国盟信息安全通报

2020 年 6 月 07 日第 217 期

全国售后服务中心

国盟信息安全通报

（第 217 期）

国际信息安全学习联盟

2020 年 06 月 07 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 312 个，其中高危漏洞 92 个、中危漏洞 182 个、低危漏洞 38 个。漏洞平均分值为 5.84。本周收录的漏洞中，涉及 0day 漏洞 121 个（占 39%），其中互联网上出现“WordPress Ultimate Member 跨站点请求伪造漏洞、OpenEMR 远程代码执行漏洞（CNVD-2018-14867）”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 3956 个，与上周（5021 个）环比减少 21%。

主要内容

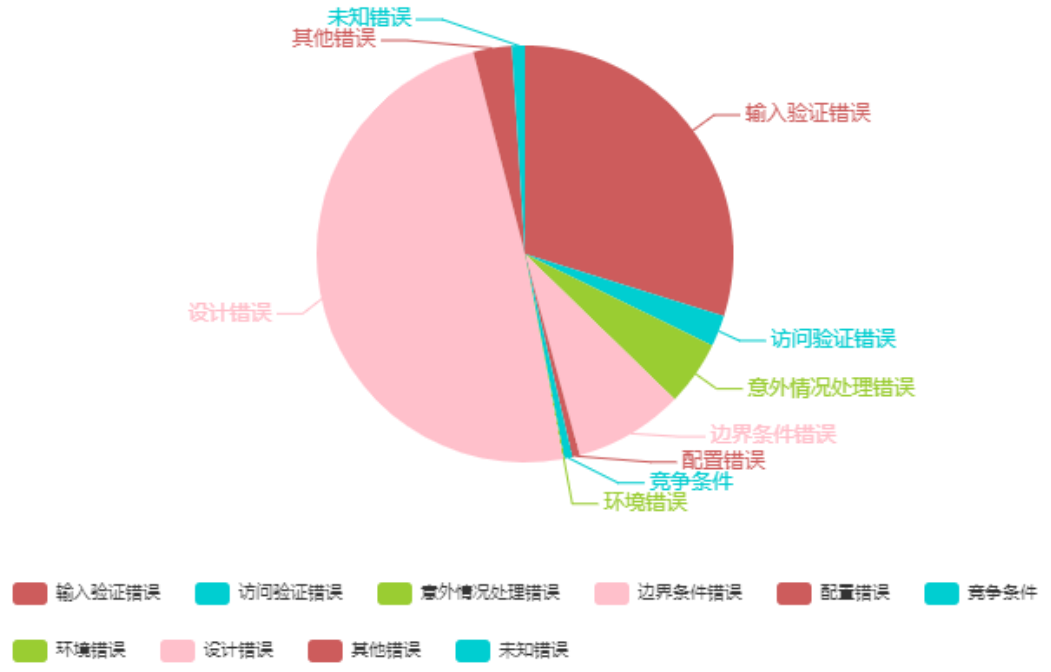
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

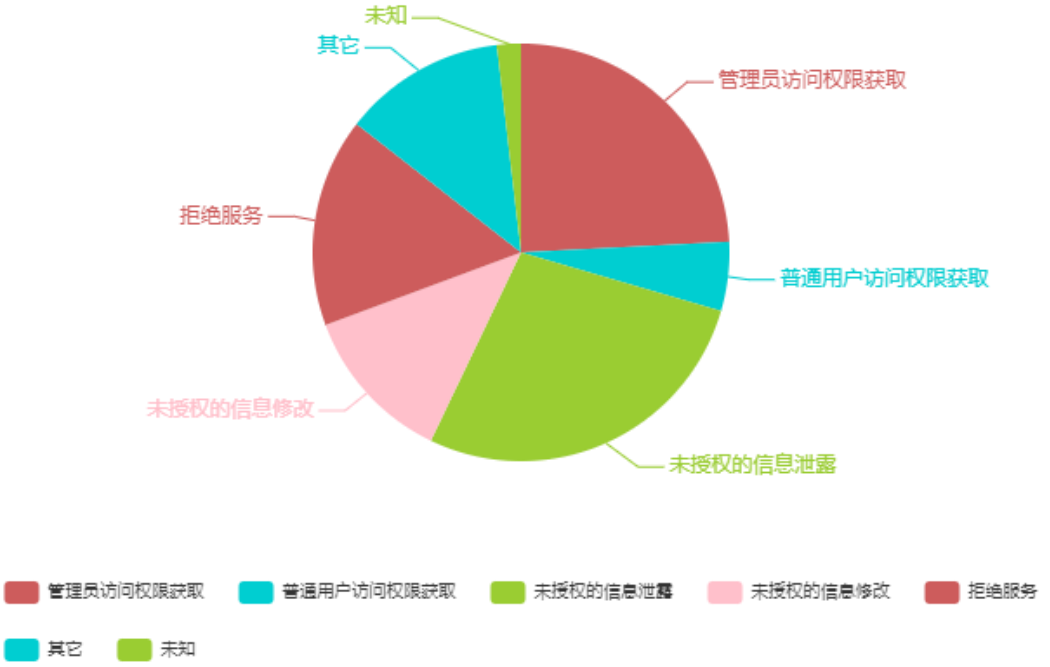
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 312 个，其中高危漏洞 92 个、中危漏洞 182 个、低危漏洞 38 个。漏洞平均分值为 5.84。本周收录的漏洞中，涉及 0day 漏洞 121 个（占 39%），其中互联网上出现“WordPress Ultimate Member 跨站点请求伪造漏洞、OpenEMR 远程代码执行漏洞（CNVD-2018-14867）”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 3956 个，与上周（5021 个）环比减少 21%。

二、安全漏洞增长数量及种类分布情况

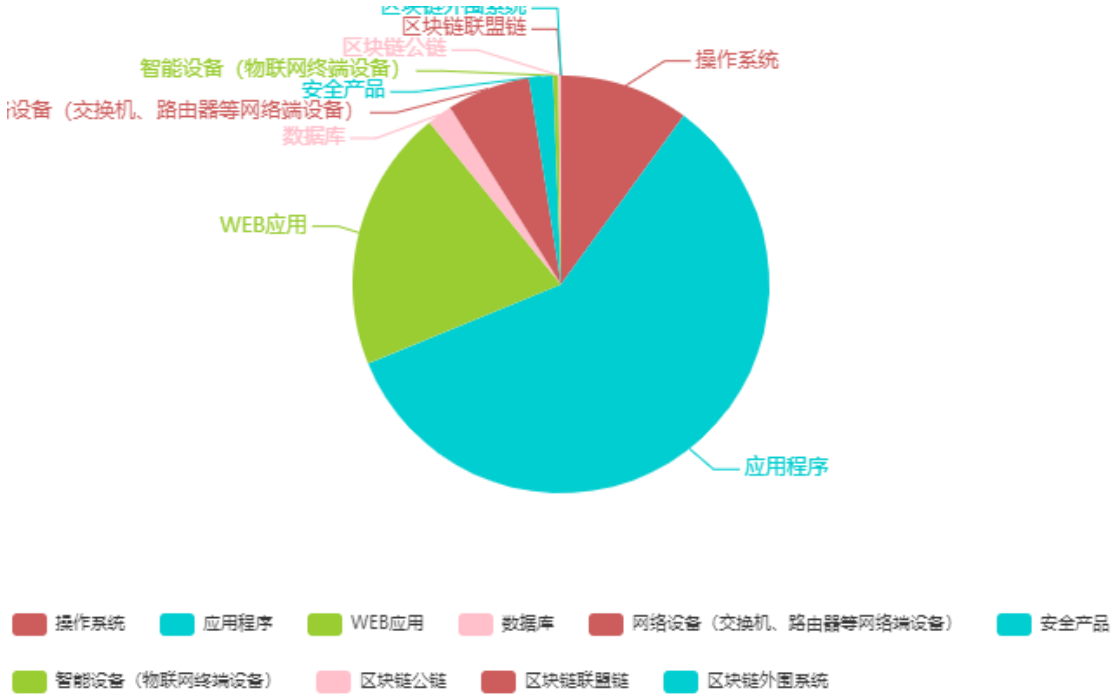
➢ 漏洞产生原因（2020 年 05 月 24 日—2020 年 06 月 07）



➢ 漏洞引发的威胁（2020 年 05 月 24 日—2020 年 06 月 07）



➢ 漏洞影响对象类型（2020 年 05 月 24 日—2020 年 06 月 07）



三、安全产业动态

➢ 民法典保护我们无处安放的隐私

2020 年 5 月 28 日，人民大会堂响起经久不息的掌声，十三届全国人大三次会议审议通过《中华人民共和国民法典》，中国的民事权利保障迎来了一个全新时代。互联网生活早已成为公共生活的一个庞大子集，这同时也给隐私保护带来了极大的挑战。我一身是嘴也说不清楚了。在经典电影《搜索》中，女主角因一小概率事件，而被“人肉搜索”。一夜之间，她所有的个人信息散布网络，毫无隐私可言。全城网民，藏在匿名 ID 背后，不计后果地指责女主角。被揭隐私的女主角，仿佛自己被强行剥光丢进人群中一般。这样的电影情节看似夸张，但现实生活中类似的事情确有发生。**很多人都在疑惑：轻点搜索就能知天下的今天，我们的隐私又该如何安放？**

日前，《中华人民共和国民法典（草案）》（以下简称民法典草案）就隐私权问题，对相关规定进行了多次修改、增加，旨在进一步保护人们的隐私权。

“互联网+”时代一丝不挂的个人信息

当下的我们，正活在一个信息爆炸，“娱乐至死”的互联网+时代。随着移动互联网、云计算、大数据、物联网以及区块链等技术的发展，实名认证、人脸识别、5G、AI 等越来越多

的新兴技术，也不断普及到了人们日新月异的生活中。与此同时，处于信息交流极其便捷、迅速这一大环境中的人们，也开始逐渐担忧自身隐私保护的问题。尤其是微博、微信朋友圈、贴吧、豆瓣、知乎等开放式网络社交平台的广泛应用，使得我们的个人信息在网上一览无余。

其中，“人肉搜索”是一种以互联网为媒介，网民们利用现代信息科学技术，以及匿名知情人提供信息的方式，搜集特定人或事的有关信息，以查找人物身份或事件真相。

关于“人肉搜索”最早的代表事件为“陈自瑶事件”，后来发生的“虐猫事件”“华南虎事件”“范跑跑事件”“躲猫猫事件”等多起事件，使得“人肉搜索”成为一种盛行于网络的群众运动。

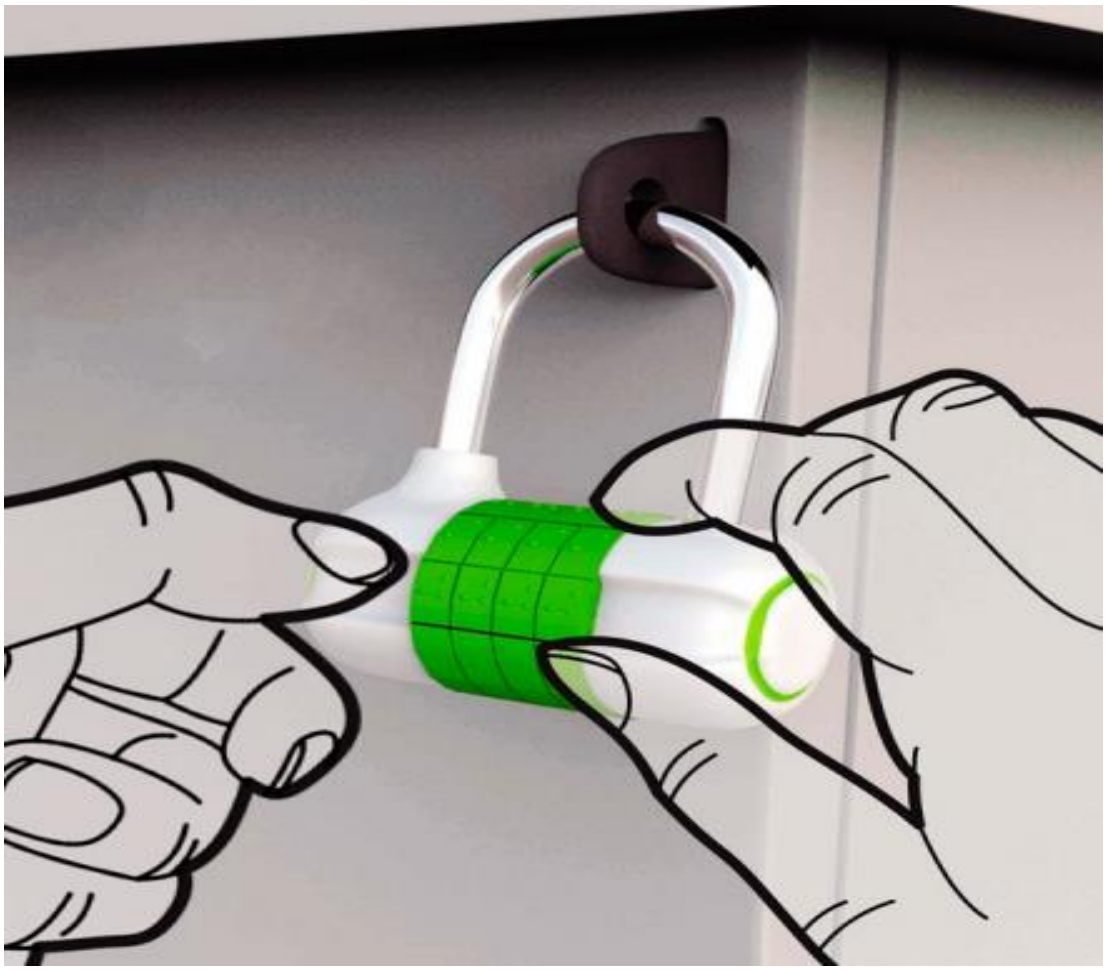
起初，“人肉搜索”在某种程度上能够起到惩恶扬善的作用，但一些网民超越道德和法律的底线，通过这种方式，将当事人的个人信息完全披露，并给当事人及其家人的生活产生巨大影响，甚至造成强烈的人身攻击。现今，过度的“人肉搜索”已经涉及侵犯人们的隐私权、名誉权、安宁权等多项权利。

曾经，北京一位女白领写下“死亡博客”后跳楼身亡，由此引出了中国第一次进入司法程序的“人肉搜索”案。女白领姜岩于生前两个月，在博客中以日记形式记载了自己的心路历程，并将丈夫真实的个人信息一同写入其中。伴随着姜岩的自杀，日记内容及其丈夫王菲的姓名、照片、住址、工作单位等身份信息全部被公之于众，从而被网民们“人肉搜索”。王菲也因此遭到了严重的人身攻击、私人生活的安宁被扰等不良影响。被“人肉搜索”的王菲将三家网站起诉至法院，最终其中两家网站被判侵犯王菲隐私权、名誉权。

由于侵犯隐私的问题频繁出现，以及人们对于隐私保护的迫切需要，同时法院也曾发出过应该对“人肉搜索”等新生网络事物进行正确引导的司法建议，从而引起了相关部门的高度重视。

本次民法典人格权编草案三次审议稿规定，隐私是自然人不愿为他人知晓的私密空间、私密活动和私密信息等。但也有一些法律人士提出，应将维护私人生活安宁、排除他人非法侵扰这一隐私权的重要内容，增加于隐私的定义中。

2019 年 12 月 23 日，提请十三届全国人大常委会第十五次会议审议的民法典草案，采纳了上述意见，将隐私的定义完善为隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。有委员表示，无论最初“人肉搜索”是出于何种善意，但现在这一行为已反向而行，正在逐步侵蚀着我们的生活。对于“人肉搜索”等一系列侵犯个人隐私的行为，我们应予以强烈反对，以维护我们的个人隐私。



新法草案全方位加强隐私保护

民法典人格权编草案不仅完善了对隐私的定义，在个人信息保护方面也作出了新的规定：自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码、电子邮箱地址、行踪信息等均属于个人信息的范围。

几年前，北京一名小学生小凡因在接受某电视台采访时说“上次我查资料，忽然蹦出一个窗口，很黄很暴力，我赶快给关了”。这一句话，引发了一场网络上的轩然大波。“很黄很暴力”瞬间成为爆款流行语，网友在恶搞的同时，也有人对小凡的话的真实性提出质疑。于是，网友们“人肉搜索”出了小凡的名字、出生年月日、所在学校、平时成绩以及所获奖励，甚至连她出生的医院也被搜出。

事情从最初的质疑，逐渐演变为讽刺、挖苦，进而升级为侮辱。一夜之间，一名未成年少女成为一众网友攻击的对象。网民们还通过视频、图片、恶搞漫画、帖子等形式疯狂恶搞“很黄很暴力”，甚至还有人用色情漫画来影射小凡。

小凡的个人信息暴露得如此彻底，与“人肉搜索”密不可分，但各类信息科学技术的突飞猛进，也使得我们的隐私在网络共享。使用身份证实名制认证后，所有的个人信息便一目

了然，这也是令我们担忧的问题之一。

对此，一些专业人士称，此种行为已严重侵害到了未成年人的隐私权。并指出通过网络舆论侵犯人们个人隐私，是一个相当大的问题，同时也呼吁加强对未成年人个人信息的保护。

近些年，有关侵犯未成年人隐私的案件不断增多。曾有一家网站采访了某教育中心，随后该网站刊出关于《探访北京戒网瘾学校》的照片和文章。此网站在未取得未成年人法定代理人同意的情况下，私自使用未经模糊处理的未成年人付某的正面全身照，并配有与“上网成瘾”有关的文字。这种擅自曝光未成年人个人隐私和个人信息的行为，已严重侵犯了未成年人的隐私权

本次民法典人格权编草案也专门对未成年人个人信息保护作出了新规定：收集使用未成年人等无民事行为能力人或者限制民事行为能力人的个人信息的,应当征得其监护人同意,但是法律、行政法规另有规定的除外。以此更好地保护未成年人的个人隐私。

此外，还特别增加了对履职过程中知悉个人信息的国家机关及其工作人员的相关规定：国家机关及其工作人员对于履行职责过程中知悉的自然人隐私、个人信息,应当予以保密,不得泄露或者非法向他人提供。

民法典人格权编草案同时还增加了任何组织或者个人不得搜查、进入、窥视、拍摄他人的宾馆房间等私密空间这一重要规定。从而严厉打击宾馆房间私装摄像头偷拍等此类恶劣行为，全方位保护我们的个人隐私。

“大护法”增强民众安全感

现在处于“互联网+”时代的我们，无论做任何事均脱离不了无处不在的网络。很久没去过医院的记者，在不久前去某医院看病时，不再需要病历本，一刷自己的医保卡，所有信息和既往病史全部出现在医生的电脑上。虽然节省了时间，但这同时也增加了个人信息、隐私安全的隐患。

不光是民法典人格权编草案对隐私的有关内容进行了修改补充，民法典侵权责任编草案也进一步完善了网络侵权、患者隐私及个人信息保护等方面的规定。

产妇刚生完孩子，早教机构就发来的“贺喜”短信无缝衔接；病患刚做完手术，康复中心便立即来电自荐。如此令人“窒息”的操作，很多人都经历过。当下，很多医生在为病人检查时，经常会带着四五个实习医生，且有男有女。当自己的身体暴露在众目睽睽之下时,大部分病人都会感到非常难堪。患者遇到医疗检查时被实习生观摩的情况常有发生。有些患者表示拒绝后，有的医生会称这种情况很正常。对于医者来说这已是司空见惯的事，但患者不是医生，他们无法理解这种医学上的学习。因此医生在做类似行为之前，也应事先征得病人

的同意。

民法典侵权责任编草案将相关规定修改为：医疗机构及其医务人员泄露患者隐私和个人信息或者未经患者同意公开其病历资料，应当承担侵权责任。

在青岛某大医院产科发生过一起案件。案犯胡肖明、冯晓、刘奇先后通过该医院的两名年轻产科护士，非法获取产妇及其家庭联系电话等各种信息，并通过售卖信息非法牟利。这两名年轻的女护士，通过微信在一年多的时间里，总共提供了包括姓名、联系电话、出生时间、家庭住址在内的近 1.3 万条产妇相关信息。医疗机构及其医务人员泄露患者隐私和个人信息，或擅自公开患者病历资料属于严重的侵权行为。最终，被告六人因侵犯公民个人信息罪，受到了应有的处罚。

民法典侵权责任编草案的修改，意味着无论其所作行为是否对病患造成损害，医疗机构及其医务人员均应承担相应的侵权责任。在更好地保护患者隐私的同时，对医疗工作者们也起到警示作用，让患者们可以安安心心看病来，健健康康回家去。

随着社会的发展，很多新问题也随之而来。民法典草案这一“大护法”正在针对当今社会的各类问题，进行不断的更新、完善，保护我们无处安放的隐私，给予民众更多的安全感。

（来源：《人民法治》）

➢ 使用民生相关 App 请认准官方版，防范山寨/高仿 App 套取个人信息！

1、“高仿/山寨”App 现象突出

当下，各式各样的 App 已成为我们生活、工作等的必需品，据统计，近 9 亿网民中手机上网比例高达 99.1%，移动互联网服务便捷、即时、普惠的特点在 App 中得到充分体现，用户每天在各类 App 上平均花费时长达 4.9 小时，占用户日均上网时长的 81.7%。因此，开发、运营 App 成为很多企业和机构为用户提供服务的优先选择。但是，一款成熟的 App 从设计、开发、运营要耗费大量人力物力，日积月累方可赢得用户对其品牌的认可，而此时，个别机构、个人却打起了“模仿、抄袭”的歪心思，短短几周甚至几天，就可以开发出一款图标、外观、名字与正版 App 极为相似，凭肉眼很难分辨的“高仿版”“山寨版”，甚至想方设法在常见“应用商店”上线，吸引用户下载使用。据统计，一款下载量超过 1 亿的 App，市场上会出现几百种各式各样的“山寨货”。

2、民生领域，非官方 App 可能存在套取个人信息风险

民生领域关系着广大群众衣食住行等根本问题，是检验群众幸福感、获得感的最重要标尺之一。近年来，涉及社保、治安、交通、教育、医疗、就业等民生相关领域的社会服务已经都逐步从线下转移到线上，随着互联网普及及上网技能被越来越多民众所掌握，“一站式购票缴费”、“数据多跑路，群众少跑路”、“一网通办”等已经成为当下有关部门重点推行的便民措施。然而，当提供社会服务的官方机构开始通过 App 等方式向大众提供“便捷”“免费”的服务时，有些“机构和个人”趁机开发出一些“非官方”App，有部分甚至通过“高仿/山寨”方式直接欺骗用户使用，直接盗取用户个人信息或诱骗用户转账、充值；有的通过扮演“中间人”“代理人”角色，在为用户提供服务的同时，掌握了用户大量个人信息，个别还打起了使用用户个人信息进行推送商业广告、借贷等进行变现的“小算盘”。

近期，就有媒体曝光有网友在使用非官方社保、公积金查询 App 后，自己频繁收到推销贷款、购房的骚扰电话，还有网友使用“山寨版”12306 购票 App，在使用抢票功能后被骗取手续费用。总之，虽然不能直接断定非官方 App 一定存在问题，但与民生领域官方推出的 App 相比，非官方的 App 除了使用个人信息达成相应服务目的后，是否会长期留存收集的个人信息，个人信息怎么用、用在哪？往往是一个未知数。因此，如果相关民生领域已经发布了官方版 App，建议广大网友尽可能识别并避免使用“非官方”的 App，防止个人信息可能被泄露、滥用。

3、认准常用民生类“官方 App”

以下是简单归纳的一些官方和非官方 App 的对比，仅供参考：


用途
官方
非官方APP
买火车票
铁路12306
中铁程科技有限责任公司
获取
发布者：中国铁路总公司
抢票王 - 12306秒杀神器
获取
发布者：个人
火车票轻松购 for 12306火车票官网
获取
发布者：个人
违章缴费
交管12123
公安部交通管理科学研究所
获取
发布者：公安部交通管理科学研究所
车助手查违章-12123交管直连查询快速准确
获取
发布者：某企业
12123查违章-交管局数据直连
获取
发布者：某企业
查缴话费
中国移动（手机营业厅）
China Mobile Limited
获取
发布者：中国移动
中国联通手机营业厅客户端(官方版)
中国联合网络通信有限公司
打开
发布者：中国联通
电信营业厅-新人领豪华大礼包
CHINA TELECOM Corporation Ltd.
获取
发布者：中国电信
流量营业厅-移动联通电信掌上营业厅！
获取
发布者：个人
中国移动网上营业厅-实体店查查！
获取
发布者：个人
查缴电费
网上国网
国家电网公司
获取
发布者：国家电网
电费查询- 国家电网电费查询
获取
发布者：个人
一度店-国家电网掌上电费充值
获取
发布者：某企业
个人所得税
个人所得税
国家税务总局
打开
发布者：国家税务总局
个人所得税2019最新
获取
发布者：个人
个人所得税计算-2019最新版APP
获取
发布者：个人
社保查询
掌上12333
人力资源和社会保障部信息中心
获取
发布者：人力资源和社会保障部信息中心
12333兼职-招聘求职兼职平台
获取
发布者：个人
掌上12333公考版
发布者：个人
医保查询
国家医保服务平台
国家医疗保障局
获取
发布者：国家医疗保障局
医保通
获取
发布者：某企业
掌上医保
发布者：某企业
消费投诉
全国12315平台
国家工商总局
获取
发布者：国家工商总局
消费保-315维权投诉
获取
发布者：某企业
化妆品查询
化妆品监管
中国食品药品监管数据中心
获取
发布者：中国食品药品监管数据中心
化妆品监管查询-测肤美妆查询
获取
发布者：个人
药品查询
中国药品监管
中国食品药品监管数据中心
发布者：中国食品药品监管数据中心
食品药品监管平台
发布者：某企业
学籍查询
学信网
中国高等教育学生信息网（学信网）
获取
发布者：中国高等教育学生信息网
学历-直连学信网
获取
发布者：某企业

4、如何判断 App 是否为官方出品？

从上图中的信息不难看出，一般来说，对于政府部门、公共服务机构等发布的 App，最主要的是要认准发布单位，如果不是职能部门或下属机构发布的 App，则需要再三查看评论，或者充分试用确保无误；其次，政府部门、公共服务机构等发布的 App 名称简洁，不夹带“最新版”“快速版”“优惠版”等诱导性强的用词。但是，需要注意的是，一些非官方版本的 App 可能会采取竞价排名、流量引导、虚假刷量等方式，吸引用户下载使用，政府部门、公共服务机构等发布的 App 在应用商店、搜索引擎等的排名中不一定排名靠前。此外，很多政府部门、公共服务机构只是通过网站提供服务，并没有发布其官方 App，但是，还是出现了一些 App 打着“权威”“官方”等名义的擦边球，通过“代理人”方式在 App 内为用户提供服务，被很多人误以为是官方出品并长期使用，因此，查看并认准发布方身份非常关键。

不光如此，很多企业发布的 App 也会被“高仿/山寨”，导致网民遭受“诈骗”“钓鱼”，引发财产受损，个人信息泄露等。

5、如何对“高仿/山寨 App”进行治理的思考

“高仿/山寨 App”为何屡禁不止？要回答这个问题，我们不妨做以下探讨：

首先，如何界定什么是“高仿/山寨”一直是个难题。如果是从名称、功能、图标、界面、宣传方式等角度发现 App 之间是否存在相似性来看，恐怕很难给出一个相对固定的标准，如果从商标、产权等角度去衡量，问题的复杂性可能更高，因为大量 App 的功能、服务模式等本身就是高度同质化的状态，即使引发“口水战”、“打官司”，恐怕是旷日持久，很难短时间内改变现状。

其次，应用商店能否进行公正把关同样是难题。有人说，为什么应用商店还会允许“高仿/山寨 App”上线，其实逻辑很简单，因为应用商店无法解决好刚才提出的界定“高仿/山寨 App”的难题。应用商店会根据国家有关法律法规以及相关监管要求，对 App 进行审核和管理。同时，出于应用商店之间的市场竞争机制，不断充实、丰富应用市场中 App 的类型、数量，吸引更多用户使用往往成为其核心经营思路。一旦从“是否为高仿/山寨”角度进行审核，一则审核机制谁来定，谁来审，其过程很难保证公正性，操作不当很有可能会被沦为竞争对手互相打压的工具；二则是否因为审核等原因会导致原有的市场竞争机制被破坏？会对鼓励创新等的氛围和环境造成影响？缺乏了新鲜血液循环，是否会导致应用市场活力、竞争力等下降等都是个未知数，利弊很难评判。

再者，开发“高仿/山寨 App”的成本低，其频繁改头换面等都加大了对其审核监督的难度和成本，另一方面，部分网民对手机系统、应用商店、常用软件等的基本情况还不够了解，

不少人对“优惠”“破解”“秒杀”“红包”等诱导性词缺乏抵抗力，未做慎重观察，直接注册使用，这也间接让恶意的“高仿/山寨 App”有机可趁，趁机牟利。

将个人信息保护的要求作为审核点可能是突破口

从上文分析来看，“高仿/山寨 App”有一个普遍的共性问题，就是在其收集使用个人信息方面存在问题甚至存在违法违规行为。以此为出发点，假如抛开“高仿/山寨 App”的界定等难点问题，就从个人信息保护的审核监督出发，如果促使存在违法违规收集使用个人信息行为的 App 不会再被用户下载使用，同样可以达到防止用户利益遭受侵害的目的。

然而，如要达成以个人信息保护为审核点避免“高仿/山寨 App”被下载使用，则需要执行对数百万款 App 收集使用个人信息行为动态、全覆盖式的审核监督。除了依赖专业的检测评估力量、高效的技术监督手段外，还需要制定相应的审核规则与应用商店等关键角色的深度参与，这就有待在持续开展 App 违法违规收集使用个人信息的治理工作过程中，深入研究和完善相关标准规范、协作程序、技术手段，形成常态化监督管理机制。

对“民生”密切相关 App 的几点建议

就当下，如何能进一步引导和保障民众安心使用“民生”密切相关 App，有以下建议供参考：一是继续推进 App 安全认证相关工作，尤其是重点民生领域 App 的安全认证，并由应用商店等进行优先展示、推介；二是充分调研有关职能部门发布的民生紧密相关领域已有 App 情况，由有关官方机构提供专用标识，设置下载专区，加大宣传力度，引导民众使用；三是持续受理民众和 App 运营单位对“高仿/山寨 App”违法违规收集使用个人信息行为的举报，进一步加大对“高仿/山寨 App”的曝光和监督管理力度；四是持续开展民众安全意识宣传科普活动，强化民众对“高仿/山寨 App”的识别能力，提升个人信息保护意识和技能。

6、结语

“高仿/山寨”App 一方面在用户使用时可能带来安全隐患，另一方面给公平竞争环境、创新活力带来挑战，在持续治理完善移动互联网生态过程中，是始终绕不开的难题之一。移动互联网的繁荣发展，App 数量是一种体现，但 App 质量更是关键，只有 App 质量过硬、用户肯定、安全可信，才能涌现出更多真正有竞争力的优秀 App，更好地服务于经济民生。（来源：APP 治理工作组）

➢ 开启网络安全审查制度建设 2.0 时代

《网络安全审查办法》将于今年 6 月 1 日正式实施，这是网络空间安全形势日益复杂、对抗性加剧的国际环境下，进一步完善我国网络安全体系建设，落实习近平总书记“加快构建关键信息基础设施安全保障体系”的重大举措，是加固我国网络空间安全的一道独特有效屏障。

一、《办法》出台具有重大现实意义

随着我国网络空间安全战略的构建与实施，网络安全审查法制化建设也走上了快车道。2015 年 7 月通过的《中华人民共和国国家安全法》第五十九条规定：“国家建立国家安全审查和监管的制度和机制，对影响或者可能影响国家安全的外商投资、特定物项和关键技术、网络信息技术产品和服务、涉及国家安全事项的建设项目，以及其他重大事项和活动，进行国家安全审查，有效预防和化解国家安全风险”。该法明确提出对网络信息技术产品和服务等进行国家安全审查，成为《网络安全审查办法》(以下简称《办法》）的基础。2016 年 11 月通过的《中华人民共和国网络安全法》第二节“关键信息基础设施的运行安全”中的第三十五条规定：“关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查”，标注了网络安全审查法治化建设的“零公里”。

2017 年 5 月，国家互联网信息办公室发布《网络产品和服务安全审查办法(试行）》（以下简称《试行办法》），可以视为我国网络安全审查制度 1.0 版。2020 年 4 月 13 日，国家互联网信息办公室等十二部委以部委令方式公布新《办法》，是在 2017 年《试行办法》的基础上，结合网络空间安全形势制定的网络安全审查制度的 2.0 版，标志着我国网络安全审查法治建设进入新时代，意义重大。

一是应对当前网络空间日益复杂安全形势的需要。据国家互联网应急中心（CNCERT）

公布的《2019 年我国互联网安全态势综述》报告，2019 年，我国持续遭受来自“方程式组织”“APT28”“蔓灵花”“海莲花”“黑店”“白金”等 30 余个 APT 组织网络窃密攻击，我国党政机关、国防军工和科研院所，以及通信、外交、能源、商务、金融、军工、海洋等行业、物联网和供应链等领域成为重点攻击对象，国家网络空间安全受到严重威胁。而这类攻击都是通过利用第三方产品和安全漏洞或薄弱环节入侵关键信息系统的，供应链安全风险十分突出。据国家信息安全漏洞库（CNNVD)报告，2019 年，新增通用软硬件漏洞数量 16374 条，达到历年最高点，其中，高危漏洞首次达到近一半的占比，且国外厂商漏洞数量占较大比重，输入型漏洞带来的风险加大。这些漏洞影响范围从主流操作系统到最常见的应用产品，广泛影响我国基础软硬件安全及其应用安全，危及我国家安全，因此，加强网络安全审查十分必要与迫切。

二是防范我网络产品和服务市场快速增长面临风险的需要。我国拥有规模庞大的信息基础设施，是网络产品和服务市场增长速度最快的国家。仅以网络安全领域市场为例，据国际数据公司（IDC）数据显示，2019 年，全球网络安全相关硬件、软件、服务投资约为 1066.3 亿美元；2019 年至 2023 年，全球网络安全相关支出复合年均增长率约 9.44%；2023 年，将达到 1512.3 亿美元。2019 年，中国网络安全市场总体支出约为 73.5 亿美元；2019 年至 2023 年，中国网络相关支出复合年均增长率为 25.1%,增速领跑全球，2023 年，支出将达到 179 亿美元。虽然我国占全球网络安全市场份额仅 10%多一点，但是增长速度领跑世界，潜力巨大。我国基础设施的供应商主要来自国外，一些核心产品如芯片、高科技材料、关键部件仍大量依赖进口。因此，网络产品和服务的供应链安全与否，供应渠道的可靠与否，直接关系到我网络安全，特别是在推进“新基建”的关键时期，《办法》的出台恰逢其时，是对诚信守法供应商的保护，更是对网络攻击等非法行为的威慑。

三是完善我国网络空间安全治理体系和治理能力现代化的重要举措。加强网络安全审查制度建设，全面提升网络安全审查能力，是贯彻习近平总书记推进治理体系和治理能力现代化重要思想的具体体现。建立网络安全审查制度，是我国国家治理体系不可缺少的重要一环，目的是及早发现并避免采购产品和服务给关键信息基础设施运行带来风险和危害，保障关键信息基础设施供应链安全。《办法》的出台，为我国开展网络安全审查工作提供了重要的制度保障，是我国网络空间安全积极防御，推进实施网络强国战略的重大举措。

四是和平利用网络空间、坚定维护网络空间安全战略的体现。《办法》借鉴了美西方发达国家网络安全审查制度，并结合了自身实际和我国网络空间安全“新理念”而制定。美国、英国、德国、澳大利亚、俄罗斯等国已先后建立网络安全审查制度，通过设立专门的审查机

构，制定审查标准，委托第三方认证等措施，对关键基础设施的产品和服务开展安全审查，包括对供应商的背景进行审查，排除安全风险和漏洞。我国制定网络安全审查制度，是通过法制手段保障国家安全，减少网络空间技术对抗与冲突的有力措施，是推动构建网络空间命运共同体的具体举措。

二、网络安全审查工作的法律保障大大增强

《办法》第一条明确《国家安全法》《网络安全法》是上位法，据此制定的《办法》具有强有力的法律约束，体现在如下几点：

一是审查对象法定化。《办法》第二条规定：“关键信息基础设施运营者（以下简称运营者）采购网络产品和服务，影响或可能影响国家安全的，应当按照本办法进行网络安全审查”，定义了直接审查对象为关键信息基础设施运营者对网络产品和服务的采购行为；第六条“对于申报网络安全审查的采购活动，运营者应通过采购文件、协议等要求产品和服务提供者配合网络安全审查”，明确了产品和服务的提供者是间接审查对象，使审查对象鲜明清晰法定。《办法》第二十条强调了“关键信息基础设施运营者是指经关键信息基础设施保护工作部门认定的运营者”，根据中央网络安全和信息化委员会《关于关键信息基础设施安全保护工作有关事项的通知》精神，电信、广播电视、能源、金融、公路水路运输、铁路、民航、邮政、水利、应急管理、卫生健康、社会保障、国防科技工业等行业领域的重要网络和信息系统运营者在采购网络产品和服务时，应当按照《办法》要求考虑申报网络安全审查。较《试行办法》直接针对“网络产品与服务”的审查，该《办法》将审查对象聚焦在运营者，其采购行为主体更加鲜明突出，防止被外国厂商误读。

二是审查工作主体法定化。《办法》第四条首先明确了网络安全审查工作是在中央网络安全和信息化委员会领导下，由国家互联网信息办公室及发改委、工信部、公安部、国家安全部、财政部、商务部、人民银行、国家市场监督管理总局、广播广电总局、保密局、密码管理局 12 个部委建立国家网络安全审查工作机制，网络安全审查办公室设在国家互联网信息办公室，负责制定审查制度规范，组织网络安全审查。将审查工作的主体通过行政法规确定下来，较《试行办法》更加透明、清晰、规范。

《办法》第十条规定：“网络安全审查办公室在规定时间内对运营者的申请进行初步审查，包括形成审查结论建议和将审查结论建议发送网络安全审查工作机制成员单位、相关关键信息基础设施保护工作部门征求意见”，该表述除明确了开展审查工作的主体单位是 12 个部委外，还有“相关关键信息基础设施保护工作部门”，强调了审查机制中各部委和关键信息基础设施保护工作部门依法行政的主体责任。

三、网络安全审查工作更聚焦核心安全利益

《办法》在审查工作内容上体现了新的网络安全观，审查重点更加清晰，操作性更强。

一是审查目标的调整是践行习近平总书记“树立正确的网络安全观”的体现。《办法》第一条审查目标强调的是“为了确保关键信息基础设施供应链安全”，将关键信息基础设施供应链安全作为审查目标的关注重点，更看重的是产品和服务的使用主体、使用目的、使用方式以及产品供应渠道的可靠程度等综合因素，深入贯彻了习总书记关于“网络安全是整体的而不是割裂的”“是相对的而不是绝对的”理念。《办法》较《试行办法》将安全审查目标放在“网络产品和服务的安全可控水平”等脆弱性上，不仅是着眼点的调整，也是对网络安全理念认识的提升。

二是审查重点更加明晰。《办法》第九条明确了重点评估采购网络产品和服务可能带来的国家安全风险的 5 个主要考虑因素。首先，将“产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏，以及重要数据被窃取、泄露、毁损的风险”作为第一项评估的风险因素，突出体现了当前网络安全面临的风险和隐患的实质和鲜明特点。其次，考虑了产品和服务供应一旦中断对关键信息基础设施业务连续性带来的危害。第三，强调了“产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险”，突出体现了对网络空间安全属性的把握，开放、透明、多样性符合国际贸易规则，对国内供应商和国外供应商一视同仁，有利于推进构建网络空间命运共同体。第四，新增加了“产品和服务提供者遵守中国法律、行政法规、部门规章情况”等非技术性因素，取代了《试行办法》中的背景审查的表述，符合依法审查的理念，更显国际通用性，审查重点更加突出清晰。

三是审查工作更具操作性。《办法》较《试行办法》新增了 6 条，在操作程序和时限、知识产权保护、保密、监督问责等方面都有更加明确的表述。首先，调整了网络安全审查的启动机制，由《试行办法》中根据国家有关部门的要求、全国性行业协会建议、市场反映和企业申请四种启动方式，调整为由运营者申报和“网络安全审查工作机制成员单位认为影响或可能影响国家安全的网络产品和服务，由网络安全审查办公室按程序报中央网络安全和信息化委员会批准后，依照本办法的规定进行审查”，可见，启动审查的环节虽然减少了，相关部委可提出审查要求，但是审批权限上调了，启动条件更加严格。其次，增加了风险预判机制，要求运营者采购网络产品和服务时，应预判安全风险，对影响或可能影响国家安全的，应当向网络安全审查办公室申报网络安全审查，将安全关口前移至初始和前端。第三，操作程序更加清晰透明，对安全审查运营者所需提交的四项申请材料做了明确规定；对网络安全

审查办公室的初步审查、征求意见、启动特别审查程序做了清晰规定，特别是新增加了不同阶段审查工作的时限等。第四，对保密、监督、问责等事宜做了明确规定。

四、《办法》落地实施亟待配套规程

《办法》尽管已具有较强的操作性，但毕竟是原则性的，在具体实施中，仍需要更详细的操作规程支撑。因此，一是建议国家互联网信息办公室尽快出台网络安全审查工作实施细则，进一步优化审查工作流程；制定风险预判标准等，让审查机构、运营者、产品和服务提供者有规可依，操作便利。二是建议国家互联网信息办公室牵头建立部级联席会议机制，确定一批具有信息安全检验检测资质、国内外普遍认可、不以赢利为目的的国家级测评机构作为第三方机构，提供网络安全审查技术支持。三是建议提高审查工作信息化水平，共享审查项目信息，让数据多跑路，让审查机构、运营者、供应商少跑腿，提高效率。使网络安全审查工作真正做到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，充分发挥好网络安全审查制度的独特安全屏障作用。（来源：《中国信息安全》杂志 2020 年第 5 期）

➢ 数据安全立法，需平衡好各方诉求

今年的全国人大常委会工作报告日前提交审议，工作报告中提到，备受关注的《个人信息保护法》和《数据安全法》正在制定中。这是继《网络安全法》之后，我国在网络安全领域另外两部重要法律。

这两部法律的核心命题围绕着数据安全问题，试图为信息社会奠定基本规则体系。随着信息化水平和互联网用户数量的不断提高，我国已经成为全球范围内首屈一指的数据大国。一方面，数据驱动了经济发展，一批在全球具有重要影响力的中国互联网企业因此而诞生；

另一方面，个人隐私泄露、数据安全问题频发不仅给用户造成了很大伤害，也在威胁着社会稳定和国家安全。

目前，全球各国纷纷加快了数据安全的立法工作。如欧盟制定和实施了极为严格的《通用数据保护条例》，保护欧盟境内的个人信息安全。我国在保护个人信息安全和数据安全方面也开展了一系列工作，如国家互联网信息办公室指导制定了《个人信息保护规范》，发布了《数据安全管理办法(征求意见稿)》，对保护我国的数据安全发挥了重要作用。

开展《个人信息保护法》和《数据安全法》立法工作，将原有的技术标准、部门规章提升到法律层面，表明了我国政府对于数据保护的重视程度在不断增加。同时，也是因为数据所带来的价值、引起的争议、造成的破坏在不断提升，需要从全局的层面予以应对。从个人角度来看，数据是个人信息，事关个人隐私，需要得到严格保护。从企业角度来看，数据是重要资产，具有重大商业价值。从政府角度来看，既要回应公众对个人信息保护的需求，也要保障企业合理使用数据的空间。同时，政府开展社会治理、维护公共安全也离不开数据的使用。当涉及到国家之间的竞争时，数据还被认为是信息社会的“石油”，具有重要的战略价值。因此，这两部法律需要解决的问题非常重要，牵涉到了国家、社会和个人不同的诉求，是极为复杂的问题。笔者认为：

一是要尽可能多地让公众参与到立法进程中，聆听公众对这两部法律的声音。个人是最重要的数据生产者，同时，也面临着个人信息滥用、隐私泄露的巨大风险。引导公众充分参与立法进程的讨论，不仅有助于培养公众个人信息保护意识，也能够让立法者更好地倾听公众的诉求，从而更加科学合理地制定法律。

二是两部法律的制定需要平衡各方的利益诉求。虽然不同行为体之间不是零和关系，但法律也需做出一定的取舍。因此，如何去平衡个人隐私、企业发展和国家安全是两部法律面临的重要任务。

三是处理好两部法律之间的关系。《个人信息保护法》更多的是从保护公民隐私的角度来看待数据安全问题，而《数据安全法》更多是从国家安全、公共安全角度出发，因此导向也会存在差异。这需要在立法的进程中统筹考虑，让两者相互配合、有效衔接，共同维护我国的数据安全和数据主权。

四是立法需要充分考虑信息社会的大背景和技术的发展，避免用工业化时代的思维来制定信息社会的法律。立法者需要对人工智能、大数据、云计算等新兴技术发展和应用有一定的前瞻性理解。同时，也要注重通过新兴技术来解决保护个人信息和数据安全中所面临的问题。（来源：环球时报）

四、政府之声

➢ 第七次全国人口普查准备中，泄露个人信息将依法追责

2020 年 6 月 1 日，《全国人口普查条例》正式实施，今天刚好是施行 10 周年。当前第七次全国人口普查准备工作正在各地如火如荼进行中。10 年来，《全国人口普查条例》（以下简称《条例》）施行情况如何，在保障人口普查顺利进行方面发挥了怎样的作用？《条例》如何持续护航第七次全国人口普查进行？国务院第七次全国人口普查领导小组办公室负责人回答了相关热点问题。

问题一：今年是《全国人口普查条例》施行 10 周年，请问在人口普查实施过程中，《全国人口普查条例》发挥了怎样的作用？

答：人口普查是重大的国情国力调查，是和平时期最大的社会动员，涉及每一个人、每一个家庭以及社会的各个方面，需要社会各界及公众的理解、支持与配合。今年在疫情防控常态化下开展人口普查，更需要调查对象和调查人员共同努力。

《条例》对普查目的、普查原则、普查任务、普查对象、普查范围、普查的组织实施等作出了明确规定。对于科学、有效地组织实施全国人口普查，依法保障人口普查的有序开展，维护人口普查对象的合法权益，赢得普查对象的信任、支持与合作，保障人口普查数据的真实性、准确性、完整性、及时性，发挥了重要作用。

问题二：《全国人口普查条例》是如何促进人口普查对象积极配合第七次全国人口普查的？

答：《条例》对人口普查的对象、内容、方法、组织实施、普查资料管理和公布、法律责任等做出明确规定，对普查对象、普查机构和普查人员在人口普查活动中的权利、义务以及违法行为所应承担的法律责任等做出具有法律效力的严格界定。

今年实施的第七次全国人口普查将采取电子化方式开展普查登记，可以由普查员使用

PAD 或智能手机入户登记数据直接上报，也可以由普查对象通过互联网自主填报。同时，此次普查还将广泛应用部门行政记录，通过在普查指标设置中增加公民身份号码，实现与公安、卫健等部门行政记录的比对核查。

同时，对于人口普查对象需要履行的普查义务，《条例》规定：人口普查对象应当按照《中华人民共和国统计法》和本条例的规定，真实、准确、完整、及时地提供人口普查所需的资料。人口普查对象应当如实回答相关问题，不得隐瞒有关情况，不得提供虚假信息，不得拒绝或者阻碍人口普查工作。

问题三：在人口普查中，人们会担心个人信息泄漏，《全国人口普查条例》如何规定人口普查中获得的个人信息必须严格保密？

答：《条例》对保护人口普查对象的合法权益作了非常明确的规定：

一是人口普查对象提供的资料，依法予以保密；

二是人口普查中获得的能够识别或者推断单个普查对象身份的资料，任何单位和个人不得对外提供、泄露，不得作为对人口普查对象作出具体行政行为的依据，不得用于普查以外的目的；

三是人口普查中获得的原始普查资料，按照国家有关规定保存、销毁；

四是对泄露或者向他人提供能够识别或者推断单个普查对象身份的资料的行为，依法追究法律责任。

同时，《国务院关于开展第七次全国人口普查的通知》也明确提出，“全流程加强对公民个人信息的保护，各级普查机构及其工作人员必须严格履行保密义务，严禁向任何机构、单位、个人泄露或出售公民个人信息。”

第七次全国人口普查将采取电子化方式开展普查登记，登记方式的改变，减少了数据收集上报的中间环节，提高了普查数据质量，也加强了对个人信息安全的保障。

问题四：《全国人口普查条例》为保证人口普查数据质量作出了哪些规定？

答：保证人口普查数据真实可靠、准确完整，是人口普查的核心要求，也是衡量普查成功与否的重要标准。为了保证人口普查数据质量，《条例》规定：

一是明确普查机构、普查人员依法独立行使调查、报告、监督的职权，任何单位和个人不得干涉。地方各级人民政府、各部门、各单位及其负责人，不得自行修改普查机构和普查人员依法搜集、整理的人口普查资料，不得以任何方式要求普查机构和普查人员及其他单位和个人伪造、篡改人口普查资料，不得对依法履行职责或者拒绝、抵制人口普查违法行为的普查人员打击报复；

二是要求人口普查对象应当在普查表上签字或者盖章确认，并对其内容的真实性负责；

三是要求普查机构和普查人员不得伪造、篡改普查资料，不得以任何方式要求任何单位和个人提供虚假的普查资料；

四是规定人口普查实行质量控制岗位责任制，普查机构对人口普查实施中的每个环节实行质量控制和检查，对人口普查数据进行审核、复查和验收；五是规定国家统计局统一组织人口普查数据事后质量抽查；六是明确了对普查数据弄虚作假等行为的处理规定。

问题五：如果人口普查中有违法行为，《全国人口普查条例》规定如何处理？

答：《条例》对人口普查中三类主体的违法行为及其法律责任作出了明确规定：

一是地方、部门、单位的负责人自行修改人口普查资料、编造虚假人口普查数据的，要求有关单位和个人伪造、篡改人口普查资料的，不按照国家有关规定保存、销毁人口普查资料的，违法公布人口普查资料的，对依法履行职责或者拒绝、抵制人口普查违法行为的普查人员打击报复的，以及对本地方、本部门、本单位发生的严重人口普查违法行为失察的，由任免机关或者监察机关依法给予处分，并由县级以上人民政府统计机构予以通报；构成犯罪的，依法追究刑事责任；

二是人口普查机构不执行普查方案的，伪造、篡改人口普查资料的，要求人口普查对象提供不真实的人口普查资料的，未按照普查方案的规定报送人口普查资料的，违反国家有关规定造成人口普查资料毁损、灭失的，泄露或者向他人提供能够识别或者推断单个普查对象身份的资料的，由本级人民政府或者上级人民政府统计机构责令改正，予以通报。对直接负责的主管人员和其他直接责任人员，由任免机关或者监察机关依法给予处分。对有上述违法行为之一的普查人员，责令其停止执行人口普查任务，予以通报，依法给予处分；

三是人口普查对象拒绝提供人口普查所需的资料，或者提供不真实、不完整的人口普查资料的，由县级以上人民政府统计机构责令改正，予以批评教育。人口普查对象阻碍普查机构和普查人员依法开展人口普查工作，构成违反治安管理行为的，由公安机关依法给予处罚。

第七次全国人口普查期间，国家统计局和各地县级以上人民政府统计机构将设立举报电话和信箱，接受社会各界对人口普查违法行为的检举和监督。（来源：北京日报）

➢ 中国互联网协会发布《防范未成年人沉迷网络倡议书》

2020 年 6 月 2 日，为保护未成年人健康成长，防范网络沉迷，中国互联网协会积极发

挥行业组织的平台纽带作用，于 2020 年 6 月 1 日主办了“防范未成年人沉迷网络公益公开课”，并公开发布了《防范未成年人沉迷网络倡议书》，以多元共治的指导思想，倡导全社会共同关注未成年人网络沉迷问题，多方协同、综合施策，为未成年人营造晴朗的网络环境，共同守护未成年人的健康成长。

近年来，因未成年人沉迷网络引起的社会矛盾凸显，引发社会普遍关注。为展现社会主流价值观，营造积极向上的网络文化环境，切实保护未成年人身心健康、防范网络沉迷，中国互联网协会向全国互联网业界、广大家长发出如下倡议：

一、网络服务提供者应自觉遵守国家法律、法规，大力弘扬社会主义优秀传统文化和道德准则，推进网络文明建设，努力提供健康绿色的网络文化产品和信息内容服务，为未成年人健康成长提供良好的网络环境。

二、网络游戏运营企业应完善未成年人保护机制建设，利用新一代互联网技术强化网络游戏防沉迷实名验证，切实履行网络游戏运营企业的社会责任。

三、网络视频平台、网络直播平台应认真履行平台监管责任，利用技术有效遏制网络不良信息的制作和传播，大力弘扬社会主义优秀文化和精神文明，不断提高网络主播等从业人员的职业素养，自觉接受公众监督，共建共享清朗网络空间。

四、新闻媒体及网络服务提供者应加强对全社会的正面引导和宣传，树立尊重、保护、教育未成年人的良好风尚，推广预防未成年人网络沉迷的有效手段，号召家长、学校共同履行未成年人监护和守护责任。

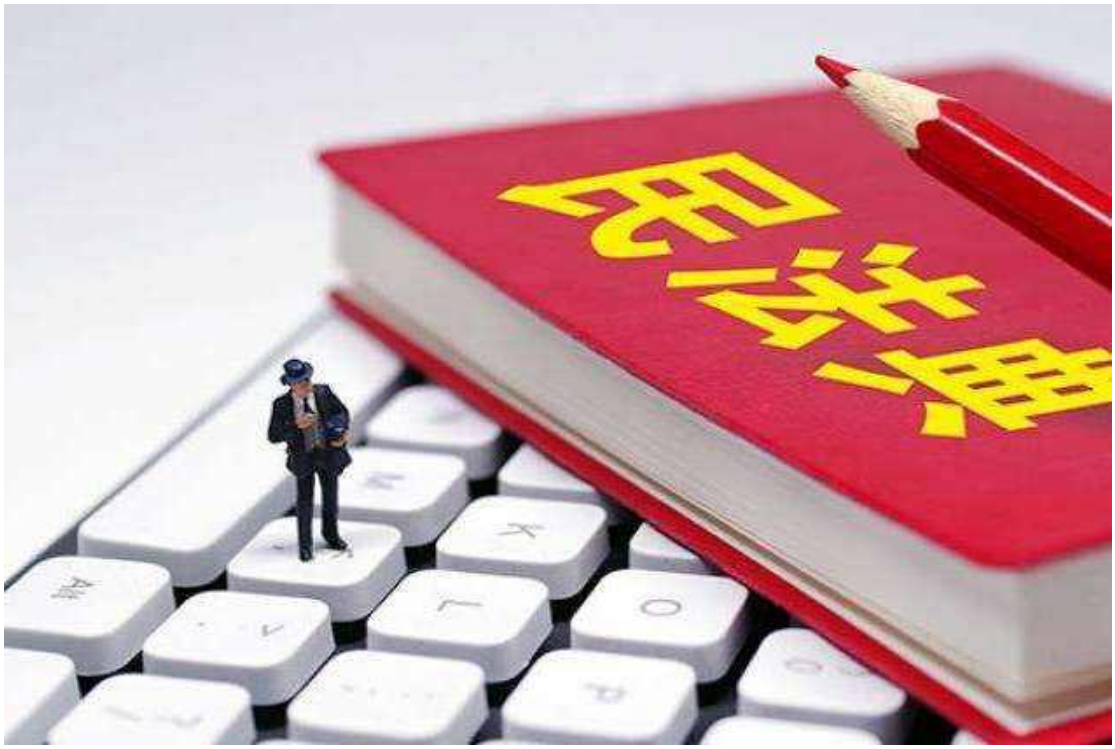
五、呼吁家长关注未成年人生理、心理状况和行为习惯，引导未成年人进行有益身心健康的活动，预防和制止未成年人沉迷网络游戏等不良行为。

防范未成年人沉迷网络需要企业、媒体、学校和家庭等社会各界共同努力，让我们携起手来，为未成年人营造清朗的网络空间，共同守护未成年人的健康成长，培养有理想、有道德、有文化、有纪律的社会主义建设者和接班人。

目前，《防范未成年人沉迷网络倡议书》已得到 31 个省、自治区、直辖市互联网协会，以及基础运营企业、网络服务提供者、网络游戏运营企业、网络视频平台、网络直播平台、新闻媒体等 157 家单位的积极响应和全力支持。（来源：新华网）

➢ 《中华人民共和国民法典》正式通过

2020 年 5 月 28 日，第十三届全国人民代表大会第三次会议通过《中华人民共和国民法典》，标志着我国正式进入“民法典时代”。民法典共 7 编，依次为总则编、物权编、合同编、人格权编、婚姻家庭编、继承编、侵权责任编以及附则，共 1260 条。



其中，《民法典》第 1019 条规定了肖像权的消极权能，明确不得“利用信息技术手段伪造等方式侵害他人的肖像权”，回应了当前利用各种网络信息技术手段非法侵害他人肖像权的社会现实。

隐私权和个人信息保护方面，《中华人民共和国民法典》第 1034 条规定，自然人的个人信息受法律保护。个人信息中的私密信息，适用有关隐私权的规定；没有规定的，适用有关个人信息保护的规定。《民法典》将个人信息的收集、存储、使用、加工、传输、提供、公开等行为统称为个人信息的处理，对信息处理者的个人信息保护义务加以明确。（来源：中国人大网）

- **《中华人民共和国民法典》全文**
- http://www.npc.gov.cn/npc/c30834/202006/75ba6483b8344591abd07917e1d25cc8.shtml

➢ 八部门集中开展网络直播行业专项整治行动

2020 年 6 月 5 日，针对网民反映强烈的网络直播“打赏”严重冲击主流价值观等行业突出问题，即日起，国家网信办、全国“扫黄打非”办会同最高人民法院、工业和信息化部、公安部、文化和旅游部、市场监管总局、广电总局等部门启动为期半年的网络直播行业专项整治和规范管理行动。此次集中行动不仅要坚决有效遏制行业乱象，也要科学规范行业规则，促进网络生态持续向好。近日，根据群众举报线索并经核查取证，首批依法依规对“皇冠直播”“嗨够直播”“UP 直播”“月爱直播”等 44 款传播涉淫秽色情、严重低俗庸俗内容的违法违规网络直播平台，分别采取约谈、下架、关停服务等阶梯处罚；部署查办了一批利用色情低俗直播内容诱导打赏案例，对“幺妹直播”“触手直播”“9158 美女视频”“喵播”“么么直播”“蜜桃直播”“啵比直播”等平台传播网络低俗直播内容作出行政处罚。

近几年来，网络直播行业虽然得到了有效治理和规范管理，但一些中小型直播平台依然乱象频出。尤其在新冠肺炎疫情期间，全国大多数网民上网时长明显增多，有的直播平台利用这一时机，为追求流量、吸引眼球，任由主播穿着暴露、言语粗俗、行为恶劣，通过“送福利”、低俗表演、下流动作等方式吸引用户进行高额打赏，甚至诱导未成年人进行充值打赏，所涉及的举报案例居高不下；有的直播平台主播向网民兜售三无产品、假冒伪劣商品等，严重侵犯消费者合法权益，扰乱正常网络购物市场秩序；有的直播平台主播大肆宣扬历史虚无主义和拜金主义错误思潮，散布谣言信息，传播封建迷信，发表负面言论，甚至从事网络诈骗等违法犯罪活动；更有一些从事淫秽色情和网络赌博的直播平台，通过社交群组和论坛传播有害链接和二维码，公然招募从事色情直播从业人员，传授躲避网络侦查方法等。网络直播平台的这些违法违规行为，严重破坏了网络生态，对青少年的健康成长带来恶劣影响，必须坚决予以治理。

针对违法违规网络直播平台开展专项整治，遏制行业乱象，督促企业落实主体责任，最终目的是为了促进行业健康有序发展。国家网信办、全国“扫黄打非”办将会同有关部门，坚持标本兼治、管建并举，在进行专项整治的同时，科学制定推动网络直播行业高质量发展的管理规则和政策导向，探索实施网络直播分级分类规范，以及网络直播打赏、网络直播带货管理规则，形成激励正能量内容供给的网络主播评价体系，严厉打击违法违规直播行为，严肃追究相关直播平台责任，进一步营造积极健康、营养丰富、正能量充沛的网络直播空间。

（来源：国家互联网信息办公室）

五、本期重要漏洞实例

➢ WordPress SiteOrigin Page Builder 插件代码执行漏洞

发布日期：2020-05-28
更新日期：2020-05-29
受影响系统：WordPress SiteOrigin Page Builder < 2.10.16
描述：

CVE(CAN) ID: CVE-2020-13643
SiteOrigin Page Builder 是 WordPress 的页面创建插件。
SiteOrigin Page Builder 2.10.16 之前版本插件，live editor 功能未验证任何 nonce，在实现上存在安全漏洞，通过 live_editor_panels_data $_POST 变量，攻击者可利用此漏洞执行恶意 JavaScript 代码。
建议：

厂商补丁：
WordPress
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://wordpress.org/plugins/siteorigin-panels/#developers
参考：
https://www.wordfence.com/blog/2020/05/vulnerabilities-patched-in-page-builder-by-siteorigin-affects-over-1-million-sites/

➢ IBM Security Identity Governance and Intelligence 信息泄露漏洞

发布日期：2020-05-28
更新日期：2020-05-29
受影响系统：IBM Security Identity Governance and Intelligence（IGI） 5.2.6
描述：

CVE(CAN) ID: CVE-2020-4246
IBM Security Identity Governance and Intelligence（IGI）是一套身份管理解决方案。IBM Security IGI 5.2.6 版本，在处理 XML 数据中存在 XML 外部实体注入安全漏洞，攻击者可利用该漏洞获取敏感信息或耗尽内存资源。
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://exchange.xforce.ibmcloud.com/vulnerabilities/175481

https://www.ibm.com/support/pages/node/6207902

➢ OpenStack Keystone 信息泄露漏洞

发布日期：2020-05-06
更新日期：2020-05-21
受影响系统：
openstack Keystone < 15.0.1
openstack Keystone 16.0.0
描述：

CVE(CAN) ID: CVE-2020-12691
OpenStack Keystone 是一个身份认证服务。OpenStack Keystone 15.0.1 之前版本、16.0.0 版本在实现中存在权限管理安全漏洞。任何经身份验证的用户均可创建自己的项目 EC2 凭证，从而冒充其他用户。攻击者可利用该漏洞以管理员身份在项目上执行操作，获取全局管理员权限。
建议：

厂商补丁：
openstack
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：
http://lists.openstack.org/pipermail/openstack-announce/

➢ QEMU megasas_lookup_frame 越界读取漏洞

发布日期：2020-05-27
更新日期：2020-05-29
受影响系统：QEMU QEMU 4.2.0
描述：

CVE(CAN) ID: CVE-2020-13362
QEMU（Quick Emulator）是一套模拟处理器软件。QEMU 4.2.0 版本，hw/scsi/megasas.c 中 megasas_lookup_frame 在实现中存在越界读取安全漏洞，通过构造的 reply_queue_head 字段，攻击者可利用此漏洞获取敏感信息。
建议：

厂商补丁：QEMU
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：
http://www.openwall.com/lists/oss-security/2020/05/28/2
https://lists.gnu.org/archive/html/qemu-devel/2020-05/msg03131.html
https://lists.gnu.org/archive/html/qemu-devel/2020-05/msg06250.html

六、本期网络安全事件

➢ 泰国移动运营商泄露 83 亿互联网记录

2020 年 5 月 25 日，研究人员发现了泰国移动运营商 Advanced Info Service (AIS)子公司控制的一个 ElasticSearch 数据库可公开访问，数据库包含大约 83 亿记录，容量约为 4.7TB，每 24 小时增加 2 亿记录。

研究人员发现，这个数据库在 2020 年 5 月 1 日首次被公开，并可以公开访问。大约 6 天后，这名研究人员发现了这个数据库。在漏后的大约 3 周时间里，数据库的数据量显著增长，每 24 小时就会添加 2 亿行新数据。截至 2020 年 5 月 21 日，数据库中存储了 8,336,189,132 个文档，这些数据是 NetFlow 数据和 DNS 查询日志的组合。数据量大得有点惊人，这意味着许多人的网络隐私被毫无保护地暴露到了公共场合。DNS 即域名系统，它作为将域名和 IP 地址相互映射的一个分布式数据库，能够使人更方便地访问互联网。

Name	Health	Status	Primaries	Replicas	Docs count	Storage size
dns-2020.05.02-01	green	open	3	1	114493031	25.5gb
dns-2020.05.04-20	green	open	3	1	68374033	16.9gb
dns-2020.05.04-19	green	open	3	1	66893803	16.6gb
dns-2020.05.04-18	green	open	3	1	65731040	16.4gb
dns-2020.05.04-23	green	open	3	1	63718868	15.1gb
dns-2020.05.04-21	green	open	3	1	63340671	15.5gb
dns-2020.05.05-01	green	open	3	1	61466058	14.7gb
dns-2020.05.05-00	green	open	3	1	60199790	14.3gb
dns-2020.05.04-22	green	open	3	1	59969654	14.5gb
dns-2020.05.07-12	green	open	3	1	58387485	14.1gb
dns-2020.05.07-13	green	open	3	1	58234563	14gb
dns-2020.05.04-17	green	open	3	1	58213586	14.4gb
dns-2020.05.07-11	green	open	3	1	56762926	13.7gb
dns-2020.05.07-05	green	open	3	1	56600905	13.7gb
dns-2020.05.04-15	green	open	3	1	56230332	13.7gb
dns-2020.05.04-16	green	open	3	1	56015268	13.8gb
dns-2020.05.07-06	green	open	3	1	55990237	13.7gb
dns-2020.05.07-07	green	open	3	1	55760186	13.6gb
dns-2020.05.04-12	green	open	3	1	54863708	13.2gb

简单来说，每一个网站都有一个独立 IP，但是 IP 记起来太复杂，所以就有了 DNS，我们只需要输入网址，DNS 就会自动查找相应的 IP 地址。查询 DNS 记录，就能看到每个 IP 访问的地址，将相关的 IP 信息汇总起来，就能轻易建立起一个人的用户画像。

通过单个 IP 地址的 NetFlow 记录，别人可以轻易查看到这个 IP 访问各类网页和应用程序的流量，从而得知你最常访问的网页和应用，比如抖音、微信。然后再通过这个 IP 的 DNS 查询记录，还能知道这个 IP 对应的个人/家庭的一些详细信息。

AIS 是泰国最大的 GSM 移动运营商，用户约有 4000 万。该研究人员多次联系 AIS 未果，后又找到能与 AIS 联系的泰国国家 CERT 团队(ThaiCERT)，成功确保了数据库的安全。与此同时，他也给普通用户提供了一些保护个人隐私的建议。（来源：solidot）

➢ 深圳某企业遭黑客入侵，报案反被行政警告处罚

2020 年 6 月 2 日报道，今年 4 月，位于深圳宝安的两家企业遭遇境外黑客入侵，且被勒索用支付比特币来解密系统，宝安网警侦查发现，涉案公司存在大量的网络漏洞和安全问题，按照“净网 2020 专项行动”的要求启动“一案双查”，以不履行网络安全义务，违反《网络安全法》给予该两家公司行政警告处罚。

以其中丰顺县培英电声有限公司深圳分公司为例，4 月 23 日下午，宝安公安分局网警大队联合镇南派出所一同到丰顺县培英电声有限公司深圳分公司进行网络安全检查。经检测，发现公司网络服务器存在系统防火墙未开启、远程连接未限制访问 IP、域控未配置安全

密码策略等多个问题，且该公司还存在违反《中华人民共和国网络安全法》的情况。

记者从网警方面了解到，涉事企业虽属被入侵方也是受害者，但侦查过程中发现涉事企业存在大量的网络漏洞和安全问题，比如存储服务器数据的机房安全责任人，只是一名仅懂得计算机基本操作知识的保安员，企业本身的安全防护网络，被第三方技术检测出几十个漏洞……

《网络安全法》第二十一条规定，国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。该规定具体包括五条细则，其中（一）为制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；（二）是采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施。

实际上，早在 2018 年 8 月 17 日，公安部宣布针对网络乱象，公安机关已实行“一案双查”制度，即在对网络违法犯罪案件开展侦查调查工作时，同步启动对涉案网络服务提供者法定网络安全义务履行情况的监督检查。该案中，按照“净网 2020 专项行动”的要求启动“一案双”查，宝安网警以不履行网络安全义务，违反《网络安全法》给予该两家公司行政警告处罚。

宝安网警大队民警翟文强表示：深圳是作为改革开放前沿阵地，先行示范区，互联网企业众多、产业成熟，也不缺网络安全相关的技术和能力，缺的只是对网络安全和自身责任的认识，不少企业往往重视产品端、对网络安全防护等技术后段缺乏足够的重视意识。

翟文强表示，遇到网络安全事件，公安机关不但要侦查破案，作为执法者和监督者，也有义务通过严格执法，督促督导企业合法合规履行网络安全义务，提升企业在网络安全防护方面的意识和水平，对于不履行不重视网络安全义务的企业，有必要依法依规通过行政处罚等手段，来让企业明白网络安全的重要性。

行业人士竞远安全深圳分公司总经理刘礼则认为：对于部分企业遇到的一些网络安全事件，其主要原因在于网络安全意识薄弱，缺乏必要的网络安全专业人员、安全管理制度及网络安全防护措施等。针对此类事件，企业需建立“事前预防-事中控制-事后治理“三位一体的网络安全体系，做到日常防范要到位，培训演练不能少，发现问题及时改，紧急情况先上报。并且在遇到黑客入侵事件后，第一时间按照网络安全应急预案操作等。

刘礼认为，首先建议相关企业应配备专业的网络安全技术人员至少一名，做好专业的防护检测，定期备份企业重要数据，能够及时主动更新补丁修复漏洞。其二，企业应加强其内网权限的管控，及时清除公司内网多余账号，防止黑客从公司内部攻击。其三，建立相关网

络安全管理制度，并根据实际情况不断完善及更新其管理制度，做好管理制度的落实工作。其四，应在企业内外网部署相关网络安全防护产品、入侵检测设备，并配备网络安全应急支撑单位。其五，在日常工作中制定网络安全应急预案，通过应急演练、员工培训等方式把网络安全意识落到实处。其六，当企业用户遇到黑客及病毒攻击时，需要第一时间保存好相关日志和入侵记录，同时联系应急支撑单位和公安机关，在其指导下开展工作，不擅自操作。（来源：南方都市报）

➢ 澳大利亚黑客在 Twitter 上发布苹果员工机密信息后被判缓刑

2020 年 6 月 4 日，一名澳大利亚男子因从苹果公司的服务器中提取员工资料并在 Twitter 上发布，被判处 5000 澳元的罚款和 18 个月的观察期。据 Bega 地区新闻报道，24 岁的 Abe Crannaford 周三在伊甸园当地法院出庭接受宣判，此前他在 2 月份对两项未经授权访问或修改受限数据的罪名表示认罪。

在 2017 年中和 2018 年初，Crannaford 从这家总部位于美国的大型企业中提取了仅针对员工的受限信息。2018 年 1 月，Crannaford 在其 Twitter 账号上发布员工信息，并据称在 GitHub 上提供了该公司固件的链接，让这起黑客事件达到了高潮。

裁判官道格-迪克对他处以 5000 美元的罚款，然而他并没有对 Crannaford 进行判刑，而是给予他 18 个月的观察期，如果在观察期内违反了相关规定，将导致额外的 5000 美元罚款。

Crannaford 的辩护律师 Ines Chiumento 辩称，苹果公司通过其赏金计划奖励寻找漏洞

和 bug 的黑客，在某种意义上 促进了黑客的发展。检察官承认苹果公司存在悬赏计划，但称 Crannaford 多次入侵网站，并与他人共享受限数据，苹果公司的悬赏的概念与 Crannaford 的行为背道而驰。（来源：cnBeta）

➢ 北京某安全公司技术员利用网络敲诈勒索比特币 获刑 3 年

2020 年 6 月 3 日，北京海淀法院报道，北京某安全技术公司技术员潘某利用网络敲诈勒索比特币，造成被害公司经济损失 20 余万元。检方以敲诈勒索罪将被告人潘某公诉至法院。海淀法院以敲诈勒索罪判处被告人潘某有期徒刑 3 年，并处罚金 5000 元。

2016 年 8 月初，被告人潘某因急需用钱，开始通过 DDOS 攻击网站，造成网站系统瘫痪后向网站运营商勒索财物。当攻击行为成功后，潘某通过互联网向网站运营商发送电子邮件，以不给付比特币就继续网络攻击相威胁，向被害单位河北某大宗商品交易公司、安徽某大宗商品电子商务公司勒索比特币。8 月 3 日，河北某大宗商品交易公司被迫支付 7 万余元，两次购买并给付潘某比特币攻击 22 个;8 月 8 日，安徽某大宗商品电子商务公司被迫支付 15 万余元，四次购买并给付潘某比特币共计 40 个。上述比特币最终存入潘某指定的网络地址内。同年 8 月中旬，潘某以同样方式向被害单位北京某云商收藏品公司勒索比特币 40 个未果。案件犯罪既遂金额共计 23 万余元。

庭审中，检方针对上述指控事实出示了相关证据材料，包括潘某的供述、证人证言、敲诈邮件、比特币地址信息、转账记录、购买比特币记录、QQ 聊天记录等。被告人潘某对上述指控事实及罪名未提出异议。但提出比特币系虚拟货币，在我国不受法律保护，不应以被害单位购买比特币价格作为认定案件数额巨大的依据，并对其量刑。

法院经审理后认为

被告人潘某以非法占有为目的，通过非法手段攻击被害单位网络交易平台，致交易平台无法正常登录后，向被害单位勒索比特币，造成被害单位因购买比特币所致的数额巨大的直接财产损失，其行为已构成敲诈勒索罪，应予惩处。

针对被告人潘某就犯罪数额所提出的意见，法院认为：首先，在被告人潘某犯罪期间，比特币仍为在网络上可自由交易的“虚拟货币”，其交易价格在短期内较为稳定、一致，故认定被告人潘某对自己可获取的收益金额系明知。其次，被害单位购买潘某索要的比特币在比特币交易网站上实际支付了货币，造成数额巨大的财产损失。故综合考虑主客观两方面，以犯罪期间比特币的交易价格认定犯罪数额具有合理性。

最终，法院作出上述判决。法院在案冻结潘某的招商银行账户内存款，退赔被害单位河北某大宗商品交易公司 7.9 万余元，退赔被害单位安徽某大宗商品电子商务公司 15.5 万余元，剩余款项折抵罚金后予以没收。此外，因比特币大幅升值，案件生效后，法院在政策允许期间，将潘某账户内被冻结的比特币及部分莱特币交易卖出后，所得交易款不仅弥补了被害单位全部损失，而且仍有部分款项用于折抵罚金及没收。

法官提示：比特币作为一种网络虚拟财产，属于刑法保护的财物范围，行为人以非法占有为目的，敲诈勒索比特币的行为符合敲诈勒索罪的构成要件。因本案行为人并未出售敲诈勒索所得的比特币，因此犯罪数额以比特币的交易价格作为认定标准。（来源：北京海淀法院）

➢ 台当局内务部门疑遭黑客入侵 2000 万笔个人信息被网上售卖

2020 年 6 月 4 日，台当局内务主管部门日前疑似遭黑客入侵，导致台湾超过 2000 万笔的个人信息被放在网络贩售。

据台媒报道，有境外信息安全网站发现，在透过特殊方式才可以连接上的暗网中，有一个叫做“台湾房屋登记数据库”的档案，大小约 3.5GB，其中有超过两千万笔台湾民众个人资料，内容包含姓名、地址、身分证字号等等。这些资料都是同一名黑客流出，表示来源是

台湾内务主管部门官方网站，资料当中最后登记的出生年为 2008 年。台湾行政事务主管部门对此表示，相关单位调查中。

事实上，台当局被黑客入侵也不是第一次了。2019 年台北市卫生局，超过两百万笔个人信息被窃取；2018 年内务主管部门新式身份证，票选活动网页遭人窜改；2012 年内务主管部门不动产实价登录，查询网被攻击瘫痪。

不过这次透过境外信息，才得知岛内又发生个人信息泄露外泄，也让外界质疑台当局有关部门是否慢半拍，信息安全防护问题存在漏洞。（来源：中国台湾网）

➢ 快递公司员工参与出售 2 万余条公民个人信息获刑并禁业

2020 年 6 月 3 日，两会期间,公民个人信息保护引起代表委员广泛关注。信息时代,个人信息泄露现象较为突出,骚扰电话、垃圾短信滋扰人民群众正常生活,有的甚至陷入诈骗案件,成为社会痛点难点问题。山东省曲阜市检察院就对一起侵犯公民个人信息认罪认罚案件提起公诉,提出从业禁止量刑建议,得到法院支持。5 月 29 日,被告人黄某被判处有期徒刑三年三个月,并处罚金人民五万元,禁止自刑罚执行完毕之日或者假释之日起三年内从事快递、物流等接触公民个人信息的相关职业。

2017 年 9 月,黄某到广州市某一快递公司工作,案发前负责该公司在广州南片区的快递

业务销售工作。张某(另案处理)是黄某公司同事,为黄某负责销售辖区的某快递站站长。

2018 年 10 月份,张某因手头紧张,网上有借款,就萌生出售客户个人信息赚钱的想法,通过贴吧联系买方,用 QQ 号传输相关公民个人信息截图,收取钱款。因公司系统升级,张某权限受限,同年 11 月份,张某遂找到黄某。黄某的公司系统账号对每日导出信息没有数量限制,且可以查询权限内所提供商户所有快递信息。黄某知情后表示同意,并与张某约定好分成,按售卖信息条数分钱,每条收取 1-2 元不等。获取信息便利了,张某出售信息更加肆无忌惮,数量多时每日出售客户个人信息达上千条。截至案发,黄某共参与出售公民个人信息 2 万余条,涉案金额近 13 万元。

2019 年 3 月,曲阜市公安局办案民警在工作中发现辖区存在买卖公民个人信息情况,遂顺藤摸瓜,将黄某查获。该院经审查后,以黄某涉嫌侵犯公民个人信息罪向曲阜市人民法院提起公诉,黄某表示认罪认罚,根据犯罪性质及危害程度,承办检察官提出精准量刑建议,并建议适用从业禁止,法院对量刑建议完全采纳。（来源：网易）

信息安全意识产品服务

021-33663299