方身份证和手机号，在机场“偶遇”是最方便的，于是，可以再找到“刷关”卖家，一位卖家承诺，只要按照他的指引，可以在得知明星的航班信息后，购买相近时间段的全价机票，过安检陪着明星一起候机，把明星送上飞机后再出来退票，只损失少量退票费：“刷关就是我帮你买机票，你拿着我买的机票正常过安检，正常过安检我就退票了，在候机厅堵他就可以了，之后再退票。”

另外一位卖家服务更“周到”，表示只要提供粉丝的身份证号与明星的航班行程，就可以坐头等舱“刷关”，甚至进入休息室与明星面对面：“你要刷谁的关，你告诉我，我给你去找票。头等舱价格200元左右，普通舱大概是100元到130元左右，两者区别你要搞清楚。头等舱的话你可以和爱豆一起进休息室，普通舱不行。”

此外，记者调查发现，有些“黄牛”还公开贩卖明星的护照、QQ号码、微信号码甚至包括“吃鸡”、王者荣耀等在内的游戏账号，为安全起见所售证件等均采用拼音缩写代替。而此类贩卖明星信息的事件，其实数年前就被媒体曝光。

早在去年7月初，一份民航部门关于“加强粉丝接送机、跟机现象管理的通知”引起广泛关注。通知中提到要严格内部人员管理，防止泄露信息，强化机场治安秩序维护，预警防范聚众扰序行为，杜绝粉丝机闹，并明确指出对于扰乱秩序的违规违法的行为从严从重处罚。

**专家：“刷关卡”可能来自内部**

中国航空法律服务中心首席专家张起淮表示，所谓的“刷关卡”很可能就是一张从值机柜台流出的重复打印的登机牌，“它的来源应该就是内部。很有可能就是值机柜台的工作人员，他们可以重复打印机票，实际上违规的。超售就会出现这种情况，但是超售的情况以及登机牌打印中出现的这些‘差错’，如果不到最终登机这一步，你都发现不了的。这就成了一个黑市场、潜规则，大家都知道但是都不去作为。”

公开报道显示，贩卖明星个人信息的情况数年前就曾被曝光，航班信息也不例外。张起淮认为，明星的航班信息被泄露的环节的确很多，不好判断：“对于明星、艺人来讲，说实话机场的工作人员、出售机票的工作人员、卖保险的工作人员还有机组成员，在这些环节，这些职能部门的工作人员可能会利用职务便利把这些信息卖给一些非法私人侦探、调查公司等。”

**律师提醒：买卖明星个人信息、扰乱机场正常秩序会被追究法律责任**

湖南金州律师事务所律师邢鑫指出，明星信息泄露涉及网络安全、个人信息保护等问题，粉丝或者黄牛买卖明星个人信息造成严重后果的或被追究刑事责任。此外，对于粉丝的“刷关”行为以及黄牛的行为，如果扰乱机场正常秩序同样会被追究法律责任：“我国《网络安全法》规定：‘任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。’同时，情节严重的，黄牛涉嫌构成公民个人信息罪。《民用航空法》规定，聚众扰乱民用机场秩序的，依照刑法‘聚众扰乱公共秩序罪’追究刑事责任。通常情况下的粉丝刷关行为，其危害程度也到不了‘严重’，可依据《治安管理处罚法》，‘处警告或者200元以下罚款’，‘情节较重的，处5日以上10日以下拘留，可以并处500元以下罚款’。”

律师提醒，粉丝追星如果掌握不好度，不仅会给明星造成困扰，还会带来负面示范效应，因此一定要守住底线、理性追星。（来源：中国日报网）

**信息安全意识产品免费大赠送**

[isa@spisec.com](mailto:isa@spisec.com)